Installation Manager

Help Guide

Version 1.23

March 2023

Anthology Inc.

5201 Congress Avenue
Boca Raton, FL 33487
Main: +1.561.923.2500
Support: +1.800.483.9106
www.anthology.com

Revision History

Rev.	Date	Description
01	Apr. 2021	Initial release of document for Installation Manager Version 1.23. See What's New.
02	Jul. 2021	Updates for Installation Manager 1.23. See What's New.
03	Sep. 2021	Updates for Student Analytics 5.2. See What's New.
04	Sep. 2021	Updates for CampusNexus CRM 14.0. See What's New.
05	Mar. 2022	Updates for Anthology Student Analytics 5.3.0. See What's New.
06	Apr. 2022	Updates for Workflow Composer 4.0.1. See What's New.
07	Jun. 2022	Updates for Workflow Composer 4.0.2. See What's New.
08	Aug. 2022	Updates for CampusNexus CRM 14.1. See What's New.
09	Sep. 2022	Updates for Analytics 5.4. See What's New.
10	Dec. 2022	Updates for Analytics 5.5. See What's New.
11	Mar. 2023	Updates for CampusNexus CRM 14.2. See What's New.

Contents

Get Started

Installation Manager is a user-friendly desktop application for installing Anthology Inc. products. This Help system assists users in recognizing and using the features of this application. For information about installing this application, see Installation Manager.

After you have installed Installation Manager, install the Anthology Inc. products you have purchased. For installation instructions, see the menu items above.

What's New

Installation Manager Version 1.23

CampusNexus CRM 14.2

- Minimum System Requirements - multiple updates
- Added Talisma-ClearPhoneSessions SQL job
- Updated details for Talisma-PurgeOldNotfns SQL job
- Updated Purpose of Talisma-Maint SQL job
- Services: Updated default port number for Chat Service Options to 8086.

Analytics 5.5

- Hardware/ Software Requirements: attached Analytics 5.5.0 Size Estimation Worksheet.xlsx

Analytics 5.4

- Added section Analytics for On-Prem and PaaS.
- Removed outdated section "Analytics for PaaS".
- Hardware/Software Requirements: attached Analytics 5.4.0 Size Estimation Worksheet.xlsx

CampusNexus CRM 14.1

- Minimum System Requirements - multiple updates
- Web Client
    - Added content to Postinstallation Tasks: "If SQL Server is running on the same computer as the Web Client web server..."
- Upgrades:
    - Added step "Apply the following scripts on the Main Database computer..."
- CRM Jobs on SQL Server
    - Added "Clean-up of Rule logs" to Purpose of Talisma-Maint job.
    - Added Talisma-CampaignCommunication-ProcessTempRecords.
- Added Configuring Web Components on a Demilitarized Zone.
- Revised:

- Postinstallation Tasks for Chat
- Student Web Client
- Upgrades

- Removed the "Knowledge Base" topic.

Workflow Composer 4.0.2

- The Windows security message is no longer displayed when installing Workflow Composer using the Click-Once application. See Install Using ClickOnce.
- The nlog.config file no longer exists (see NLog). The NLog configuration settings have been placed in the app config file (WorkflowComposer.exe.config).

Workflow Composer 4.0.1

- Workflow Composer 4.0.1 introduces the option to change the configuration upon launching the application. See Workflow Composer Installation.

Analytics 5.3

- Permissions: Installing Student Analytics enables the “Change Data Capture” feature on the Student DB and creates a user “cdc” and assigns the db_owner group level permission.
- Run the Initial ETL Job: Student Analytics 5.3.0 provides an option to run the initial load process in two steps.
- Hardware/Software Requirements: attached Analytics 5.3.0 Size Estimation Worksheet.xlsx

CampusNexus CRM 14.0

- Upgrades:
  - Added steps 22, 23, and 24.
  - Removed "Move Proactive Chat Information to the Main Database"
  - Removed "Before upgrading to version 11.0.0, perform the following steps on the Application Server... "
- Minimum System Requirements: Updated .NET Framework requirement from 4.7.2 to 4.8.
- Minimum System Requirements: Removed support for:
  - Microsoft SQL Server 2016
  - Windows 2012 R2
  - Excel 2013

    - Word 2013 SP1
    - IIS Servers 8.0 and 7.5

- Web Client: Added note on the Web Client Settings screen reminding users to verify all settings.
- Removed content related to Customer Portal. This component is deprecated with CampusNexus CRM 14.0.
- Student Web Client: Added note about upgrading Web Client and iServices.
- Other Jobs: Added SQL jobs "Talisma-ApplicationMonitoring" and "Talisma-TableMonitoring".

Analytics 5.2

- Added prerequisite check for "SQL server 2017 CU 23" on the Anthology Student Data Warehouse. See Prerequisites and Requirements.
- Added "Contact Manager" to the SIS Semantic Model options.
- Renamed SQL server jobs for ETL from "CampusAnalytics" to "StudentAnalytics". See Run the Initial ETL Job, Manage Jobs, and Configure AcademicYearOffset, FiscalPeriodMonthOffset, and CleanupRetentionDays.
- Hardware/Software Requirements: attached Analytics 5.2.0 Size Estimation Worksheet.xlsx

Installation Manager Prerequisites

The Installation Manager application is a single user interface for installing and managing Anthology products. Its integrated Package Manager enables users to download installation packages for the products to be installed. Access to the installation packages is controlled via a unique customer identification key.

The Installation Manager setup process can only be performed after certain requirements are met. These prerequisites must be met on the local machine and/or target machine, depending upon the method of installation.

⚠	The machine where Installation Manager is installed must have Internet connectivity so that the installation packages for the products to be installed can be downloaded.

Note: Installing to a target machine located in a DMZ (demilitarized zone) is not supported from a machine outside the DMZ (if the required ports are not open on the DMZ machine). If you are going to install to a machine in the DMZ, you must run Installation Manager on that machine.

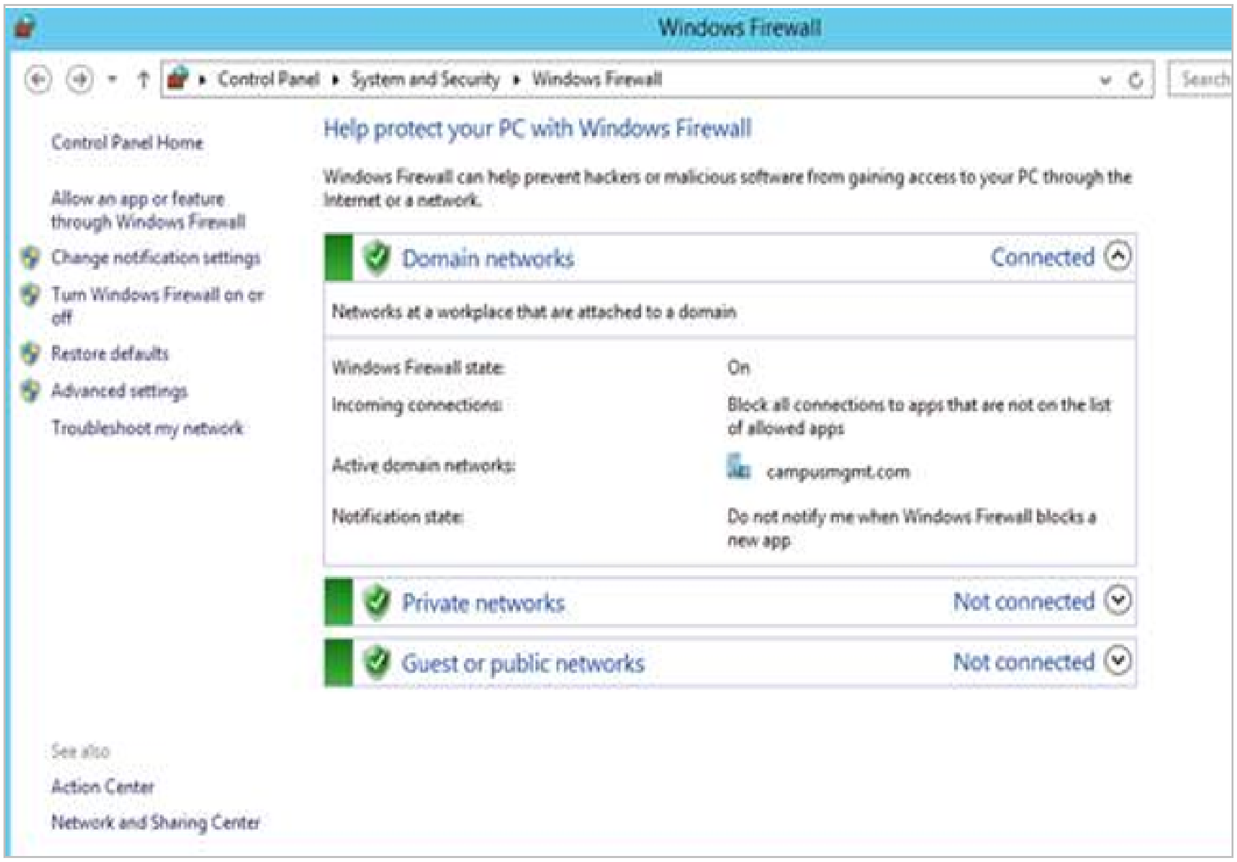
Prerequisites

1. Make sure that the local and/or target machines use **.NET Framework 4.5**.
2. The Windows Firewall *service* (see Administrator Tools > Services) needs to be set to **enabled**, but the Windows Firewall must be turned **off**. This step must be executed on all systems except for a dedicated SQL Database Server.

   To turn off the Windows Firewall

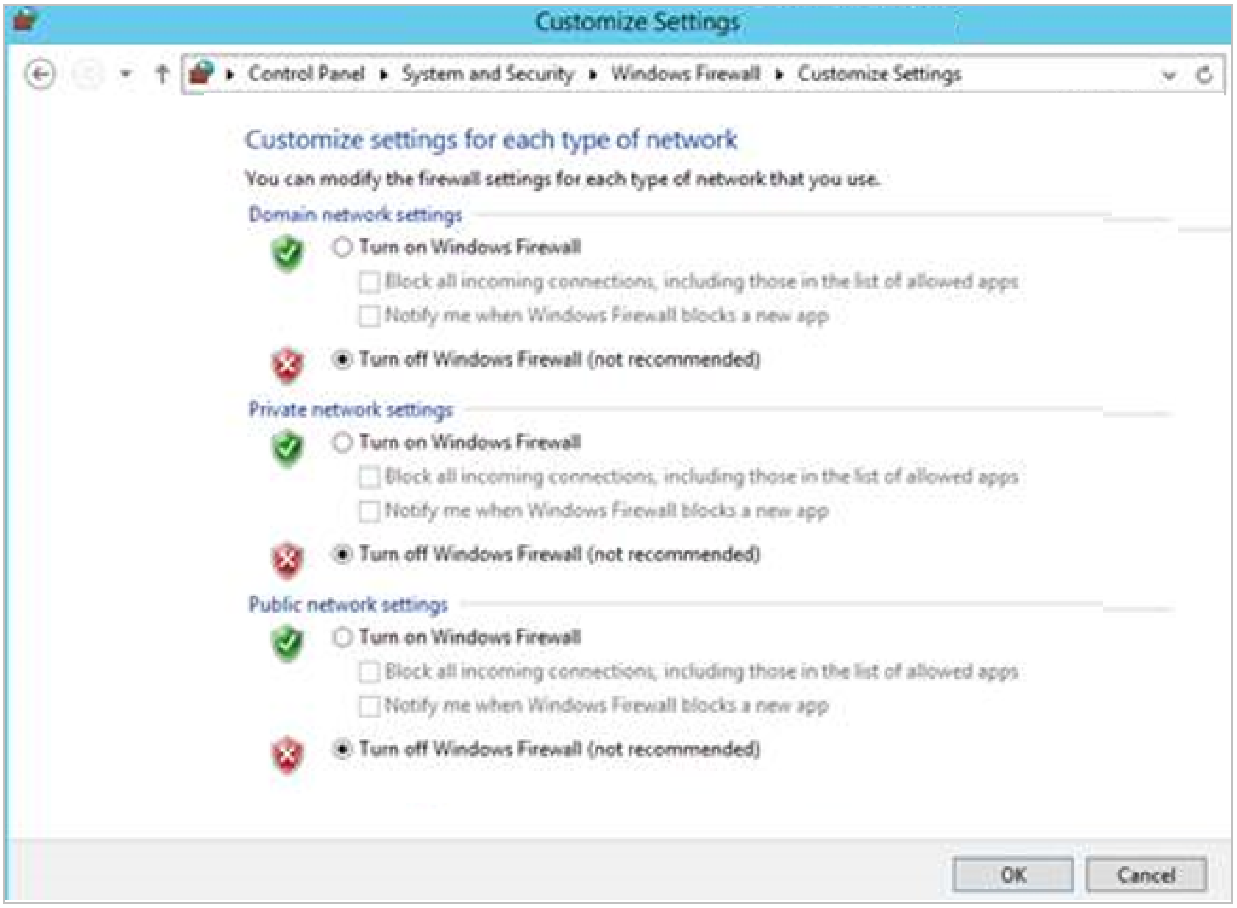
   a. Navigate to **Control Panel > System and Security > Windows Firewall**.

   b. Click the **Turn Windows Firewall on or off** link in the left-hand menu.



c. In the Customize Settings window, select the **Turn off Windows Firewall** option in the following sections:

- Domain network location settings
- Home or work (private) network location settings



d. Click **OK**.

e. Close the Control Panel > Windows Firewall window.

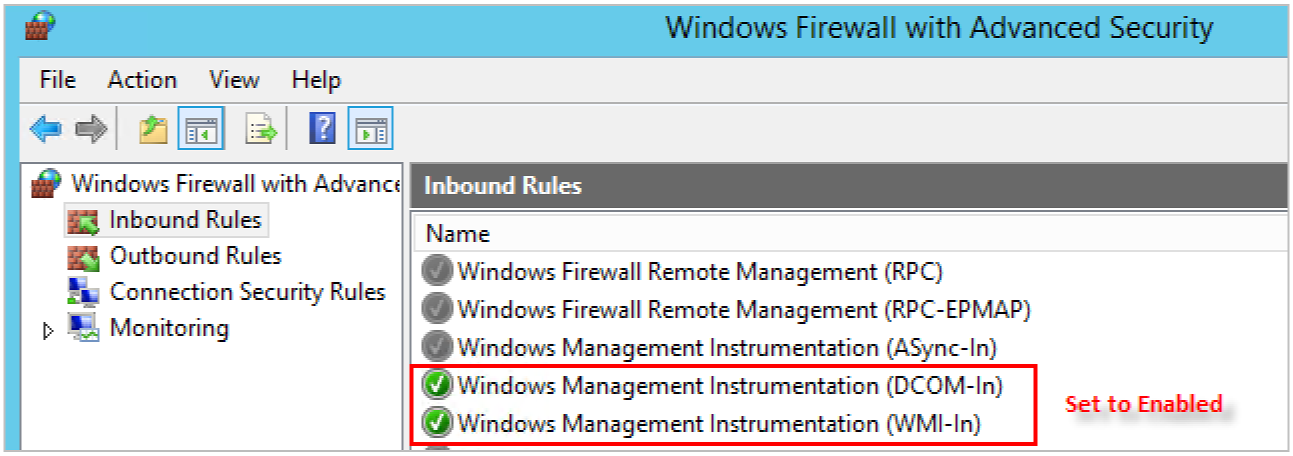
3. In cases where the firewall cannot be turned off, the following ports must be open and Windows Management Instrumentation (WMI) predefined rules must be enabled on any target machine to which you are installing components:

Ports Used by Installation Manager

Port Definition	Port Number	Comments
TCP	139	These ports are used by Windows File Sharing. For more information, see "Understanding Shared Folders and the Windows Firewall" at https://technet.microsoft.com/en-us/library/cc731402.aspx. **Note**: The WF.msc has a predefined rule for Windows File Sharing.
TCP	445	
UDP	137	
UDP	138	
TCP	8889-8890	Installation Manager Agent

Port Definition	Port Number	Comments
MSSQL	1433	Port 1433 (default SQL port) or any custom port that is configured for SQL communications must be open if the target machine is an SQL Server.

The pre-defined rules (Windows Management Instrumentation (DCOM-In) and Windows Management Instrumentation (WMI-In)) in Windows Firewall Configuration have to be enabled.



4. Disable the **"User Account Control: run all Administrators in admin approval mode"** Security Policy in Local Security Policy under Local Policies, Security Options.

5. Reboot the appropriate machines.

6. Installation Manager requires unique keys tied to the installation packages available to particular customers to ensure that incorrect, outdated, or inappropriate packages are not installed. To obtain a customer key, call Anthology Inc. Customer Support at **1-800-483-9106**.

Note: The Installation Manager log file provides information on the current configuration status.

Start

Once Installation Manager has been installed, Installation Manager enables you to choose an Anthology Inc. product and perform the installation using a GUI instead of command prompts.

Important: Only persons with the proper permission can perform this installation. If you are not sure you have all the permissions needed, contact your system administrator.

Prerequisites

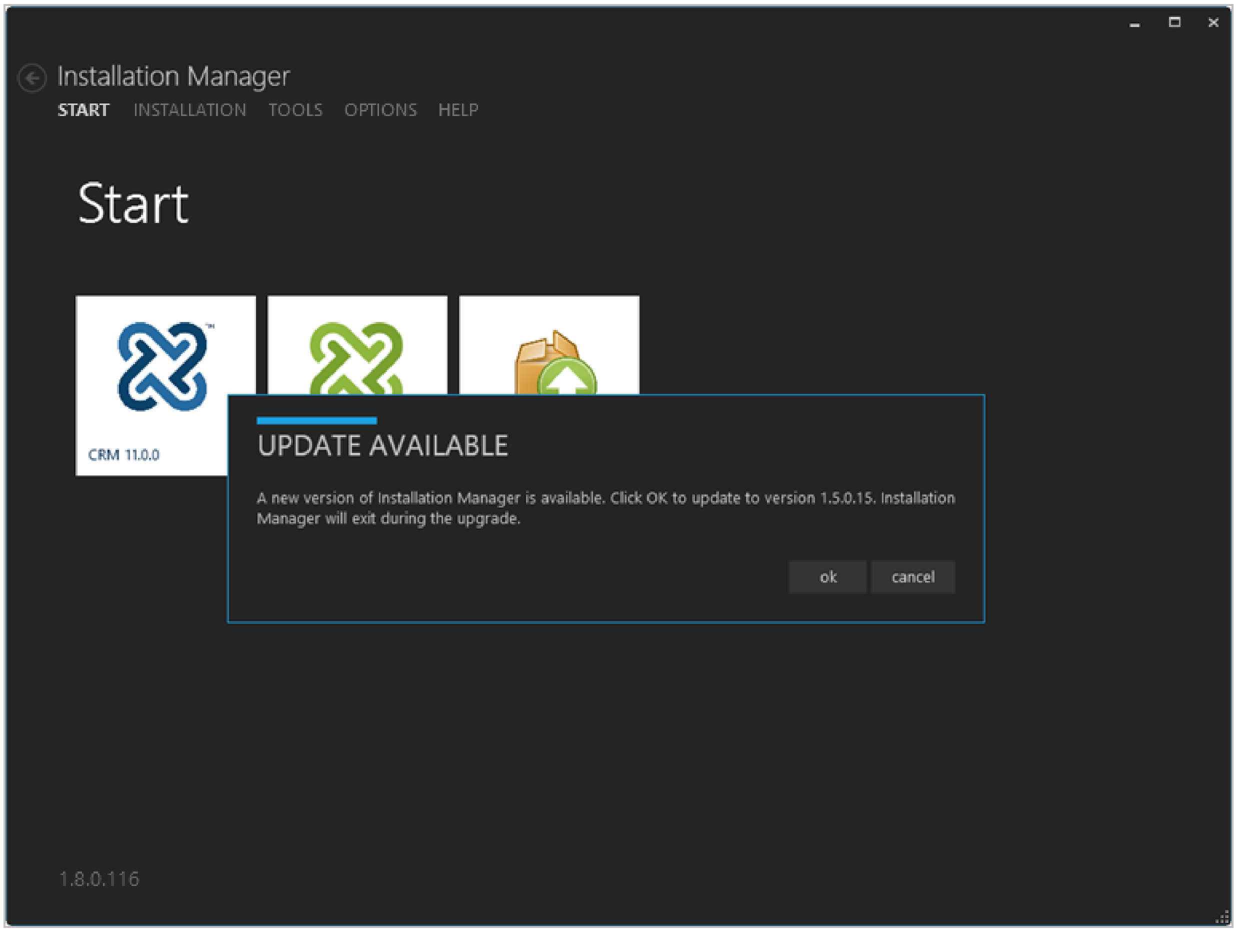
Installation Manager requires unique keys tied to the installation packages available to particular customers to ensure that incorrect, outdated, or inappropriate packages are not installed. To obtain a customer key, call Anthology Inc. Support at **1-800-483-9106**.

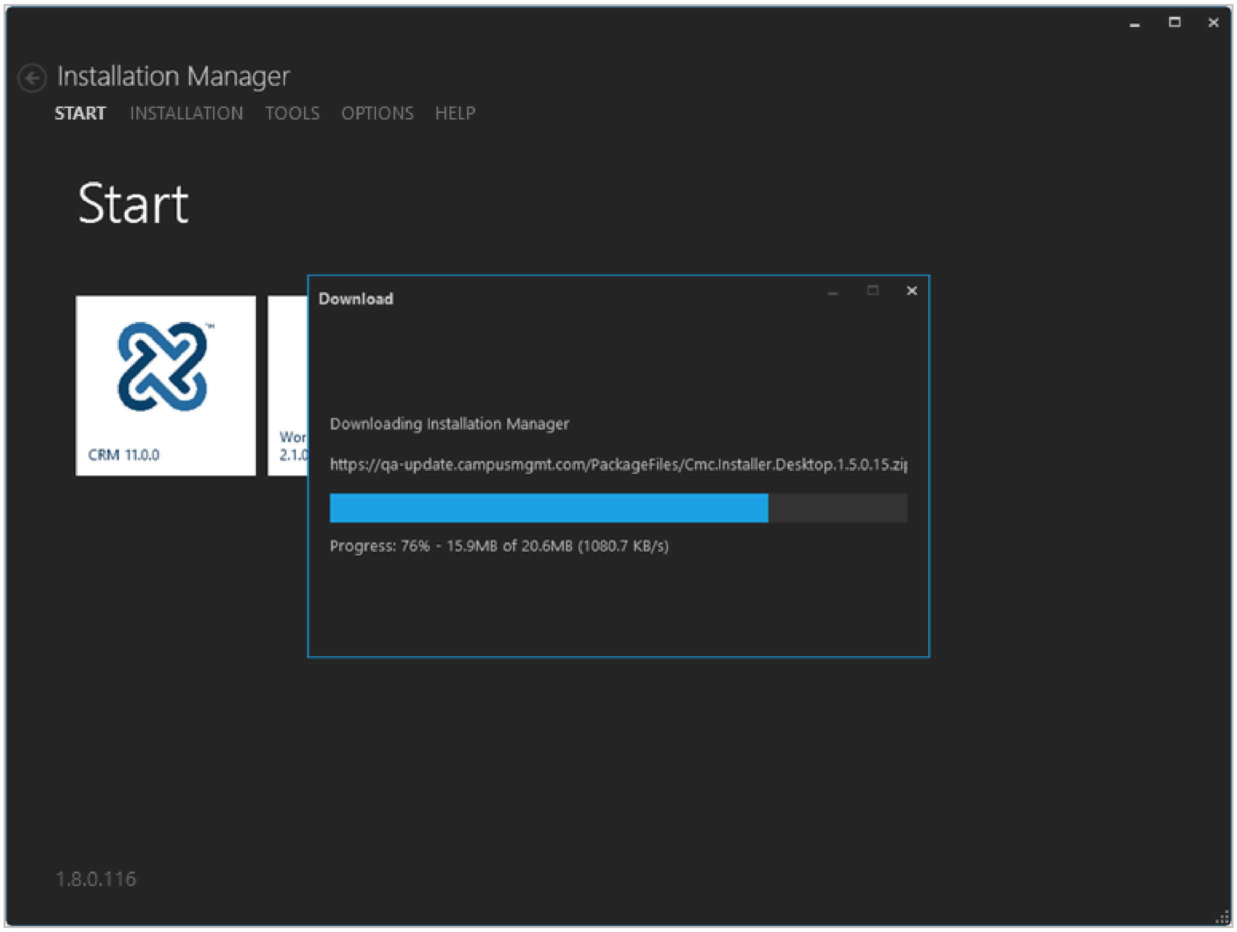
1. To launch Installation Manager from your desktop, click the shortcut icon 

.

   Upon startup, Installation Manager checks the Package Manager server for the latest available Installation Manager version.

   a. If the locally installed version is lower than the remote version, you are prompted to install the new version. Click **OK** to install the new build of Installation Manager.


Installation Manager
START INSTALLATION TOOLS OPTIONS HELP
Start
CRM 11.0.0
UPDATE AVAILABLE
A new version of Installation Manager is available. Click OK to update to version 1.5.0.15. Installation Manager will exit during the upgrade.
ok
cancel
1.8.0.116

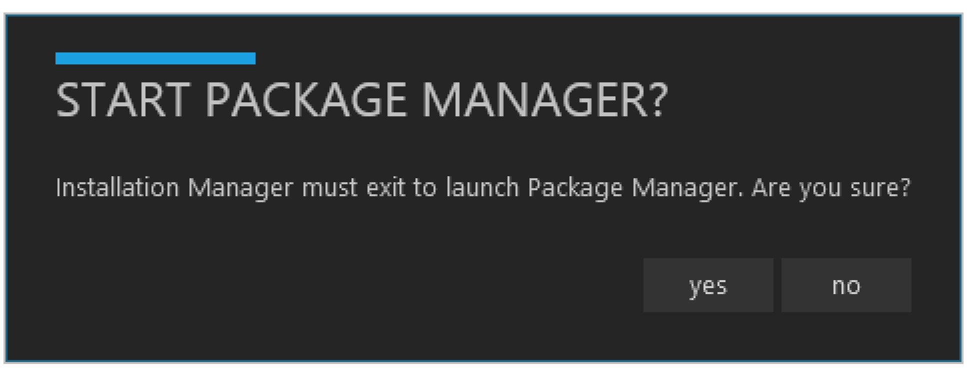


b. When the download completes, the installer for Installation Manager starts automatically and installs the new version.

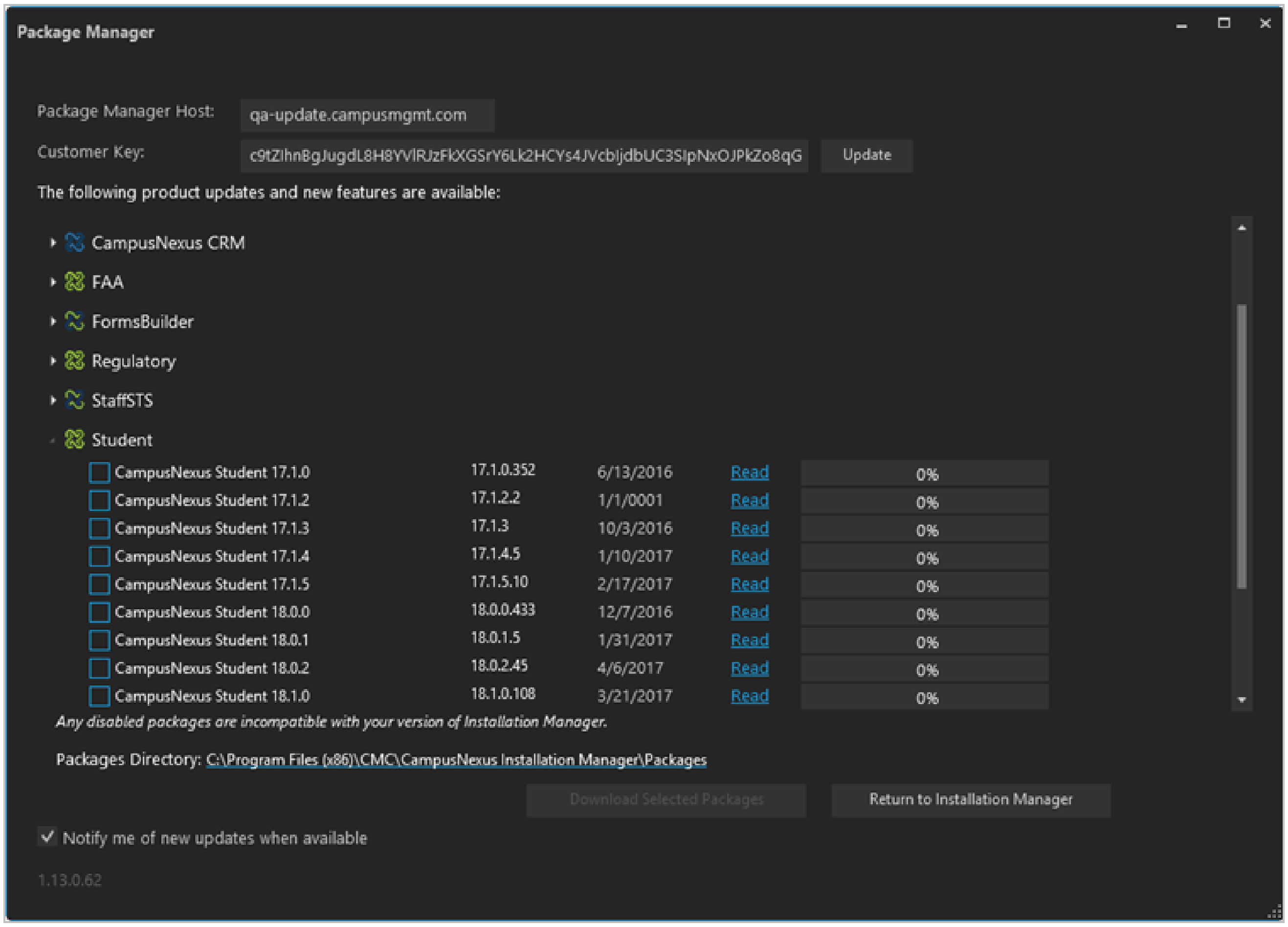
c. When the installation is complete, launch the new version of Installation Manager. All previous settings are retained.

2. On the Start screen, click the **Package Manager** tile.

3. Click **Yes** to confirm that you want to launch Package Manager.

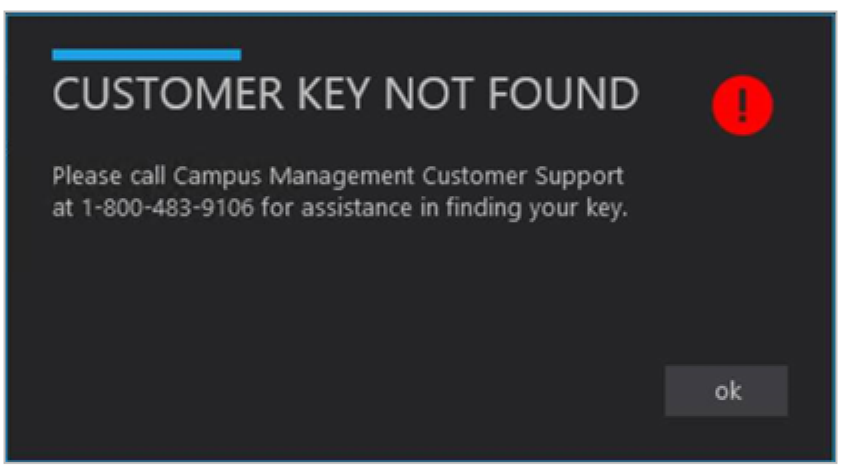


4. Installation Manager exits and launches Package Manager. The packages available for download are listed.



5. When you use the Installation Manager for the first time, paste the key (see Prerequisites) into the **Customer Key** field and click the **Update** button.

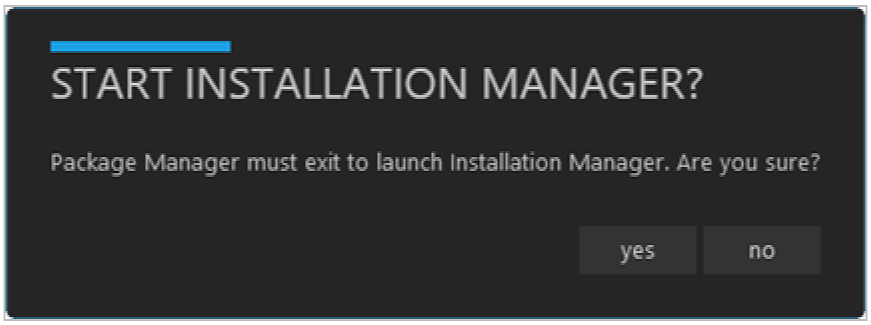
   If you do not have a key, the following message is displayed. Proceed as instructed.



6. Click the **Download** link in the Release Notes column to review information about new features and resolutions.
7. Select the packages you want to install and click **Download Selected Packages**.

   Notes:

   - The option **Notify me of new updates when available** is selected by default and ensures that you are alerted to updates.
   - If you do not want to install any packages at this time, click **Return to Installation Manager**.
8. When the download is completed, the following message is displayed. Click **Yes** to exit Package Manager and launch Installation Manager.

9. Click the tile representing the product to install.

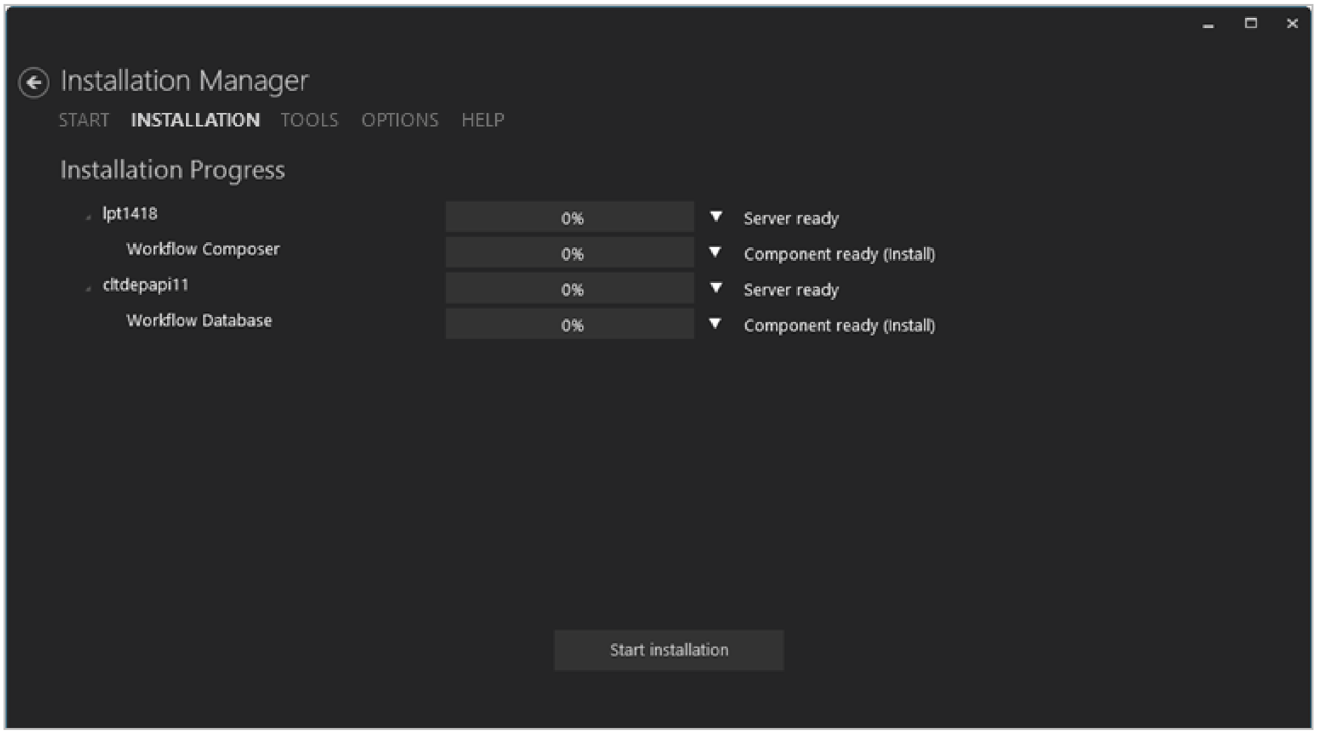
   Important: Before installing a product, ensure that the installation prerequisites for that product are met. You can find the prerequisites at the beginning of the Help sections for each product.

   Complete the installation process by filling out the installation screens as described in this Help system.

Installation

Installation Manager provides installation menus and screens that are specific to each product being installed. The last screen in the sequence of product-specific installation screens enables you to review the chosen configuration and access tools such as Log Viewer, Event Viewer, and others.

1. Once all setup screens have been properly updated and successfully tested (by clicking the appropriate Test buttons), click **Review Configuration** to see all of the information on one screen. The Installation Progress screen is displayed.

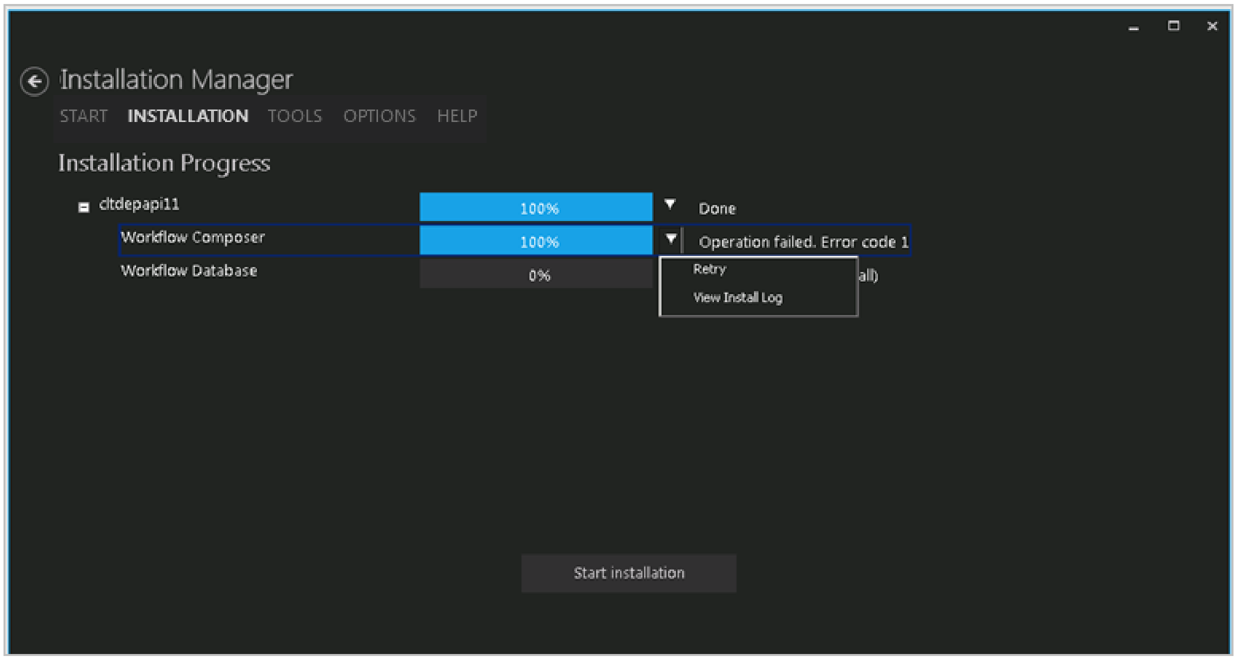


2. Click next to the progress bar for a server to access the following Windows Server tools:

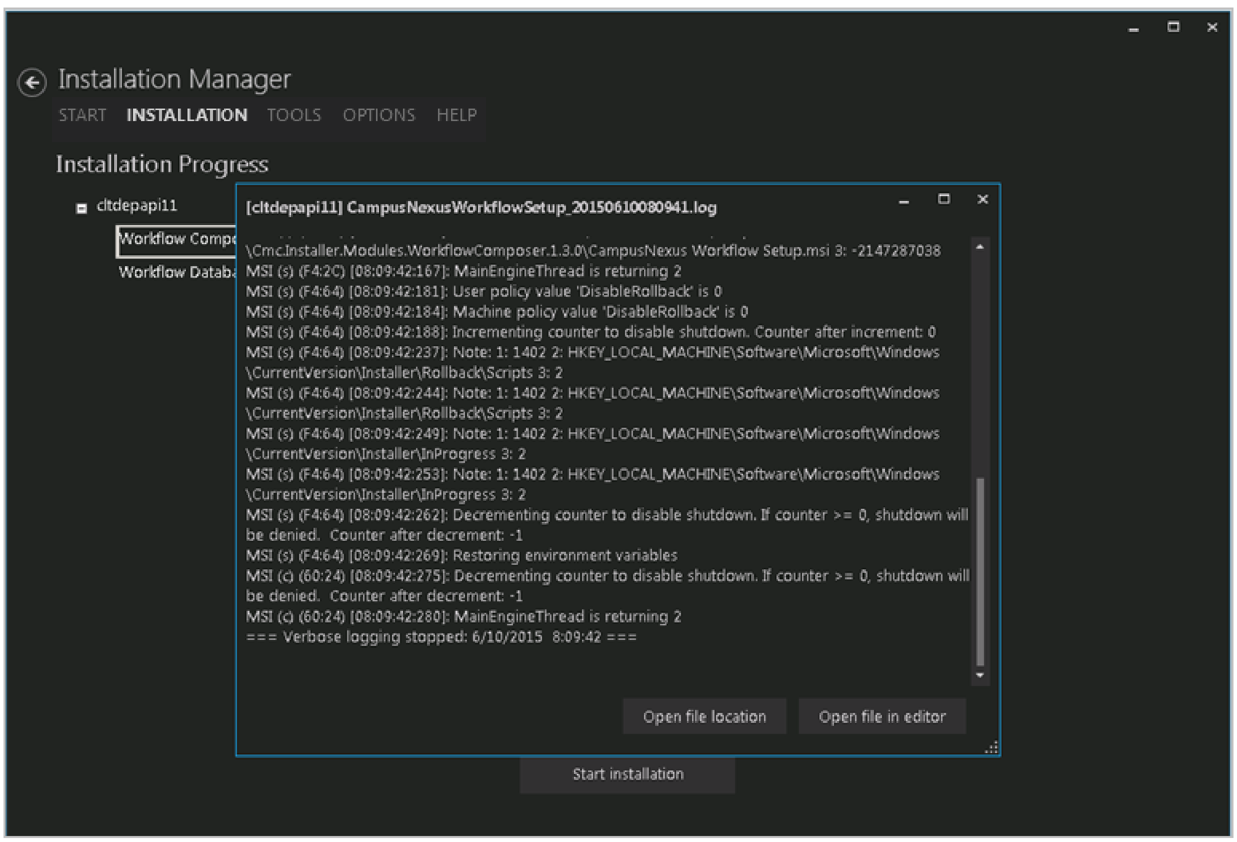
   - Remote Desktop
   - Event Viewer
   - Continuous Ping
   - Computer Management
   - Services
   - Users & Groups

3. Click next to the progress bar for a component to access the following options:

- **Retry** (enabled after a failed installation)

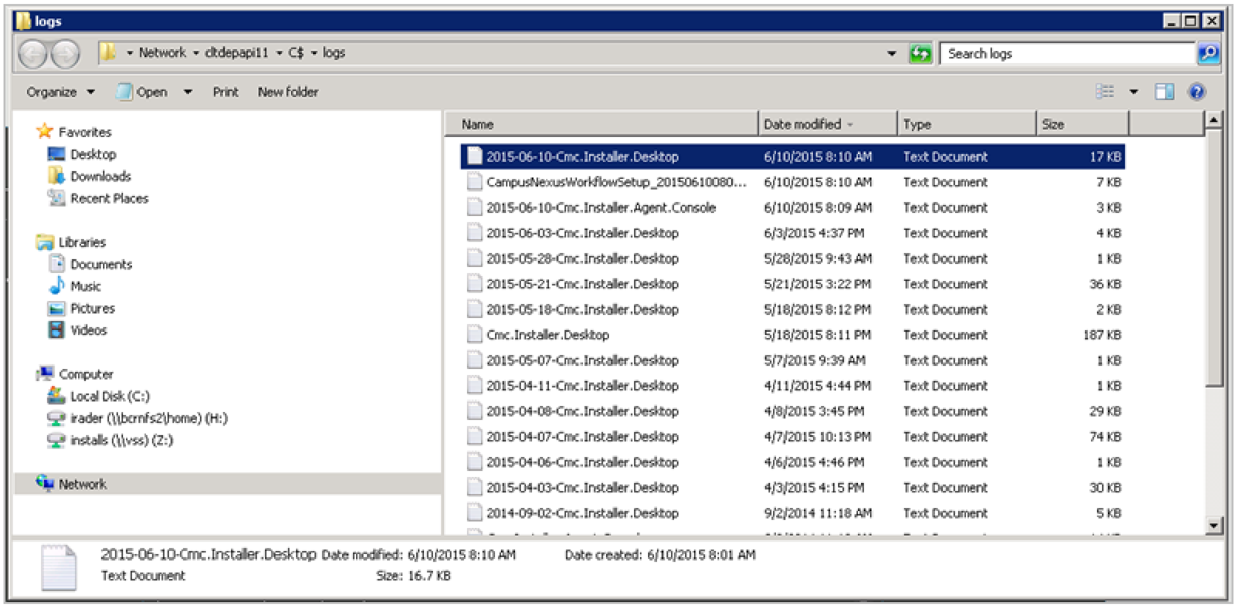


- **View Install Log**



Click **Open file in editor** to view the log file in an editor such as Notepad.

Click **Open file location** to view the log file in the directory where it resides. This can be a local or remote location.



4. Click **Start installation** to proceed.

   If an error occurs while installing one or more components, select the **Retry** option on the component's context menu. The installation of failed and new components resumes. Successfully installed components are skipped.

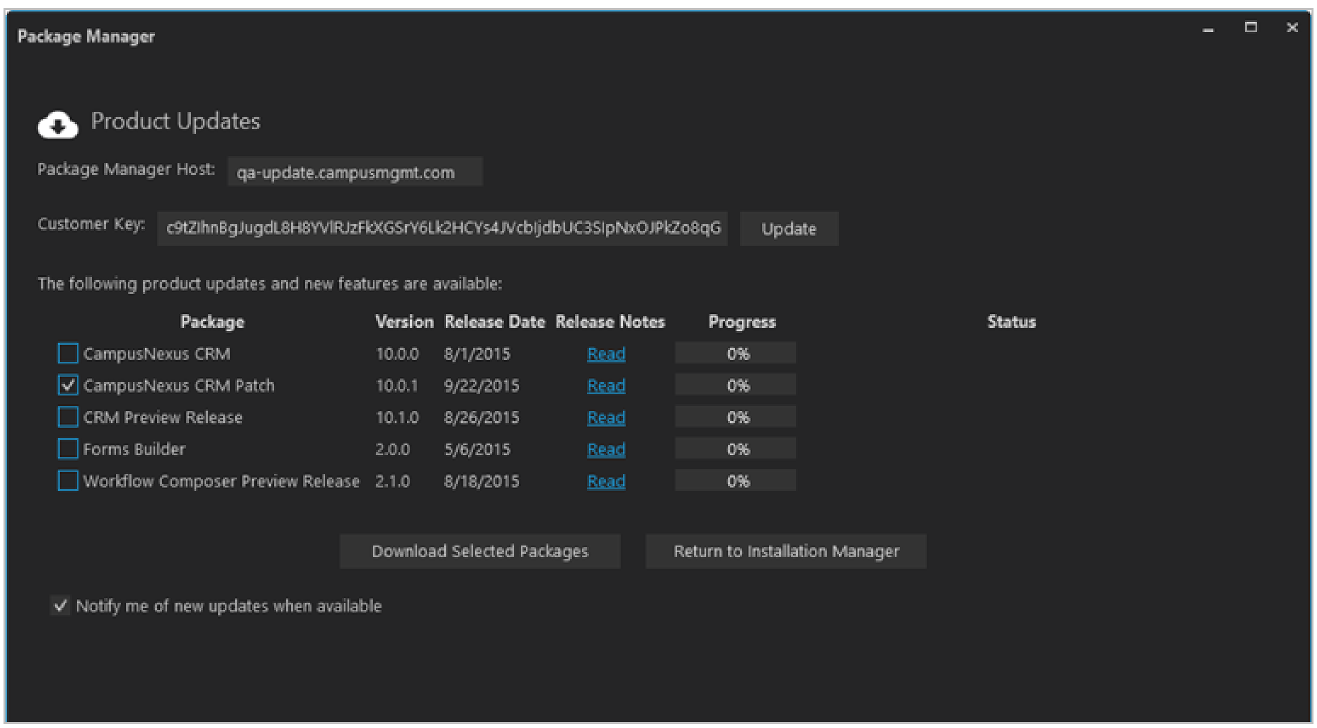
Patches

Installation Manager supports the installation of patches for Anthology products.

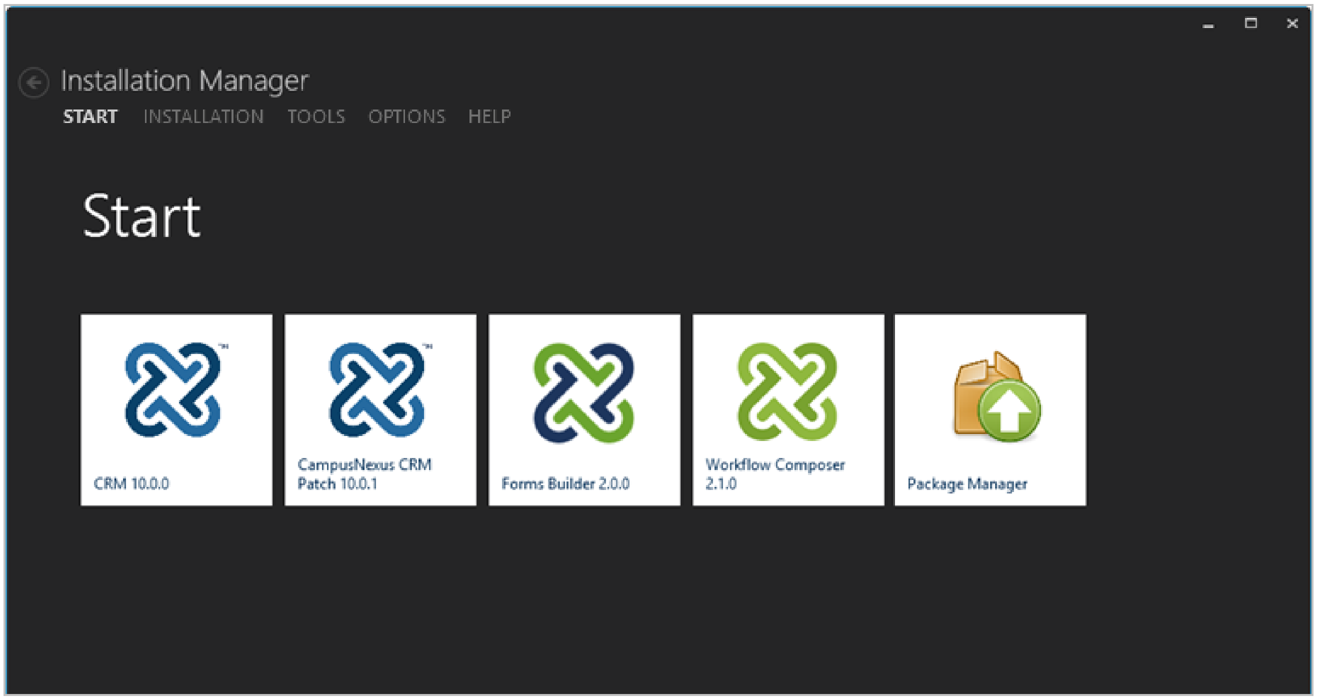
- When patches become available, they are listed on the Package Manager screen.
- When a patch is installed, the configuration settings of the product are applied during patch installation.
- The configuration settings cannot be changed when a patch is applied.
- Installation Manager displays the Prerequisite Validation screen before installing a patch.
- Patches need to be deployed to all the servers listed on the Prerequisite Validation screen.

Install Patches

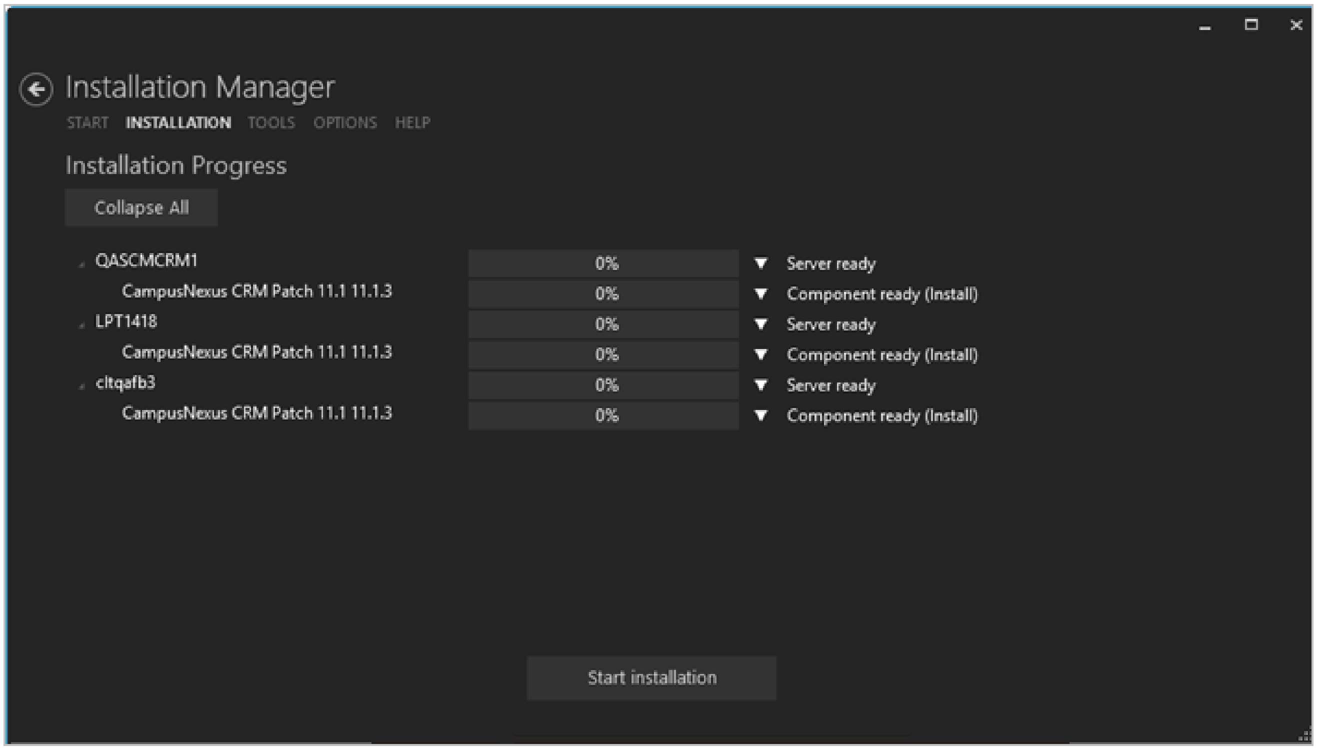
1. On the Start screen of Installation Manager, click the **Package Manager** tile and confirm that you want to launch Package Manager. The Product Updates screen is displayed.
2. On the Product Updates screen, select a patch package and click **Download Selected Packages**.



3. When the package download is completed, click **Yes** to restart Installation Manager.
4. When the restart is completed, a tile for the downloaded patch package is displayed on the Start screen. Click the **Patch** tile.



5. Depending on the selected patch, a Patch Configuration or Prerequisite Validation screen is displayed.
   - On the Patch Configuration screen, provide appropriate configuration information and click **Review Configuration** to proceed to the Installation Progress screen.
   - On the Prerequisite Validation screen, click **Check prerequisites** to validate the configuration, or click **Skip Prerequisite Check** to proceed directly to the Installation Progress screen.
6. On the Installation Progress screen, click **Start Installation** to install the patch.



If an error occurs while installing one or more components, select the **Retry** option on the component's context menu. The installation of failed and new components resumes. Successfully installed components are skipped.

Tools

The Tools menu in Installation Manager provides tiles to access the following options:

- Log

  The log screen displays exceptions and error messages that occurred during the installation of a product. The log screen is used by Installation Manager and not one particular product that is being installed. Installation Manager application logs are written to `C:\logs`. Logs for the products that are installed with Installation Manager are written to different folders. For example, CampusNexus CRM logs are written to `C:\Program Files (x86)\Common Files\Talisma Shared\SetupLog`.

- Export Settings

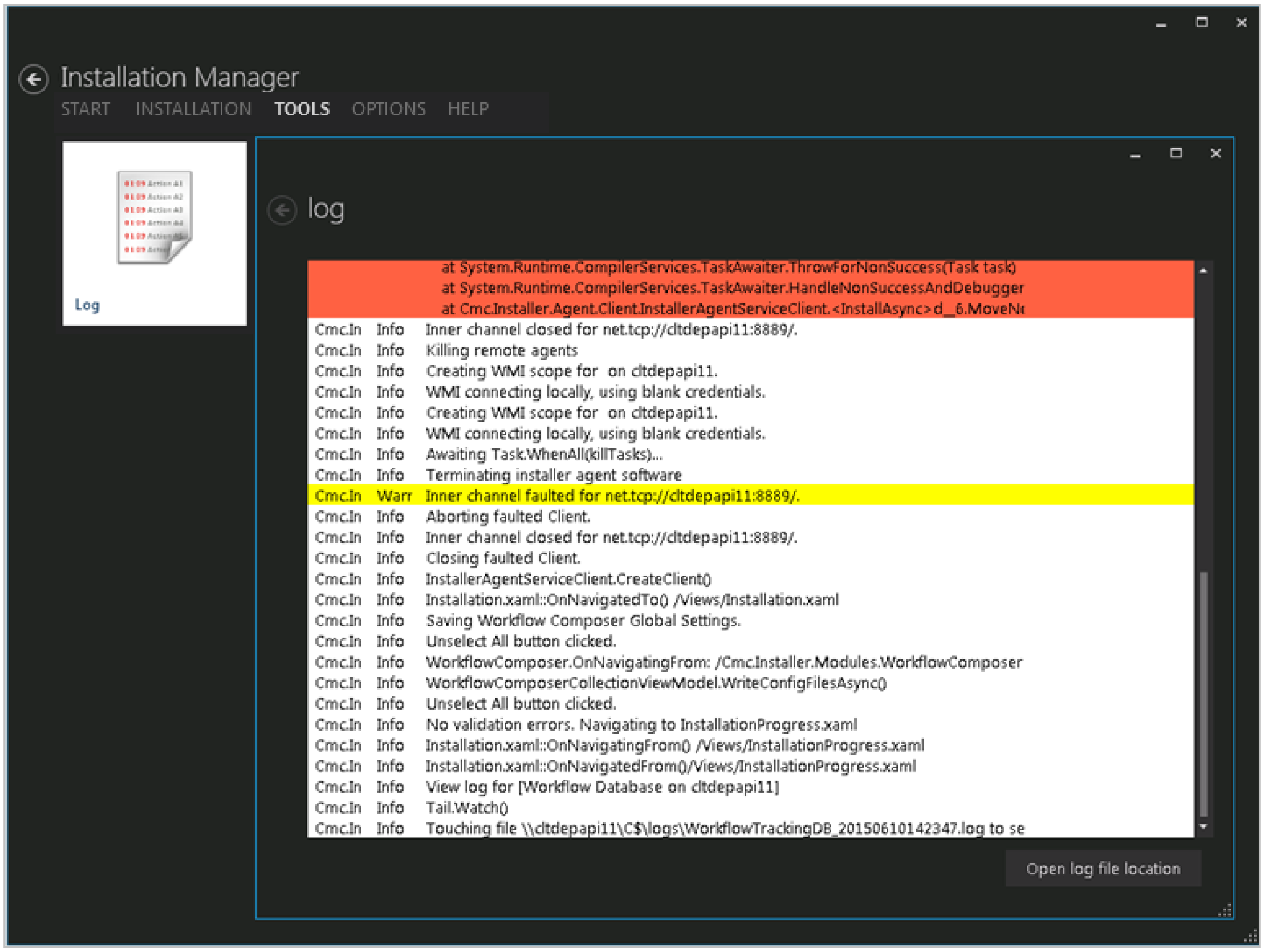
  This option enables you to copy all configuration settings of Installation Manager to a ZIP file.

- Import Settings

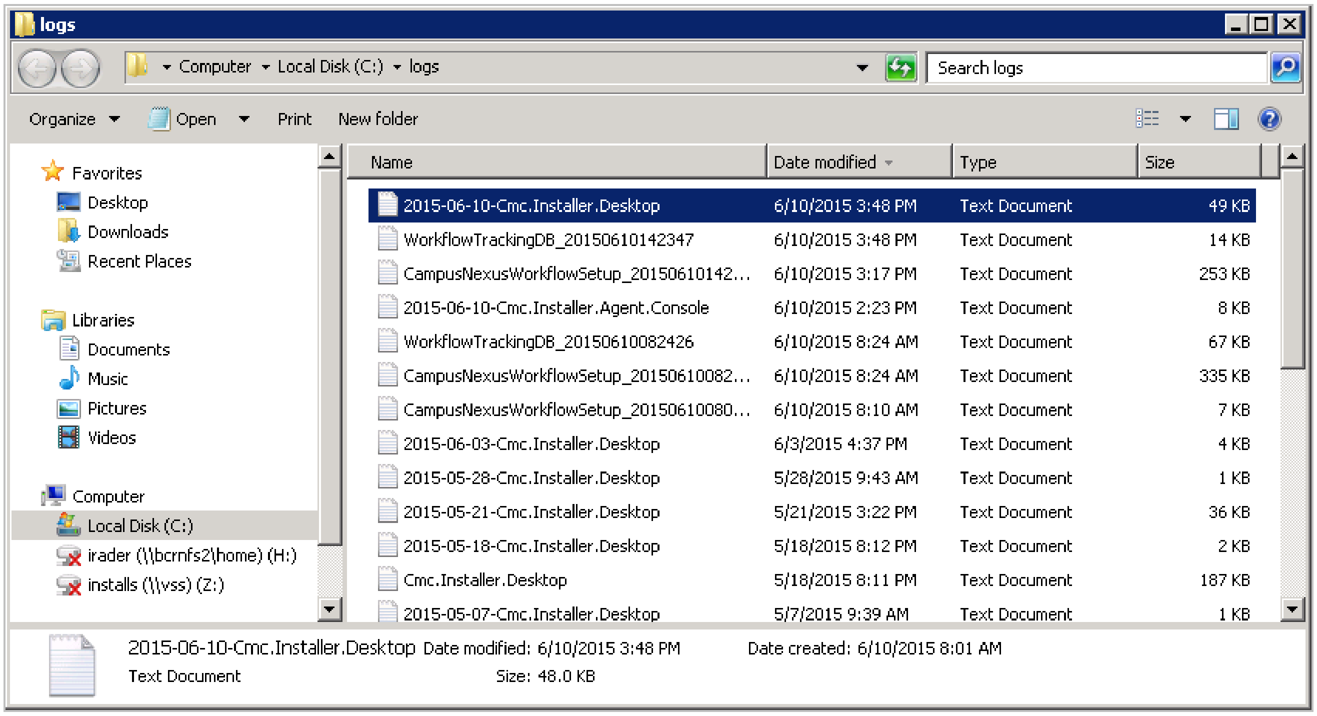
  This option restored the configuration settings of Installation Manager from a previously exported ZIP file.

View Logs

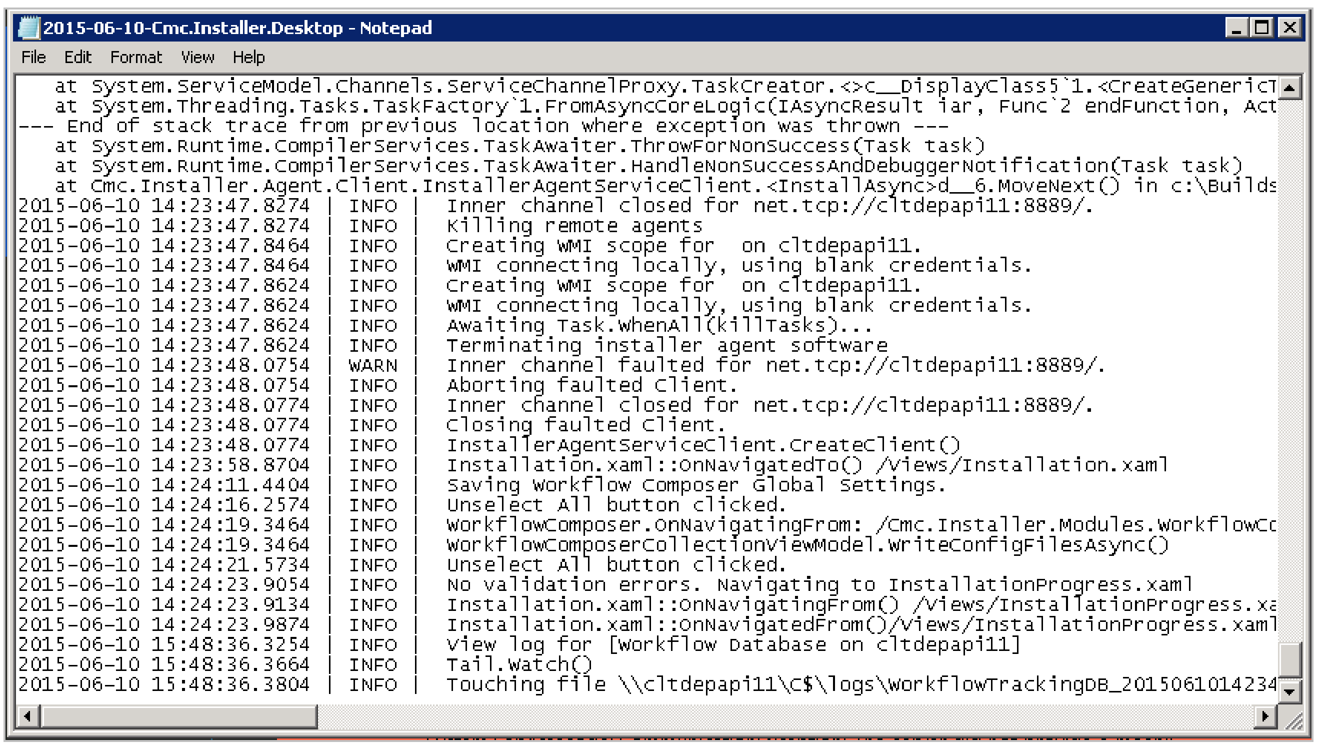
1. Navigate to **Tools** and click the **Logs** tile. The Log Viewer screen is displayed.



2. Click **Open log file location**. The `C:\logs` directory is displayed.



3. Select the appropriate log file and double-click it to view it in a text editor.

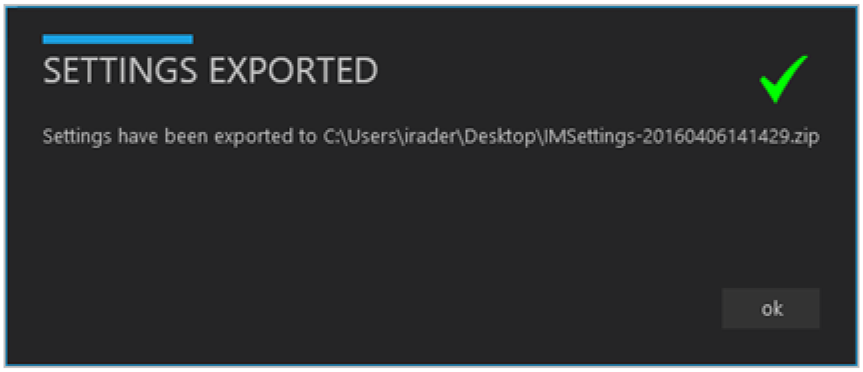


4. Close the editor and the Log Viewer screen to return to Installation Manager.

Export Settings

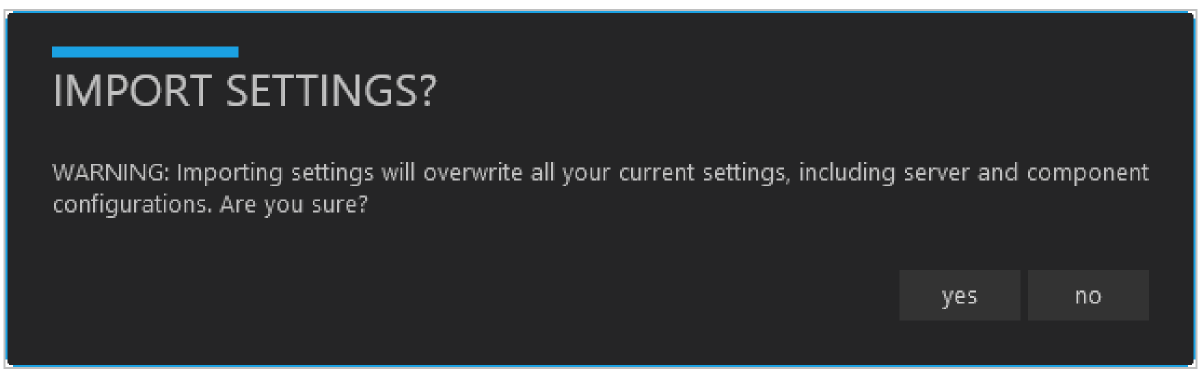
1. Click the **Export Settings** tile to copy all the configuration settings of Installation Manager. This is useful if you want to copy the settings from one machine to another machine or if you have removed them from C:\\Program Files (x86)\CMC\CampusNexusInstallation Manager\Packages and want to apply the previous Installation Manager settings after re-adding packages.

2. A confirmation message is displayed indicating the location of the IMSettings-<datetime>.zip file that contains the configuration settings.



Import Settings

1. Click the **Import Settings** tile to import the configuration settings of Installation Manager. The Import Settings warning message is displayed.



2. Click **Yes** on the Import Settings warning message to continue.

3. Select the IMsettings-<date-time>.zip file and click **OK**. The Restart Installation Manager message is displayed.

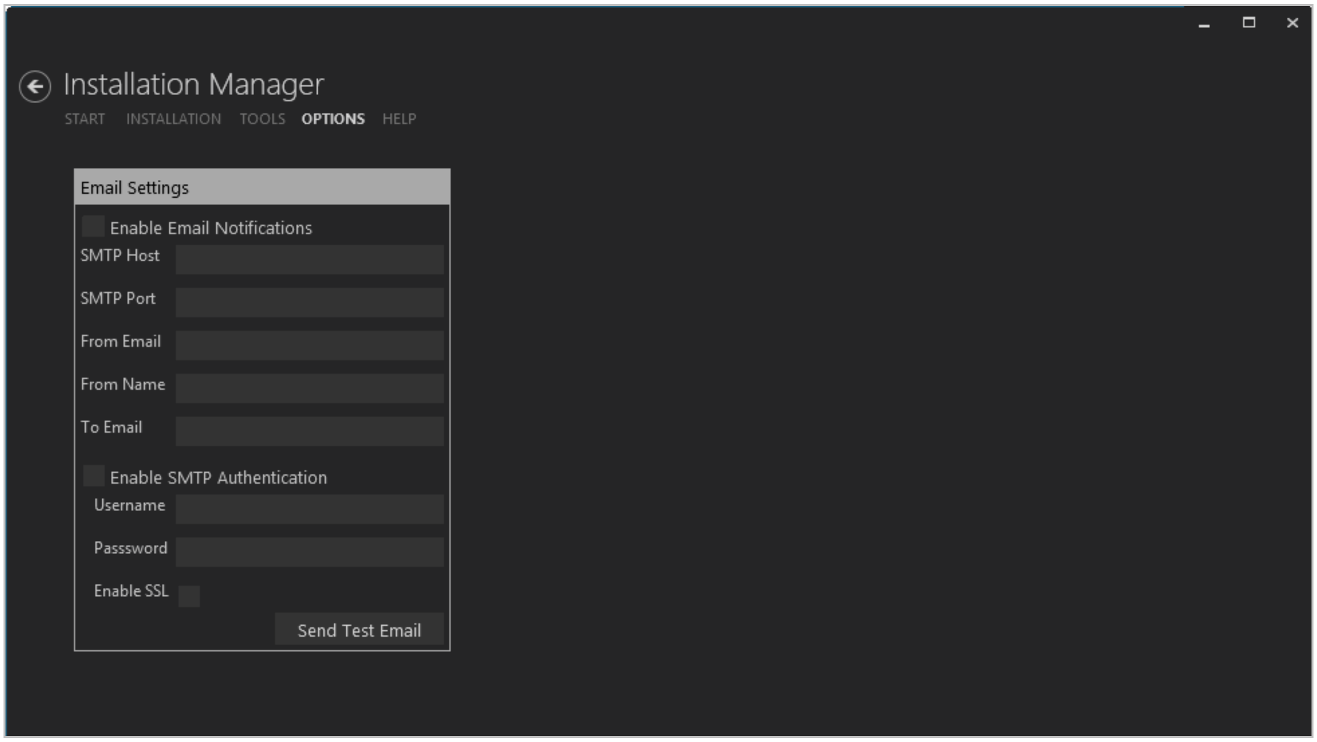
4. Click **Yes** to restart Installation Manager.

Options

Installation Manager can notify users whenever a product installation begins and ends. The Options menu enables you to configure the email settings for these notifications.

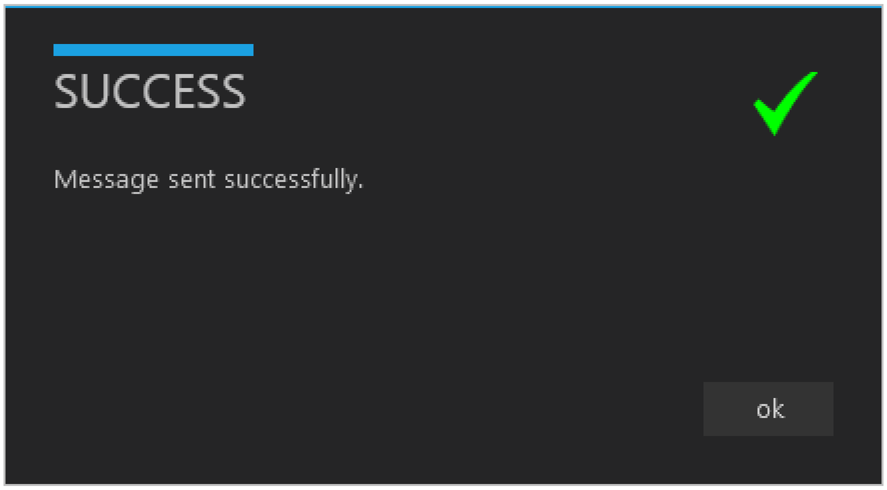
Set Up Email Notifications

1. Select the **Options** menu in Installation Manager.



2. Select **Enable Email Notifications**.
3. In the **SMTP Host** field, enter the domain address of the SMTP host used for sending out email notifications, e.g., cmcsmtphost.campusmgmt.com.
4. Specify the **SMTP Port** number.
5. In the **From Email** field, enter the email address of the account that sends out notifications, e.g., serviceaccount@campusmgmt.com.
6. In the **From Name** field, enter the display name for the 'From' field of the notification email, e.g., Installation Manager Notification.
7. In the **To Email** field, enter the email address of the recipient of the notifications. You can enter multiple email addresses separated by a semicolon (;). This list receives messages indicating an installation has started and finished. The list should include anyone in charge of monitoring the installation.

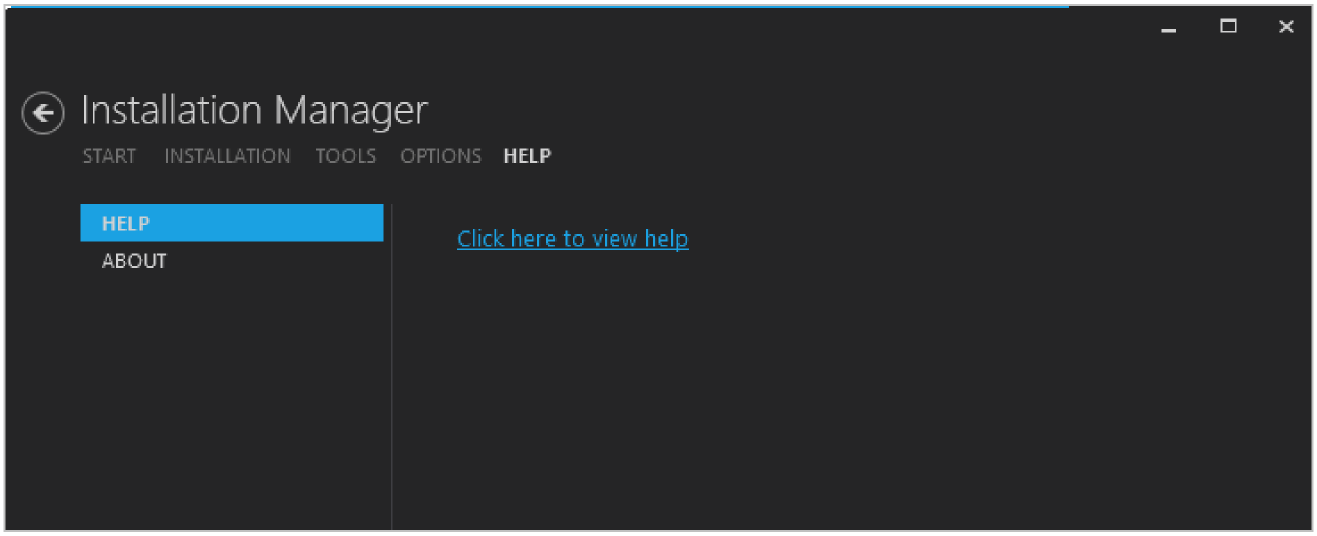
8. Select **Enable SMTP Authentication** and enter the **Username** and **Password** of the sender's email account.
9. If applicable, select **Enable SSL**. Installation Manager will check for a valid certificate.
10. Click **Send Test Email**. A confirmation message is displayed.



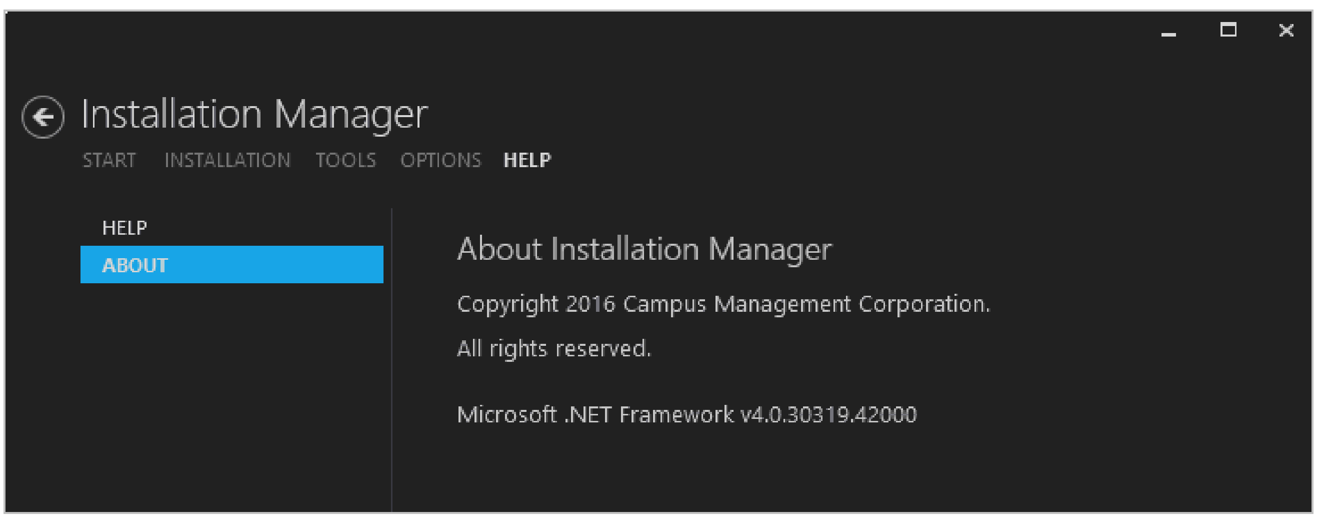
Help

The Help screen provides access to this Help system and the About screen for Installation Manager.

1. Select the **Help** menu in Installation Manager.
2. On the Help screen, select **Help** and click the link to view the Help system.



3. Select **About** to view the copyright and version information.



Staff STS

Installation Manager enables you to install a Staff STS component on a local or remote machine. The Staff STS component provides centralized security token service for Staff Administrators of the following components:

- Web Client for Anthology Student version 17.1.0 and later

  Note: Anthology Student version 19.0.3 or later requires Staff STS version 2.1.2 or later.

- Web Client for CampusNexus CRM version 11.0 .0 and later
- Forms Builder 2.3 and later

Staff STS must be installed before installing the indicated versions of these components.

Prerequisites

The prerequisites for the Staff STS installation are as follows:

- Microsoft .NET Framework 4.5 or higher
- Microsoft Internet Information Server (IIS) 7.0 or higher

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

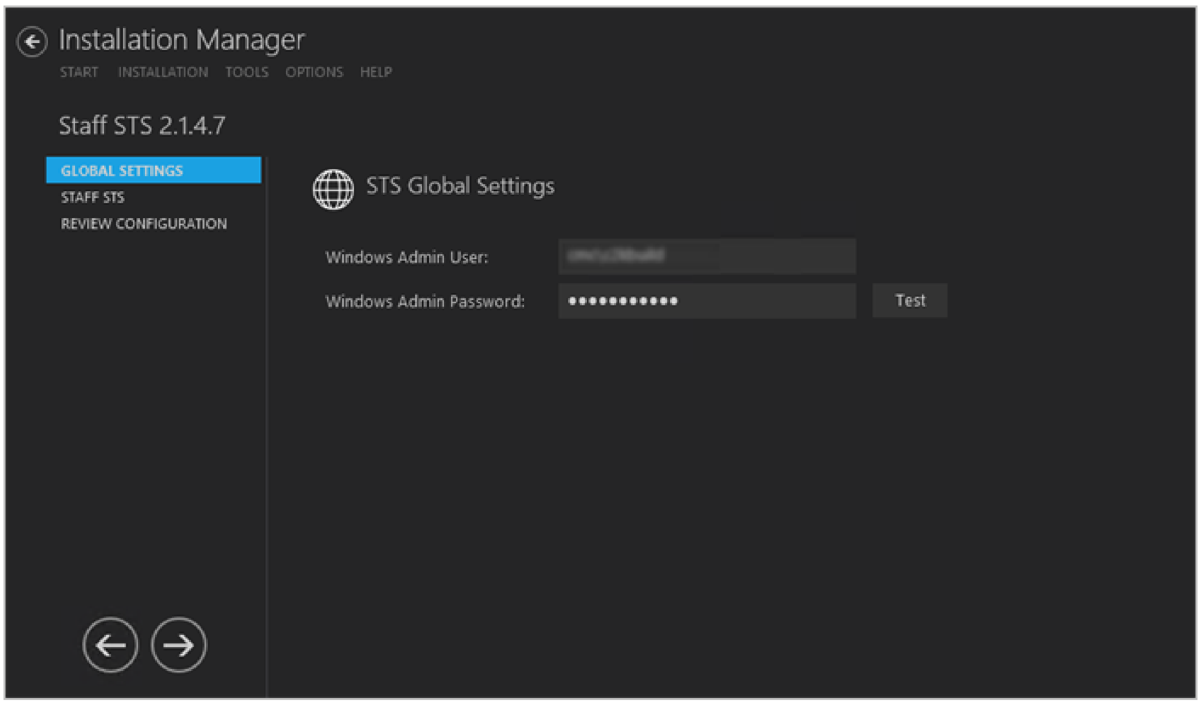
Global Settings

The Global Settings screen contains the Windows Admin user name password used when starting a Staff STS installation. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Staff STS** tile. The Global Settings screen is displayed.



2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer on which the installation will occur. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

   Note: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.

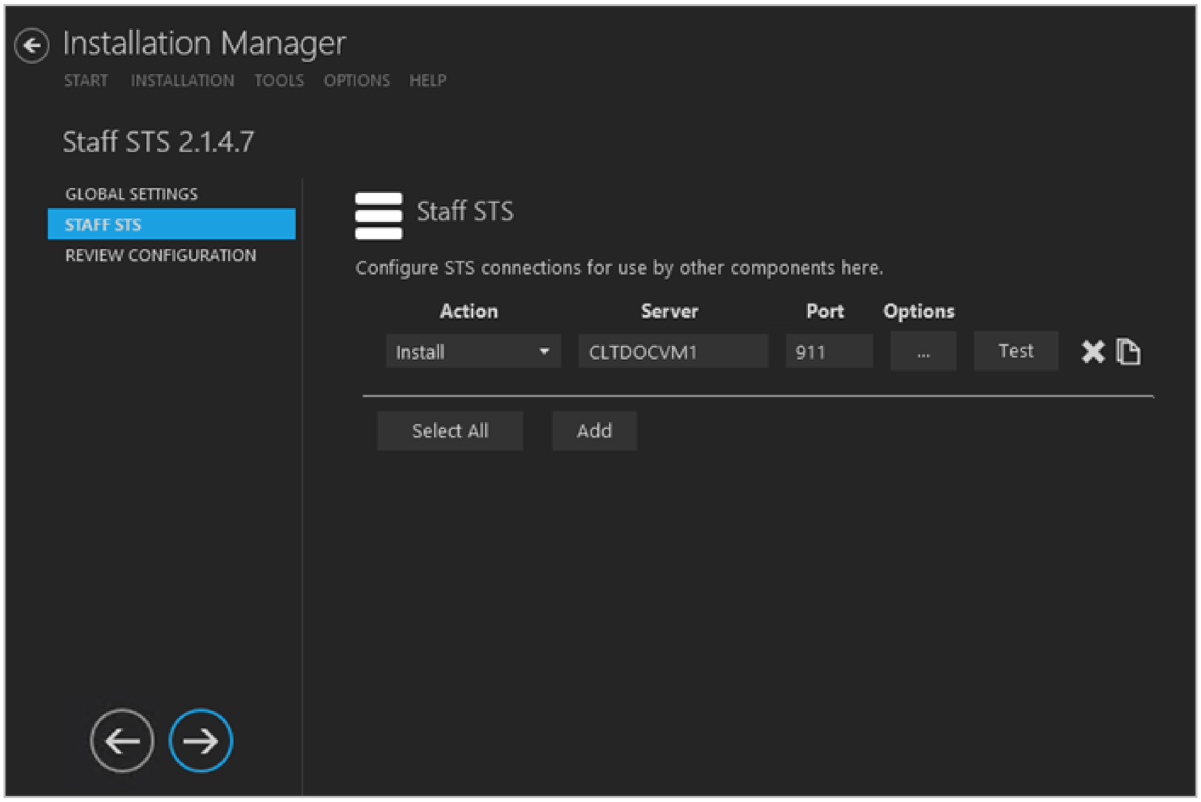
4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
5. If the user is authenticated, click **OK** and click  to continue.

Staff STS

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to configure the STS connections for Anthology Student, CampusNexus CRM, Portal Administrator, and Forms Builder.

Set Up the Staff STS

1. In the Installation menu, click **Staff STS**. The Staff STS screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

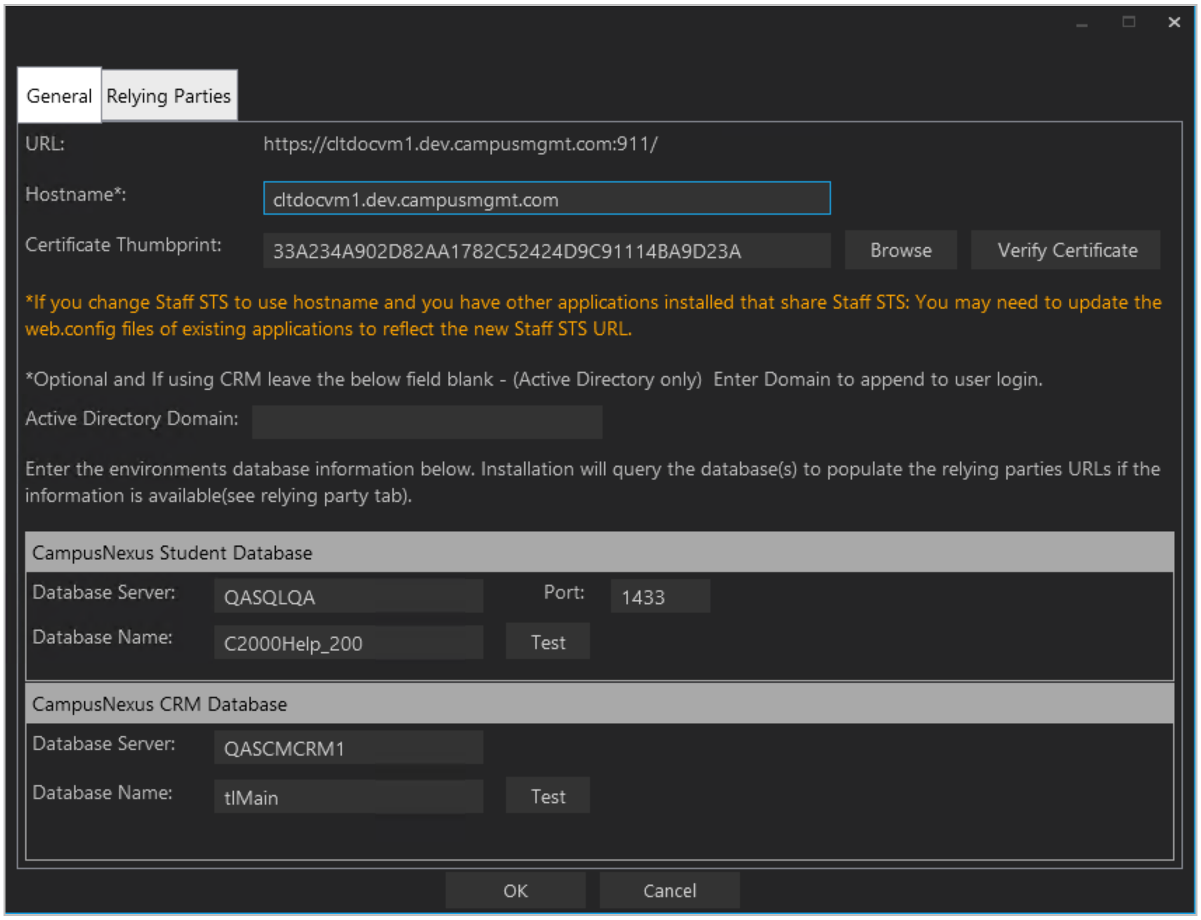
4. Enter the name of the **Server** where the Security Token Service will be installed.
5. Specify the name of the **Port** for the Staff STS connection or accept the default (91).
6. Click  to copy a line. Edit the copied line as needed.
7. Click  to view and edit the Options form.

   General Tab

   Use this tab to specify the certificate thumbprint and hostname of the Staff STS.

   Notes:

   - The certificate thumbprint for Staff STS can be the same as the one used for Anthology Student, CampusNexus CRM, Portal, and Forms Builder, or it can be a different certificate.
   - If the Hostname is specified, this hostname will be added to the IIS bindings.
   - The URL with the custom hostname needs to be provided to the web.config files of all the relying parties.
   - Since Staff STS always uses SSL, it is always HTTPS.



General Tab Fields

Field	Description
URL	This is a friendly URL to access the Staff STS. The default port is 911. The default format is: `https://machinename.domain.com:port`

Field	Description
Hostname	This is an optional field. When selected, the web.config file of Staff STS will be updated with the custom host URL. If this field is left blank, the URL for Staff STS accessed by end users and the URL in the config files will be `https://machinename.domain.com:port` Microsoft Internet Information Services (IIS) allows you to map multiple websites with the same port number to a single IP address by using a feature called Host Header Names. By assigning a unique Host Header Name to each website, this feature allows you to map more than one website to an IP address. Enter a hostname if you want to assign a hostname (DNS name) in IIS. If you specify a hostname, clients must use the hostname instead of the machine name or IP address to access the website. This feature is often used when a TCP Port must be shared. If you change Staff STS to use the hostname and you have other applications installed that share Staff STS, you may need to update the web.config files of the existing applications to reflect the new Staff STS URL. Staff STS is shared between: • Forms Builder Designer 2.3.x • Forms Builder Designer 3.x • Anthology Student • Portal 18.2 or higher • CampusNexus CRM For Web Client for Anthology Student, ensure the ‘Authentic-ationProvider:WsFedIssuerUri’ app setting value matches the Staff STS URL. For Forms Builder Designer and Web Client for CampusNexus CRM, ensure the 'Issuer' under federationConfiguration matches the Staff STS URL.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Certificate Thumbprint</td><td>Certificate Thumbprint from IIS.

Copy and paste the thumbprint into Options form, or click Browse to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint will be added to the web.config file of the component that uses the STS connection. Click Verify Certificate to make sure the certificate is valid.

Note: Only RSA-based certificates are supported.

The thumbprint for Staff STS can be the same one used for Anthology Student, CampusNexus CRM, Portal, or Forms Builder, or it can be a different certificate.

To extract a .CER file from IIS:

a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from Server Certificates.
b. Double-click to open the certificate properties.
c. Select Root level and in the Details tab, click the Copy to File... button.
d. Click Next. Select No, do not export the private key, and click Next.
e. Select DER encoded binary X.509 (.CER) and click Next.
f. Specify a file path and name (root) to export to and click Next.
g. Click Finish</td></tr>
<tr><td>Active Directory Domain</td><td>This field is available in Staff STS 2.1 or later. It supports the DefaultDomain key in the app settings of config files for products that use the Staff STS, e.g., Anthology Student, Forms Builder, Portal.

If the environment is Active Directory enabled, the Active Directory Domain value can be set to the users' domain. This enables users to log in without typing the domain value.

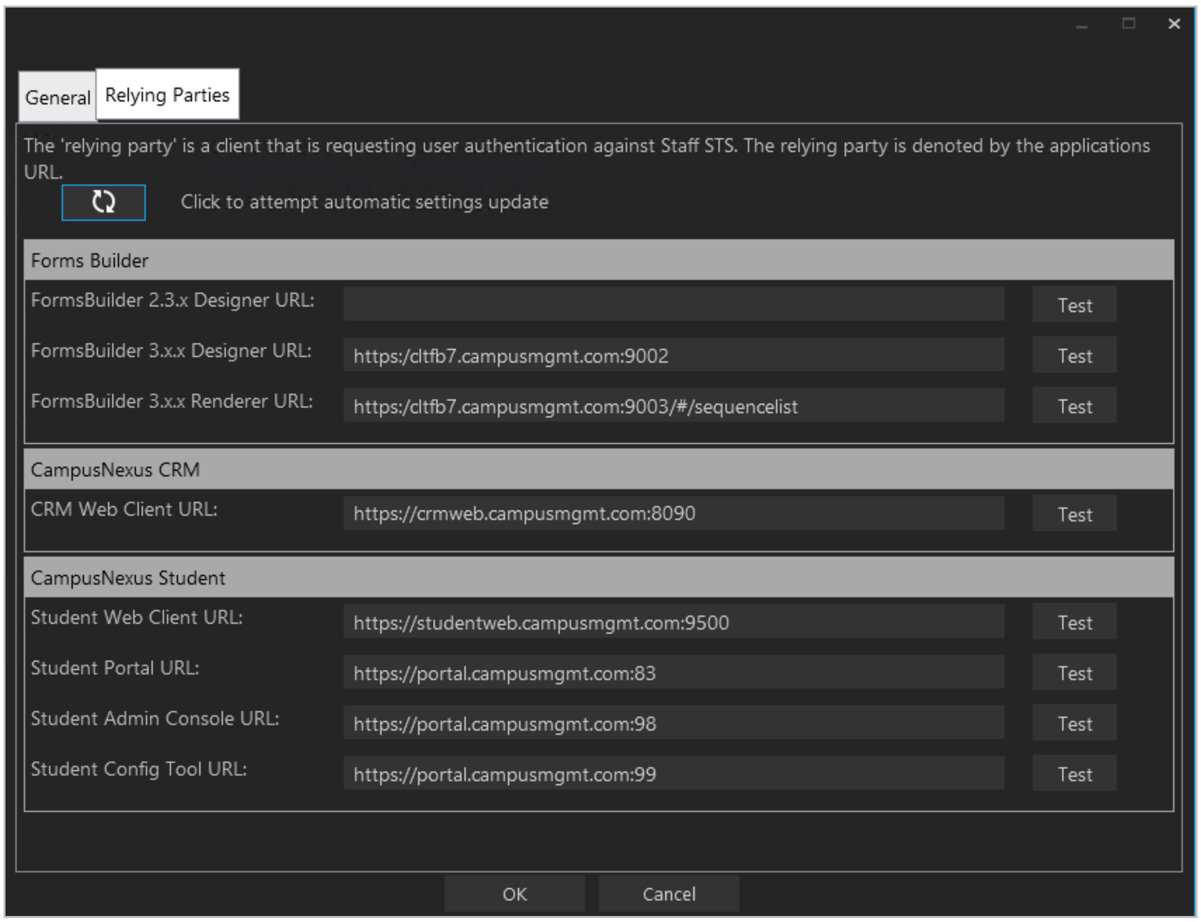
<add key="DefaultDomain" value=""/>

Note: If Staff STS 2.1 or later is installed for CampusNexus CRM, the default domain value will not affect CampusNexus CRM.</td></tr>
<tr><td colspan="2">Enter the database information for your environment. Installation Manager will query the database(s) to populate the relying parties' URLs if the information is available (see Relying Parties Tab).</td></tr>
<tr><td colspan="2">Anthology Student Database</td></tr>
<tr><td>Database Server</td><td>Name of the SQL server on which the Anthology Student database resides.</td></tr>
<tr><td>Port</td><td>Specify the port number of the SQL server or accept the default (1433).</td></tr>
<tr><td>Database Name</td><td>Name of the Anthology Student SQL database.</td></tr>
<tr><td>Test</td><td>Click Test to verify the database connection.</td></tr>
</table>

Field	Description
CampusNexus CRM Database	
Database Server	Name of the SQL server on which the CampusNexus CRM database resides.
Database Name	Name of the CampusNexus CRM SQL database.
Test	Click **Test** to verify the database connection.

Relying Parties Tab

Use this tab to specify the URLs of the components that rely on the Staff STS for staff authentication. The fields on this tab are optional.



The default format of the URLs is: `http(s)://machinename.domain.com:port`

The URLs of the relying parties are inserted into web.config file of Staff STS 2.0 or later to support backward compatibility.

Examples:

- If a customer has Forms Builder 3.2 (Staff STS 1.1) and then you install Anthology Student 18.2 (Staff STS 2.0 or later), the Forms Builder Designer URL must be inserted into the web.config file of Staff STS 2.0 or later with the following key:

  ```
  <add key="FormsBuilder.Designer.WsFed" value=""/>
  ```

- If a customer has CampusNexus CRM 11.1 (Staff STS 1.1) and then you install Anthology Student 18.2 (Staff STS 2.0 or later), the URL of the Web Client for CampusNexus CRM must be added to the web.config file of Staff STS 2.0 or later.

- If a customer has CampusNexus CRM 12.0 (Staff STS 2.0 or later) but Anthology Student 18.1, the following URLs must be added to the web.config file of Staff STS 2.0 or later:

  - Anthology Student
  - Portal
  - Portal Admin Console
  - Portal Config Tool

- If a customer has Anthology Student 18.2, CampusNexus CRM 12.0, and Forms Builder 3.1 or lower, the Form Designer URL must be added to the web.config file of Staff STS 2.0 or later.

Relying Parties Tab Fields

Field	Description
	Click the **Refresh** button to attempt an automatic settings update.
Forms Builder	
Forms Builder 2.3.x Designer URL	URL of the Forms Builder 2.3.x Designer
Forms Builder 3.x.x Designer URL	URL of the Forms Builder 3.x.x Designer
Forms Builder 3.x.x Designer URL	URL of the Forms Builder 3.x.x Renderer
CampusNexus CRM	
CRM Web Client URL	URL of the Web Client for CampusNexus CRM
Anthology Student	
Student Web Client URL	URL of Anthology Student
Student Portal URL	URL of the Portal
Student Portal Admin Console URL	URL of the Portal Admin Console

Field	Description
Student Portal Config Tool URL	URL of the Portal Configuration Tool
Test	Click **Test** to check each URL entered on this tab. If HTTPS is configured for any of these URLs, ignore the certificate error.

8. Click **OK** to save changes on the Options form. The form is closed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    The Test button checks the connectivity of the Admin user to the machine specified in the Server name field.

11. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

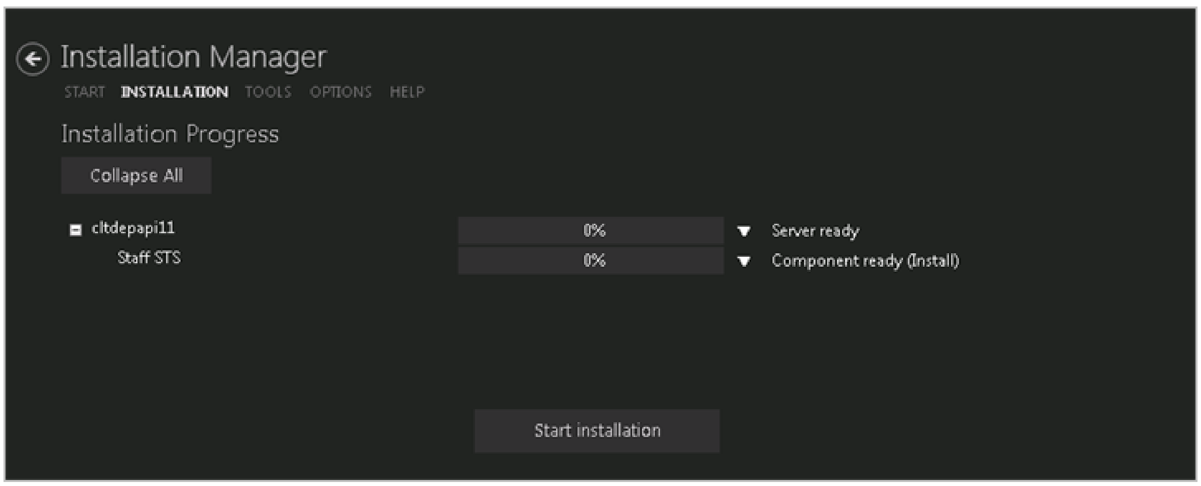
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration**. The Prerequisite Validation screen is displayed.

2. Click **Skip Prerequisite Check**. The Installation Progress screen is displayed.

3. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Click **Expand All** and scroll through the list of items. Or, click **Collapse All** and then click to expand a section.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

4. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

5. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

CampusNexus CRM

Installing CampusNexus CRM components using Installation Manager consists of ensuring that the SQL instances are properly created and creating relationships between the servers and databases.

CampusNexus CRM can be scaled from a simple installation of all components on a single server to a complex deployment where the components are installed on different servers.

Before setting up the databases, set Global Settings on the CampusNexus CRM Global Settings screen and then add the proper passwords, license key, and, if needed, the proper SQL Server user name and password if the SQL Integrated Security option is not selected.

Set up CampusNexus CRM components in the order of the navigation menu displayed in Installation Manager.

You can install a single instance or multiple instances of the Main database. For every instance of the Main database, you can create or attach the following database types:

- Main
- Analytics
- Distributor
- Media
- WebTrak
- Archive

These databases can reside on the server where the Main database is installed or on a different server.

> ⚠ The Web Client for CampusNexus CRM version 11.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

API Keys

To enhance the security of Anthology Inc. products, API keys were added to products released in May 2018 and later. An API key is a secret token that is submitted with a web service request to identify the origin of the request. The key for the consumer of the service needs to match the key of service provider, otherwise, access to the service is rejected. The API key is unique for each customer.

The API key is an AppSetting in the web.config files of applications built on the CampusNexus framework. It uses the following syntax:

```
<add key="apiKey" value=""/>
```

Depending on the installed products and versions, the apiKey is installed automatically by Installation Manager or needs to be updated manually.

If you are installing CampusNexus CRM (regardless of the version) and have or will have Anthology Student **19.0**, update the apiKey under <appSettings> in the web.config file in Cmc.Crm.Workspaces with the key found in the Package Manager screen of Installation Manager.

Minimum System Requirements

This section lists the hardware and software required for installing CampusNexus CRM components.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Hardware Requirements

Hardware Requirements

Component	Minimum Requirements
Database (previously referred to as Talisma Server)	• Intel Xeon with EM64T support • 8 GB RAM • 1 GB available hard disk space on the operating system drive • 4 GB available hard disk space on the drive where the Database component (Data files) is installed
Application Server	• Intel Xeon with EM64T support • 8 GB RAM • 500 MB available hard disk space
Web Components • Business Administrator • WebTrak • Scripting	• Intel Xeon with EM64T support • 8 GB RAM • 1 GB on the drive where the operating system is installed • 1 GB available hard disk space on the drive where Web Components are installed
Web Components • Media	• Intel Xeon with EM64T support • 8 GB RAM • 1 GB on the drive where the operating system is installed • 4 GB available hard disk space on the drive where Web Components are installed
iServices	• Intel Xeon with EM64T support • 8 GB RAM • 500 MB available hard disk space
Web Client and Notification Server	• Intel Xeon with EM64T support • 8 GB RAM • 500 MB available hard disk space

Component	Minimum Requirements
CRM Services (previously referred to as Talisma Services)	• Intel Xeon with EM64T support • 8 GB RAM • 1 GB on the drive where the operating system is installed • 500 MB available hard disk space on the drive where CRM Services are created
Database Administrator	• 64-bit (x64) processors, Dual-core, 2.0 GHz or faster processor • 8 GB RAM • 500 MB available hard disk space **Note**: We recommend installing Database Administrator on the computer on which you will create CRM Services.
Client • Win32 Client • Data Management Utility (DMU)	• 32-bit (x86) or 64-bit (x64) processors, Dual-core, 2.0 GHz or faster processor • 8 GB RAM • 1 GB available hard disk space on the operating system drive • 500 MB available hard disk space on the drive where Client is installed

Notes:

- For optimal system performance, it is recommended to maintain free hard disk space of at least 1 GB in the drive where the operating system is installed.
- To determine the hardware sizing for your deployment, contact Anthology Inc. Professional Services.

Software Requirements

Notes:

- For a fresh installation or upgrade of CampusNexus CRM, it is recommended to install Server components on the most recent supported operating systems and SQL Server versions.
- CampusNexus CRM is not supported on touch screens.
- Before installing any CampusNexus CRM component, ensure that all applicable updates are installed on the supported Windows operating system.

Clients and Servers

The CampusNexus CRM client and server computers require the following minimum operating system and Visual Studio versions.

Client and Server Software Requirements

Component	Requirements
Server Components	• One of the following operating systems: ◦ Microsoft Windows 2019 Standard Edition ◦ Microsoft Windows 2016 Standard Edition • Visual C++ Redistributable for Visual Studio 2019 (32-bit) • Visual C++ Redistributable for Visual Studio 2019 (64-bit)
Client Components	• One of the following operating systems: ◦ Microsoft Windows 2019 Standard Edition ◦ Microsoft Windows 2016 Standard Edition ◦ Windows 10 (32 and 64-bit) ◦ Windows 11 (64-bit) • Visual C++ Redistributable for Visual Studio 2019 (32-bit)

Components

The following software requirements are specific to the CampusNexus CRM components.

Software Requirements by Component

Component	Requirements
Database (previously referred to as Talisma Server)	• One of the following: ◦ Microsoft SQL Server 2019 Standard Edition ◦ Microsoft SQL Server 2017 Standard Edition • Microsoft ODBC Driver 13.1 for SQL Server • Microsoft Distributed Transaction Coordinator Service (MSDTC) • Microsoft Excel 365, 2019, 2016, or 2013 **Note**: The Database component has also been tested in an Active-Passive cluster environment on a Microsoft Hyper-V server.
Application Server	• Microsoft .NET Framework 4.7.2 • Microsoft .NET Framework 4.8 • Microsoft Distributed Transaction Coordinator Service (MSDTC) • For Internet connections: Microsoft IIS Server 10.0 **Note**: Application Server has been tested in a Network Load Balancing (NLB) environment.

<table>
<tr><th>Component</th><th>Requirements</th></tr>
<tr><td>Services
(previously referred to as Talisma Services)</td><td>

To work with Scheduled Report Services, you need Microsoft Excel 365, 2019, 2016, or 2013.
To work with Campaign Dispatchers, you need:

Microsoft ODBC Driver 13.1 for SQL Server
Visual C++ Redistributable for Visual Studio 2019 (64-bit)

To install Chat and Transmit Services, you need Microsoft SQL Server 2012 Native Client.

Note: To work with Campaign Dispatchers and JSF services in the Modern Auth environment, ensure that TLS 1.2 cipher suite is enabled on the server.</td></tr>
<tr><td>Web Components:

Business Administrator
WebTrak
Media
Scripting
Calendar
Transmit Tracker
Staff Authentication Service
Forms Builder Contact STS
Co-browse
</td><td>

Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8
For Internet connections: Microsoft IIS Server 10.0
Latest versions of Google Chrome or Mozilla Firefox
Microsoft SQL Server 2012 Native Client

Note: Media (Chat) has been tested in Network Load Balancing (NLB) and Network Address Translation (NAT) environments.</td></tr>
<tr><td>iServices</td><td>

Microsoft .NET Framework 4.7.2
Microsoft .NET Framework 4.8
For Internet connections: Microsoft IIS Server 10.0
Microsoft Web Service Enhancement (WSE) 3.0
</td></tr>
</table>

<table>
<tr><th>Component</th><th>Requirements</th></tr>
<tr><td>Client

• Windows Client</td><td>Ensure that the following prerequisite software is installed on the Client computer:

• Microsoft .NET Framework 4.7.2

• Microsoft .NET Framework 4.8

• Visual C++ Redistributable for Visual Studio 2019 for Windows 32-bit operating systems. The software is available in the Prerequisites\Visual C++ Redistributable for Visual Studio 2019 folder.

• Microsoft OLE DB Driver 18 for SQL Server

• Latest versions of Google Chrome or Mozilla Firefox

• To work with Print Templates, ensure that the following components are installed on the computer before the Client is installed:

◦ MS Word 2019 and MS Word 365 (32-bit or 64-bit)
◦ MS Word 2016 Standard or higher (32-bit)
◦ Visual Studio 2010 Tools for Office Runtime

• To work with Analytics for CampusNexus CRM, Microsoft Excel 365, 2019, 2016, or 2013 is required.</td></tr>
<tr><td>• Data Management Utility (DMU)</td><td>Ensure that the following components are installed on the Client computer:

• Client tools of the Microsoft SQL Server version that is identical to the version available on the Main Database computer

Ensure that the following components are installed before installing DMU:

◦ Microsoft OLE DB Driver 18 for SQL Server

◦ Microsoft Access Runtime 2016 (For MS Office 2016 and earlier)

◦ Microsoft ODBC Driver 13.1 for SQL Server

• Microsoft Access 2016 Runtime (Required only for .xlsx or .csv files)

• Microsoft Access Database Engine 2016 Redistributable (Required for Microsoft Office 365 and Office 2019 or Office 2013)

To install Microsoft Access Database Engine 2016 Redistributable, at the command prompt, type the following command and then press Enter:

<Drive name>:\AccessDatabaseEngine.exe /quiet

To verify that the installation is successful, the following program will be displayed in the Control Panel (Control Panel > Programs and Features):

Microsoft Access database engine 2016 (English)

If the above text is not displayed, the installation is unsuccessful. To complete the installation, perform the following steps at the command prompt:

1. To extract the file:

<Drive name>:\AccessDatabaseEngine_X64.exe /extract <Drive name>:\<Folder to which the file must be extracted>

2. To install the file:

msiexec /i <Drive name>:\<Folder to which the file was extracted in step 1>\aceredist.msi /quiet

• Microsoft .Net 4.8 Framework Software Development Kit</td></tr>
</table>

Component	Requirements
Database Admin-istrator	• Microsoft Management Console (MMC) • Microsoft SQL Server 2012 Native Client
SMS	• VC++ Redistributable 2019 • Microsoft ODBC Driver 13.1 for SQL Server • Microsoft OLE DB Driver 18 for SQL Server
Web Client and **Notification Server**	• Microsoft .NET Framework 4.7.2 • Microsoft .NET Framework 4.8 • Microsoft ODBC Driver 13.1 for SQL Server • For Internet connections: Microsoft IIS Server 10.0 Microsoft Web Service Enhancement (WSE) 3.0 • Microsoft OLE DB Driver 18 for SQL Server • Microsoft SQL Server 2012 Native Client **Note**: Web Client has been tested in a Network Load Balancing (NLB) environment.

Continue with Install Prerequisite Software.

Install Prerequisite Software

Properly installing the prerequisite software for CampusNexus CRM ensures that using the Installation Manager encounters few errors.

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Before you install CampusNexus CRM, ensure that:

- The IIS user account is configured to use the Domain User credentials.
- The Domain user has permissions to the Crypto folder.
- For Windows Server, the Crypto folder is available in the following path:

  `<Drive name>:\ProgramData\Microsoft\Crypto`

- There are no Remote or Linked Servers configured between the computers on which you want to install the CRM databases.

  If the Database is being installed in a time zone that provides support for automatic adjustments for DayLightSaving, perform the following steps before installing the Database component:

  1. Select **Settings**, **Control Panel** from the Start menu, and double-click the **Date/Time** icon.
  2. Click the **Timezone** tab.
  3. Select the **Automatically adjust clock for daylight saving changes** check box.

- The folder where SQL Server is installed does not contain ")" or "(" in its name. If these characters are present in the SQL Server folder name, and you install the Database afresh, the following error message is displayed:

  "Unable to configure the distributor on the Publisher machine? Contact Talisma Support for more information."

- You performed the SQLCMD and OSQL check if you are installing or upgrading the Database.

  To do so, check whether sqlcmd.exe and Osql.exe are available in the environment path.

  1. Run **sqlcmd.exe** or **Osql.exe** from the command prompt.
  2. If sqlcmd.exe and Osql.exe fail to start, add the path of sqlcmd.exe and Osql.exe to the system environment variable path. Both sqlcmd.exe and Osql.exe must be available in the path you specify.

- You are logged on to the system as a local administrator where you are installing CampusNexus CRM using a domain account.
- All SQL Server Services accounts are running under the same domain account.

- You use the same user account while installing databases on different servers.
- The MSDTC, SQL Server Agent, and Microsoft SQL Server Services are started on all the servers if you want to install the databases on different servers.
- The number of characters in the system variable path does not exceed 900.
- The SQL Server is configured to run under the Mixed Mode. CampusNexus CRM has not been tested to run under the Native or Windows Authentication mode.

  Ensure that Server Authentication option in Microsoft SQL Server Management Studio is set to SQL Server and Windows Authentication.

Continue with Install CRM Components.

Install CRM Components

The following topics guide you through the installation of CampusNexus CRM components using Installation Manager.

Global Settings

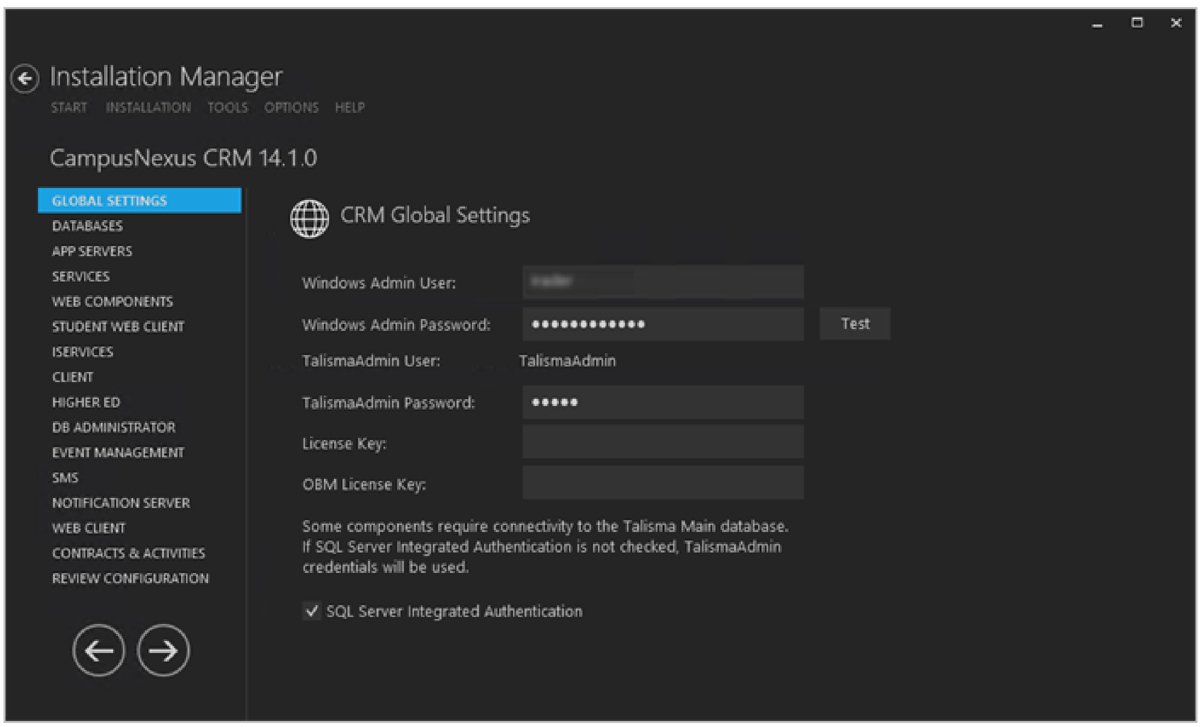
The Global Settings screen contains the password and license information used when starting an installation. Users can also test this information without moving from the screen.

CampusNexus CRM database passwords are specific to servers and SQL instances and must conform to all rules applying to the servers before setup can begin. This information must be gathered before running this tool. The information is subsequently stored in the Settings folder of the Installation Manager directory.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **CampusNexus CRM** tile. The CRM Global Settings screen is displayed.



CRM Global Settings Fields

Field	Description
Windows Admin User	User name with Administrator permissions on the computer on which the installation will occur, as well as local machine. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Windows Admin Password	Password for the Administrator user name. This password is used in the background for other installation steps.
TalismaAdmin User	When the SQL Integrated Security option is cleared, the static "TalismaAdmin" user and TalismaAdmin Password specified in Global Settings are used to install all components except the Main database.
TalismaAdmin Password	Password used when installing the application and at the time of login to the CRM application. This password applies to the TalismaAdminUser account that is used to log in to the Client component.
License Key	The CampusNexus CRM license key needs to be installed, otherwise the CRM application will be in trial mode once installed.
OBM License Key	The key for Outbound Mailer License which determines the number of Targets to whom a CRM user can send campaign mailers.
SQL Integrated Security	Select the Integrated Security check box to use this feature and click **Test** to verify the connection. Clear this check box if the database user name and password will be used. **Note**: Integrated Security must be ON if Distributor Databases are set up in the Database screen.

2. Using information gathered from Windows and the CampusNexus CRM configuration, populate the Global Settings fields. The content is used in the background by Installation Manager for subsequent steps in the installation.
3. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
4. If the user is authenticated, click **OK** and click  to continue.

Databases

The Database component is a Microsoft SQL Server that services the Main database for requests from Client, Business Administrator, and Database Administrator. The Main database is attached to the Microsoft SQL Server when the Database component is installed.

Note: The Database component was referred to as "Talisma Server" or "Talisma Main Database" in previous versions.

Preinstallation Tasks

Identify and install the prerequisite software. See [Software Requirements by Component — Database].

Important: While installing the Main database of multiple customers on a single SQL Server instance, ensure to specify unique license keys for each customer database. You can specify the license key when installing the database in the Global Settings screen of Installation Manager or while running the setup.exe of the Database component.

- Uninstall and reinstall MSDTC service on the computer where you plan to install the Database component. To do so:
    1. Log in as the administrator of the computer.
    2. Open the command prompt and run the **MSDTC -uninstall** command.
    3. Restart the computer.
    4. Type **Services.msc** in the Run dialog box. The Services screen is displayed.
    5. Ensure that the **Distributed Transaction Coordinator** service is removed from the list.
    6. Open the command prompt and run the **MSDTC -install** command.
    7. Open the **Services.msc** and set the **Startup type** for the **Distributed Transaction Coordinator** service to **Automatic**.
- In a distributed server scenario, ensure that the SQL Server Agent service is stopped on all the servers.
- In an environment where the Main database and Subscriber database have to be installed, ensure that you complete the installation of the Main database followed by the Subscriber database.

Notes:

- After installing the Database component in a distributed environment, depending on the permission of the SQL Login of the user who performed the installation, the option in the Linked Server Properties dialog box for the Publisher and Subscriber databases is set to the following:
    - **Be made using the login's current security context** – If the SQL Login has the sysadmin Role.
    - **Not be made** – If the SQL Login does not have the sysadmin Role.

- The recommended option to be set in the Linked Server Properties dialog box is **Be made using the login's current security context**. However, if you want to further tighten the security for connecting with the linked servers, you can select the **Not be made** option. When this option is selected, even if the user has sysadmin permission, the user will not be able to access the databases of the Linked Server. The user must be explicitly mapped to the appropriate users in the **Local server login to remote server login mappings** area to perform the required operations.

  For example, to run a CampusNexus CRM installer, the user must be added as a Local Login in the **Local server login to remote server login mappings** area and the Remote User must be a SQL Login that has SQL Server Authentication with sysadmin permission on all the Subscriber databases.

Preinstallation Tasks in a Distributed Environment

- Before installing a Subscriber database (Analytics, Archive, Media, or WebTrak), ensure that the **Require distributed transactions for server-to-server communication** option in MS SQL Server Management Studio is cleared.
- Ensure that the Windows user who installs the Database component has a corresponding SQL Login with sysadmin role.

Installation in a Cluster Server Environment

- Configure and install the Main database, Distributor database, and all Subscriber databases on the Primary Node (Active) of the MS Cluster Server.
- Provide the path of the Cluster Disk for the target and backup folders of the Database component during installation.

Note: It is not mandatory to install Distributor and Subscriber databases in a clustered environment. The Destination directory should be on a shared drive.

On the Database screen in Installation Manager, use the following options for the Main database, Distributor database, and all Subscriber databases:

- Specify the SQL Cluster Name in the **SQL Server** field.
- Select the **Cluster** check box.
- Enter the name of the Active cluster node in the **Cluster Node** field.

For more details, see Cluster Server Environment.

Support for Multiple Databases on a Single Server

In previous versions, multiple versions of the Database component could not be installed on a single SQL Server instance. In this release, CampusNexus CRM provides the ability to install multiple versions of the Database component on a single SQL server instance. On a single Database, databases of multiple customers can be installed and hosted simultaneously.

Important: You can install only one of the following:

- Multiple versions of Database and its components (such as Higher Education Foundation, and Event Management on a single SQL Server instance.
- Database of a single customer along with other components.

You cannot install multiple versions of Databases and other components such as Application Server, Services, Web Components, Web Client, Client, or Data Management Utility on a single computer.

This enhancement has the following impact on CampusNexus CRM:

- **Services** – In previous releases, Health Check Service, Job Service, and Offline Sync Service were created by the Database installer. In this release, you can create these services using Database Administrator on any computer.

  Note: In this release, Offline Service is renamed to Webform Sync Services.

  In addition, Scheduled Report (TLRptXL.exe) will also be removed. You can create this service using Database Administrator on any computer.

- **Database folders** – While installing the Database component, you must specify the name of the Main databases of multiple customers being installed. For example, if you are hosting databases of WorldWaves University and Global Education Society, you can specify the database names as **WorldWaves_tlmain** and **Global_tlmain** during the installation process. When the installation is complete, the following folders are created on the computer where the Database component is installed:

  For WorldWaves-tlmain

  <Drive name>:\Program Files\Common Files\Talisma Shared\WorldWaves_tlMain\

  <Drive name>:\Program Files(x86)\Common Files\Talisma Shared\WorldWaves_tlMain\

  <Drive name>:\TalismaServer\WorldWaves_tlmain

  For Global-tlmain

  <Drive name>:\Program Files\Common Files\Talisma Shared\Global_tlMain\

  <Drive name>:\Program Files(x86)\Common Files\Talisma Shared\Global_tlMain\

  <Drive name>:\TalismaServer\Global_tlmain

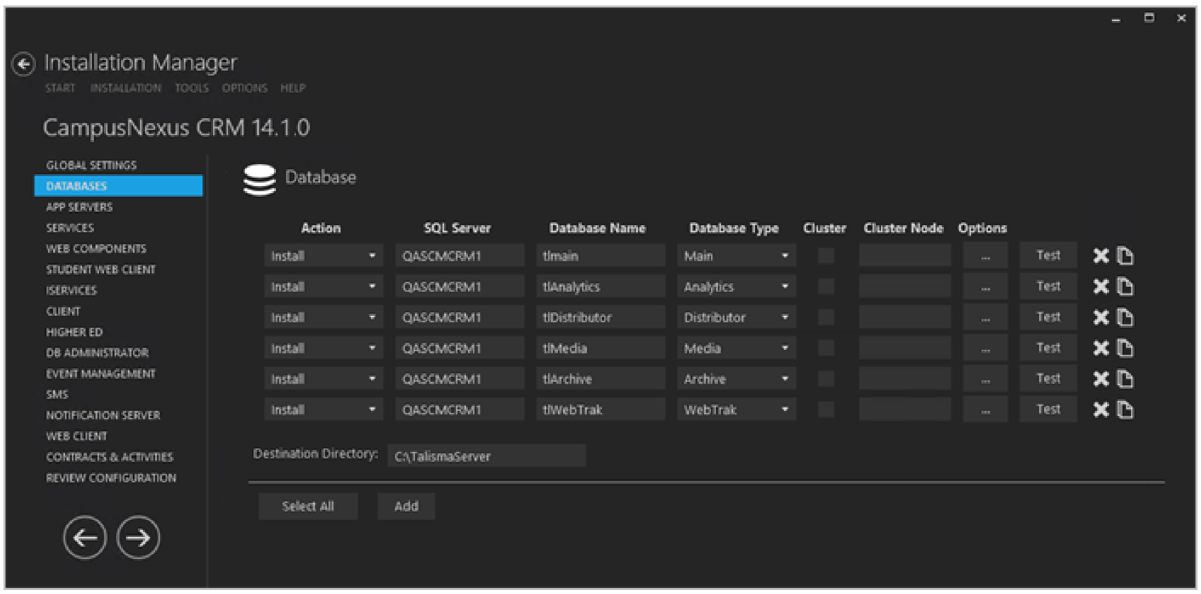
- **Setup Logs** – Log folders are suffixed with the database name. For example, if the name of the WorldWaves database is WorldWaves-tlmain, log files of the WorldWaves database will be stored in the <Drive name>:\Program Files\Common Files\Talisma Shared\SetupLog\WorldWaves-tlmain folder.

- **Registry keys** – Registry key folder suffixed by the database name is created in the HKEY_ LOCAL_ MACHINE\SOFTWARE\Talisma\Talisma Server\<database name> path. For example, if the database name specified during the installation of Database is WorldWaves- DB, the registry keys are created in the HKEY_ LOCAL_MACHINE\SOFTWARE\Talisma\TalismaServer\WorldWaves-tlmain path.

- The **TLSchExport.exe** will now be copied in the <Drive name>:\Program Files (x86) \Common Files\Talisma Shared\<database name> path. Hence, if you have multiple versions of database installed on a single SQL server instances, TLSchExport.exe will be available for every database.

Set Up Databases

1. In the Installation menu, click **Database**. The Database Settings screen is displayed.



The Database screen contains configurable fields that users can change to add, delete, copy, and test databases being used in an installation. The elements of this screen are unique to the CampusNexus CRM installation.

Note: Ensure that the default SQL Server settings are appropriate.

- Installation Manager supports multiple databases (listed in the Database Type column), but only one type of database is allowed to be installed at a time on one machine.
- Multiple databases cannot be installed on the same SQL Server at the same time.
- Different Database Types can be installed on different SQL servers at the same time.
- To install multiple Main databases on a same server, one must be set to **Install**, but the other Main database must be set to **None**.
- A Main database must be present on this screen with action set to **None**, even if the Main database is not going to be installed.
- All Subscriber databases must be pointed to a Main database.

2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Detach** – Detaches one Subscriber database at a time per machine. Action can be set to Detach on multiple Subscriber databases on multiple servers at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features. Select **Uninstall** from the Action menu to Uninstall all databases on the SQL Server.

     Important: Main and Subscriber databases attached to the Main database on the same machine will be uninstalled.
   - **Reinstall** – Retries to install a subcomponent.
   - **InstallFailover** - Installs a cluster failover component.
   - **AttachFailover** - Attaches a cluster failover component.
   - **DetachFailover** - Detaches a cluster failover component.
   - **ReinstallFailover** - Reinstalls a cluster failover component.
   - **UninstallFailover** - Uninstalls a cluster failover component.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Specify the name of the **SQL Server** on which the database resides. User credentials from the Global Settings screen are used to access this server.

   If CampusNexus CRM is installed in an SQL cluster environment, specify the SQL cluster name (not the node name) in the **SQL Server** field.
5. Specify the **Database Name** of a valid CampusNexus CRM database. User credentials supplied in the Global Settings screen are also valid for this database.
6. Select the **Database Type**. The following Database Types are available:
   - Main
   - Analytics
   - Distributor
   - Media
   - WebTrak
   - Archive

7. If CampusNexus CRM is installed in an SQL cluster environment, select the **Cluster** check box and specify the name of the *Active* cluster node in the **Cluster Node** field for the Main database, Distributor database, and all Subscriber databases.

   If a failover cluster is deployed, enter Failover Node name in the **Cluster Node** field and select an appropriate failover action in the **Action** field.

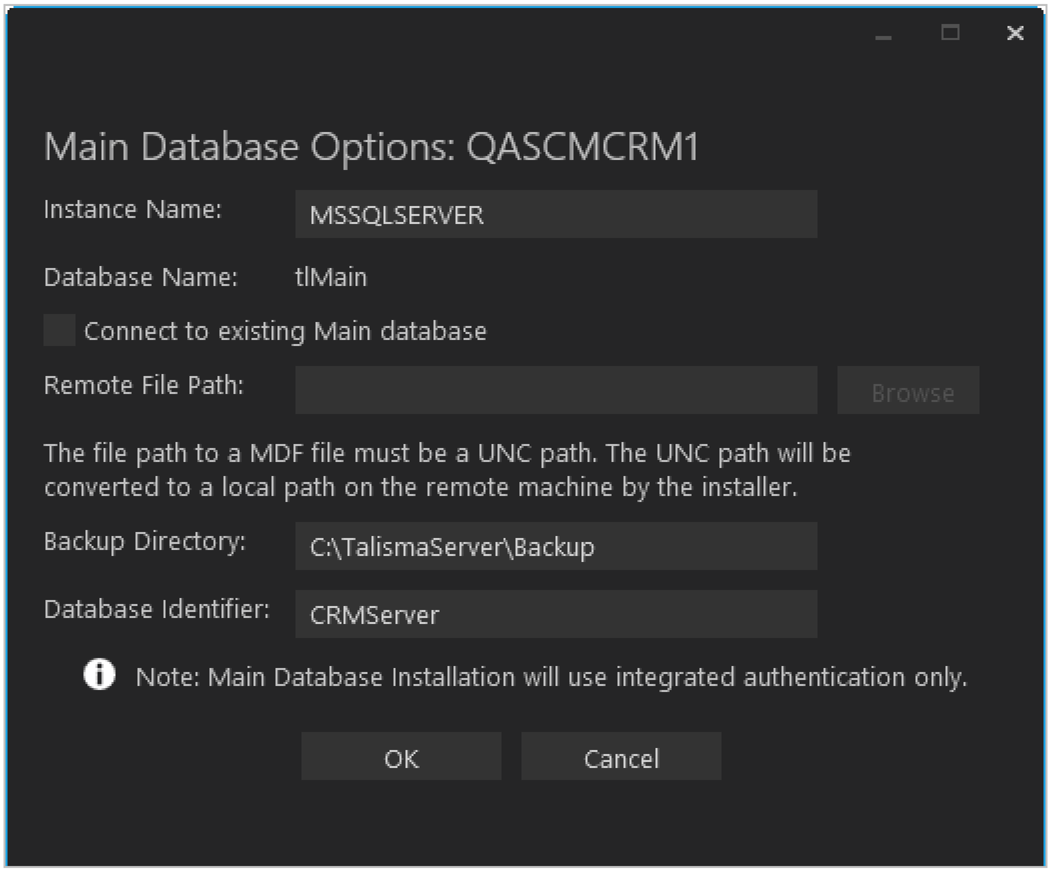
   Refer to Cluster Server Environment for additional instructions.

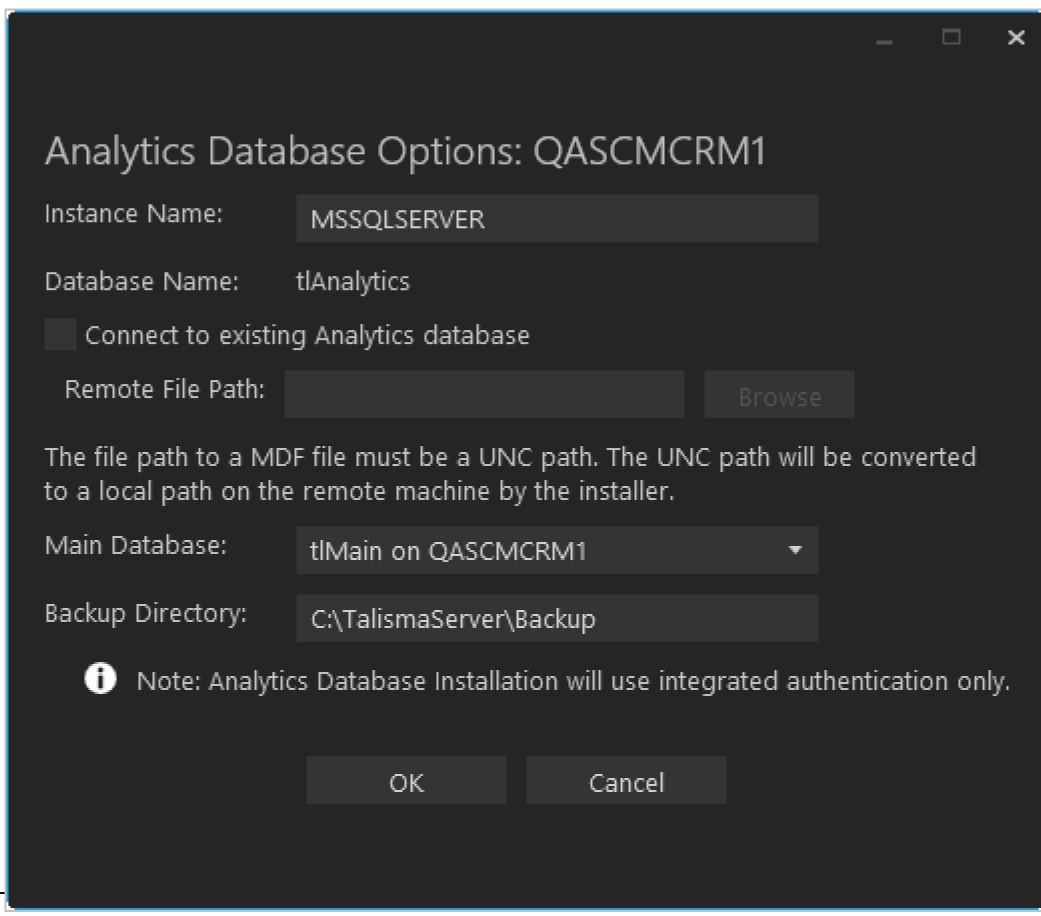
8. Click to copy a line. Edit the copied line as needed.

   Copy as many lines as needed to create the Database / Database Type combinations required for the installation.

9. Click ··· to view and edit the Options form for each Database / Database Type combination. Options forms include the following:

   - Main Database Options
   - Analytics Database Options
   - Distributor Database Options (**Note**: Distributor databases can only be run with SQL Integrated Authorization turned. See Global Settings.)
   - Media Database Options
   - WebTrak Database Options
   - Archive Database Options


Main Database Options: QASCMCRM1
Instance Name:
MSSQLSERVER
Database Name:
tlMain
Connect to existing Main database
Remote File Path:
Browse
The file path to a MDF file must be a UNC path. The UNC path will be converted to a local path on the remote machine by the installer.
Backup Directory:
C:\TalismaServer\Backup
Database Identifier:
CRMServer
Note: Main Database Installation will use integrated authentication only.
OK
Cancel


Analytics Database Options: QASCMCRM1
Instance Name:
MSSQLSERVER
Database Name:
tlAnalytics
Connect to existing Analytics database
Remote File Path:
Browse
The file path to a MDF file must be a UNC path. The UNC path will be converted to a local path on the remote machine by the installer.
Main Database:
tlMain on QASCMCRM1
Backup Directory:
C:\TalismaServer\Backup
Note: Analytics Database Installation will use integrated authentication only.
OK
Cancel

Database Options Fields

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Instance Name</td><td>SQL Server instance name where server will be installed.</td></tr>
<tr><td>Database Name</td><td>Machine Name on the Database Settings screen.

To connect to an existing Main database, users must select Connect to existing Main database and add the remote file path for the MDF.</td></tr>
<tr><td>Connect to existing <Database Type> database</td><td>Select to connect to the named Database Type.</td></tr>
<tr><td>Remote File Path</td><td>The Universal Naming Convention (UNC) path of the share where the Main Database File (MDF) exists. Becomes active when Connect to existing Main database is selected. The MDF can exist on the local machine.

Click Browse to open a File Dialog to browse to the UNC path of the share where the MDF exists. The Installer converts the UNC path to a local path on the remote machine.</td></tr>
<tr><td>Backup Directory</td><td>Use this field to specify the backup directory for the database.</td></tr>
<tr><td>Database Identifier</td><td>This field is displayed for the Main database only. Unique database identifier consisting of 3-10 characters.

The Database Identifier appears in the Subject line of outgoing messages, therefore identifying from which server the email message was sent. This line only appears if the interaction ID in the Subject Threading Model is selected when configuring an Alias. All database installation is done using integrated authentication only.

Note: Use only supported characters as part of the Database Identifier. Do not use the following characters:

Unsupported Characters for Database Identifier
<table>
<tr><th>Character</th><th>Description</th></tr>
<tr><td>[ ]</td><td>square brackets</td></tr>
<tr><td>\</td><td>backslash</td></tr>
<tr><td>& CR</td><td>ampersand followed by carriage return (CR)</td></tr>
<tr><td>& including LWS</td><td>ampersand including linear white space (LWS), i.e., any number of spaces, horizontal tabs, or newlines</td></tr>
</table></td></tr>
<tr><td>Main Database</td><td>This field is displayed in the Options screens for databases other than Main. Select the Main database from the drop-down list.

Note: The Database Options forms must point to the proper Main database. Database Types with the same name can point to different Main databases. Some users might have a different Instance Name for the default SQL server; this name would be changed in the Options form.</td></tr>
</table>

10. Click **OK** to save changes on the Options form. The form is closed.

11. Click  to delete a selected line.
12. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.

    To install a Database to a custom path, type the path in the Destination Directory text box. This appends the directory location with Main database name at the time of install.

    For example for Main database called ASUMainDB, the default destination directory would be C:\TalismaServer\ASUMainDB and a Subscriber database attaching to this Main database would go under ASUMainDB directory.
13. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
14. If all tests pass, click .

Postinstallation Tasks

- After installing the Database component, it is mandatory to restart the computer.

  In a scenario where multiple customer Main databases are installed, you must restart the computer after installing the Main database of the first customer. Restarting the computer after subsequent installations of other customer databases is optional.
- Start the SQL Server Agent service manually. Ensure that the service is running in a domain user account which has administrative privileges.
- In a distributed server scenario, ensure that the value of the Data Access option is True in the Linked Servers Properties dialog box for all the computers where CampusNexus CRM databases are installed. To do so:
  1. Open **SQL Server Management Studio**.
  2. Navigate to the **Server Objects\Linked Servers** folder.
  3. Right-click on the server name and select **Properties** from the shortcut menu. The Linked Server Properties screen is displayed.
  4. Click the **Server Options** in the left pane.
  5. In the right pane, ensure that the value of the **Data Access** option is set to **True**.
- Ensure that the Talisma-CreatePreDefObjects job has already run. To do so:
  1. Start **Microsoft SQL Server Management Studio**.
  2. Navigate to the **Jobs** node under the **SQL Server Agent** node.

3. Locate the **Talisma-CreatePreDefObjects** job, and confirm that the **Enable** option is dimmed.

- Check the Replication Monitor settings. To do so:
  1. Start **Microsoft SQL Server Management Studio**.
  2. Navigate to the **Replication** node. Right-click on the Replication node and select **Launch Replication Monitor**.
  3. In the Replication Monitor, check whether the **Snapshot Agent**, **Distributor Agent**, and **Subscriber Agent** are created, and whether the **Initial Snapshot** has been generated.
- If errors are encountered during the setup of the Main database, check all log files in the **<Drive name>:\Program Files\Common Files\Talisma Shared\Setuplog\<database name>** path.
- When the Database component is installed afresh, by default the value of the Recovery model option for Database is set to **Simple**. Perform the following step for Distributor Server, Analytics Server, Media Server, and WebTrak Server:
  1. Start **Microsoft Server Management Studio**.
  2. Navigate to <Server name>, <Database name for which the Recovery model has to be set>.
  3. Right-click and select **Properties** from the shortcut menu.
  4. Select **Options** and set the **Recovery model** option to **Full**.
- In a distributed server environment, on the computer where Main database is installed, navigate to the **Securities** tab of the Linked Server Properties dialog box, and set the login name (format: Talisma<Main database name>) and password details for subscriber database servers.

  Ensure that the login name is set in the **Local Login** and **Remote User** fields, and the password must be identical to the value set in the **Talismaadmin Password** field of the CRM Global Settings screen.

  Perform the same step on computers where subscriber databases are installed, i.e., set the same login name and password details for the linked server of Main database server.
- To create non-clustered indexes for ReportMailer and CampaignTarget, run the following script on the computer where the Main database is installed:

```
If Not Exists(Select Top 1 1 From sys.indexes Where name = 'IDX_tblOBMReportMailer_nCustomerID_
nBaseObjectType' And Object_ID = OBJECT_ID('tblOBMReportMailer'))
Begin
CREATE NONCLUSTERED INDEX IDX_tblOBMReportMailer_nCustomerID_nBaseObjectType
ON [tblOBMReportMailer] ([nCustomerID],[nBaseObjectType])
End
GO
If Not Exists(Select Top 1 1 From sys.indexes Where name = 'IDX_tblCampaignTarget_nCustomerID_
```

```
nBaseObjectType' And Object_ID = OBJECT_ID('tblCampaignTarget'))
Begin
CREATE NONCLUSTERED INDEX IDX_tblCampaignTarget_nCustomerID_nBaseObjectType
ON [tblCampaignTarget] ([nCustomerID],[nBaseObjectType])
End
GO
```

- For scheduled export configurations to run in the current version, perform the following steps on the Main database computer:
  1. In the Properties dialog of the scheduled export job, navigate to **Steps**, **Export Step**, **Edit**.
  2. Specify the full path of the tlschexport.exe in the following format

     `’“<Drive name>:\<path>\tlschexport.exe”. . . . .other details’`

     Ensure that the double quotation marks are specified at the beginning (after the single quotation mark) and after `tlschexport.exe`. The single quotation marks must continue to be specified at the beginning and at the end.

Note: When the Analytics database is moved to a different computer and the Analytics database is attached, jobs specific to scheduled reports will not migrate to the new computer. In this scenario, run the stored procedure sproc_CreateScheduleReportJobForUpgrade after the attachment operation is complete:

- To create all scheduled jobs in the database after it is attached, type the command **Exec sproc_CreateScheduleReportJobForUpgrade N''**
- To create a specific job, type the command **Exec tsproc_CreateScheduleReportJobForUpgrade N'50'**
- To create specific jobs in the attached database, type the command **Exec sproc_CreateScheduleReportJobForUpgrade N'50,100,150'**

In the second statement, the value 50 is an example of a schedule ID. In the final statement, the values 50, 100, and 150 are examples of schedule IDs. The comma character (,) is used as a separator when multiple IDs are specified.

These IDs can be identified from the aScheduleID column of the tblReportSchedule table in the Analytics database.

Database Version in Control Panel

When the Database component is installed, an entry is recorded in the Programs and Features screen of Control Panel. If a single version of Database is installed on a SQL Server instance, the version number of the installed Database is displayed in the Version column. If multiple versions of Database are installed on a single SQL Server instance, the value "Multiple versions" is displayed in the Version column.

Note: You cannot uninstall Database through Control Panel. To uninstall Database, use the **Uninstall** option in Installation Manager.

Application Servers

The Application Server component handles all application operations between client computers and databases. It increases the scalability of the product by maintaining the client connections and their state, thereby relieving the Database server of a huge load.

Application Server uses connection Objects to create a temporary connection between various clients and databases and executes client requests. Once a request is executed, the connection is closed and the Object is returned to the connection pool.

Preinstallation Tasks

Identify and install the prerequisite software. See Software Requirements by Component — Application Server.

- If you are installing Application Server on a Windows NLBS cluster and connections to Application Server are made through HTTP (with load balancing), follow these steps:

  1. Ensure that:

     - Application Server is installed on all NLBS host machines.
     - Virtual root names of Application Server are identical on all servers.

  2. Execute **sproc_AddMachinestoNLBS** with the following parameters:

     - **Parameter1**: @tNLBS: This parameter represents the virtual IP address of the NLBS Cluster.
     - **Parameter2**: @tMachines: This parameter contains the list of computer names that are part of the NLBS Cluster.

       The computer names must be separated by the comma delimiter. For example, Exec sproc_AddMachinestoNLBS N'172.17.32.100', N'HostMac1, HostMac2'

  3. Ensure the following are configured in the Windows Firewall Settings dialog box:

     - In the **Exceptions** tab, select the **COM+ Network Access**, **Distributed Transaction Coordinator**, and **COM Surrogate** check boxes.
     - Select the **Notify me when Windows Firewall blocks a new program** check box.

- When connecting to Application Server using HTTP, we recommend that you modify the settings in the Web.config file as indicated below:

```
<httpRuntime
executionTimeout="900"
maxRequestLength="5248"
useFullyQualifiedRedirectUrl="false"
minFreeThreads="8"
```

```
minLocalRequestFreeThreads="4"
appRequestQueueLimit="2000"
enableVersionHeader="true"
/>
```

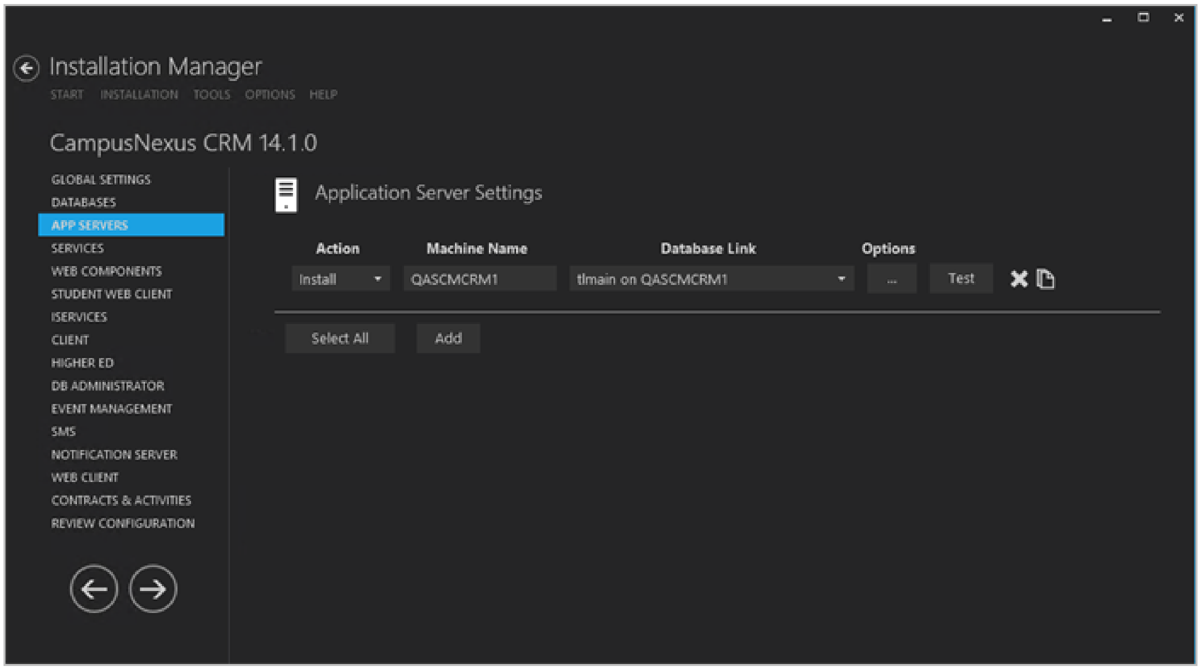
These settings are explained below:

- `executionTimeout`="[seconds]": This attribute represents the time (in seconds) before a request automatically times out.
- `maxRequestLength`="[KBytes]": This attribute indicates (in kilo bytes), the maximum size for a request that can be accepted.
- `useFullyQualifiedRedirectUrl`="[true|false]": This attribute indicates whether the URL for Client redirects must be fully qualified.
- `minFreeThreads`="[count]": This attribute specifies the minimum number of free threads to enable the execution of new requests.
- `minLocalRequestFreeThreads`=" [count] ": This attribute specifies the minimum number of free threads to enable execution of new local requests.
- `appRequestQueueLimit`="[count]": This attribute specifies the maximum number of requests that can be queued for the application.
- `enableKernelOutputCache`="[true|false]": This attribute indicates whether the http.sys cache must be enabled on IIS 7.5 and higher versions. By default, this value is True.
- `enableVersionHeader`="[true|false]": This attribute indicates whether the X-AspNet-Version header must be output with each request.

The **Web.config** file is located in the folder in which Application Server is installed.

Set Up Application Servers

1. In the Installation menu, click **App Servers**. The Application Server Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

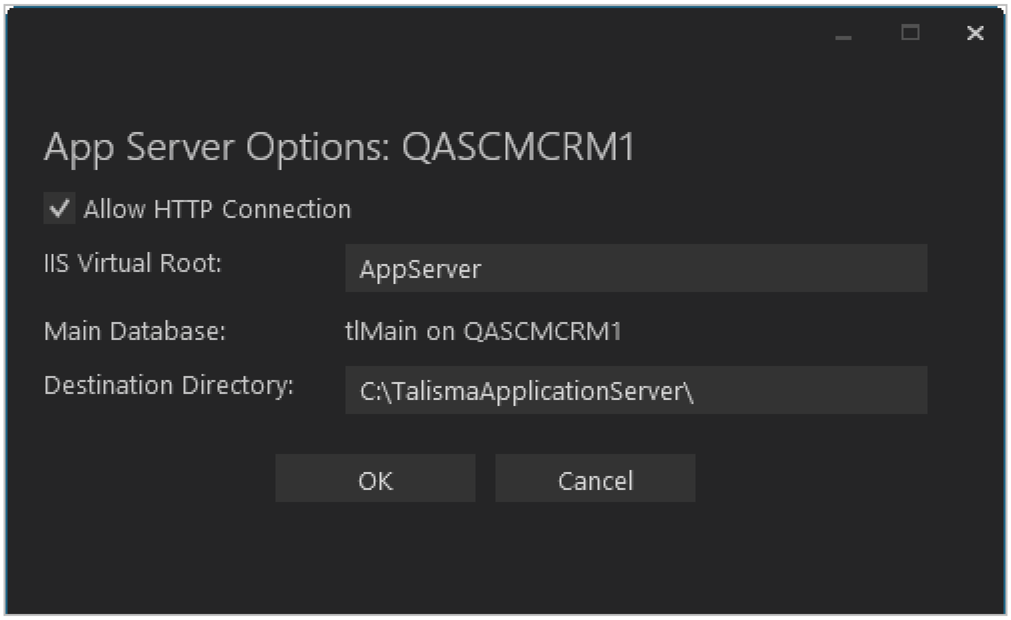
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
   - **Reinstall** – Retries to install a subcomponent.
   - **Add** – Installs an additional component on the computer where one or more components already exist. You can add only one component at a time.
   - **Remove** – Uninstalls a single component. You can remove only one component at a time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.

5. Select a **Database Link** for Application Server.

6. Click  to view and edit the Options form.



Options Fields

Field	Description
Allow HTTP Connection	Enables a connection from Client to Database through HTTP or HTTPS. The check box is selected by default.
IIS Virtual Root:	If Allow HTTP Connection is selected, the IIS Virtual Root text box is enabled and you can change the name of IIS virtual root. If the check box is cleared, the IIS Virtual Root text box remains blank and Application Server uses DCOM configuration. For a **Trusted log on**: <Application Server Name>_Trusted. This virtual root is used for authenticating Trusted Security Users over HTTP. This virtual root is created for users who will log on to Application Server using a trusted connection. The user will not be required to specify information in the above format to log on to Application Server. This information will be automatically interpreted when the user logs on to the computer on which Application Server is installed. For an **Application or Custom log on**: <Application Server Name>.
Main Database	Main database and name of the database server selected in the Database Settings screen.
Destination Directory	The destination directory of the Main Database File (MDF) for Application Server.

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.

10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

11. If all tests pass, click .

Note: Trace logs for Application Server must be enabled only from Talisma Trace Client available in the Application Server installation folder. While trace logs for other components can also be enabled from this location, Application Server traces cannot be enabled from Talisma Trace Client available in other locations.

Perform Other Operations

Restart the Application Server

1. From the **Start** menu, select **Programs, Administrative Tools, Component Services**. The Component Services screen is displayed.

2. Browse to the following path: `Console Root/Component Services/Computers/My Computer/COM+ Applications`

3. Right-click **ApplicationServer**, and select **Shut down** from the shortcut menu.

4. Right-click **ApplicationServer**, and select **Start** from the shortcut menu.

Notes:

Ensure that Application Server is restarted in the following scenarios:

- When a CampusNexus CRM license is updated.
- When a database is configured after the installation of Application Server.
- When the date or time has been modified on Application Server.
- When one or more of the following values are modified in the TalismaObjectAssembly.Config file, which is located in the Talisma Shared folder:
    - Compression size
    - Poll Interval
    - Pool Size
    - Internal Account Password

Restart the IIS Server if HTTP Connection Has Been Specified

1. From the **Start** menu, select **Run**. The Run dialog box is displayed.

2. Type **iisreset** in the Open field.

3. Click **OK**. The IIS Service is stopped and restarted.

Configure a Local User Account for Application Server

By default, Application Server is configured to run using an interactive account, which is for the User who is currently logged on. It is recommended that you configure Application Server to run under an Account that has been granted administrative privileges. To do so:

1. From the **Start** menu of the Application Server computer, select **Settings, Control Panel**. The Control Panel is displayed.
2. Double-click the **Administrative Tools** icon. The Administrative Tools screen is displayed.
3. Double-click the shortcut for **Component Services**. The Component Services screen is displayed.
4. Expand the following nodes: **Component Services, Computers, My Computer, COM+ Applications**. All COM+ applications are listed.
5. Right-click **Application Server**, and select **Properties** from the shortcut menu. The COM+ Application Server Properties dialog box is displayed.
6. Select the **Identity** tab.
7. In the **Account** area, select the **This user** option, and click **Browse** to locate a User who has administrative privileges on the Application Server computer.
8. Specify a password for the User in the **Password** field.
9. Type the password again in the **Confirm Password** field.
10. Click **OK**. Application Server is now configured to run using a local administrator account.

If you have installed iServices, carry out the following steps for each iService:

1. Select an iService component node.
2. Right-click on the node, and select **Properties** from the shortcut menu. The relevant Properties dialog box is displayed.
3. Click the **Identity** tab.
4. Select the **This User** option.
5. In the **User** field, click **Browse** to select the domain **User name**.
6. In the **Password** field, type the password of the domain User account.
7. In the **Confirm password** field, type the password you have specified in the Password field.
8. Click **OK**. The Properties screen is closed.
9. Start the Service of the iService component node. To do so, right-click on the iService component node you have selected in step **1**, and select **Start** from the shortcut menu.
10. Close the Component Services screen.

Create a Local User Account on the Computer on which the Application Server is Installed

You can create a local user account so that it is accessible even without logging on to the computer. To do so, follow these steps:

1. From the **Start** menu, select **Programs, Administrative Tools, Computer Management**. The Computer Management screen is displayed.
2. Browse to the following path: `Computer Management/System Tools/ Local Users and Groups/Users`.
3. Right-click in the right pane and select **New User** from the shortcut menu. The New User dialog box is displayed.
4. Type the required details.
5. Clear the selection for the **User must change password at next logon** option.
6. Select the **User cannot change password and Password never expires** options.
7. Click **Create**.

The local user account is created on the computer on which Application Server is installed.

Set the Cache Refresh Interval

On the computer where Application Server is installed, the value of the cacherefreshtime tag in the application.config file is set to 180, which indicates that the Application Server cache is refreshed every 3 minutes. The file will be available in the Installation folder.

It is recommended to set the value of cacherefreshtime Key to 14400 to ensure that the Application Server cache is not refreshed frequently.

```
<add key="CacheRefreshTime" value="14400" />
```

When the value of the cacherefreshtime tag is set to 14400, the Application Server cache is refreshed at the interval specified in this tag. Operations performed in Business Administrator such as creation of Users, Teams, Rules, and enabling Permissions to Users and so on will be reflected in Web Client only when the Application Server cache is refreshed.

For the operations performed in Business Administrator to be reflected immediately, perform the following steps on the computer where Application Server is installed:

1. Reset IIS.
2. Shut down and start the Application Server COM + Component. To do so:
    a. From the **Control Panel**, open **Administrative Tools**, and double-click **Component Services**.
    b. Navigate to the **Component Services, Computers, My Computer, COM+ Applications** node.

c. Select the **ApplicationServer** node.

d. Right-click the **ApplicationServer** node and select **Shut down** from the shortcut menu.

e. Right-click the **ApplicationServer** node and select **Start** from shortcut menu.

Configure Databases

You can configure additional connections to the database.

1. From the **Start** menu, select **Settings, Control Panel**.
2. Double-click **Add/Remove Programs**.
3. From the list of programs, select **Application Server <version number>**.
4. Click **Change/Remove**. The Add/Remove/Reinstall dialog box is displayed.
5. Click **Configure Databases**. The Configure Database Servers page is displayed. Configure additional HTTP or DCOM connections to Application Server.

Configure the File Size for Compression

The file size for compression can be configured for Application Server and Client. By default, compression is disabled when connections to Application Server are made over a Local Area Network (LAN). To enable compression:

1. On the computer where Client is installed, run **Regedit** from the command prompt. The Registry Editor is displayed.
2. Browse to the following key: **HKEY_LOCAL_MACHINE\SOFTWARE\Talisma\Common\ConnectionParameters\LAN**
3. Right-click the **DWORD** values Request and Response, and select **Modify** from the shortcut menu. The Edit DWORD Value dialog box is displayed.
4. Specify the required data size in the **Value data** field, after selecting **Decimal** in the **Base** area. Compression is enabled for DCOM connections. Requests and responses that are greater than or equal to the specified size are compressed.

Notes:

- By default, the value for the Request and Response DWORDs for the LAN key is 0, indicating that compression is disabled. Setting a value greater than 0 enables compression.
- Values specified in the **Value data** field must be in bytes, indicating the file size for which compression must be enabled.

By default, data greater than or equal to 1024 bytes will be compressed when connections to Application Server are made over HTTP. You can modify this value. To do so:

1. Browse to the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Talisma\Common\ConnectionParameters\Internet
2. Modify the DWORD values Request and Response, and specify the required data size in the **Value data** field, after selecting **Decimal** in the **Base** area.

Postinstallation Tasks

Add Client User Details to the Distributed COM Users Group

On the Application Server and Database Server computers, perform the following steps:

1. Right-click the **My computer** icon, and select **Manage** from the shortcut menu. The Server Manager screen is displayed.
2. In the left pane, navigate to the **Configuration, Local Users and Groups, Groups** node.
3. In the right pane, right-click the **Distributed COM Users** group, and select **Add to Group** from the shortcut menu. The Distributed COM Users Properties dialog box is displayed.
4. Click **Add**. The Select Users, Computers, or Groups dialog box is displayed.
5. In the **Enter the object names to select** area, specify the names of the users you want to add to the **Distributed COM Users** group. Use a semicolon (;) to separate the names of multiple users.
6. Click **Check Names**.
7. Click **OK**. The users are added to the group.
8. Click **OK**.

Configure the Logoff Setting in the Local Group Policy Editor

On the computer on which Application Service is installed, perform the following steps:

1. Click **Start**, **Run**, type **gpedit.msc**, and click **OK**. The Local Group Policy Editor is displayed.
2. Navigate to **Computer Configuration, Administrative Templates, System, User Profiles**.
3. Double-click **Do not forcefully unload the users registry at user logoff**.
4. Select **Enabled**.
5. Click **OK**.
6. Close the Local Group Policy Editor.
7. Restart the Application Server computer.

Services

The Services screen is used to install, upgrade, or uninstall the following service types:

- **DBAdminService** (previously referred to as 'CRM Service' or 'Talisma Services'): This service type upgrades the following CampusNexus CRM services.
  - JobService
  - Webformservice
  - Healthcheckservice
  - Dispatcher service
  - Scheduled report service

  When you run the Server setup, only the Database server will be upgraded. To upgrade CampusNexus CRM Services, you must run the DBAdminService setup. This procedure is applicable if Database and Services are available on the same computer or multiple computers.

- **ChatService**: This service type is associated with the Web Components that support chat.

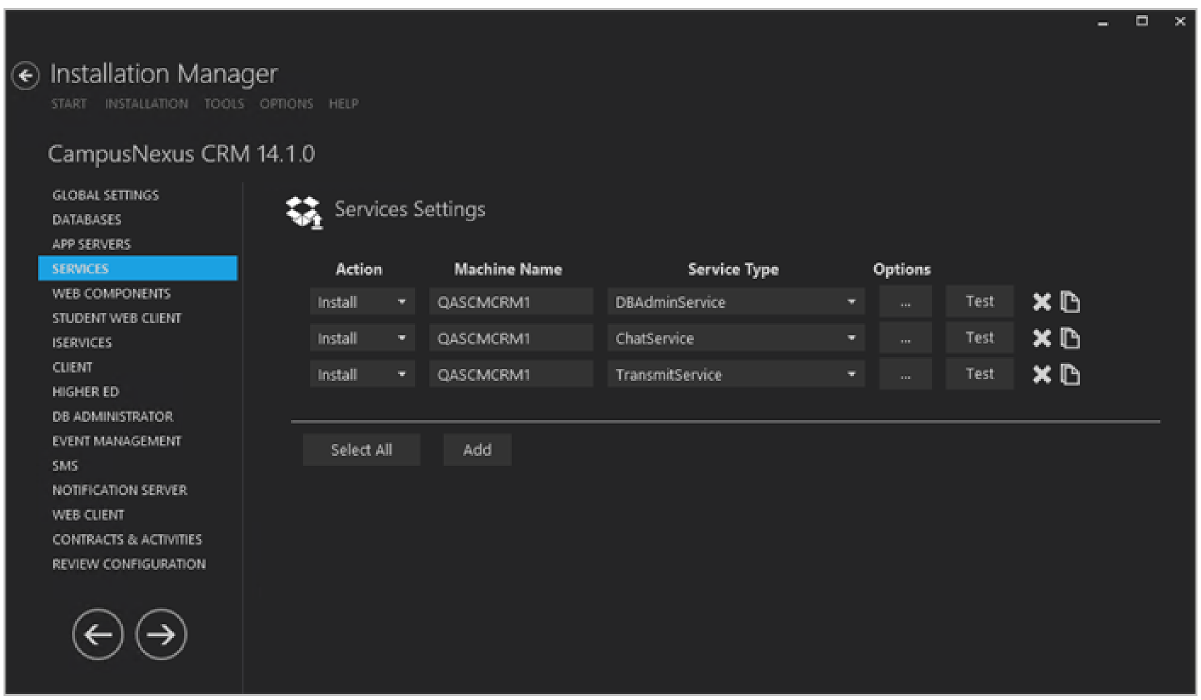
- **TransmitService**: This service type is required for TransmitTracker.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — Services.

Set Up Services

1. In the Installation menu, click **Services**. The Services screen is displayed.



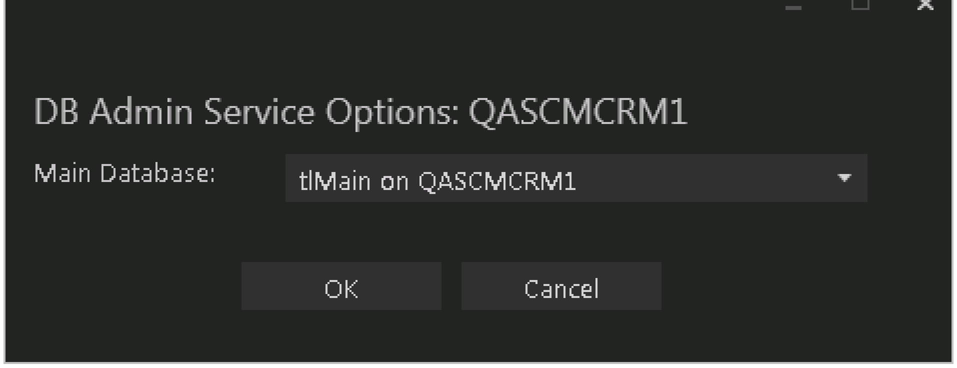
2. Click **Add** to add a line to the Settings screen.

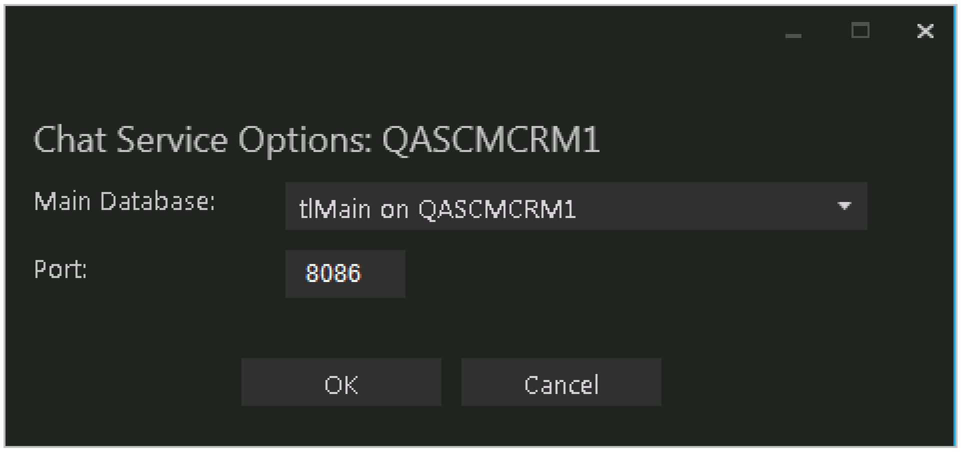
3. Select an appropriate **Action**. The following Action values are available:

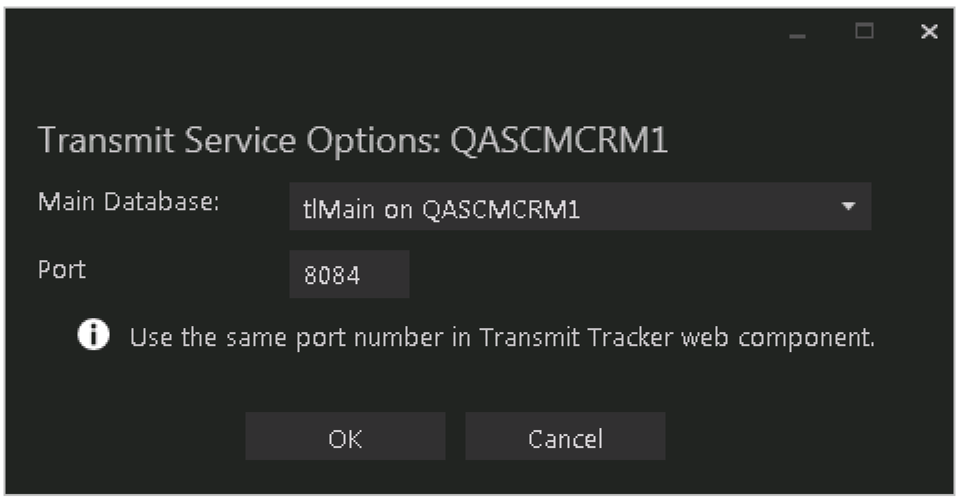
- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Upgrade** – Performs an upgrade of the CRM Services.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Select the **Service Type**. The following Service Types are available:
   - DBAdminService
   - ChatService
   - TransmitService
6. Click  to copy a line. Edit the copied line as needed.
7. Click  to view and edit the Options form for the selected Service.
   a. Select the **Main Database** to be used by each Service.
   b. For ChatService and TransmitService specify the **Port** number or accept the default.







8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

Web Components

The Web Components screen enables you to install the following Web Components:

- **Business Administrator** — Installs the Business Administrator component. You can log on to Business Administrator using any computer over the network if the computer has Microsoft Internet Explorer 11.0 or later installed on it. You can create aliases, users, and teams, specify their roles, create rules, and use other administration features of CampusNexus CRM.
- **Media** — Installs the files required for chat or any media integrated with CampusNexus CRM. It creates a virtual root on the selected server for the Chat module.
- **Scripting** — Installs a presentation tool that you can use to create a sequence of Frequently Asked Questions (FAQs) and their answers that help agents provide solutions to customers in a call center. It ensures standardization of responses and enables call centers to draw on the experience of their best agents.
- **WebTrak** — Installs files required for the WebTrak feature and creates a virtual root for WebTrak on the selected server. It provides a Web page on the server that contains the WebTrak code snippet. It also tracks visitors to your corporate site and helps you start a chat session with visitors.
- **Calendar** — Installs the services that are used to create and publish a calendar feed for the user, so that users can view their published calendar events on their own third party calendar.
- **Transmit Tracker** — Installs a web Application Programming Interface (API) component that enables you to do the following:
    - Track the number of times a campaign URL was accessed by targets.
    - Determine the date and time when a recipient last accessed an email.
    - Include the Unsubscribe option in campaign mailer templates that provides mailer recipients with the option to **unsubscribe** from a campaign mailer.

  If a URL tracking enabled template is used on a campaign mailer, all hyperlinks on the generated emails sent to targets are tracked when clicked. The data collected by Transmit Tracker is written to a database.
- **Staff Authentication Service** — Installs the security web service that is used to authorize and authenticate Staff and Admin users to log in to CampusNexus CRM.
- **Forms Builder Contact STS** — Installs the security web service that is used by Contact/Lead users to log in to Forms Builder Renderer.
- **CoBrowse** — Installs the service that enables the CampusNexus CRM user or the visitor to initiate a co-browsing session. The **Node.js** installer is a prerequisite for the Cobrowse feature. It is available in **Prerequisites.rar**.

All Web Components can be installed by running a single setup program.

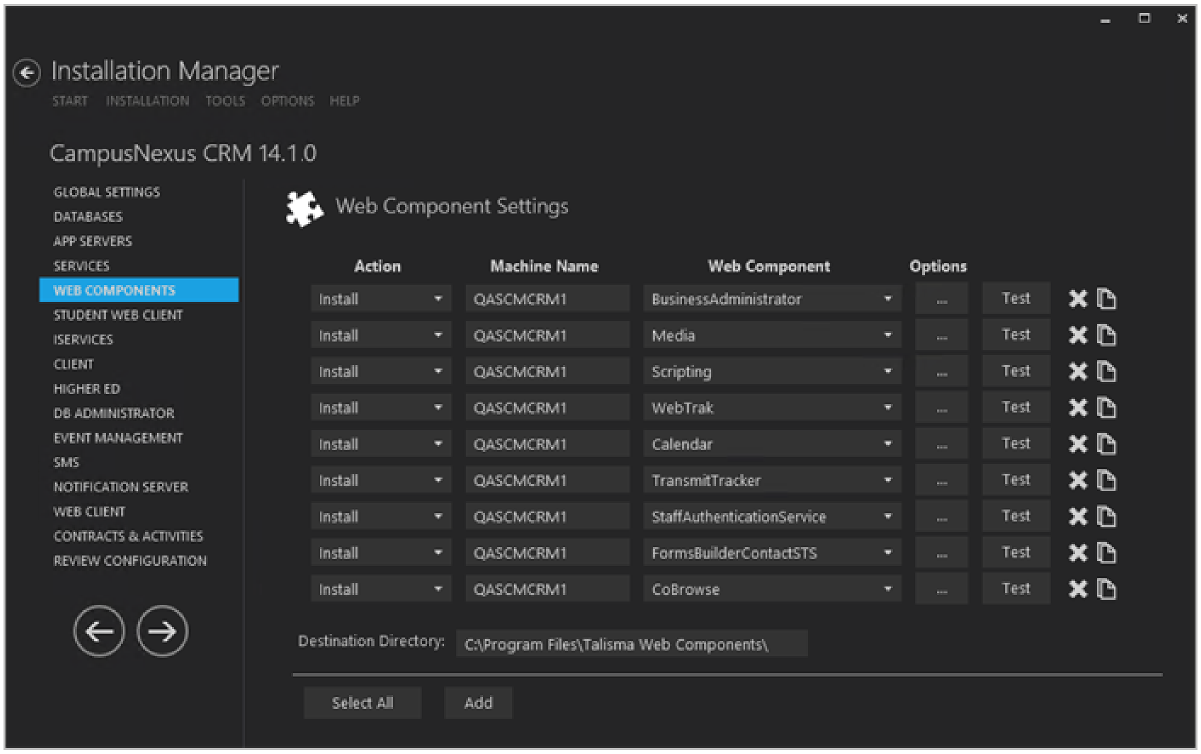
Web Components can be configured to work in multiple languages simultaneously. For a list of supported languages, and details on language options, see the “Managing Language Options” in CampusNexus CRM Business Administrator Help.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — Web Components.

Set Up Web Components

1. In the Installation menu, click **Web Components**. The Web Component Settings screen is displayed.



Note: Ensure that the Database settings and Application Server settings are appropriate. Installation Manager allows multiple machine names listed in the Machine Name column.

2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
   - **Reinstall** – Retries to install a subcomponent.

- **Add** – Installs an additional component on the computer where one or more components already exist. You can add only one component at a time.
- **Remove** – Uninstalls a single component. You can remove only one component at a time.

  Note: The Add and Remove options are not applicable to Calendar and TransmitTracker.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Select the **Web Component** to associate with the machine in the Machine Name field. More than one machine can be associated with the same Web Component. The following Web Components are available:
   - BusinessAdministrator
   - Media
   - Scripting
   - WebTrak
   - Calendar
   - TransmitTracker
   - StaffAuthenticationService
   - FormsBuilderContactSTS
   - CoBrowse
6. Click to copy a line. Edit the copied line as needed.

   Copy as many lines as needed to create the Web Components required for the installation.
7. Click to view and edit the Options form for each Web Component. Depending on the selected Web Component, the Options form contains the fields listed below or a subset of those fields.

Options Fields for Web Components

Field	Description
Business Administrator Options	
IIS Virtual Root	Name of the Virtual Root for the Web Component.
Host Name	Specify the Host Name for the Web Component.
Application Server	Select an Application Server set up in the App Servers screen.
Main Database	Select a Main Database set up in the Databases Screen.
Scripting Options, WebTrak Options, and Calendar Options	
IIS Virtual Root	Name of the Virtual Root for the Web Component.

Field	Description
Application Server	Select an Application Server set up in the App Servers screen.
Main Database	Select a Main Database set up in the Databases Screen.
Media Options	
Media Virtual Root	Name of the Virtual Root for the Media Web Component (default: Media).
Media Upload Virtual Root	Upload name for content going to the Virtual Root for the Web Component (default: MediaUpload).
Application Server	Select an Application Server set up in the APP Servers screen.
Main Database	Select a Main Database set up in the Databases Screen.
Media Directory	Directory where the Media Components are stored (default: Program Files\Common Files\Media).
Media Upload Directory	Path where this Web Component is uploaded (default: Program Files\Common Files\MediaUpload).
Transmit Tracker Options	
Port	Port number used by Transmit Tracker.
Transmit Service Server	Select a Transmit Service Serve set up in the Services screen.
Main Database	Select a Main Database set up in the Databases Screen.
Staff Authentication Service Options	
Hostname	This is an optional field. When selected, the web.config file of the Web Components for CampusNexus CRM will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port` Enter a hostname if you want to assign a hostname (DNS name) in IIS. If you specify a hostname, clients must use the hostname instead of the machine name or IP address to access the website. This feature is often used when a TCP Port must be shared.
Port	Port number used by the Staff Authentication Service.
Use HTTPS	Select this check box if you want the Staff Authentication Service to be accessed through HTTPS. When this option is selected, the Certificate Thumbprint field is enabled.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Certificate Thumbprint</td><td>Certificate thumbprint from IIS.

The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click Browse to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file.

To extract a .CER file from IIS:
a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from Server Certificates.
b. Double-click to open the certificate properties.
c. Select Root level and in the Details tab, click the Copy to File… button.
d. Click Next. Select No, do not export the private key, and click Next.
e. Select DER encoded binary X.509 (.CER) and click Next.
f. Specify a file path and name (root) to export to and click Next.
g. Click Finish</td></tr>
<tr><td>Main Database</td><td>Select a Main Database set up in the Databases Screen.</td></tr>
<tr><td colspan="2">Forms Builder Contact STS Options</td></tr>
<tr><td>Main Database</td><td>Select a Main Database set up in the Databases Screen.</td></tr>
<tr><td>Certificate Thumbprint</td><td>Certificate thumbprint from IIS.

The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click Browse to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file.

To extract a .CER file from IIS:
a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from Server Certificates.
b. Double-click to open the certificate properties.
c. Select Root level and in the Details tab, click the Copy to File… button.
d. Click Next. Select No, do not export the private key, and click Next.
e. Select DER encoded binary X.509 (.CER) and click Next.
f. Specify a file path and name (root) to export to and click Next.
g. Click Finish</td></tr>
<tr><td colspan="2">CoBrowse Options</td></tr>
</table>

Field	Description
Protocol	Select **HTTP** or **HTTPS** protocol. The Port, Service Name, and Install Directory must be specified for HTTP. All fields are mandatory for HTTPS. **Note**: If CoBrowse was installed with HTTP protocol and you want to install CoBrowse with HTTPS on the same machine, uninstall CoBrowse and install CoBrowse with HTTPS option.
Port	Specify the port for the CoBrowse service. The recommended port is 8086.
Service Name	Specify the Service Name or accept the default: CoBrowseService
Install Directory	Specify the install directory or accept the default: `C:\CoBrowse`
Certificate Path	Provide the full .pfx file path. The file format must be .pfx. Click **Browse** to navigate to the certificate.
Password	Specify the password for the certificate pfx file. Click **Test** to verify access to the certificate.

8. Click **OK** to save changes on the Options form. The form is closed.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. Click  to delete a selected line.
11. If all tests pass, click .

Postinstallation Tasks

In the right pane of IIS Manager, double-click **ISAPI and CGI Restrictions** and ensure that the **Allowed** option is enabled for all the Web Service Extensions.

Web Components on a Windows Server Computer

The following are the postinstallation steps for Web Components installed on a Windows Server computer:

Note: Ensure that the Business Administrator URL is configured with the prefix https, and the value https is set in the Type field in the Edit Site Binding dialog.

1. Configure the following settings for the **DefaultAppPool** Application Pool. To do so:
   a. Open the Internet Information Services (IIS) Manager in one of the following ways:

      Go to Start, Run. Type **inetmgr**.

      — OR —

      Type inetmgr in the Search box of the Start menu.

b. Click **ENTER**.

c. Navigate to the **<Server Name>, Application Pool** node. The Application Pools screen is displayed.

d. In the Application Pools screen, right-click the **DefaultAppPool** Application Pool, and select **Basic Settings**.

   The Edit Application Pool dialog box is displayed.

a. Set the value of the fields in the Edit Application Pool dialog box as follows:

   - Set the value of the **.Net Framework Version** field to **.Net Framework v4.0.30319**.
   - Set the value of the **Managed Pipeline Mode** field to **Classic**.

e. In the Application Pools screen, right-click the **DefaultAppPool** Application Pool, and select **Advanced Settings**. The Advanced Settings dialog box is displayed.

f. In the Process Model section, set the value of the **Identity** field as **Local System**.

2. In IIS ensure that the Business Administration Virtual Directory is running under domain user account. To do so:

   a. Open Internet Information Services (IIS) Manager in one of the following ways:

      Go to Start, Run, and type **inetmgr**.

      — OR —

      Type inetmgr in the Search box of the Start menu.

   b. Go to **<computer name>/Sites/Default Web Site/BusinessAdministrator** virtual directory. The areas and corresponding applications are displayed in the right pane.

   c. Click **Basic Settings** in Actions pane (right pane). The Edit Application screen is displayed.

   d. Click **Test Settings**.

   e. If Test Setting Authorization fails, provide domain user credentials by clicking **Connect as** in the **Edit Application** dialog box.

   If the Website does not display the page, perform the following steps:

   a. Open Internet Information Services (IIS) Manager in one of the following ways:

      Go to **Start**, **Run**, and type **inetmgr**.

      — OR —

      Type inetmgr in the Search box of the Start menu.

b. Go to **<computer name>/Sites/Default Web Site/BusinessAdministrator** virtual directory. The areas and corresponding applications are displayed in the right pane.

c. In the IIS area, right-click the **ASP** icon and select **Open Feature**. The Features View of ASP is displayed.

d. In the **Behavior** section, set the **Enable Parent Paths** options to **True**.

3. When Application Server and Business Administrator are installed on different computers, you must perform the following steps on IIS.

   - Perform the following steps for the **Classic .NET AppPool** option on the Web Components computer:

     a. Open the Internet Information Services Manager.

     b. In the Connections pane, expand the server node and click **Application Pools**. The Application Pools page is displayed.

     c. Select **Classic .NET AppPool**, and click **Advanced Settings**.

     d. For the Identity property, click . The Application Pool Identity dialog box is displayed.

     e. In the **Built-in Account** option, ensure that **LocalSystem** is selected.

     f. Click through **OK** twice.

   - Perform the following steps for the **DefaultAppPool** option on the Web Components computer:

     a. Open the Internet Information Services Manager.

     b. In the Connections pane, expand the Server node, and click **Application Pools**. The Application Pools page is displayed.

     c. For the Identity Property, click . The Application Pool Identity dialog box is displayed.

     d. Select the **Custom account** option and click **Set**. The Set Credentials dialog box is displayed.

     e. Specify **User name** and **Password** details of a CampusNexus CRM user who has domain administration permissions on the computer.

     f. Click through **OK** three times.

Postinstallation Tasks for Chat

1. Update the TLChatWinService.exe.config file. To do so:

   a. On the computer where the Chat windows service is installed, navigate to the following path: <Drive name>:\ChatService.

   b. Open the **TLChatWinService.exe.config** file in an edit mode.

c. Update the **<bindings>** tag.

Three binding types, HTTP, HTTPS and TCP are supported. Ensure that the tag related to the binding type used by Chat is uncommented. For example, if the binding type used by Chat is:

- HTTP, then uncomment the <basichttpbinding> tag.
- HTTPS, then uncomment the <basichttpsbinding> tag
- TCP, then uncomment the <Nnettcpbinding> tag

Comment or remove the binding type which is not applicable.

d. Update the **<endpoint address>** tag.

The hostname and the port number of the computer where Web Components are installed is updated automatically in the <endpoint address> tag. The default port number is 80. If you are using a different port number, change the value accordingly. Comment or remove the <endpoint address> tag which is not applicable.

e. Update the **<baseAddresses>** tag.

The hostname and the port number of the computer where Web Components is installed is updated automatically in the <add baseAddress> tag. The default port number is 80. If you are using a different port number, change the value accordingly. Comment or remove the <add baseAddress> tag which is not applicable.

f. Set the Identity credentials and then restart Application Server.

g. In the Run dialog box, type **EventVwr** and press **ENTER**.

h. In the **Windows Logs, Application** node, ensure that only one event with the entry *"Service started successfully."* is available for TLChatWinService. If other errors are found, resolve the issue and restart service.

Note: Ensure that the port that is used for Chat connections is free and not used by any other process.

2. If you are using the TreatCode.js file, perform the following steps:

a. Open the **TreatCode.js** file in edit mode.

Note:

A sample TreatCode.js file is available in the following path:

For desktop and laptop devices: `\Samples\Web\WebTrak\Desktop`

For mobile devices: `\Samples\Web\WebTrak\Mobile`

b. Locate the following lines:

```
var sChatURL = "http://<Chat Server>/Media";

var sTrackURL = "http://<Chat Server>/Webtrak";
```

c. Replace the variable **<Chat Server>** with the hostname or IP address of the computer where Web Components are installed.

d. Save the **TreatCode.js** file.

Note: If the WebTrak server and Chat server are installed on different computers, the value of the sTrackURL must include the hostname or IP address of the computer where WebTrak is installed.

3. On the computer where Web Components are installed, specify the domain names of the web pages from where Chat is initiated in the Web.Config file that is available in the <Drive name>:\Program Files\Talisma Web Components\Media path. To do so:

   a. Open the **Web.Config** file in edit mode.

   b. Locate the following tag: **<add key="HostDomains" value=""/>**

   c. Specify the domain names of the web pages from where Chat is initiated.

   For example, if www.talisma.in/chat.htm and www.talisma.com/initiatechat.htm are the web pages that are configured for initiating Chat, in the Web.Config file of the Media Web Component, specify the value as follows:

   <add key="HostDomains" value="www.talisma.in, www.talisma.com"/>

4. If Media and WebTrak applications are installed on different computers belonging to the same domain, you must specify the common domain name in the Web.Config file that is available in the <Drive name>:\Program Files\Talisma Web Components\WebTrak path on the computer where Web Components are installed. To do so:

   a. Open the **Web.Config** file in edit mode.

   b. Locate the following tag: **<add key="HostDomains" value=""/>**

   c. Specify the common domain name suffix of the computers where WebTrak applications are installed and domain name of the web pages from where Chat is initiated.

   For example, if the Media application is installed on media.talisma.com, and the WebTrak application is installed on webtrak.talisma.com, in the Web.Config file of the WebTrak Web Component specify the value as follows:

   <add key="HostDomains" value="talisma.com"/>

5. Specify the required Team Routing Rules and User Assignment Rules. This step is optional. If Team Routing Rules and User Assignment Rules are not configured, the Chat requests will be routed to the Home Team.

6. To ensure that Chat traces are captured for all processes, perform the following steps:

   - Configure the following settings for the DefaultAppPool Application Pool. As a best practice, a separate application pool must be created instead of using the default application pool.

a. Open the Internet Information Services (IIS) Manager in one of the following ways:

   Go to Start, Run. Type **inetmgr**.

   — OR —

   Type inetmgr in the Search box of the Start menu. The Internet Information Services (IIS) Manager screen is displayed.

b. Navigate to the **<Server Name>, Application Pool** node. The Application Pools pane is displayed.

c. In the Application Pools pane, right-click the **DefaultAppPool** Application Pool, and select Advanced Settings. The Advanced Settings dialog box is displayed.

d. In the Process Model section, set the value in the **Identity** field.

e. Navigate to the **Process Model** area and click the ellipsis in the Identity field. The Application Pool Identity dialog box is displayed.

f. Select the **Custom account** option and click Set.

g. In the **Set Credentials** dialog box, specify the domain user account details.

h. Click **OK** twice.

- Configure the following settings for the Media Site:

  a. In the Internet Information Services (IIS) Manager screen, navigate to the **<Server Name>, Sites, Default Web Site, Media** node.

  b. In the right pane, select **Basic settings** from the Actions area. The Edit Application dialog box is displayed.

  c. Click **Connect as**. The Connect as dialog box is displayed.

  d. Select the **Specific user** option and click Set. The Set Credential dialog box is displayed.

  e. Specify user name, and password details of the user that is specified in step (g).

  f. Click **OK** three times.

- Enable trace for Chat. To do so:

  a. Log on to **Trace Client**.

  b. Select **Chat server** from the Process list.

7. Before initiating a chat request ensure the following:

   a. Log on to **SQL Server Management Studio**.

   b. Ensure that the database replication is working fine. Else, drop the replication and reconfigure it.

c. In the **Object Explorer**, right-click the **Server name** and select **Facets**.

d. In the **View Facets** screen, select **Surface Area Configuration** from the Facets field.

e. Ensure that the value for the following options is set to True:

  - OleAutomationEnabled
  - XpCmdShellEnabled

f. The correct URL is provided in Business Administration.

g. The **TLChatWinService.exe.config** service is running.

Postinstallation Task for Transmit Tracker

Ensure that the Port number you specify for the Transmit Tracker (web service) is not used by any other service.

If required, you can change the Port value in the web.config file. An extract of the file is illustrated here:

<client>

<endpoint binding="basicHttpBinding" bindingConfiguration="BasicHttpBinding_ITrackableService" contract="TrackableService.ITrackableService" name="BasicHttpBinding_ITrackableService" address="http://CLTTRCK:**8082**/Cmc.NexusCrm.Common.Services/TrackableService/"/>

</client>

Common Post Installation Tasks for Chat, Transmit Tracker, and Notification Service

Perform the following steps If Transmit Tracker and Chat are using <basichttps> binding:

1. At the command prompt, navigate to the path **c:\windows\system32**.
2. Run the following command:

   netsh http add sslcert ipport=0.0.0.0:<port number> certhash=<thumb print of the certificate> appid=<unique GUID> clientcertnegotiation=enable

   Replace the following values:

   - **<port number>** - the unique port number that you specified when you updated the endpoint address tag.
   - **<thumb print of the certificate>**
   - **<unique GUID>** - To generate this value:

a. In the **Start** menu, type **Windows Powershell**.

b. Type the following command:

   [guid]::newguid()

   Ensure that you copy the generated value including the curly braces.

Postinstallation Task for CoBrowse

For information about configuring the CoBrowse feature, see CampusNexus CRM Web Client Help.

Configuring Web Components on a Demilitarized Zone

Perform the following steps when a customer is requesting to host any student facing CampusNexus CRM web applications (Media, Transmit Tracker, Forms Builder contact STS) in a Demilitarized Zone (DMZ).

Assumption: The customer does not require any ports to be opened apart from the standard http or https ports.

1. Copy the installation path of the web application to the DMZ server.
2. Create a web application in IIS with the copied files. Name the application appropriately.
3. In Business Administrator, update global settings with the URL that is pointing to the DMZ server:
   - For the Transmit Tracker: Update the **Clicked URL Tracker** and **Email Opened Tracker** fields.
   - For the Media component: Update the **Chat Cluster URL** field.

Student Web Client

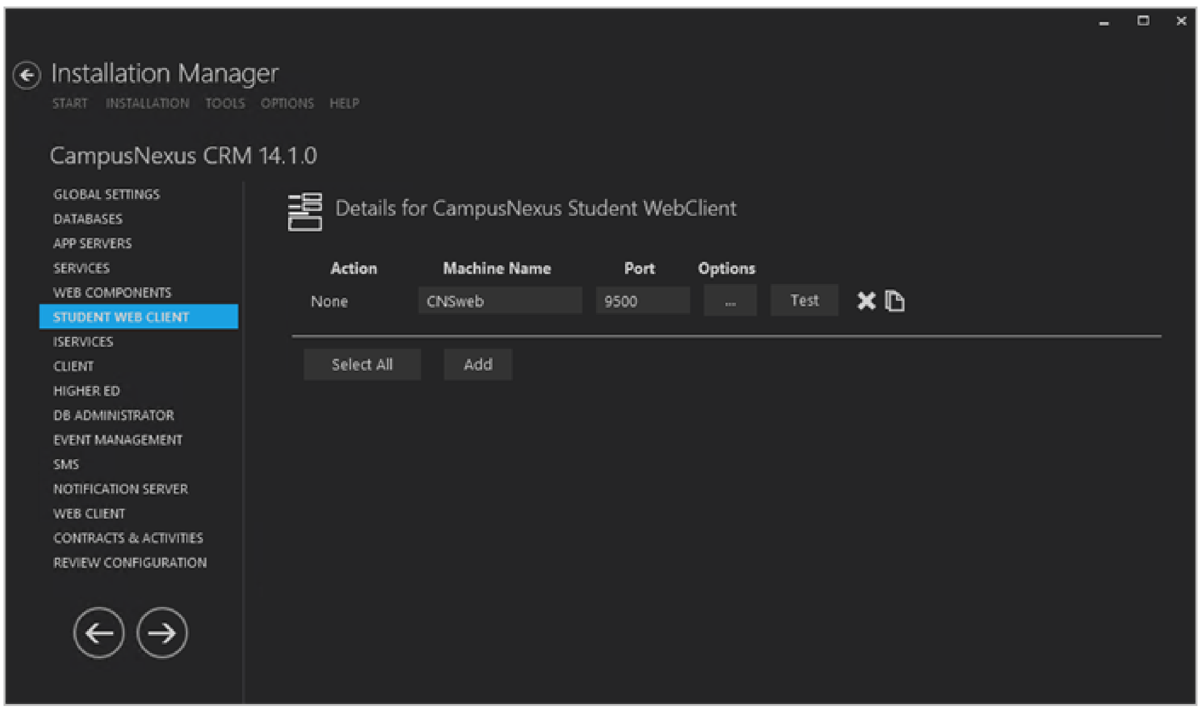
To enable CampusNexus CRM Web Client to use the same instance of Workflow Composer that is connected with Anthology Student, configure the settings on the Student Web Client screen.

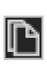
These settings will update Server Name and DB Name in the Workflow connection string of the following:

- web.config file of the Web Client
- config file of each iService

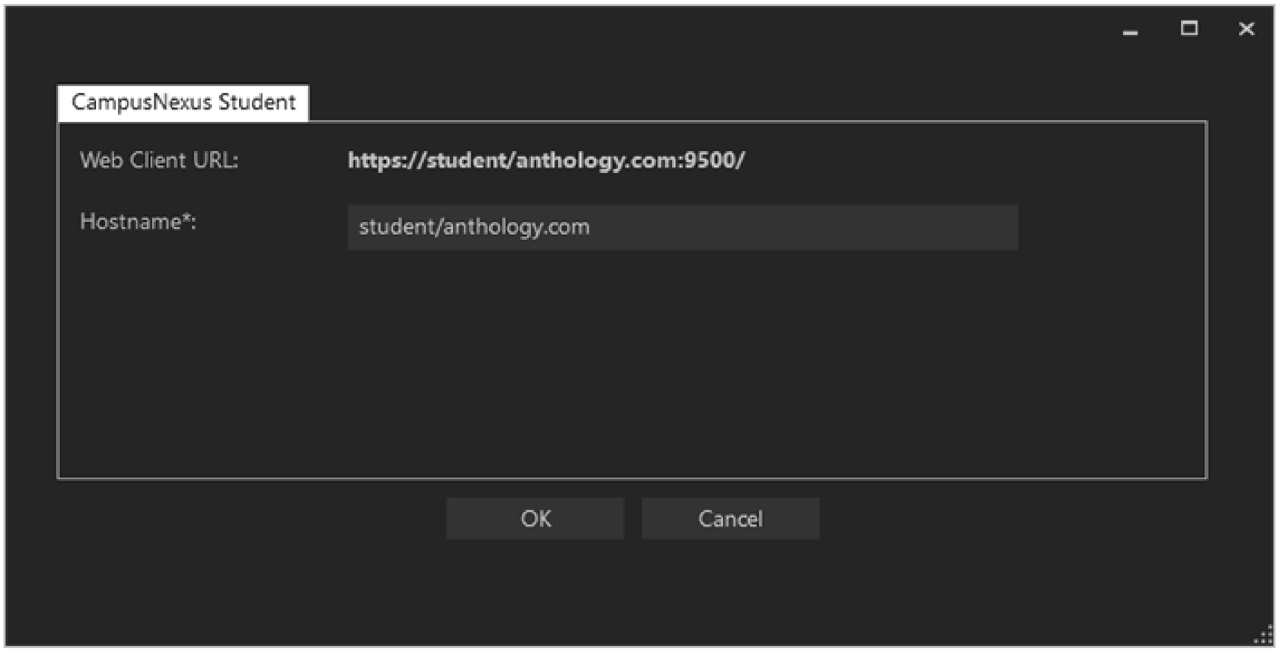
Steps

1. Set up the Student Web Client.
2. In the Installation menu, click **Student Web Client**. The Student Web Client Settings screen is displayed.



3. Click **Add** to add a line to the Settings screen.
4. Enter the **Machine Name** for the component to be installed.
5. In the **Port** field, enter the port number or accept the default (9500).
6. Click  to copy a line. Edit the copied line as needed.

   Copy as many lines as needed to create the iService components required for the installation.
7. Click  to view or edit the Options form.



8. Specify the Hostname for the Anthology Student Web Client.

   The Hostname will become part of the Web Client URL

9. Click **OK** to save changes on the Options form. The form is closed.

10. Click to delete a selected line.

11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

12. If all tests pass, click .

Note:

When upgrading Web Client and iServices, if Student Web Client that was associated with the previous version of Web Client and iServices is no longer required:

1. In the Student Web Client Settings screen, click .

2. Upgrade Web Client and iServices.

iServices

The iServices are web services through which an external application interacts with CampusNexus CRM. The Web Service Definition Language (WSDL) interface acts as an interface between the external application and iServices.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — iServices.

The prerequisites for installing iServices are:

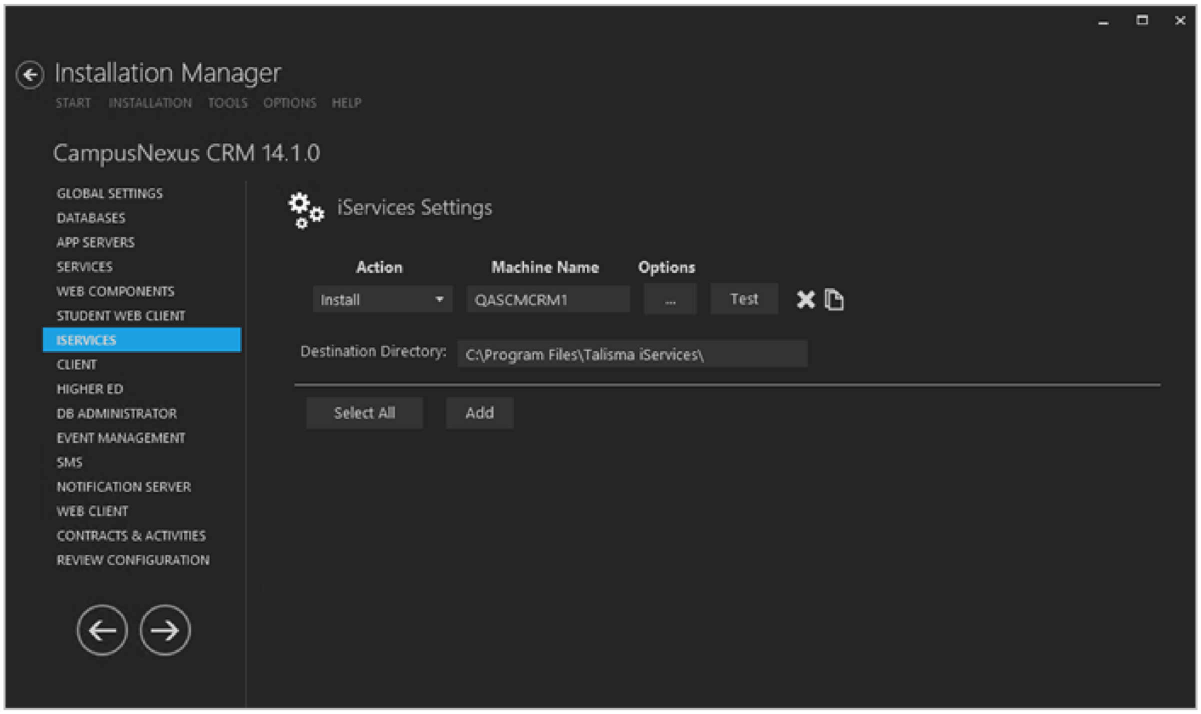
- The Database component must be installed.
- Microsoft Microsoft Web Service Enhancement 3.0 (WSE 3.0) and iServices must be installed on the same computer.

  To install WSE 3.0, navigate to the **Prerequisites\WSE 3.0** folder and run **MicrosoftWSE3.0.msi**.
- You must obtain the following licenses:
  - iService - Service: for installing and using Contact, Account, Interaction, Utils, Reports, and Portal iServices.
  - iService - COF: for installing and using COF iService.

  For information about iServices licenses, contact Anthology Inc. Professional Services.

Set Up iServices

1. In the Installation menu, click **iServices**. The iServices Settings screen is displayed.

   Note: The iServices are not licensed individually. They are bundled together and are installed all at once. The Options form enables you to change the virtual directory names for the iServices separately.

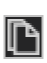
2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

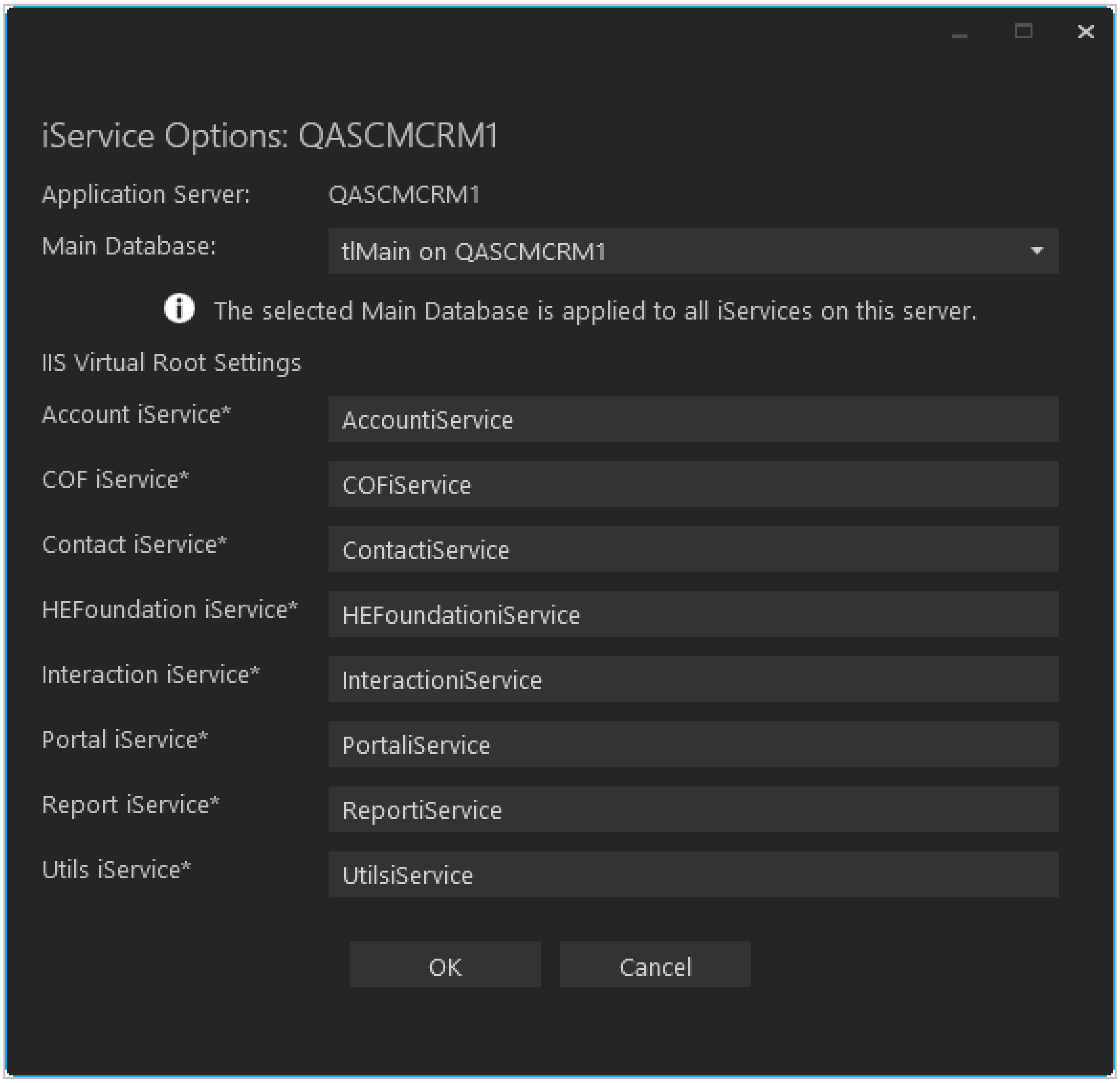
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.

5. Click  to copy a line. Edit the copied line as needed.

   Copy as many lines as needed to create the iService components required for the installation.

6. Click  to view or edit the Options form.



7. Verify or edit the **Application Server**, **Main Database**, and **IIS Virtual Root Settings** in the Options form.
8. Click **OK** to save changes on the Options form. The form is closed.
9. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.
10. Click  to delete a selected line.
11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
12. If all tests pass, click .

Postinstallation Tasks

Following are the postinstallation steps for iServices:

1. Configure the following settings for the **DefaultAppPool** Application Pool. To do so:
    a. Open the Internet Information Services (IIS) Manager in one of the following ways:

       Go to Start, Run. Type **inetmgr**.

       — OR —

       Type inetmgr in the Search box of the Start menu.

    b. Click **ENTER**.
    c. Navigate to the **<Server Name>, Application Pool** node. The Application Pools screen is displayed.
    d. In the Application Pools screen, right-click the **DefaultAppPool** Application Pool, and select **Basic Settings**. The Edit Application Pool dialog box is displayed.
    e. Set the value of the fields in the Edit Application Pool dialog box as follows:
        - Set the value of the **.Net Framework Version** field to **.Net Framework v4.0.30319**.
        - Set the value of the **Managed Pipeline Mode** field to **Integrated**.
    f. In the Application Pools screen, right-click the **DefaultAppPool** Application Pool, and select **Advanced Settings**. The Advanced Settings dialog box is displayed.
2. In the Process Model section, set the value of the **Identity** field as **Local System**.

Note: The iServices API documentation is available in the Service Catalog (login required).

Client

The Client component ("thick client") provides an interface from which a CampusNexus CRM user can log and track interactions with contacts, respond to queries from contacts, and work with items of other objects.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — Client.

If the Data Management Utility (DMU) is installed on the Client computer, the previous DMU version must be uninstalled before installing the new DMU version.

Install the Client in Silent Mode

You can perform a fresh installation, reinstallation, or upgrade of the Client in silent mode. Depending on the type of installation you want to perform, you must rename the FreshInstall.iss, Reinstall.iss, or Upgrade.iss files to Setup.iss. To do so:

1. Copy all files in the **ClientSetup** folder from the host computer to the folder on the computer where you want to install the Client.
2. Identify the type of installation that must be performed on the computer. Depending on the type of installation, perform one of the following steps:
   - To upgrade the Client version, rename **Upgrade.iss** to **Setup.iss**.
   - To reinstall an existing Client, rename **Reinstall.iss** to **Setup.iss**.
3. If you are doing a fresh installation, perform the following steps:
   a. Open the **Setup.iss** file in an editor.
   b. Provide the installation path for 32-bit and 64-bit computer in the following code:
      ```
      32bitmachinePath= C:\Program Files\Talisma Client
      64bitmachinePath= C:\Program Files (x86)\Talisma Client
      ```
   c. Save and close the file.
4. Open the Windows command prompt.
5. Navigate to the folder where the setup.exe file is located, and type:
   ```
   setup.exe /s
   ```
6. Press **ENTER**.

   The Client is installed on the computer and a log file is created in the following drive:

- On a 32-bit computer: `<Drive name>:\Program Files\Common Files\Talisma Shared\SetupLogpath`
- On a 64-bit computer: `<Drive name>:\Program Files (x86)\Common Files\Talisma Shared\SetupLogpath`

View the log file to check for any errors occurred during installation. Events are added to the Application Log of the Windows Event Viewer on the computer.

Notes:

- In a scenario where you have removed the Client using silent mode, rename **FreshInstall.iss** to **Setup.iss** to perform a fresh installation using silent mode.
- If the computer where the Client is being installed in silent mode has other CampusNexus CRM components such as Data Management Utility (DMU), these components will not be installed or upgraded through silent mode. You must install or upgrade these components manually.
- When the Client is installed manually, the success and failure messages are not logged in the Windows Event Viewer. These messages are added to a log file available in the following paths on the computer where the Client is installed:
  - On a 32-bit computer: `<Drive name>:\Program Files\Common Files\Talisma Shared\SetupLog`
  - On a 64-bit computer: `<Drive name>:\Program Files (x86)\Common Files\Talisma Shared\SetupLogon`
- The Client can be installed in silent mode using a systems management tool such as System Center Configuration Manager (SCCM) by Microsoft. When a systems management tool is used for installing in silent mode:
  - A single package that is created in the systems management tool can be used for any of the Windows operating systems (32-bit and 64-bit) that are supported by the Client.
  - If you are upgrading or re-installing the Client in silent mode using SCCM, before creating a package for these operations, you must rename the **Upgrade.iss** and **Reinstall.iss** file to **Setup.iss** based on the scenario.
  - Similarly, before creating a package for removing the Client installation in silent mode, you must rename the **Remove.iss** to **Setup.iss**.
  - The failure or success of the Client installation will be reported in the systems management tool.

Automatically Restart the Computer after the Client is Installed or Removed in Silent Mode

When the Client is installed or removed in silent mode, by default, the computer does not restart automatically. You can enable automatic restart of the computer once the Client is installed in silent mode. To do so:

1. Navigate to the folder where the Client setup files are located.
2. Depending on the type of installation that must be performed, open the **FreshInstall.iss**, **Upgrade.iss** or **Reinstall.iss**, **Remove.iss** in an editor, and locate the following code:

   `BootOption=0`
3. Change the value of **BootOption** from **0** to **3**.
4. Save and close the **.iss** file.
5. Repeat steps 2 to 6 of Install the Client in Silent Mode.
6. The computer will automatically restart when the Client is installed or removed.

Remove the Client in Silent Mode

1. Navigate to the folder where the Client setup files are located.
2. Rename **Remove.iss** to **Setup.iss**.
3. Open the Windows command prompt.
4. Navigate to the folder where the setup.exe file is located, and type: `setup.exe /s`
5. Press **ENTER**.

The Client will be removed from the computer and a log file is created in the `<Drive name>:\Program Files\Common Files\Talisma Shared\SetupLogpath`. View the log file to check for any errors occurred while removing the Client. Additionally, events are added to the Application Log of the Windows Event Viewer on the computer.

Events Logged in the Event Viewer

Following are the various success and failure scenarios for which events are logged in the Windows Event Viewer:

Success scenarios for which events are logged:

- When the Client is installed successfully through a fresh installation.
- When the Client is reinstalled successfully.
- When an upgrade of the Client is installed successfully.
- When the Client installation is removed successfully.

Failure scenarios for which events are logged:

- When the user who is running the Client setup is not a local administrator.
- When the installation path provided in the setup.iss file exceeds the 116 characters limit.
- When the drive name provided for the 32-bit and 64-bit paths in the setup.iss file does not exist on the computer where the Client is being installed.

- When the Visual C++ Redistributable for Visual Studio 2015 (Update 1) prerequisite is not installed.
- When the tlc3setup.dll file failed to be copied.

Install the Client in a Citrix Environment

The Client can also be installed centrally on a Microsoft Windows Terminal Server with Citrix Server installed. The Citrix Client program can then be installed on computers that need to use the Client on the Microsoft Windows Terminal Server.

You have only one installation of the Client and avoid installing it on all client computers individually. You have to install the Citrix Client program, and use the Client on the Terminal Server. Upgrades too, are made very easy, where you have to just upgrade the Client on the central computer, and not on every client computer.

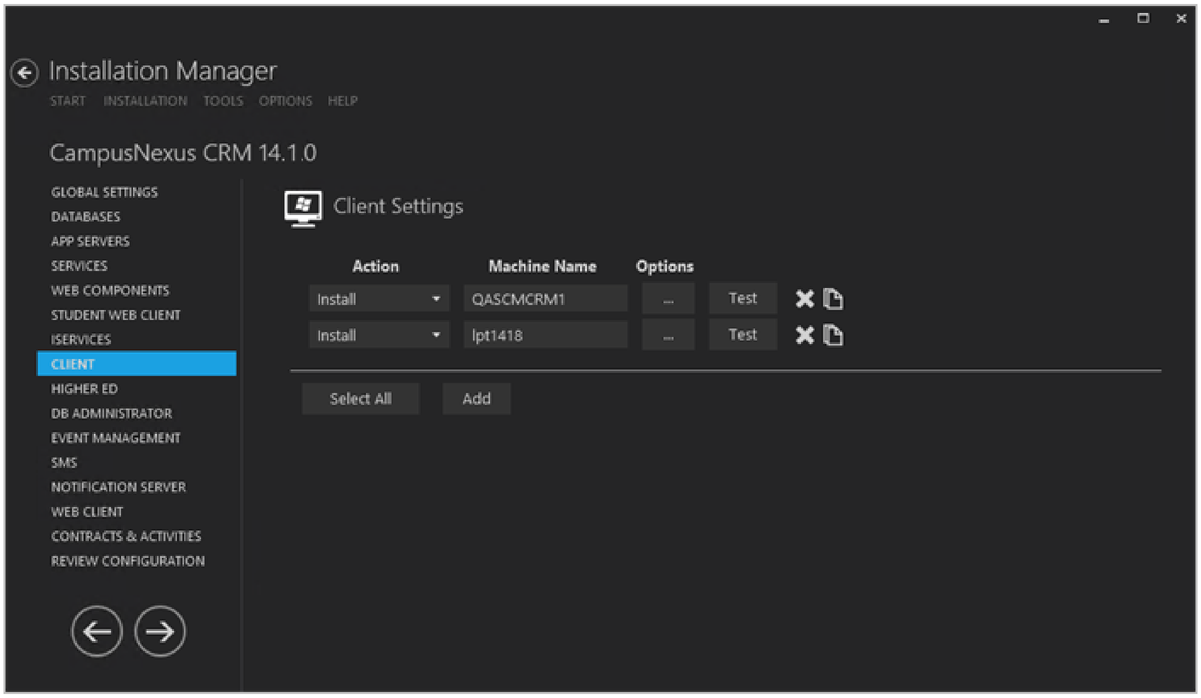
Notes:

- On a fresh Client, the Manage Filters Permission is enabled by default for users with System Administration, or Business Administration Permissions.
- On a fresh Client, audit is disabled for all the Properties and events except:
    - Message Objects
    - Health Check Objects
    - URL property in Link Object

  Configuration for Message and Health Check Objects cannot be changed.

Set Up Clients

1. In the Installation menu, click **Client**. The Client Settings screen is displayed.

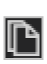
   

   Client Settings identify client machines in a client-server relationship so that manipulations of multiple client machines can be handled in one location.

   Note: Ensure that the database settings are appropriate. Installation Manager allows multiple machine names listed in the Machine Name column.

2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
   - **Reinstall** – Retries to install a subcomponent.

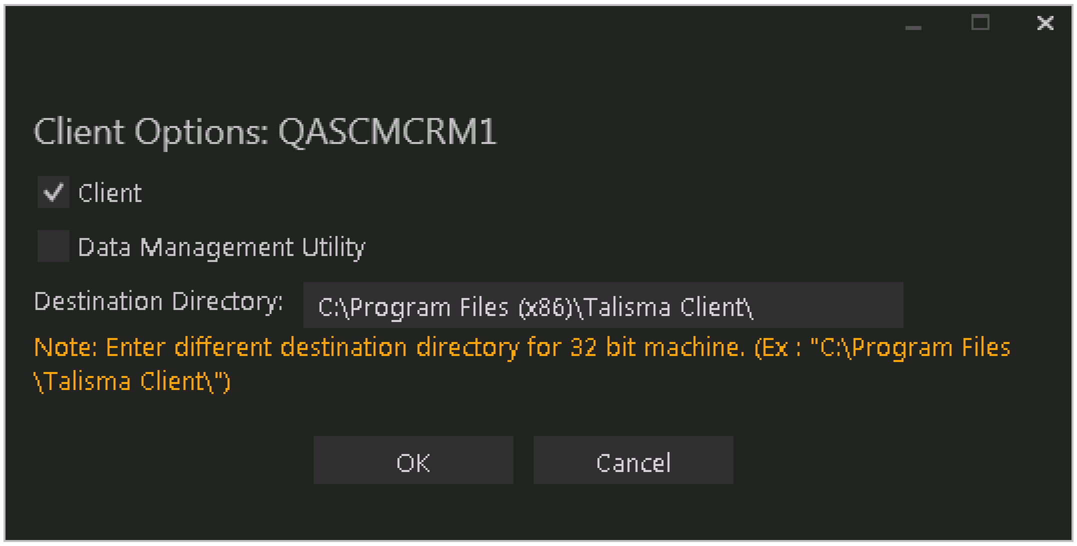
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Click  to copy a line. Edit the copied line as needed.

6. Click to view and edit the Options form for each Client. The options include the following:

   - Client (selected by default)
   - Data Management Utility

   The default Destination Directory is `C:\Program Files (x86)\Talisma Client\`.
   Enter a different Destination Directory for a 32-bit machine, e.g., `C:\Program Files)\Talisma Cli-ent\`.



7. Click **OK** to save changes on the Options form. The form is closed.

8. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.

9. Click to delete a selected line.

10. Click **Test** to ensure the setup for the corresponding line is correct.

    If a test on a particular line fails, check all associated fields and click **Test** again.

11. If all tests pass, click .

Postinstallation Tasks

- To work with Analytics, on the Client computer, ensure that the logged on user has the **Modify** permission for the **Talisma Client** folder. The folder is available in the **<Drive name>:\Program Files** path.

- On the Web Server computer on which trackable URLs and Forms that will be inserted into Mailers are configured, install the AspEmail component obtained from Persits Software Inc. Alternatively, you can install any component with a Send Mail feature.

Log on to the Client

You can log on to the Client using Application, Trusted, or Custom Security. This section covers the procedures for these options.

1. Double-click the Client icon on your desktop.

   — OR —

   From the **Start** menu, point to **Programs**, click **Talisma Client <version>**, and select **Talisma**.

2. Type your user name in the **Login** name field.
3. Type your password in the **Password** field.
4. Select a profile from the **Profiles** list. The Talisma Profile is selected by default.

   Note: When you log on to the Client for the first time, you must either create a profile, or edit the default profile, by specifying the Server and Database details.

5. To create a user profile:
   a. Click **Profiles**. The Profiles dialog box is displayed.
   b. Click **Add**. The New Profile dialog box is displayed.
   c. Type a name for the profile in the **Profile Name** field.
   d. To log on using Application Security, select **Application Security** from the Login Security field.

      — OR —

      To use your Microsoft Windows login name and password for logging on to the Client, select **Trusted Security** from the Login Security field.

      — OR —

      To use a custom login name and password for logging on to the Client, select **Custom Security**. This login name and password can reside in any database. For example, it could be a Microsoft Access database or any other database from where these details are retrieved for logging on to the Client.

   e. In the **Application Server** field, type the name of the Application Server to which you want to connect when logging on to the Client.
   f. From the **Database Server** list, select the SQL Server on which the Main database is installed.
   g. In the **Database Name** field, type the name of the database to which you want to connect.
   h. If you select **Internet** from the Connection Type list, the Internet Security option is enabled. Select the required level of security that needs to be implemented when connecting over the Internet.
   i. Click **OK**.

Note: You can also edit, delete, or copy a profile in the Profiles Dialog box. For more information about Profiles, see the Client Help system.

6. In the Profiles dialog box, the Talisma profile is selected by default in the **When starting Talisma, use this Profile** list. You can select the newly created profile to set it as the default profile for logging on to the Client.
7. Click **OK**.

   Note: When license information is updated, ensure that you log off from the Client, and log on again.

Perform Other Operations

This section describes Client-side settings for tracking Interaction actions, the procedure for handling E-mail messages without Character Sets, and configurations for various workspaces and the Campaign Dashboard in the Client.

Track Interaction Actions

The actions performed on an Interaction are tracked as they occur, and are recorded periodically in the Main database. While actions are tracked in real time, they are updated in the Main database every 300 seconds, or when a user logs out of CampusNexus CRM. An updated record of these actions is displayed in the Actions tab of the Message screen only after the predefined time interval lapses. If you want to set this time to a different number, you must create an appropriate registry key on the computer where the Client is installed.

To Set the Time for Updating Frequency in the Registry:

1. From the Command prompt, run **Regedit**.
2. Browse to **HKLM\Software\Talisma\Talisma Client\CurrentVersion**.
3. Create a key of type **DWORD** called **SaveTrackInfoDuration** under **CurrentVersion**.
4. In the **Base** section of the **Edit DWORD Value** dialog box, select **Decimal**.
5. Specify the required value for the "**SaveTrackInfoDuration**" key in the **Value data** field. The value you specify is in seconds.
6. Click **OK**.

Notes:

- If the registry key is not created, the actions are updated in the Main database every 300 seconds.
- You must set the value of the "SaveTrackInfoDuration" registry key to 0 if you want the actions to be written in the Main database in real time.

Handle Incoming E-mail Messages Without Character Sets

CampusNexus CRM provides two methods to handle incoming e-mail messages received with blank Character Sets:

Method 1

If the value of the AutoResolveCharset row in the tblGlobalInfo table is 1, CampusNexus CRM uses the default Character Set "iso-8859-1" for the Message. By default, the value of the AutoResolveCharset row is 1.

Disadvantages of deploying Method 1

- If an e-mail message with a blank Character Set is received, CampusNexus CRM uses the default Character Set "iso-8859-1" for it. As a result, the message content may be distorted. Subject Line-based threading may fail and a new Interaction may be created.
- Language detection may fail, and an improper Canned Response may be sent to the Contact.

Note: If Method 1 is deployed, messages will not be sent to the Inbox Workspace.

Method 2

If the value of the AutoResolveCharSet row in the tblGlobalInfo table is set to 0, e-mail messages without Character Sets are received in the Inbox Workspace, if they satisfy any of the following conditions:

- The Contact's Default E-mail Character Set Property is blank, and the value of the AutoDetectUSASCII row in the tblGlobalInfo table is 0.
- The Contact's Default E-mail Character Set Property is blank, and the value of the AutoDetectUSASCII row in the tblGlobalInfo table is 1, but the message content does not conform to the US ASCII Character Set.

Note: The default value of the AutoDetectUSASCII row in the tblGlobalInfo table is 1. It is recommended that you do not modify this value.

Benefits of deploying Method 2

- Client users can set the character set for e-mail messages in the Inbox Workspace. The Contact's Default E-mail Character Set property is automatically set using this value, and is used for subsequent messages coming into CampusNexus CRM from the Contact.
- Language detection will not fail.
- Threading will not fail.

Disadvantage of deploying Method 2

There is no option available to send an e-mail message or any notification to Client users when e-mail messages are received in the Inbox Workspace.

Users' Access to the Inbox Workspace

When Method 2 is deployed, Client users will be able to open the Inbox Workspace if any one of the following conditions is satisfied:

- The value of the InboxSecAccessBased row in the table tlbGlobalInfo is 0 and the user has been granted the System Administration Permission.
- The value of the InboxSecAccessBased row in the table tlbGlobalInfo is 1.

Notes:

- Although CampusNexus CRM supports Character Sets in several languages, when selecting a Character Set for a Message, a Client user can only choose a language supported by the operating system on the user's computer.
- To enable language detection in the Inbox Workspace, Microsoft Word must be installed on the Client computer.

Customize the Message ID for E-mail Messages

You can customize the Message ID for the Interaction and Campaign Objects with custom envelope tokens. To do so, specify custom envelop tokens in the tblEnvelopeIdTokens table for the Interaction and Campaign Objects. The tblEnvelopeIdTokens table consists of four columns.

"tblEnvelopeIdTokens" Table Columns

Column Name	Description
aIndex	Auto generated ID.
nEvpMarker	The envelope token for the Interaction Object. For example, #MyCompanyInteraction.
CampEvpMarker	The envelope token for the Campaign Object. For example, %MyCompanyCampaign.
nEvpSeparator	The character used as separator. **Notes**: • You cannot specify numbers and the @ symbol in this column. • Ensure that the value specified in this field does not contain characters from the tinstallationID column of the tblglobalconfig table.

Notes:

- You cannot update the values specified in the tblEnvelopeIdTokens table. To modify the values of an existing row, you must delete the row and add new values.
- The value in the nEvpMarker and CampEvpMarker columns cannot be same.
- You must specify values in all columns of the tblEnvelopeIdTokens table.
- The first row of the tblEnvelopeIdTokens table stores the default envelope tokens for the Interaction and Campaign Objects, @TLZ and TLC respectively.

- If a single character is specified in the nEvpMarker or CampEvpMarker column, the threading of Interaction fails when the Threading Model, Interaction in Reply-To or Interaction in Reply-To with Subject Match is selected in Business Administrator.
- The Message ID parameter can store a maximum of 999 characters.
- After adding custom envelope tokens for the Interaction and Campaign Objects in tblEnvelopeIdTokens table, you must restart JSF and Campaign Dispatcher Services.
- If there are issues with threading of undelivered messages with an Interaction and update of undelivered messages for a Campaign in the Campaign Dashboard, you can create custom tokens to resolve this issue.

Set the Auto Refresh Option for Campaign Dashboard

You can use the Campaign Dashboard to monitor and control the dispatch of Mailers, and view the status of Campaign Dispatchers configured in CampusNexus CRM. The Campaign Dashboard is automatically updated with the most current information at intervals of 5 minutes. You can modify this value. To do so:

1. From the **Start** menu, select **Run**. The Run dialog box is displayed.
2. In the **Open** field, type **Regedit**. The Registry Editor is displayed.
3. Browse to the following key, and specify the required value:

   HKEY_CURRENT_USER\Talisma\TalismaClient\RefreshRate.

   The value you specify is in minutes.

Higher Ed

The Higher Education Foundation (Higher Ed) setup enables the Client user to work with the Lead Object in the Higher Education environment.

The Client user also works with other operational Objects. While the Client user can work with instances of reference Objects by including, or associating them in operational Objects, the Client user typically does not create reference Objects in CampusNexus CRM; however, a Client user with Business Administration permission or higher can create reference Object items in the Client component.

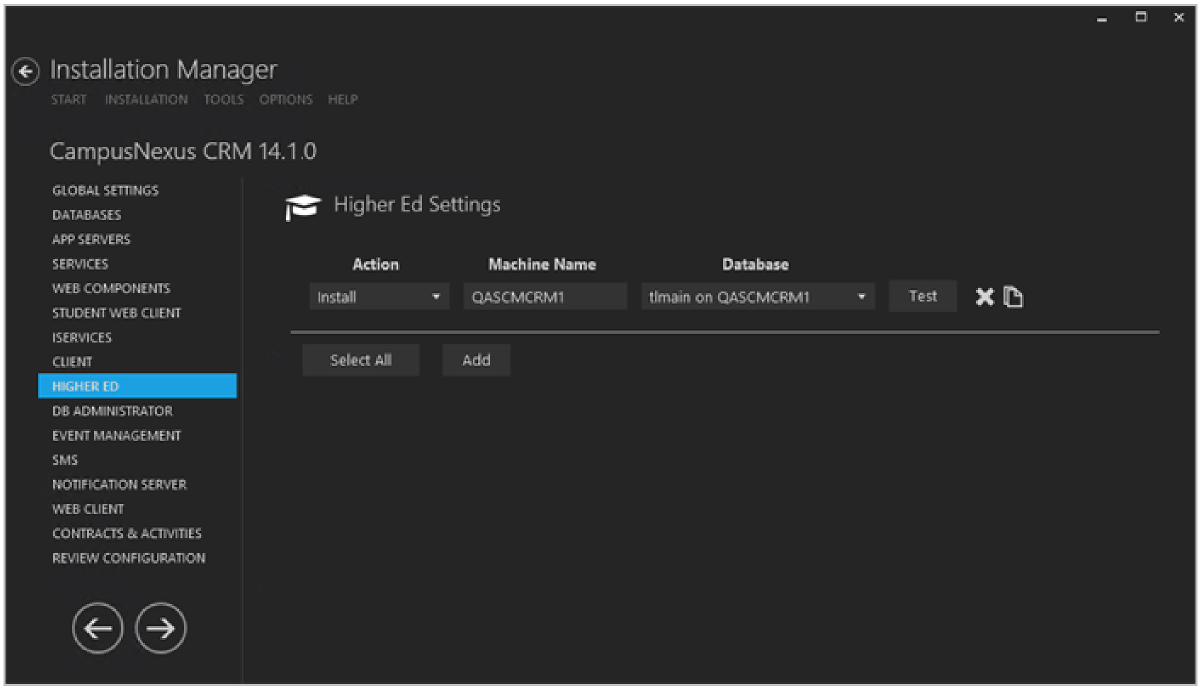
Preinstallation Tasks

1. Stop the SQL Server Agent on the computers where the Main and Subscriber databases are installed.
2. Set the value of Linked Servers, Data Access option to True. To do so:
   a. Navigate to **Microsoft SQL Management Studio**, open **Server Objects**, and select **Linked Servers**.
   b. Select **Properties** from the shortcut menu. The Linked Server Properties screen is displayed.
   c. Click **Server Options** in the left pane.
   d. In the right pane, ensure that the value of the **Data Access** option is set to **True**.
   e. Perform steps (a) through (d) for all **Linked Servers**.

Set Up Higher Ed

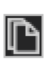
1. In the Installation menu, click **Higher Ed**. The Higher Ed Settings screen is displayed.

   This screen enables users to install or delete machine/database combinations used in the Higher Education Foundation module. The settings on this screen may be affected by information added in other steps of the setup process.



Note: Ensure that the default SQL Server settings are appropriate. Installation Manager allows multiple machine names listed in the Machine Name column.

2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select a **Database** from the Database list.
6. Click  to copy a line. Edit the copied line as needed.
7. Click  to delete a selected line.
8. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
9. If all tests pass, click .

Postinstallation Tasks

- If you are migrating from a non-Higher Ed environment to a Higher Ed environment with this installation, run the **sproc_UpgradeCountryAndStateForSis** script manually by executing the following commands:

  ```
  Declare @nUserID int = 2,@tTraceString  nvarchar(max) = N'',@retval int = 0
  EXEC @retval =   sproc_UpgradeCountryAndStateForSis @nUserID = @nUserID , @tTraceString =
  @tTraceString  output
  SELECT @retval ,@tTraceString
  ```

  Note: The time taken to execute this script completely may vary depending on the number contact, account, and order object instances that exist in the system.

  Start the SQL Server Agent service on computers where the Main and Subscriber databases are installed.

- Run the following script:

  ```
  CREATE NONCLUSTERED INDEX [IX_tblObjectType20005_bDeleted_nMergedWithID_aID_nTeamID_
  tName]
  ON [dbo].[tblObjectType20005] ([bDeleted],[nMergedWithID],[aID],[nTeamID])
  INCLUDE ([tName])
  GO
  ```

DB Administrator

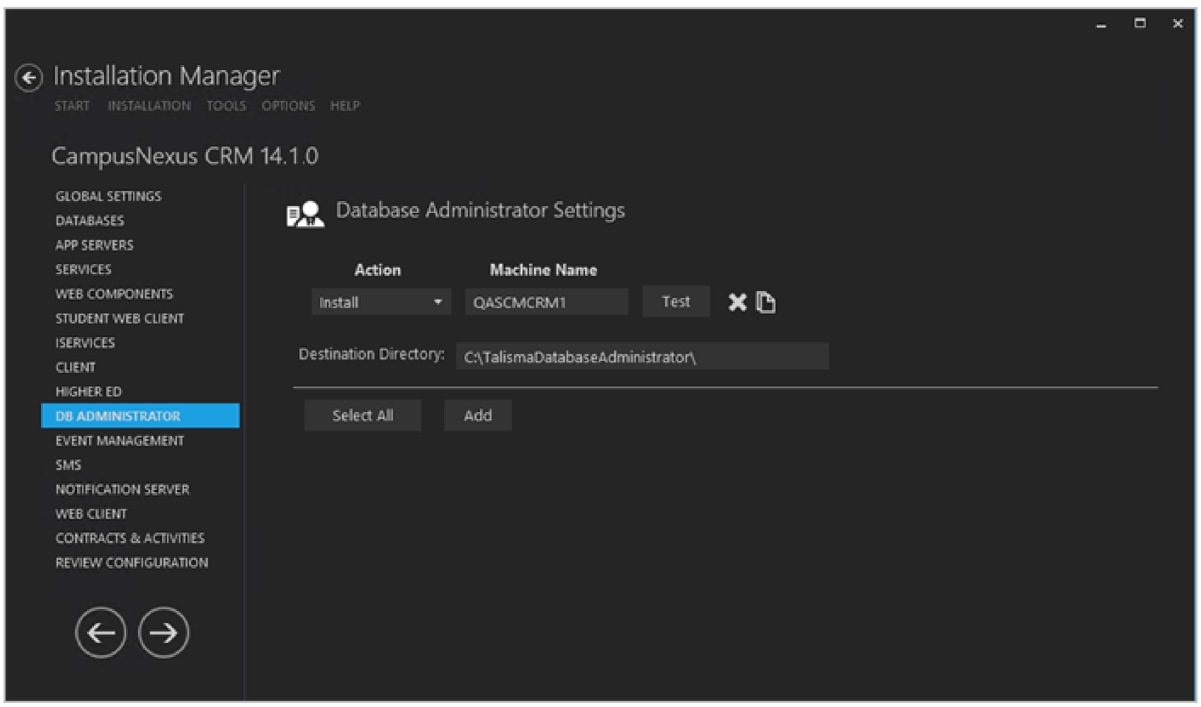
The Database Administrator component is a snap-in for the Microsoft Management Console (MMC) and can be used to manage the functioning of CampusNexus CRM databases. The Database Administrator component controls all the administrative tasks performed on CampusNexus CRM databases, Campaign Dispatchers, and Services.

Prerequisite

Identify and install the prerequisite software. See Software Requirements by Component — Database Administrator.

Set Up the Database Administrator

1. In the Installation menu, click **DB Administrator**. The Database Administrator Settings screen is displayed.

   This screen contains essential information associated with installing the Database Administrator Module.

   Note: Ensure that the Database settings are appropriate. Installation Manager allows multiple machine names listed in the Machine Name column.

2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
- **Reinstall** – Retries to install a subcomponent.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Click  to copy a line. Edit the copied line as needed.
6. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.
7. Click  to delete a selected line.
8. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
9. If all tests pass, click .

Postinstallation Tasks

Before using Database Administrator, you must perform the following configurations:

1. On the computer where the Main database is installed perform the following steps:
    a. On the computer where Database Administrator is installed, download the **PsExec.exe** and save it in the **<Drive name:\Program Files\Common Files\Talisma Shared** folder.
    b. Double-click **PsExec.exe** using the **Run as administrator** option.
2. As the Database computer establishes a remote connection with the Services computer, ensure that File and Printer Sharing for Microsoft Networks component is turned on for remote-management functions to work.

Event Management

When you install Event Management, two new Objects are created: *Event* and *Participant*. The Event Object enables you to create free and paid Events in Client. The Participant Object enables you to identify Object items added to an Event.

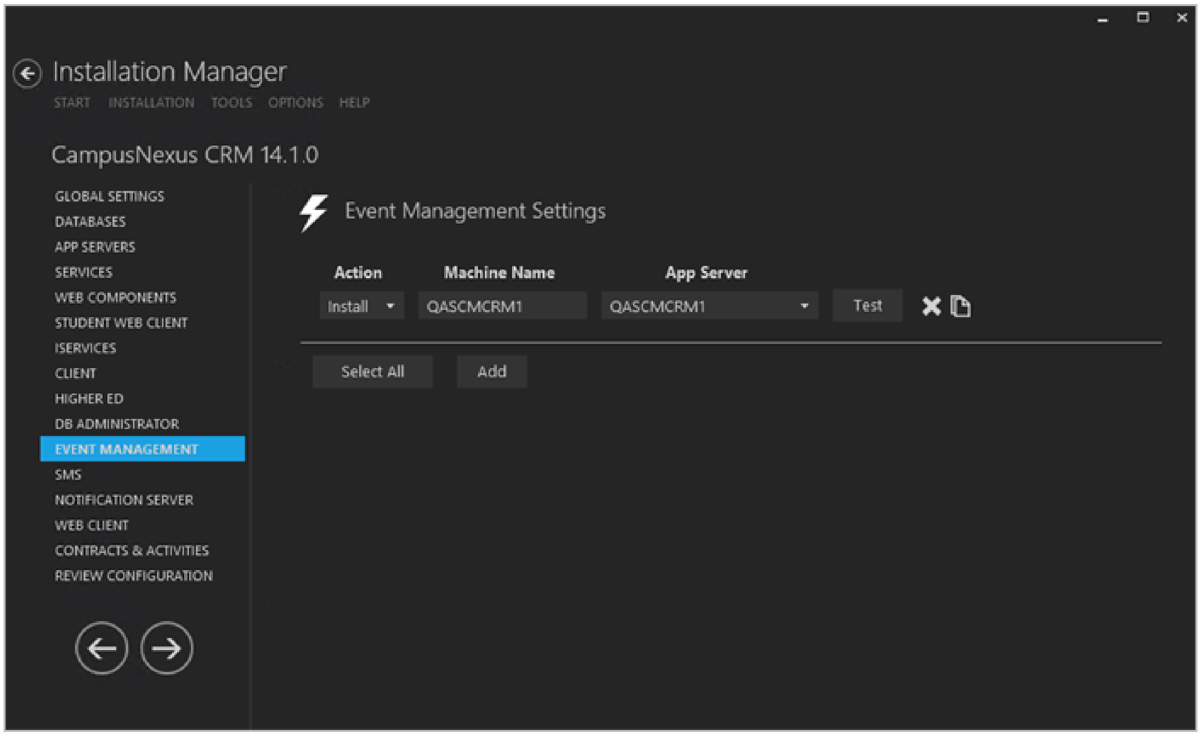
Institutions can customize the Event Management feature by including forms to enable students to manage their online participation in events. This can be accomplished using applications such as Forms Builder.

Prerequisites

1. Your installation of CampusNexus CRM does not already include custom Objects called Event and Participant.
2. Your installation of CampusNexus CRM does not already include Tabs or Properties that have the same names as the Tabs and Properties of the Event and Participant Objects.
3. You have a valid license to install Event Management.
4. You have removed any previous version of Event Management from your computer.
5. The Database replication is complete.
6. The SQL Server Agent service is stopped on the following computers:
   - Computer on which the Main database is installed.
   - Computer on which the Analytics database is installed.

Set Up Event Management

1. In the Installation menu, click **Event Management**. The Event Management Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select a **Database** from the Database list.
6. Click to copy a line. Edit the copied line as needed.
7. Click to delete a selected line.
8. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
9. If all tests pass, click .

Postinstallation Tasks

Start the SQL Server Agent service on the following computers:

- Computer on which the Main database is installed.
- Computer on which the Analytics database is installed.

SMS

To implement Short Messaging Service (SMS) in your organization, install the following components:

- **SMS Dispatcher Service** – This is a Windows service that dispatches SMS messages to the web server of the service provider. The service provider dispatches these messages to recipients.
- **SMS Extractor Service** – This is a Windows service that must be installed. SMS messages are pushed to this Windows service from the web server to which they were pushed by the service provider, or extracted from the service provider. The service processes SMS content received in a specific format from the service provider. This processed information (SMS message or SMS Status) is then transferred to the Main database.
- **SMS Web Service** – This is the IIS virtual root to which the service provider pushes SMS messages or delivery statuses (e.g., SMS-Magic) specific to your organization. Alternatively, this web service can be configured to pull SMS messages from the service provider.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — SMS.

Install the SMS dispatcher and extractor services as follows:

1. To install the SMS Dispatcher Service, obtain the following information from the respective service provider:
   - Credentials of your account with service provider like user name, password, APP ID or Label. These details can change from provider to provider.
   - If your organization is integrating SMS with Clickatell, in addition to the above information, create an API ID using the XML POST method from Clickatell.

     To do so:

     a. Log on to the Clickatell website using the Clickatell user name and password details.

     b. Click the **Manage my Products** tab.

     c. In the Connection Setup page, click **XML**. The Add Connection, XML API page is displayed.

     d. In the Description field, specify a description for the XML API, and click the **Submit and Get API ID** button. An XML API is created.
   - Public URL – The URL from the service provider to which the SMS Dispatcher Service will send the SMS message.

     Example of Public URL for:

    - Clickatell: `https://api.clickatell.com/xml/xml`
    - SMS-Magic: `https://api.sms-magic.co`
2. To install the SMS Extractor Service, obtain the following details:

   When the service provider is ValueFirst:

   - URL of the service provider
   - User name and password details of your account

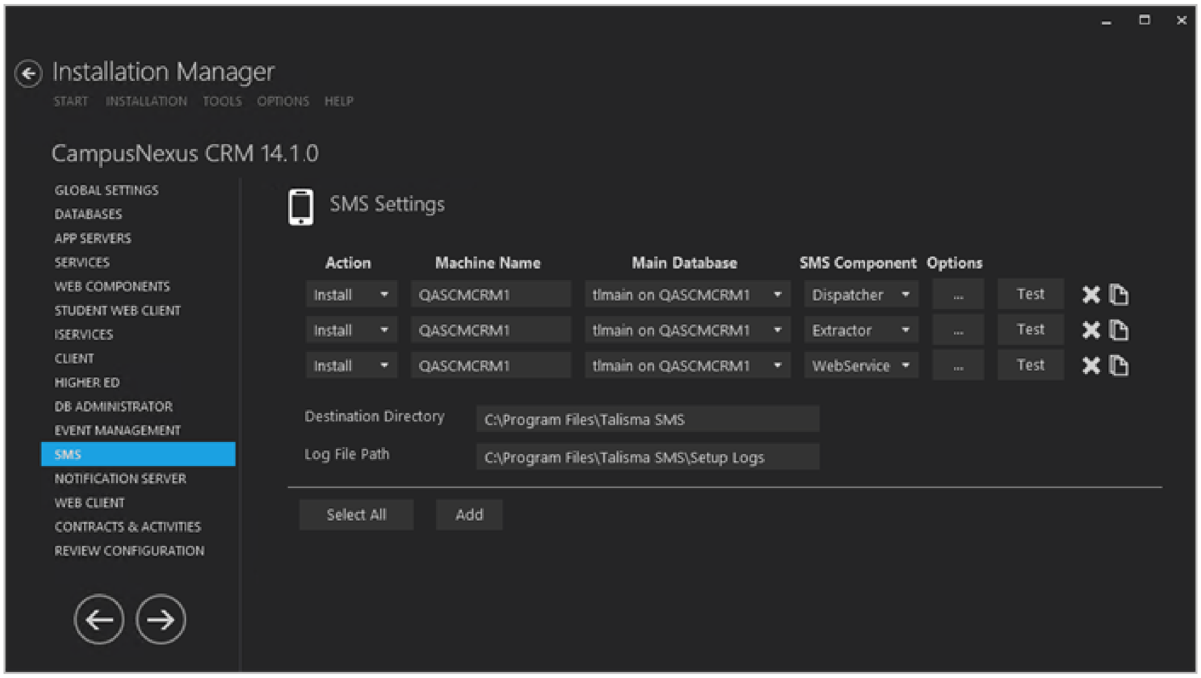
   If you are integrating with any service provider, including ValueFirst:

   - **Short Code or Long Code** – A code provided by the service provider that customers will use to respond to SMS messages.

     Occasionally, the same Short Code is shared among multiple organizations. This is referred to as a **Shared Short Code**. If an organization requests a Shared Short Code, the service provider provides a Keyword to the organization which helps the service provider to dispatch the SMS messages received from the customers to the correct organization based on the Keyword specified in the SMS message.
   - **Keyword** – A text, numeric, or a combination of text and numeric characters that an organization requests a recipient of an SMS message to type in the response SMS message. The organization performs specific actions based on the Keyword typed by the recipients in the response SMS message. This is optional based on the service provider and account of the customer. It is required only with the short code.

Set Up SMS

1. In the Installation menu, click **SMS**. The SMS Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
   - **Reinstall** – Retries to install a subcomponent.
   - **Add** – Installs an additional component on the computer where one or more components already exist. You can add only one component at a time.
   - **Remove** – Uninstalls a single component. You can remove only one component at a time.

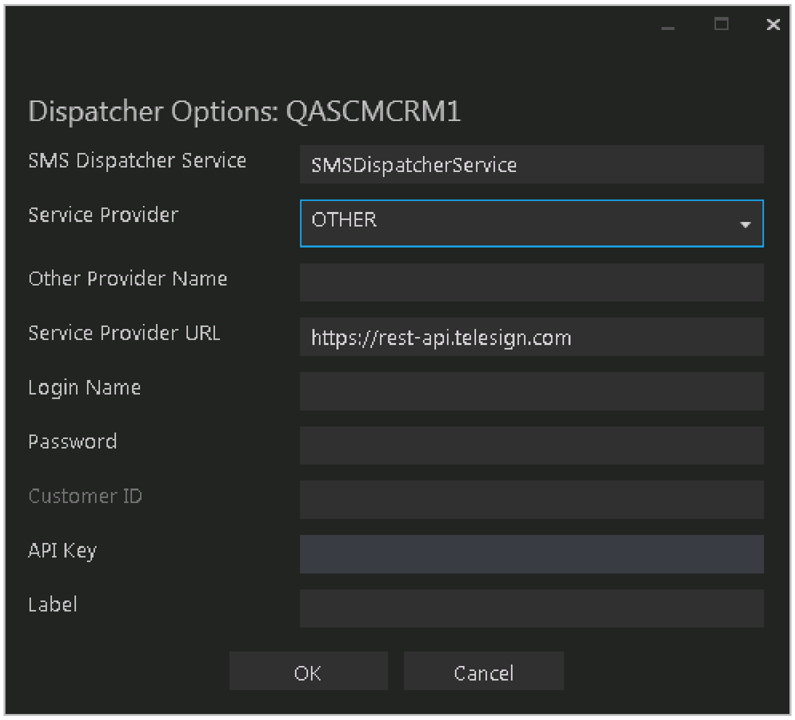
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select a **Database** from the Database list.
6. Select an **SMS Component**. The options are:

- Dispatcher
- Extractor
- WebService

Note: If you are installing all SMS components, make sure Extractor Service is installed before WebService.

7. Select **Dispatcher** from the SMS Component list.

8. Click to view and edit the Options form.



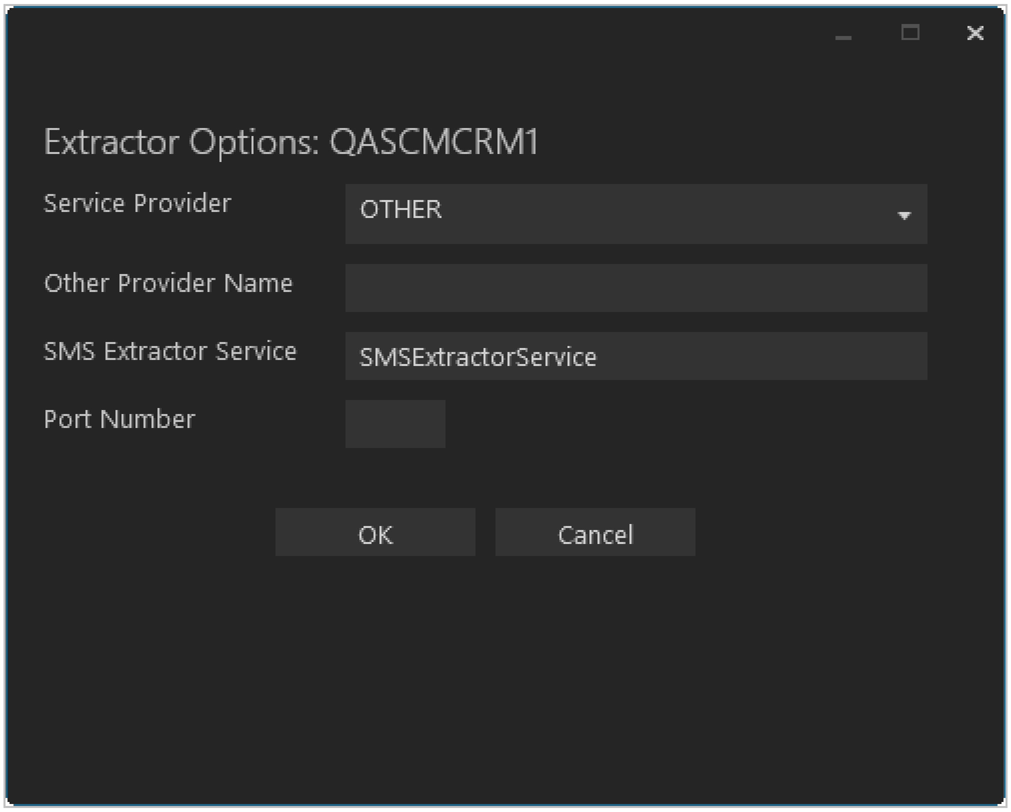
9. In the **Dispatcher Options** form, complete the following fields as applicable:
   - SMS Dispatcher Service
   - Service Provider
   - Other Provider Name — displayed only when OTHER is selected.
   - Service Provider URL
   - Login Name — disabled for TELESIGN
   - Password — disabled for TELESIGN
   - Customer ID — enabled only when TELESIGN is selected.
   - API Key
   - Label

10. Click **OK** to save changes on the Options form. The form is closed.

11. Click to copy a line. Edit the copied line as needed.

12. Select **Extractor** from the SMS Component list.

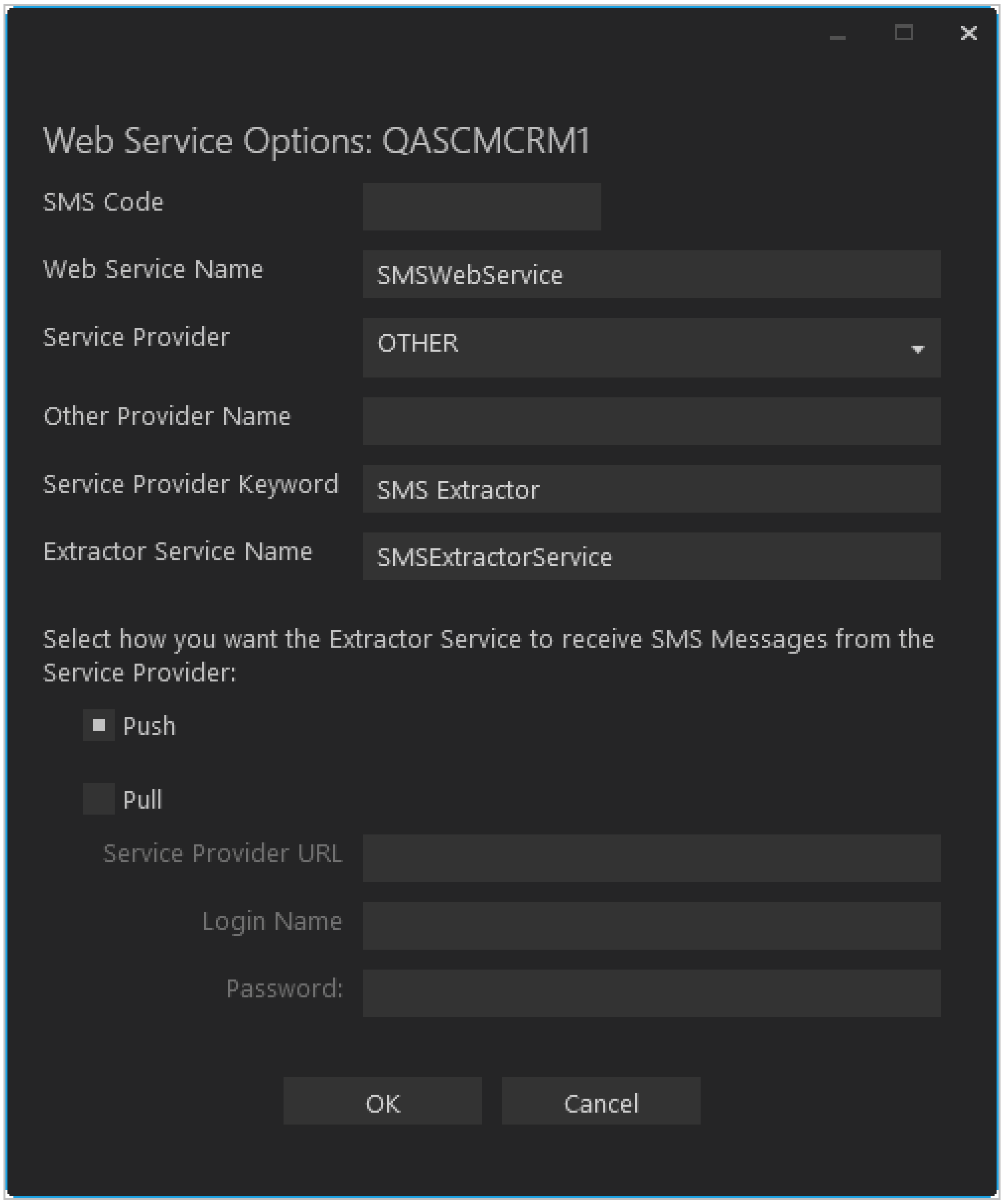
13. Click ··· to view and edit the Options form.



14. In the **Extractor Options** form, complete the following fields as applicable:
    - Service Provider
    - Other Provider Name – This field is displayed only when the Service Provider OTHER is selected.
    - SMS Extractor Service Name
    - Port Number

    Notes:

    - Do not specify the value 80 or other known port numbers in the Port Number field.
    - Ensure that the TCP port specified in the Port Number field is open between servers where the SMS virtual root and SMS Extractor Service are installed.
15. Click **OK** to save changes on the Options form. The form is closed.
16. Click to copy a line. Edit the copied line as needed.
17. Select **WebService** from the SMS Component list.
18. Click ··· to view and edit the Options form.



19. In the **Web Service Options** form, complete the following fields as applicable:

    - SMS Code — Depending on the Service Provider, the SMS Code field allows the following input values:

Service Provider	SMS Code
CLICKATELL	Numeric
OTHER	Any character
SMSMAGIC	Alphanumeric

Service Provider	SMS Code
TELESIGN	Numeric
VALUEFIRST	Numeric

- Web Service Name
- Service Provider
- Other Provider Name — This field is displayed only when the Service Provider "Other" is selected.
- Service Provider Keyword — This is optional based on the service provider. Specify this if your provider has given this information.
- Extractor Service Name

The supported method to receive SMS Messages is **Push** for all services providers except VALUEFIRST, which uses the **Pull** method.

If you select the **Pull** method, specify the following:

- Service Provider URL
- Login Name
- Password

20. Click **OK** to save changes on the Options form. The form is closed.
21. Click  to delete a selected line.
22. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.
23. Specify the **Log File Path** or accept the default: `C:\Program Files\Talisma SMS\Setup Logs`

    The Log File Path applies to all the machine names configured in the SMS Settings screen.
24. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
25. If all tests pass, click .

Note: In a scenario where multiple long codes are available in your organization, to ensure that the auto response to the contact is sent from the correct dispatcher, the **AutoResponseDispatcherID** parameter must be updated in the **TLSysSMSWindowService.exe.config** file of the associated extractor. This file is available in the path where the SMS Extractor is installed.

1. Navigate to the path were the extractor is installed.
2. Open the **TLSysSMSWindowService.exe.config** file using a text editor (e.g., Notepad) and update the value in the following code:

   ```
   <add key="AutoResponseDispatcherId" value="" />
   ```

3. In the value field, type the dispatcher's ID that is associated with the long code. The ID is available in the **tblSMSServices** table of Main database in the **aSMSServiceID** column.
4. Save the file and then restart the SMS Extractor service.

Configuration

Configure Multiple SMS Dispatcher Services

You can install multiple SMS Dispatcher Services which can be configured to send SMS messages to customers of a specific country using the SMS Dispatcher Service installed for that country. To configure SMS Dispatcher Service for a country, perform the following steps:

1. Obtain the name of the SMS Dispatcher Service installed for a specific country from the **tblsmsservices** table in the Main database.
2. Add a row in the **tblglobalinfo** table for the SMS Dispatcher Service obtained in Step 1.

   You can use the following SQL query to add a row in the **tblglobalinfo** table:

   ```
   Insert into tblglobalinfo(tValueName, tValueData, nLanguageID, bShowInBizAdmin,
   nDataType, tDisplayName, tGroupName, tComments) values('<SMSDispatcherService
   name>','<country code>',

   NULL, 0, NULL, NULL, 'General','<Comment>')
   ```

   Example

   To add a row in the **tblglobalinfo** table for the **SMSISDCode_4** SMS Dispatcher Service, installed for UK, use the following SQL:

   ```
   Insert into tblglobalinfo(tValueName, TValueData, nLanguageID, bShowInBizAdmin,
   DataType, tDisplayName,

   tGroupName, tComments) values('SMSISDCode_4','+44', NULL,0, NULL, NULL, 'Gen-
   eral','UK')
   ```

3. Restart the SMS Dispatcher Service.

In Client, the user must select the required SMS Dispatcher Service configured for the country in the **SMS Dispatcher** field in the New SMS Message dialog box before sending an SMS.

Configure the Clickatell Page to Extract SMS Messages

To configure the Clickatell page to extract SMS messages sent by end users perform the following steps:

1. Using your login credentials, log on to http://www.clickatell.com.
2. Click the **Manage my Products** tab.
3. In the left pane, click **Two-Way Messaging**. The Two Way SMS (MO) page is displayed.
4. In the Primary Callback area, perform the following steps:
    a. Select **XML POST** from the **Reply Path** list.
    b. In the **Target Address** field, specify the public URL of the **sms.aspx** file. The sms.aspx file is created when you install the SMS Web Service.

    Note: Ensure that the URL specified in the Target Address field is accessible from a public domain.
5. Click **Commit**. The configuration is saved.

Configure the SMS-Magic Page to Extract SMS Messages

1. Using your login credentials, log on to http://www.sms-magic.co.
2. In the dropdown of your login name, click **Product Inventory**. The Product Inventory page is displayed.
3. In the SMS Products tab, click **Configure**.
4. In the **Delivery Reports URL** field, type the URL of the SMS Web Service for delivery reports in the following format:

    http://<publicly available IP address>/<web service name>/api/push/PushSMSStatuses
5. Click **Save**. A message is displayed that the configuration is saved.
6. In the Number Products tab, click **Configure**.
7. In the **Incoming URL** field, type the URL of the SMS Web Service for incoming SMS messages in the following format:

    http://<publicly available IP address>/<web service name>/api/push/PushSMSMessages
8. Click **Save**. A message is displayed that the configuration is saved.

Integrate with TeleSign

Configurations

1. Run the following insert statement on Main database:

```
insert into tblGlobalInfo values (N'smsISDCode_<SMS_Dispatcher_Service_ID>', N'<Country_Code>',
NULL, 0, NULL, NULL, N'General', NULL)
```

2. Replace the following placeholders:
    - <SMS_Dispatcher_Service_ID> - obtain the ID of the SMS dispatcher service from the aSMSServiceID column of the tblSMSServices table.

      To do so, run the following query on Main database:

      SELECT aSMSServiceID FROM tblSMSServices WITH (NOLOCK) WHERE nProviderId = 4 AND nServiceType = 1

      Run the insert statement in step 1 for all Telesign dispatcher service IDs that are retrieved.
    - <Country_Code> - the country code of the recipient's phone number.

   For example, insert into tblGlobalInfo values (N'smsISDCode_6', N'1', NULL, 0, NULL, NULL, N'General', NULL).

   Ensure that an SMS Dispatcher service that's associated with a specific country code is not associated again with another country code.

   When the SMS message is sent by the TeleSign service provider, the recipient's phone number will be suffixed to the country code.

Configure the TeleSign Page to Extract SMS Messages

To complete SMS configuration for TeleSign, the Delivery Reports URL field and the Incoming URL field must be sent to TeleSign. Further steps to complete the configuration will be performed by TeleSign.

The URLs must be in the following format:

- Delivery Reports URL: http://<publicly available IP address>/<web service name>/api/push/PushSMSStatuses
- Incoming URL: http://<publicly available IP address>/<web service name>/api/push/PushSMSStatuses

Increasing the Count of SMS Dispatcher Threads – TeleSign

By default, SMS messages in campaigns are dispatched in a single thread. An institution can increase the count of threads in the SMS dispatcher. This will enable all threads to be processed concurrently, thus speeding up the count of dispatched SMS messages.

1. In the SMS dispatcher service, open the file **TLSysSMSDispatcherWindowsService.exe.config** using a text editor.
2. Change the value of the **ConcurrentThreads** key to a different value (in the range 1 - 25).

<add key="ConcurrentThreads" value="1" />. Its default value is 1.

Restart the SMS dispatcher.

Note: If the value of the **ConcurrentThreads** key is changed to:

- A value less than 1, the value 1 will be considered.
- A value greater than 25, the value 25 will be considered.

Configurations for the Double Opt-In Feature

To work with the Double Opt-In functionality of SMS, Opt-In and Opt-Out keywords are available. In the initial SMS message sent to Contacts or Leads, organization requests the recipients to respond with a specific Opt-In or Opt-Out keyword. Based on the type of keyword in the response SMS from the recipients, the Double Opt-In (SMS) Property of the Contact and Lead is updated appropriately. For more information on working with the Double Opt-In feature, see Client Help.

Note: Keywords are words or phrases that an organization requests a recipient of an SMS message to type in the response SMS Message. The organization performs specific actions based on the keyword typed by the recipients in the response SMS message.

The information about the Opt-In and Opt-Out keywords are stored in the following tables in the Main database:

- **tblSMSStopCommands** — This table stores the details of the commands that are used to unsubscribe or Opt-Out from SMS services. By default, the following commands are available in the tblSMSStopCommands table.
  - STOP
  - END
  - CANCEL
  - UNSUBSCRIBE
  - QUIT
  - STOP STOP
  - STOP ALL

  A Database Administrator can insert additional unsubscribe commands in this table based on the business requirements. For example, to insert `No` as the unsubscribe command use the following SQL statement.

  ```
  Exec sproc_AddSMSCommands 1, No
  ```

  To configure another Opt-Out keyword, replace the text in red with the Opt-Out keyword in the above SQL statement.

  Note: If you have integrated SMS with Clickatell, the Opt-Out keywords configured in CampusNexus CRM must match with the Opt-Out keywords provided by Clickatell.

- **tblSMSSubscribeCommands** — This table stores the details of the commands that are used to subscribe or Opt-In for SMS services. By default, the following commands are available in the tblSMSSubscribeCommands table.

- START
- OPT IN

The CampusNexus CRM database administrator can insert additional subscribe commands in this table based on the business requirements. For example, to insert Yes as the subscribe command, use the following SQL statement.

```
Exec sproc_AddSMSCommands 2, Yes
```

To configure another Opt-In keyword, replace the text in red with the Opt-In keyword in the above SQL statement.

Notification Server

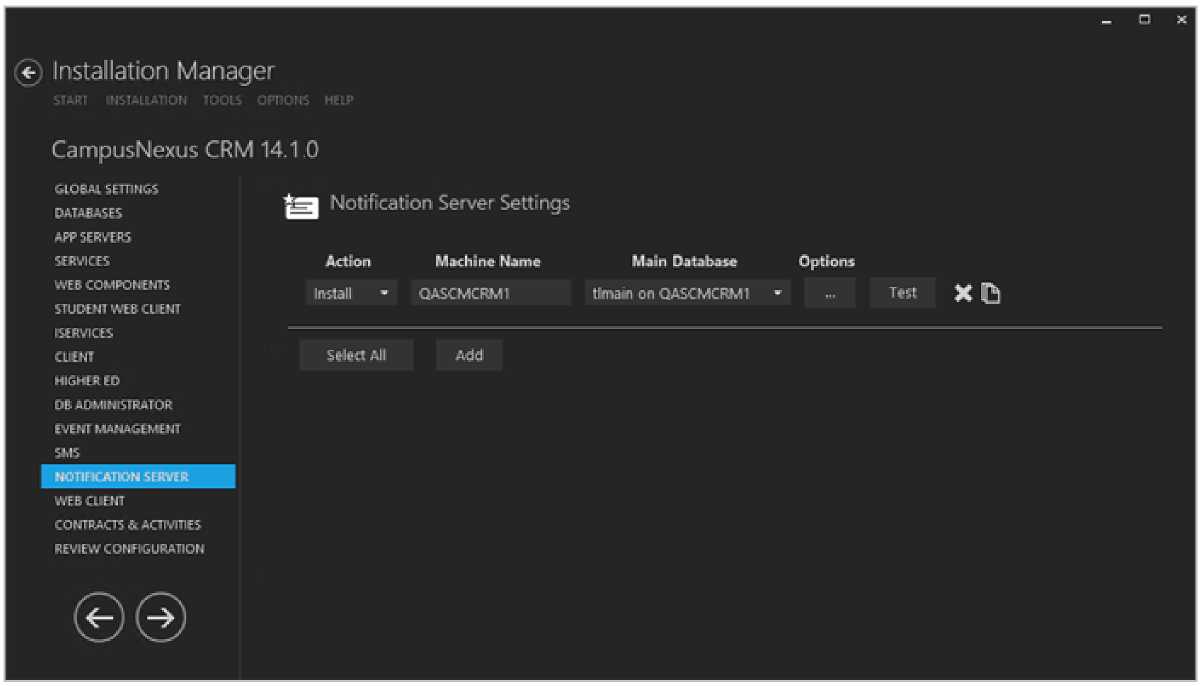
The Web Client Notification component is used to send notifications about chat sessions, incoming phone calls and interactions, and broadcast messages to end users.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — Notification Server.

Set Up Notification Servers

1. In the Installation menu, click **Notification Server**. The Notification Server Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

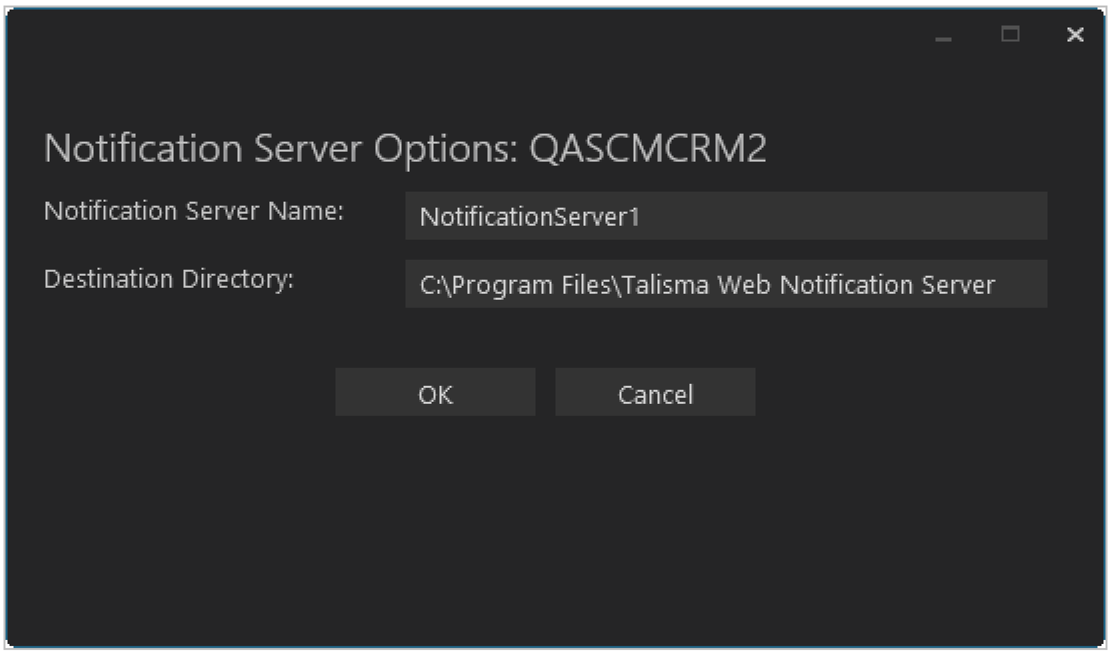
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.
   - **Reinstall** – Retries to install a subcomponent.

- **Add** – Installs an additional component on the computer where one or more components already exist. You can add only one component at a time.

- **Remove** – Uninstalls a single component. You can remove only one component at a time.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Select a **Database** from the Database list.
6. Click to copy a line. Edit the copied line as needed.
7. Click to view and edit the Options form.



8. In the **Notification Server Options** form, complete the following fields as applicable:
   - Notification Server Options Name
   - Destination Directory
9. Click **OK** to save changes on the Options form. The form is closed.
10. Click to delete a selected line.
11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
12. If all tests pass, click .

Postinstallation Tasks

The following code in the web.config file that is available in the <Talisma Web Notification Server installation folder>\Web.config path enables you to specify the Web Client URL that will use the functionality of the notification service to send notifications to Web Client users.

1. Navigate to the following code using a text editor (e.g., Notepad).

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
    <add name=”Access-Control-Allow-Origin” value=”*” />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

2. Replace the asterisk (*) with the Web Client URL and then save and close the web.config file.

Web Client

The Web Client component supports browser-based access allowing agents to access critical CampusNexus CRM functions through the Internet from anywhere in the world.

Prerequisites

Identify and install the prerequisite software. See Software Requirements by Component — Web Client.

- Before installing the Web Client for CampusNexus CRM, uninstall previous versions of Web Client.
- The Web Client for CampusNexus CRM version 11.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

  As a result of the installation, the following appSettings are added to the web.config of the web service.

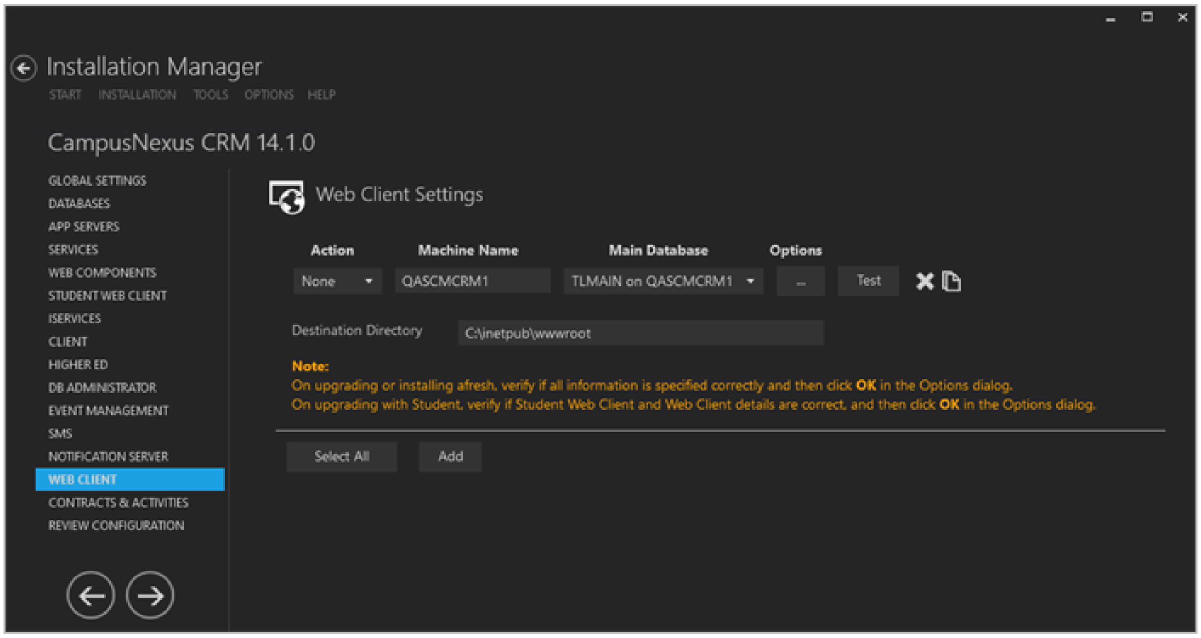
  ```
  <appSettings>
  <add key="ServerConfig" value="<server>/<MainDB>" />
  <add key="UserName" value="<UserName>" />
  <add key="CoreLogging" value="1" />
  </appSettings>
  ```

  The Staff STS uses this new web service to authorize and authenticate CampusNexus CRM Web Client Staff logins.

  ```
  <SecurityServiceCollection>
  <add name="<name>" address="<URL>" enabled="false" />
  <add name="CRM" address="http://StaffSTSServiceServer/<VirtualDirectoryName>/ Secur-
  ity/SecurityService.svc" />
  </SecurityServiceCollection>
  ```

Set Up Web Clients

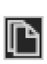
1. In the Installation menu, click **Web Client**. The Web Client Settings screen is displayed.



Note:

- When upgrading or installing CampusNexus CRM, verify all settings and then click **OK** in the Options dialog.
- When upgrading with Anthology Student, verify the Student Web Client and Web Client details and then click **OK** in the Options dialog.

2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

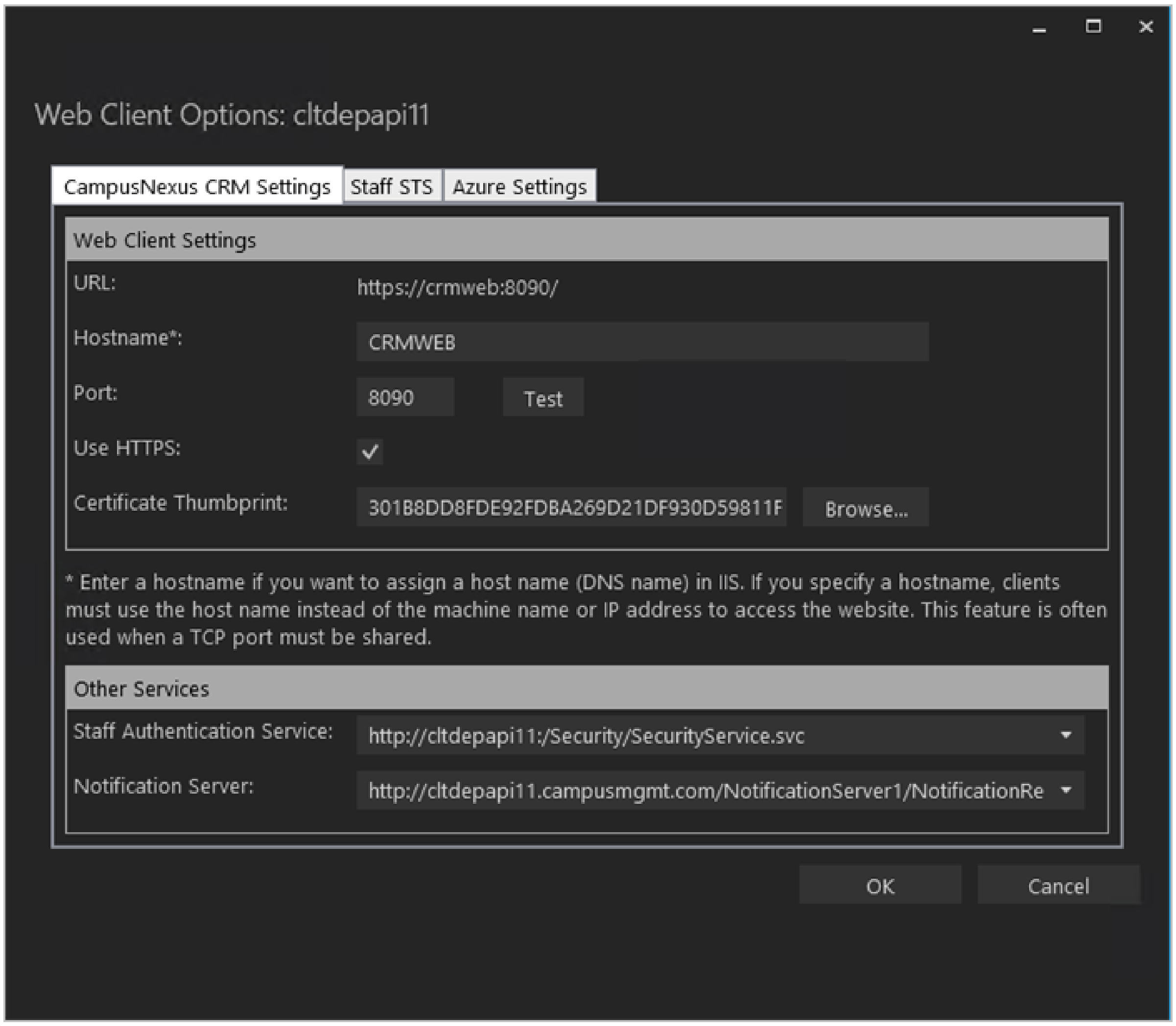
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select a **Database** from the Database list.
6. Click  to copy a line. Edit the copied line as needed.

7. Click  to view and edit the Options form.

CampusNexus CRM Settings Tab

Used this tab to specify settings for the CRM Web Client, Staff Authentication Service, and Notification Server.

If multiple instances of Web Client are installed, they must all be associated with a common instance of Notification Server.



CampusNexus CRM Settings Tab Fields

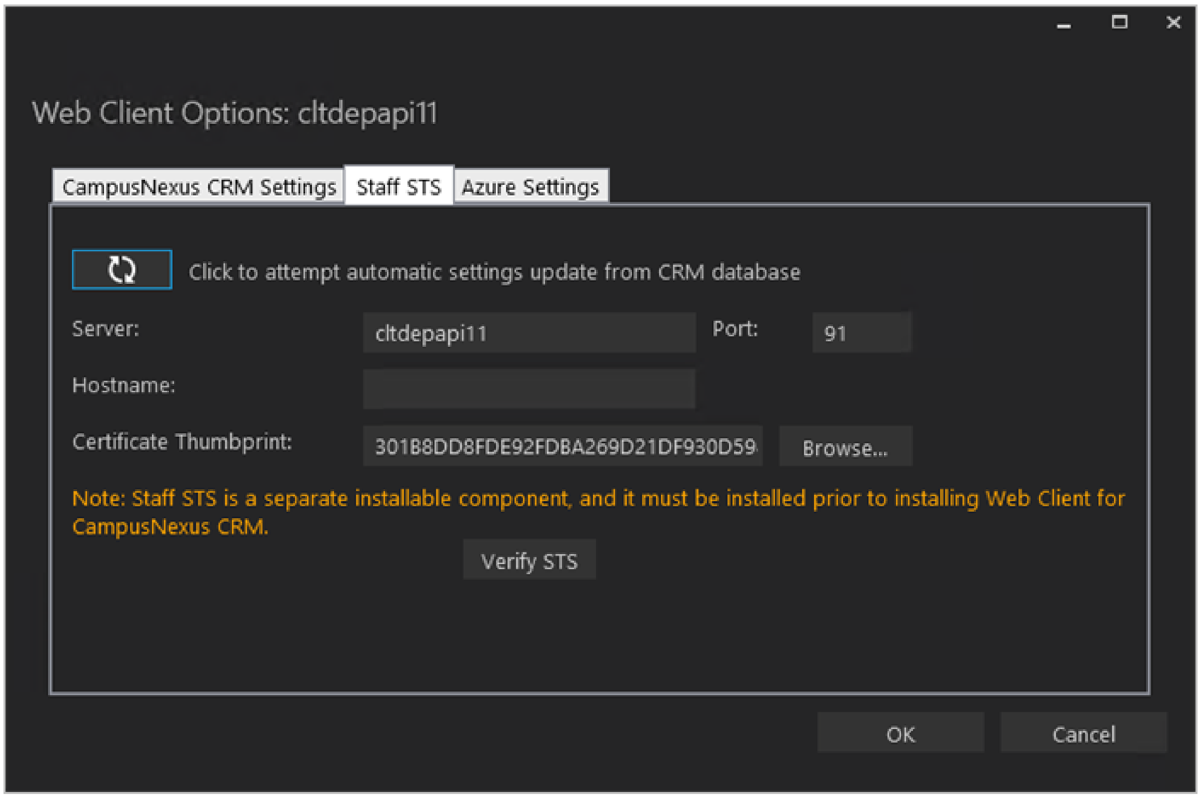
Field	Description
Web Client Settings	

Field	Description
URL	The Web Client URL is populated with <machine name.domain.com> by default. You can override the default URL with another URL. The specified URL will be updated in the web.config file of the Web Client for CampusNexus CRM and in the CampusNexus CRM database. If you change the Web Client URL during an upgrade in an environment where Forms Builder is used, the Web Client URL must be manually updated in the web.config files of Forms Builder Designer and Renderer.
Hostname	This is an optional field. When selected, the web.config file of the Web Client for CampusNexus CRM will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port` Enter a hostname if you want to assign a hostname (DNS name) in IIS. If you specify a hostname, clients must use the hostname instead of the machine name or IP address to access the website. This feature is often used when a TCP Port must be shared.
Port	Specify the port number of the Web Client for CampusNexus CRM or accept the default (8090).
Test	Click **Test** to ensure that the Staff STS setup is correct.
Use HTTPS	Select this check box if you want the CRM Web Client to be accessed through HTTPS. When this option is selected, the Certificate Thumbprint field is enabled.
Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected. It is not added to the web.config file. This certificate is used only for the CRM Web Client. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Other Services	

Field	Description
Staff Authentic-ation Service	Click ▼ to view the complete URL.
Notification Server	Click ▼ to view the complete URL.

Staff STS Tab

Use this tab to specify the Staff STS server, port, hostname (if applicable), and certificate. Staff STS must be installed prior to installing the Web Client for CampusNexus CRM.



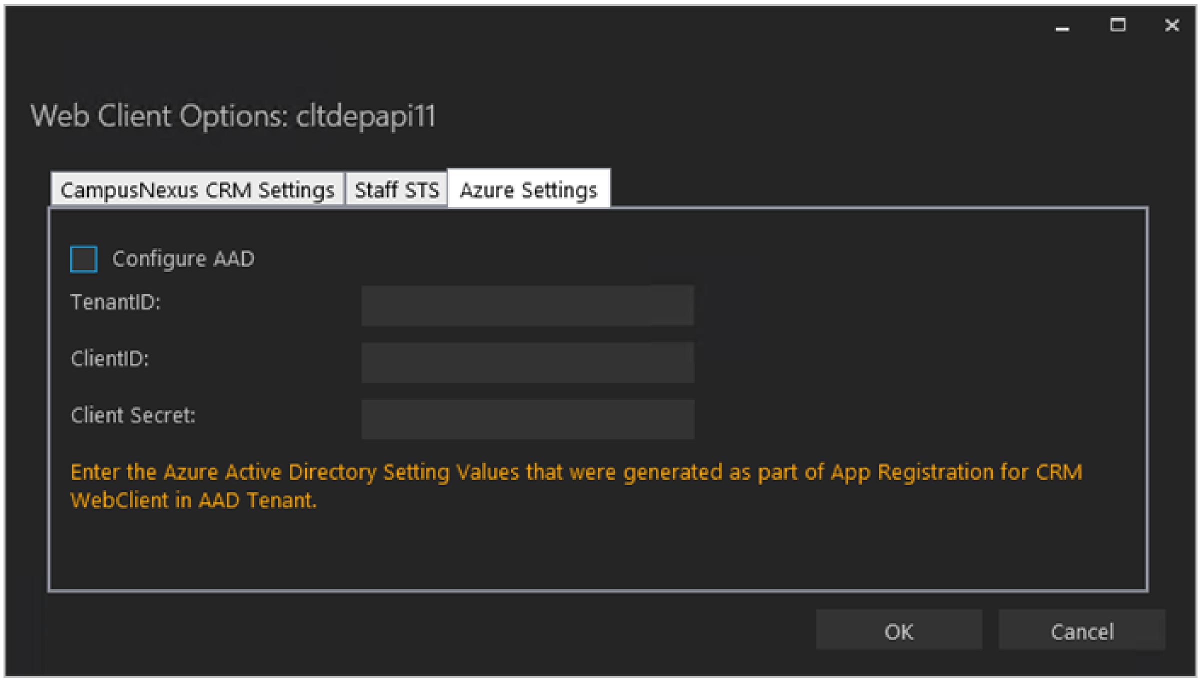
Staff STS Tab Fields

Field	Description
	Click the **Refresh** button to attempt an automatic settings update.
Staff STS Server	Specify the name of the Staff STS Server. The Staff STS Server must have been pre-viously installed. See Staff STS.
Port	Specify the port number of the installed Staff STS server or accept the default (91).
Staff STS Host-name	If you have configured Staff STS to use a custom hostname, fill out the hostname. Example: Staffsts.campusmgmt.com

Field	Description
Certificate Thumbprint	Certificate thumbprint from IIS. The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **Note**: Only RSA-based certificates are supported. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Verify STS	Click **Verify STS** to • Verify that the Staff STS is installed. • Validate that the certificate is installed in the personal store.

Azure Settings Tab

Use this tab to specify the Azure settings for the Web Client.



Azure Settings Tab Fields

Field	Description
Configure AAD	Select this check box if Azure Active Directory is used for the CampusNexus CRM web client.
Tenant ID	Specify the Azure tenant identifier.
Client ID	Specify the Azure client identifier.
Client Secret	Specify the Azure client secret.

8. Click **OK** to save changes on the Options form. The form is closed.
9. Click  to delete a selected line.
10. Accept the default **Destination Directory** or select a directory where the information for this component is stored. Changing this directory will apply across all machines in the Machine Name column.
11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
12. If all tests pass, click .

Postinstallation Tasks

Perform the following postinstallation steps for Web Client:

1. In the right pane of IIS Manager, double-click **ISAPI and CGI Restrictions** and ensure that the **Allowed** option is enabled for all the Web Service Extensions.

When the Web Client is installed on a Windows 64-bit computer, set the value of the Enable 32-Bit Applications option to False in the Internet Information Service Manager (IIS). To do so:

1. On the computer where Web Client is installed, open Internet Information Service Manager.
2. Click **Application Pools**.
3. Right-click the Application Pool on which Web Client is running, and select **Advanced Settings**.
4. Set the value of the **Enable 32-Bit Applications** option to **False**.
5. Click **OK**.

If the regional settings of the Web Client computer are not set to a 24-hour format, perform the following steps:

1. Launch IIS Manager on the Web Client computer.
2. Navigate to **Sites\Default Web Site\cmc.crm.workspaces**.
3. In the right pane, double-click **.NET Globalization**.
4. In the **Culture** list, select a language that supports a 24-hour format (E.g.: English (United Kingdom) (en-GB) or English (United States) (en-US)).
5. Reset IIS.

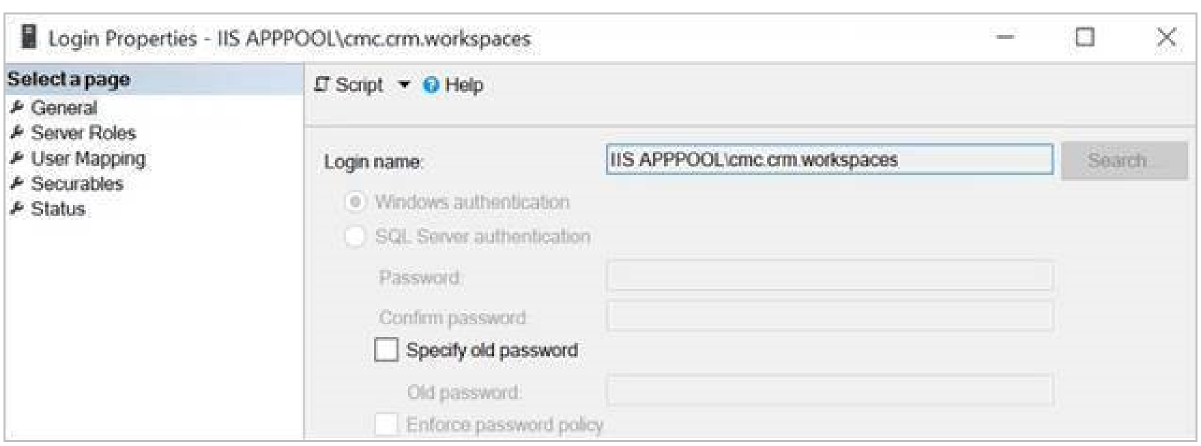
If SQL Server is running on the same computer as the Web Client web server and regardless of whether Workflow Composer is configured to work with CampusNexus CRM (From CampusNexus CRM 13.2 and later, Workflow Composer is integrated with CampusNexus CRM by default.):

a. Add the application pool account to the Main database:

   IIS APPPOOL\appPoolName

   For example:

   IIS APPPOOL\cmc.crm.workspaces



b. Make sure to give **db_datareader** and **public** access to the Main database.

Configuration Settings

You can set the value of the maxAttachmentSize and RestrictedFileFormat tags in the web.config file. To do so, perform the following steps:

1. Navigate to `<CampusNexus CRM installation folder>\cmc.crm.workspaces`.
2. Open the **web.config** file.
3. Add the maxAttachmentSize and RestrictedFileFormat tags and values.

"maxAttachmentSize" and "RestrictedFileFormat" Tags and Values

<table>
<tr><th>Tag</th><th>Description</th></tr>
<tr><td>maxAttachmentSize</td><td>

Enables you to set the maximum limit of the files that can be attached in Web Client.

For example, if the value of this parameter is set to 2048 kilobytes, a Web Client User can attach single or multiple files totaling to a size of 2 MB.

By default, the value of this tag is **25 MB**.

Important:

By default, the maximum allowed IIS (Internet Information Services) limit for file upload on any Website is 28.6 MB.

If you want to increase the maximum upload limit to a value that is greater than 25 MB, you must first configure your IIS file upload limit to the required value.

To do this, ensure you specify the appropriate value (in bytes) in the maxAllowedContentLength attribute. A sample code extract is shown here:

```
<security>
   <requestFiltering>
      <requestLimits>
         <headerLimits>
            <add header="Content-type" sizeLimit="30000000" />
         </headerLimits>
      </requestLimits>
   </requestFiltering>
</security>
```

After configuring the file upload limit value in IIS, you must configure the maxAttachmentSize

</td></tr>
<tr><td>RestrictedFileFormat</td><td>

Enables you to specify the file formats that cannot be attached in Web Client. To add a list of file formats that are not supported, add the extension of the file format in this tag. To add multiple file formats, separate the file extensions by the comma delimiter.

For example: `.txt,.jpeg,.gif`

The default value is `.exe, .bat`, which indicates that files with the .exe and .bat format cannot be attached in Web Client.

</td></tr>
</table>

4. **Save** the web.config file.

5. You can configure the execution time-out period for the Web Client server in the web.config file of Web Client. The execution time-out period is the elapsed time after which an execution request from the Web Client server is timed out. By default, the execution time-out period is set to 120 seconds.

   To specify a custom value for the execution time-out period, add the following line of code in the web.config file:

`<httpRuntime executionTimeout="<<Time-Out Period>>"/>`, where `<<Time-Out Period>>` is the elapsed time after which an execution request from the Web Client server must be timed out.

For example, specify: `<httpRuntime executionTimeout="360"/>`

6. **Save** and **close** the web.config file.

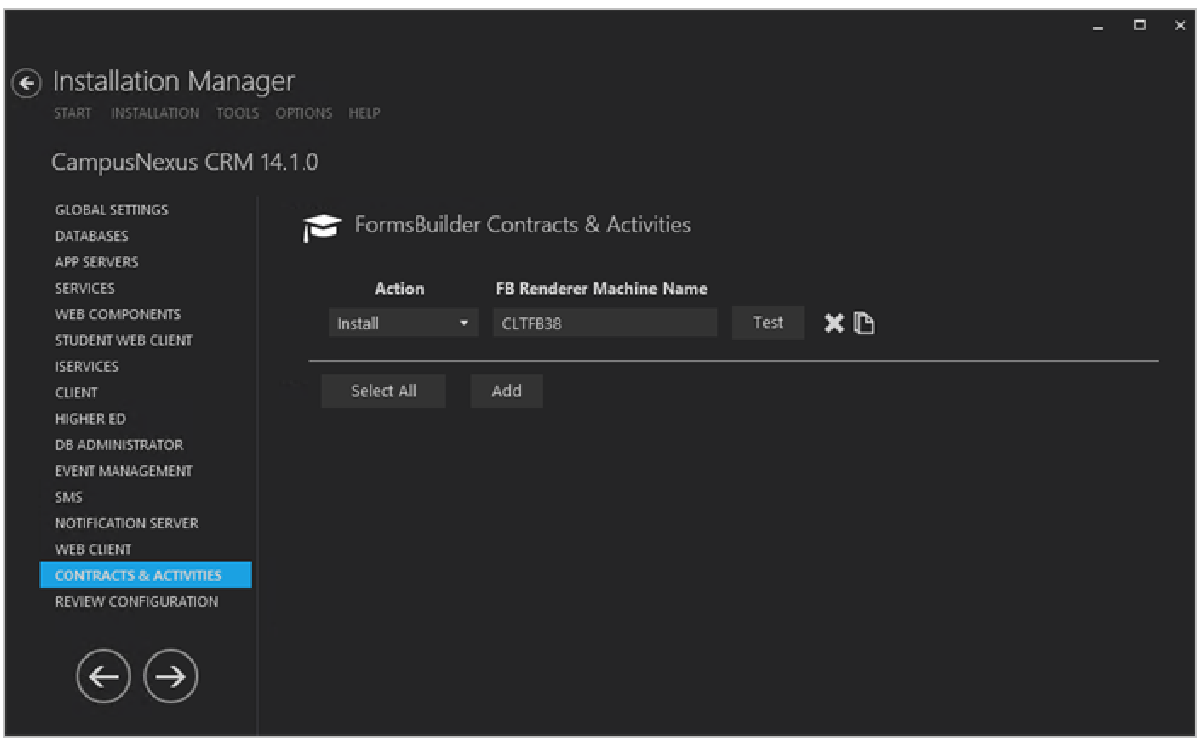
Contracts & Activities

Forms Builder 3.x and later is installed with a base set of Workflow Contracts and Activities. When CampusNexus CRM is upgraded to version 12.x, the CampusNexus CRM Contracts and Activities used by Forms Builder need to be upgraded as well.

This Settings screen enables you to select the actions to be taken by Installation Manager and to specify the machine name of the Forms Builder Renderer where the CampusNexus CRM Workflow Contracts and Activities for Forms Builder are used.

Set Up Contracts & Activities

1. In the Installation menu, click **Contracts & Activities**. The Forms Builder Contracts & Activities screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter a **Machine Name** of the Forms Builder Renderer where the Contracts & Activities are used.
5. Click  to copy a line. Edit the copied line as needed.
6. Click  to delete a selected line.
7. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
8. If all tests pass, click .

Postinstallation Tasks

If you have Forms Builder installed for CampusNexus CRM, perform the following steps:

1. Log in to the Web Client for CampusNexus CRM.
2. Navigate to **{SystemDrive}\inetpub\wwwroot\cmc.crm.workspaces\bin**.
3. Copy the **Cmc.NexusCrm.Contracts.dll** file and paste it into the following locations:

   {SystemDrive}\Program Files (x86)\CMC\Workflow for Workflow Composer

   {SystemDrive}\inetpub\wwwroot\CMCFormsRenderer_V3\bin for Forms Builder 3.x and later

   {SystemDrive}\inetpub\wwwroot\CMCFormsRenderer\bin for Forms Builder 2.x (if applicable)

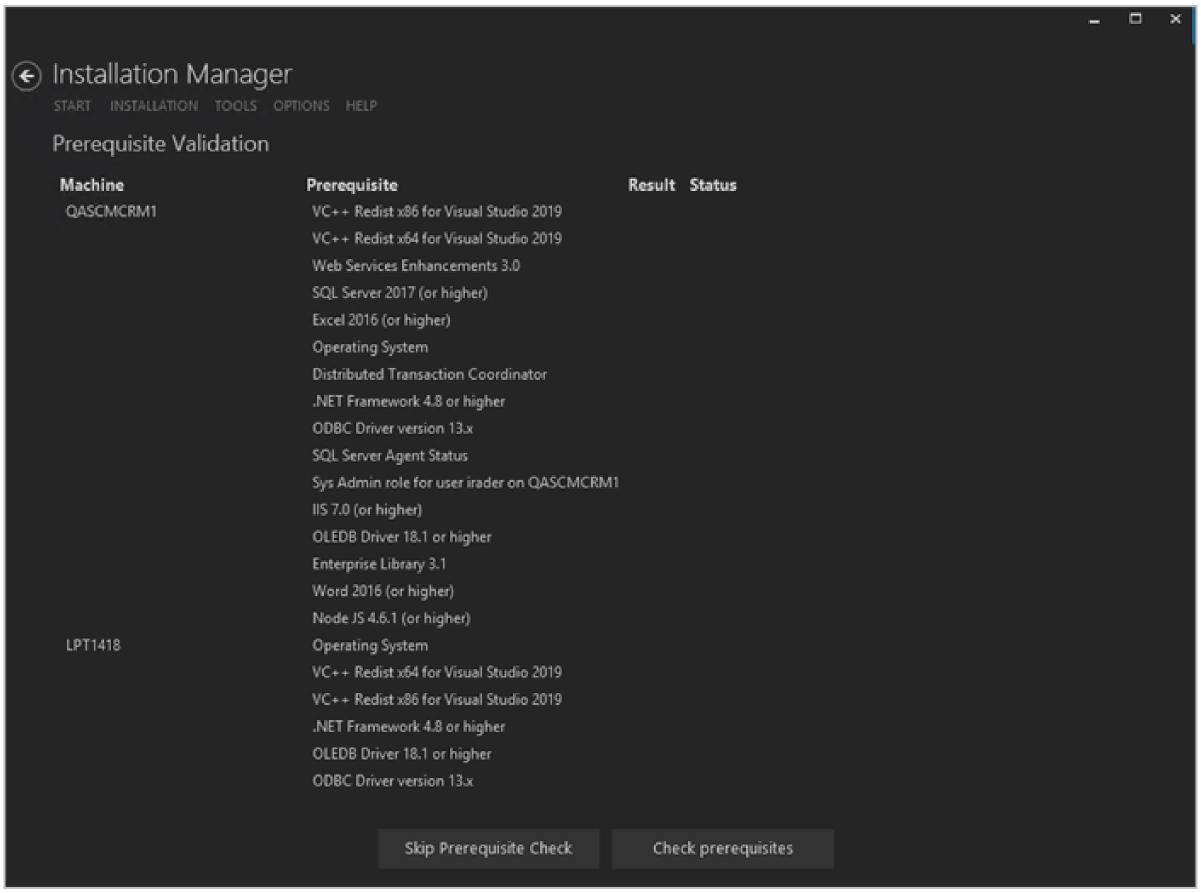
> ⚠ The Cmc.NexusCrm.Contracts.dll file must be copied to all the locations above whenever a property is added for any entity in CampusNexus CRM.

Review Configuration

The CampusNexus CRM installation supports multiple setup configurations depending upon the SQL instance, role of the server, and business needs. All of this information is displayed in the Review Configuration screen.

Review the Configuration and Start Installation

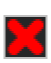
1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.



2. Review the configuration. Only unique machines are displayed; if multiple databases on one machine are noted in the Database Settings screen, the machine named on the screen is only shown once.

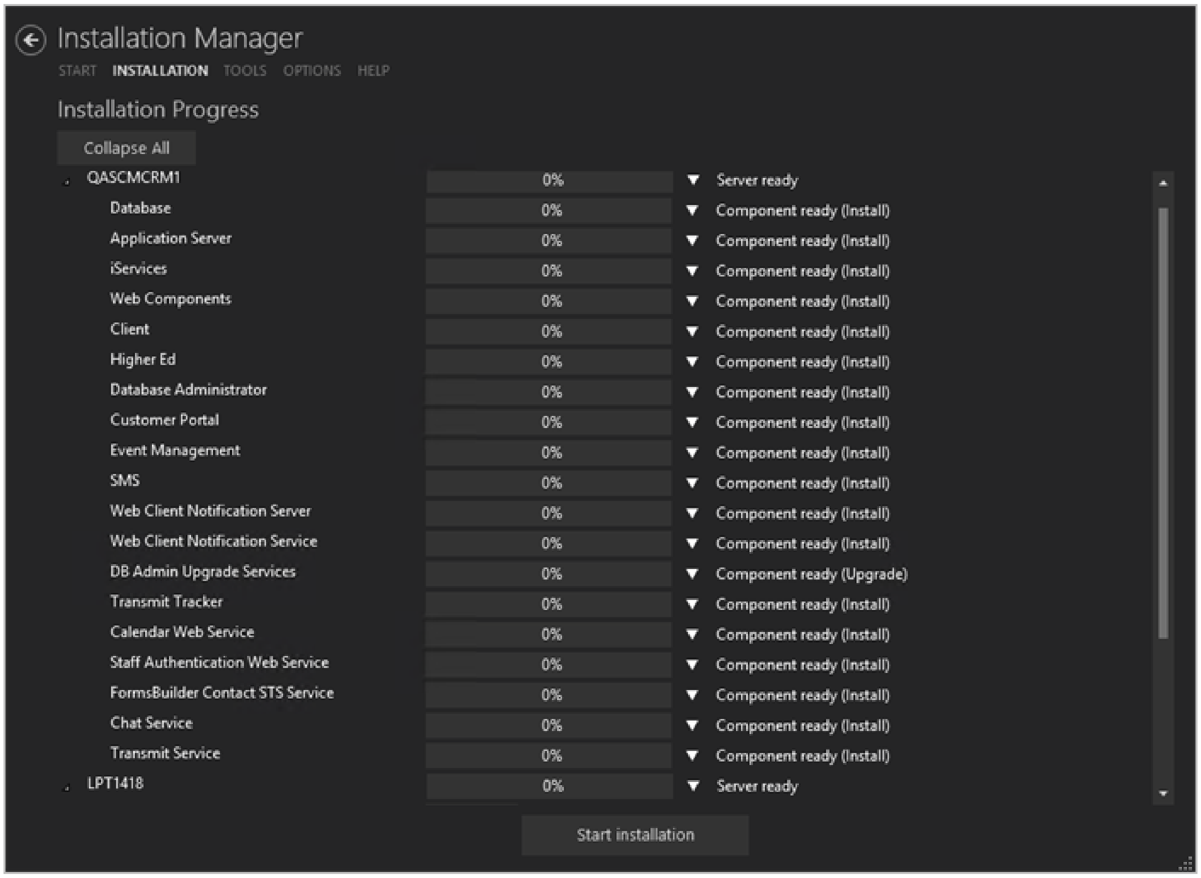
3. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

4. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.



5. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

6. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

7. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

   The log files are stored in the following location: `C:\Program Files\Common Files\Talisma Shared\SetupLog`

Upgrades

You can upgrade to CampusNexus CRM from earlier versions. Be sure to confirm that the upgrade path from one version to another is tested and certified.

Note: In CampusNexus CRM the *Talisma Server* is referred to as the *Database* component.

Before Upgrading

1. Ensure that your current environment meets the minimum hardware and software requirements as specified in Minimum System Requirements.
2. The Data Management Utility cannot be upgraded from earlier versions and must be installed afresh after uninstalling earlier versions.
3. Ensure that all CampusNexus CRM Services are stopped before you start the upgrade process.
4. Uninstall and reinstall the MSDTC service on the computer where you plan to install the Database component. To do so:
    a. Log on as the administrator of the computer.
    b. Open the command prompt and run the **MSDTC -uninstall** command.
    c. Type **Services.msc** in the Run dialog box. The Services screen is displayed.
    d. Ensure that the **Distributed Transaction Coordinator** service is removed from the list.
    e. Restart the computer.
    f. Open the command prompt and run the **MSDTC -install** command.
    g. In Services.msc, set the **Startup type** for the **Distributed Transaction Coordinator** service to **Automatic**.
5. If the Subscriber databases (Analytics/Media/WebTrak) are installed on different servers, run the upgrade process individually on every server for all Subscriber DB Servers.
6. Ensure that all users have logged off from the Database component prior to the upgrade process. In addition, ensure that you have taken a backup of all Server components, and that all the servers on which components are installed conform to the minimum system requirements.
7. The Database, Subscriber databases, and Archive upgrade must be performed only after you ensure that replication has been configured, and is running properly. Otherwise, the upgrade process will fail.
8. Ensure that all the steps of **Talisma-Media-CustomScript** Job are completed successfully before you start the upgrade process.

9. Ensure that the SQLServerAgent Service is not running during the upgrade process. In a distributed server scenario, ensure that the SQLServerAgent Service is stopped on all the servers.
10. Ensure that all the Services are running under the same domain User Account on all computers.
11. 'Log On As' should not be under the Local System Account for these Services.
12. If Database or Archive is installed on a named instance of Microsoft SQL, ensure that the related MS SQL Services are running.
13. Upgrade Application Servers before upgrading Web Components. If you upgrade Web Components before upgrading Application Servers, information relating to Web Servers is not updated in the relevant databases.
14. Set the value of Linked Servers, Data Access option to True. To do so:
    a. Navigate to **Microsoft SQL Management Studio**, open **Server Objects**, and select **Linked Servers**.
    b. Select **Properties** from the shortcut menu. The Linked Server Properties screen is displayed.
    c. Click **Server Options** in the left pane.
    d. In the right pane, ensure that the value of the **Data Access** option is set to **True**.
    e. Perform steps a through d for all Linked Servers.
15. For the following databases, ensure that you run the indicated scripts. They can be run before upgrading or attaching the database, or at any time after the databases are upgraded.

Database	Script
Archive	PreSetup_Archive.sql
Media	PreSetup.Chat.sql
Main	PreSetup.Main.sql
Analytics	PreSetup.Reports.sql

The scripts are available in the Scripts folder on the Anthology Inc. FTP site.

Notes:

- Before running the scripts, ensure that SQL Server Agent is stopped on the database computers.
- The scripts may take a long time to run depending on the size of the databases or the number of index entries in specific tables.
- Run the scripts only once when upgrading from any version to the current version. If they were run when the databases were previously upgraded, it is not required to run the scripts again.

- Any customizations on the Target ID column need to be updated to use the BIGINT data type to support a bigger range of values in the Target ID column.
- To resolve issues that occur in custom views or relationships of the Target object created in a previous version, see the Troubleshooting Tips section of Administrator Help.

16. For enhanced Mailer Tab performance in the Web Client, run the following code snippet in the Main Database. It can be run before upgrading or attaching Main database, or at any time after the database is upgraded:

```
IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'IX_tblOBMReportMailer_nOBMailerID_nTargetID' AND object_id = OBJECT_ID('tblOBMReportMailer'))
BEGIN
    CREATE INDEX IX_tblOBMReportMailer_nOBMailerID_nTargetID ON tblOBMReportMailer (nOBMailerID, nTargetID )
    INCLUDE (nSentStatus, dtDateOfAction, nBounceType)
END
GO
```

Notes:

- Before running the code snippet, ensure that SQL Server Agent is stopped on the Main database computer.
- The code may take a long time to run depending on the number of rows in the tblOBMReportMailer table.

17. If you are upgrading Main Database, run the following script if Higher Ed is installed:

```
CREATE NONCLUSTERED INDEX [IX_tblObjectType20005_bDeleted_nMergedWithID_aID_nTeamID_tName]
ON [dbo].[tblObjectType20005] ([bDeleted],[nMergedWithID],[aID],[nTeamID])
INCLUDE ([tName])
GO
```

Notes:

- Before running the script, ensure that SQL Server Agent is stopped on the Main database computer.
- The script may take a long time to run depending on the number of rows in the tblObjectType20005 table.

18. If your institution uses the Campaign module, run the following scripts on the Main database computer before upgrading or attaching the database or after it is upgraded:

- Create_clustered_index_on_tblOBMReportMailer.sql
- Create_clustered_index_on_tblCampaignTarget.sql
- Create_clustered_index_on_tblTargetHistory.sql

Running these scripts improves the performance of campaign processing.

Note:

Before running the script:

- Ensure that SQL Server Agent is stopped on the Main database computer.
- Campaign Dispatcher Services are stopped.

19. It's recommended to run the following index script on Main database to avoid deadlocks while processing campaigns:

```
IF EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = N'IDX_tblCampaignTarget_nPre-
viousElementID')
BEGIN
    DROP INDEX IDX_tblCampaignTarget_nPreviousElementID ON tblCampaignTarget
END
GO

CREATE NONCLUSTERED INDEX [IDX_tblCampaignTarget_nPreviousElementID] ON [dbo].[tblCam-
paignTarget] ([nPreviousElementID])
INCLUDE ([bMoved])
GO
```

Notes:

- Before running the script, ensure that SQL Server Agent is stopped on the database computers.
- The scripts may take a long time to run depending on the size of the databases or the number of index entries in specific tables.
- Run the scripts only once when upgrading from any version to the current version. If they were run when the databases were previously upgraded, it is not required to run the scripts again.

20. To improve CTI performance in Web Client, it's recommended to run the following scripts before upgrading or attaching the following databases or after they are upgraded:

- **Create_clustered_index_on_tblRequest_Main.sql** - On the Main database computer
- **Create_clustered_index_on_tblRequest_Media.sql** – On the Media database computer

Apply the following index script on each of the above computers. If both databases are installed on the same computer, apply the index only once.

```
IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'tblSessionParticipants_nUserID_
nStatus')
BEGIN
    CREATE NONCLUSTERED INDEX [tblSessionParticipants_nUserID_nStatus]
    ON [dbo].[tblSessionParticipants] ([nUserID],[nStatus])
    INCLUDE ([nRequestID])
END
```

The above script will be available in the Scripts folder on the Anthology Inc. FTP site.

Note: The Notes of the previous step also apply to this step.

21. It's recommended to apply the following index script on the Main database if campaigns include the Create Object step. The script will improve any slowness that may occur in campaign processing and in the overall system due to high data volumes in the tblCampaignCreatedObjects table.

    Run the script before upgrading or attaching the Main database, or at any time after the database is upgraded:

```
IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'PK_tblCampaignCreatedObjects')
BEGIN
    ALTER TABLE dbo.tblCampaignCreatedObjects
    ADD CONSTRAINT PK_tblCampaignCreatedObjects PRIMARY KEY CLUSTERED (aID ASC)
END
GO

IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'IX_tblCampaignCreatedObjects_nTar-
getID_nObjectType_nPropID_nBaseObjectType')
BEGIN
    CREATE NONCLUSTERED INDEX [IX_tblCampaignCreatedObjects_nTargetID_nObjectType_
nPropID_nBaseObjectType]
    ON [dbo].[tblCampaignCreatedObjects] ([nTargetID],[nObjectType],[nPropID], [nBaseObjectType])
END
GO
```

    Notes:

    - Before running the script, ensure that SQL Server Agent is stopped on the database computers.
    - The script may take a long time to run depending on the number of rows in the tblCampaignCreatedObjects table.

22. It's recommended to run the following index script on the Main database to avoid slowness of operations in Desktop and Web Client due to data growth in the tblCampCommTargetMergeValueResultSet table:

```
IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = N'IX_tblCampCom-
mTargetMergeValueResultSet_nTargetBatchResultSetID')
BEGIN
    CREATE INDEX IX_tblCampCommTargetMergeValueResultSet_nTargetBatchResultSetID
    ON dbo.tblCampCommTargetMergeValueResultSet (nTargetBatchResultSetID)
END
GO
```

23. Run the following index scripts on the Main database to prevent SMS dispatchers from occasionally switching to a hung state:

```
IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'IX_tblObjectType20042_nCom-
municationType_nTargetID_nElementID')
BEGIN
    CREATE NONCLUSTERED INDEX [IX_tblObjectType20042_nCommunicationType_nTargetID_nEle-
mentID]
    ON [dbo].[tblObjectType20042] ([nCommunicationType],[nTargetID],[nElementID])
    INCLUDE ([aID],[nDeliveredStatus],[nStatus])
END
GO

IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'IX_tblOutboundSMS_nCampaignID_
nTargetID_nCustID')
BEGIN
    CREATE NONCLUSTERED INDEX [IX_tblOutboundSMS_nCampaignID_nTargetID_nCustID]
    ON tblOutboundSMS ([nCampaignID], [nTargetID], [nCustID])
    INCLUDE ([aSMSMessageID])
END
GO

IF NOT EXISTS(SELECT TOP 1 1 FROM sys.indexes WHERE name = 'IX_tblSMSDetails_nMsgId')
BEGIN
    CREATE NONCLUSTERED INDEX [IX_tblSMSDetails_nMsgId]
    ON tblSMSDetails (nMsgId)
END
GO
```

24. Apply the following scripts on the Main Database computer. They will improve any slowness in Business Administrator performance during rule modification. Additionally, the rule log clean-up process is optimized, and the maximum limit for deleting rule log records is increased:

- Create_clustered_index_on_tblActionTrace_Main.sql
- Create_clustered_index_on_tblRuleTrace_Main.sql
- Create_clustered_index_on_tblConditionTrace_Main.sql

The above scripts are available in the Scripts folder on the Anthology Inc. FTP site.

Note:

- Before running the scripts, ensure that SQL Server Agent is stopped on the Main database computer.
- The scripts may take a long time to run depending on the size of Main database or the number of index entries in specific tables.
- Run the scripts only once when upgrading to the current version. If they were run when Main database was previously upgraded, it’s not required to run the scripts again.

Upgrade to CampusNexus CRM

Perform the steps described in this procedure if you are upgrading to CampusNexus CRM from a version prior to Talisma 9.2.

To upgrade to CampusNexus CRM, follow this sequence:

1. Stop the SQLServerAgent Service. In a distributed server scenario, ensure that the SQLServerAgent Service is stopped on all servers.
2. If you are using Print Templates, upgrade Print Templates before upgrading the Database component.
3. Upgrade to CampusNexus CRM Database. Upgrade the Main database before upgrading the Subscriber database on a distributed environment.
4. Check the error log file to ensure that the upgrade is successful. This file is located in the **<Drive name>:\Program Files\Common Files\Talisma Shared\Setuplog\<database name>\dbupdatelog** folder on your computer. Check all output files in the **dbupdatelog** folder for errors.
5. Check the Setup log files. These files are located in the **<Drive name>:\Program Files\Common Files\Talisma Shared\Setuplog\<database name>** folder on your computer.
6. Upgrade Application Server.
7. Upgrade all other CampusNexus CRM components.
8. If the Database component and CRM Services are installed on the same computer, upgrade the CRM Services by running the **ServiceUpgrade** setup.
9. After the upgrade process, ensure that all computers are restarted.

Notes:

If you upgrade Web Components, the following error message is displayed when users log on to Business Administrator:

The directory '/bizadmin/App_GlobalResources/' is not allowed because the application is precompiled.

Solution: Navigate to the path **<Drive name>:\Program Files\Talisma Web Components\BusinessAdministrator** on the Web Components computer and delete the **precompiledapp.config** file.

This step is not required if you upgrade from a fresh 9.X installation.

Upgrade the Database Component

This section describes the procedure to the Database component in a distributed server scenario.

Example

The Database component is installed on two different computers with Main database on one computer (A) and Distributor, Analytics, Media, and WebTrak databases on another computer (B).

Before upgrading the Database component, perform the steps described in the following procedures:

Run the Sproc_GetRulesAndCampaignWithFireEvent.sql Script

The following features are deprecated in CampusNexus CRM:

- The **Fire external action** option in the **Automatic Step** and **Manual Task** Campaign Actions in Client
- The **Fire Event <Text>** action in rules in Business Administrator

Perform the following steps before upgrading to CampusNexus CRM:

1. Run the **Sproc_GetRulesAndCampaignWithFireEvent.sql** script on the computer where the Main database is available.

   It lists campaigns in which the **Fire external action** option is selected and rules in which the **Fire Event <Text>** action is included.

2. Use the information to clear the following:

   - In Client – Clear the **Fire external action** option in the **Automatic Step** and **Manual Task** Campaign actions.
   - In Business Administrator – Delete the **Fire Event <Text>** action in rules.

   Review and modify business flows of the affected campaigns and rules, if required.

   The script is available in the path Scripts\Sproc_GetRulesAndCampaignWithFireEvent.sql.

Notes:

If the script is not run, and the deprecated Campaign and Rule features are in use when you upgrade the Main database, the upgrade process aborts and the following content is logged in the TLSetupDBErrors_<Date>_<Time>.log file:

Following Rules are associated with FireEvent Action Type:<<*Rule name*>>

Following Campaigns Steps are associated with FireExternalEvent Option:<<*Campaign name*>>-<<*Step name*>>

Use the information in the log file to clear Campaign and Rule settings as described in step 2 above.

Upgrade the Database

After upgrading the database Component in a distributed environment, depending on the permission of the SQL Login of the User who performed the upgrade operation, the option in the Linked Server Properties dialog box for the Publisher and Subscriber databases is set to the following:

- **Be made using the login's current security context** - If the SQL Login has the sysadmin Role.
- **Not be made** - If the SQL Login does not have the sysadmin Role.

The recommended option to be set in the Linked Server Properties dialog box is **Be made using the login’s current security context**. However, if you want to further tighten the security for connecting with the linked servers, you can select the **Not be made** option. When this option is selected, even if the user has sysadmin permission, the user will not be able to access the databases of the Linked Server. The user must be explicitly mapped to the appropriate users in the **Local server login to remote server login mappings** area to perform the required operations.

For example, to run a CampusNexus CRM installer, the user must be added as a Local Login in the **Local server login to remote server login mappings** area and the Remote User must be a SQL Login that has SQL Server Authentication with sysadmin permission on all the Subscriber databases.

Impact of Upgrading the Database

Perform the steps described in this procedure if you are upgrading to CampusNexus CRM from a version prior to Talisma 9.2.

Note: In a scenario where you want to upgrade the Database component prior to Talisma 9.2 version, and install databases of multiple customers on a single SQL Server instance, you must first detach any previous versions of databases and then install the Database component afresh by attaching the databases. Databases of multiple customers can then be attached or installed afresh on the same SQL Server instance.

When you upgrade a previous version of the Database component, the following changes are reflected:

Consider a scenario where a single CampusNexus CRM database named **tlmain** is upgraded to CampusNexus CRM. The name of the customer is **tlmain**.

- While upgrading the Database component using the Installation Manager, specify the name of the Main database, for example, **tlmain**.
- When the upgrade process is completed successfully:
    - A folder named **tlmain** is created under Talisma Shared folder.
    - All files related to Database Administrator will be removed from Talisma Shared and Talisma Server folders. You must install Database Administrator afresh using Installation Manager. It is recommended to install Database Administrator on the computer where you want to create the CRM Services.
    - Registry key folder is suffixed by the database name.
- When you run the Database setup, only the Database component will be upgraded. To upgrade CRM Services, you must run the CRM Services Upgrade setup. This procedure is applicable if the Database component and CRM Services are available on the same computer or multiple computers.
    - The Job Service and Campaign Dispatcher services will continue to remain as is. You must run the CRM Services Upgrade setup to upgrade these services.
    - The Offline Sync and HealthCheck Services will be deleted. You must use Database Administrator to create Webform Sync (previously known as Offline Sync Service) and HealthCheck Services.
    - The Notification Service will be deleted; however, the Notification feature will continue to function as is. You can change the Notification frequency using the Global Options in Business Administrator.
    - In addition, Scheduled Report (TLRptXL.exe) will be removed. You can create this service using Database Administrator on any computer.

CRM Patches

Properly installing the Installation Manager CRM Patches module using default settings helps reduce potential issues when performing upgrades of the CampusNexus CRM product.

Important: Ensure that Installation Manager is installed on the same machine where the previous version of Installation Manager was installed and configured.

Prerequisites

Before installing CampusNexus CRM patches, the following conditions must exist:

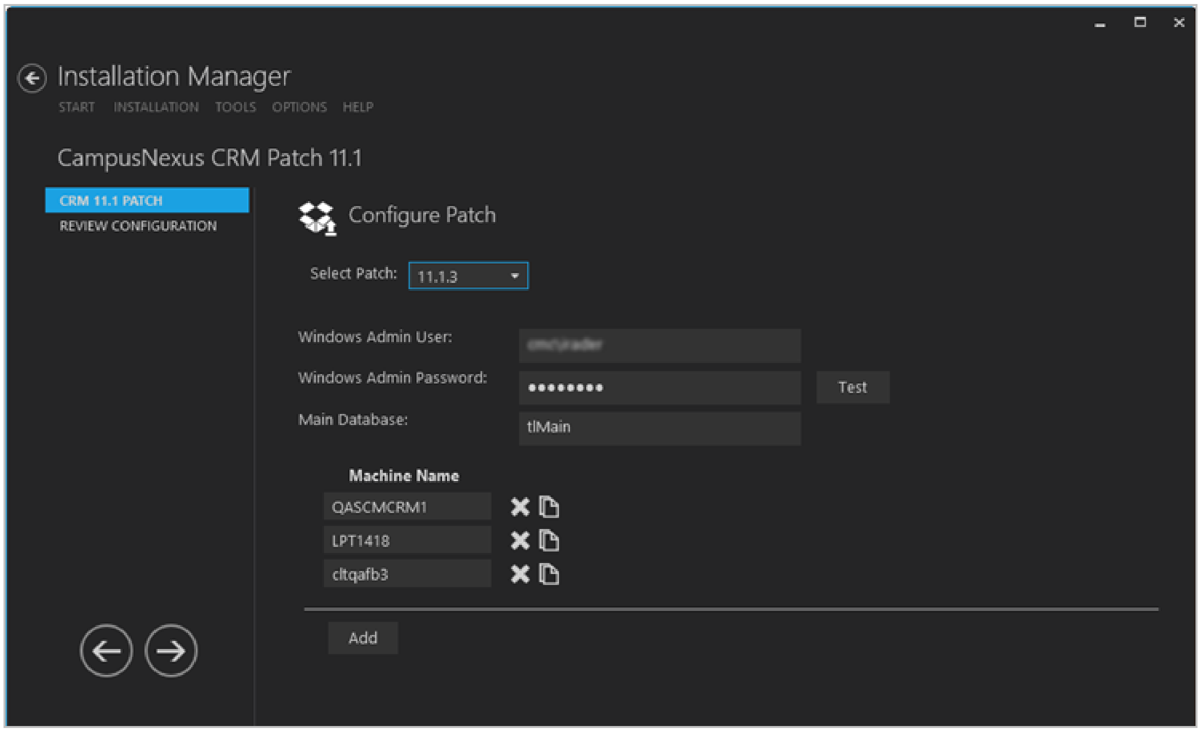
- All users are logged off from CampusNexus CRM.
- The Windows NT user account has administrator permission to the Database.
- The SQL Server Service is running.
- The SQL Server Agent is stopped.
- All CampusNexus CRM services are stopped.

Important: Users do not have to delete any files or folders before installing a new version, but they will have to access the Installation Manager and add any new machine names and associate them with the Windows User Name and Password for them to be installed properly.

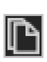
Configure Patch

After you have downloaded the CampusNexus CRM using Package Manager, the Start screen of Installation Manager displays a tile for the downloaded patch. The patch tile links to the Configure Patch screen used to specify patch installation settings.

1. In the Start screen of Installation Manager, click the **CampusNexus CRM Patch <Version>** tile. The Configure Patch screen is displayed.



2. From the **Select Patch** list, choose the patch version.
3. In the **Windows Admin User** field, specify a user name with Administrator permissions on the computer on which the installation will occur, as well as the local machine. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
4. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.
5. In the **Main Database** field, specify the name of the Main Database.

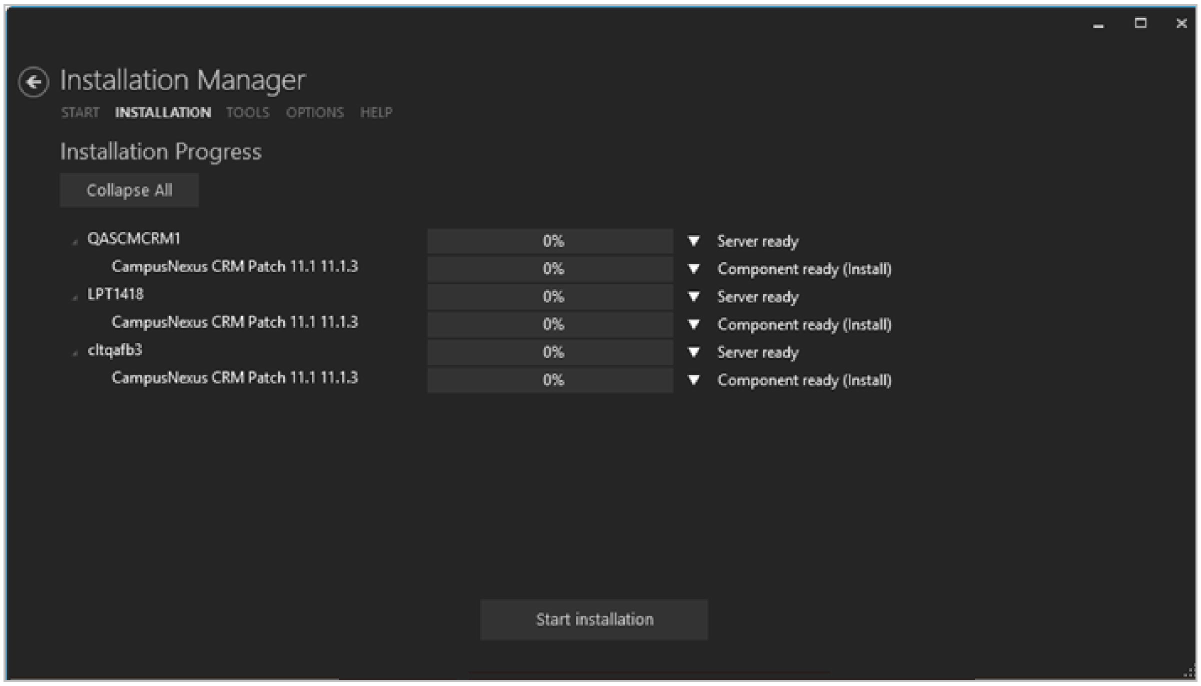
   Note: The Machine Name fields on this form are populated with information entered in a previous installation.
6. Click **Add** to add a line to the Settings screen.
7. Enter the **Machine Name** for the component to be installed.
8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.
10. Click **Review Configuration**.

Review Configuration

CampusNexus CRM Patch installation requires multiple setup configurations depending upon the SQL instance, role of the server, and business needs. All of this information is reviewed from the Review Configuration screen.

Review the Configuration and Start Installation

1. Once the Configure Patch screen has been populated, click **Review Configuration** to see all of the information in one screen.



2. Click **Start Installation** and review the installation process for each machine.

3. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

   The log files are stored in the following location: `C:\Program Files\Common Files\Talisma Shared\SetupLog`

Network Environment

The following topics provide instructions related to the network environment.

Security Settings

Various COM and DCOM applications, and Windows services are used in CampusNexus CRM. Users must be given access to these components in addition to permissions to other files and folders accessed by CampusNexus CRM.

Database Servers

The MSSQL Server Service, and MSSQL Server Agent on all CampusNexus CRM Database Servers must run using a single Domain account which is a member of the Windows Administrators group, and the **SysAdmin** SQL Server role. By default, the **TalismaAdmin** user is the owner for all CampusNexus CRM Jobs.

The following table describes the roles required for the various CampusNexus CRM user accounts.

CampusNexus CRM User Accounts

Account Name	Security Type	SQL Server Role	Database Role for each database
Talisma Admin	Application	SysAdmin	• Master: public • MSDB: public, TargetServersRole • DBs: public, db_owner
Windows User under which CampusNexus CRM is installed	Trusted	SysAdmin	• Master: public • MSDB: public, TargetServersRole • DBs: public, db_owner
Talisma Internal Account (Name = Talisma<License>)	Application	None	• Master: public • MSDB: public, TargetServersRole • DBs: public, db_owner
Talisma Internal Account (Name = Talisma<GUID>)	Application	None	• Main • Database: public

Account Name	Security Type	SQL Server Role	Database Role for each database
Data Import Account (Name = TalismaDSN)	Application	SysAdmin	• Master: public • MSDB: public, TargetServersRole • DBs: public, db_owner

CRM Services

The following table lists the accounts that must be used to log on to the respective CRM Services.

CRM Services Accounts

Service Name	Log On Credentials
Job Service	Domain Account
Campaign Dispatcher	Domain Account and SQL Server User
Health Check Service	Domain Account
Webform Sync Service	Domain Account
Scheduled Report Service	Domain Account

Notes:

The following components on the Scheduled Report Service computer must also work in the same domain account as the service:

- TlRptToFile
- Microsoft Excel Application

If a service is managed remotely using Database Administrator, the service must run using the Administrator account.

Application Server Service

The Application Server service is configured to run under the Interactive User account, which requires the user to be logged on to the computer on which Application Server is installed.

You can also configure the Application Server service to run under a Domain account. To do so:

1. From the **Start** menu of the Application Server computer, select **Settings**, **Control Panel**. The Control Panel is displayed.
2. Double-click the **Administrative Tools** icon. The Administrative Tools screen is displayed.
3. Double-click the shortcut for **Component Services**. The Component Services screen is displayed.

4. Expand the following nodes: **Component Services**, **Computers**, **My Computer**, and **COM+ Applications**. All COM+ applications are listed.
5. Right-click the **Application Server** component, and select **Properties** from the shortcut menu. The COM+ Application Server Properties dialog box is displayed.
6. Select the **Identity** tab.
7. In the **Account** area, select the **This user** option, and click **Browse** to locate a user who has administrative privileges on the Application Server computer.
8. Specify a password for the user in the **Password** field.
9. Type the password again in the **Confirm Password** field.
10. Click **OK**. Application Server is now configured to run using a Local Administrator account.

Notes:

- The Domain User must have the **Launch**, and **Access** permissions.
- The CampusNexus CRM Information Server DCOM Application must have **Launch**, and **Access** permissions.

Web Servers

The following table lists the permissions, and user accounts that must be configured using IIS Manager for the various CampusNexus CRM virtual directories.

CampusNexus CRM Virtual Directories

Virtual Root Name	Directory Security	Permission
Business Administrator	Read Execute: Scripts, and Executables	Anonymous access, mapped to a guest account.
Media Web Server		
WebTrak Web Server		
Media Upload Virtual Root		
Scripting		
Web Client		

Notes:

- It is recommended that you use SQL Roles with Windows users or groups added to the role. However, the following accounts use local groups:
  - Talisma Admin
  - Windows User under which CampusNexus CRM is installed
  - Talisma Internal Account (Name = Talisma<License>)

- While no other account must have **dbo** access, the **SQL dbo** must have access to all database objects. The Talisma internal account has **SQL dbo** access.
- For the **Scripting** virtual directory, type a Windows NT user name and password. This user must have access to the Main Database.

Cluster Server Environment

CampusNexus CRM can be installed and configured in a Cluster Server environment. For detailed instructions follow the links below.

Preinstallation Tasks

Perform the following steps on the computer where you want to install the Cluster Server:

1. Configure Microsoft (MS) Cluster Server in an Active-Passive cluster environment (2-node cluster).
2. Install Microsoft SQL Server using the **New SQL Server Failover Cluster Installation** option (single-node) on Cluster Node 1 computer using SQL Server Setup.
3. Install Microsoft SQL Server using the **Add node to a SQL Server Failover Cluster** option on Cluster Node 2 using SQL Server Setup.
4. Provide the SQL Server Network name and Cluster Network IP address during the installation of Microsoft SQL Server.
5. Provide the path of the Cluster Disk for the target and backup folders of the CampusNexus CRM Database component during installation.

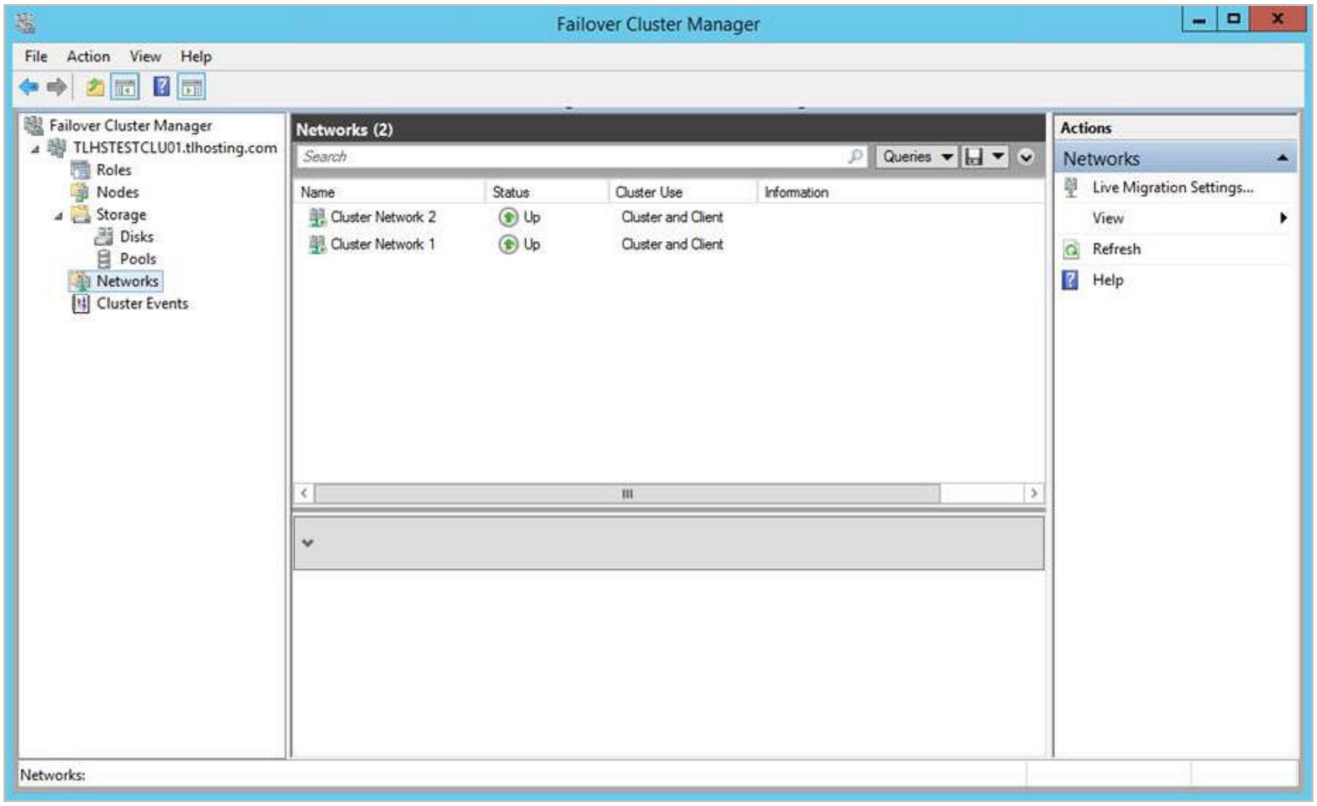
Note: The Primary Cluster Node on MS Cluster Server owns all Cluster Resources.

For more information, see http://technet.microsoft.com/en-us/library/dn505754.aspx and http://technet.microsoft.com/en-in/library/hh231721(v=sql.110).aspx.

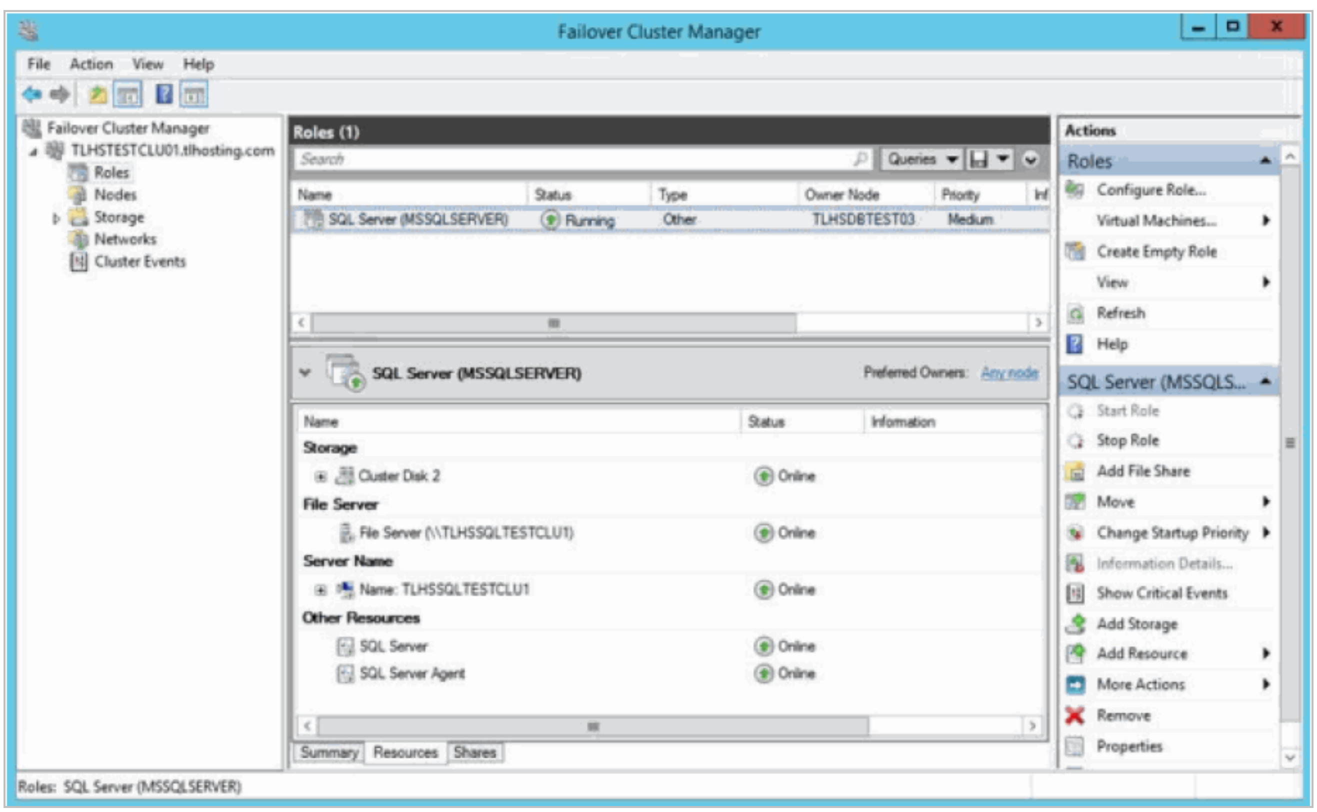
Open and View the Failover Cluster Manager

To open the Failover Cluster Manager and view the details, perform the following steps:

1. From the **Start** menu, open **Failover Cluster Manager**. The Failover Cluster Manager is displayed.
2. Click **<Virtual Cluster Name>.<Domain Name>.com\Networks** in the left pane to view the network details.



3. Click **<Virtual Cluster Name>.<Domain Name>.com\Roles** in the left pane to view details of the Roles.



Install and Configure CampusNexus CRM

Note: In the testing environment, Application Server, Client, and Data Management Utility are installed outside the Cluster environment.

To install CampusNexus CRM, perform the following steps:

1. Install the Main database, Distributor database, and all Subscriber databases on the Primary Node of MS Cluster Server.
2. Provide the path of the Cluster Disk for the target and backup folders of the Database component during installation.
3. Restart the Primary Cluster Node.
4. Ensure that all Cluster Resources are assigned to the Primary Node after the computer is restarted.
5. Install Application Server on a computer that is outside the Cluster environment.
6. Install all CampusNexus CRM components across multiple computers outside the Cluster Server.

Notes:

- It is not mandatory to install Distributor and Subscriber databases in a clustered environment.
- Every time the Primary Cluster Node is restarted, it is mandatory to assign all Cluster Resources to the Primary Cluster Node.

To configure CampusNexus CRM on the Secondary Cluster Node, perform the following steps:

1. Shut down the active Cluster Node.
2. Enter the Failover Node on the Cluster Node field and then install.

Notes:

- Ensure that the registry information on the Primary Cluster and Secondary Cluster Nodes is identical.
- The installation of the Failover Node needs to be done after the installation of all other CampusNexus CRM components is completed.

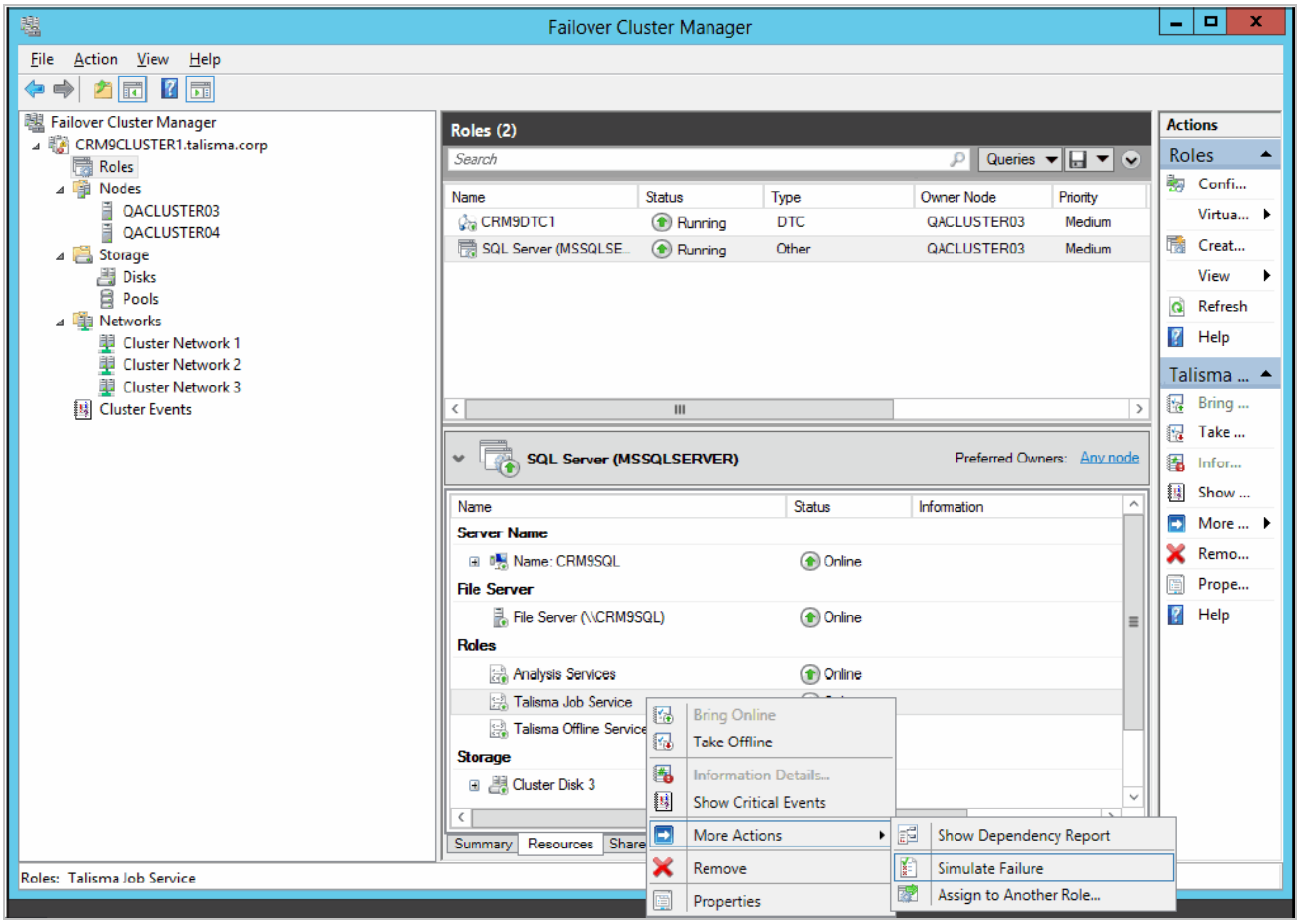
Simulate a Resource Failure

You can simulate the failure of a Resource and verify its status on the Primary Cluster Node. Further, you can verify if the failed Resource starts automatically on the Secondary Cluster Node.

To simulate the failure of a service, perform the following steps:

1. Open the Failover Cluster Manager on the Primary Cluster Node. For steps to open the Failover Cluster Manager, see Open and View the Failover Cluster Manager. All available Resources are displayed in the right pane.

2. Right-click a Resource and select **More Actions**, **Simulate failure of this resource**.



Optimize CampusNexus CRM

- Ensure that sufficient free space is available on the temporary database.
- Ensure that the transaction Log and data files are stored on different drives.
- It is recommended that you do not configure all databases on the same computer.
- Minimize heuristic threading when configuring an Alias.
- Schedule the Extractor/Dispatcher jobs to ensure that the jobs do not start simultaneously. In addition, you can configure the Extractor and Dispatcher jobs to run every 30 minutes instead of every 5 minutes. Since the mail delivery takes place over the Internet, an Asynchronous medium, the 30-minute delay is acceptable.
- Minimize the usage of message text-based search in Rules and the Advanced Query Builder.
- Switch off diagnostics on the server. Since the trace file is not thread-safe, it is known to cause exceptions.
- Disable the Archive job to stop archiving of Interactions.
- When working on a Terminal Server, log off from CampusNexus CRM on completion of your work, instead of disconnecting.
- Configure the backup drive as a network drive. This improves disk throughput. In addition, you can restore the system in the event of the hard disk crashing.
- Depending on the load on the CampusNexus CRM system, determine the job schedule time for full backup, and the maintenance and transaction log backups.

Tips on Optimal Use of Rules

- Create filters based on subject line, instead of the message.

  If a rule contains a filter comprising multiple search conditions that use the same “search in message” condition, ensure that the “search in message” condition is defined separately to improve the performance.

  For example, if a rule has been created as:

  When new Interaction is created
  If MessageContent contains “support escalation” and MessageCustomProp = “Product1” Then Set CustomProp = “Product A”
  If MessageContent contains “support escalation” and MessageCustomProp = “Product2” Then Set CustomProp = “ProductB”

  To optimize the performance, you can define the above rule as:

  If MessageContent does not contain “support escalation”
  Exit current rule

If MessageCustomProp = “Product1” Then
Set CustomProp = “Product A”
If MessageCustomProp = “Product2” Then
Set CustomProp = “Product B”

Note: Any “Contains” search must follow the guidelines given in this section.

Windows Server Configurations

Perform the following Windows Server specific configurations for CampusNexus CRM components.

Configure the Database Component

If Database is installed in a distributed environment, perform the following procedures on all the distributed computers.

Configuring MSDTC Settings

1. From the **Start** menu, select **Run**.
2. Type **dcomcnfg**. The Component Services screen is displayed.
3. Browse to **Console Root**, **Component Services**, **Computers**, **My Computer**, Distributed Transaction Coordinator, Local DTC.
4. Right-click **Local DTC** and select **Properties**. The Local DTC Properties dialog box is displayed.
5. Click the **Security** tab.
6. Select the **Network DTC Access** option.
   a. Select **Allow Remote Clients**.
   b. Select **Allow Remote Administration**.
7. In the Transaction Manager Communication area, select the following options:
   - **Allow Inbound**
   - **Allow Outbound**
   - **No Authentication Required**
   - **Enable XA Transactions**
   - **Enable SNA LU 6.2 Transactions**
8. Click **OK**.

Configure RPC Security for MSDTC

Perform the following steps on Windows computers where CampusNexus CRM databases are hosted.

1. Open the Registry editor on the computers where CampusNexus CRM databases are hosted.
2. Navigate to the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC.
3. On the **Edit** menu, click **New**, **DWORD Value**, and create a new value called **TurnOffRpcSecurity**, and set its value to **1**.

Configure Web Components

On the Windows Server computer where any or all the Web Components are installed, perform the following steps:

1. From the **Start** menu, select **Run**.
2. Type **inetmgr**. The Internet Information Services (IIS) Manager is displayed.
3. Ensure that all the virtual roots configured for Web Components are configured with a valid Windows user as the Anonymous User. To do so:
   a. For every virtual root, select **Basic Settings** from the right pane. The Edit Site dialog box is displayed.
   b. Click **Connect as, Specific user, Set** and set the domain user credentials in the Set Credentials dialog box.
4. Configure the identity account for the Application Pool under which the Web Components are running. To do so:
   a. In the right pane, click **Advanced Settings**. The Advanced Settings dialog box is displayed.
   b. Navigate to the **Process Model** area and click the ellipsis in the Identity field. The Application Pool Identity dialog box is displayed.
   c. Select the **Custom account** option and click **Set**.
   d. In the Set Credentials dialog box, specify the domain user account details.
   e. Click **OK**.
5. Ensure that the **Allow**ed option is enabled for all the ISAPI and CGI Extensions. To do so:
   a. Select the Web server node in the IIS Manager.
   b. In the right pane, double-click **ISAPI and CGI Restrictions**.
   c. Ensure that the **Allow**ed option is enabled for all the ISAPI and CGI Extensions.
   d. For both the **ASP.NET v4.0.30319** extensions, click the **Edit Feature Settings** link.
   e. In the Edit ISAPI and CGI Restrictions dialog box, ensure that the two check boxes are selected and click **OK**.

Configure Job Service Framework and Application Server

Grant remote access permission to Domain Users on Windows computers where Job Services Framework (JSF), and Application Server are installed.

1. From the **Start** menu, select **Run**.
2. Type **dcomcnfg**. The Component Services screen is displayed.
3. Browse to **Console Root, Component Services, Computers, My Computer**.
4. Right-click on My Computer, and select **Properties**. The My Computer Properties dialog box is displayed.
5. In the COM Security tab, click **Edit Limits** in the Access Permissions area.
6. In the Access Permissions dialog box, select the Distributed COM Users group, and select the **Allow** option for all the permissions.
7. Click **OK**.
8. In the Launch and Activation Permissions area, click **Edit Limits**.
9. In the Launch Permission dialog box, select the Distributed COM Users group, and select the **Allow** option for all the permissions.
10. Click through **OK** twice.
11. For Job Services Framework, browse to the **DCOM Config, TLSCMgr** node.

    — OR —

    For Application Server, browse to the **DCOM Config**, **Talisma Information Server** node
12. Right-click the node, and select **Properties**.
13. In the General tab, select the **Authentication Level** as Connect.
14. In the Security tab, select **Customize** in the Launch and Activation Permissions area, and click **Edit**.
15. In the Launch Permission dialog box, click **Add**.
16. Type **Everyone**, and click **OK**.
17. Select **Allow** for all the permissions.
18. Click **OK**.
19. In the Security tab, select **Customize** in the Access Permissions area, and click **Edit**.
20. In the Access Permission dialog box, click **Add**.
21. Type **Everyone**, and click **OK**.
22. Select **Allow** for all the permissions.
23. Click **OK**.
24. In the Identity tab, select **This user**, and configure a valid Domain User account.
25. If you have configured the Job Services Framework, restart the Job Services Framework.

— OR —

If you have configured the Talisma Application Server, restart Talisma Application Server.

Enable Permissions on the Application Server

Domain Users need to be given permissions on the Application Server computer. To do so:

1. On the Application Server computer, right-click the **My Computer** icon on the desktop, and select **Manage**. The Computer Management screen is displayed.
2. In the left pane, navigate to **System Tools**, **Local Users and Groups**, **Groups**. In the right pane, double-click **Distributed COM Users**. The Distributed COM Users Properties dialog box is displayed.
3. Click the **Add** button, and add the Users, or Groups who will be logging on to CampusNexus CRM.
4. Click through **OK** twice.
5. Close the Computer Management screen.

Configure the File Size for Compression

You can configure the file size for compression for Application Server and Client. By default, compression is disabled when connections to Application Server are made over a Local Area Network (LAN). To enable compression, follow these steps:

1. On the computer where Client is installed, run **Regedit** from the command prompt. The Registry Editor is displayed.
2. Browse to the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Talisma\Common\ConnectionParameters\LAN
3. Right-click the DWORD values Request and Response, and select **Modify** from the shortcut menu. The Edit DWORD Value dialog box is displayed.
4. Specify the required data size in the **Value data** field, after selecting **Decimal** in the **Base** area. Compression is enabled for DCOM connections. Requests and responses that are greater than or equal to the specified size are compressed.

Notes:

- By default, the value for the Request and Response DWORDs for the LAN key is **0**, indicating that compression is disabled. Setting a value greater than **0** enables compression.
- Values specified in the **Value data** field must be in bytes, indicating the file size for which compression must be enabled.

By default, data greater than or equal to 1024 bytes will be compressed when connections to Application Server are made over HTTP. You can modify this value. To do so:

1. Browse to the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Talisma\Common\ConnectionParameters\Internet

2. Modify the DWORD values Request and Response, and specify the required data size in the **Value data** field, after selecting **Decimal** in the **Base** area.

Install ASP.NET on Application Server

1. From the **Start** menu, select **Settings**, **Control Panel**. The Control Panel is displayed.
2. Double-click the **Add/Remove Programs** icon. The Add/Remove Programs wizard is displayed.
3. Click the **Add/Remove Windows Components** tab. The Windows Component wizard is displayed.
4. In the Components list, select **Application Server**.
5. Click **Details**.
6. Select **ASP.NET** from the **SubComponents of Application Server** list, and click **Details**.
7. Click **OK**.
8. Click **Next**.
9. When ASP.NET is installed, click **Finish**.

Configure the Imports on a 64-bit Computer

It is recommended to update the path of the **dtexec.exe** file to use the MS SQL Server folder for the Jobs created for Import Configurations.

1. Log on to Microsoft SQL Server as an administrator.
2. Expand the **SQL Server Agent** node.
3. Expand the **Jobs** node.
4. Double-click on the Job created for the existing Import Configuration. The Job Properties - <Job name> dialog box is displayed.
5. Click on the **Steps** node in the **Select a page** pane.
6. Double-click on the first **Step** in the **Job step list:** table. The Job Step Properties - <Job name> dialog box is displayed.
7. In the **Select a page** pane, click **General**.

8. In the **Command** area, update the path for the **dtexec.exe** file to the following:

   <System Drive>:\Program Files(x86)\Microsoft Sql Server\110\DTS\Binn

9. Click the **OK** button.
10. Repeat steps 4 through 9 for all the jobs of existing Import Configurations.

Log on to Web Components Using Custom Login

When Web Components are installed on a Windows Server computer with IIS, you must carry out the following steps to enable users to log on to Web Components using Custom security:

1. Create an application pool in IIS Manager. To do so:
   a. From the **Start** menu, point to **Programs**, **Administrative Tools**, and select **Internet Information Services (IIS) Manager**. The IIS Manager is displayed.
   b. In the left pane of IIS Manager, right-click the **Application Pools** node, and select **Add Application Pool**. The Add New Application Pool dialog box is displayed.
   c. In the **Application Name** field, specify a name for the new application pool. This name will be displayed under the **Application Pools** node in the IIS Manager.
   d. Click **OK**. The new application pool is created, and is displayed under the Application Pools node.
2. Set the security account for the newly created application pool as **Local System**. To do so:
   a. In the left pane of IIS Manager, expand the **Application Pools** node, and right-click the newly created application pool.
   b. Click **Advanced Settings** from the right pane. The Advanced Settings dialog box is displayed.
   c. Navigate to the **Process Model** area and click the ellipsis in the Identity field. The Application Pool Identity dialog box is displayed.
   d. Select the **Custom account** option and click **Set**.
   e. In the Set Credentials dialog box, specify the domain user account details.
   f. Click **OK**.
3. Set the newly created application pool in the Properties dialog box for all the virtual roots representing the Web Components. To do so:
   a. In the IIS Manager, expand the **Default Web Site** node under the **Web Sites** node in the left pane.
   b. Right-click the required virtual root, and click the **Basic Settings** link. The Edit Site dialog box is displayed.

c. Click **Connect as** and select the Specific user open and specify the Local User credentials in the Set Credentials dialog box.

d. Click **OK** twice.

Users will now be able to log on to Web Components using Custom security.

Allow Active Server Pages

If Active Server Pages (ASP) are not allowed on the computer where Web Components are installed on a Windows Server computer with IIS, the login page for Business Administrator and other Web Components will not be displayed.

Perform the following steps on the computer where Web Components are installed, to allow ASP pages:

1. From the **Start** menu, point to **Programs**, **Administrative Tools**, and select **Internet Information Services (IIS) Manager**. The IIS Manager is displayed.
2. In the left pane of IIS Manager, select the **<Computer name> (local computer)** node.
3. In the right pane of IIS Manager, double-click **ISAPI and CGI Restrictions**.
4. Ensure that **Active Server Pages** is set to **Allowed**. This operation adds the .asp extension to the list of allowed file extensions.

The login pages for the various Web Components are now displayed.

Domain Password Change

The CampusNexus CRM product is installed for a customer in different ways. In a scenario where CampusNexus CRM is installed on a network, the product works under a domain account, which is an administrator account on computers where CampusNexus CRM is installed. If the domain account password is changed, CampusNexus CRM will stop working as some of the CampusNexus CRM components run under the domain user account. A domain password change on the network does not change the password on these CampusNexus CRM installations. The installations have to be re-initialized by updating the password at several locations.

The following topics describe the configuration changes required for various CampusNexus CRM components when there is a domain password change:

Database Server Computers

SQL Server

Perform the following changes for all SQL services such as SQL Server Service, SQL Server Agent, SQL Server Browser, and SQL Server Integration Services on all computers where the Database component or CampusNexus CRM databases are installed:

1. Go to **Start**, **Administrative Tools**, **Services**. The Services screen is displayed.
2. Select the service.
3. Right-click and select **Properties**.
4. Select the **Log On** tab.
5. Select **This account**, and change the password.
6. Click **OK**.

CRM Services Computer

DCOM Configuration

If the following components are running under the domain account, update the DCOM configuration settings:

- TLSCMgr
- TlRptToFile
- TLCosmosSvr

To update the DCOM configuration settings:

1. Go to **Start**, **Administrative Tools**, **Component Services**.
2. Go to **Console Root**, **Component Services**, **Computers**, **My Computer**, **DCOM Config**.

3. Select the required component.
4. Right-click and select **Properties**.
5. Select the **Identity** tab.
6. Select **This user**, and change the password.
7. Click **OK**.

Services

A CampusNexus CRM installation involves the running of several services. These services are part of different CampusNexus CRM components installed at different locations. Modify each installation of all Services using the procedure given below for Campaign Dispatcher, Job Service, Webform Sync Service, Health Check Service, DNC Service, and Scheduled Report Service.

1. In Database Administrator, go to the **Services** node and check for details of the Service.
2. On the computer where the Service is running, go to **Start**, **Administrative Tools**, **Services**. The Services screen is displayed.
3. Right-click a Service and select **Properties** from the shortcut menu.
4. Select the **Log On** tab.
5. Select **This account**, and change the password.
6. Click **OK**.

SMS Services Computer

Update the domain user password for the following SMS components:

- SMS Extractor Service
- SMS Web Service
- SMS Dispatcher Service

Services

To update the SMS Extractor Service and SMS Dispatcher Service:

1. On the computer where SMS Extractor Service or SMS Dispatcher Service is installed, go to **Start**, **Administrative Tools**, **Services**. The Services screen is displayed.
2. Select **SMS Extractor Service**.
3. Right-click and select **Properties**.
4. Select the **Log On** tab.

5. Select **This account**, and change the password.
6. Click **OK**.
7. Repeat steps 2 through 6 for SMS Dispatcher Service.

Internet Information Services

To update the SMS Web Service:

1. Go to **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**. The Internet Information Services Manager is displayed.
2. Expand the <Name of Computer> node.
3. Select the Default Web Site node.
4. Select the <SMS Web Service name> node.
5. Click **Basic Settings** from the Action pane. The Edit Site dialog is displayed.
6. Click the **Connect As** button.
7. In the **Specific User** option click the **Set** button.
8. Change the password and click through **OK** three times.

Application Server Computer

DCOM Configuration

If the CampusNexus CRM Information Server component is running on a domain account, update its DCOM configuration settings.

1. Go to **Start**, **Administrative Tools**, **Component Services**.
2. Go to **Console Root**, **Component Services**, **Computers**, **My Computer**, **DCOM Config**.
3. Select the CampusNexus CRM Information Server component.
4. Right-click and select **Properties**.
5. Select the **Identity** tab.
6. Select **This user**, and change the password.
7. Click **OK**.

COM+ Applications

If the Application Server component is running on a domain account, update its COM+ Application settings.

1. Go to **Start**, **Administrative Tools**, **Component Services**.
2. Go to Console Root, **Component Services**, Computers, My Computer, COM+ Applications.
3. Select the Application Server component.
4. Right-click and select **Properties**.
5. Select the **Identity** tab.
6. Select **This user**, and change the password.
7. Click **OK**.

Internet Information Services

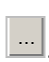
This section is applicable if the HTTP channel is configured for the Application Server.

Further, this section is applicable if the websites and application pools used for the CampusNexus CRM installation are running on a domain user account.

To update the Web Sites:

1. Go to **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**. The Internet Information Services Manager is displayed.
2. Expand the <Name of Computer> node.
3. Select the Default Web Site node. (Check for the details of the web servers in the Web Components node of Database Administrator.)
4. Click **Basic Settings** from the **Action** pane. The Edit Site dialog is displayed.
5. Click the **Connect As** button.
6. In the **Specific User** option click the **Set** button.
7. Change the password and click through **OK** three times.

To update the Application Pools:

1. Go to **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2. Select the **Application Pools** node. The Application Pools form is displayed.
3. Select the **DefaultAppPool**.
4. Right-click and select **Advanced Settings**. The Advanced Settings dialog is displayed.
5. In the **Identity** field, click . The Application Pool Identity dialog is displayed.
6. Select the **Custom account** option and click **Set**. The Set Credentials dialog is displayed.
7. Change the password and click through **OK** three times.

Web Components Computers

These steps are applicable for Business Administrator, Media, Scripts, Web Client, Web Client Notification Server, and iServices,

Internet Information Services

If the websites and application pools used for the CampusNexus CRM installation are running on a domain user account, update the Web Sites and Application Pools.

To update the Web Sites:

1. Go to **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**. The Internet Information Services Manager is displayed.
2. Expand the <Name of Computer> node.
3. Select the Default Web Site node.
4. Click **Basic Settings** from the Action pane. The Edit Site dialog is displayed.
5. Click the **Connect As** button.
6. In the **Specific User** option click the **Set** button.
7. Change the password and click through **OK** three times.

To update the Application Pools:

1. Go to **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**. The Internet Information Services (IIS) Manager is displayed.
2. Select the **Application Pools** node. The Application Pools form is displayed.
3. Select the **DefaultAppPool**.
4. Right-click and select **Advanced Settings**. The Advanced Settings dialog is displayed.
5. In the **Identity** field, click .... The Application Pool Identity dialog is displayed.
6. Select the **Custom account** option and click **Set**. The Set Credentials dialog is displayed.
7. Change the password and click through **OK** three times.

Alias on Business Administrator

You must change the passwords of all the Aliases created in Business Administrator that use the domain user account. To do so, log on to Business Administrator, and edit the Alias. In Database Administrator, start the extractor and dispatcher jobs and verify that their status is successful.

Web Form Integration

About Web Forms

For fields in the CampusNexus CRM Main database to be automatically updated when a Contact fills out a Web Form, a simple segment of code that generates an e-mail must be added to the Web Form from which you want to capture the desired information.

Anthology Inc. provides sample Web Forms that demonstrate how to integrate Web Forms with CampusNexus CRM. The code for a Sample Web Form is developed for Microsoft Internet Information Server (IIS), using Active Server Pages (ASPs). The code uses the AspEmail Component to send data from the Web Form as e-mail to CampusNexus CRM. This can be substituted with any other component that offers the Send Mail feature.

Implement the Sample Web Form on a page frequented by your Contacts to save the data collected through the Web Form into CampusNexus CRM.

The Webform Sync Service, which runs on the CampusNexus CRM Database is used to process Web Form e-mail messages on the Database component.

Sample Web Forms for all CampusNexus CRM Objects and other required information are available in the **\Samples\Web\WebForm** folder.

In addition to using code snippets to create and deploy Web Forms, you can use Template HTML pages to customize Normal Web Forms, and Mailer Web Forms by using the Web Form Generator, **WebFormGenerator.asp**.

You can customize the HTML pages to suit the business needs of your organization. Further, Normal, and Mailer Web Forms are processed using a generic ASP processor (**WebFormGenerator.asp**) that is designed to distinguish between each type of Web Form.

To process Normal Web Forms, and Mailer Web Forms, modify code only in the **WebFormGenerator.asp** file.

You can work with Normal or Mailer type of Template Web Forms from the **\Samples\Web\WebForm** folder. However, you can also work with Mailer Web Forms (MailerForm.html) available in the **\Samples\Web\MailerForm** folder.

Web Forms in the **\Samples\Web\WebForm** and **\Samples\Web\MailerForm** folders are processed by **.asp** files available in the same path.

For details on how you can use the Web Form Generator, see the **Business Administrator Help**.

About Web Form Integration

Web Form integration enables you to create or update the following Objects in CampusNexus CRM:

- Interaction (an e-mail request from a Contact.)
- Contact (a person sending a request to CampusNexus CRM.)
- Account (a company with which your organization has business relations, usually relevant to Business to Business scenarios.)
- Opportunity (an Opportunity is a lead that has turned into a prospect.)
- Order (an Order is received from a Contact.)
- Target (a Target is a Contact who is part of a Campaign.)
- Custom Objects (a custom Object is an Object created by the Business Administrator User.)

You can also implement Web Forms so that the **Can be called for this Campaign** Target system Property, and other user-defined Target Properties are automatically updated when a visitor or Contact submits a form on your organization's website. However, you cannot implement Web Forms to create Targets, and update other Target system Properties.

Web Form integration enables you to categorize Objects in CampusNexus CRM. Each of these Objects has its own set of Properties or fields that store data specific to the Object. You will often create or update the Contact Object, containing fields such as **First Name**, **Last Name**, and **Address**.

Your Web Form’s code to generate an e-mail will be executed on the Post command and does not interfere with your current processes, such as automatically updating your Contact database with the data the Contact enters, regardless of which Mail Send Component you use. The code you create will generate an e-mail with the following information:

1. The To field should contain the address of the Alias which is configured in CampusNexus CRM, and to which e-mail will be sent such as, customerservice@yourcompany.com.
2. The From field should contain the e-mail address of the Contact filling out the form. If the form does not require the Contact to fill in the e-mail address, retrieve the address from the Contact database.
3. The Subject line should contain a Magic String concatenated with one of the following:

   A hard-coded subject string such as Member Registration Web Form.

   — OR —

   The content entered by the Contact in the Subject field

   — OR —

   The value selected by the Contact from a list.

   The body of the e-mail contains the values the Contact entered in the Web Form passed in Special Tags, which CampusNexus CRM recognizes.

Note: By default, the Magic String is ‘CDXDFGVCJVCHGFJHNB30’. If this value has been changed, contact your administrator for the new Magic String.

When CampusNexus CRM receives the e-mail you generated from the Web Form, it automatically scans the subject line. If it locates the Magic String, it creates an Interaction or any of the other Objects, as appropriate, and displays the event, “Web Form message received...” in the Interaction history.

After identifying the e-mail received from a Web Form, CampusNexus CRM searches the body of the e-mail for special tags, retrieves the values passed to those tags, and updates the Main database. Values to be automatically updated in CampusNexus CRM should be sent as Special Tags in the body of the mail. Given below is an example of an Interaction created from data retrieved from a Web Form.

Special Tag Examples

The Object Name, Tab Name, Group Name, Property Name, and Category Name values will be given to you by the CampusNexus CRM Administrator. These Properties must be created in CampusNexus CRM for Web Form integration to work.

Note: Web Form integration will not work unless the name of each parameter matches the respective name in CampusNexus CRM. These names are not case sensitive, but the spellings must match.

Example for Account Object XML Tags

myArray(0)="<WebForm>"

myArray(1)="<Object><ObjectID>-1</ObjectID><LANG>English</LANG><DLID>1033</DLID><SQLLANGID>0</SQLLANGID><Object.Name>Account</Object.Name>"

myArray(2)="<EventList/><PropList>"

myArray(3)="<Tab><Tab.Name>Properties</Tab.Name>"

myArray(4)="<Group><Group.Name></Group.Name>"

myArray(5)="<Property><Property.Name>AccountName</Property.Name><Value><![CDATA["&name&"]]></Value></Property>"

myArray(6)="<Property><Property.Name>ParentAccount</Property.Name><Value><![CDATA["&parent&"]]></Value></Property>"

myArray(7)="<Prooperty><Property.Name>AccountManager</Property.Name><Value>"&manager&"</Value></Property>"

myArray(8)="<Property><Property.Name>Notes</Property.Name><Value><![CDATA["&notes&"]]></Value></Property>"

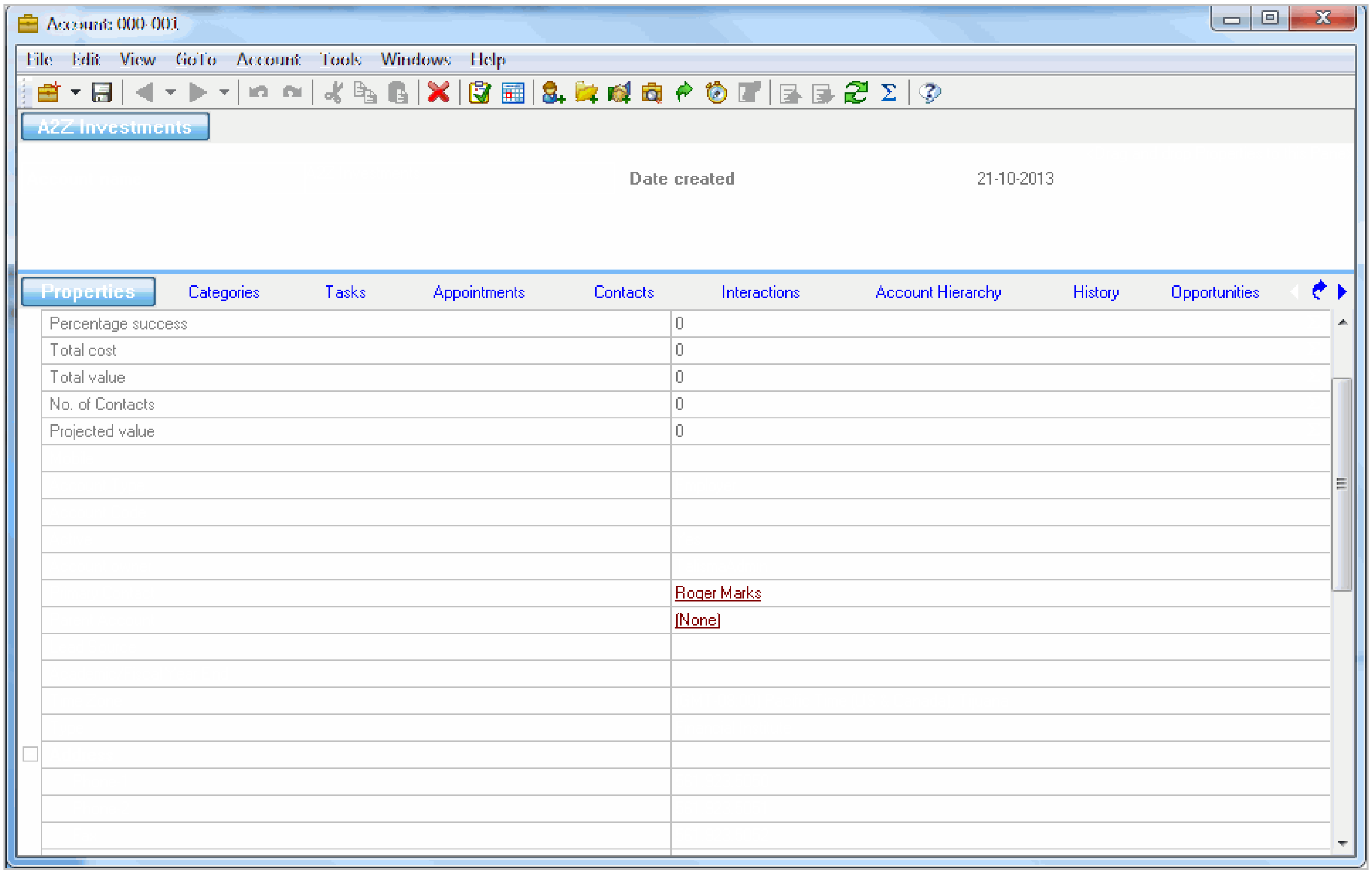
myArray(9)="<Property><Property.Name>Type</Property.Name><Value>"&acctype&"</Value></Property>"

myArray(10)="</Group>"

myArray(11)="<Group><Group.Name>Address</Group.Name>"

```
myArray(12)="<Property><Property.Name>Company</Property.Name><Value><![CDATA["&com-
pany&"]]></Value></Property>"

myArray(13)="<Property><Property.Name>Phone-1</Prop-
erty.Name><Value>"&phone1&"</Value></Property>"

myArray(14)="<Property><Property.Name>e-mailID</Prop-
erty.Name><Value>"&email&"</Value></Property>"

myArray(15)="<Property><Property.Name>Address-Street</Property.Name><Value><![CDATA
["&street&"]]></Value></Property>"

myArray(16)="<Property><Property.Name>Address-City</Property.Name><Value><![CDATA
["&city&"]]></Value></Property>"

myArray(17)="<Property><Property.Name>Address-State</Property.Name><Value><![CDATA
["&state&"]]></Value></Property>"

myArray(18)="<Property><Property.Name>Address-Country</Property.Name><Value><![CDATA["&coun-
try&"]]></Value></Property>"

myArray(19)="<Property><Property.Name>Address-Pin</Prop-
erty.Name><Value>"&zipcode&"</Value></Property>"

myArray(20)="</Group>"

myArray(21)="</Tab></PropList></Object></WebForm>"
```

The Object Type, Tab, Group, Property, and Property Value fields indicated in the figure demonstrate the corresponding XML tag values mentioned in the example. Follow the same method of field definition for the Interaction, Contact, Opportunity, Order Objects, and custom Objects, and to update the **Can be called for this Campaign** system Property.



Where:

- Account is an Object type in CampusNexus CRM.
- Properties is the Tab name for the Account Object.
- There is no Group name associated with the first set of Properties such as Account Name, Account Manager, and so on.
- Account Name is the Property name in the Properties tab, with no Group associated. This Property name on the Web Form must match the Property name in the Main database.

Example for Contact Object XML Tags

myArray(0)="<WebForm>"

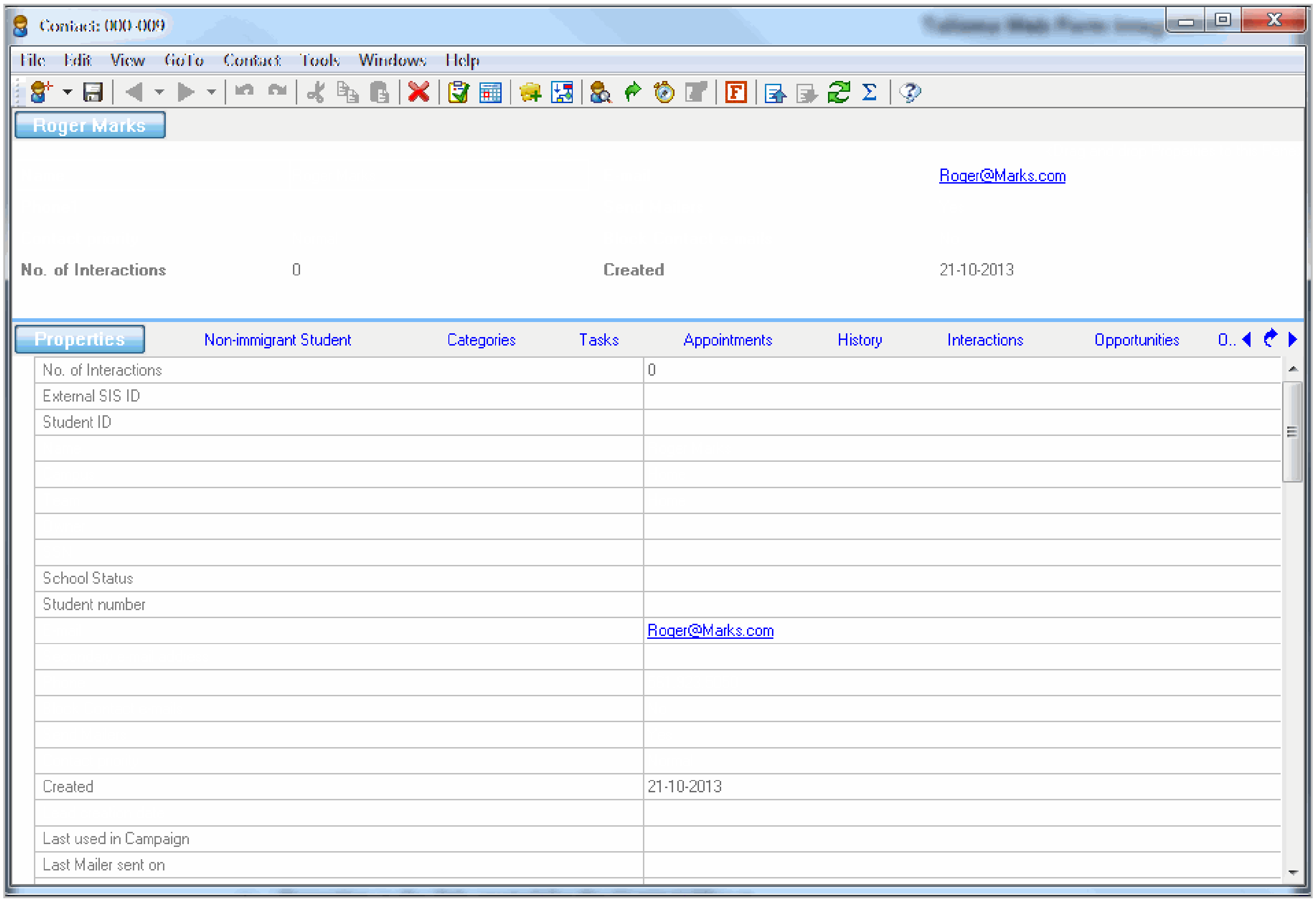
myArray(1)="<Object><ObjectID>-1</ObjectID><LANG>English</LANG><DLID>1033</DLID><SQLLANGID>0</SQLLANGID><Object.Name>Contact</Object.Name>"

myArray(2)="<EventList/><PropList>"

myArray(3)="<Tab><Tab.Name>Properties</Tab.Name>"

```
myArray(4)="<Group><Group.Name></Group.Name>"

myArray(5)="<Property><Property.Name>Name</Property.Name><Value>"&name&"</Value></Property>"

myArray(6)="<Property><Property.Name>E-mail</Property.Name><Value>"&email&"</Value></Property>"

myArray(7)="<Property><Property.Name>Phone</Property.Name><Value>"&phone&"</Value></Property>"

myArray(8)="</Group>"

myArray(9)="<Group><Group.Name>Full Name</Group.Name>"

myArray(10)-
)="<Property><Property.Name>FirstName</Property.Name><Value>"&fname&"</Value></Property>"

myArray(11)-
)="<Property><Property.Name>LastName</Property.Name><Value>"&lname&"</Value></Property>"

myArray(12)="</Group>"

myArray(13)="<Group><Group.Name>Address</Group.Name>"

myArray(14)="<Property><Property.Name>Street</Property.Name><Value><![CDATA
["&street&"]]></Value></Property>"

myArray(15)="<Property><Property.Name>City</Property.Name><Value><![CDATA
["&city&"]]></Value></Property>"

myArray(16)="<Property><Property.Name>State</Property.Name><Value><![CDATA
["&state&"]]></Value></Property>"

myArray(17)="<Property><Property.Name>Country</Property.Name><Value><![CDATA["&coun-
try&"]]></Value></Property>"

myArray(18)="<Property><Property.Name>Zip</Property.Name><Value>"&zipcode&"</Value></Property>"

myArray(19)="</Group>"

myArray(20)="</Tab></PropList></Object></WebForm>"
```

The **Object Type**, **Tab**, and **Property Value** fields indicated in the figure demonstrate the corresponding XML tag values in the example. Follow the same method of field definition for the Interaction, Account, Opportunity, and Order Objects.



Where:

- Contact is the Object type in CampusNexus CRM.
- Properties is the Tab created for the Contact Object.
- There is no Group name associated with the first set of Properties such as Actual value, and Language.
- First name is the Property name under the Full Name Group in the Properties tab.

Example for Setting Categories

You can also set or change the Categories for a selected Object. The following examples illustrate this process. The tags must be placed before the ending </object> and </webform> tags.

To Categorize an Object

```
myArray(40)="<CategorizeList>"

myArray(41)="<Category><Category.Name>"&categories&"</Category.Name>\</Category>"

myArray(42)="</CategorizeList>"
```

To Remove the Categorization of an Object

myArray(43)="<UnCategorizeList>"

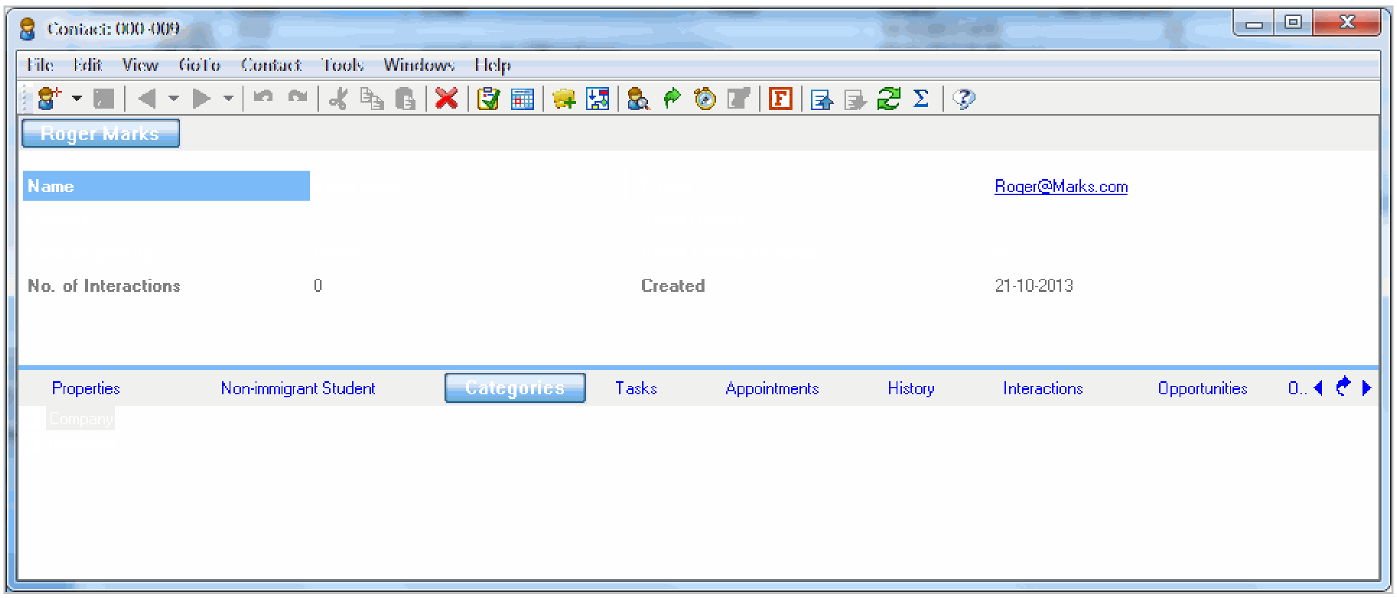
myArray(44)="<Category><Category.Name>"&categories&"</Category.Name></Category>"

myArray(45)="</UnCategorizeList>"

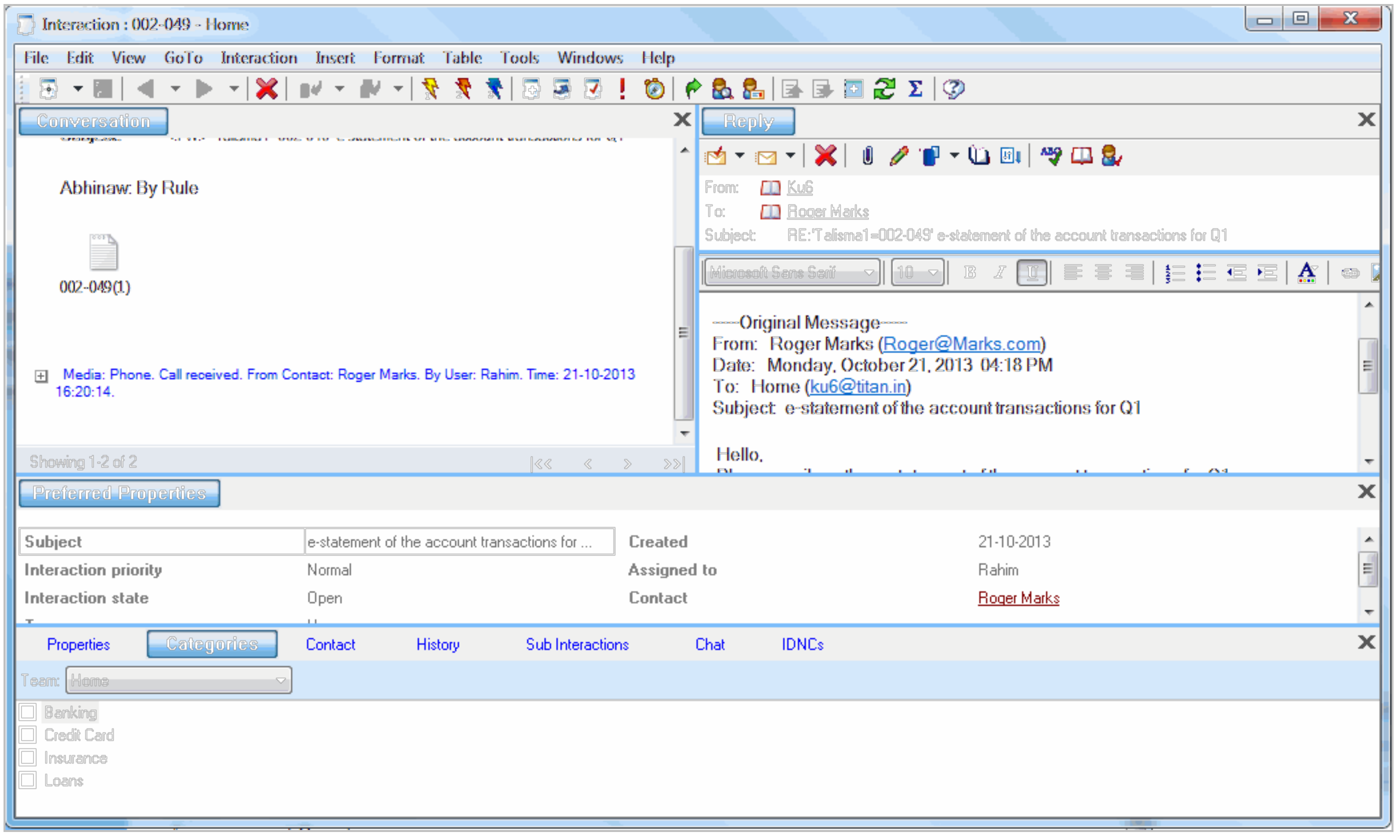
myArray(46)="</Object>"

myArray(47)="</WebForm>"

The image below illustrates the Categories associated with the Contact Object. CampusNexus CRM enables you to set Categories for every Object.



The following image illustrates a Category for the Interaction Object. CampusNexus CRM enables you to set Categories for every Object.



Multilingual Support

The Web Form can contain a tag specifying the Language ID for the Property names in it. For example, <Lang>English</Lang>.

The Web Form may also contain a tag specifying the language of the data in the Web Form. For example, <DLID>1033</DLID>, where ‘1033’ is the Language ID for English (United States).

When the Web Form is being processed by the Webform Sync Service, the language tags are picked up and processed accordingly. If the tags are not specified, the Offline Service assumes the Default Server Language for both (this can be configured using Business Administrator).

The Web Form can be displayed in one language, and the values you enter can be internally mapped to any language when the Web Form is being sent to the Database component. This will enable the same Web Form to be used across language sites.

Test Web Form Integration

1. Create the XML tags for your Web Form in a staging environment. Generate an e-mail and send it to your personal mailbox rather than sending it directly to CampusNexus CRM. The subject line should begin with: CDXDFGVCJVCHGFJHNB30 and the body of the message should contain the XML tags.

2. Copy and paste the XML tags which are in the body of the e-mail into a Notepad file. Save the Notepad file as **test.xml**.
3. Open the **text.xml** file. If your XML tags contain errors, the errors are displayed. If the XML tags do not contain errors, each tag in the file is displayed. The Web Form sample also contains a sample for directly generating the XML file.
4. After verifying the XML tags from the Web Form, generate an e-mail to an Alias, which is to be retrieved by CampusNexus CRM.
5. Log on to CampusNexus CRM by obtaining the login details from Business Administrator. Verify whether each of the fields you want to update is filled in appropriately. Also, ensure that the Interaction case history displays an event with the message 'Web Form interaction created'. Use the figures in this chapter to determine how to verify whether the fields are updated. Contact the Business Administrator User, if it is necessary.

Example of Web Form Integration in ASP

1. **ExecuteEnhancementRequest.asp** updates Contact Properties and uses the CDONTS Send Mail Component.
2. **Interaction.asp** and **Interaction.htm** are samples for creating an Interaction in CampusNexus CRM. This uses the Persits.MailSender AspSendmail Component. You will find additional samples for the Account, Opportunity, Order, and Contact Objects on the CD under \\Explore CD\ Samples\Web

Tips to Use Web Forms

This section provides tips and best practices to remember when using Web Forms.

Integrate Simple Properties

CampusNexus CRM Properties, which reside in the Tab-Group- <Property> structures, can be integrated as shown in the following code snippet:

Sample for Integrating Properties

Assumption: The Property "Balance Value" needs to be added in the Opportunity Object in a tab named "Custom" and group named "Details". Check the code below:

```
myArray(n)="<Tab><Tab.Name>Custom</Tab.Name>"

myArray(n)="<Group><Group.Name>tabProperties</Group.Name>"

myArray(n)="<Property><Property.Name>Balance Value</Property.Name><Value>"&bVal&"</Value></Property>"

myArray(n)="</Tab></Group>"
```

Here, bVal => variable, which has the value, that comes from the Web Form user interface.

Tab and group tags should be opened and closed as displayed.

Integrate Categories

When some Categories need to be integrated with CampusNexus CRM, you should decide which interface elements are to be associated with the Categories.

They can be displayed either as check boxes or as "Yes/No" type of Properties. This is specified in the **.htm(l)** file of the Web Form as normal Web coding.

Mapping of the values for each of the interface elements is similar as Properties.

Sample for Categorizing an Object

For categorizing a CampusNexus CRM Object using Web Forms, the following code can be used.

Assumption: Category 1 and Category 2 are two sample Categories that will be assigned to an Object.

```
categorize = Category 1

categorize1 = Category 2

myArray(11)="<CategorizeList>"

myArray(12)="<Category><Category.Name>"&categorize&"</Category.Name></Category>"

myArray(13)="<Category><Category.Name>"&categorize1&"</Category.Name></Category>"

myArray(14)="</CategorizeList>"
```

Sample for Removing the Category Associated with an Object

The following code can be used to remove the category associated with a CampusNexus CRM Object using Web Forms.

Assumption: An Object that has been categorized as Category 1 has to be changed.

```
uncategorize= Category 1

myArray(15)="<UnCategorizeList>"

myArray(16)="<Category><Category.Name>"&uncategorize&"</Category.Name></Category>"

myArray(17)="</UnCategorizeList>"
```

Support Special Characters in Web Forms

CampusNexus CRM, by default does not support all special characters in its Web Forms. To enable supporting of all the special characters, the CDATA sections in the Web Form Sample must be used as follows:

Assumption:

Special characters for a Property called "Hobby" need to be supported. The Property will be used in the code array as follows:

```
myArray(n)=“<Property><Property.Name>Hobby</Property.Name><Value><![CDATA
[“&HobbyData&”]]></Value></Property>”
```

Here, HobbyData => variable which has the value that comes from the Web Form interface, and contains special characters such as &, “, ”, <, ', >, and so on.

Working of Web Forms

Note the following points about the working of Web Forms in CampusNexus CRM:

- Ensure that the names of the Custom Property, tab, and the group in the Web Form are specified exactly as in CampusNexus CRM. However, they are not case sensitive.

  For example, a Property called “balance value” in CampusNexus CRM can be specified as “BALANCE VALUE” in the Web Form to capture its value.

- If the same e-mail address is used to create an Interaction and a Contact, here is how CampusNexus CRM works:

  The e-mail address specified in the request Web Form is used to create a Contact. This Contact is linked to an Interaction in CampusNexus CRM. The e-mail address specified in the Contact Web Form is used to create a new Contact with the specified e-mail address and other details.

- The Object ID is displayed as –1.

  -1 indicates a new Object. It means that a new Object will be created with the details specified.

- The maximum number of characters allowed in a single line is 76.

  This is an SMTP restriction.

Solution Options

The following topics provide instructions for the configuration of solution options.

Configure Services as Clustered Services

To configure Talisma Server on a Cluster Server, the Talisma Job Service, Talisma Webform Sync Service, and Talisma Health Check Servicemust be configured as clustered services.

Talisma Job Service

To configure Talisma Job Service on the Secondary Cluster Node and set it to the **Online** state, perform the following steps:

1. Type the following command in the **Open** field in the **Run** dialog box:

   ```
   "<Drive name>:\Program Files\Common Files\Talisma Shared\<Database
   name>\TlJobSvc.exe" -Service- Name="TlJobSvc_ SQLVirtualServerName_MainData-
   baseName"
   ```

   For example,

   ```
   "<Drive name>:\Program Files\Common Files\Talisma Shared\<Database
   name>\TLJobSvc.exe" -Service-Name="tlJobSvc_VSQL_INST1_tlMain"
   ```

   The Talisma Job Service is configured on the Secondary Cluster Node.

2. From the Services window, ensure that the service is set to the **Manual** mode. To do so, perform the following steps:

   a. Type **services.msc** in the **Open** field of the **Run** dialog box. The Services window is displayed.

   b. In the right pane, right-click Talisma Job Service and select **Properties** from the shortcut menu. The Properties dialog box is displayed.

   c. Ensure that the value in the **Startup type** field is **Manual**.

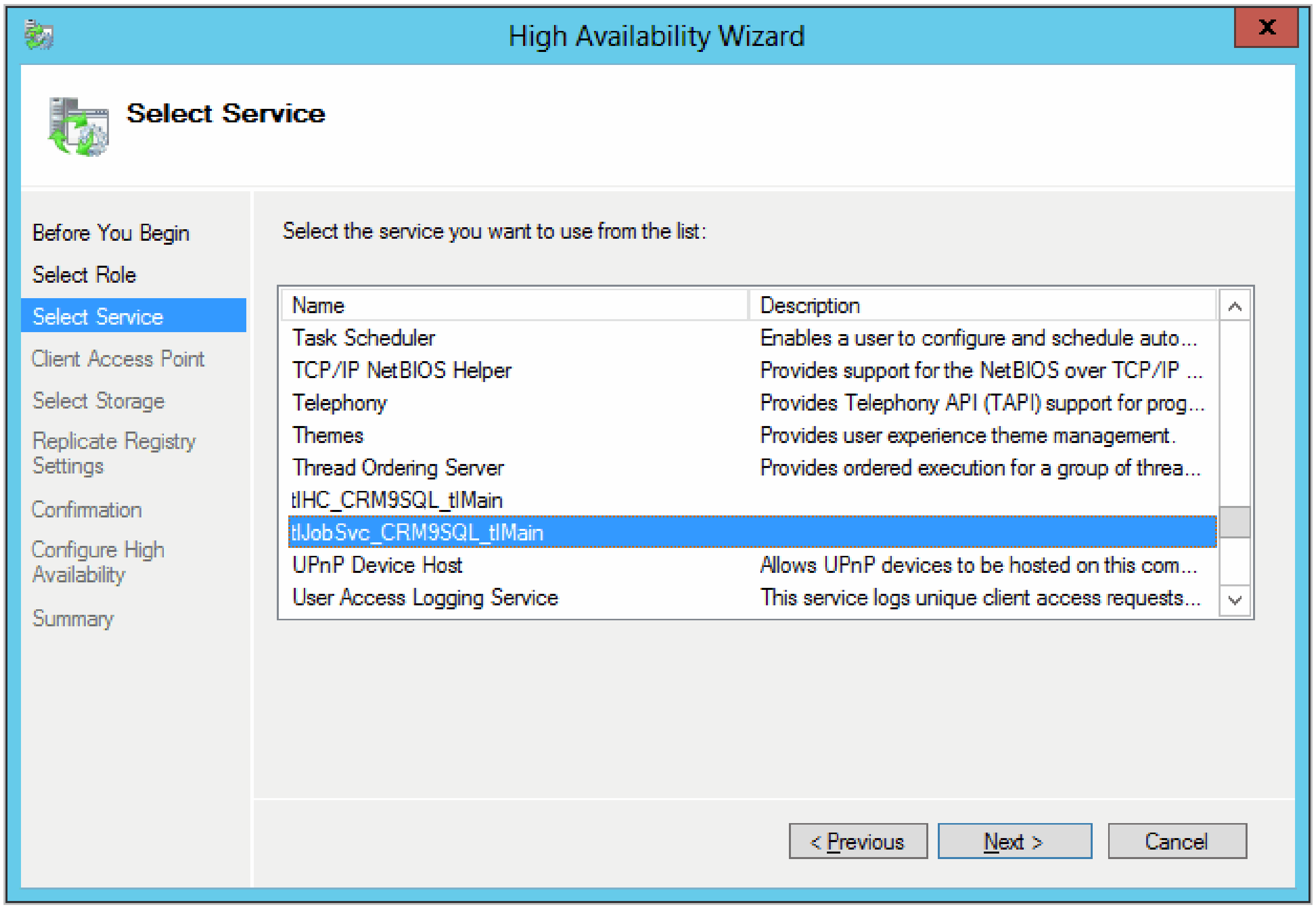
3. Export the following Talisma Job Service registry keys from the Primary Cluster Node, and then import the same to the Secondary Cluster Node:

   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Talisma Job Service
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<tlJobSvc_ SQLVirtualServerName>_ <MainDatabaseName>

4. Open the Failover Cluster Manager on the Primary Cluster Node. For steps to open the Failover Cluster Manager, see Opening and Viewing the Failover Cluster Manager.

5. In the left pane, navigate to **<Cluster Server Name>, Roles**.

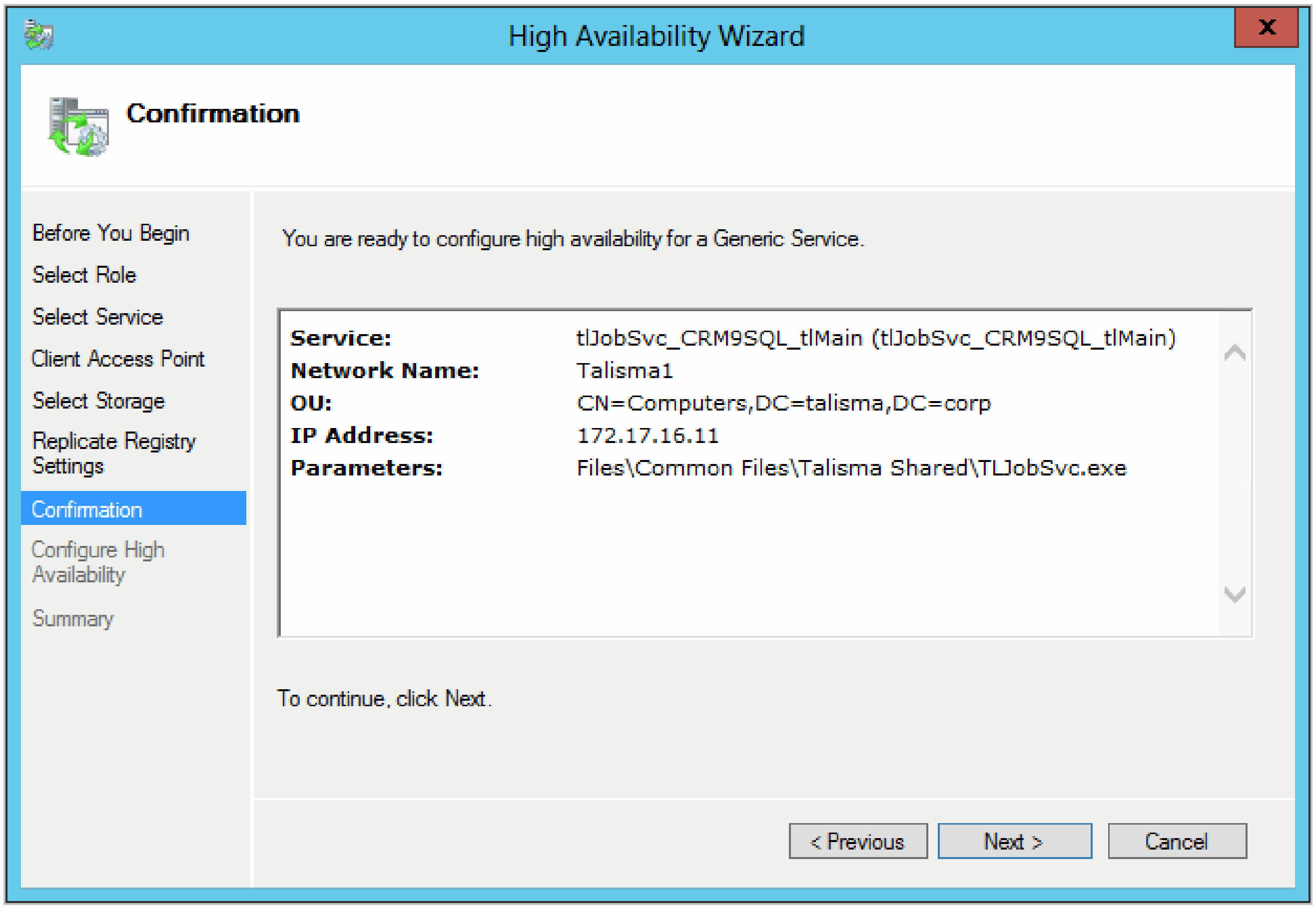
6. Right-click **Roles** and select **Configure Role** from the shortcut menu. The High Availability Wizard - Select Role window is displayed.
7. Select **Generic Service**. The High Availability Wizard - Select Service window is displayed.
8. In the New Resource Wizard, select **tlJobSvc_<Name of the Virtual SQL Server>_<Name of the Virtual SQL Server Instance>_<Name of the Database>**. For example, **tlJobSvc_CRM9SQL_tlMain**.



9. Click **Next**.
10. In the Client Access Point window, specify a name in the **Name** field. The name must be unique.
11. Select a network in the Networks column and specify the IP address in the Address column. The IP address must be unique and must belong to the range specified in the Networks column.
12. Click **Next**.

    If applicable, specify details in the Select Storage and Replication Registry Settings windows.

    The Confirmation window is displayed.

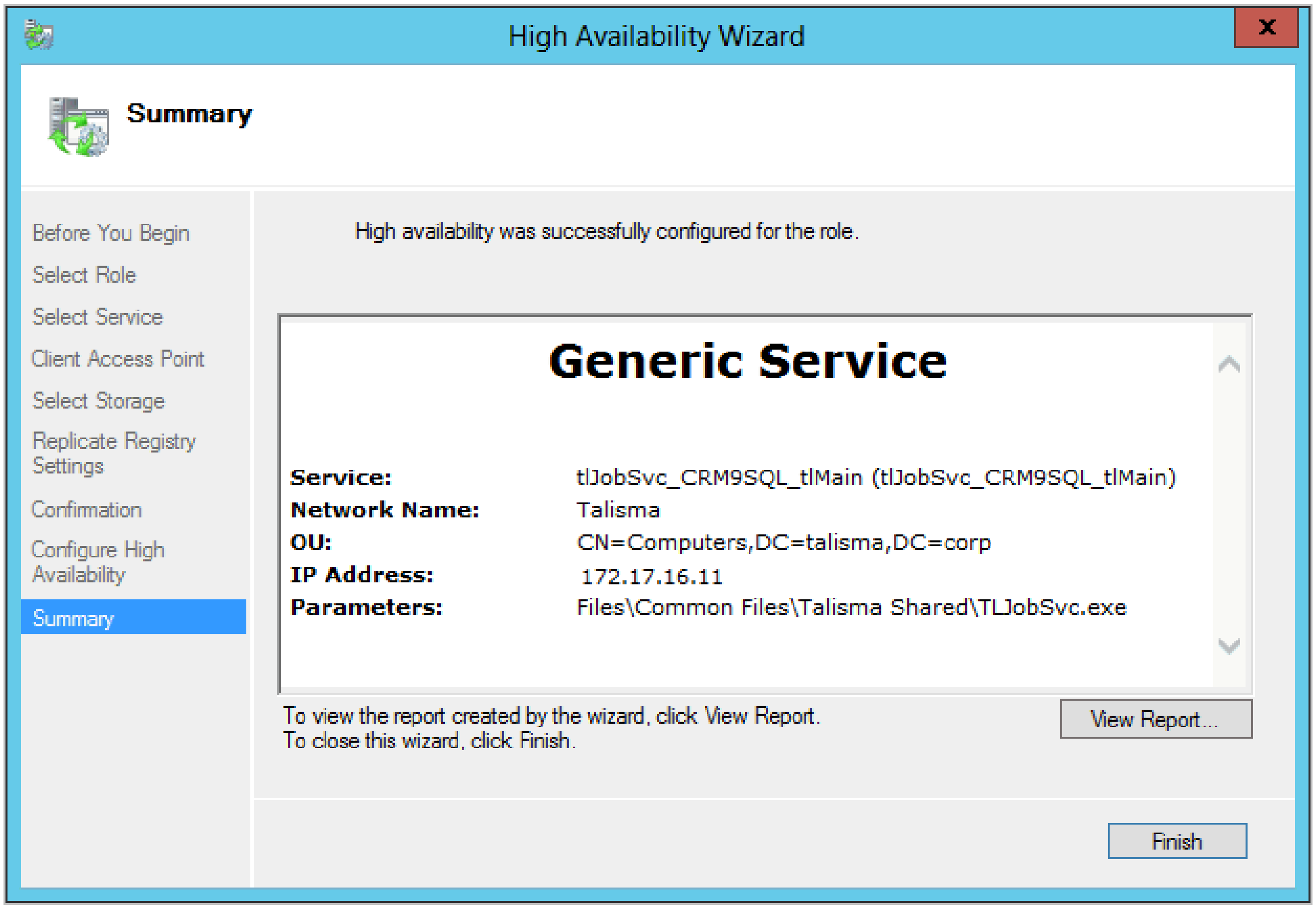


13. Click **Next**.

    The Configure High Availability window is displayed and the process of configuring High Availability begins.

14. Click **Next**.

    The Summary page is displayed. Click on the **View Report** button to view the report of the configuration.

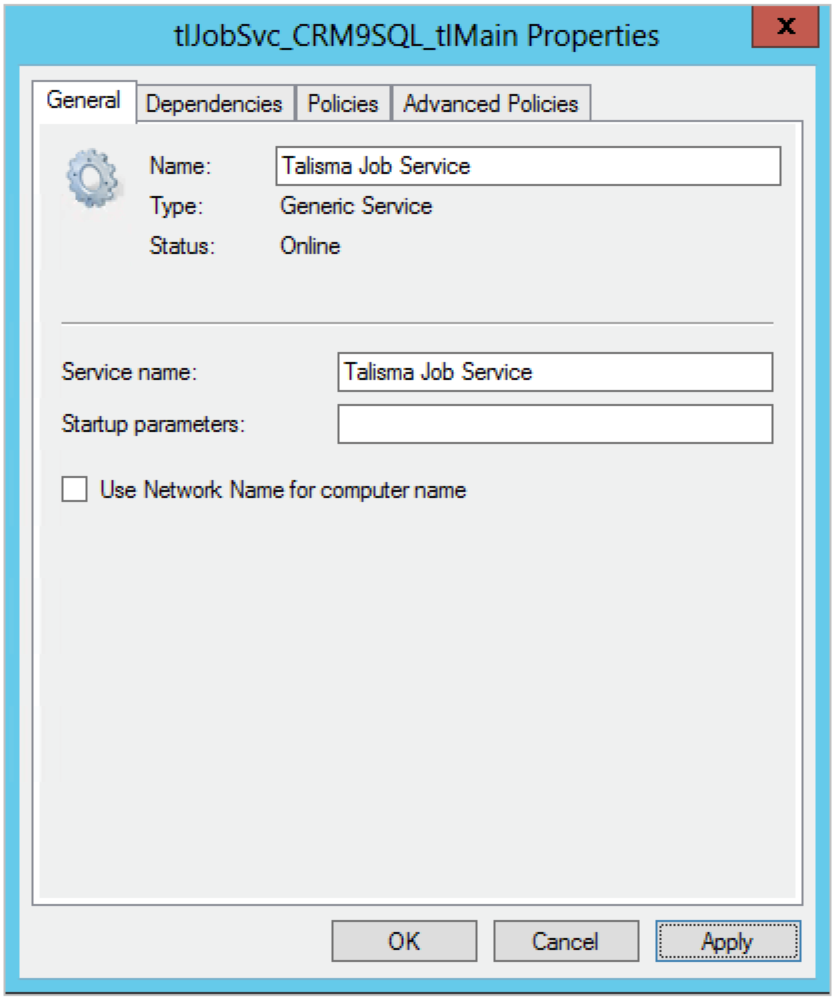


15. Click **Finish**.

    The Talisma Job Service is added as a Cluster Resource and is displayed in the right pane of the Failover Cluster Manager window. By default, the status of the Resource is **Offline**.

16. In the Failover Cluster Manager window, right-click **Talisma Job Service** and select **Properties**.

    The Talisma Job Service Properties page is displayed.

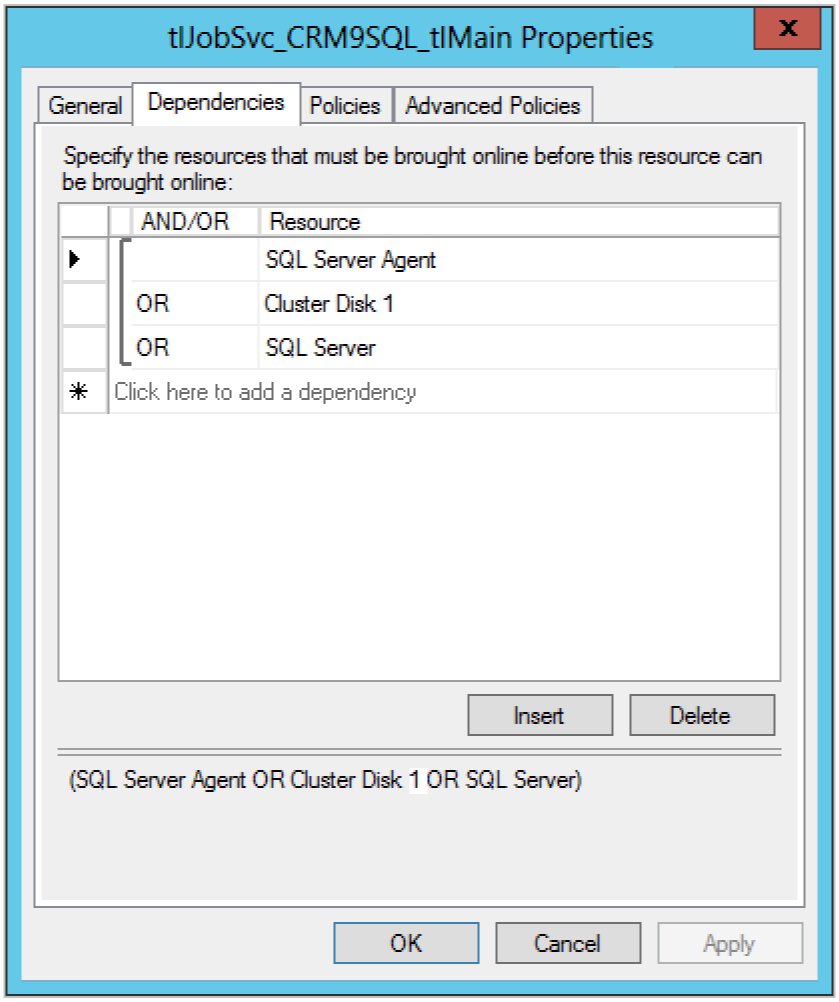


17. In the **General** tab, perform the following steps:

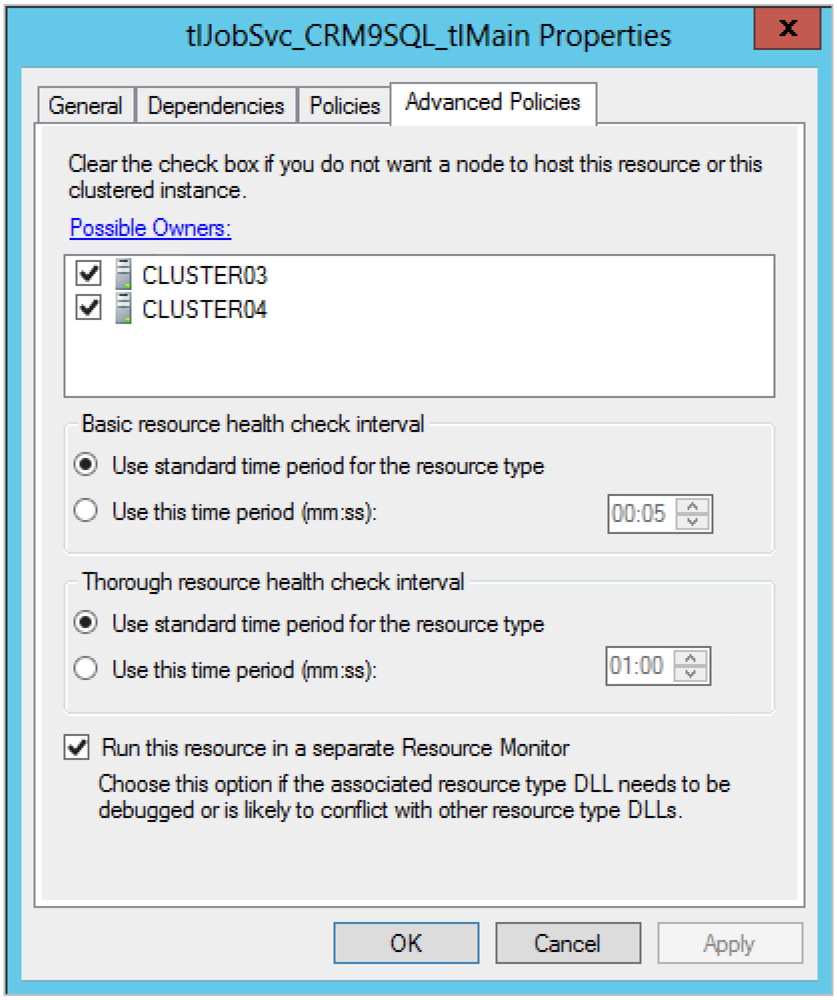
    a. Type Talisma Job Service in the **Name** and **Service name** field. Delete the value in the **Startup parameters** field.

    b. Clear the selection of the **Use Network Name for computer name** option. By default, this option is selected.

18. In the **Dependencies** tab, add **SQL Server**, **SQL Server Agent**, and **Cluster Disk 1** in the **Resource** column.



19. In the **Advanced Policies** tab, select the **Run this resource in a separate Resource Monitor** option.



20. Click **OK** in the Talisma Job Service Properties page.

    The Failover Cluster Manager is displayed.

21. In the Failover Cluster Manager window, right-click **Talisma Job Service** and select **Bring online** from the shortcut menu.

    The Service is set to the **Online** state.

Talisma Webform Sync Service

To configure Talisma Webform Sync Service on the Secondary Cluster Node and set it to the Online state, perform the following steps:

1. Move all Cluster Resources to the Secondary Cluster Node.
2. Type the following command in the **Open** field of the Run dialog box:

```
<Target Drive>:\<Talisma Server Target folder>\Binn\MainDBName\TlOfSyncU.exe”
/Service /ServiceName:"SQLVirtualName_MainDatabaseName"
```

```
/User:"DomainName\UserName" /Password:"password of user" /Data-
base:"MainDatabaseName" /Server:"SQLVirtualName"
```

For example,

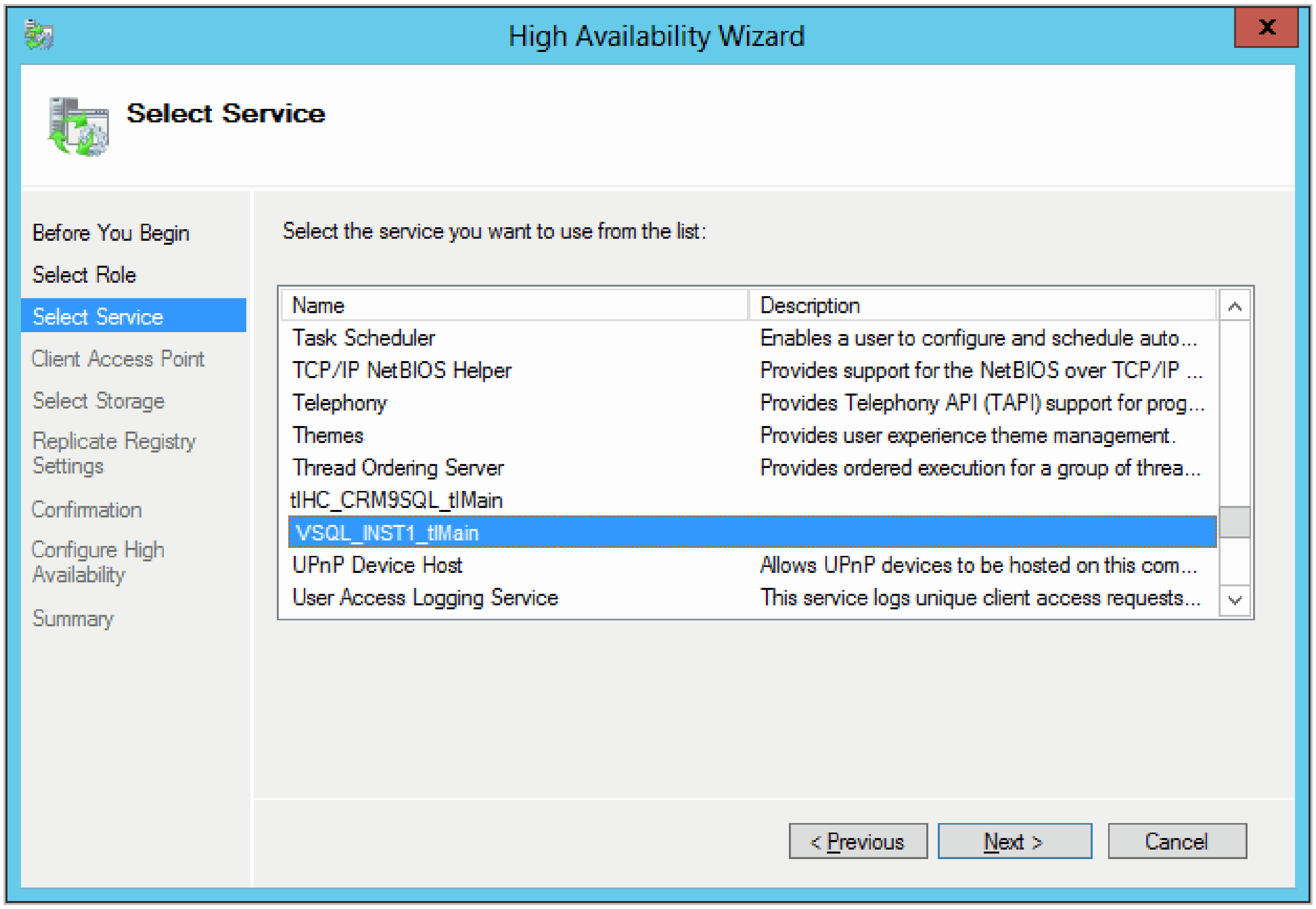
```
"J:\TalismaServer\Binn\INST1tlMain\TLOfSyncU.exe" /Service /ServiceName:"VSQL_
INST1_tlMain" /User:"crmtest" /Password:"Testlab4" /Database:"tlMain" /Server-
:"VSQL"
```

The Talisma Webform Sync Service is configured on the Secondary Cluster Node.

3. Export the following Talisma Job Service registry keys from the Primary Cluster Node, and then import the same to the Secondary Cluster Node:
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Talisma Job Service
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<tlJobSvc_ SQLVirtualServerName>_ <MainDatabaseName>
4. From the Services window, ensure that the service is set to the **Manual** mode. To do so, perform the following steps:
   a. Type **services.msc** in the **Open** field of the Run dialog box. The Services window is displayed.
   b. In the right pane, right-click Talisma Webform Sync Service and select **Properties** from the shortcut menu. The Properties dialog box is displayed.
   c. Ensure that the value in the **Startup type** field is **Manual**.
5. Open the Failover Cluster Manager on the Primary Cluster Node. For steps to open the Failover Cluster Manager, see Opening and Viewing the Failover Cluster Manager.
6. In the left pane, navigate to **<Cluster Server Name>, Roles**.
7. Right-click **Roles** and select **Configure Role** from the shortcut menu.

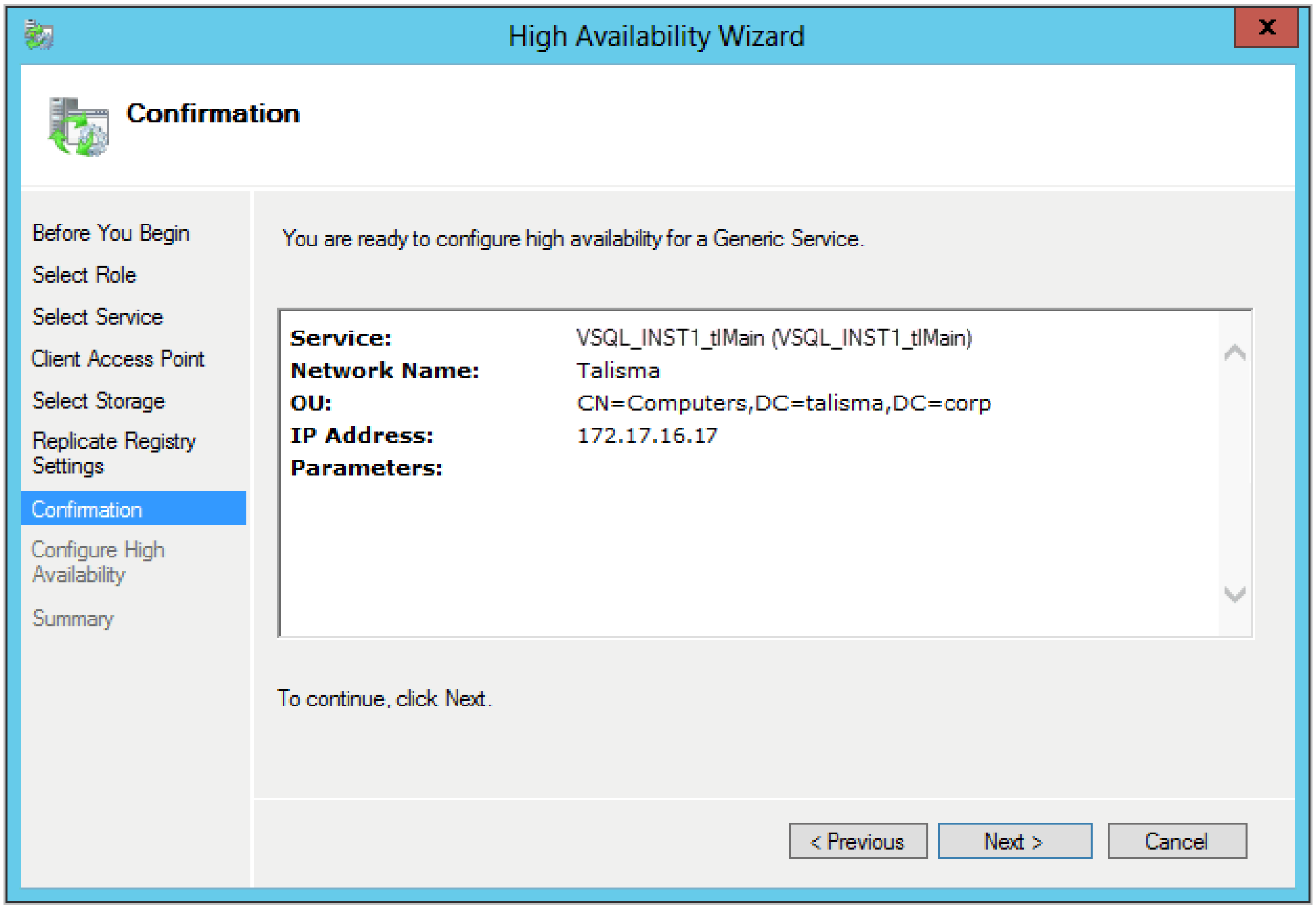
   The High Availability Wizard - Select Role window is displayed.
8. Select **Generic Service**.

   The High Availability Wizard - Select Service window is displayed.
9. Select **<SQLVirtualServerName>_<MainDatabaseName>**. For example, **VSQL_tlmain**.



10. In the Client Access Point window, specify a name in the **Name** field. The name must be unique.
11. Select a network in the Networks column and specify the IP address in the Address column. The IP address must be unique and must belong to the range specified in the Networks column.
12. Click **Next**. If applicable, specify details in the Select Storage and Replication Registry Settings windows.

    The Confirmation window is displayed.

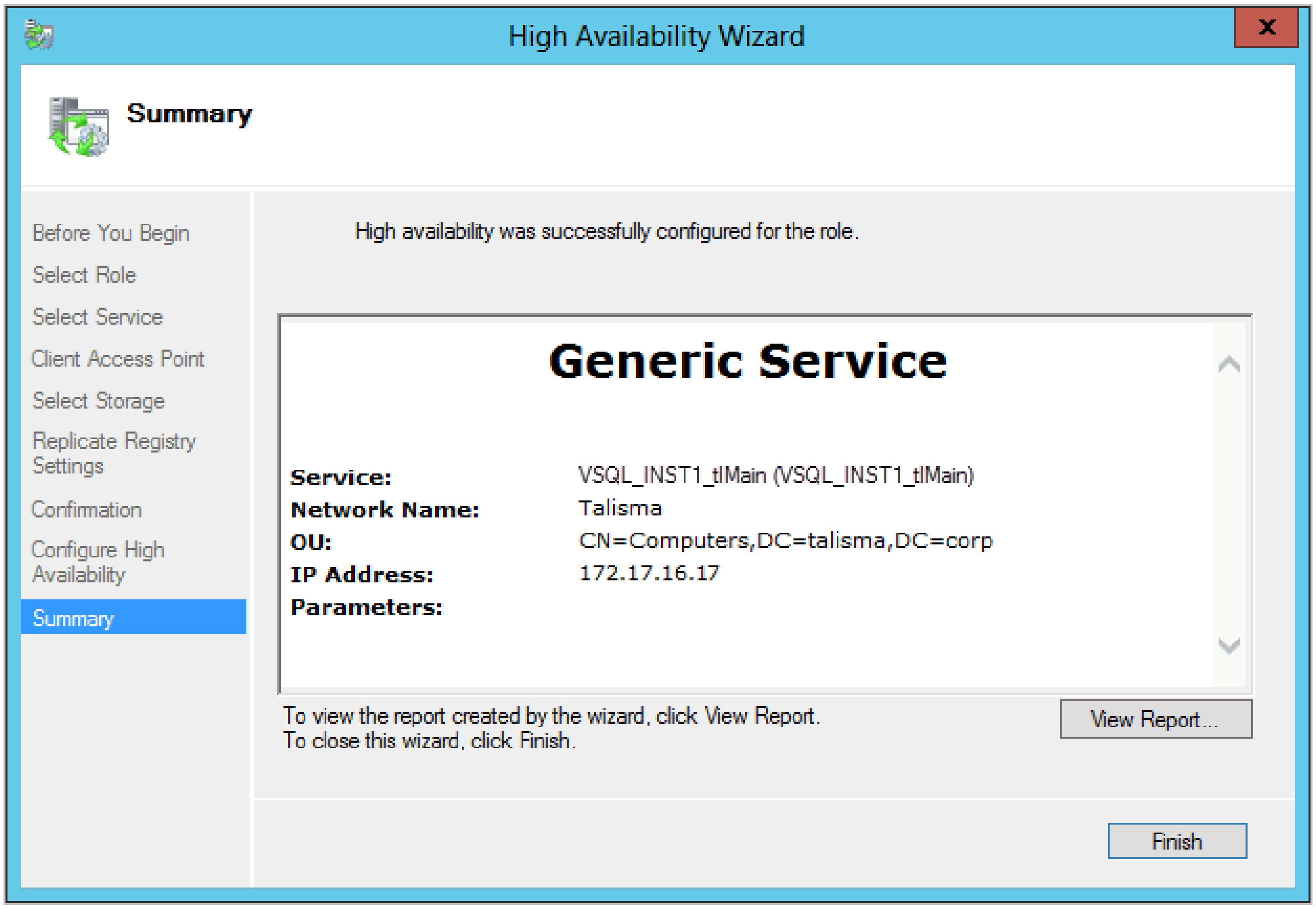


13. Click **Next**.

    The Configure High Availability window is displayed and the process of configuring High Availability begins.

14. Click **Next**.

    The Summary page is displayed. Click on the **View Report** button to view the report of the configuration.

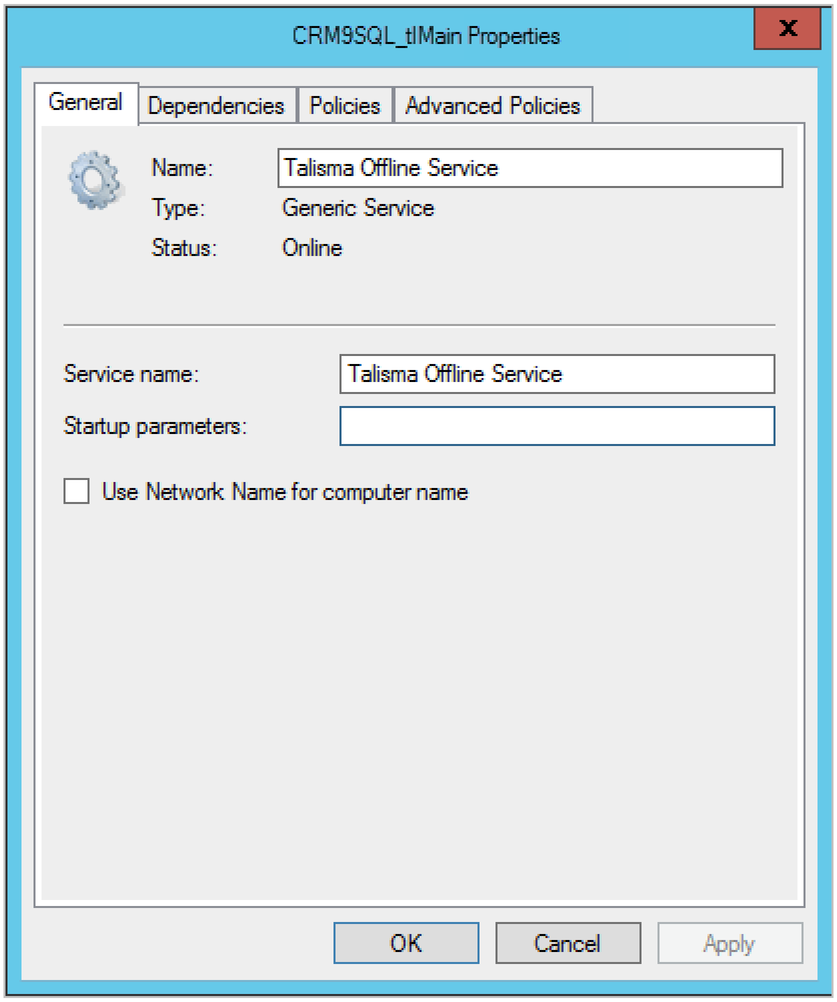


15. Click **Finish**.

    The Talisma Webform Sync Service is added as a Cluster Resource and is displayed in the right pane of the Failover Cluster Manager window. By default, the status of the Resource is **Offline**.

16. In the Failover Cluster Manager window, right-click **Talisma Webform Sync Service** and select **Properties**.

    The Talisma Webform Sync Service Properties page is displayed.



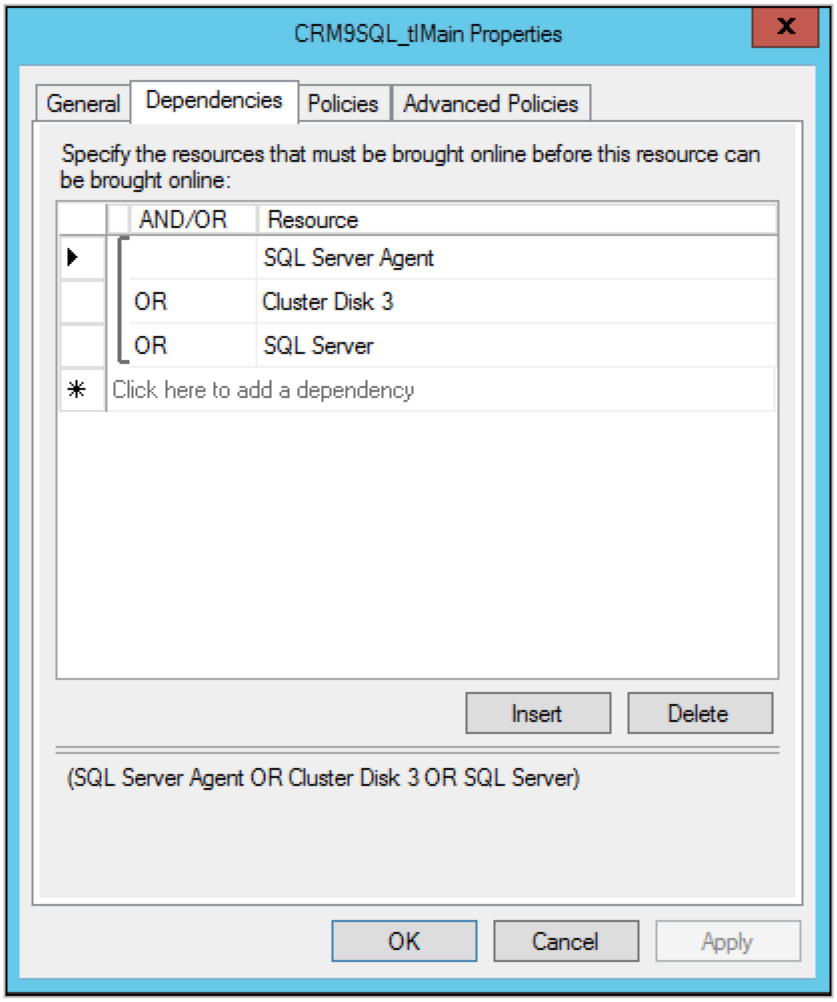
17. In the **General** tab, perform the following steps:

    a. Type Talisma Webform Sync Service in the **Name** and **Service name** fields.

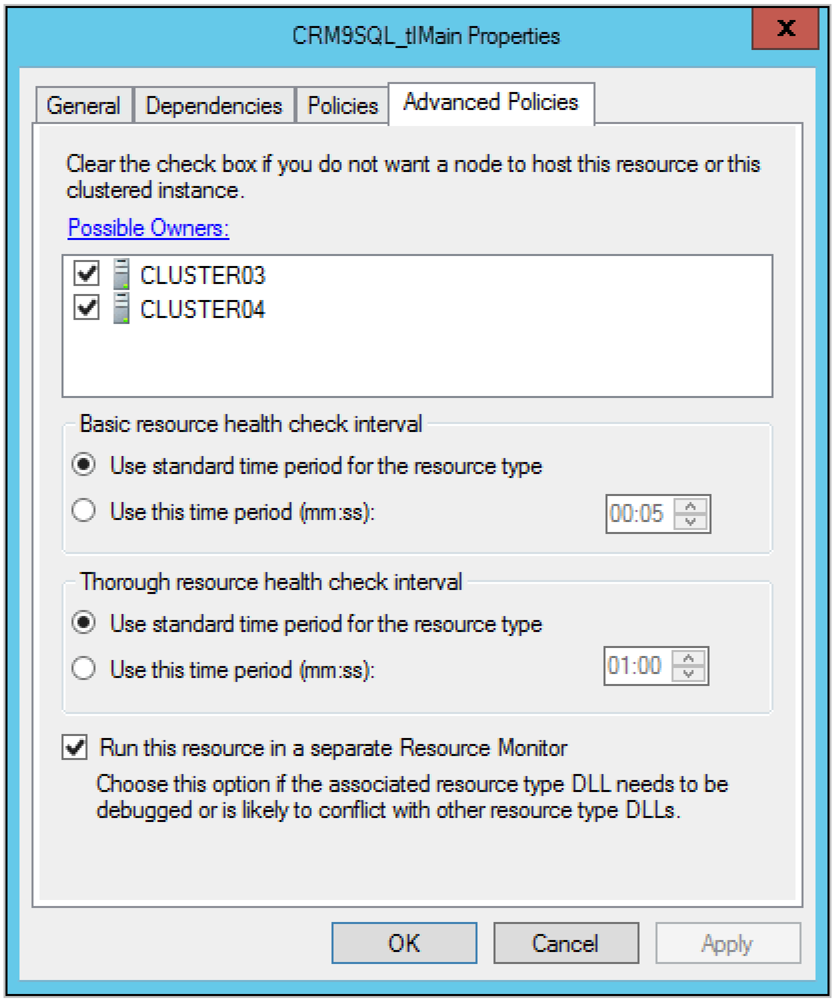
    b. Delete the value in the **Startup parameters** fields.

    c. Clear the selection of **Use Network Name for computer name** option. By default, this option is selected.

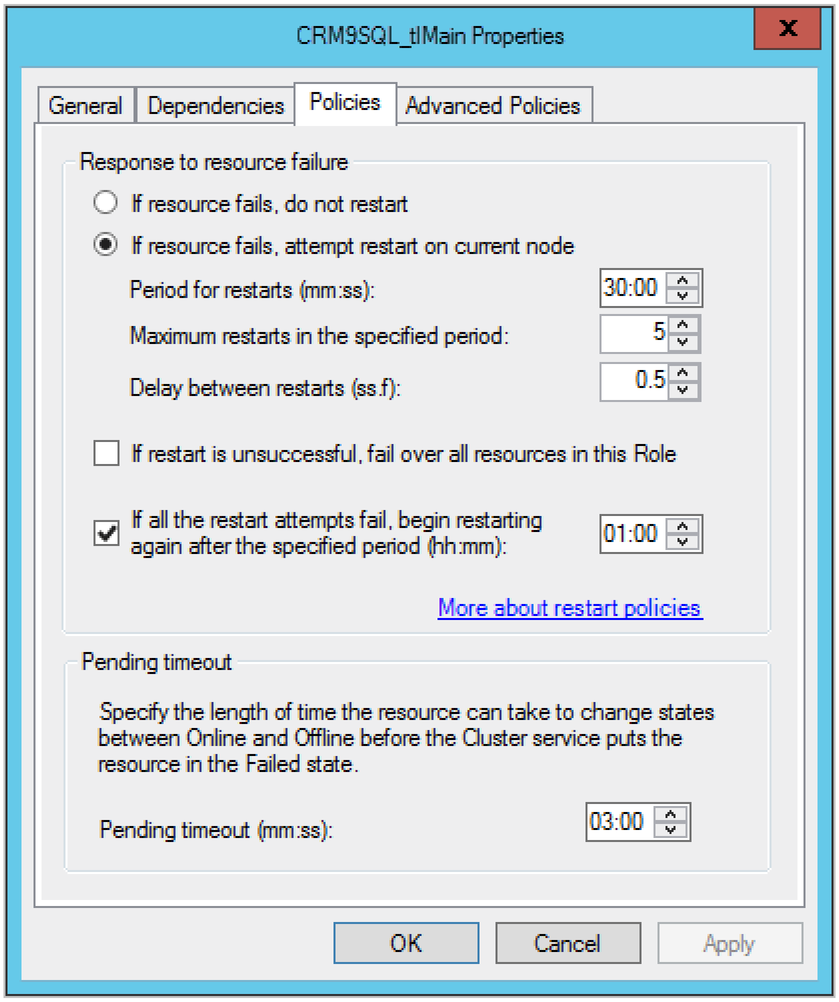
18. In the **Dependencies** tab, add **SQL Server**, **SQL Server Agent**, and **Cluster Disk 1** in the **Resource** column.



19. In the **Advanced Policies** tab, select the **Run this resource in a separate Resource Monitor** option.



20. In the **Policies** tab, set the policy as per the requirement.



21. Click **OK** in the Talisma Webform Sync Service Properties page.

    The Failover Cluster Manager window is displayed.

22. Right-click Talisma Webform Service and select **Bring online** from the shortcut menu.

    The Service is set to the **Online** state.

Talisma Health Check Service

To configure the Talisma Health Check Service on the Secondary Cluster Node and set it to the **Online** state, perform the following steps:

1. Type the following command in the **Open** field of the Run dialog box:

   ```
   Talisma Shared Folder\ TLHealthCheckU.exe /Service /ServiceName:"tlHC_ SQLVirtualName_MainDatabaseName" /User:"DomainName\UserName" /Password:"password of user" /Database:"MainDatabaseName" /Server:"SQLVirtualName"
   ```

   For example,

```
"<Drive name>:\ Program Files (x86)\Common Files\Talisma Shared\<Database
name>\TLHealthCheckU.exe" /Service /ServiceName:"tlHC_VSQL_INST1_tlMain" /User-
:"crmtest" /Password:"Testlab4" /Database:"tlMain" /Server:"VSQL"
```

The Talisma Health Check Service is configured on the Secondary Cluster Node.

2. From the Services window, ensure that the service is set to the **Manual** mode. To do so, perform the following steps:

    a. Type **services.msc** in the **Open** field of the Run dialog box: The Services window is displayed.

    b. In the right pane, right-click Talisma Health Check Service and select **Properties** from the shortcut menu. The Properties dialog box is displayed.

    c. Ensure that the value in the **Startup type** field is **Manual**.

3. Open the Failover Cluster Manager on the Primary Cluster Node. For steps to open the Failover Cluster Manager, see [Opening and Viewing the Failover Cluster Manager].

4. In the left pane, navigate to **<Cluster Server Name>, Roles**.

5. Right-click **Roles** and select **Configure Role** from the shortcut menu.

    The High Availability Wizard - Select Role window is displayed.

6. Select **Generic Service**.

    The High Availability Wizard - Select Service window is displayed.

7. Select **<tlHC_SQLVirtualName>_<MainDatabaseName>**.

8. Click **Next**.

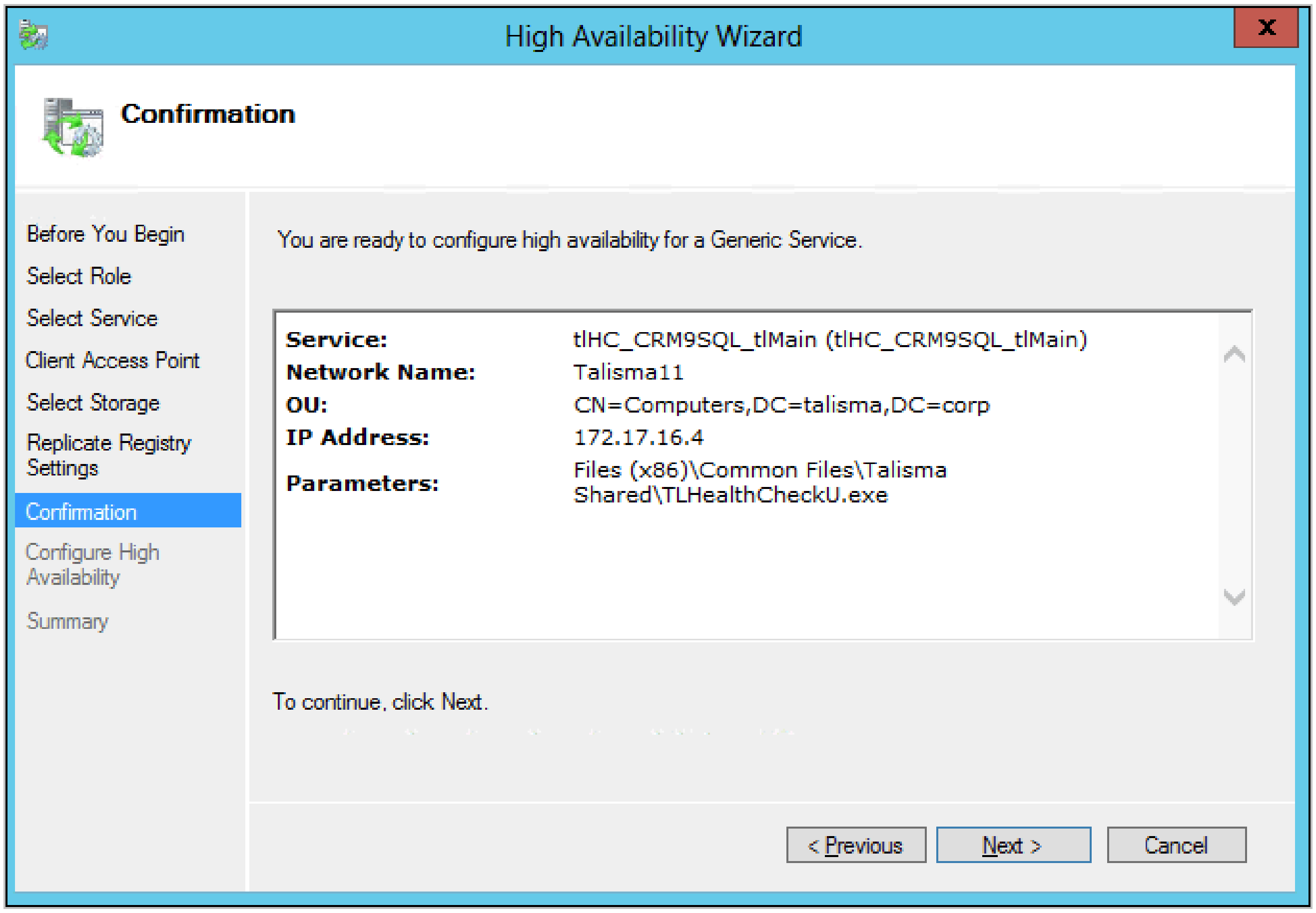
9. In the Client Access Point window, specify a name in the **Name** field. The name must be unique.

10. Select a network in the Networks column and specify the IP address in the Address column. The IP address must be unique and must belong to the range specified in the Networks column.

11. Click **Next**.

    If applicable, specify details in the Select Storage and Replication Registry Settings windows.

    The Confirmation window is displayed.

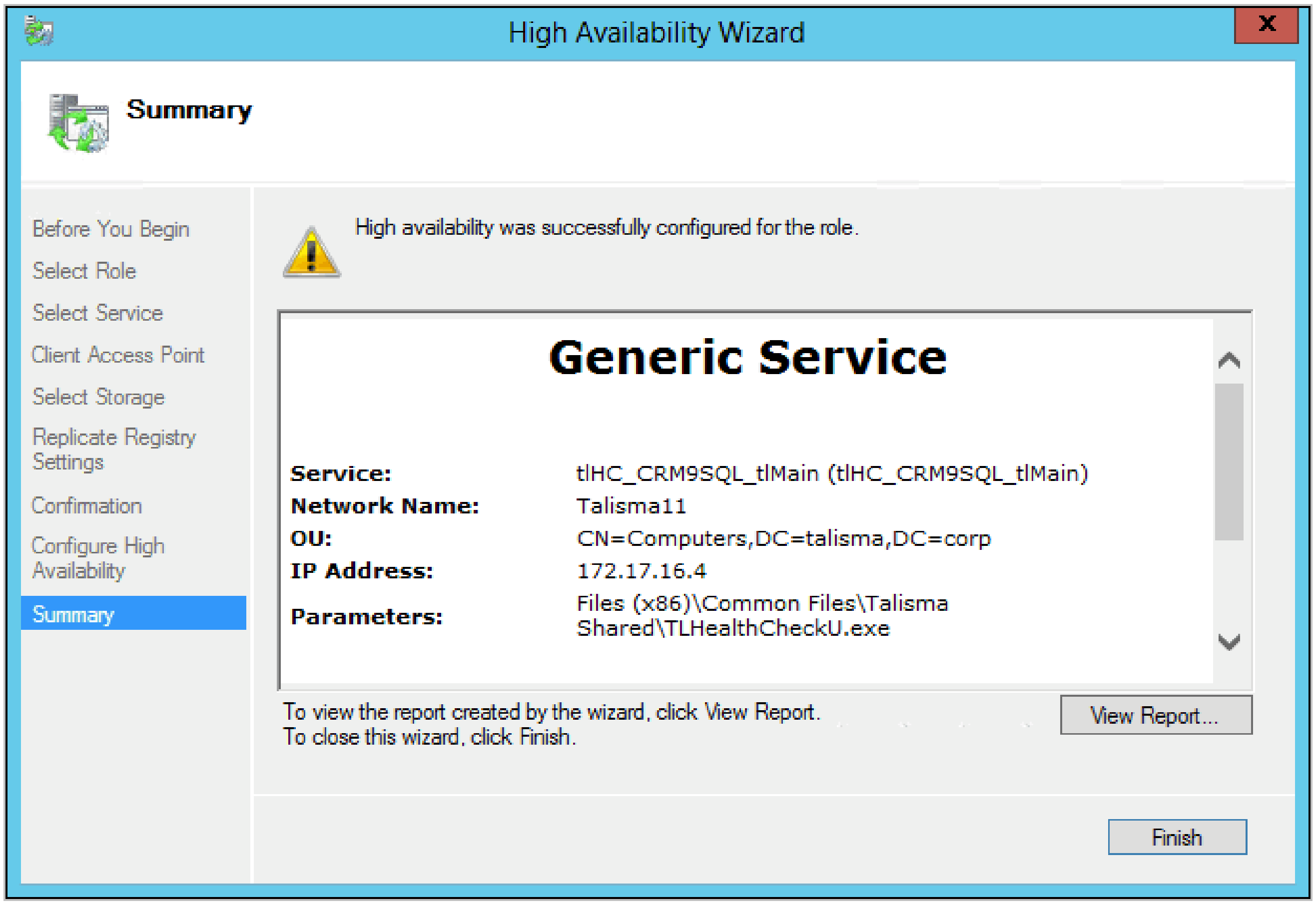


12. Click **Next**.

    The Configure High Availability window is displayed and the process of configuring High Availability begins.

13. Click **Next**.

    The Summary page is displayed. Click on the **View Report** button to view the report of the configuration.

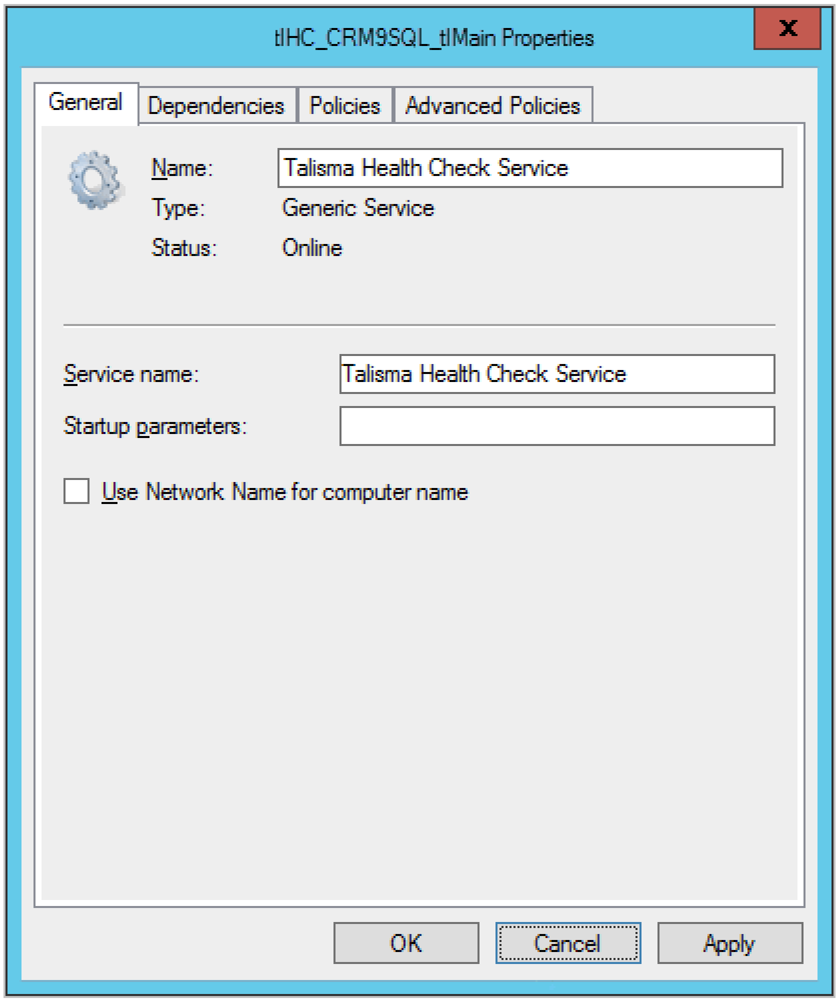


14. Click **Finish**.

    The Talisma Health Check Service is added as a Cluster Resource and is displayed in the right pane of the Failover Cluster Manager window. By default, the status of the Resource is **Offline**.

15. In the Failover Cluster Manager window, right-click **<tlHC_SQLVirtualName>_<MainDatabaseName>** and select Properties.

    The **<tlHC_SQLVirtualName>_<MainDatabaseName>** window is displayed.



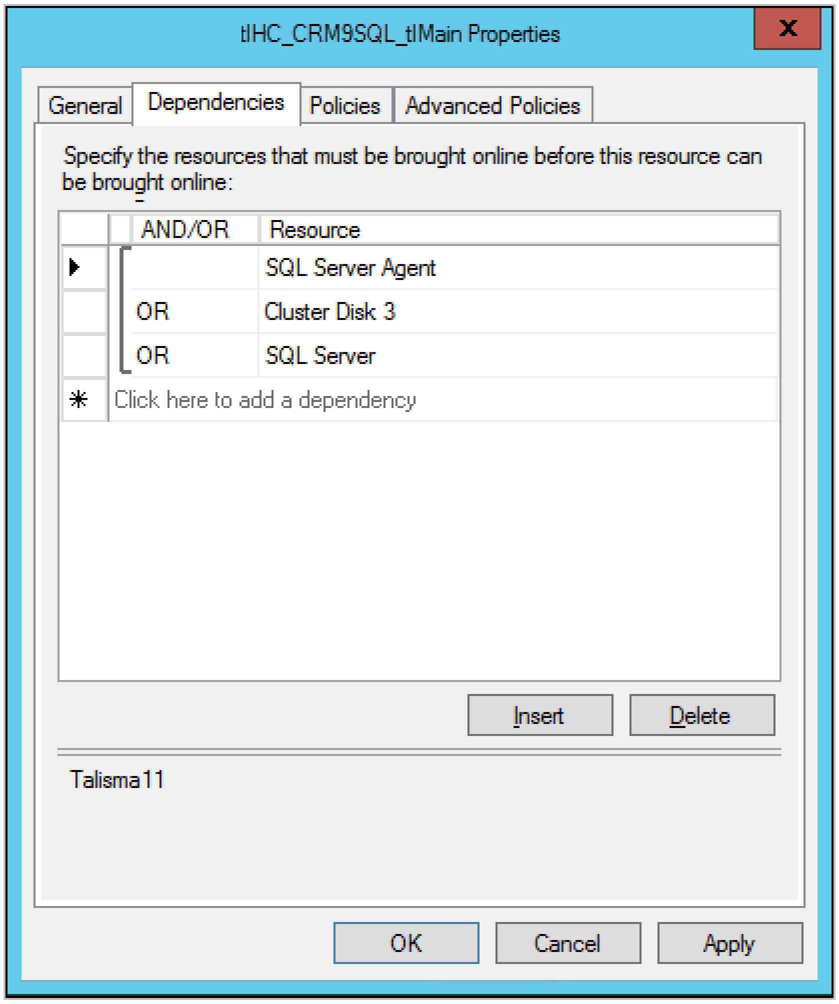
16. In the **General** tab, perform the following steps:

    a. Type **Talisma Health Check Service** in the **Name** and **Service name** fields.

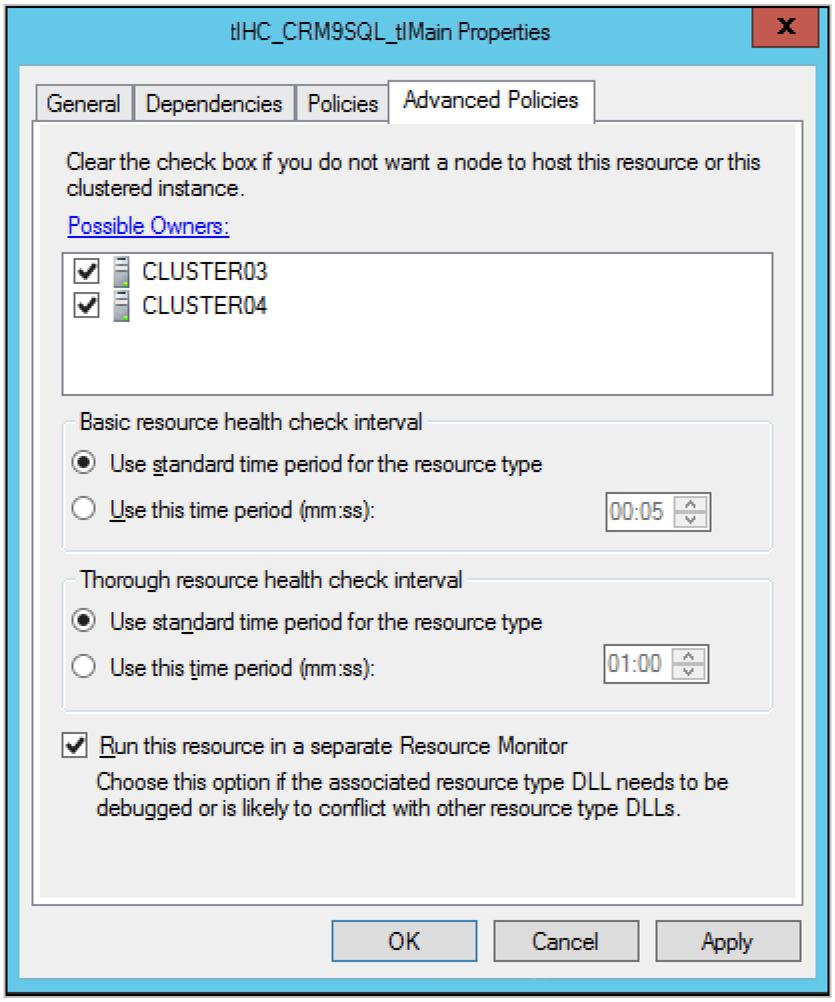
    b. Delete the value in the **Startup parameters** field.

    c. Clear the selection of the **Use Network Name for computer name** option. By default, this option is selected.

17. In the **Dependencies** tab, add **SQL Server**, **SQL Server Agent**, and **Cluster Disk 1** in the Resource column.



18. In the **Advanced Policies** tab, select the **Run this resource in a separate Resource Monitor** option.



19. Click **OK** in the Talisma Health Check Service Properties page.

    The Failover Cluster Manager is displayed.

20. In the Failover Cluster Manager, right-click **Talisma Health Check Service** and select **Bring this resource online** from the shortcut menu.

    The Service is set to the **Online** state.

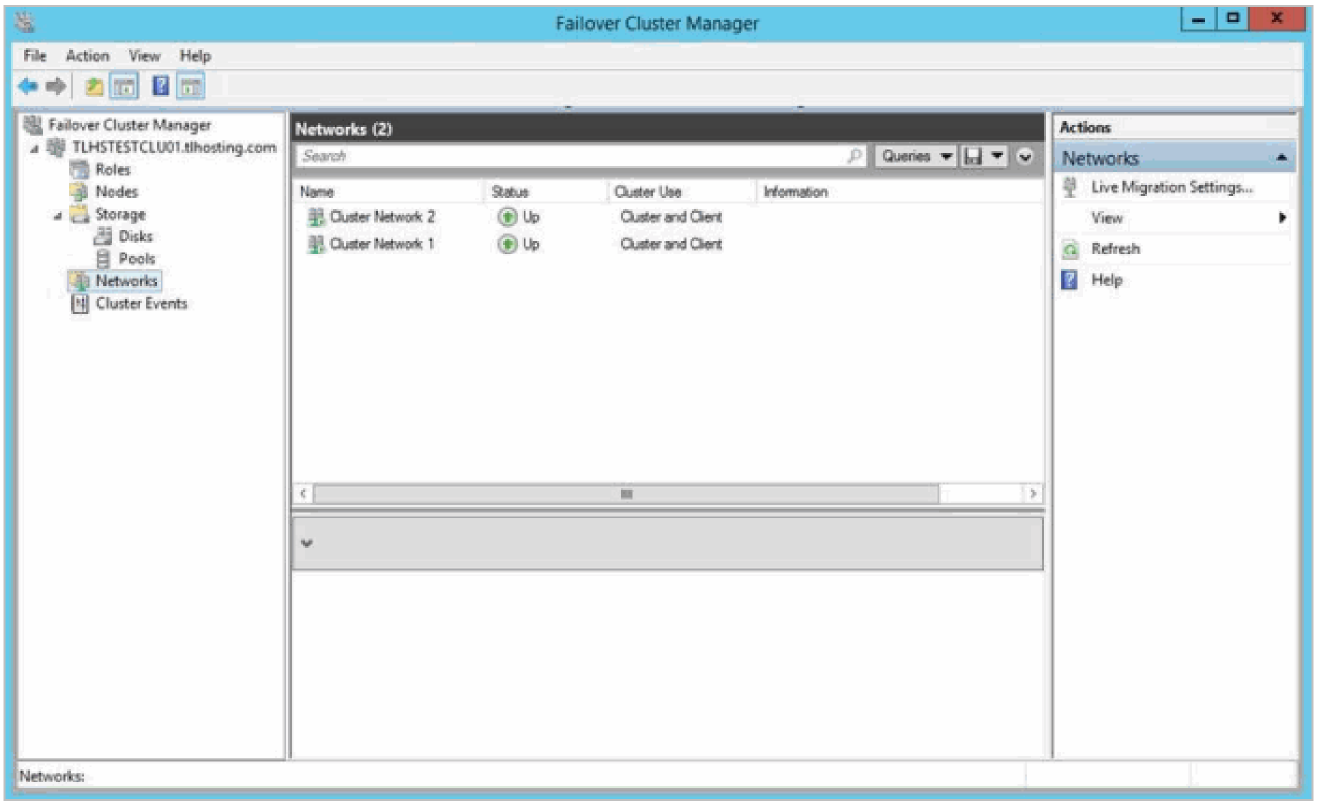
Opening and Viewing the Failover Cluster Manager

To open the Failover Cluster Manager and view the details, perform the following steps:

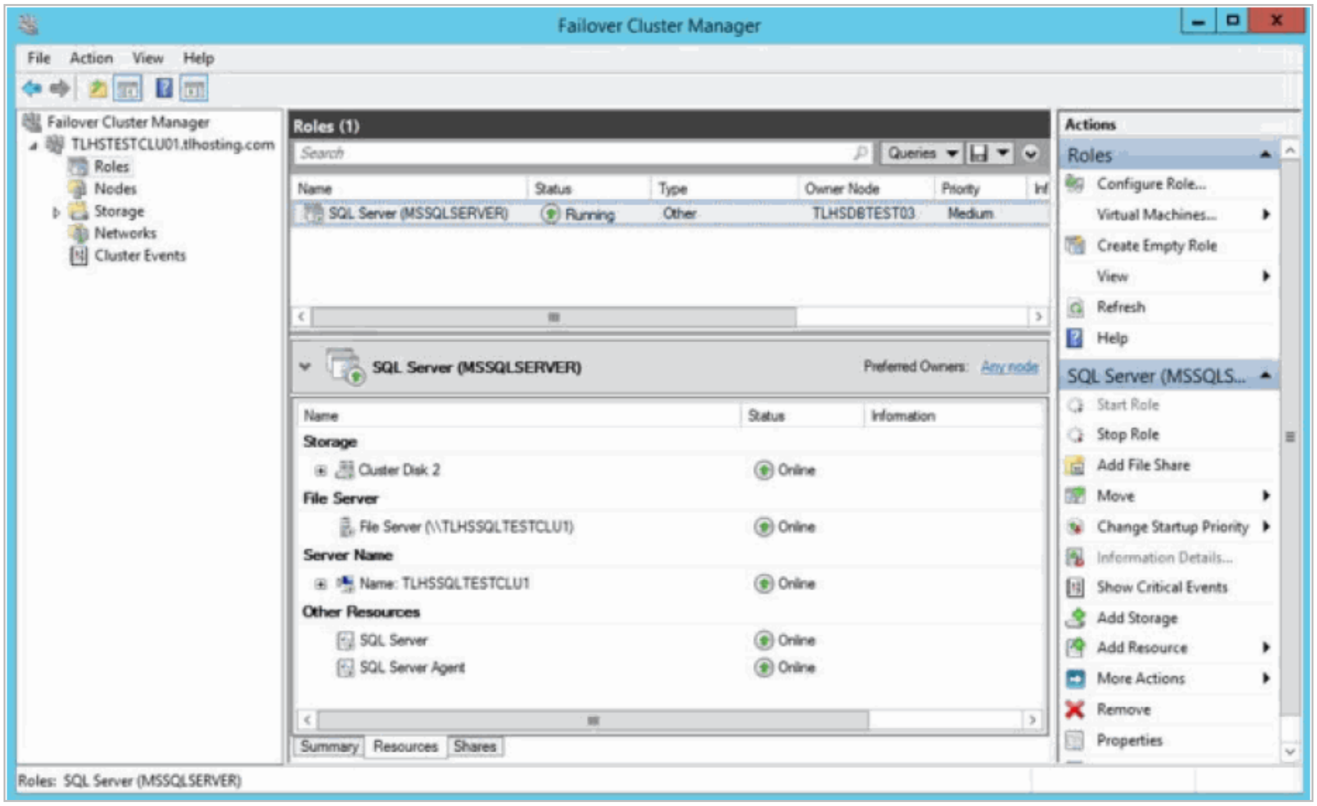
1. From the **Start** menu, open **Failover Cluster Manager**.

   The Failover Cluster Manager is displayed.

2. Click **<Virtual Cluster Name>.<Domain Name>.com\Networks** in the left pane to view the network details.



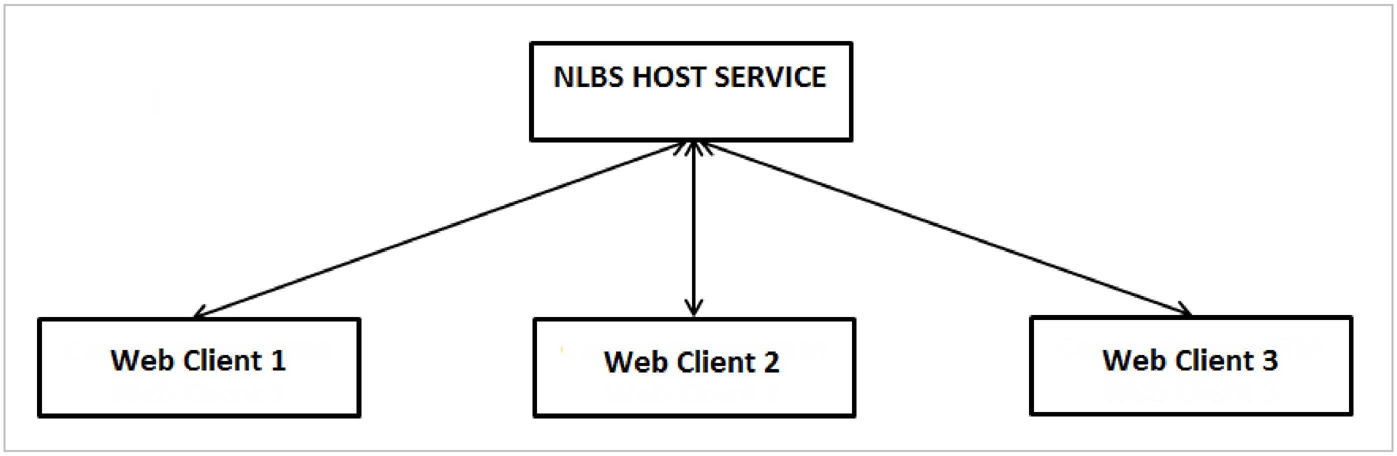
3. Click **<Virtual Cluster Name>.<Domain Name>.com\Roles** in the left pane to view details of the Roles.



Configure the Web Client in an NLBS Environment

The Web Client is supported to work in a Network Load Balancing Services (NLBS) environment. This article describes steps that are required to configure Web Client in an NLBS environment. When NLBS is implemented, the configuration ensures that requests received in multiple Web Client computers are distributed and the load is balanced across all computers.

The configuration requires that multiple Web Client computers must all be connected to a computer on which the NLBS service is hosted. The following figure illustrates this configuration:



In this scenario, user requests are routed to different Web Client computers to ensure that the load is balanced among all computers.

Prerequisites

The same STS certificate must be installed on the NLBS service host computer and the Web Client computers.

Modify Configuration in the Web.config File

In the Web.config file, modify configurations as indicated in this section on each Web Client computer. The Web.-config file is available in the following paths

- <system drive>:\inetpub\wwwroot\cmc.crm.workspaces - The Web.config file in this path is applicable to Web Client on a Windows computer.

Navigate to the indicated code snippets and change the highlighted code to its modified value.

Make the following configuration changes in the Web.config file that is applicable to Web Client on a Windows computer. The text in red must be replaced with the NLBS configured URL.

- <add key="issuer" value="https://Staff STS URL/Identity/connect/token"/> -- The Staff STS URL. The above URL must not be changed unless Staff STS is in NLBS mode.

<add key="realm" value="http://<Web Client URL>/"/> -- This is the Workspace URL.

- <add key="OAuthEndPoint" value="https://Staff StS URL/Identity/connect/token"/>

The above URL must not be changed unless Staff STS is in NLBS mode.

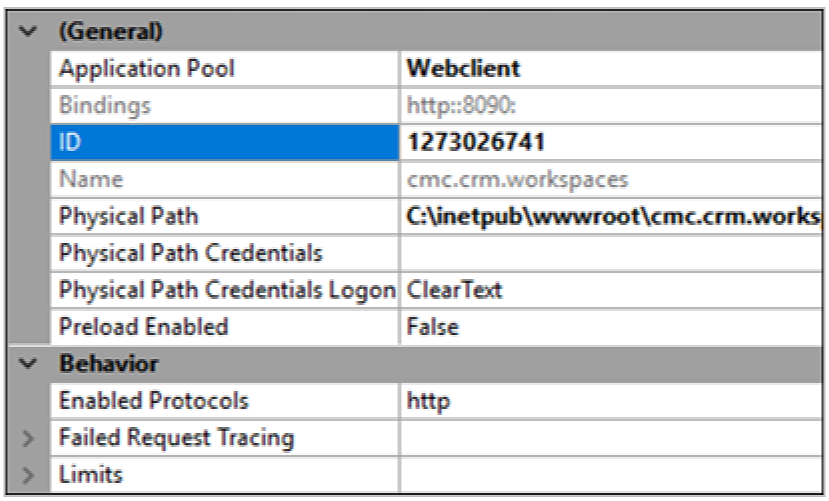
Note: After the code changes are saved, perform these steps on the following node on each Web Client computer:

- cmc.crm.workspaces

1. In the Internet Information Services Manager (IIS), click the node in the Connections pane.
2. In the right pane, double-click **Machine Key**.

   In the **Validation key** and **Decryption key** areas, clear the following option:

   - Automatically generate at runtime
3. Click **Generate Keys** in the Actions pane. Key values are generated in the **Validation key** and **Decryption key** areas. Copy these keys and apply then on all Web Client computers which are participating in the NLBS configuration. Across all Web Client computers, ensure that values are identical in both areas.
4. In the Advanced Settings dialog (click the Web Client website in the Connections pane and then click **Advanced Settings** in the Action pane), the value in the ID field must be identical in the NLBS nodes:



Setting Up Non-Sticky Support

Non-sticky support in an NLBS environment is efficient and speeds up communication because Web Client resources are optimally utilized and scale up appropriately. Non-sticky support can be configured in IIS and Azure environments. To enable non-sticky support, make the following changes to the Web.config file that is available in the path <system drive>:\inetpub\wwwroot\cmc.crm.workspaces.

When Web Client is Hosted on an IIS Web Server

1. Navigate to the following code in the **Web.config** file:

   <sessionState mode="InProc" stateConnectionString="tcpip=<web client>:42424" sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes" cookieless="false" timeout="20" />

2. Ensure that the value of the **sessionState mode** parameter is changed from **InProc** to **StateServer**. Make this change on all computers where Web Client is installed.

3. A single instance of the ASP.Net State service is required to run across all Web Client computers. On computers where the service is not running, in the **Web.config** file replace the text <web client> (in the tcpip parameter of sessionState) with the name of the Web Client computer where the service is running.

4. Navigate to the following code:

   <add key="AttachmentSharedFolder" value=”” />

   Update the value field with the network path where attachments will be saved.

5. Save the **Web.config** file.

Where Web Client is Hosted in an Azure Environment

1. Navigate to the following code in the **Web.config** file:

   <add key="AttachmentSharedFolder" value="" />

   <add key="AzureStorageAccountName" value="" />

   <add key="AzureStorageKey" value="" />

   Specify appropriate values for the following parameters:

   - AttachmentSharedFolder: The Web Client attachments Azure storage folder path
   - AzureStorageAccountName: The user name to access the Azure storage location
   - AzureStorageKey – the password to the Azure storage location

2. Uncomment configuration 1 and comment configuration 2:

   Configuration 1

   <!--<sessionState mode="Custom" customProvider="MySessionStateStore">

   <providers>

   Configuration 2

   <!-- <sessionState mode="InProc" stateConnectionString="tcpip=127.0.0.1:42424" sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes" cookieless="false" timeout="20" />

   -->

3. Locate the following code and specify values for the indicated parameters:

   <add name="MySessionStateStore" type="Microsoft.Web.Redis.RedisSessionStateProvider" host="" accessKey="" ssl="false" port="" />

   </providers>

</sessionState>

- Host: The name of the redis computer
- accessKey: Type the key value
- port: Port that will be accessed by redis

4. Save the **Web.config** file.

On the ASP.NET State Server:

1. If the sessionstate request does not communicate with the sessionstate service in a load-balanced environment even if the "Windows Firewall" is disabled or it’s turned on and the TCP port is enabled through inbound rules, update the “AllowRemoteConnection” registry key value from 0 to 1 on the session-state server where the "ASP.NET state” service is running. It must be updated in the following path to accept remote requests:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\aspnet_state\Parameters\AllowRemoteConnection

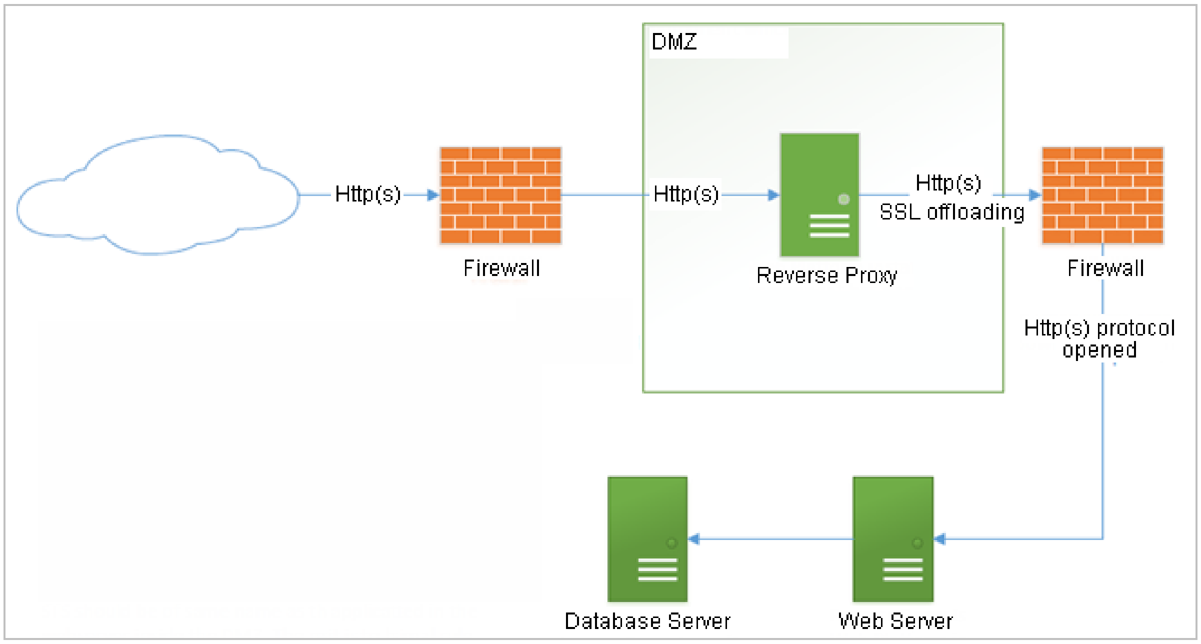
2. The **Startup Type** value of the **ASP.NET state service** Windows service must be set to **Automatic**.

Important: Ensure that Web Client and other components (in Azure – IaaS) all have identical time zone settings.

Host the Web Client in a DMZ

This article describes the manual steps that must be performed to enable users to connect to Web Client on a reverse proxy server that is hosted in a Demilitarized Zone (DMZ).

The reverse proxy server must be configured using the URL Rewrite component, which can be downloaded using Web Platform Installer, and is available in IIS Manager. The URL Rewrite component is dependent on Application Request Routing (ARR), a component that is downloaded along with URL Rewrite.



The Web Client hosted in the DMZ must have the same name as the Web Client installation hosted inside the network (and behind the firewall). The identical names ensure that minimal processing and configuration is required to configure rewrite rules using the URL Rewrite component. Further, it is not required to install Web Client (and STS) or create Web Client and STS-specific folders on the reverse proxy server.

Configurations on Web Client Installed inside the network:

1. Navigate to the following code in the **web.config** file and update the parameters in angular brackets with appropriate values:

   <audienceUris>

   <add value-
   ="h-
   ttp://<Re-
   verseProxyWeb-
   siteName>:<ReverseProxyPortNumber>/<ReverseProxyServerWebclientApplicationName>/" />

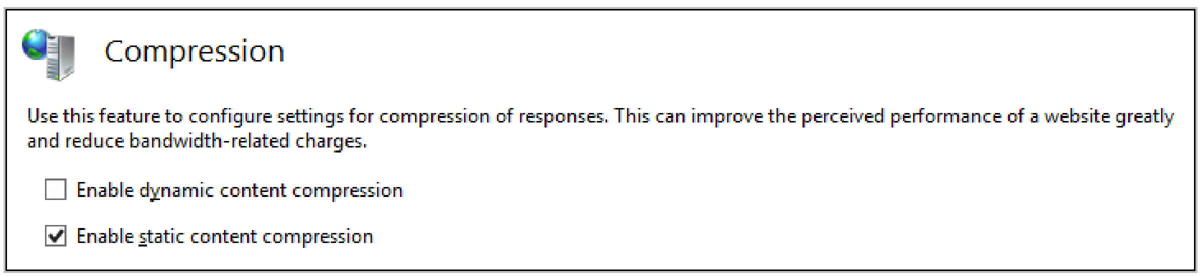
   </audienceUris>

<wsFederation passiveRedirectEnabled="true" issuer-
="h-
ttp://<Re-
verseProxyWeb-
siteName>:<ReverseProxyPortNumber>/<ReverseProxyServerWebclientSTSApplicationName>"
realm-
="h-
ttp://<Re-
verseProxyWeb-
siteName>:<ReverseProxyPortNumber>/<ReverseProxyServerWebclientApplicationName>/"
requireHttps="false" />

2. Save and close the **web.config** file.

3. In the IIS Manager, double-click **Compression** and then clear the **Enable dynamic content compression** option.

   Perform the above steps on the STS Component also.

   Save your changes in IIS Manager.

   Reverse Proxy Server Configuration

   After configuring Web Client & STS Application in IIS, configure the following:

4. Create a Rule to Enable SSL for Web Client

   On the reverse proxy website, create two server variables - HTTPS and HTTP_X_FORWARDED_PROTO (if a load balancer is available).

   a. Click the URL Rewrite option in IIS Manager.

   b. In the **Actions** menu in the right pane, click the **View Server Variables** link and then click **Add** to add the server variables indicated above.

5. Add a new Inbound Rule

   The inbound rule adds the HTTPS header to enable forms authentication to work correctly with SSL.

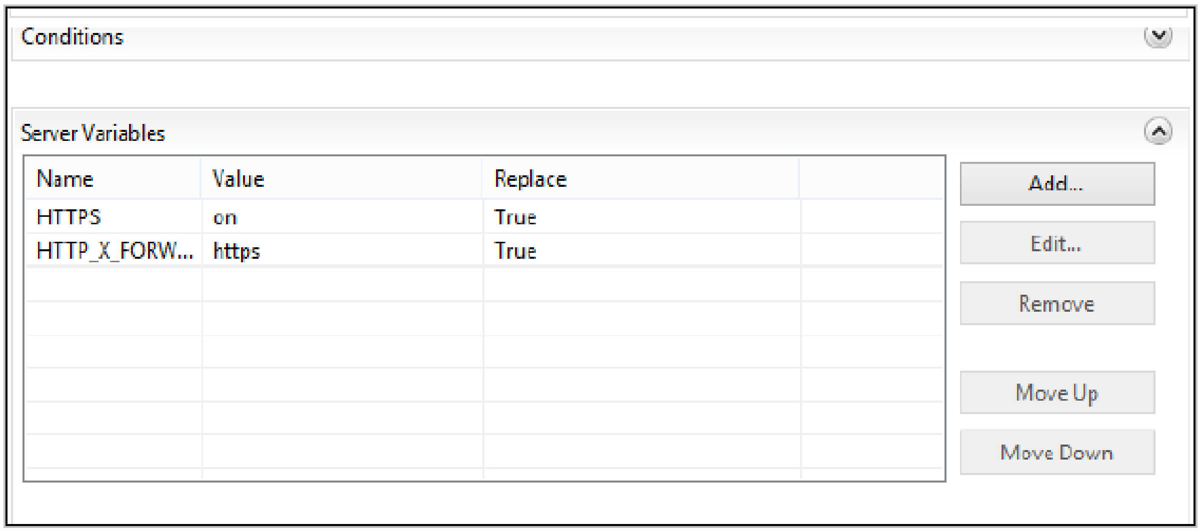
a. In the Actions pane on the right, click **Add Rules**. The Add Rule(s) dialog box is displayed.

b. Select **Blank rule** and click **OK**. The Edit Inbound Rule page is displayed.

c. In the **Name** field, type a name that uniquely identifies the rule.

d. In the **Pattern** field, type .*. This ensures that any call that is routed through the reverse proxy website has the HTTPS header set correctly.

e. Under **Conditions**, set the server variables that were defined earlier. See the following figure:



f. In the **Action Type** list, set the value **None**. This procedure completes the setting of the server variable.

6. Create an Inbound Rule to Match any Pattern

a. Perform the steps described in step 5 (ignore step e). However, in the **Pattern** field, type the value (.*). This ensures that any request can land on the website.

b. In the **Action type** list, select the value **Rewrite**.

c. In the **Rewrite URL** field, type the URL of the Web Client website located inside the network where the request needs to be routed and suffix the URL with {R:1}. This ensures that subfolders, if any, are also mapped and routed appropriately.

d. As query string is used in Web Client, WebAPI and XMLHttp request calls, ensure that the **Append query string** option is selected.

e. Ensure that the rule is stopped after processing so that additional rules, if any, are not processed. To do so, select the option **Stop processing of subsequent rules**.

7. On the reverse proxy computer, create individual virtual directories for Web Client and STS. The names of these directories must match with virtual directory names on the computer where Web Client is installed.

Save your changes in IIS Manager.

Deploy Multiple Web Client Instances on the Same Computer

Install an instance of Web Client and Web Notification Server from Installation Manager. For more information on the installation process, see Installation Manager Help. Perform the following tasks after the installation is complete.

A typical Web Client Installation requires the following components:

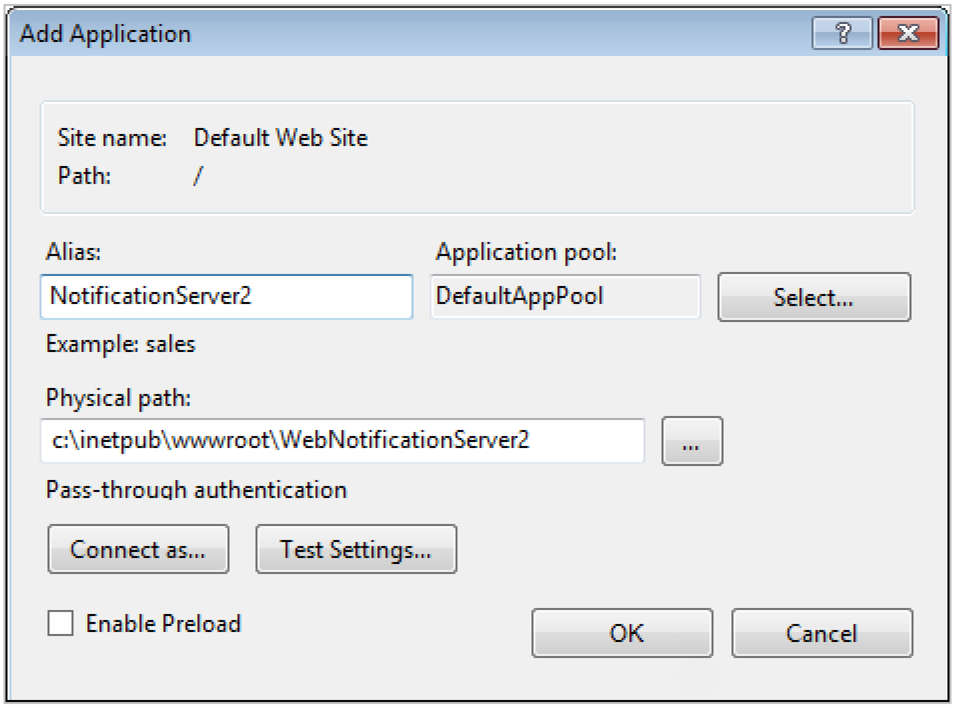
- Web Notification Server
- Windows Notification Service
- Cmc.Crm.Workspaces
- Staff STS
- Security Web Service

To install a second instance of Web Client to connect to a different database on the same computer, the components must be recreated manually.

Host the Web Notification Server in IIS

1. Copy the Web Notification Server installation folder to a desired location.
2. In IIS, host this folder as a Web Application. In the Default Web Site's context menu, select **Add Application**.
3. In the Add Application dialog box, specify the alias of your choice in the **Alias** field and then select the required application pool. Ensure that you select an application pool of type .Net 4.5 in integrated mode.
4. In the **Physical path** field, specify the folder path where the files will be copied.

   Note: The application pool must be configured for a user with administrator privileges.



5. Click **OK**.

Update the Web.config File

1. In the **Web.config** file that is available in the new Web Notification Server installation folder, navigate to the following code:

   <client>

   <endpoint address="net.tcp://localhost:**8083**/TLWebNtfSvr/NotificationRequestService" binding="netTcpBinding" bindingConfiguration="NetTcpBinding_IRequestNotification" contract="WebNtnRequestService.IRequestNotification" name="NetTcpBinding_IRequestNotification" />

   </client>

2. Change the port (bold text) to an unused port address.
3. Save and close the file.

Create Another Instance of Windows Notification Service

1. Create a copy of the WebNotificationService installation folder to a desired location.
2. Launch the command prompt window with administrator rights.
3. Type the following command:

sc create <Web Notification Service Name> binPath-
h="\"<WebNotificationServiceInstallFolder>\TLWebNtfSvr.exe\"" DisplayName="<Web Notification Service display name>".

4. Replace **<Web Notification Service Name>** and **<Web Notification Service display name>** with names of your choice. Ensure that the specified text is not used by any other windows service on the computer.

5. Replace **<WebNotificationServiceInstallFolder>** with the folder path created in step 1, and then press ENTER. The new service will be displayed in the Service window.

6. Right-click the service and set the following configurations:

   a. In the General tab: Configure the Startup type to Automatic

   b. In the Log On tab: set appropriate log on credentials.

Configure the TLWebNtfSvr.exe.config File

1. In the new Web Notification Service folder, open the **TLWebNtfSvr.exe.config** file and navigate to the following code:

   <service name="TLWebNtfSvr.Service.NotificationRequestService" behaviorConfiguration="TLWebNtfSvrBehavior">

   <endpoint address="net.tcp://localhost:**8083**/TLWebNtfSvr/NotificationRequestService" binding="netTcpBinding" bindingConfiguration="PlainNotification" contract="TLWebNtfSvr.Interface.IRequestNotification" />

   <endpoint address="mex" binding="mexTcpBinding" bindingConfiguration="" contract="IMetadataExchange" />

   <host>

   <baseAddresses>

   <add baseAddress="net.tcp://localhost:**8083**/TLWebNtfSvr/NotificationRequestService" />

   </baseAddresses>

   </host>

   </service>

2. Change port 8083 (bold text) to the port used to configure the Web.config file of the of Web Notification Service.

3. Navigate to the following code:

<service name="TLWebNtfSvr.Service.NotificationPostService" behaviorConfiguration="TLWebNtfSvrBehavior">

<endpoint name="netTcp" address="net.tcp://localhost:**8082**/TLWebNtfSvr/NotificationPostService" binding="netTcpBinding" bindingConfiguration="PlainNotification" contract="TLWebNtfSvr.Interface.IPostNotification" />

<endpoint name="mexTcp" address="mex" binding="mexTcpBinding" bindingConfiguration="" contract="IMetadataExchange" />

<host>

<baseAddresses>

<add baseAddress="net.tcp://localhost:8082/TLWebNtfSvr/NotificationPostService" />

</baseAddresses>

</host>

</service>

4. Change port 8082 (bold text) to an unused port.
5. Save and close the file.

Updates in the Notification Service Folder

1. In the new Web Notification Service folder, locate the Web.config file.
2. Perform the steps described in Configure the Web.config File.

Configure the Web.config File

1. Run the following query on the Main Database computer to fetch the internal user details.

   Select tLoginName, tPassword from tblTlDataBases where nDBID = 1

   Note the user name and password returned from this query.

2. Open the **Web.config** file in a text editor and navigate to the following code:

   <appSettings>
   <add key="ServerConfig" value="**<Server>**" />
   <add key="userName" value="TalismaAdmin" />
   </appSettings>

3. Replace the value of **<Server>** with the server you need to connect to.
4. Navigate to the following code:

   <connectionStrings>

<add name="CrmDbConnection" providerName="System.Data.SqlClient" connectionString="Data Source=**<Server>**;Initial catalog=**<DbName>**;Trusted_ Connection=No;UID=**<UserID>**;PWD=**<Password>**;Connect Timeout=120;Max Pool Size=500;Min Pool Size=0;MultipleActiveResultSets=True" />

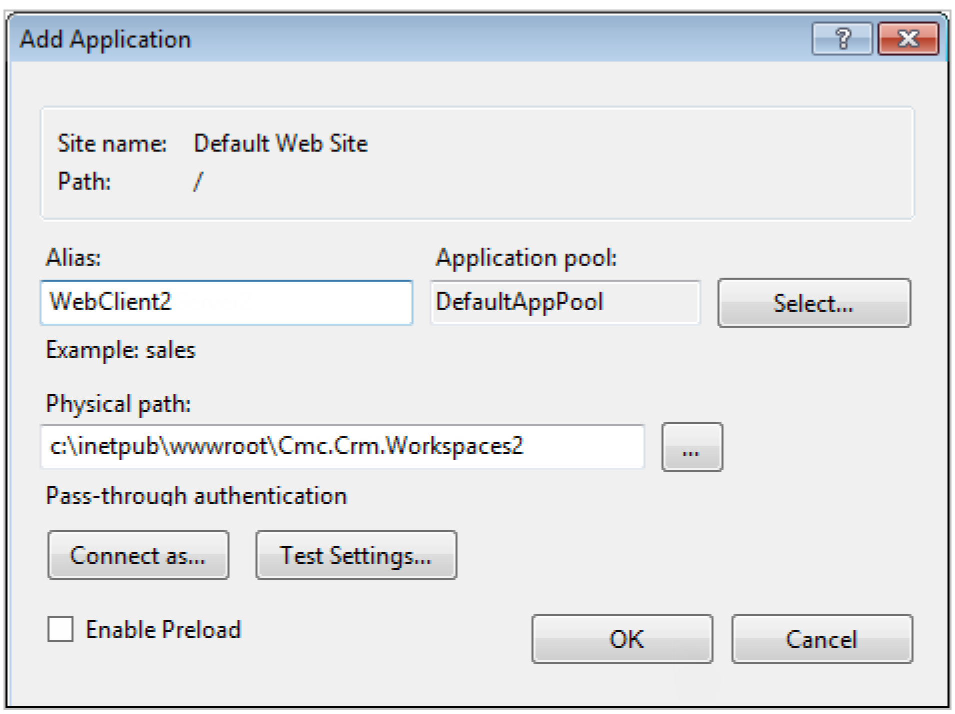
</connectionStrings>

5. Replace the values **< Server>**, **<DbName>**, **< UserID>**, and **< Password>** with appropriate values.
6. Save and close the file
7. Restart the service if it is already running.

Configure the Security Web Service

1. Copy the Security Web Service installation folder to a desired location.
2. In IIS, host this folder as a Web Application. In the site's context menu, select **Add Application**.
3. In the Add Application dialog box, specify the alias of your choice in the **Alias** field and then select the required application pool. Ensure that you select an application pool of type .Net 4.5 in integrated mode.
4. In the **Physical path** field, specify the folder path where the new Security Web Service folder has been copied.

   Note: The application pool must be configured for a user with administrator privileges.



5. Click **OK**.

Updates in the Security Service Web Folder

1. In the new Security Web Service folder, locate the **Web.config** file.
2. Perform the steps described in Configure the Web.config File.

Configure Staff STS

1. Copy the Staff STS installation folder to a desired location.
2. In IIS, host this folder as a website. In the site’s context menu, select **Add Website**.
3. In the Add Website dialog box, specify the site name of your choice in the **Site name** field and then select the required application pool. Ensure that you select an application pool of type .Net 4.5 in integrated mode.
4. In the **Physical path** field, specify the folder path where the new Staff STS folder has been copied.

   Note: The application pool must be configured for a user with administrator privileges.
5. In the **Binding** section, specify an unused port number.
6. Click **OK**.

Configure the Web.config File

1. In the second instance of the Staff STS folder, locate the **Web.config** file.
2. Locate the **SecurityServiceCollection** section in the path **configuration\SecurityServiceConfigSection**.
3. In the key <add name=”CRM” address=”<CRM Security Service URL>”>, replace <CRM Security Service URL> with the URL of the new Security Web Service configured in the previous procedure.
4. Save and close the file.

Configure the Cmc.Crm.Workspaces Application

1. Copy the Cmc.Crm.Workspaces installation folder to a desired location.
2. In IIS, host this folder as a web application. In the Default Web Site’s context menu, select **Add Application**.
3. In the Add Application dialog box, specify the alias of your choice in the **Alias** field and then select the required application pool. Ensure that you select an application pool of type .Net 4.5 in integrated mode.
4. In the **Physical path** field, specify the folder path where the files will be copied.

   Note: The application pool must be configured for a user with administrator privileges.
5. Click **OK**.

Configure the Web.config File

1. Using a text editor, open the **Web.config** file that is available in the new Web Client folder, and navigate to the following code:

   <add key="ServerConfig" value="<**ServerName**>/<**DbName**>" />

2. Replace the value of <**ServerName**> and <**DbName**> with the server and database name that you need to connect to.

3. Navigate to the following section:

   <add key="NotificationServerConfig" value="http://<MachineName>/<**WebNotificationServerAlias**>/NotificationRequest.ashx" />

4. Replace the value of **WebNotificationServerAlias** with the alias used while creating the new Web Notification Server.

5. Navigate to the following section:

   <system.identityModel>

   <identityConfiguration>

   <audienceUris>

   <add value="<**Workspaces URL**>" />

   </audienceUris>

   <issuerNameRegistry type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry, System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089">

   <trustedIssuers>

   <add thumbprint="XXXX" name="STS" />

   </trustedIssuers>

   </issuerNameRegistry>

   </identityConfiguration>

   </system.identityModel>

   <system.identityModel.services>

   <federationConfiguration>

   <wsFederation passiveRedirectEnabled="true" requireHttps="false" issuer="<**Staff STS Url**>" realm="<**Workspaces URL**>" />

   <cookieHandler requireSsl="false" />

   </federationConfiguration>

   </system.identityModel.services>

6. Replace the <**Workspaces URL**> with the new Web Client URL and <**Staff STS URL**> with the new Staff STS URL configured previously.

7. Save and close the file.

Updates in the Web Client Folder

1. In the second instance of the Web Client folder, locate the **Web.config** file.
2. Perform the steps described in Configuring the Web.config File.

Sproc_CreateMetaForAllSetup Stored Procedure – Upgrade Issues

In upgraded CampusNexus CRM environments, administrators may encounter scenarios where new out-of-the-box entities such as objects, tabs, groups, properties or relationships are not created. Administrators must view upgrade setup logs to identify a list of these missing entities.

Onsite administrators and CampusNexus CRM support staff (including Hosting and Professional Services) and are encouraged to run the stored procedure as a first step to resolve such upgrade issues.

Resolution

Administrators must run the **sproc_CreateMetaForAllSetup** stored procedure on the Main database computer; it identifies and creates the missing information.

While the stored procedure is not designed to resolve all upgrade issues, it attempts to create the missing entities. If a missing entity fails to be created again, the stored procedure returns a reason that describes the failure.

Before running the stored procedure, administrators must ensure that:

- Database replication is complete
- The SQL Server agent service is stopped on the subscriber and Main database computers

Enable Custom Security in CampusNexus CRM

To enable custom security, work with the following files. The generation of these files is described in the **Custom Security** book in Database Administrator Help.

- **CustomComponent.dll** – This file is the COM interface described in the topic **About Custom Security**.
- **TalismaPublic.txt** – The public key that is generated. This is described in the topic **Generating Cryptography Keys for the Login Component**.
- **CustomerPrivate.txt** – The private key that is generated. This is described in the topic **Generating Private and Public Keys for the Custom Component**.

Desktop Client

As Desktop Client is a 32-bit application, the 32-bit version of the file **CustomComponent.dll** needs to be used.

Copy the following files into the Desktop Client installation folder:

- CustomComponent.dll (32-bit version)
- TalismaPublic.txt
- CustomerPrivate.txt

At the command prompt, register the CustomComponent.dll file using the regsvr32 command.

Business Administrator

As Business Administrator is a 64-bit application, the 64-bit version of the file **CustomComponent.dll** needs to be used.

On the computer where Business Administrator is installed, copy the following files to the path **<system drive>:\Program Files\Common Files\Talisma Shared**:

- CustomComponent.dll (64-bit version)
- TalismaPublic.txt
- CustomerPrivate.txt

At the command prompt, register the CustomComponent.dll file using the regsvr32 command.

Database Administrator

As Database Administrator is a 64-bit application, the 64-bit version of the file **CustomComponent.dll** needs to be used.

On the computer where Database Administrator is installed, copy the following files to the path **<system drive>>:\Program Files\Common Files\Talisma Shared**:

- CustomComponent.dll (64-bit version)
- TalismaPublic.txt
- CustomerPrivate.txt

At the command prompt, register the CustomComponent.dll file using the regsvr32 command.

Web Client

Web Client is authenticated through the Staff Authentication Service. Custom security logic is also in-built into the Staff Authentication Service. The following files must be copied in the bin folder where the Staff Authentication Service is installed:

- CustomComponent.dll (64-bit version)
- TalismaPublic.txt
- CustomerPrivate.txt

At the command prompt, register the **CustomComponent.dll** file using the regsvr32 command.

Customize the Web Client URL

Typically, Web Client is accessible through a URL that uses name of the computer where the Web Server is installed. This topic describes how Web Client can be accessible from a host name instead of the computer name.

Open the Web.Config file of Web Client in a text editor and make the following code changes:

Code	Changes
<audienceUris> <add value="http://COMPUTER.campusmgmt.com/cmc.crm.workspaces/" /> </audienceUris>	Change the text in red to the host name of the Web Client computer.
<federationConfiguration><wsFederation passiveRedirectEnabled="true" requireHttps="false" issuer-r="https://COMPUTER.campusmgmt.com:91/" realm="http:// COMPUTER1.campusmgmt.com/cmc.crm.workspaces/" /><cookieHandler requireSsl-l="false" /></federationConfiguration>	• Change the first instance of the red text to the host name of the STAFF STS computer. • Change the second instance to the host name of the Web Client computer.
<add key="NotificationServerConfig" value="http:// COMPUTER.campusmgmt.com/NotificationServer1/NotificationRequest.ashx" />	Change the text in red to the host name of the Web Notification Server computer.

Ports Used by CRM

The following table lists the ports used by CampusNexus CRM components.

Used Ports

Port Definition	Port Number
MSSQL Server	1433
MSSQL Monitor	1434
DCOM/RPC	135
DNS	53
HTTP	80
HTTPS	443
File Sharing	445, 139
SMTP (non-encrypted/TLS)	25
SMTP (SSL)	465
POP3 (non-encrypted/TLS)	110
POP3 (SSL)	995
IMAP (non-encrypted/TLS)	143
IMAP (SSL)	993
LDAP	389
Default dynamic port range	49152 - 65535

Notes:

1. During installation of CampusNexus CRM components, file and printer sharing must be enabled. Additionally, all ports must be opened bi-directionally between all servers.
2. The DNS port must be open on the DNS Server for name resolution.
3. Print Template services require access to port 445 to access the network path where merged Print Templates are saved.

Port Matrix

To view the Port Matrix in Microsoft Excel, click here.

Note: If the Excel file is not opened in your browser, right-click the link and select **Save target as**.

Using a Different Port for Web Components

By default, port 80 is used to connect to Business Administrator from Client. You can modify this setting.

In the **tbltlwebservers** table, modify the values of the **tmachinename** fields for the **tName** properties that have the Web Server name for Business Administrator. Specify the port to be used to connect to Business Administrator in the following format:

```
http://<computername>:PortNumber>/
```

Example

If Business Administrator is installed on the **Talisma109** computer, and the user must connect to it using port 2222, modify the entry in the **tmachinename** field for Business Administrator to http://Talisma109:2222. When a user selects Business Administrator in the **GoTo** menu in Client, the user will be connected to Business Administrator using port 2222.

A user can also connect to Business Administrator using the required port, by specifying the URL of the component in the following format:

```
http://<computername:Portnumber>/<Name of Web Component>/
```

CRM Jobs on SQL Server

A number of Jobs related to CampusNexus CRM are created on the SQL Server on which CampusNexus CRM is installed.

Interaction-related Jobs

Interaction-related Jobs

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Threader	sproc_ addjob_Threader	sproc_threader	DB-spe- cific	Every 15 minutes	Main threading task
Talisma- AutoAssignAllTeams	sproc_ CreateAutoAssign JobAllTeams	Exec sproc_Auto AssignAllTeams	-	Every 15 minutes	Load balances all open Interactions belonging to the current Team in the mailbox. This is for users who are currently logged on
Talisma-AutoAssign- RoundRobin	sproc_Create AutoAssignJobRR	Exec sproc_Auto AssignRR	-	Every 15 minutes (starts at 0005 hrs)	Load balances all open Interactions belonging to the current Team in the mailbox. This is for users who are currently logged on

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-AutoSuggest GUIDTeam#TeamID Team wise: Talisma-AutoSuggestAllTeams	sproc_Create AutoSuggestJob sproc_Create AutoSuggest JobAllTeams	Exec sproc_Auto Suggest nTeamID Exec sproc_Auto Suggest	Team specific	Every 15 minutes	Updates the Canned Responses applicable to an Interaction based on the team to which it belongs, and on the Canned Responses belonging to the Team. Additional Information Common job that performs this operation for all Teams added - either Team-specific, or common jobs can be enabled. Default: allteam job enabled

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-PrioritizeGUID Team#TeamID Team wise: Talisma-PrioritizeAllTeams	sproc_Create AutoSuggest JobAllTeams	Exec sproc_ Prioritize 0 (from trigger = false), nTeamID Exec sproc_ Prioritize AllTeams	Team-specific	Every 15 minutes	Updates the Canned Responses applicable to an Interaction based on the Team to which it belongs, and on the Canned Responses belonging to the Team. Additional Information Common job which will perform this operation for all Teams added - either Team specific, or common job can be enabled. Default: allteam job enabled
Auto Response	sproc_addjob_ AutoResponse	exec [Talisma020209]. dbo.sproc_Start AutoResponse	DB-specific	Once daily	Handles AutoResponses instead of the Threader. Not in use now.
Auto Age	sproc_ addjob_AutoAge	exec sproc_ AutoAge	DB-specific	Once daily	Ages the Interactions by a day

Report-related Jobs

Report-related Jobs

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma Report Schedule	sproc_CreateJob ForSchedule	Exec sproc_Run-Scheduled Report nScheduleID	-	As specified by the user	-

Job Name	File Name	Steps	Type	Frequency	Purpose
Run Queued Reports Jobs	sproc_AddJob_ RunQueuedReports	Exec sproc_Run-BkGround RptsForUserSet 10,4	Only on the Reports server. Uses the Analytics DB. Number of jobs is configurable through tblG-lobalInfo. The default number is 10.	Every 10 minutes	Run reports that are requested to be run in the background by users.

Maintenance Jobs

Maintenance Jobs

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Stop Licens-ing	sproc_ addJob StopLicence	exec sproc_ TrialExpire	DB-spe-cific	Every 6 hours	On a trial license, this will dis-able all CampusNexus CRM Jobs, and users will not be able to work with Cam-pusNexus CRM after this.
Talisma-PurgeOldNot-fns	sproc_ AddJob_ PurgeOldNot-fns	exec sproc_ PurgeOldNotfns exec sproc_ PurgeOldChatNotfns	DB-spe-cific	Once daily	Deletes notifications that are older than 15 days. The default value 15 is stored in the PurgeNo-tificationsOlderThanXDays parameter in the tblGlobalInfo table.
Purge Deleted	sproc_ addjob_ PurgeDeleted	exec sproc_ PurgeTalismaObjects	DB-spe-cific	Every 6 hours	Purges deleted Objects (Inter-actions, Orders, and Oppor-tunities) from CampusNexus CRM.
Talisma-Maint	sproc_ addjob_ Maintenance	exec sproc_ Maintenance	DB spe-cific	Once a week (Sunday, 0105 hrs)	Reindexes tables Clean-up of Rule logs Deletes a configured count of phone sessions which do not have associated interactions and that are older than a con-figured number of days.

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Talisma-ChatDB-Maint	sproc_ChatDB Maintenance	exec sproc_ ChatDBMaintenance	-	Once a week (Sunday, 0333 hrs)	-
Talisma-ReportDB-Maint	sproc_ Report_ Maintenance	exec sproc_ Report_Maintenance	-	Once a week	-
Talisma-WebtrackDB-Maint	sproc_WebDB Maintenance	exec sproc_ WebDBMaintenance	-	Once a week	-
Talisma Rep-lication	sproc_ addjob_ Replicate	exec sproc_ ReplicateObjects	-	Automatic (when SQL Server Agents starts)	-
Watchdog Job Talisma-MainDB-Watchdog Talisma-ReportDB-Watchdog Talisma-ChatDB-Watchdog Talisma-WebTrackDB-Watchdog	sproc_ addjob_ Watchdog	exec [Talisma020211]. dbo.sproc_ Watchdog 1 (Main DB) exec [TalismaChat020211]. dbo.sproc_ Watchdog 2 exec [TalRe-port020211]. dbo.sproc_ Watchdog 3 exec [Talisma Web020211]. dbo.sproc_ Watchdog 4	DB-spe-cific	Every 10 minutes (starts at 0003 hrs)	Checks the health of running jobs and verifies whether they are actually running.

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Log Backup Talisma-MainDB-LogBackup Talisma-ChatDB-LogBackup Talisma-ReportDB-LogBackup Talisma-WebTrackDB-LogBackup	sproc_AddBackupJob	Exec sproc_Backup 2, 'Talisma020208', 'Backup Talisma Transaction Log', 1 2) Exec sproc_Backup 2, ' TalismaChat020208', 'Backup Talisma Transaction Log', 2 Exec sproc_Backup 2, 'TalReport020208', 'Backup Talisma Transaction Log', 3 Exec sproc_Backup 2, 'Talisma Web020208', 'Backup Talisma Transaction Log', 4	DB-specific	Every 30 minutes	Takes an incremental backup of the DB based on the Transaction Log. Additional Information Runs every 30 minutes by default, and can be scheduled.
Full Backup Talisma-MainDB-FullBackup Talisma-ChatDB-FullBackup Talisma-ReportDB-FullBackup Talisma-WebTrackDB-FullBackup	sproc_AddBackupJob	Exec sproc_Backup 1, 'Talisma020208', 'Backup TalismaTalisma Talisma Talisma Talisma Database', 1 Exec sproc_Backup 1, 'TalismaChat020208', 'Backup Talisma Database', 2 Exec sproc_Backup 1, 'TalReport020208', 'Backup Talisma Database', 3 Exec sproc_Backup 1, 'Talisma Web020208', 'Backup Talisma Database', 4	DB specific	Once a week (Sunday, 1500 hrs)	Takes a full backup of the DB Additional Information Runs every Sunday. Can be changed using the schedule backup.

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Talisma Trace	sproc_ addjob_ Trace	exec master.dbo.xp_ sqlagent_ monitor “START”	DB specific	Automatic (when SQL Server Agents starts)	Monitors the SQL Agent service.
Talisma-CheckSpace	sproc_ addjob_ CheckSpace	exec sproc_Check-Space	DB specific	Every 6 hours	Checks free space available on all the servers.
Talisma Refrag Job	sproc_ addjob_ Refrag	exec sproc_Refrag On failure of first step, exec sproc_ ToggleJobs 1	Only on the Main server. DB specific.	Once a month (first Sunday, 0333 hrs)	If installed on SQL: • Several tables are reindexed. • Indexes of all CampusNexus CRM tables are defragmented.
Job Talisma toggle jobs	sproc_ addjob_ ToggleJobs	exec sproc_Job ToToggleJobs	Only on the Main server. DB specific.	Once a month (first Sunday, 0400 hrs)	If commented jobs remain commented, this job uncomments such jobs.
Talisma-CreateView	sproc_ addjob_ CreateView	Exec sproc_ Recreate Iden-tityColumnPostSetup Exec sproc_ CreateViewsEx	DB-Specific	Every 15 minutes	If archive is installed, create the identity column if it's not created. If archive is installed, it recreates the views to include data from Archive database for filters.
Talisma-ChatDB-Maint	sproc_ addjob_ ChatDBMaintn	Exec [tlMedia].dbo. sproc_ ChatDBMaintenance	DB-Specific	Occurs every week on Sunday at 03:33:00 AM	Performs basic maintenance activity: • Shrinks the database files • Recreates the index • Clears the rule logs
Talisma-ReportDB-Maint	sproc_ addjob_ ReportMaintn	Exec [tlAnalytics].dbo. sproc_ Report_Maintenance	DB-Specific	Every week on Sunday at 03:33:00 AM	Performs basic maintenance activity • Shrinks the database files • Recreates the index

Import Jobs

Import Jobs

Job Name	File Name	Steps	Type	Frequency	Purpose
Import Threader	sproc_addjob_ ImportThreader	exec sproc_ ImportThreader	-	Once daily (0000 hrs)	Imports mail from any PST file/mail storehouse to CampusNexus CRM.
Import Contact	sproc_addjob_ ImportContact	exec sproc_ UpdateCustDetails update tblImportContactJobDetails set tStepText = N'Completed' update tblImportContactJobDetails set tStepText = N'Failed'	DB specific	Once daily (0000 hrs)	Imports Contacts to CampusNexus CRM.
Talisma-ProcessImportTable	sproc_addjob_ ProcessImportTable	exec [Talisma020209]. dbo.sproc_Check-ImportTasks	DB specific	Automatic (when SQL Server Agents starts)	Updates the records in ImportTables and starts ImportThreader job.

Campaign-related Jobs

Campaign-related Jobs

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Campaign Communication-ProcessTempRecords	sproc_ CreateComm HistoryProcess TempRecordsJob	EXEC sproc_ProcessComm HistoryTempRecords	DB specific	Every day at 00:00:00 hours	This job creates campaign communication records.
Talisma-Check CampaignDispatcher ServiceStatus	sproc_ AddJob_ CheckCampaign DispatcherServiceStatus	Exec sproc_Check-Campaign Dispatcher ServiceStatus	DB specific	Every 30 minutes	Runs the Job for 30 minutes to restart the campaign dispatcher if valid targets are stuck in the table tbloutgoingobms for more than 30 minutes.

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Talisma OBM Error Notification	sproc_ CreateOBM NotificationJob	Exec sproc_Send Noti-ficationForOBMs	DB spe-cific	Every 2 hours	Sends notifications associated with errors in outbound Mailers
Talisma-Campaign-Pro-cessAllCampaigns	sproc_ CreateProcess AllCampaignsJob	Exec sproc_ Pro-cessAllCampaigns	DB spe-cific	Every hour (starts at 0007 hrs)	Processes the activ-ated Campaigns and moves the Targets to the next step in the associated Campaign after the Targets have been processed in that step.
Talisma-Campaign-Pro-cessExportRecords	sproc_ CreateCampaign ExportRecordsJob	Exec sproc_ CreateCampaign ExportRecordsJob	DB spe-cific	Every 30 minutes (starts at 0015 hrs)	After the Targets have been processed, Tar-gets are exported to the file and path spe-cified in the Bulk Export Configuration. **Note**: It is recom-mended to schedule this job 2 hours after the Talisma-Cam-paign-Pro-cessAllCampaigns is processed to ensure all processed Targets are available for export.
Talisma-Campaign-StartUnScheduled	sproc_ CreateStartAll Unscheduled CampaignsJob	Exec sproc_ StartAll Unscheduled Campaigns	DB spe-cific	Every 6 hours (starts at 0200 hrs)	Creates the Targets from Mailing Lists for non-recursive Cam-paigns. Additional Information Also starts when a Campaign is activated, and at the exact time when a Mailing List is scheduled.
Talisma-Campaign-ProcessReplys	sproc_ CreateProcess ReplyJob	Exec sproc_ ProcessReply	DB spe-cific	Every 30 minutes (starts at 0012 hrs)	Process replies sent for Campaigns.

Job Name	File Name	Steps	Type	Fre-quency	Purpose
Talisma-Purge-Campaign Communication	sproc_ AddJob_Purge Campaign Communication	EXEC sproc_ Purge Campaign Communications	DB spe-cific	Every Sunday at 00:00:00 hours	This job purges cam-paign communication records that are older than the count of days specified in the **Purge Campaign Com-munication data older than n days** option in Business Admin-istrator. Orphaned cam-paign communication records are also purged regardless of whether they are older than the specified count of days.
Not applicable	sproc_ Debug SingleCampaign	Exec sproc_ Debug SingleCampaign	DB Spe-cific	As spe-cified by the user	Displays the following details in the tblPro-cessSingleCampaign table: • The ID of the cam-paign • The date and time before which the campaign returned from running the sproc_ DebugSingleCam-paign stored pro-cedure can be processed.

Health Check Jobs

Health Check Job

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Health Check	sproc_ HealthCheck	Exec sproc_ HealthCheck	DB specific. Runs only on Main DB.	Every 5 minutes (starts at 0000 hrs)	Updates Health Check related tables with inform-ation from the DB.

Other Jobs

Other Jobs

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Applic-ationMonitoring	sproc_AddJob_ExecuteAp-pMonitoring	exec dbo.sproc_ExecuteAp-pMonitoring	DB-spe-cific (Main DB)	30 mins	Monitors execution of the following modules: Campaign Dispatchers Job Service Dispatcher Job Service Extractors SMS Dispatchers Templates SMS Campaign Dis-patchers Notification Service
Talisma-TableMonitoring	sproc_AddJob_ExecuteT-ableMonitoring	exec dbo.sproc_ExecuteT-ableMonitoring	DB-spe-cific (Main DB)	60 minutes	Monitors the growth of tables in Main database.
Talisma-ResetCurren tLeadLoadCount	sproc_ResetCur-rent LeadLoadCount	Exec sproc_Reset CurrentLead LoadCount	DB-spe-cific (Main DB)	Every 24 hours	Reset the number of Leads that are assigned using the Weighted Round Robin method.
Talisma-Archive-New	sproc_ ArchiveNew.cql	Exec sproc_ CleanupEventData Exec sproc_ ArchiveNew	DB-spe-cific	Weekly on Sunday at 08:00:00 PM	Move records from Main DB to Archive DB
Talisma-Store SMSDetails	sproc_ StoreSMSDetails	exec sproc_Store SMSDetails @ nDurationInDays = 7 /*One Week*/, @nBatchSize = 500	DB-spe-cific	Weekly on Sunday at 08:00:00 PM	Move records from the tblSMSDetails table to the tblSMSReport table.

Job Name	File Name	Steps	Type	Frequency	Purpose
Timer Based Rule	sproc_addjob_ TimerBasedRule	Declare @dNow as DateTime Set @dNow = GetDate() Exec sprocRun-Scheduled Rules @dNow, 1 Exec sprocSchedule RuleJob @dNow	DB spe-cific	Scheduled by timer based rules.	Fires timer-based rules.
Audit Job	sproc_Create JobForAudit	osql -S “Talisma199” -d “Talisma020208” -E -Q sproc_Pro-cessEvents	DB-spe-cific (Main DB)	Every 15 minutes (starts at 0009 hrs)	Processes the audit events stored in the tem-porary table.
Computed Prop-erty Job	sproc_CreateJob ForCompProp	osql -S “Talisma 199” -d “Talisma 020208” -E -Q Sproc_ ProcessCompProp	DB-spe-cific (Main DB)	Every 15 minutes (starts at 0009 hrs)	Updates the values for computed Properties.
Talisma-Visitor-Purge (WebTrak Data-base)	Sproc_addjob_ VisitorPurgeJob	exec sproc_ PurgeVisitorDB	-	Once daily (0000 hrs)	-
Talisma-CreateView	sproc_addjob_ CreateView	Talisma-CreateView	-	Every 15 minutes	-
Talisma-Main-Medi-aService	sproc_CreateJob ForMe-diaService.cql	exec sprocCheck ServiceTimings N'Talisma020206'	-	Automatic (when the SQL Server Agent starts) Once daily (1200 hrs) The day after install-ation (0000 hrs)	-
Talisma-ClearCrashedRpt-User	sproc_ Clean CrashedUsers.cql	exec sproc_Clean CrashedUsers	-	Once every 5 minutes	-

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Main-CreateDSTDates	sproc_CreateDSTDatesForCurYr.cql	exec Sproc_CreateDSTDatesForCurYr	-	Every year on the first day of the month	Runs at the beginning of every year to generate the DST dates for that year
Talisma-RecuringHolidayConverter	sproc_ScheduleRecuringHolidayConverter.cql sproc_ConvertRecuringHolidaysForAllTeams.cql	[GPP030224]..sproc_ScheduleRecuringHolidayConverter Exec [GPP030224]..sproc_ConvertRecuringHolidaysForAllTeams	-	Updated dynamically.	-

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Media-Cus-tomScript	cus-tompostscript.sql sproc_updateb NewFields.sql cus-tompostscript2.sql	osql -E -S"LOST\I1" -d"tlMedia" -i" C:\Program Files\ Common Files\Talisma Shared\ cus-tompostscript.sql" -o" C:\Program Files\ Common Files\Talisma Shared\ <database name>\ cus-tompostscript.out" Exec sproc_updateb NewFields osql -E -S"LOST\I1" -d "tlMedia" -i" C:\Program Files\ Common Files\Talisma Shared\ cus-tompostscript.sql" -o"C:\Program Files\ Common Files\Talisma Shared\ <database name>\ custompostscript2. out"Exec	DB-spe-cific	Every 30 minutes daily	For adding Microsoft SQL Server fields in the Media DB.
Talisma-Update SchNextRunDate	Sproc_ UpdateSchedule NextRunDate	Exec sproc_Update Sched-uleNextRunDate	-	Occurs every 1 minute	Updates the next run date and time for all schedules
Talisma-Calculate ResponseTime	sproc_ReportCal-culate EventTimeDiffs	exec sproc_Report Cal-culateEventTimeDiff-s	DB Spe-cific (Main DB)	Every 4 hours	Runs sproc_ ReportCal-culateEventTimeDiffs

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-Campaign-Defrag Cam-paignTablesJob	sproc_Defrag CampaignTables	exec sproc_Defrag CampaignTables	DB Spe-cific (Main DB)	Every 30 minutes	Runs scheduled Job to start a specific cam-paign.
Talisma-Cam-paign-AddTar-getsFromFilter	sproc_AddTar-getsTo Cam-paginFromFilter	exec sproc_Add TargetsToCampagin FromFilter	DB Spe-cific (Main DB)	Every 6 hours	Job to add Targets to a Campaign from Filters.
Talisma-Campaign-Pro-cess SendOBM	sproc_Send Out-boundMailerJOB	exec sproc_Send OutboundMailerJOB	DB Spe-cific (Main DB)	Every 30 minutes	A scheduled job to start processing steps with outbound Mailers.
Talisma-Chat-UpdateLoad OnMainDB	sproc_Update LoadOnMainDB	exec Sproc_Update LoadOnMainDB	DB Spe-cific (Media DB)	Every 5 minutes	Updates load from Media to Main DB for Chat requests handled by each user.
Talisma-CleanUp CrashedUsers	sproc_Detect CrashedUsers	exec sproc_Detect CrashedUsers	DB Spe-cific (Main DB)	Every 5 minutes	Used to log out users from Main DB. Users whose login sessions have stopped respond-ing are logged out.

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-CleanUpMail CompTraceInfo	sproc_Purge ThreaderContacts sproc_DeleteMail CompTraceInfo sproc_DeleteMail CompTraceInfo sproc_DeleteMail CompTraceInfo sproc_DeleteMail CompTraceInfo	exec [FreshMain]. dbo.sproc_Purge ThreaderContacts 1 exec [FreshMain]. dbo.sproc_ DeleteMail CompTraceInfo 1, 1 exec [FreshMain]. dbo.sproc_ DeleteMail CompTraceInfo 2, 1 exec [FreshMain]. dbo.sproc_ DeleteMail CompTraceInfo 3, 1 exec [FreshMain]. dbo.sproc_ DeleteMail CompTraceInfo 4, 1	DB Spe-cific (Main DB)	Every day at 12:00 AM.	Deletes Mail Component Trace Information.
Talisma-CreatePreDe-fObjects	sproc_Create PreDefinedObjects sproc_Disable COFOb-jCreationJob	exec exec Sproc_ Create PreDefinedObjects exec SprocDisable COFObjCreationJob	DB Spe-cific (Main DB)	Starts auto-matically when SQL Agent starts	Creates Health Check Objects, Print Template and Link.
Talisma-PurgeDuplicate MailData	sproc_Purge DuplicateMail MessageIDData 30 sproc_Purge DuplicateMail MessageData 30	exec sproc_Purge DuplicateMail MessageIDData 30 exec sproc_Purge DuplicateMail MessageData 30	DB Spe-cific (Main DB)	Every day at 2:00 AM.	Duplicate Interactions will not be created when any incoming Message (new mail / reply / for-ward / consult) is sent with multiple Cam-pusNexus CRM Aliases in the To or Cc fields.
Talisma-RouteAfter-Threader	sproc_Route AfterThreader	exec [tlMain].dbo. Sproc_Route AfterThreader	DB Spe-cific (Main DB)	Every 15 minutes.	When a new mail comes into CampusNexus CRM after the Threader Job runs, this job is used to create the Interaction.

Job Name	File Name	Steps	Type	Frequency	Purpose
Talisma-UserMedia HistoryCleanUp	sproc_MediaRecords CleanUp	exec [tlMain].dbo. sproc_MediaRecords CleanUp	DB Specific (Main DB)	No frequency set.	Cleans history records of user availability for various Media.
Talisma-Purge-Team-Objects	sproc_ ArchiveTeam	exec [tlMain].dbo. sproc_ArchiveTeam	DB Specific (Main DB)	Every 4 hours	Cleans up the Objects related to the deleted Team.
Talisma-Audit Event	sproc_ProcessEvents	osql -S "TALISMALAB97" -d "FreshMain" -E -Q sproc_ ProcessEvents	DB Specific (Main DB)	Every 15 minutes	Processes the audit events for the Interaction, Contact, Account, Order, Opportunity, Campaign, Mailer, Offer, Product, Target, and Canned Response Objects.
Talisma-Audit Event [ObjectTypeID]	sproc_10000_Process Events	osql -S "TALISMALAB97" -d "FreshMain" -E -Q sproc_10000_ ProcessEvents	DB Specific (Main DB)	Every 15 minutes	Processes the audit events for the Link, Print Template, Health Check Objects, and custom Objects with the corresponding [ObjectTypeID].
Talisma-CustomReservation <DBGUID> <(Main DB Name)>	sproc_Custom Reservation	osql -S "TALISMALAB97" -d "FreshMain" -E -Q sproc_ CustomReservation	DB Specific (Main DB)	Every 15 minutes	For supporting custom user reservation. By default it is disabled.
Talisma-ClearPhoneSessions	sproc_AddJob_ CleanUp_ DailyActive PhoneSession	Exec sproc_ EndOrPurge ActivePhoneSession	DB specific	Once daily (0000 hrs)	Unsaved phone sessions will be purged. Saved phone sessions will be ended.

Job Name	File Name	Steps	Type	Frequency	Purpose
Prerequisite The value of Recover active phone sessions upon login to Desktop or Web Client in Business Administrator must be set to No. **Description** Open phone sessions of users who have closed their browsers more than 5 minutes before the Talisma-ClearPhoneSessions job's scheduled run time or who have automatically logged out from Web Client: Will be purged if they were not saved. Will be ended if the phone sessions were saved. **Note** In the Message object, while information about ended phone sessions will be updated in the Interaction Actions tab, the Live Actions tab will not be updated.					

Supported RFCs

A Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) that describes methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. The RFCs supported in this release are:

- RFC 821: Simple Mail Transfer Protocol (SMTP)
- RFC 112: Requirements for Internet Hosts
- RFC 1869: SMTP Service Extensions
- RFC 1870: SMTP Service Extension for Message Size Declaration
- RFC 1652: SMTP Service Extension for 8bit-MIME Transport
- RFC 2197: SMTP Service Extension for Command Pipelining
- RFC 2034: SMTP Service Extension for Returning Enhanced Error Codes
- RFC 1894: An Extensible Message Format for Delivery Status Notifications (DSNs)
- RFC 1893: Enhanced Mail System Status Codes
- RFC 1891: SMTP Service Extension for Delivery Status Notifications
- RFC 2442: The Batch SMTP Media Type
- RFC 822: Standard for the Format of Arpa Internet Text Messages
- RFC 854: Telnet Protocol Specification
- RFC 855: Telnet Option Specifications
- RFC 959: File Transfer Protocol
- RFC 1268: Application of the Border Gateway Protocol
- RFC 1282: BSD Rlogin
- RFC 1738: Uniform Resource Locators (URL)
- RFC 1939: Post Office Protocol - Version 3
- RFC 1521: MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
- RFC 1035: Domain names - implementation and specification
- RFC 1891: SMTP Service Extension for Delivery Status Notifications
- RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies

- RFC 2047: MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
- RFC 2076: Common Internet Message Headers
- RFC 2060: Internet Message Access Protocol - Version 4rev1
- RFC 2109: HTTP State Management Mechanism
- RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2617: HTTP Authentication: Basic and Digest Access Authentication

Anthology Student

Installation Manager can be used to install Anthology Student and related applications:

- Anthology Student standard interface and legacy interface (including optional components such as Portal, STAR COD, and Shopping Sheet/College Finance Plan)
- Financial Aid Automation
- Regulatory
- Regulatory 1098-T Processing Utility

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

API Keys

To enhance the security of Anthology Inc. products, API keys were added to products released in May 2018 and later. An API key is a secret token that is submitted with a web service request to identify the origin of the request. The key for the consumer of the service needs to match the key of provider of the service, otherwise access to the service is rejected. The API key is unique for each customer.

The API key is an AppSetting in the web.config files of applications built on the Anthology framework. It uses the following syntax:

```
<add key="apiKey" value=""/>
```

Depending on the installed products and versions, the apiKey is installed automatically by Installation Manager or needs to be updated manually.

If you are installingAnthology Student 19.0 and have CampusNexus CRM (regardless of the version), update the apiKey under <appSettings> in the web.config file in Cmc.Crm.Workspaces with the key found in the Package Manager screen of Installation Manager. The website for CampusNexus CRM is called Cmc.Crm.Workspaces.

Preinstallation Steps for Student Upgrades

If you are upgrading Anthology Student 16.0.X and earlier, the CampusVue Student database needs to be prepared for the installation of the Anthology domain model. This preparation involves creating tables and moving data using preinstallation scripts.

The preinstallation scripts should be executed a few days before the actual upgrade, preferably during non-peak hours. Anthology Inc. recommends running them one (1) week before the actual upgrade.

All customers currently using CampusVue Student version 16.0.X or earlier should follow these pre-installation steps.

Background for the Data Model Migration

Installation Procedure

Course Categorization

Resilient Replication

If you are upgrading from Anthology Student 20.0 or earlier, you must copy the data from the C2000_DNC database used in previous versions of the product to the new tables in the Anthology Student database for version 21.0.

All customers currently using Anthology Student 20.0.0 or earlier should follow these preinstallation steps.

National Do Not Call

Any preinstallation scripts can be found at https://filetransfer.campusmgmt.com in /softwareupdates/CampusNexus_Student/Pre-Installation Files.

National Do Not Call

Introduction

The purpose of this pre-upgrade procedure is to copy the data from the C2000_DNC database used in previous versions of the product to the new tables in the Anthology Student database for version 21.0. To use the Lookup tab on the National Do Not Call page to look up phone numbers, your System Administrator or other technical professional must follow this procedure before upgrading to version 21.0.

In previous versions of Anthology Student, files from the Federal Trade Commission (FTC) National Do Not Call (DNC) Registry were imported to the C2000_DNC database in the same instance as the Anthology Student database.

In version 21.0, Anthology Student imports the files into tables prefixed with dnc in the Anthology Student database. It does not use the C2000_DNC database.

Prerequisites

You:

- Should have downloaded the DNC_Database_Migration_Script.sql script from https://filetransfer.campusmgmt.com/softwareupdates/CampusNexus_Student/Pre-Installation Files.
- Must have db_owner permission for the Anthology Student database.
- Should not be performing an import to the old C2000_DNC database.

Installation Steps

1. In the Microsoft SQL Server Management Studio window, connect to the Anthology Student SQL Server instance.
2. Execute the following pre-upgrade script on the Anthology Student database:

   DNC_Database_Migration_Script.sql

The script displays a message when processing is complete and the phone numbers from the C2000_DNC database ([dbo].[syDNCImportWork] table) have been copied to the Anthology Student database ([dnc].[syDNCImportWork] table).

Background for the Data Model Migration

Person Centric Data Model

One of the significant enhancements that will be gained with Anthology products is the ability for applications to share and reuse person centric data. Even within individual applications such as CampusVue Student, there is a large amount of redundancy in person centric data that is stored. For example, if a person attends school as a student and later becomes a staff member at the same institution, the current implementation in CampusVue Student requires completely separate and disparate records be stored for the student and the staff member even though it is the same person. Name, address, phone number, and email address information is some of the data that is keyed in twice in this scenario. This obviously results in extra data entry for the customer and increases the likelihood of some of the data becoming stale and incorrect over time. Further, the ability to see a 360 degree view of data for the person is compromised by virtue of not connecting this data under the umbrella of a common person record.

The Anthology domain includes a concept of person centric data with the ability to have a person owning multiple functional roles such as Student and Staff. The goal of this model is to have a single, common place where data about the person is stored or persisted. Thus, when any changes occur for a person regarding name, address, phone numbers, email addresses, etc., the changes only need to be made one time and in one place. When users of Anthology applications are viewing data regarding this person from any context of Student, Staff, Instructor, or any other defined functional role, they will be viewing the same person centric data.

This is a large change that will be achieved through multiple incremental implementation steps. The initial step toward achieving and supporting the Anthology domain model is to prepare the database. Tables need to be created that will store the person centric data. These tables will be automatically populated with existing data in the CampusVue Student tables and exposed in the new query builder of Anthology Student. For now, the Query builder will be the only place where the person centric tables will be exposed. CampusVue Student users who are not licensed for Anthology will have no indication from working inside Anthology Student that these person centric tables exist.

Database Schema Changes

To achieve the business requirement, the following schema changes are introduced in release 16.1:

- The following new tables are created:
  - *SyPerson*
  - *SyPersonEmail*
  - *SyPersonAddress*
  - *SyPersonPhoneNumber*
- The SyPersonId column is introduced in following tables:
  - *SyStudent*
  - *SyStaff*
  - *SyOrganizationContact*
  - *PlEmployerContact*

Data Model

Click here to view the complete Data Model in a separate PDF file.

Migration Logic

Data from the following tables is migrated to new person related tables.

- *SyStudent*
- *SyStaff*
- *SyOrganizationContact*
- *PlEmployerContact*

In addition, SyPersonAddress is populated from the additional SyAddress table.

The rows in each of these tables are copied to the SyPerson record.

Duplicate Logic for SSNs

During the migration, simple duplicate logic is applied. This is based on a valid SSN (Social Security Number).

- If no SSN is associated with any of the functional role records, a new person record is created.
- If a valid SSN is associated with any of the functional role records, the migration script checks if a SyPer-

son record already exists with the same SSN.

- If a SyPerson record exists, the functional role record is associated with the existing person record.

The SSN will be considered valid if the following conditions are satisfied:

- The SSN format is: XXX-XX-XXXX
- The SSN does not start with 999 or 777 or 888 or 000.

If the SSN satisfies these criteria, the record will be associated with the same SyPerson record.

Example

An existing CampusVue Student database contains a person who has three records in the SyStudent table. The same person also is a staff member and has one record in the SyStaff table.

Table 1

SyStudentId	FirstName	LastName	SSN	Table
100	John	Miller	123-456-7890	SyStudent
8000	Johnathan	Miller	123-456-7890	SyStudent
12000	Johnny	Miller	123-456-7890	SyStudent
6000	J.	Miller	123-456-7890	SyStaff

After the migration of data to the person centric tables, one row will exist in SyPerson. The three SyStudent and one SyStaff records will be associated with the same SyPerson record (see Table 2).

Since the first name is represented differently in the existing records (see Table 1), the first name in the record that is migrated last will used to populate the first name in the SyPerson record.

The initial implementation (release 16.1) does not include logic to handle instances with discrepancies in data for different functional role records (i.e., SyStudent, SyStaff, etc.) that contain the same SSN.

Table 2

SyStudentId	SyPersonId	SSN	Table
100	1000052	123-456-7890	SyStudent
8000	1000052	123-456-7890	SyStudent
12000	1000052	123-456-7890	SyStudent
6000	1000052	123-456-7890	SyStudent

Modified Insert/Update Triggers

After successful migration and installation, the records in person related tables are maintained using insert/update triggers. The following triggers are modified to support the schema change:

- trg_SyStaff_Update
- Trg_SyStaff_Ins
- Trg_SyOrganizationContact_Upd
- Trg_SyOrganizationContact_Ins
- Trg_PlEmployerContact_Upd
- Trg_PlEmployerContact_Ins
- syStudent_Upd_trg
- syStudent_Ins_trg
- trg_SyAddress_Insert
- trg_SyAddress_Update

CVueSourceTypeId is used to identify the specific place in the existing CampusVue Student tables where the data came from. This is primarily used to account for the absence of certain planned implementations in Anthology around supporting address types, phone number types, and email address types. Additionally, the CVueSourceTypeId allows for the trigger logic to know precisely which person centric record should be updated when address, phone number, or email address data is changed in CampusVue Student. Table 3 shows the enumerations that are implemented:

Table 3

TableName	Enumeration
SyPersonPhoneNumbers	1. Phone 2. SyStudent.Work 3. SyStudent.OtherPhone 4. Systudent.Mobilenumber 5. SyStaff.HomePhone 6. SyStaff.CellPhone 7. SyStaff.WorkFax 8. PlEmployerContact.Fax 9. PlEmployerContact.Phone2 10. SyOraganizationContact.Fax 11. SyOraganizationContact.Phone2
SyPersonAddress	1. StaffAddress 2. StaffWorkAddress 3. SyAddress 4. SyStudentAddress 5. PlEmployerContact 6. SyOrganizationContact

TableName	Enumeration
SyPersonEmail	1. Email 2. Other 3. ReplyTo

Installation Procedure

Introduction

The migration scripts are very long running based on the database size and number of records in the tables. To migrate the data within the down time window, scripts are categorized as:

- Preinstallation Scripts
- Installation Scripts

Preinstallation Scripts

All customers currently using CampusVue Student version 16.0.X or earlier should follow these pre-installation instructions.

The preinstallation scripts should be executed a few days before the actual upgrade, preferably during non-peak hours. Anthology Inc. recommends running them one (1) week before the actual upgrade. The scripts should be executed in the order listed below.

- TFS0193057-00-SyPersonMigration-Objects.sql
- TFS0193057-01-SyPerson_Stage-Update.sql

The scripts create jobs and will be executed in the background. The default batch size is 100,000. The batch size can be modified if any performance issue occurs while executing the scripts.

The above scripts insert records into the following new tables and perform data migration to new tables:

- *SyPerson*
- *SyPersonEmail*
- *SyPersonAddress*
- *SyPersonPhoneNumber*

Installation Scripts

The following scripts are executed in the first step of the installation. The scripts create jobs in the background and will be executed as part of the installation. Manual intervention is not required.

- TFS0193057-02-SyPerson_Delta-Processing.sql
- TFS0193057-03-Person_DDL.sql
- TFS0193057-04-SyPerson-Update.sql
- TFS0193057-05-SyPersonFinal-Update.sql

Preinstallation Steps

Note: All customers currently utilizing version 16.0.X or earlier should follow these preinstallation instructions.

Depending on size of the CampusVue Student database, preinstallation step may run into extended period of time. So it is advised to determine the preinstallation time during upgrade testing. Based on the test upgrade outcome, determine the time to start the preinstallation script. It is recommended to execute the installation during non-peak hours.

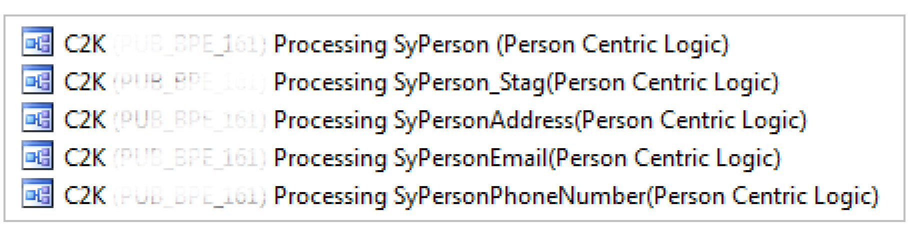
1. Copy the script **TFS0193057-00-SyPersonMigration-Objects.sql** in SQL Management Studio (SSMS) and select the correct production database.
2. Click **Execute**.

   The following objects are created as part of the script:

   - dbo.tblPersonMigration_Errors
   - usp_PersonMigration_SyPerson_PlEmployerContact
   - usp_PersonMigration_SyPerson_Stag_PlEmployerContact
   - usp_PersonMigration_SyPerson_Stag_SyOrganizationContact
   - usp_PersonMigration_SyPerson_Stag_SyStaff
   - usp_PersonMigration_SyPerson_Stag_SyStudent
   - usp_PersonMigration_SyPerson_SyOrganozationContact
   - usp_PersonMigration_SyPerson_SyStaff
   - usp_PersonMigration_SyPerson_SyStudent
   - usp_PersonMigration_SyPersonAddress_PlEmployerContact
   - usp_PersonMigration_SyPersonAddress_SyAddress
   - usp_PersonMigration_SyPersonAddress_SyOrganizationContact
   - usp_PersonMigration_SyPersonAddress_SyStaff
   - usp_PersonMigration_SyPersonAddress_SyStudent
   - usp_PersonMigration_SyPersonEmail_PlEmployerContact
   - usp_PersonMigration_SyPersonEmail_SyOrganizationContact
   - usp_PersonMigration_SyPersonEmail_SyStaff
   - usp_PersonMigration_SyPersonEmail_SyStudent
   - usp_PersonMigration_SyPersonPhoneNumber_PlEmployerContact
   - usp_PersonMigration_SyPersonPhoneNumber_SyOrganizationContact
   - usp_PersonMigration_SyPersonPhoneNumber_SyStaff
   - usp_PersonMigration_SyPersonPhoneNumber_SyStudent
   - usp_PersonMigration_SyRegistry_InsUpd

3. On successful execution of step 2, **copy/open** the script **TFS0193057-01-SyPerson_Stage-Update.sq**l and make sure it is connected to correct database.
4. Click **Execute**.

   The following jobs are created and executed:

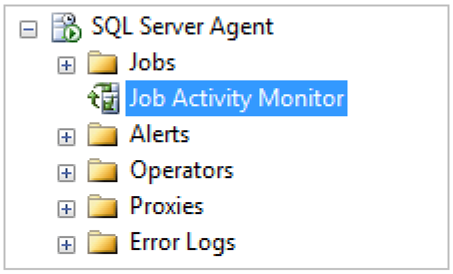
5. Monitor the jobs.

6. If the jobs are creating a performance issue, try to **lower the batch size** by executing the following statement. Change the highlighted section to a smaller number based on the server performance.

```
EXEC dbo.usp_PersonMigration_SyRegistry_InsUpd 'xxxSyPerson_BatchSize','100000'
```

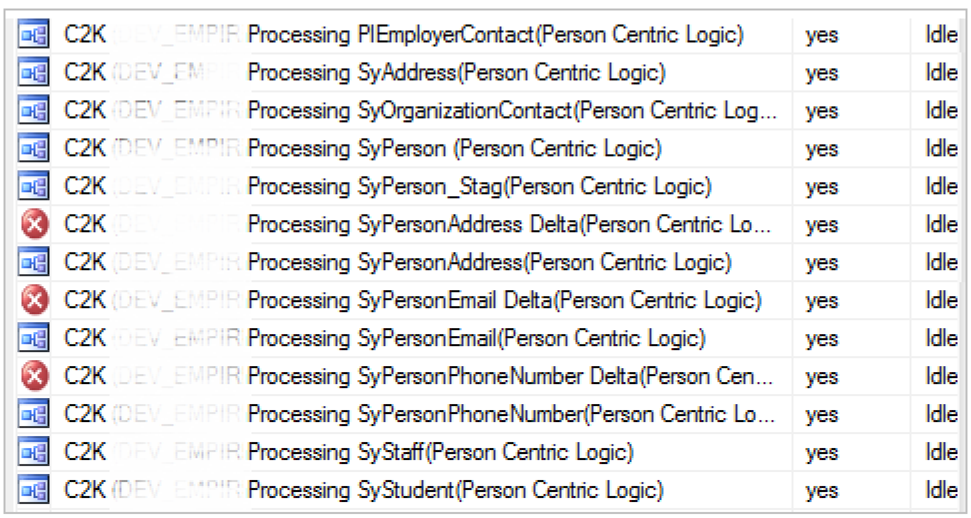
7. Monitor the jobs.

   a. Expand **SQL Server Agent** in SQL Server Management Studio.



   b. Double-click **Job Activity Monitor**.

   If any exceptions occurred, the job icons are displayed as shown below:



   c. If there is any exception in the script logic, the error message will be recorded in the **tblPersonMigration_Errors** table.

```
SELECT * FROM dbo.tblPersonMigration_Errors WITH (NOLOCK)
```

   d. Progress of the script can be also monitored from the **registry key**.

```
select * from dbo.SyRegistry WITH(NOLOCK) where regkey like 'xxxSyPerson%'
```

e. If all the jobs are executed successfully, verify the registry key. The **RegValue** for all keys should be **1**.

	RegKey	RegValue	DisplayOrder	Prompt	ListType	ValueList
1	xxxSyPerson_BatchSize	100000	1			
2	xxxSyPerson_PlEmployerContact	1	1			
3	xxxSyPerson_Stag_PlEmployerContact	1	1			
4	xxxSyPerson_Stag_Staff	1	1			
5	xxxSyPerson_Stag_SyOrganizationContact	1	1			
6	xxxSyPerson_Stag_SyStudent	1	1			
7	xxxSyPerson_SyOrganizationContact	1	1			
8	xxxSyPerson_SyStaff	1	1			
9	xxxSyPerson_SyStudent	1	1			
10	xxxSyPersonAddress_PlEmployerContact	1	1			
11	xxxSyPersonAddress_SyAddress	1	1			
12	xxxSyPersonAddress_SyOrganizationContact	1	1			
13	xxxSyPersonAddress_SyStaff	1	1			
14	xxxSyPersonAddress_SyStudent	1	1			
15	xxxSyPersonEmail_PlEmployerContact	1	1			
16	xxxSyPersonEmail_SyOrganizationContact	1	1			
17	xxxSyPersonEmail_SyStaff	1	1			
18	xxxSyPersonEmail_SyStudent	1	1			
19	xxxSyPersonPhoneNumber_PlEmployerContact	1	1			
20	xxxSyPersonPhoneNumber_SyOrganizationC...	1	1			
21	xxxSyPersonPhoneNumber_SyStaff	1	1			
22	xxxSyPersonPhoneNumber_SyStudent	1	1			

8. If all jobs are completed successfully, execute following statement on the publisher database (before install):

IF EXISTS (SELECT 1 FROM sys.indexes WHERE name = 'Nk_SyPersonAddress_RecordId_ CVueSourceTypeId' and object_id = object_id('SyPersonAddress'))
    DROP INDEX SyPersonAddress.Nk_SyPersonAddress_RecordId_CVueSourceTypeId

IF NOT EXISTS (SELECT 1 FROM sys.indexes WHERE name = 'Nk_SyPersonAddress_RecordId_ CVueSourceTypeId' and object_id = object_id('SyPersonAddress'))
    CREATE NONCLUSTERED INDEX [Nk_SyPersonAddress_RecordId_CVueSourceTypeId] ON [dbo].[SyPersonAddress]
    (

```
        [RecordId] ASC,
        [CVueSourceTypeId] ASC
    )
    INCLUDE (
         StreetAddress
        , City
        , [State]
        , Zip
        , YearsAtAddress
        , EffectiveBeginDate
        , EffectiveEndDate
        )
    WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, SORT_IN_TEMPDB = on, DROP_EXISTING
= OFF, ONLINE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, FILLFACTOR = 80) ON
[C2000_Index]
    GO
```

9. On Successful completion of the script, proceed with the installation steps.

Installation Steps

1. Start the regular installation through the installer.

   This logic covers two parts:

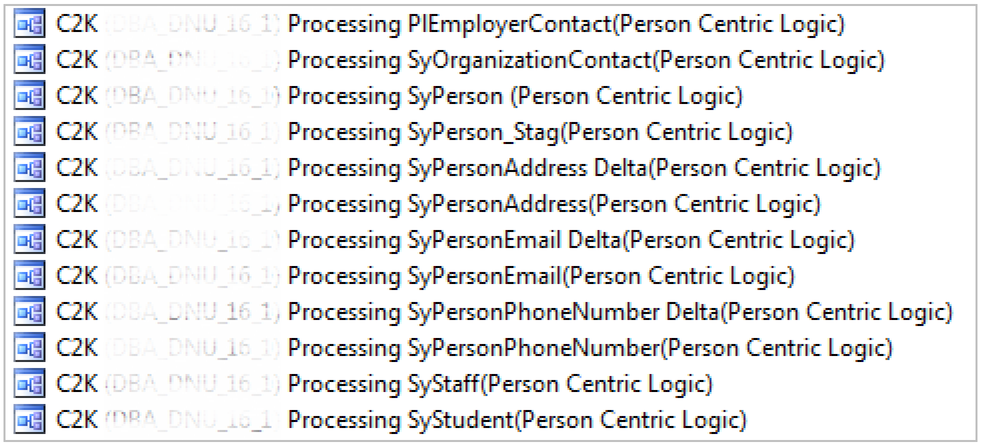
   a. Handle delta records

   b. Handle updating the SyPersonId in the following tables:

      - *SyStudent*
      - *SyStaff*
      - *SyOrganizationContact*
      - *PlEmployerContact*

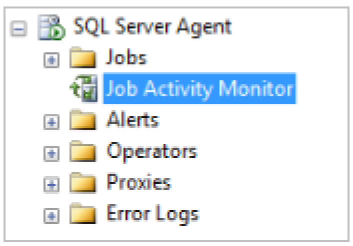
2. The following additional jobs will be created.

   - C2K (<DBName>) Processing SyPersonAddress Delta(Person Centric Logic)
   - C2K (<DBName>) Processing SyPersonEmail Delta(Person Centric Logic)
   - C2K (<DBName>) Processing SyPersonPhoneNumber Delta(Person Centric Logic)
   - C2K (<DBName>) Processing SyStaff(Person Centric Logic)
   - C2K (<DBName>) Processing SyStudent(Person Centric Logic)
   - C2K (<DBName>) Processing PlEmployerContact(Person Centric Logic)
   - C2K (<DBName>) Processing SyOrganizationContact(Person Centric Logic)



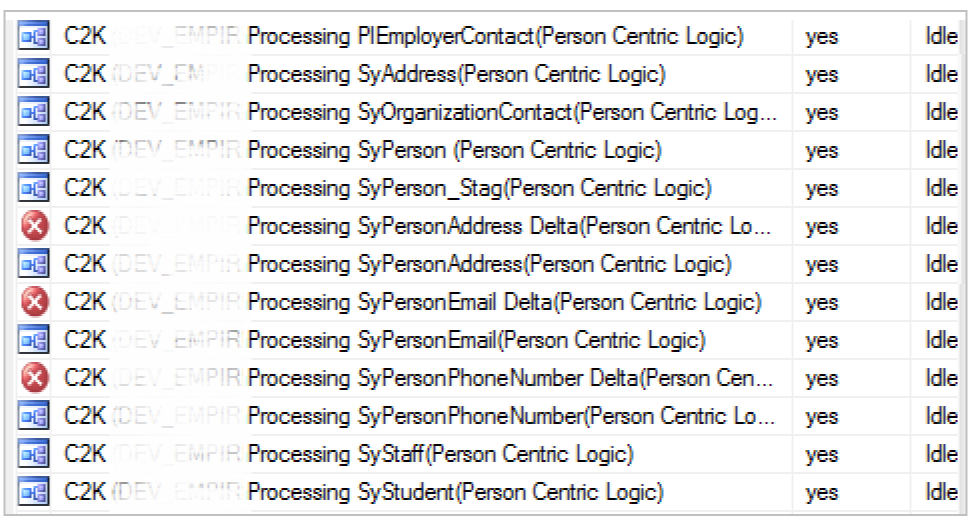
3. Monitor the jobs.

   a. Expand **SQL Server Agent** in SQL Server Management Studio (SSMS).



   b. Double-click the **Job Activity Monitor**.

   If exceptions occur, the job icons are displayed as shown below:



   c. If an exception occurs in the script, the error message will be recorded in the **tblPersonMigration_Errors** table. Use the following statement to find error messages.

```
SELECT * FROM dbo.tblPersonMigration_Errors WITH (NOLOCK)
```

d. Monitor the progress of the script from the **registry key**.

```
select * from dbo.SyRegistry WITH(NOLOCK) where regkey like 'xxxSyPerson%'
```

e. If all jobs are executed successfully, verify the registry key. The **RegValue** for all keys should be updated with '**1**'.

4. If all jobs are completed successfully, the installer will proceed with the rest of the database installation.

Course Categorization

Introduction

The purpose of this pre-upgrade installation procedure is to perform Course Categorization for those existing courses that were registered for an enrollment prior to the previous upgrade but remained uncategorized. Currently, Course Categorization occurs in real-time for only those enrollments that undergo certain changes, such as a new course being registered or dropped. When a given course is categorized, the category information is stored in a table called **AdSPECourseCategory**. The backfilling of the AdSPECourseCategory table is done for performance reasons and to avoid possible deadlocks when more than one process tries to do course categorization involving simultaneous inserts and updates.

Since the backfilling the AdSPECourseCategory table could be a lengthy process based on the volume of selected enrollments, it is advised to carry out this pre-upgrade installation a few days ahead of the actual production upgrade.

Note: Try to execute the pre-upgrade steps during non-peak hours and execute the script against the Production OLTP a minimum of 2-3 days prior to the actual upgrade.

This document and the pre-upgrade installation requirement is applicable to Anthology Student and CampusVue Student upgrades from database versions 16.0.x to 16.0.7, and from 16.x.x to 16.1.1 or 17.0 and above. Also note that this Pre-Upgrade Course Categorization is a one-time activity only. For example, if this process was executed during the course of an upgrade from 16.0.2 to 16.0.7, when an upgrade was performed from 16.0.7 to 17.0 and above, this Pre-Upgrade Course Categorization backfill process is not required.

Installation Steps

Note: Depending on the volume of the enrollments for Course Categorization, the process to backfill may run for an extended period of time. It is advised to determine the preinstallation time during upgrade testing and based on that outcome, determine the best time to start the preinstallation script. Remember, it is recommended to execute the installation during non-peak hours.

1. In the Microsoft SQL Server Management Studio window, connect to the CampusVue Student SQL Server instance.
2. Execute the following pre-upgrade script on the **CampusVue Student** database:

   TFS270714_Pre-UpgradeScript_Backfill Course Categorizations.sql
3. The objects listed below are created using the preinstallation script.
   a. Tables:

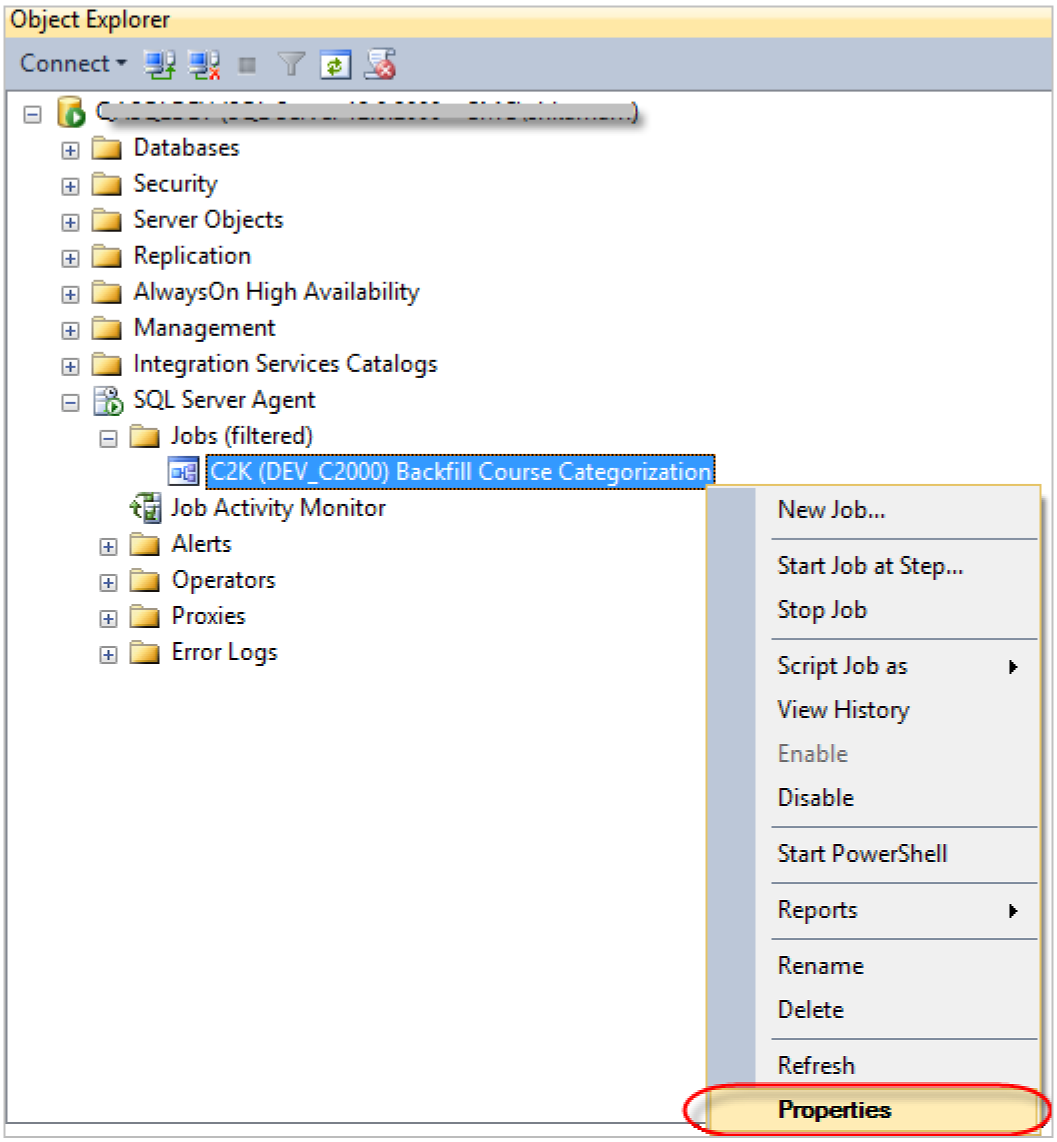
      (1) dbo. SyEnrollmentsForCategorizationWork
   b. SQL Server Job:

1) 'C2K (<CampusVue Student Database name>) Backfill Course Categorization'

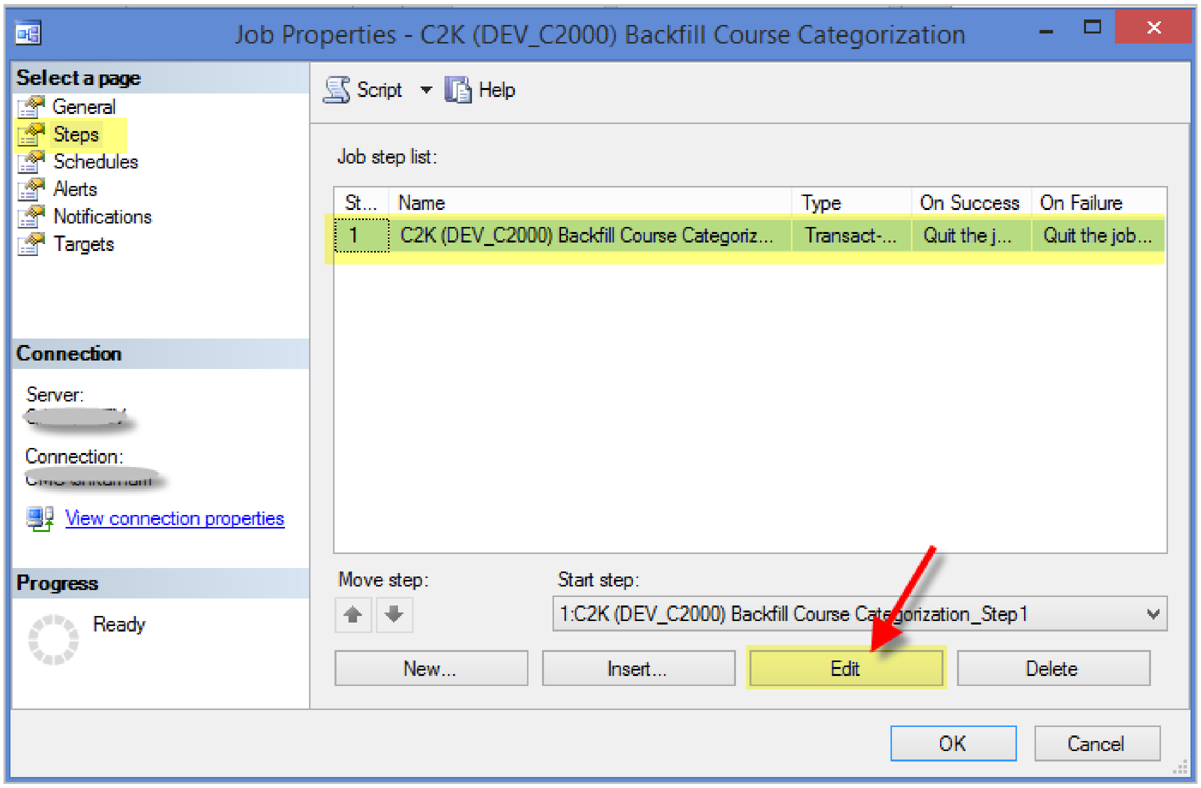
Example: 'C2K (C2000) Backfill Course Categorization'

4. In the Microsoft SQL Server Management Studio window, click the (+) sign to expand the **SQL Server Agent** node.

   Right-click the SQL Server Job that was just created (as mentioned in the previous step) and click **Properties**.

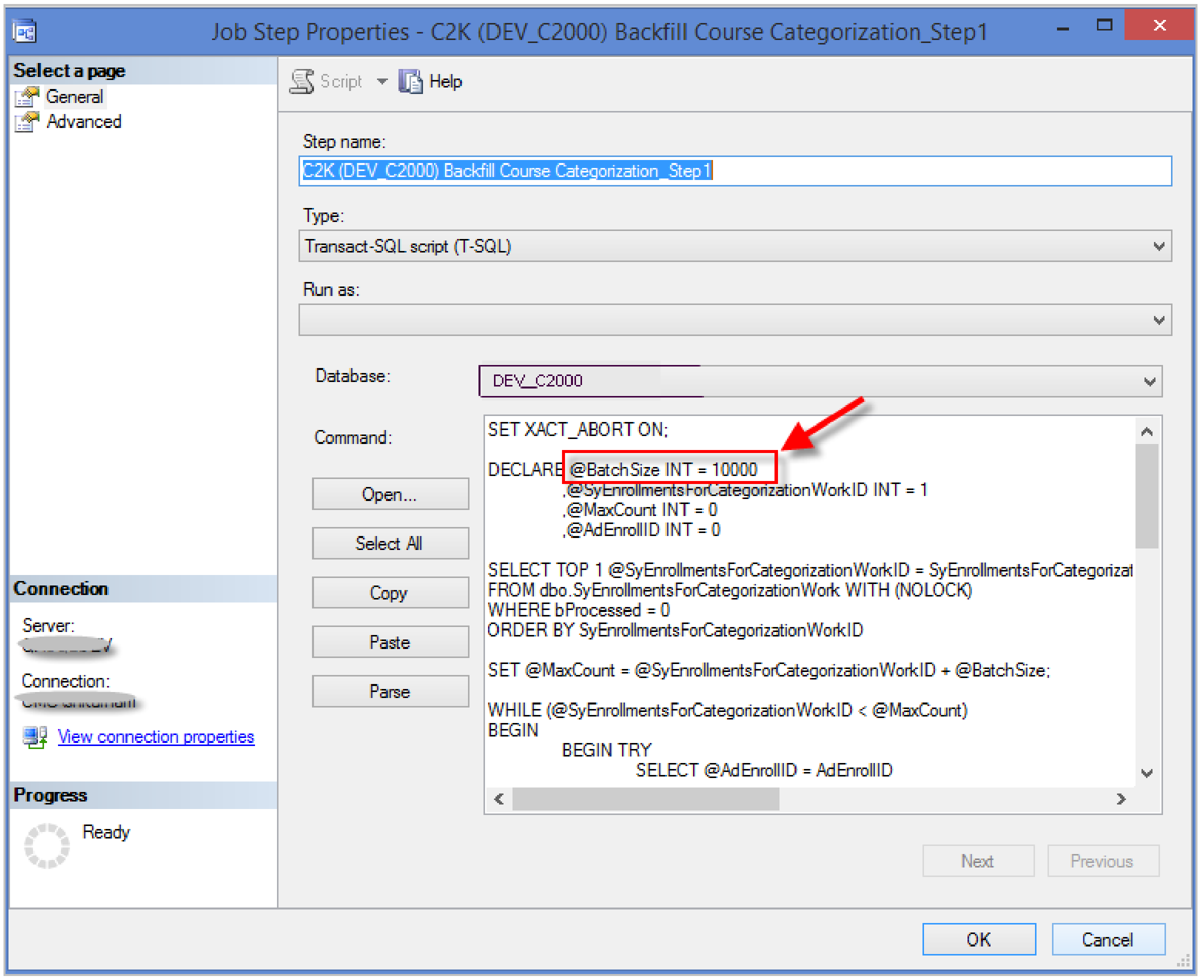


5. On the **Steps** page, select the only available step and click **Edit**.

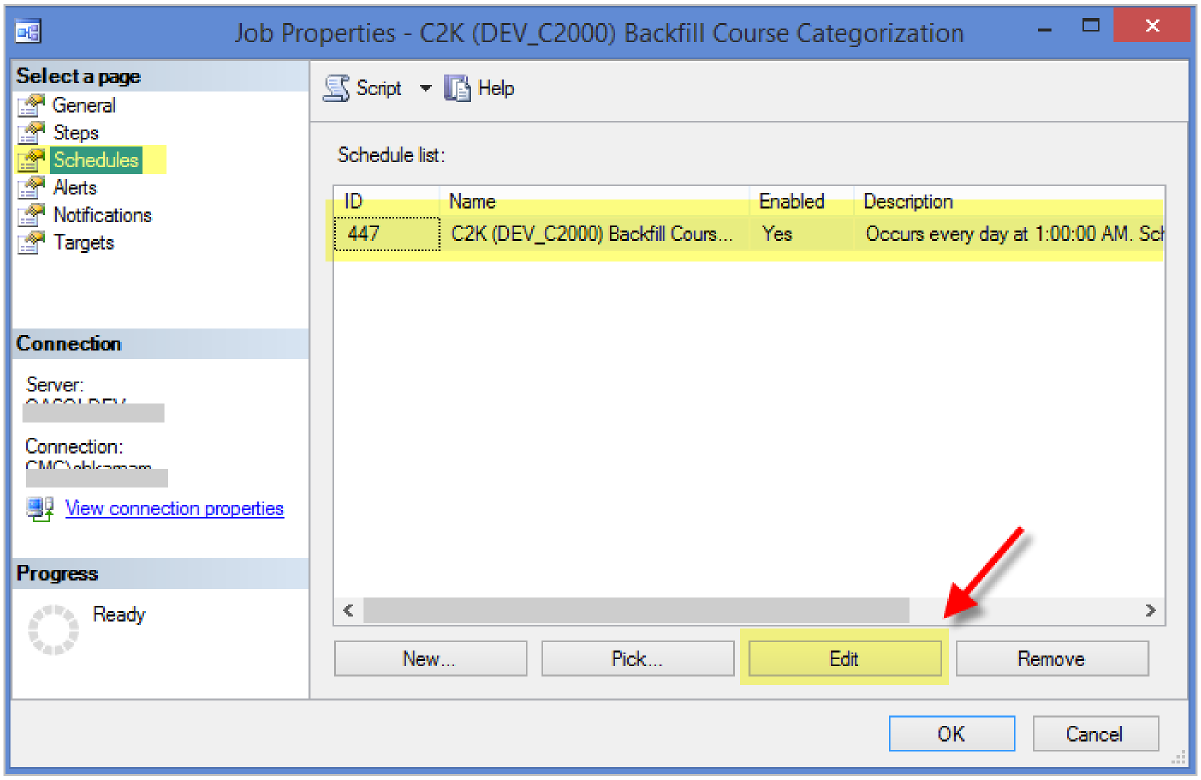


6. On the **Steps** page, change the **@BatchSize** value to a higher value if required, based on the time window available for batch processing and click **OK**.

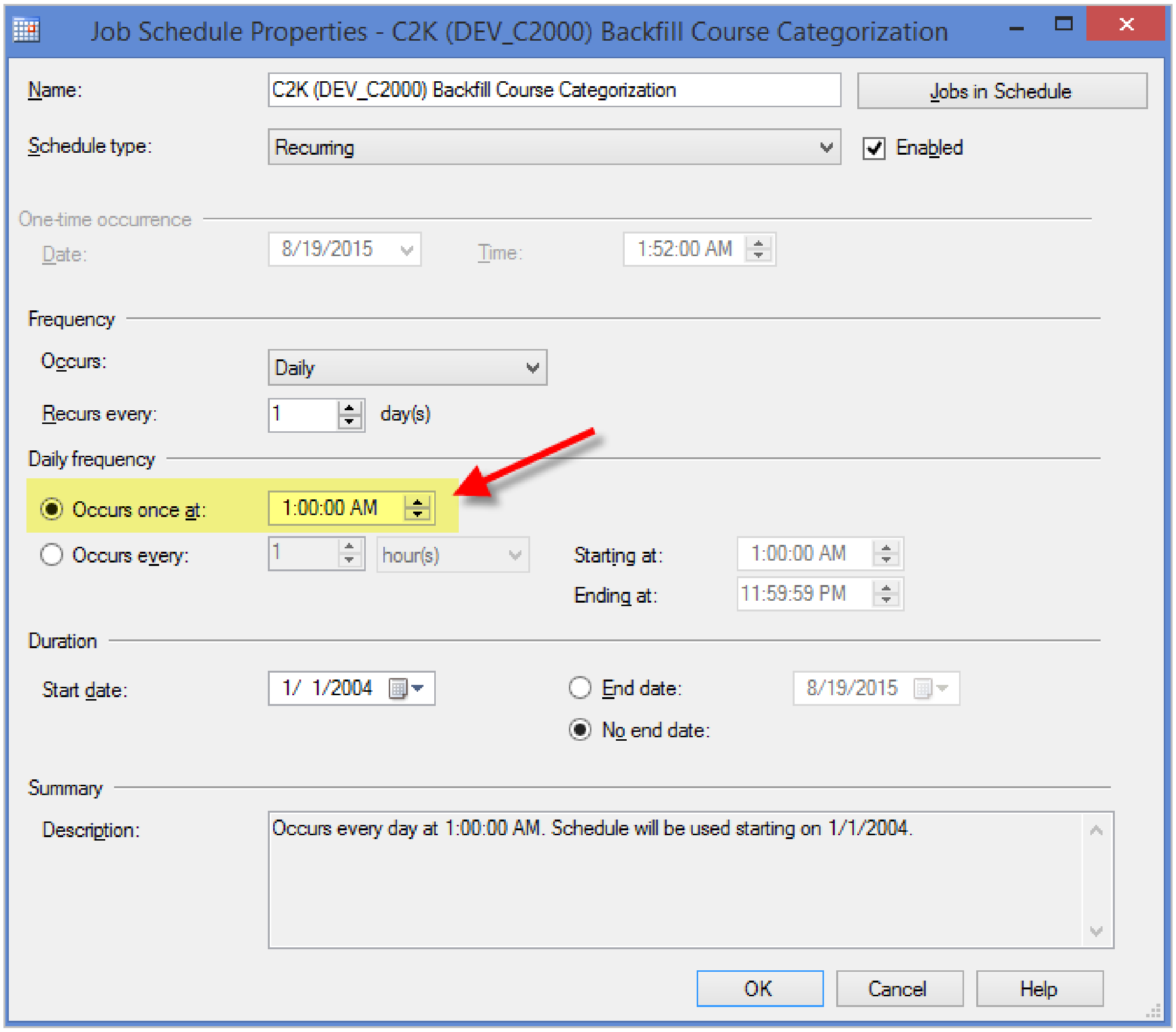
   Note: This Batch Size determines how many enrollments will be processed with every execution of this job.



7. On the **Schedules** page, select the default schedule (Occurs every day at 1:00 AM) and click **Edit** if you choose to change the schedule time.



8. If you have chosen to Edit the schedule and have opened the Schedule Edit page, change the **Daily frequency time** as required and click **OK**.



9. Click **OK** on the Job Properties dialog to save the changes.
10. Wait for the Job to start on its selected schedule and let it perform the Course Categorization backfill process.
11. To determine if the backfill process is complete, execute the SQL Query shown below against the CampusVue Student database in SQL Management Studio.

    --Query to show status of Course Categorization Backfill process

    IF EXISTS(SELECT 1 FROM dbo.SyRegistry WITH (NOLOCK) WHERE RegKey = 'xxxCourseCategorizationBackfill' AND RegValue = '0')
    AND OBJECT_ID('dbo.SyEnrollmentsForCategorizationWork') IS NOT NULL
    BEGIN
    SELECT CASE
    WHEN bProcessed = 0

```
            THEN 'Pending'
        WHEN bProcessed = 1
            THEN 'Completed'
        END AS [Status]
    ,Counts AS [Count of Enrollments]
FROM (
    SELECT bProcessed
        ,COUNT(1) AS Counts
    FROM dbo.SyEnrollmentsForCategorizationWork WITH (NOLOCK)
    GROUP BY bProcessed
    ) TEMP
ORDER BY 1 DESC
END
ELSE IF EXISTS(SELECT 1 FROM dbo.SyRegistry WITH (NOLOCK) WHERE RegKey = 'xxxCourseCat-
egorizationBackfill' AND RegValue = '1')
    PRINT 'Course Categorization Backfill process is completed during upgrade. No further action is
required'
```

Resilient Replication

Introduction

Resilient Replication improves the resiliency of the transactional replication process employed by Anthology Student for scaling out SQL Server reporting workloads to a separate SQL Server Instance. These improvements to the replication process should negate the need to break and rebuild replication for upgrades to Anthology Student, FAA, and Regulatory.

Preinstallation Steps

Note: Try to execute the preinstallation steps during non-peak hours. Execute the script against the Production OLTP and reporting databases at a minimum of 48 hours prior to the actual upgrade to release 17.0 and above.

If the current Anthology Student database version is 15.x.x or 16.0.x and Replication has been configured, perform the following steps for a resilient upgrade without breaking the replication:

1. In the Microsoft SQL Server Management Studio window, connect to the Publisher server. In the Object Explorer, click the (+) sign to expand the **Replication** folder, then click the (+) sign to expand the **Local Publications** folder.

   a. Right-click the Publication(s), then click **Properties**.

   b. On the Subscription Options page of the Publication Properties dialog box, set the **Replicate schema changes** option to **True**.

   c. Click **OK** to close the window.

2. Execute the following preinstallation script on the **Publisher** database and the **Subscriber** database:

   ```
   ..\17.1 - Pre-Installation Files\TFS155940-00-PreUpgradeScript-CreateRe-
   silientReplicationObjects.sql
   ```

3. Execute the script below on the **Publisher** database. Specify the value of the @publication parameter with the name of the publication to add the new table ‘SyReplTablesAltered’ as an article. If there are multiple publications with the same Subscriber dbs, then add the article to any one of the publications.

   ```
   PRINT 'Adding SyReplTablesAltered table as Article'

   EXEC sp_addarticle @publication = 'Name Of Publication'
       ,@article = N'SyReplTablesAltered'
       ,@source_owner = N'dbo'
       ,@source_object = N'SyReplTablesAltered'
       ,@type = N'logbased'
       ,@description = N''
   ```

```
    ,@creation_script = NULL
    ,@pre_creation_cmd = N'drop'
    ,@schema_option = 0x00000000084359DF
    ,@identityrangemanagementoption = N'manual'
    ,@destination_table = N'SyReplTablesAltered'
    ,@destination_owner = N'dbo'
    ,@vertical_partition = N'false'
    ,@ins_cmd = N'CALL sp_MSins_dboSyReplTablesAltered'
    ,@del_cmd = N'CALL sp_MSdel_dboSyReplTablesAltered'
    ,@upd_cmd = N'SCALL sp_MSupd_dboSyReplTablesAltered'
GO

exec sp_refreshsubscriptions @publication = N' Name Of Publication'
GO
--  Test the repl cmd
INSERT INTO dbo.SyReplTablesAltered (tablename, ColumnAltered)
SELECT 'Test', 'Test'
```

4. Run the following statement in the **Subscriber** database to confirm the table is replicating.

   ```
   SELECT * FROM dbo.SyReplTablesAltered WHERE TableName = 'Test'
   ```

5. Execution of the above script should be a non- empty result set.

6. Once the ‘SyReplTablesAltered’ table is replicated, the below mentioned objects (created using the pre-installation script) exist in the Publisher and Subscriber database, the CampusVue database can be upgraded without breaking the Replication.

   a. Tables:

      (1) dbo.SyReplTablesAltered (article)

      (2) dbo.SyIndexRecreatePostUpgradeWork

   b. Stored Procedures:

      (1) dbo.cmc_PrepTableForAlter

      (2) dbo.cmc_PrepTableColumnForAlter

   c. Trigger:

      (1) dbo.SyReplTablesAltered_Insert_trg ON dbo.SyReplTablesAltered

Preinstallation Steps – 16.1

If the current Anthology Student database version is 16.1.x and Replication has been configured, perform the following additional step before the upgrade:

Execute the following preinstallation script on the **Subscriber** database.

```
IF EXISTS (SELECT 1 FROM sys.indexes WHERE name = 'Nk_SyNexusOrganization_Code' and object_id =
object_id('SyNexusOrganization'))
BEGIN
  DROP INDEX [Nk_SyNexusOrganization_Code] ON [dbo].[SyNexusOrganization]
END

IF EXISTS (SELECT 1 FROM sys.foreign_keys WHERE name = 'FK_SyNexusOrganizationSyCampusGrpId_SyCam-
pusGrpSyCampusGrpId' and parent_object_id = object_id('SyNexusOrganization'))
BEGIN
  ALTER TABLE dbo.SyNexusOrganization
    DROP CONSTRAINT FK_SyNexusOrganizationSyCampusGrpId_SyCampusGrpSyCampusGrpId
END



GO
Exec [dbo].[cmc_DropConstraintsAndTriggersOnSubscriber]
GO
IF EXISTS (SELECT 1 FROM sys.columns WHERE is_identity = 1
AND COLUMNPROPERTY(OBJECT_ID('dbo.SyIndexRecreatePostUpgradeWork'), 'SyIn-
dexRecreatePostUpgradeWorkID', 'IsIdNotForRepl') = 1
)
BEGIN
   ALTER TABLE dbo.SyIndexRecreatePostUpgradeWork ALTER COLUMN SyIn-
dexRecreatePostUpgradeWorkID DROP NOT FOR REPLICATION
END
GO
```

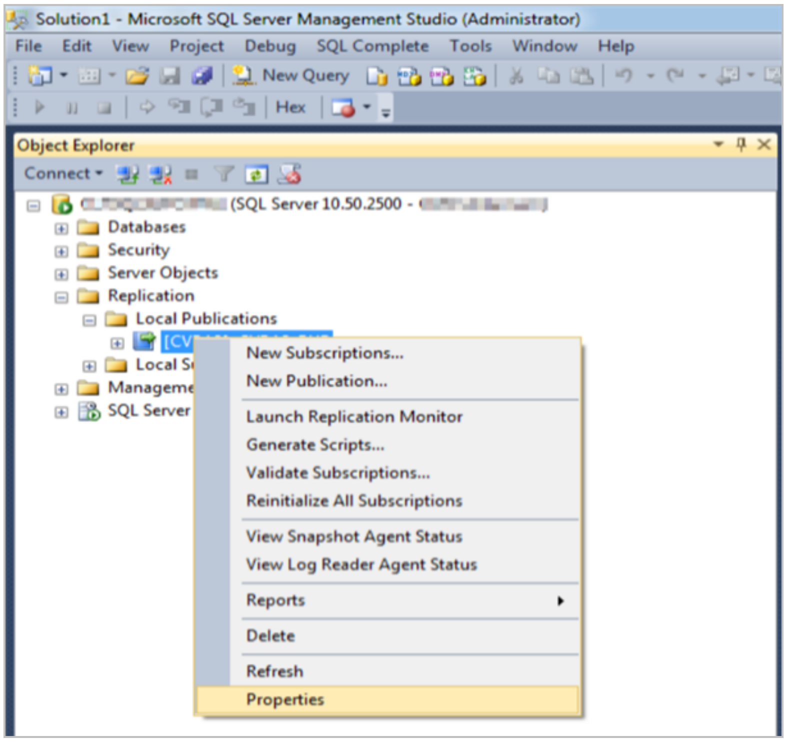
Preinstallation Steps – Regulatory 8.x and 9.x

If the current Regulatory version applied to the Anthology Student database is lower than 8.x and Replication has been configured, the following error could occur while upgrading the Regulatory version:

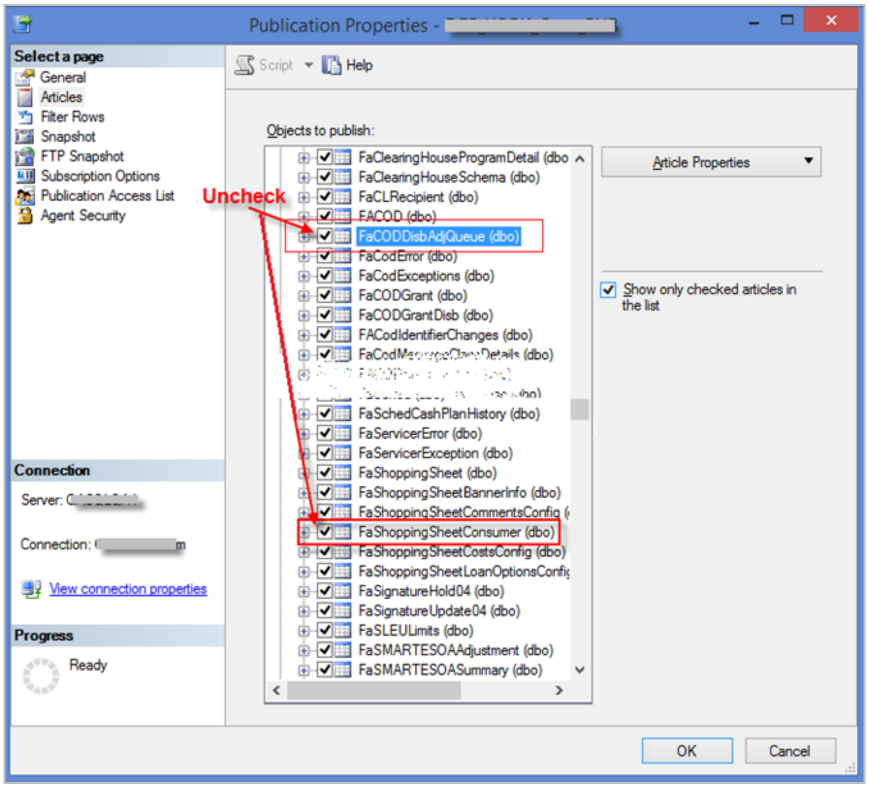
- Cannot truncate table 'dbo.FaShoppingSheetConsumer' because it is published for replication or enabled for Change Data Capture. Script fragment that caused an error: TFS0324456-00-FaShoppingSheetConsumer_Insert_2016_17_ShoppingSheetData.sql
- Cannot truncate table 'dbo.FaCODDisbAdjQueue' because it is published for replication or enabled for Change Data Capture.Script fragment that caused an error: TFS0325072-FaCODDisbAdjQueue_Truncate.sql

Perform the following steps before upgrading:

1. In the Microsoft SQL Server Management Studio window, connect to the SQL Server instance where the Anthology Student database exists.
2. Click the (+) sign to expand the **Replication** folder, and expand the **Local Publications** folder.
3. In the list of publications, right-click the publication belonging to the Anthology Student database being upgraded, and click **Properties**.



4. On the Articles page of the Publication Properties dialog box, locate the following two tables and clear the check marks to remove them from the article list.
    a. FaCODDisbAdjQueue (dbo)
    b. FaShoppingSheetConsumer (dbo)



Note: If multiple publications exist for the same Anthology Student database that is being upgraded, find the publication that contains the above mentioned tables as articles and clear the check marks to remove them from replication.

5. Now upgrade the Anthology Student database with a Regulatory version greater than 8.x.

6. Once upgrade is complete and the post installation/upgrade steps are complete, repeat the above steps 1 to 3 and check the “FaShoppingSheetConsumer (dbo)” table to include it back to the replication.

Student Web App

You can use Installation Manager to install Anthology Student.

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

Prerequisites

The prerequisites for the installation include:

- Login credentials to connect to the Anthology Student database.
- Definition of the Application Pool Identity for Anthology Student.

If you are using Reports feature in Anthology Student, the SQL Server 2016 Reporting Services (SSRS 2016) must be installed. Anthology Student will function for student record management without SSRS 2016 installed, but it has incomplete functionality without reports. SSRS 2016 is required for reporting functionality and should be included in the installation and configuration of the product. For testing purposes in student record management, Anthology Student can be installed without SSRS 2016.

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Installation Manager installs the following components:

- Security Token Service (STS)

  > ⚠ Anthology Student version 17.1.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

  Anthology Student version 19.0.3 or later requires Staff STS version 2.1.2 or later.

- Anthology Student

After installing Anthology Student, proceed to install the Security Console utility. For more details, see Security Console.

Application Pool Identity and Integrated Security

To enhance security and simplify configuration and maintenance, Anthology Student will use (by default) application pool identity and integrated security to access local and network resources such as SQL Server.

Application Pool Identity

Application pool identity was introduced in Service Pack 2 (SP2) of Windows Server 2008. An application pool identity allows you to run an IIS application pool under a unique account without having to create and manage domain or local accounts. This unique account is ideal for running web applications as it has limited access to resources, uses the machine account which cannot be impersonated, and does not require you to store passwords within configuration files.

When using application pool identity, local resources are accessed using the identity of the application pool (e.g., IIS AppPool\DefaultAppPool) and network resources are accessed using the identity of the machine account (e.g., CMC\WebServer1$).

ApplicationPoolIdentity is the Microsoft recommended (and default) identity for IIS application pools. For more information on application pool identity and how to secure local and network resources, please read [Application Pool Identities] on iis.net.

Integrated Security

Integrated security uses the identity that is executing the process to authenticate against SQL Server. Integrated security is more secure than SQL Server authentication as it does not require credentials to be present within the database connection string. When using application pool identity with integrated security, connections to SQL Server use the identity of the application pool or machine account.

SQL Server Authentication

```
Data Source=Server01; Initial Catalog=CampusVue; User ID=username; Password=password
```

Integrated Security

```
Data Source=Server01; Initial Catalog=CampusVue; Integrated Security=True
```

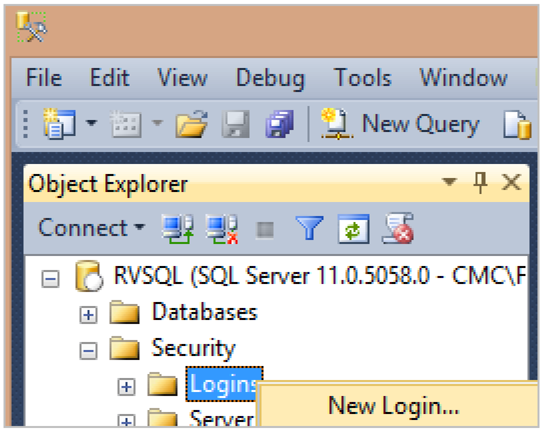
Application Pool Identity for Anthology Student

- By default, *ApplicationPoolIdentity* will be the identity used by the application pool (CampusNexusStudentAppPool).
- By default, all connection strings within the `web.config` will use integrated security.

It is a common and recommended practice to use an Active Directory group to maintain the list of application servers that have access to the database. This allows you to associate resource access to the group as a whole rather than each individual application server.

To authorize a web server's access to the SQL server:

1. On the server that hosts the SQL database for Anthology Student, open Microsoft SQL Server Management Studio.
2. Connect to the database and in Object Explorer navigate to **Security**.
3. Right-click **Logins** and select **'New Login...'**.



4. Grant access to the SQL server to CampusNexusStudentAppPool.

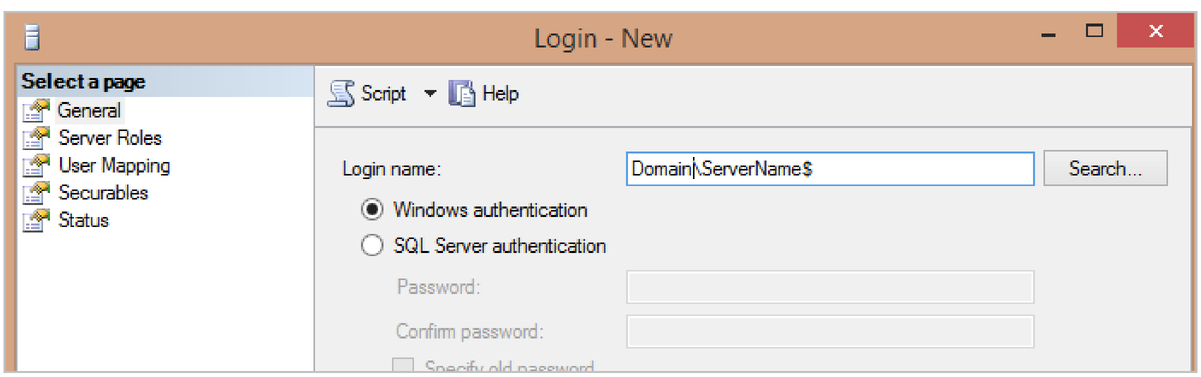
   - **If SQL Server is running on a different machine than the web server (most common):**

     In the Login name field of the Login - New window, add **Server Name$**. (Do no click Search.)

     `Domain\ServerName$`

     For example:

     `CMC\WebServer1$`

   - **If SQL Server is running on the same machine as the web server:**

     Add the application pool account to the database:

     `IIS AppPool\appPoolName`

For example:

```
IIS AppPool\CampusNexusStudentAppPool
```

5. Make sure to give DB_Owner access to the Anthology Student database.

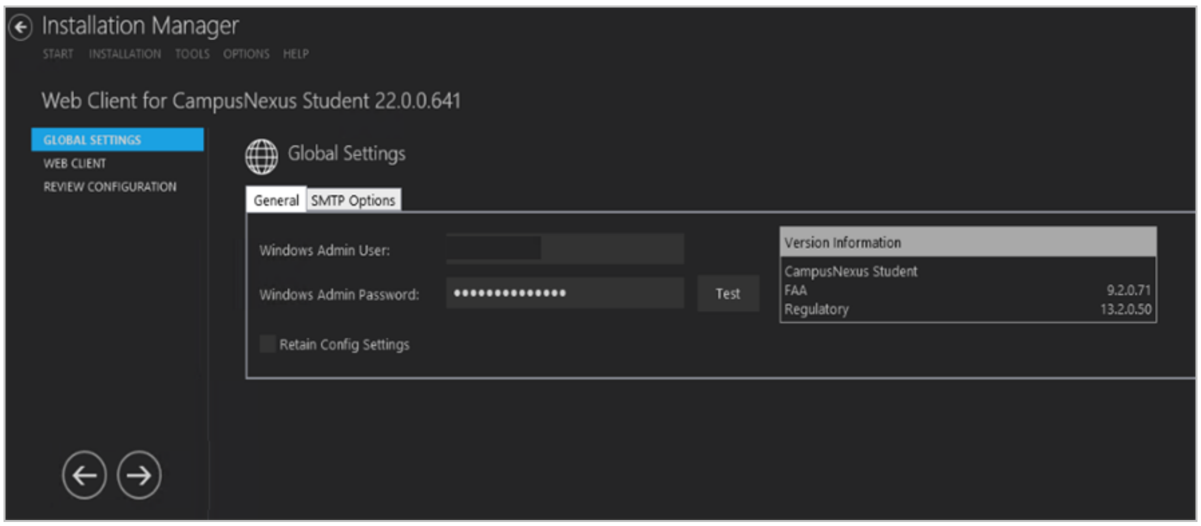
Global Settings

The Global Settings screen contains the Windows Admin user name password used when starting the Anthology Student installation. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Web Client for Anthology Student** tile. The Global Settings screen is displayed.

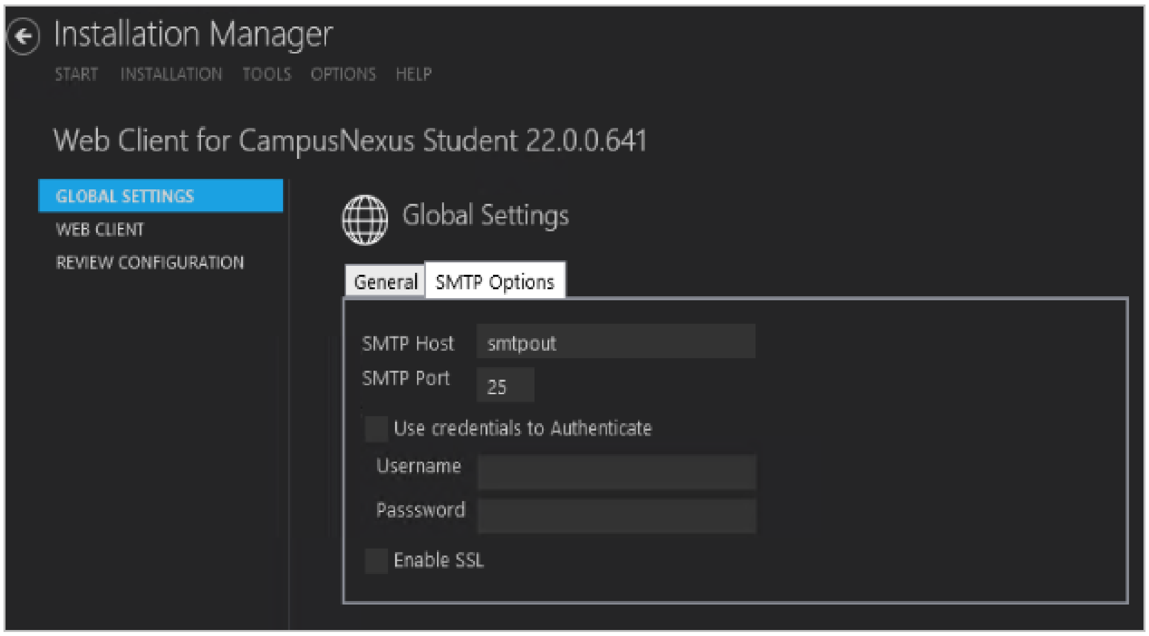
2. On the General tab, in the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer on which the installation will occur. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

   Note: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.
4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
5. Select the **Retain Config Settings** check box if you want to deploy the latest web.config file and also run a config merge that will merge any settings that were set outside of the install process.

If Retain Config Setting is not selected, the install process will not retain and will not merge any configuration settings that were set outside of install process.

6. On the SMTP Options tab, provide the following information:

    - In the **SMTP Host** field, enter the domain address of the SMTP host used for sending out email notifications from Anthology Student, e.g., CNSweb1.campusmgmt.com.
    - Specify the **SMTP Port** number.
    - Select **Use credentials to Authenticate** and enter the **Username** and **Password** of the sender's email account.
    - If applicable, select **Enable SSL**. Installation Manager will check for a valid certificate.



7. Click  to continue.

Web Client

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, upgrade, uninstall) and to specify the machine name and options of the standard interface (web client) for Anthology Student.

Prerequisites

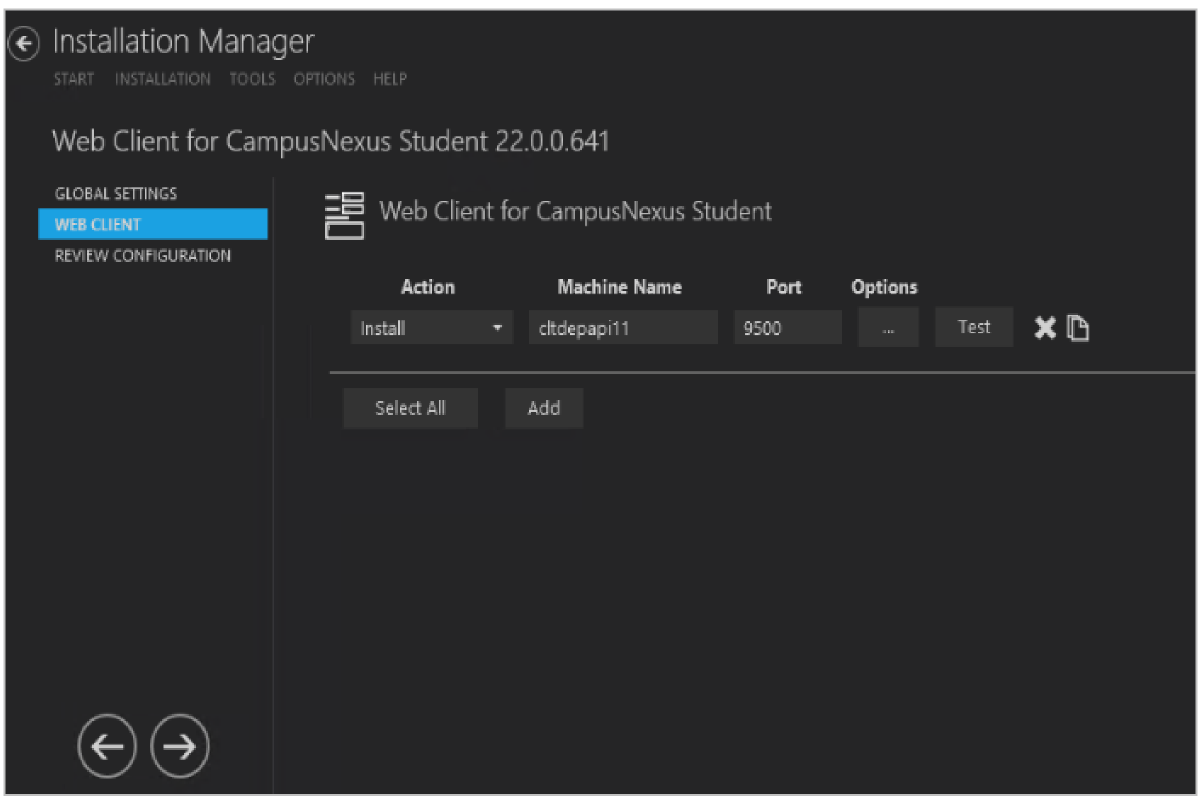
Anthology Student version 17.1.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

During installation of Anthology Student, the following is added to the web.config of the Staff STS:

```
<SecurityServiceConfigSection>
<SecurityServiceCollection>
<add name="NexusWebClient" address="http://<server>:<port>/" enabled="true" />
</SecurityServiceCollection>
</SecurityServiceConfigSection>
```

Set Up the Web Client

1. In the Installation menu, click **Web Client**. The Web Client for Anthology Student screen is displayed.



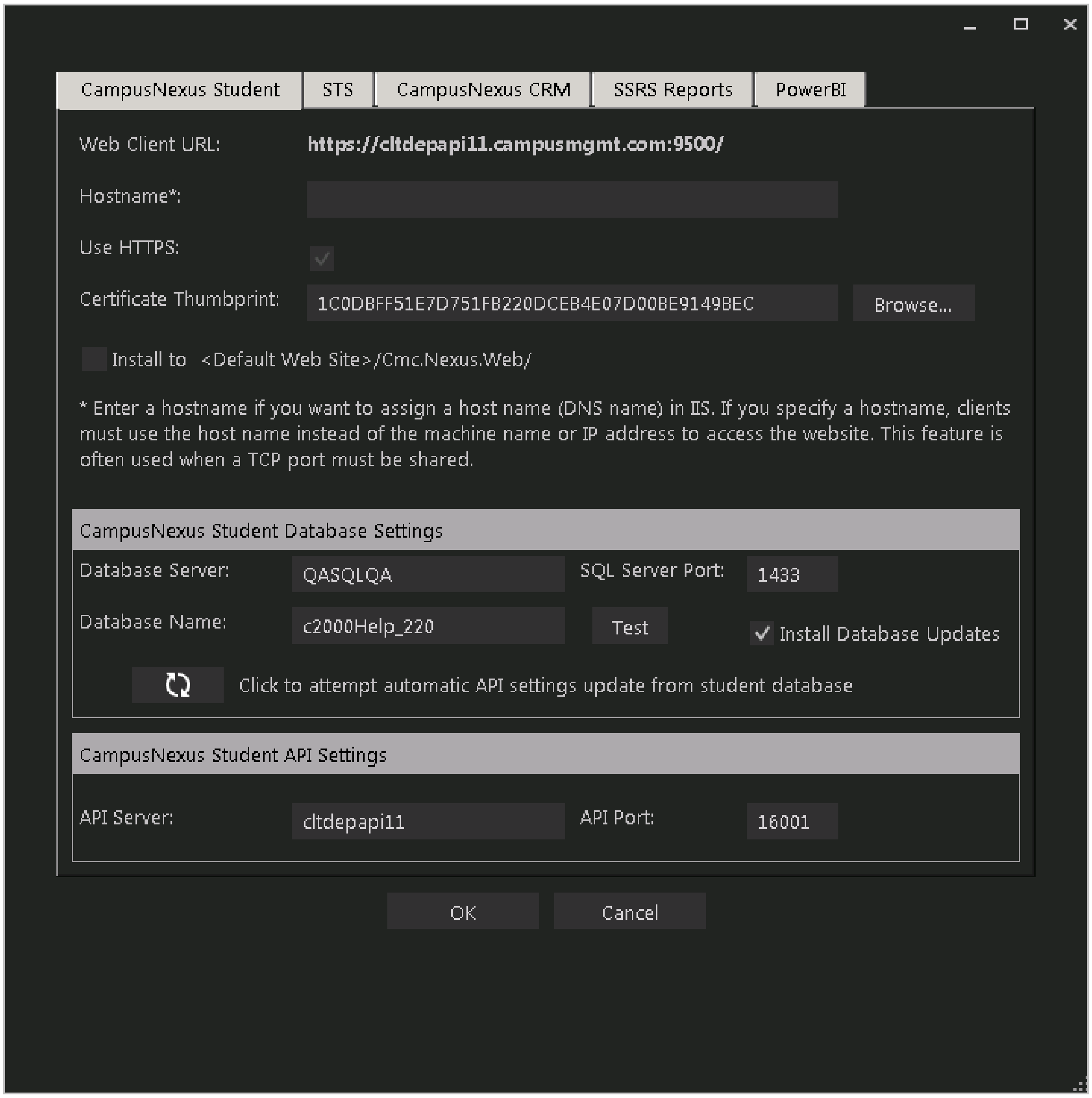
2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. In the **Port** field, specify a port number of accept the default (80). If you specify a custom port, Installation Manager will update the port number in the config file of Anthology Student
6. Click  to copy a line. Edit the copied line as needed.
7. Click  to view and edit the Options form.

   Anthology Student Tab

   Use this tab to specify the URL, the connections to the Anthology Student API server and database server.



Anthology Student Tab Fields

Field	Description
Web Client URL	The URL is populated with <machine name.domain.com> by default. You can override the default URL with another URL. The specified URL will be updated in the web.config file of Anthology Student and in the Anthology Student database. If you change the URL during an upgrade in an environment where Forms Builder is used, the URL must be manually updated in the web.config files of Forms Builder Designer and Renderer.

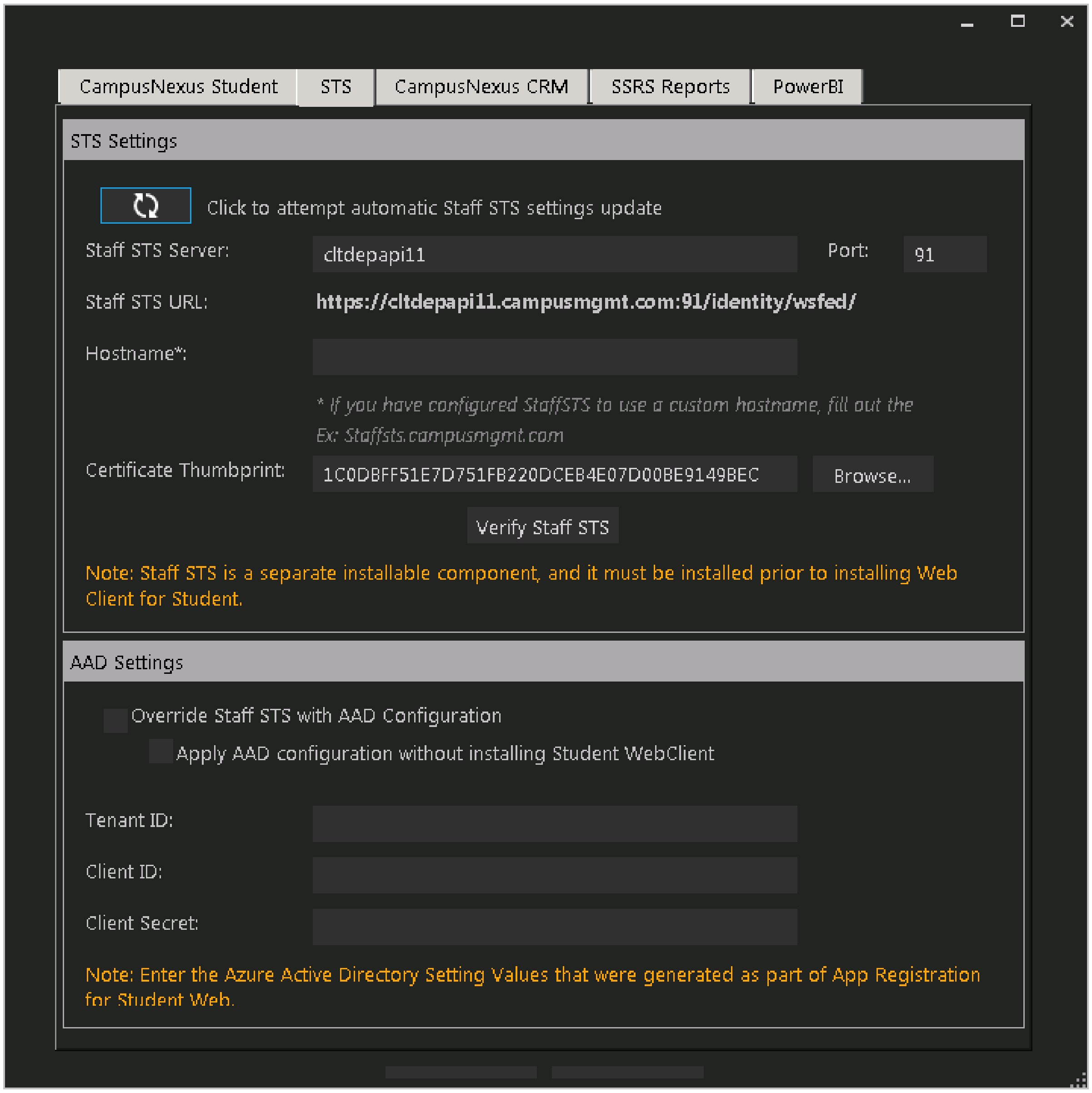
Field	Description
Hostname	This is an optional field. When selected, the web.config file of Anthology Student will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port` Enter a hostname if you want to assign a hostname (DNS name) in IIS. If you specify a hostname, clients must use the hostname instead of the machine name or IP address to access the website. This feature is often used when a TCP Port must be shared.
Use HTTPS	This option is selected by default and cannot be cleared. All components must use HTTPS.
Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected. It is not added to the web.config file. This certificate is used only for Anthology Student, which provides authentication for Renderer (and Portal) to applicants, students, and employers. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Install to <Default Web Site>/Cmc.Nexus.Web/	The default behavior of Installation Manager is to install Anthology Student to its **own** website under the IIS sites. If backward compatibility requires the continued use of the default website, select the **Install to <Default Web Site>/Cmc.Nexus.Web/** check box. In this case an upgrade will not delete the website and reinstall the website as it did previously. Any manual configurations made to the website (via IIS manager for example) will be retained on upgrade. An uninstall will remove the website to clean up the environment.
Anthology Student Database Settings	
Database Server	Name of the SQL server on which the Anthology Student database resides.

Field	Description
SQL Server Port	Specify the port number of the SQL server or accept the default (1433).
Database Name	Name of the Anthology Student SQL database.
Test	Click **Test** to verify the database connection.
Install Database Updates	Select this check box to install updates to the Anthology Student database. Click **Test** to verify the database connection.
	Click the **Refresh** button to attempt an automatic settings update.
Anthology Student API Settings	
API Server	Name of the Anthology Student API server.
API Port	Specify the port number of the API server or accept the default (18001).

STS Tab

Use this tab to specify the STS server, port, and certificate. Note that Staff STS must be installed prior to installing Anthology Student.

For deployments in a cloud environment, specify the Azure Active Directory (AAD) settings. Enter the values that were generated as part of the web application registration for Anthology Student in the AAD tenant.



STS Tab Fields

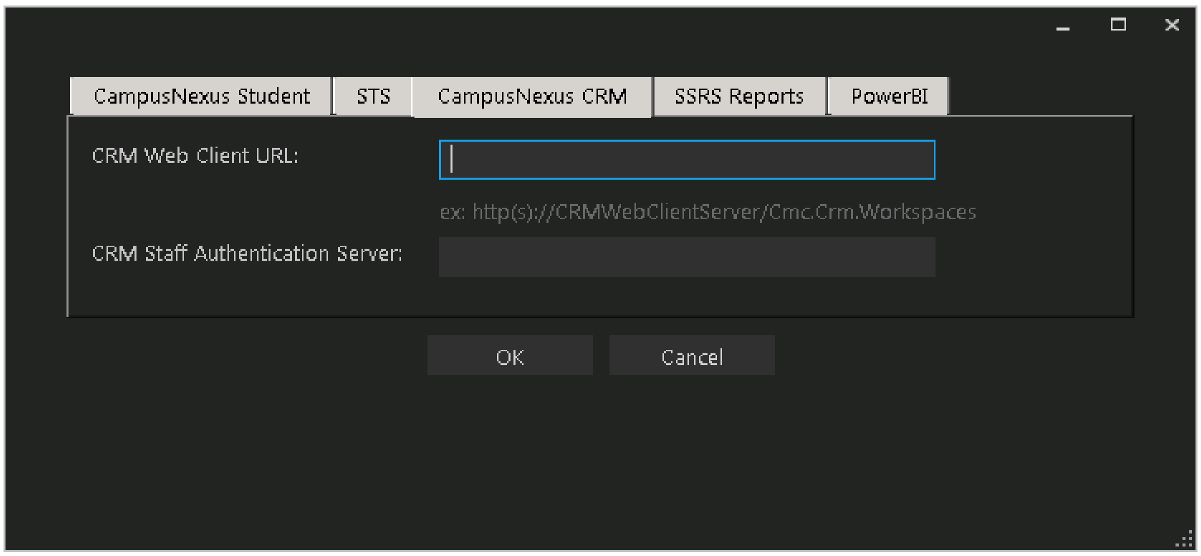
Field	Description
STS Settings	
	Click the **Refresh** button to attempt an automatic settings update.
Staff STS Server	Specify the name of the Staff STS Server. The Staff STS Server must have been previously installed. See Staff STS.
Port	Specify the port number of the installed Staff STS server or accept the default (91).

Field	Description
Staff STS URL	Staff STS URL is populated by default with machine name.domain.com. The user can override it with custom URL, e.g., Studentweb.campusmgmt.com, and that URL will be updated in the Anthology Student config file and Anthology Student database.
Hostname	If you have configured Staff STS to use a custom hostname, fill out the hostname. Example: Staffsts.campusmgmt.com
Certificate Thumbprint	Certificate thumbprint from IIS. The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Verify Staff STS	Click **Verify Staff STS**. This button: • Verifies that the Staff STS is installed. • Validates that the certificate is installed in the personal store.
AAD Settings	
Override Staff STS with AAD Configuration	Select this check box to enable the AAD Settings fields.
Apply AAD configuration without installing Student Web Client	Select this check box if AAD is used without installing Anthology Student.

Field	Description	
Tenant ID	Specify the Azure tenant identifier.	Customers create app registrations in their Azure AD tenant and provide the Tenant ID, Client ID, and Client Secret that are generated as part of creating the app registration. **Note**: One app registration is created for Anthology Student legacy interface and standard interface.
Client ID	Specify the Azure client identifier.	
Client Secret	Specify the Azure client secret.	

CampusNexus CRM Tab

If CampusNexus CRM is deployed, specify the URL and the authentication server for the CampusNexus CRM web client.

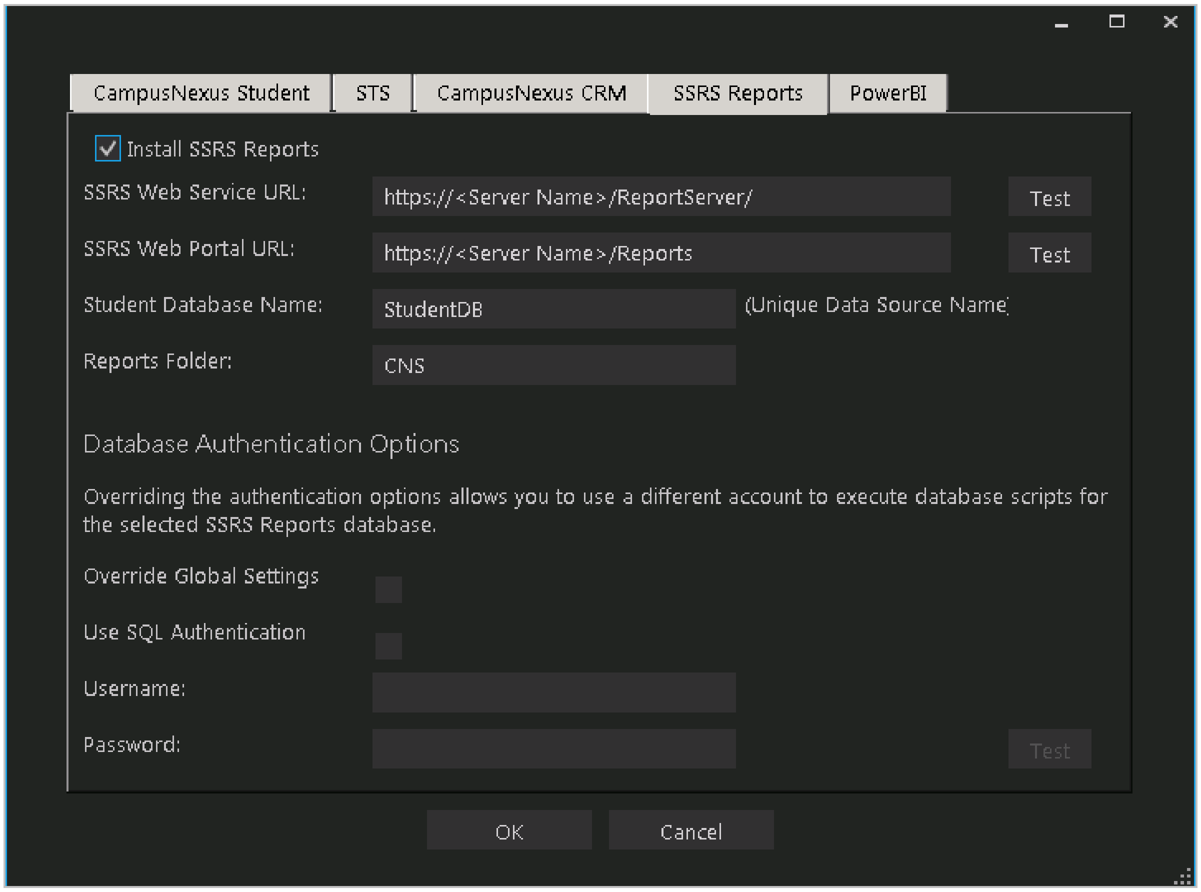


CampusNexus CRM Tab Fields

Field	Description
CRM Web Client URL	If applicable, enter the URL of the CampusNexus CRM web client, for example: `http(s)://CRMWebClientServer/Cmc.Crm.Workspaces` The URL will be added as a key in the web.config file of Anthology Student. The format of the key is as follows: <add key="uri:CRM" value="{{CrmWebClientUrl}}"/>
CRM Staff Authentication Server	If applicable, enter the name of the server where the CRM Staff Authentication Service is installed. Installation Manager will construct the complete URL based on the Server name. `http://StaffAuthenticationServiceServer/Cmc.NexusCrm.WebServices` The CRMStaffAuthenticationServiceURL will be inserted into the syregistry table in the Anthology Student database.

SSRS Reports Tab

Use this tab to integrate SQL Server Reporting Services (SSRS) 2016, the server-based report generating software system, into Anthology Student.

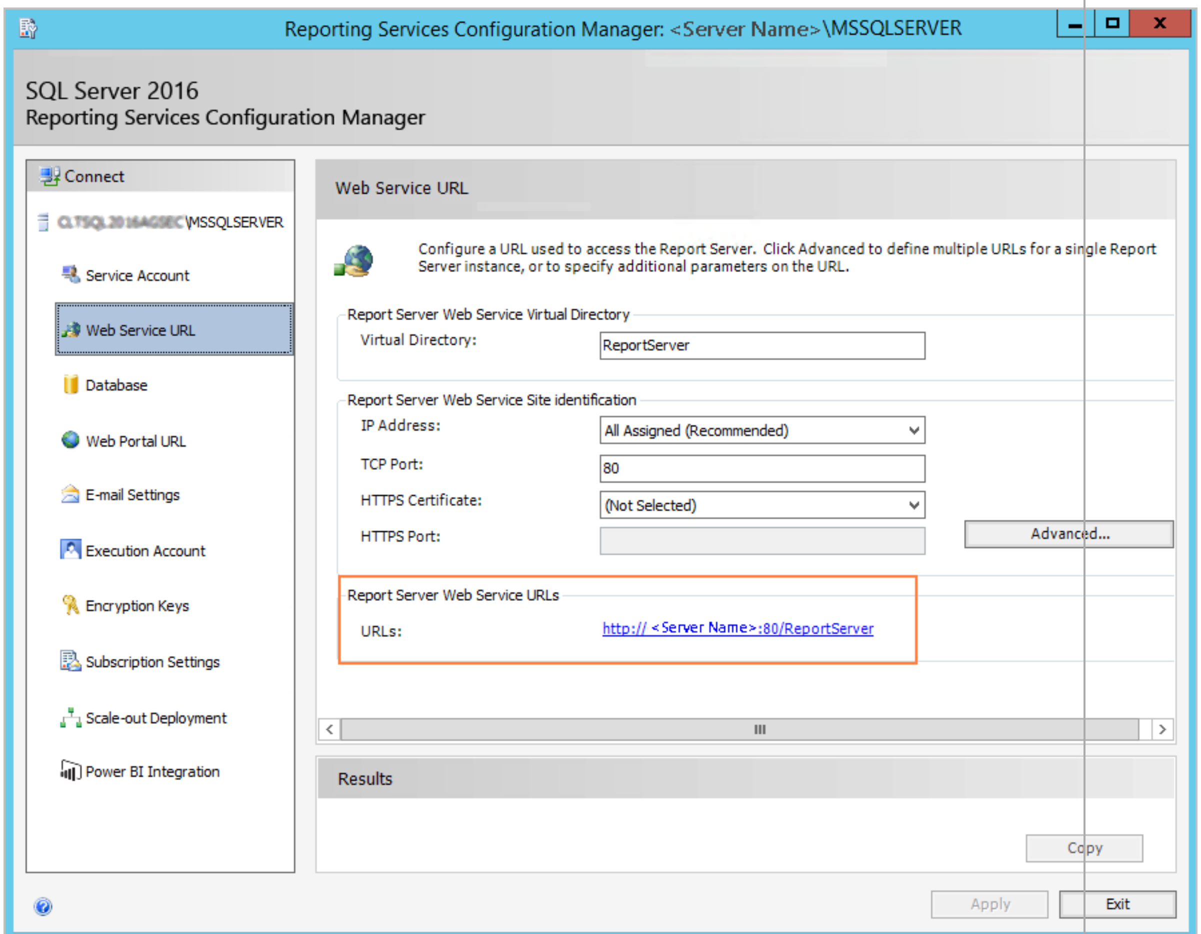


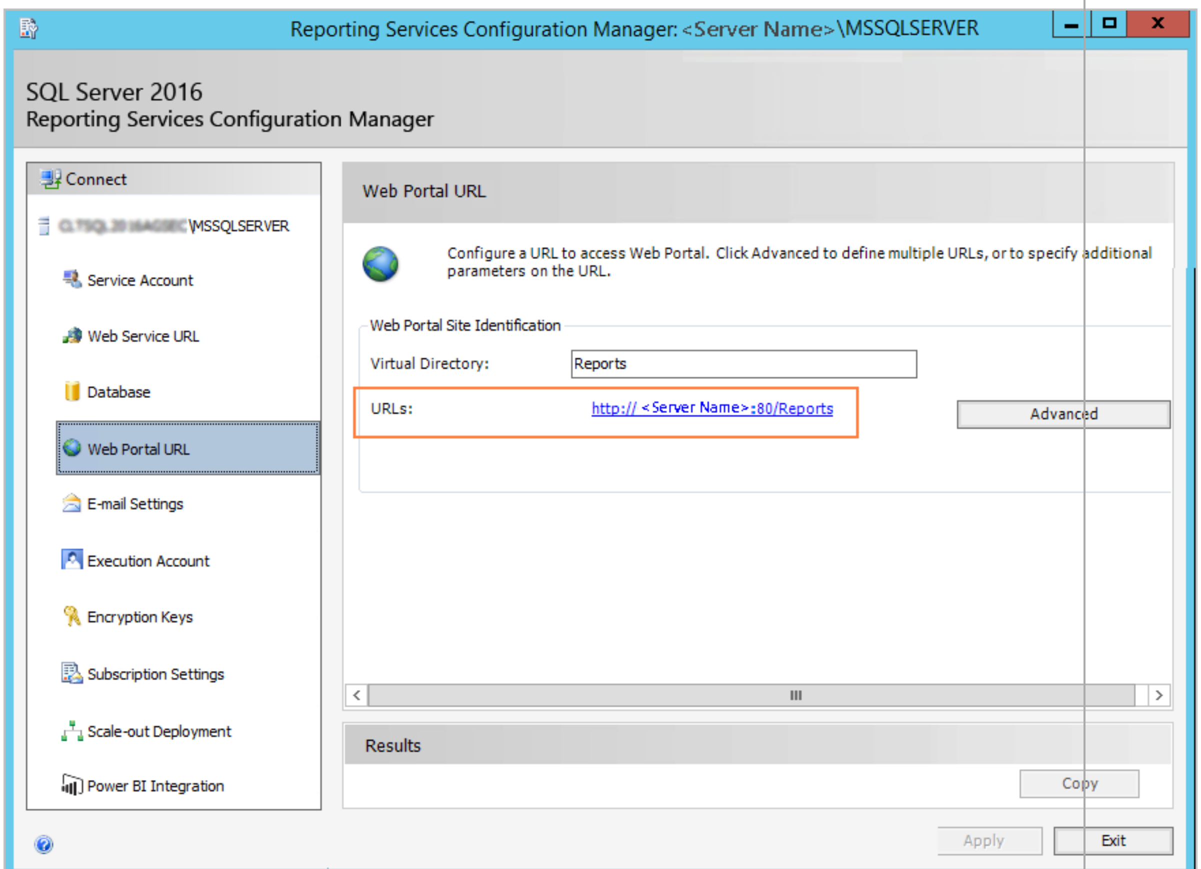
SSRS Reports Tab Fields

Field	Description
Install SSRS Reports	Select this check box to enable the fields on this tab.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Service URL</td><td>Specify the Web Service URL configured to access the Report Server. The specified URL will be stored in the web.config file.

This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager.


</td></tr>
</table>

Field	Description
SSRS Web Portal URL	Specify the Web Portal URL configured to access the Web Portal. The specified URL will be stored in the web.config file. This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager page. 
Data Source Name	Specify the name of the Anthology Student database that is the source for the reports.
Reports Folder	Specify the path for the reports folder on the Report Server. A folder will be created if one does not exist. The folder name can be unique to the environment. The reports folder root path will be stored in the web.config file. *Example* `QA/CNS` where `QA` is one folder and `Student_Test` is a folder under `QA`.
Database Authentication Options	
Override Global Settings	Optional: Select this check box to enable the database authentication options.

Field	Description
Use SQL Authentication	Optional: Select this check box if SQL authentication is applied.
Username	Enter the user name of the account that is given override permissions for the SSRS reports database.
Password	Enter the password of the account that is given override permissions for the SSRS reports database.
Test	Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

In addition to the settings on the SSRS Reports tab in Installation Manager, the setup of reporting services requires configurations in the SQL Server Reporting Services Configuration Manager (see Configure Access to Reports).

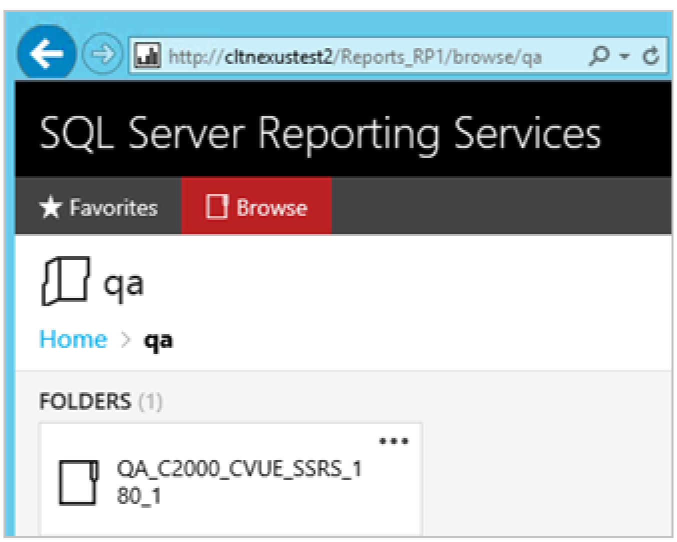
You also need to create folders in the Anthology Student and assign permissions using the Security Console. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Configure Access to Reports

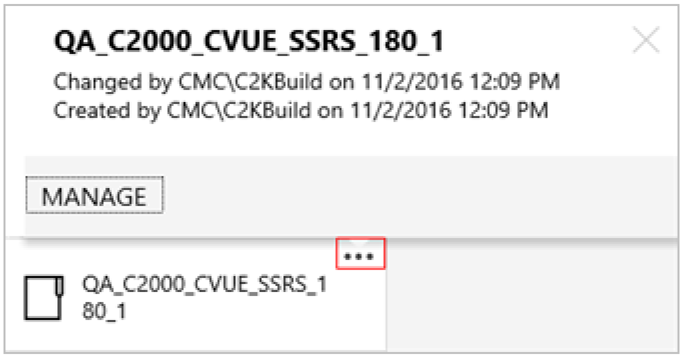
To enable access to the “Reports” menu item in Anthology Student, perform the following steps in the Reporting Services Configuration Manager on the report server:

a. Navigate to the /Reports folder path.

   In the example below the reports folder path is `http://cltnexustest2/Reports_RP1/browse/`**qa**.



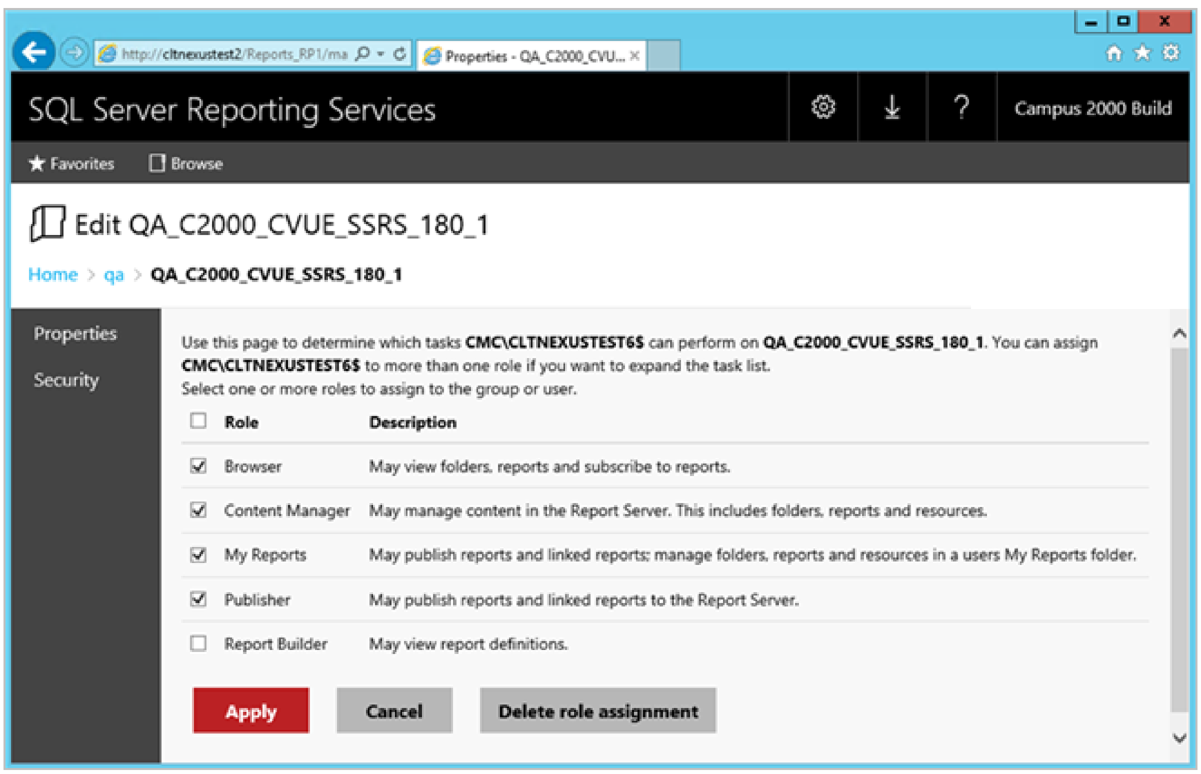
b. Right-click on the ellipsis of the reports folder root and select **Manage**.



c. Select the **Security** tab, click **Customize security**, and click **Add group or user**.

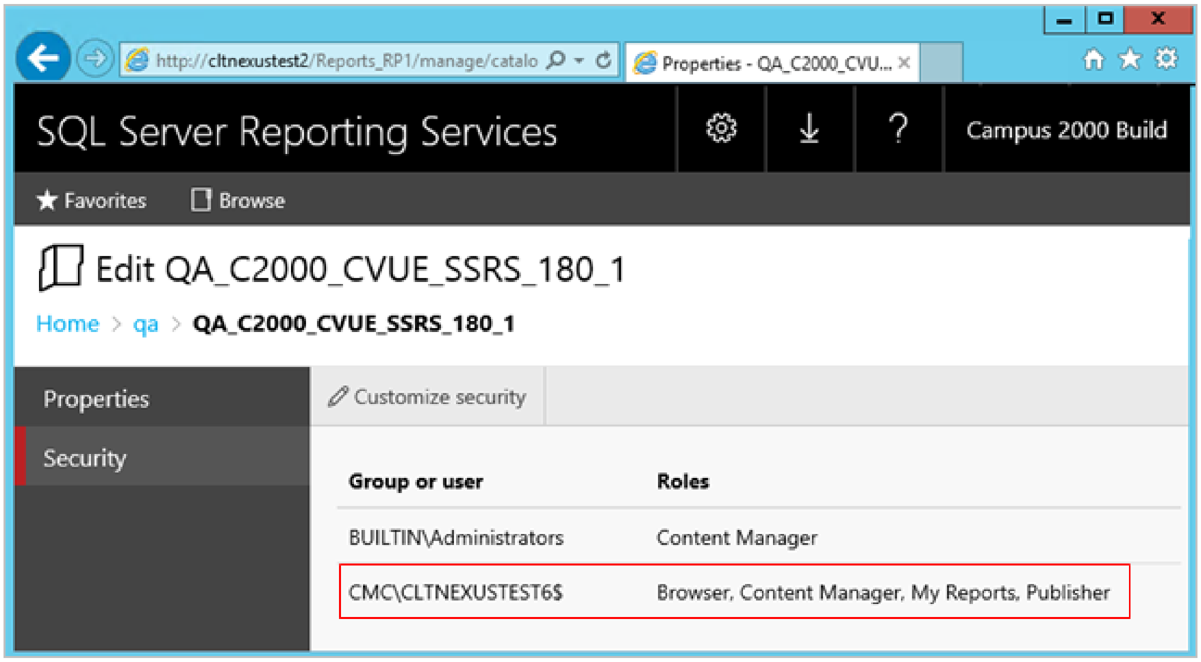
d. Add the **domain\<machine name$>** of Anthology Student and select the following **Roles**:

- Browser
- Content Manager
- My Reports
- Publisher



e. Click **Apply**.

Security for the Reporting Service should be set up as shown below, where CMC\CLTNEXUSTEST6 is the domain\machine name of Anthology Student from which the reports are accessed.



Configure SSRS for HTTPS

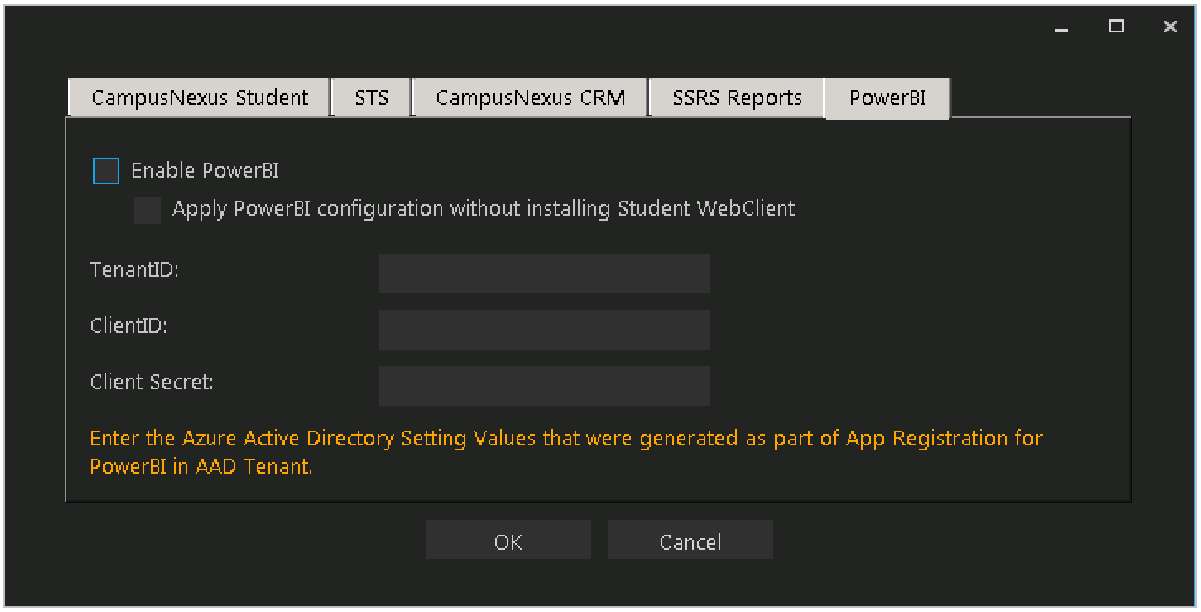
Once the reporting services are installed and configured, test access to the reports in Anthology Student. Select the Reports tile and navigate to any report listed in the menu.

If Anthology Student displays only the title of the report (without any data selection fields), use the browser developer tools (**F12**) and check the **Console** tab. If an error similar to the following is displayed, configure SSRS for secure access with an SSL certificate. For detailed instructions, see https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-ssl-connections-on-a-native-mode-report-server

```
⚠ Mixed Content: The page at 'https://googlesamples.github.io/web-      jquery.js:5562
  fundamentals/samples/discovery-and-distribution/avoid-mixed-content/image-gallery-
  example.html' was loaded over HTTPS, but requested an insecure image
  'http://googlesamples.github.io/web-fundamentals/samples/discovery-and-
  distribution/avoid-mixed-content/puppy.jpg'. This content should also be served
  over HTTPS.
```

Power BI Tab

If Power BI used for applications such as Occupation Insight or Analytics, configure settings on the Power BI tab. Enter the Azure Active Directory Setting values that were generated as part of the web application registration for the Power BI in the AAD tenant.



Power BI Tab Fields

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Enable Power BI</td><td colspan="2">Select this check box to enable the Power BI setting fields.</td></tr>
<tr><td>Apply Power BI configuration without installing Student Web Client</td><td colspan="2">Select this check box if Power BI is used without installing the standard interface (web client) for Anthology Student.</td></tr>
<tr><td>Tenant ID</td><td>Specify the Azure tenant identifier.</td><td rowspan="3">Customers create app registrations in their Azure AD tenant and provide the Tenant ID, Client ID, and Client Secret that are generated as part of creating the app registration.

Note: One app registration is created for Anthology Student legacy interface and standard interface.</td></tr>
<tr><td>Client ID</td><td>Specify the Azure client identifier.</td></tr>
<tr><td>Client Secret</td><td>Specify the Azure client secret.</td></tr>
</table>

8. Click **OK** to save changes on the Options form. The form is closed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

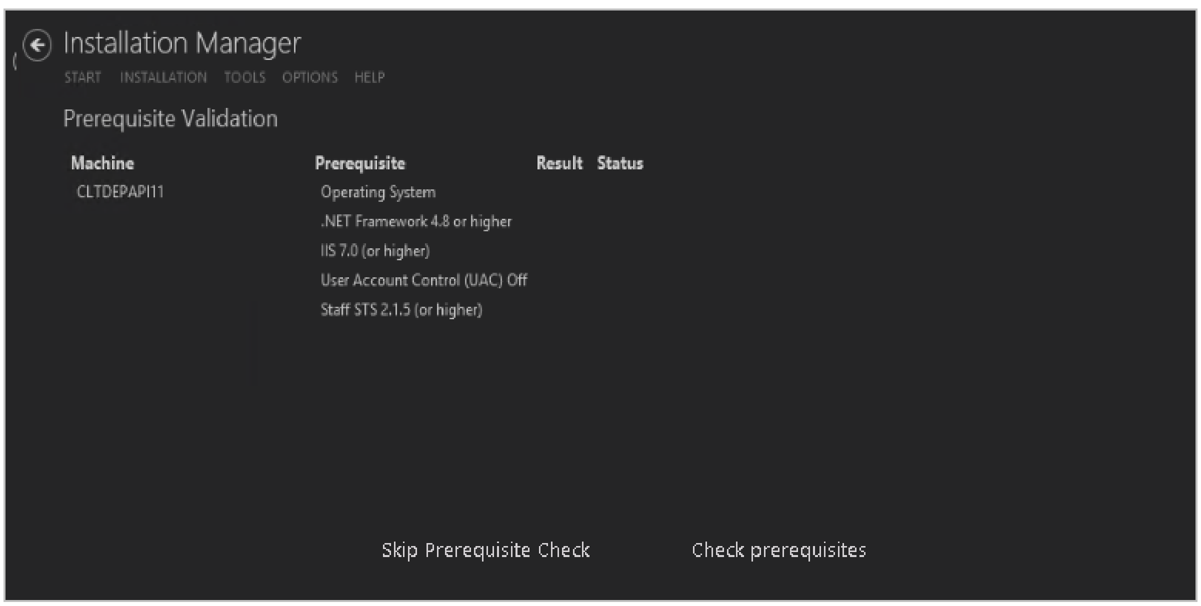
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

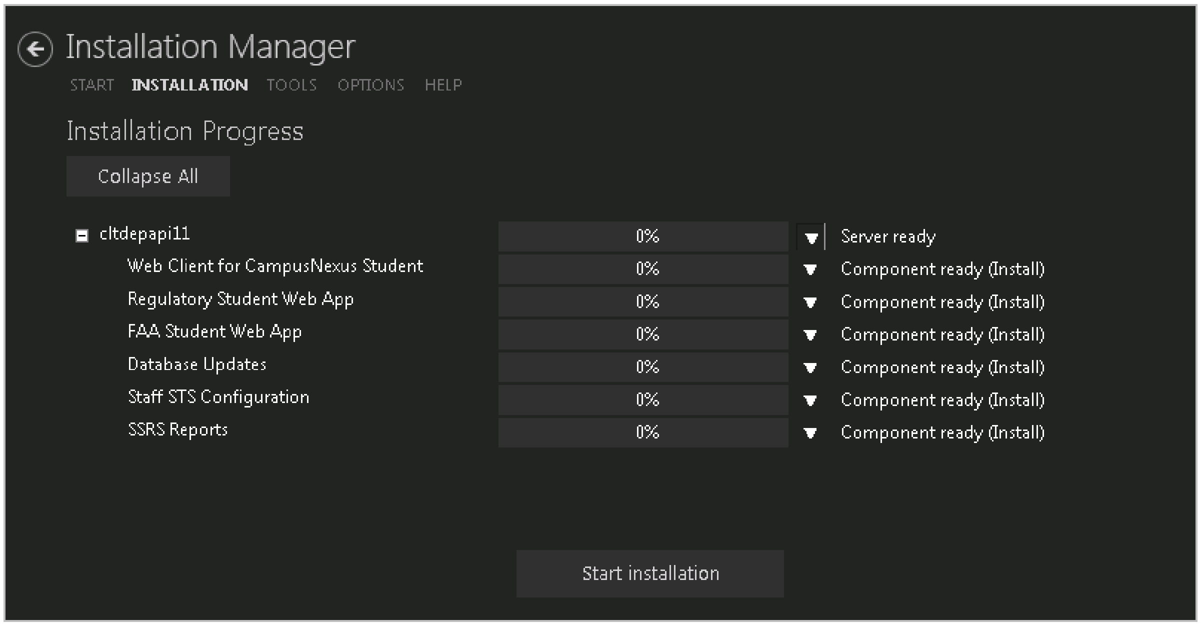
    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.



4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click  next to a progress bar to access installation logs and other tools (see Installation).

Continue with the Postinstallation Tasks.

Postinstallation Tasks

After installing Anthology Student, ensure that the web application can be accessed and that an initial administrative user has sufficient permissions to view the web application.

Resolve Port Conflicts

By default Installation Manager installs Anthology Student on the IIS Server's Default Web Site under "Cmc.Nexus.Web". If other websites are hosted on the same IIS Server, ensure that there are no conflicts in the ports used by different websites. If necessary, change the port used by Cmc.Nexus.Web in the web.config under

```
<add key="WSFedRealm" value="http://<server name>:<port>/Cmc.Nexus.Web/"/>
```

Test the Administrator Login

Access the URL for the Cmc.Nexus.Web site in a browser and log in as administrator:

After you click the **Sign In** button, the following message is displayed: *"Access denied. Only members of CampusNexus Web group are allowed access."*

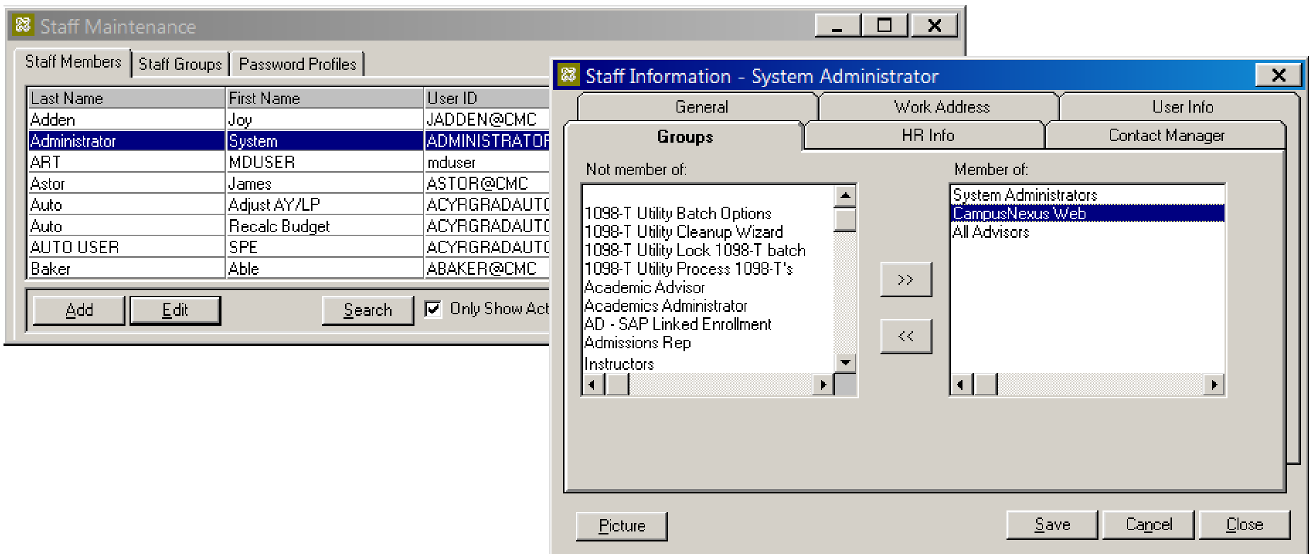
This message indicates that the administrator needs to be added to the **CampusNexus Web Group** in the legacy interface (desktop) for Anthology Student. The CampusNexus Web Group is created by scripts during the installation of Anthology Student.

Assign the Administrator to the Web Group

To give the administrative user permissions to log in to Anthology Student, the user needs to be added to the CampusNexus Web group.

1. In the legacy interface for Anthology Student, navigate to **Setup > Staff**, select **Administrator** in the Staff Members list, and click **Edit**.

2. In the Staff Information form, select the **Groups** tab, click  to make the Administrator a Member of the **CampusNexus Web** group, and click **Save**.



3. Access the URL for Cmc.Nexus.Web in a browser again and log in as administrator. Now, the browser displays the header of the Anthology Student and indicates that the System Administrator is logged in.

The administrative user now has login permission, but cannot perform any tasks in Anthology Student. We now need to give the user permissions to view, create, edit, or delete data. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Change the Web Client URL on Upgrade

> ⚠ If you change the Web Client URL during an upgrade in an environment where Forms Builder is used, the Web Client URL must be manually updated in the web.config files of Forms Builder Designer and Forms Builder Renderer (search for 'baseURL').

```
<fieldsServiceConfigSection>

<products>

<add name="Student" commandModelPath="/api/commands/Core/Metadata/get" odataPath-
h="/ds/campusnexus" mod-
ules-
s="Academics,Admissions,CareerServices,Common,Crm,FinancialAid,StudentAccounts,StudentServices"
baseUrl="http://CLTQAAPI10.campusmgmt.com:80/Cmc.Nexus.Web/" enabled="true"/>
```

Security Console

After installing Anthology Student, proceed to install the Security Console. The Security Console is used to manage authorizations for Anthology Student and set permissions for all active staff members to use the features in Anthology Student.

You can install Security Console using either of the following options:

- Installation Manager
- ClickOnce

Prerequisites

The Security Console requires:

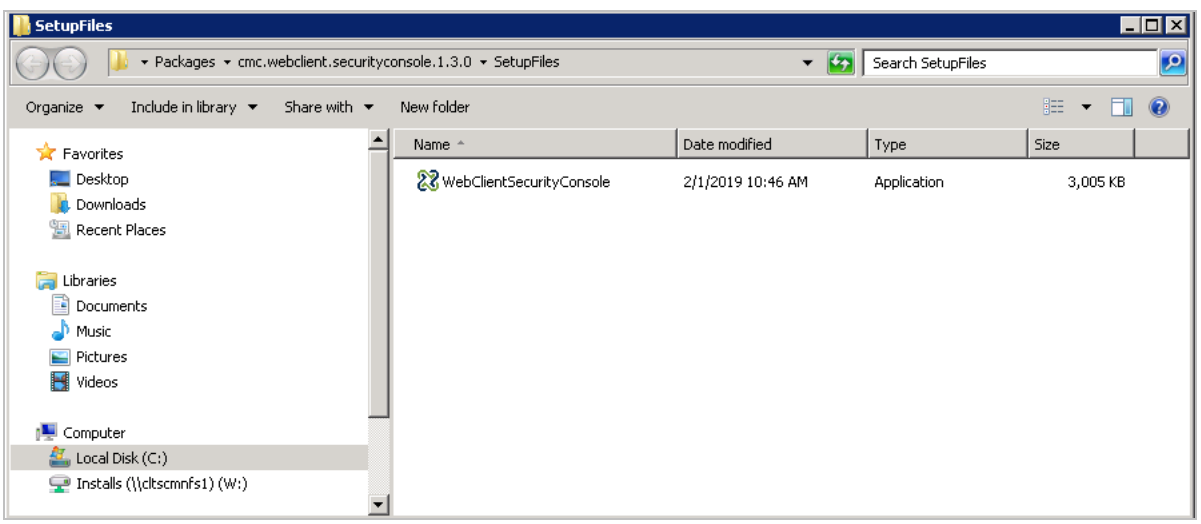
- Microsoft .NET Framework 4.8 (x86 and x64)
- .NET Framework 3.5 SP1

Install the Security Console

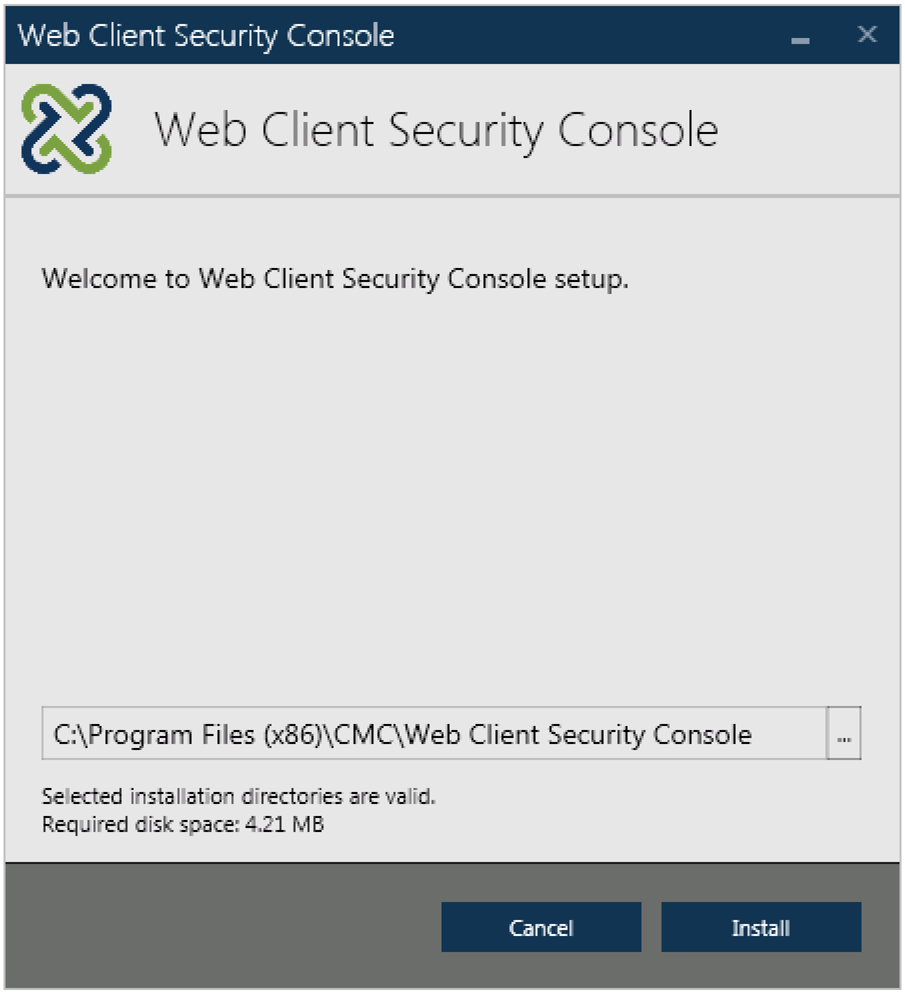
Install Using Installation Manager

1. Click the **Package Manager** tile in the Start screen of Installation Manager.
2. Download the package for the **Security Console**.
3. When the download is completed, return to the Start screen of Installation Manager.
4. Click the **Web Client Security Console** tile in the Start screen.

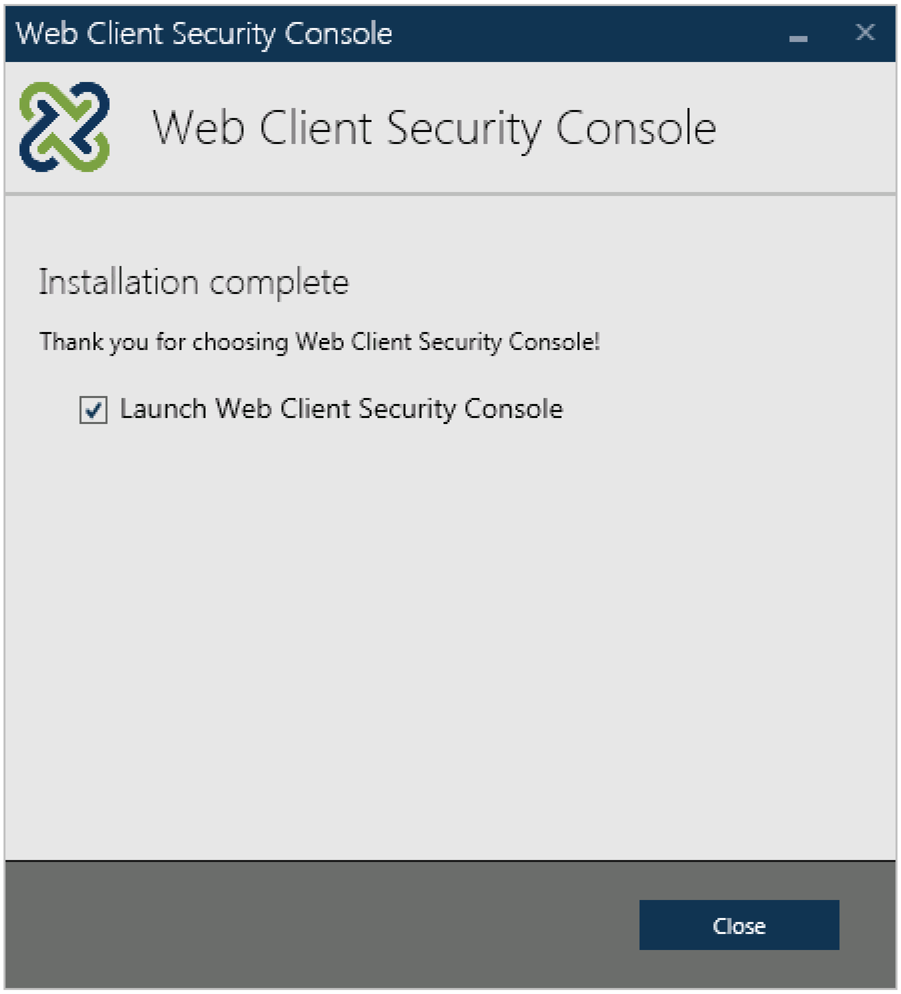
   File Manager displays the SetupFiles folder containing the WebClientSecurityConsole.exe file. You can run the .exe installer directly or copy and distribute it to other users within your organization.

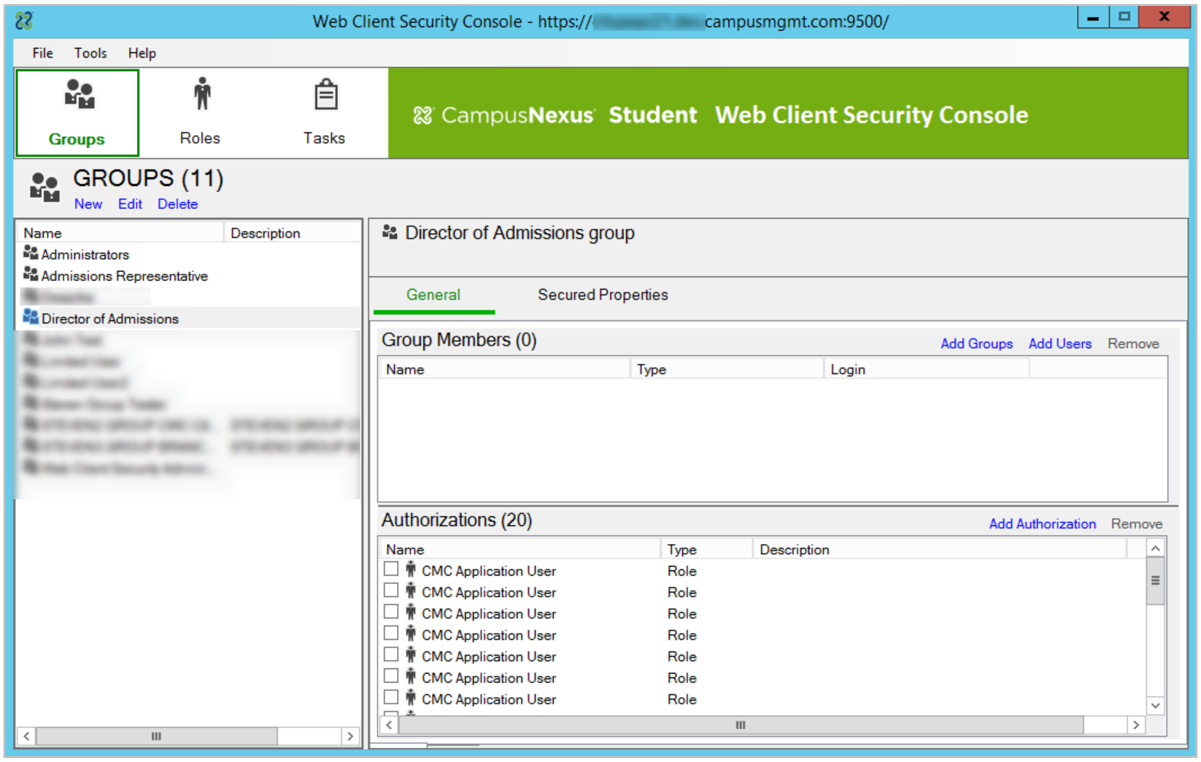
5. Double-click the **WebClientSecurityConsole.exe** file. The Welcome screen is displayed.



6. Click **Install**. The Installation Complete screen is displayed when the process is done.



7. Click **Close**. The Connect dialog is displayed.
8. Specify your Anthology Student sign in.
9. Click the **Connect** button. The Security Console is displayed when the connection is successful.



Install Using ClickOnce

Anthology Cloud 2.0 customers install Security Console 2.0 using a ClickOnce application. ClickOnce allows self-updating Windows-based applications to be installed and run with minimal user interaction. Users install the Security Console with one click on the **Install** button or **launch** it from a website.

For details about the ClickOnce URL and login credentials, refer to **https://filetransfer.campusmgmt.com** > **softwareupdates** > **SecurityConsole** > **SCInstallationSteps.pdf**.

Locate Additional Information for Using the Security Console

Refer to the *Administration and Configuration Guide* for using the Security Console at https://help.campusmanagement.com/Content/DocSets/CNSDocSet.htm.

Student Legacy Interface

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

Installation Manager supports the installation of Anthology Student including all of its components and optional modules.

The core components are:

- Legacy interface
- SQL Server database
- Business Objects (COM+ platform)
- Web Services (APIs)

Optional modules that enhance the client functions of Anthology Student include:

- Financial Aid Automated Processes (FAA)
- Regulatory
- Add-ons such as STAR COD Transfer Manager

Prerequisites

- Anthology Student version 19.0.3 or later requires Staff STS version 2.1.2 or later.

- The database for Anthology Student version 19.0.4 or later requires Microsoft SQL Server 2016 or later.

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Recommended Environments

The recommended deployment architecture is referred to as a “4-tier” configuration. The SQL Server, Business Objects (COM+), Web Services (APIs), and legacy interface are hosted on separate machines. This configuration gives the most stable and responsive system for a live production environment.

For a testing and evaluation environment, a “3-tier” architecture may be implemented (COM+ and client components on the same system). This configuration is not recommended for a production environment.

Note: For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Enterprise (Large-Scale) Environments

- Dedicated 64-bit SQL server machines with the Anthology Student “Transaction” database and a replicated Anthology Student “Reporting” database
- Separate COM+ Business Objects servers — Load balanced if multiple machines
- Citrix machines with Anthology Student client and COM+ proxies installed — Load balanced if necessary
- Dedicated Web Services / Automated Processes systems — Load balanced if multiple machines

Distributed (Small-Scale) Environments

- Dedicated 64-bit SQL server with the Anthology Student database
- Separate machines with COM+ Business Objects and the legacy interface for Anthology Student

  Note: If the legacy interface and COM+ are on the same machine, MDAC v2.8 **MUST** be installed
- Separate Anthology Student client machines
- Dedicated Web Services system

Test / Staging Environments

- Dedicated SQL server with the Anthology Student database
- Separate machine with COM+ Business Objects and the legacy interface for Anthology Student
- Web Services test system (with IIS installed)

  Note: This testing configuration is not recommended for a production environment.

Accounts and Permissions

Before running the Anthology Student installation, ensure that the following accounts and permissions are created.

Windows Admin Account

Prior to the initial installation of Anthology Student, an administrator account must be established on all machines where the software will be installed. This should be an administrator ID with a password that never expires. If the password expires, Anthology Student must be reinstalled.

The Windows Admin account is used to:

- Run the install task on each machine when installing.
- Verify access to the COM+ server when Anthology Student is started.
- Enable API access to the database.

The user account that is being used (logged into) while running Installation Manager must be configured for each machine where the Anthology Student application will be installed. This account is used for permission to copy the installation files to each remote machine. With recent Microsoft security patches, the Windows Admin ID must also be added to the Backup Operators group on all systems. This account must also be enabled as an Administrator for the SQL Server instance.

The admin account must have the "Log on as a batch job" permissions (which generally are assigned to the Backup Operators group). This permission may be applied to the local administrators group depending upon the security policy permissions applied for the installation domain.

Student Administrator Account

An Anthology Student administrator account must also be set up for installation. The Web Services API uses this account for its access and Anthology Student permissions. The password for this administrator account cannot contain the special characters ^ | &” < >.

Permissions for the C2000 Share

Installation Manager checks for an existing C2000 share on the machine and installs to that folder. If the C2000 folder does not exist, Installation Manager creates the folder in C:\Program Files\CMC\C2000 (for Windows Server 32-bit systems) or in C:\Program Files (x86) for 64-bit systems.

The user account that is logged in while running Installation Manager and the Windows Admin account must have full access permission to the C2000 share for the installation to complete successfully.

Global Settings

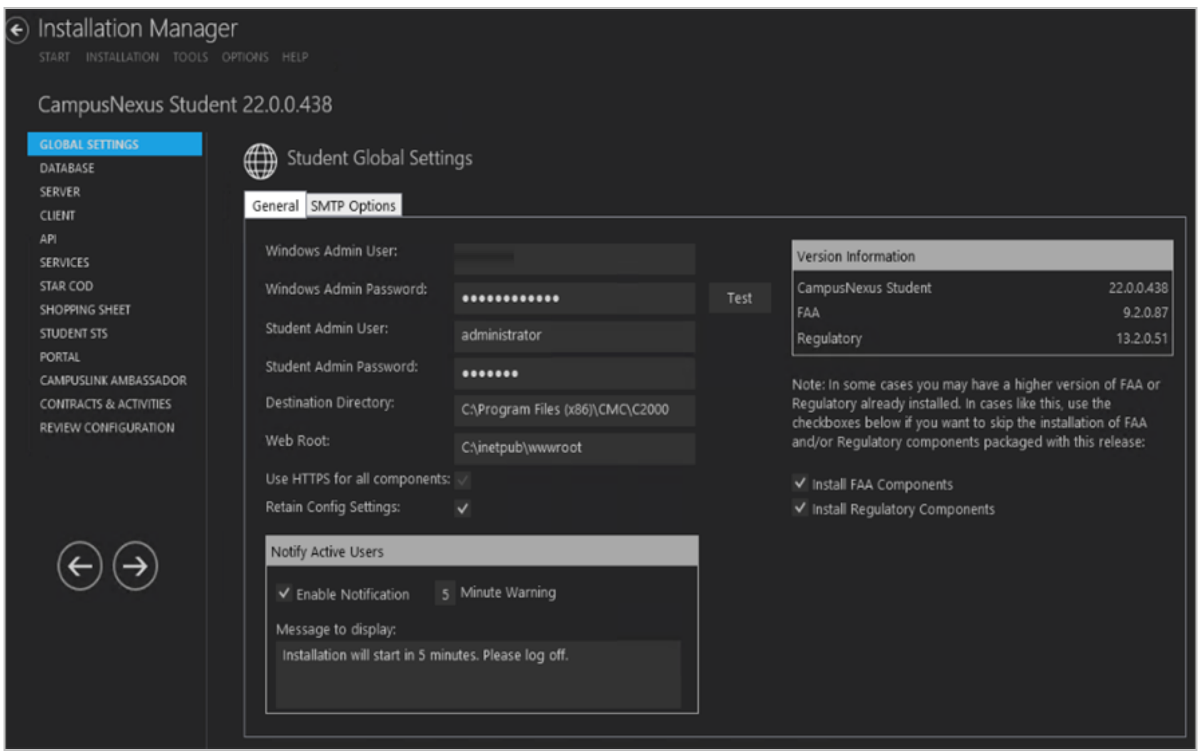
The Global Settings screen contains the Windows Admin user name password used when starting an installation of the legacy interface for Anthology Student. Users can also test this information without moving from the screen.

The **Version Information** displayed on this screen indicates the versions of Financial Aid Automation and Regulatory that are compatible with the Anthology Student version to be installed. Financial Aid Automation and Regulatory can be installed with Anthology Student (see Services) or added later.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Anthology Student** tile. The Global Settings screen is displayed.



2. Complete the fields on the Global Settings tab as described in the table below.

General Tab Fields

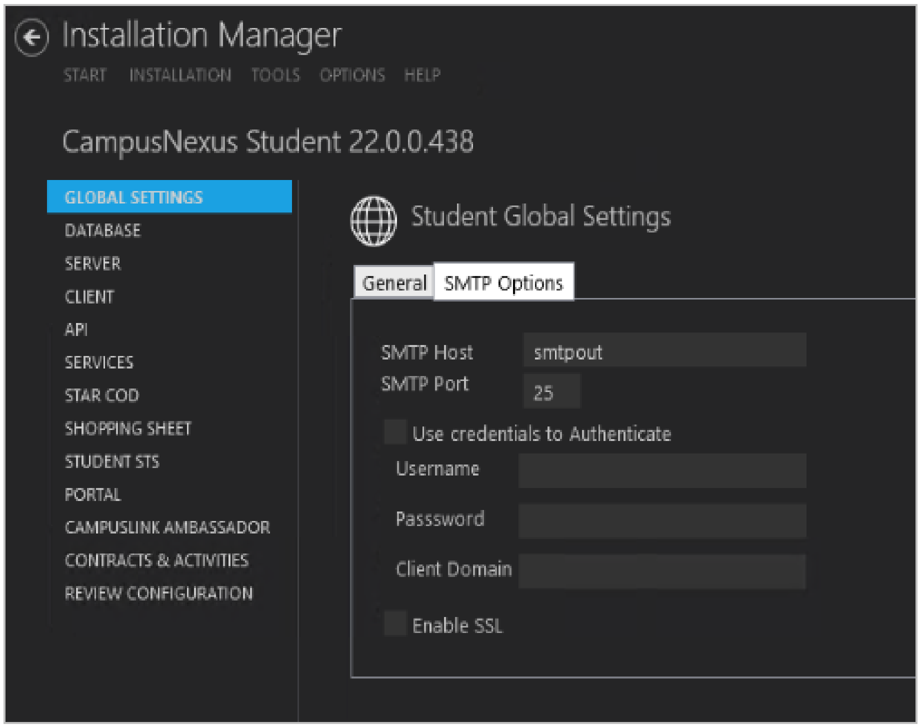
Field	Description
Windows Admin User	Specify the user name of the user with administrator permissions on the computer where the COM, Windows, and Web Services will run. This account must have administrative access to all the machines being installed to. It must be a sysadmin on the database as integrated security is the only option that will be used. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Windows Admin Password	Specify the password for the Administrator user name. This password is used in the background for other installation steps. **Note**: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.
Student Admin User	Specify the user name of the Anthology Student user with administrator permissions. This is the Anthology Student administrator account that the Windows and Web Services use for Anthology Student access. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Student Admin Password	Specify the password for the Anthology Student Admin User.
Destination Directory	The default directory for the Anthology Student legacy interface and Server is C:\Program Files (x86)\CMC\C2000. You can override the default by choosing another path.
Web Root	The default web root for the APIs to be installed is C:\inetpub\wwwroot. You can override the default by choosing another path.
Use HTTPS for all components	This option is selected by default and cannot be cleared. All components must use HTTPS.
Retain Config Settings	Select the Retain Config Settings check box if you want to deploy the latest web.config file and also run a config merge that will merge any settings that were set outside of the install process. If Retain Config Setting is not selected, the install process will not retain and will not merge any configuration settings that were set outside of install process.
Notify Active Users	
Enable Notification	Select this check box to enable notification of active Anthology Student users when an installation is about to begin.
Minute Warning	Specify the notification time, that is, the number of minutes until the installation starts.
Message to display	Enter the message to be displayed in the notification window.

Field	Description
Version Information	
Install FAA Components	This check box is selected by default. Clear the check box to skip the installation of FAA components if you have already installed a higher FAA version than the one listed in the Version Information field.
Install Regulatory Components	This check box is selected by default. Clear the check box to skip the installation of Regulatory components if you have already installed a higher Regulatory version than the one listed in the Version Information field.

3. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
4. On the **SMTP Options** tab, provide the following information:
   - In the **SMTP Host** field, enter the domain address of the SMTP host used for sending out email notifications from Anthology Student, e.g., smtpout.campusmgmt.com.

     Enter the Email (SMTP) Server address used for sending out email notifications by doing the following:

     a. Determine the desired Email (SMTP) Server IP address and DNS names.
     b. On the Exchange Server, an entry for an open relay on TCP Port 25 must be allowed and open to receive SMTP traffic from the MTS Server. This traffic must not be routed through a firewall. OSI Layer 7 firewalls can interfere with the service.
     c. Ping the Email (SMTP) Server from the MTS Server and the SQL Server.
     d. Telnet to the Email (SMTP) Server on Port 25 and verify successful connection from the MTS Server.
     e. Enter the IP address in the SMTP Server field.
   - Specify the **SMTP Port** number or accept the default (25).
   - Select **Use credentials to authenticate** and enter the **Username** and **Password** of the sender's email account.
   - If applicable, select **Enable SSL**.



5. Click  to continue.

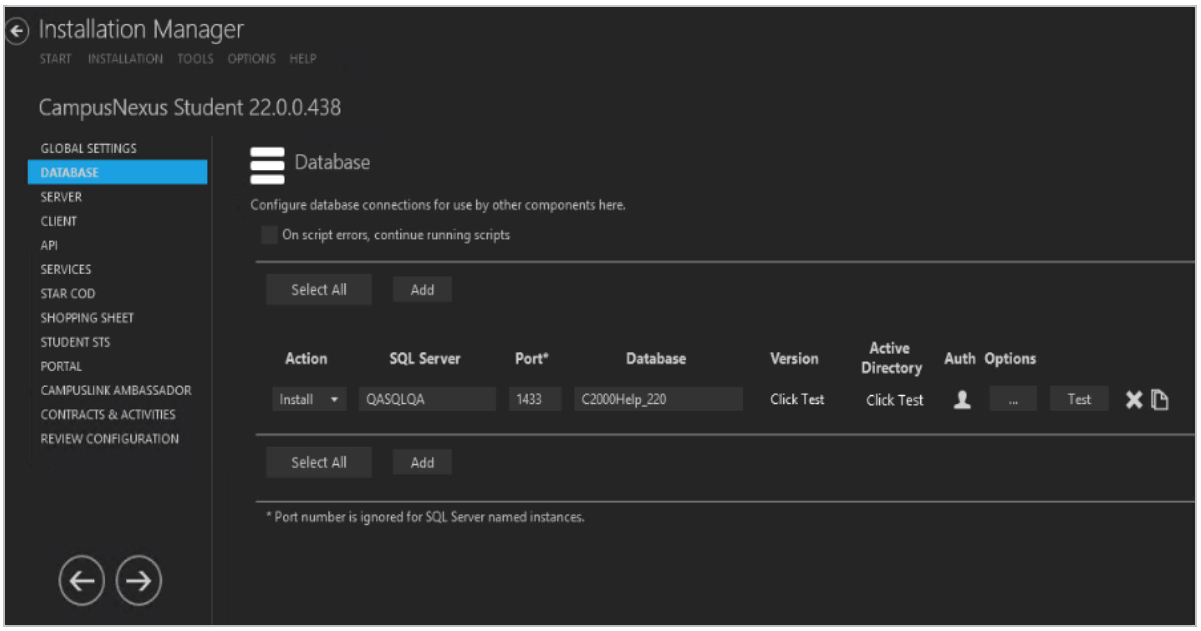
Database

This screen enables you to select the actions to be taken by Installation Manager (e.g., install) and to specify the machine name, the Anthology Student database, and, if applicable, additional databases for Portal and Talisma Fundraising.

The database for Anthology Student 19.0.4 and later requires **.Microsoft SQL Server 2016** or higher. The prerequisites check will fail for lower versions.

Set Up the Database

1. In the Installation menu, click **Database**. The Database screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

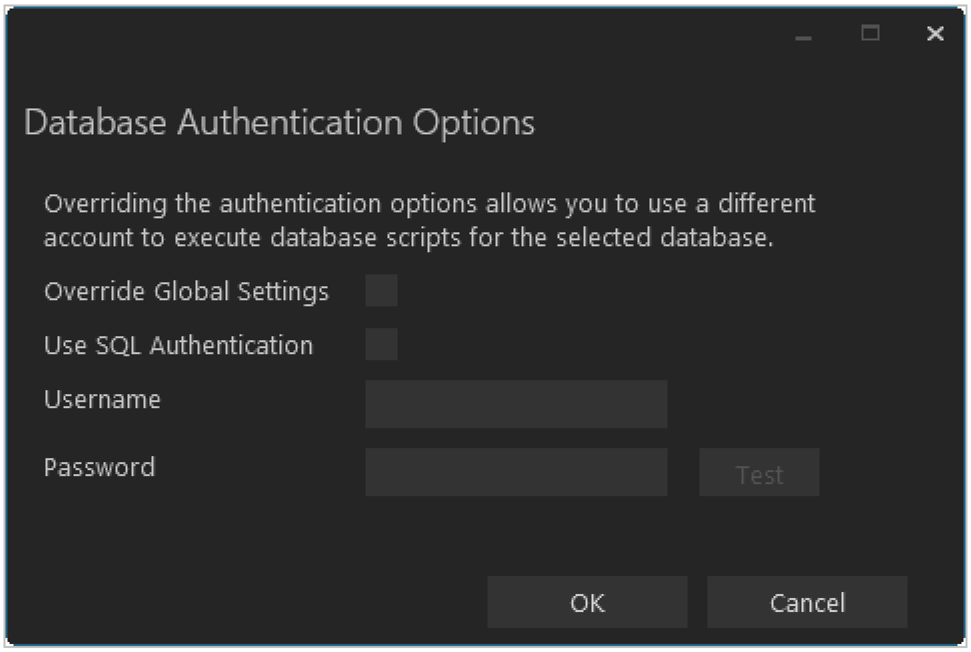
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the name of the **SQL Server** where the Anthology Student database is installed.
5. Specify the **Port** number of the SQL server or accept the default (1433).

6. Specify the name of the **Database** for Anthology Student. The database name must be unique — 'master' is not allowed.

7. The **Version** field is populated when you click the **Test** button.

8. The **Active Directory** field is populated when you click the **Test** button.

9. Click in the **Auth** column if you want to override the authentication options from Global Settings for the selected database, for example, to give another user permissions to execute scripts for the selected database. The Database Authentication Options form is displayed.



   a. Select the **Override Global Settings** check box to enable the fields on the form.

   b. Optional: Select the **Use SQL Authentication** check box if SQL authentication is applied.

      The license checks, version number check, SQL script execution, student admin role check, and MSI parameters will use SQL authentication if selected.

   c. Enter the **Username** and **Password** of the account that is given the override permissions for the selected database.

   d. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

   e. Click **OK** to save changes on the Options form. The form is closed.

10. Select the check box for **On script errors, continue running scripts** if you want the installation process to continue regardless of errors encountered.

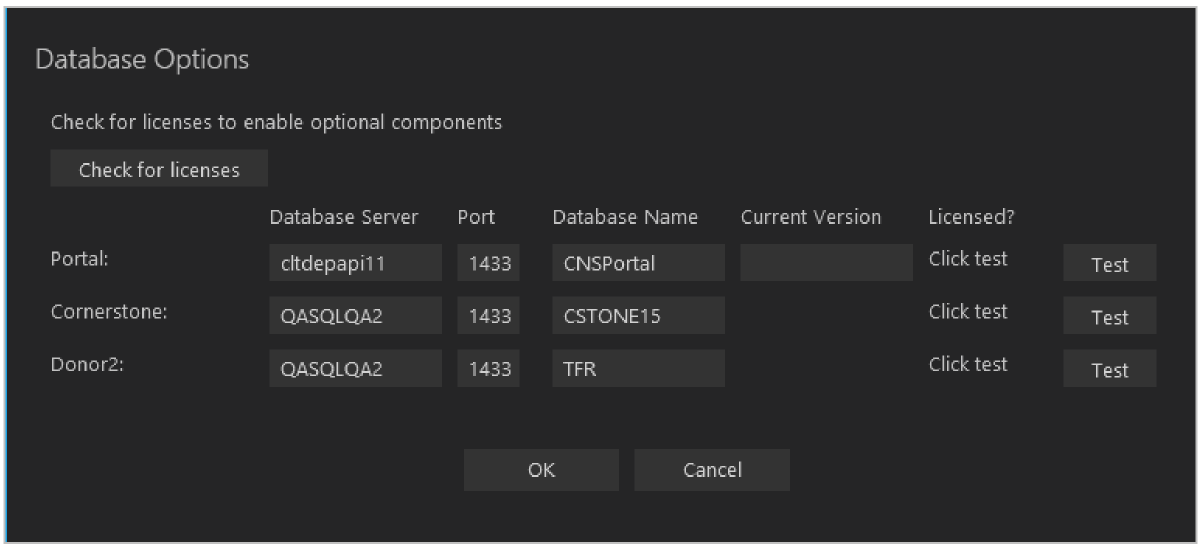
By default, database upgrades will stop if the script encounters any errors. This selection is used if there are custom modifications to the database that are known to cause errors in the upgrade scripts. Selecting this option enables all scripts to be run against the specified database.

Whether the check box is selected or not, any errors are written to a separate error file for each script, which may be investigated after the script execution. Error logs are stored in the following folder: `DatabaseServer\C:\Logs\Output`.

The error log is the name of the script, SQL Server, and database name appended with `_Errors.txt`, for example,
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Errors.txt`)

There is also an output file that has all of the script output:
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Output.txt`

11. Click  to view and edit the Options form.



The Options form is used to specify databases for Portal and Talisma Fundraising. Corresponding licenses are required.

- Entering a Portal database is only necessary for an installation that includes the e-Learning component that has a Portal component and license key associated with Anthology Student.
- The Cornerstone and Donor2 databases are used for Talisma Fundraising in conjunction with the primary Anthology Student database. Installation Manager detects if Talisma Fundraising is enabled in the Anthology Student database.

Database Options Fields

Field	Description
Check for Licenses	This button queries the Anthology Student database and checks for product licenses. Based on the licenses found, Installation Manager enables the **Portal**, **Cornerstone**, and **Donor2** fields. If the licenses are not found, the Licensed? field indicates "False" and the fields remain disabled.
Database Server	Name of the SQL server on which the database resides.
Port	Specify the port number of the SQL server or accept the default (1433).
Database Name	Name of the SQL database.
Current Version	This field is populated when you click the **Test** button.
Licensed?	Indicates whether a license for the product is available.

12. Click **OK** to save changes on the Options form. The form is closed.
13. Click  to copy a line. Edit the copied line as needed.
14. Click  to delete a selected line.
15. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Note: The Test button operates as follows:

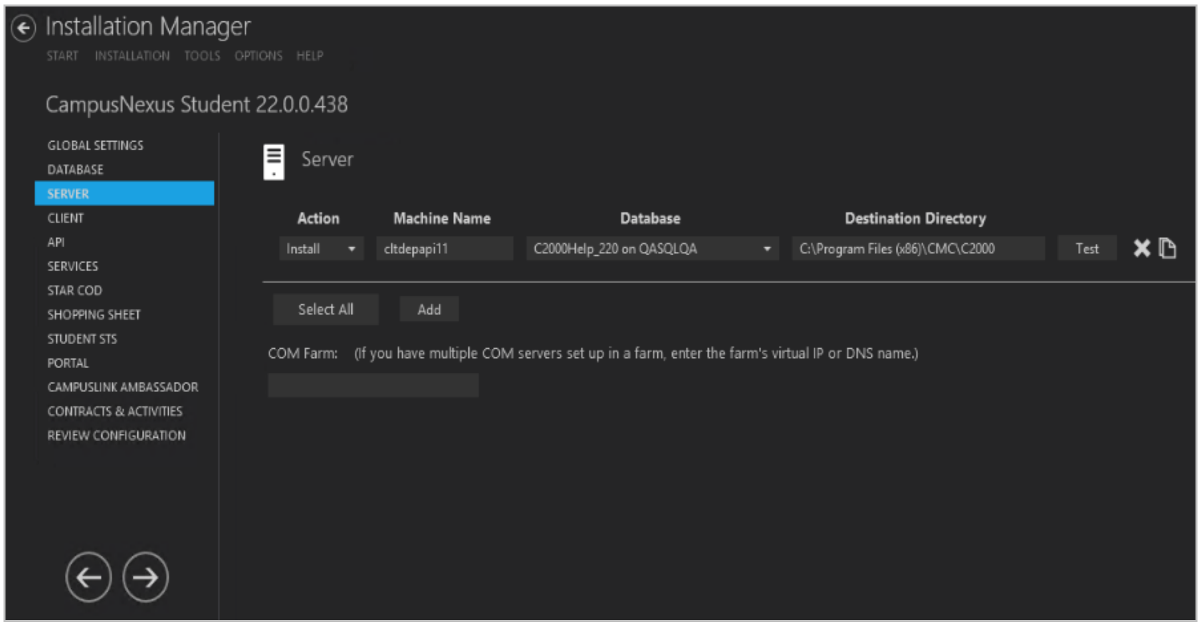
    - Queries the database to get the latest version of Anthology Student and populates the current version field.
    - Uses Windows Admin credentials (see Global Settings) and tests connectivity to the SQL server.
    - Uses the Student Admin user name (see Global Settings) and checks if it exists in the Anthology Student database.
16. If all tests pass, click .

Server

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and database connection of the COM Server for Anthology Student.

Set Up the Server

1. In the Installation menu, click **Server**. The Server screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the COM server for Anthology Student will be installed.
5. Select the name of a **Database** for Anthology Student. The drop-down list contains all Anthology Student databases configured in the Database settings screen.

   Notes:

- Only one Server can be installed against one database.
- Multiple Servers can be installed against different databases.

6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
7. Click  to copy a line. Edit the copied line as needed.
8. In the **COM Farm** field, enter the farm's virtual IP address or DNS name if you have multiple COM servers set up in a server farm with a load-balancing system.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

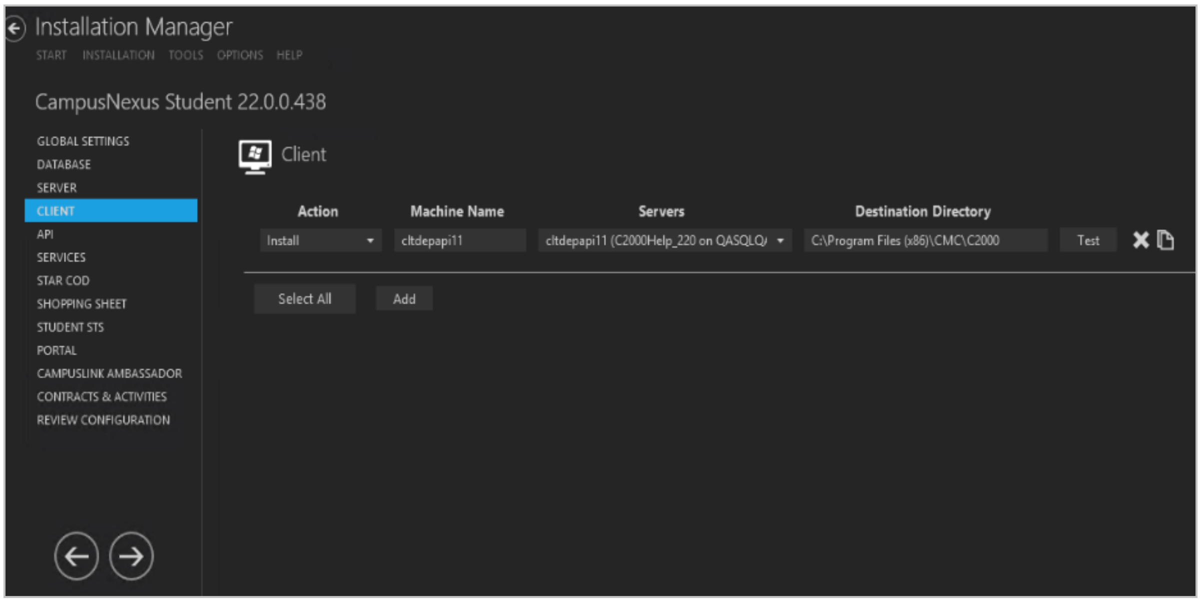
    Note: The Test button uses the Windows Admin credentials (see Global Settings) to test connectivity to the machine specified in the Machine Name field on the Server screen (this screen).
11. If all tests pass, click .

Client

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and server connections of the legacy interface (desktop client) for Anthology Student.

Set Up the Client

1. In the Installation menu, click **Client**. The Client screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the legacy interface for Anthology Student will be installed.
5. In the **Servers** field, select the name of a server. The drop-down contains a list of Servers configured in the Server settings associated with the Anthology Student database.

   Example

COM1 (CNS_171 on QASQLQA1)

Where *COM1* is the COM Server, *CNS_171* is the Anthology Student database, and *QASQLQA1* is the SQL server where the Anthology Student database resides.

Note: Multiple clients can be installed against one server.

6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
7. Click to copy a line. Edit the copied line as needed.
8. Click to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

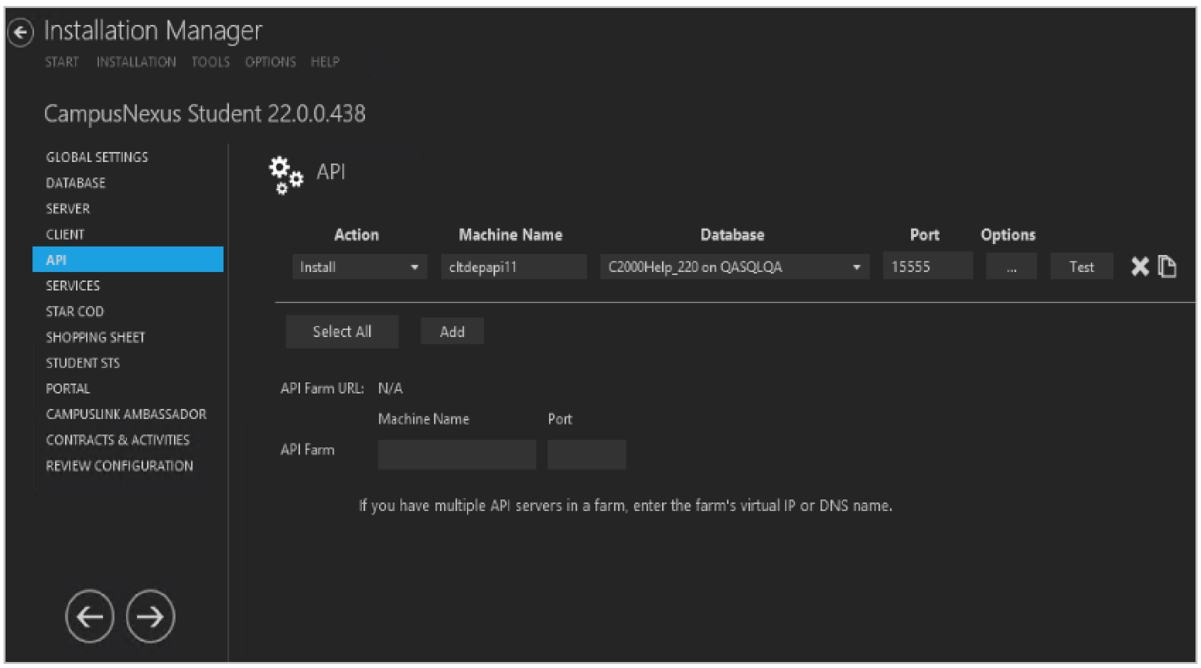
API

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database server, and port to be used by the Web Services (APIs) for Anthology Student.

> The APIs for Anthology Student 19.0 and later require **.NET 4.6.2** or higher. The prerequisites check will fail for lower versions.

Set Up the APIs

1. In the Installation menu, click **API**. The API screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed. This is the machine where the APIs for Anthology Student will be installed.

5. In the **Database** field, select a database for Anthology Student. The drop-down contains a list of databases configured in the Database settings screen.

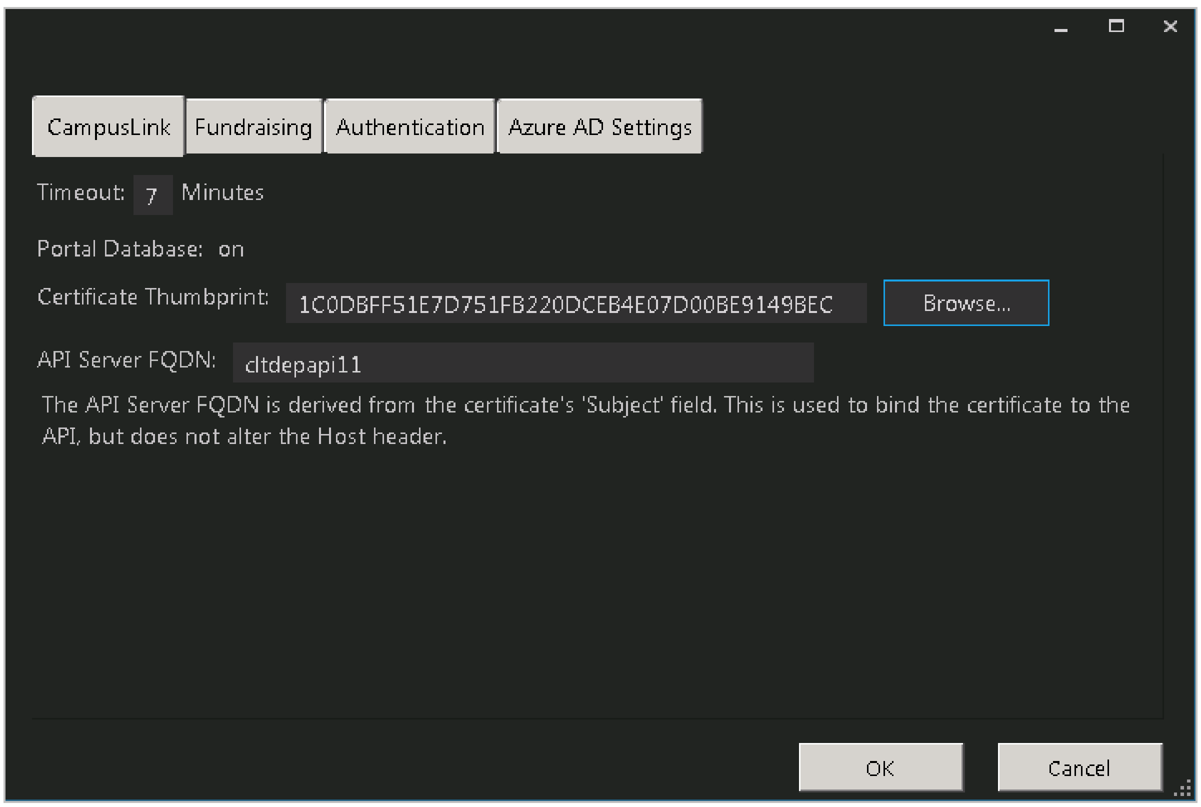
6. In the **Port** field, enter the name of the port where all the Web Services will be installed.

7. Click ... to view and edit the Options form.

   Depending on the licenses, the Options form can have following tabs:

   - **CampusLink Tab**

     This tab contains a timeout value, the Portal database name, the certificate thumbprint, and the API Server FQDN.

     - You can adjust the **Timeout** value.
     - Based on the Portal license, the **Portal Database** associated with the Anthology Student database is populated with a read-only values from the Database Options.
     - The **Certificate Thumbprint** is required for HTTPS connections.

To extract a .CER file from IIS:

a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**.

b. **Double-click** to open the certificate properties.

c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button.

d. Click **Next**. Select **No, do not export the private key**, and click **Next**.

e. Select **DER encoded binary X.509 (.CER)** and click **Next**.

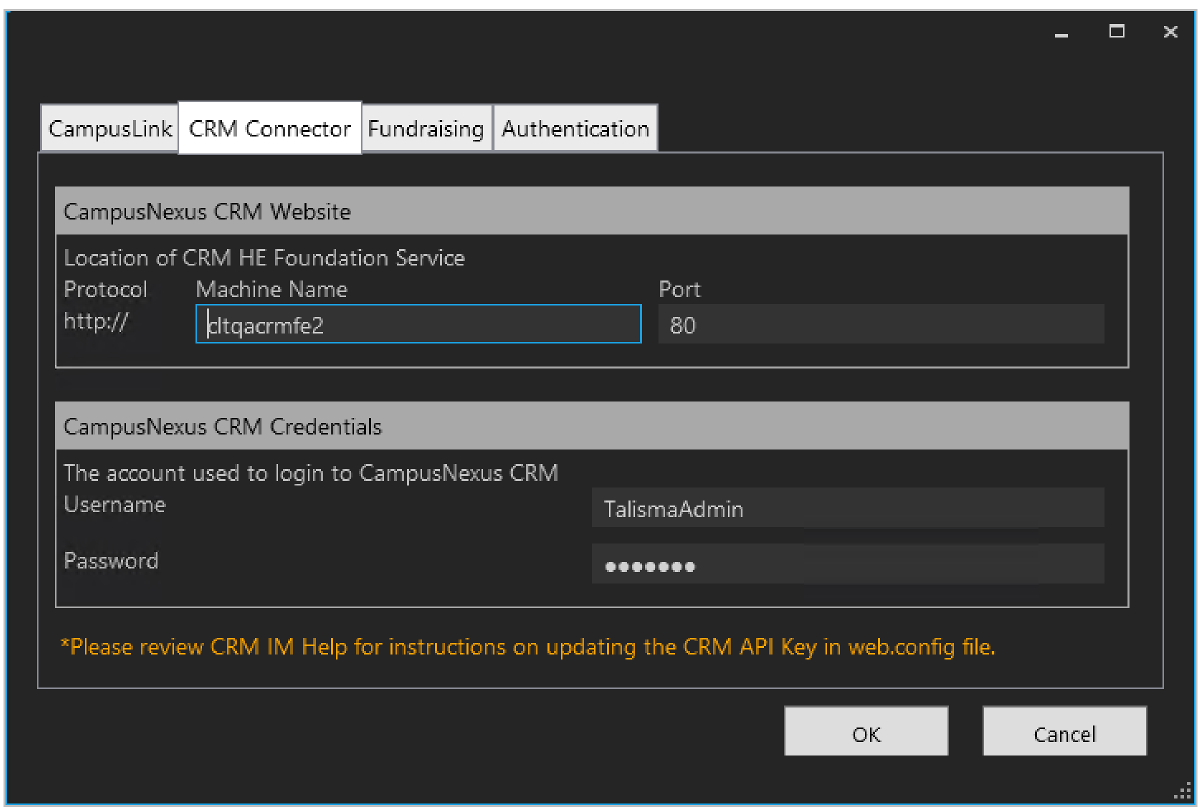
f. Specify a file path and name (root) to export to and click **Next**.

g. Click **Finish**

◦ The API Server Fully Qualified Domain Name (FQDN) is derived from the certificate's 'Subject' field. It is used to bind the certificate to the API, but does not alter the Host header.

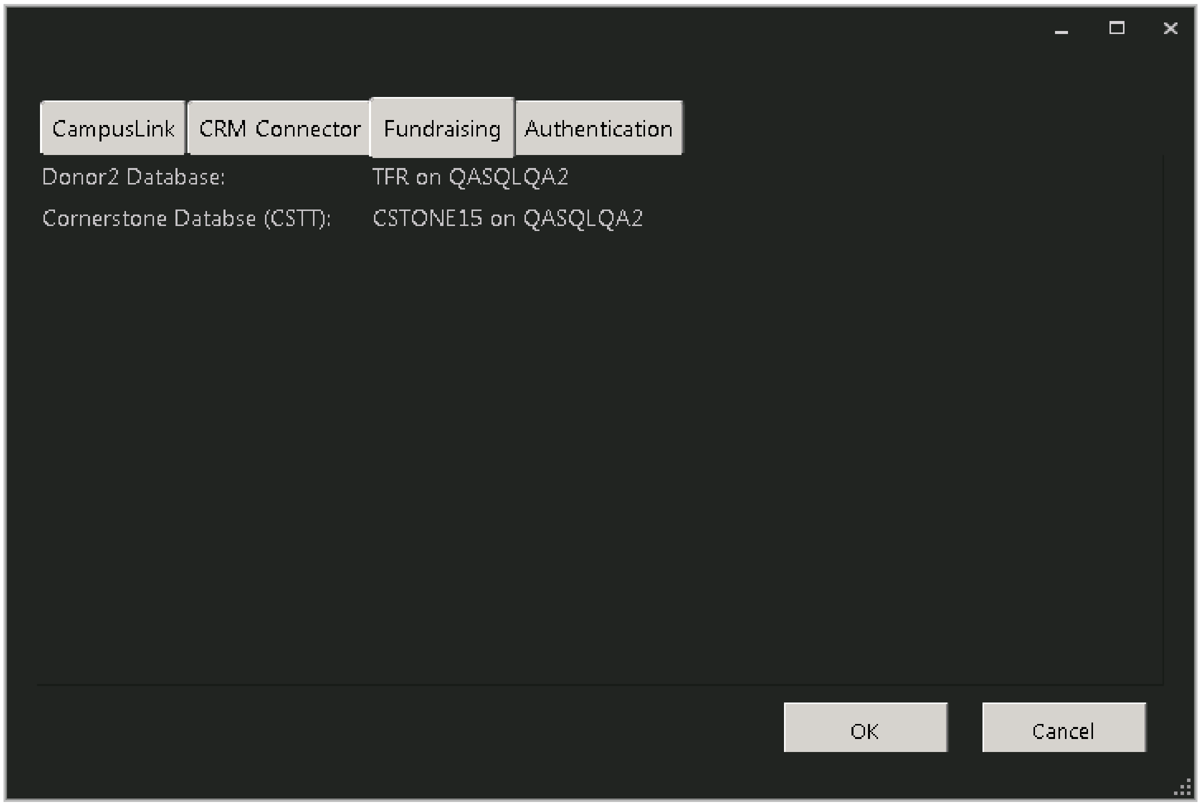
- **CRM Connector Tab**

  This tab is enabled only if the database is licensed with CampusNexus CRM. On this tab, specify the machine name and port for the CampusNexus CRM Higher Education (HE) Foundation Service and the TalismaAdmin credentials used to log in to CampusNexus CRM.



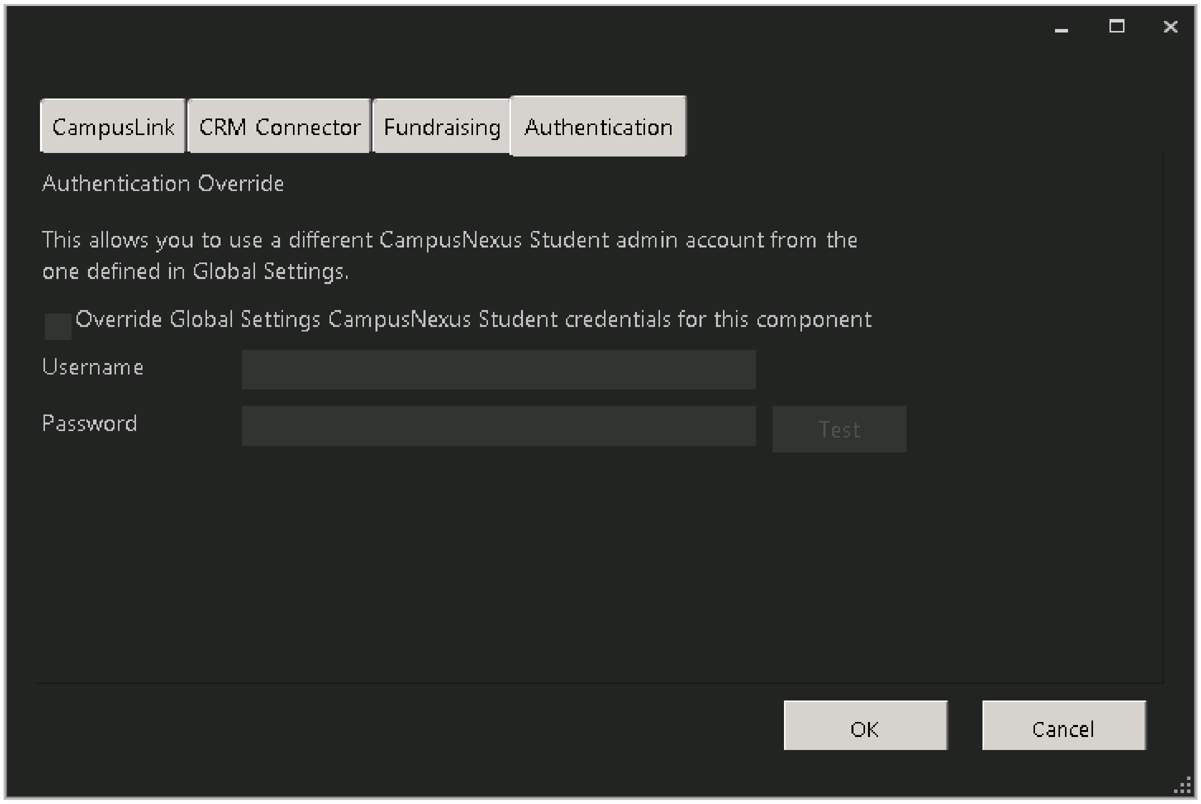
- **Fundraising Tab**

  Based on the Talisma Fundraising license, the Donor2 and Cornerstone database names associated with Anthology Student database are populated with read-only values from the Database Options.

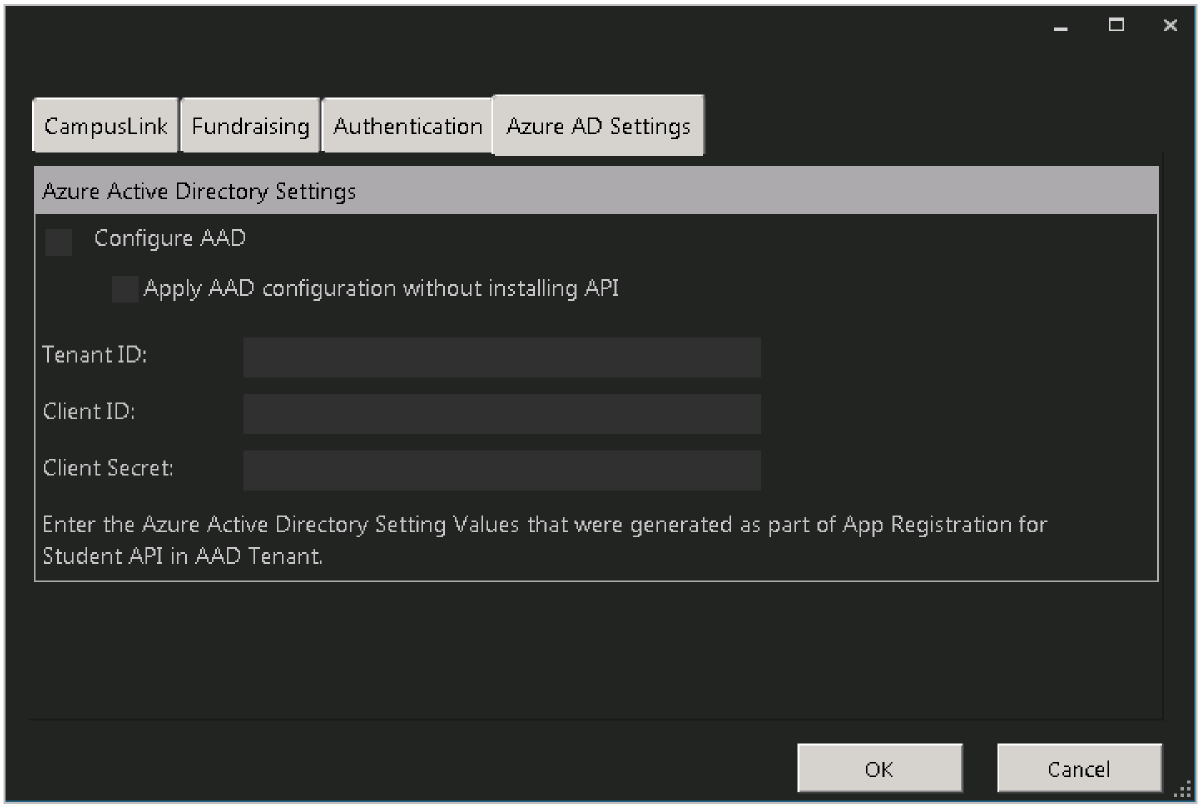
- **Authentication Tab**

  The Authentication tab allows you to specify an Anthology Student administrator account that is different from the account defined in the Global Settings.



- **Azure AD Settings Tab**

  In the Azure AD Settings tab, enter the values that were generated as part of the web application registration for the Student API in the AAD Tenant.



Azure AD Settings Tab Fields

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>Configure AAD</td><td colspan="2">Select this check box if Azure Active Directory (AAD) is used to log in to Anthology Student.</td></tr>
<tr><td>Apply AAD configuration without installing API</td><td colspan="2">Select this check box if AAD is used without installing the Student API.</td></tr>
<tr><td>Tenant ID</td><td>Specify the Azure tenant identifier.</td><td rowspan="3">Customers create app registrations in their Azure AD tenant and provide the Tenant ID, Client ID, and Client Secret that are generated as part of creating the app registration.

Note: One app registration is created for Anthology Student legacy interface and standard interface.</td></tr>
<tr><td>Client ID</td><td>Specify the Azure client identifier.</td></tr>
<tr><td>Client Secret</td><td>Specify the Azure client secret.</td></tr>
</table>

8. Click **OK** to save changes on the Options form. The form is closed.

9. Click to copy a line. Edit the copied line as needed.

10. Click to delete a selected line.

11. If multiple API servers are installed in a server farm (one-to-many NAT), enter the farm's virtual IP address or DNS name in the **Machine Name** field and specify the **Port** number. Installation Manager will display the resulting API Farm URL.

12. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Notes:

    - The Test button checks if the port number is in use; if so, the user is prompted to enter a different port number.
    - If an upgrade is performed, Installation Manager first checks if the port number is in use by the same Web Service that's being installed.

13. If all tests pass, click .

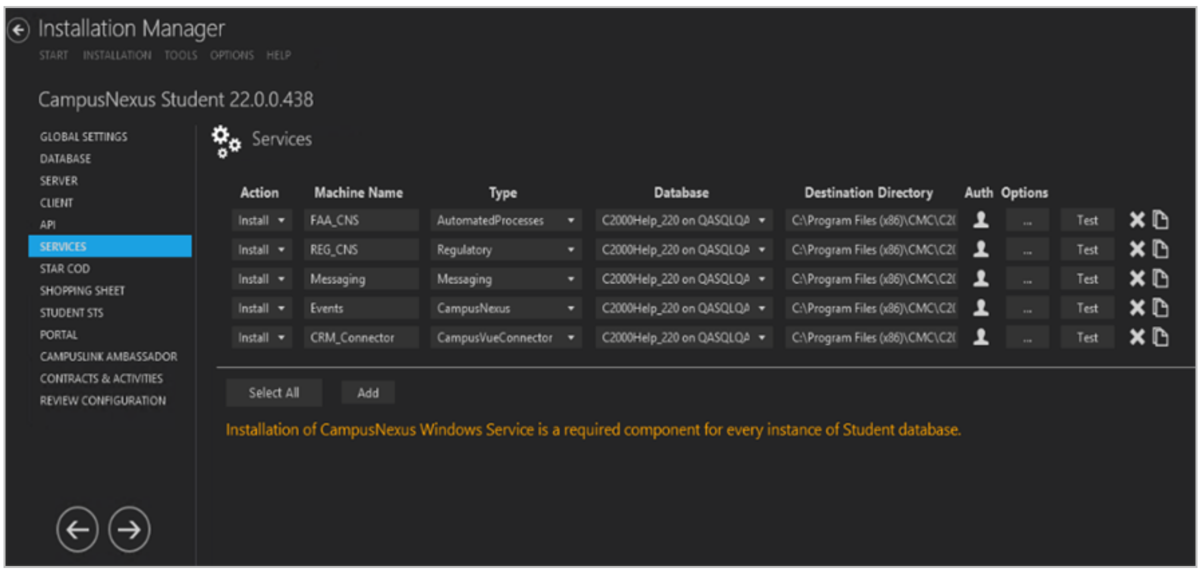
Services

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, type, database, and options for Windows Services that are supported by Anthology Student. The Services are optional modules that enhance the functions of Anthology Student.

> ⚠ Installation of CampusNexus Windows Service is a required component for every instance of the Anthology Student database.

Set Up the Services

1. In the Installation menu, click **Services**. The Services screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select an option from the **Type** list:

- Automated Processes
- CampusLink Ambassador
- CampusVue Connector
- Messaging
- Regulatory
- CampusNexus

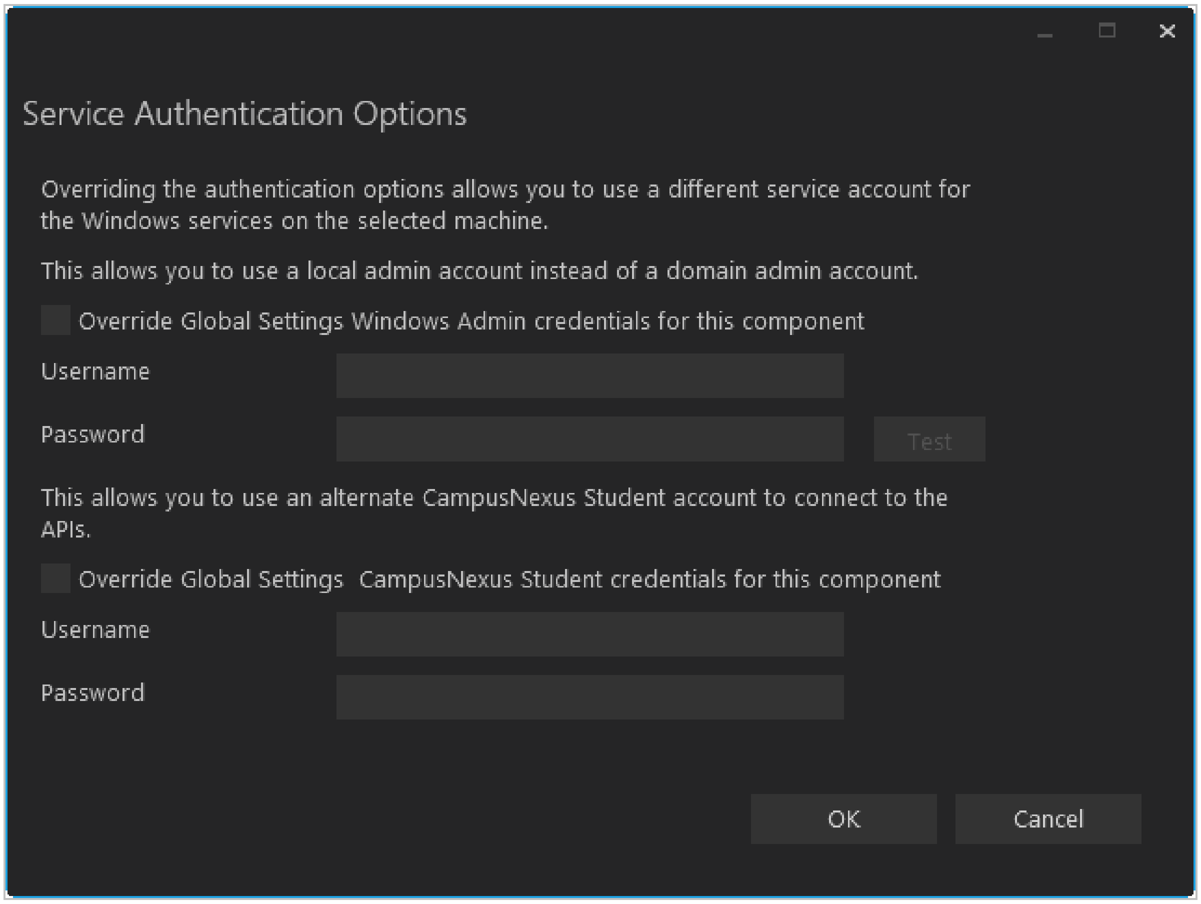
Notes:

- The same service may be installed to multiple machines by adding a line for each machine for one database and selecting the service type.
- Different services may be installed to the same machine by entering a line for each service and using the same machine name.
- Use the **Add** or **Copy** button to define additional machines.

> Automated Processes (FAA) services can be installed only on one server. Installing these services on multiple servers will result in unpredictable results.

Regulatory services and Automated Processes services can be installed on Database Authentication, Active Directory, and Single Sign-on authenticated environments.

6. Select the name of a **Database** for Anthology Student. The drop-down list contains all Anthology Student databases configured in the Database settings screen.
7. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
8. Click in the **Auth** column if you want to override the authentication options from Global Settings to use a different account for the Windows services and alternate Anthology Student credentials on the selected machine. The Service Authentication Options form is displayed.



a. Select the check box **Override Global Settings Windows Admin credentials for this component** to enable the associated fields on the form. This option allows you to use a local admin account instead of the domain admin account.

b. Enter the **Username** and **Password** of the local admin account for the selected machine.

c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

d. Select the check box **Override Global Settings Anthology Student credentials for this component**.

e. Enter the **Username** and **Password** of Anthology Student account for the selected machine.

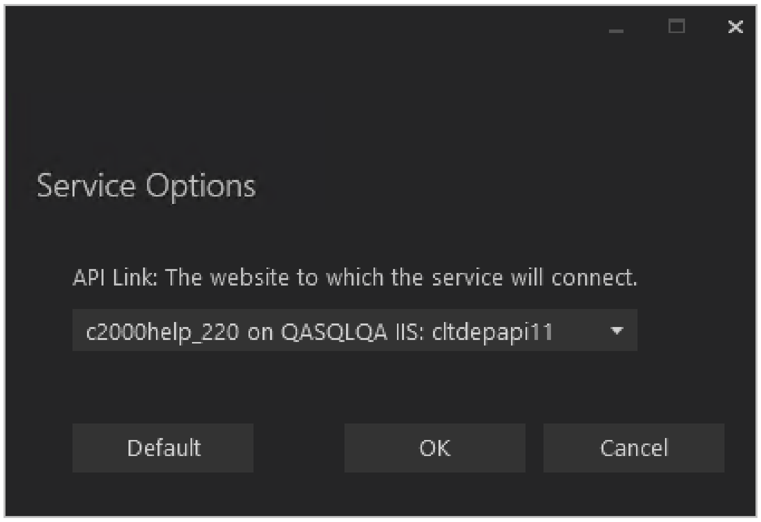
f. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

g. Click **OK** to save changes on the Options form. The form is closed.

9. Click  to view and edit the Options form.

- The Messaging Options window is displayed when the selected Service Type is Messaging.
- The Service Options window is displayed for all other Services.

Service Options



In the Service Options window, select the database and installed system to be used by the Web Service (API).

— OR —

Click **Default** to use the API server based on the database selected.

Notes about the Service Options:

- Automated Processes

  Select the API database and installed system for configuring the Automated Processes components.

- CampusVue Connector

  Select the API database and installed system for configuring the CampusVue Connector components.

- Regulatory

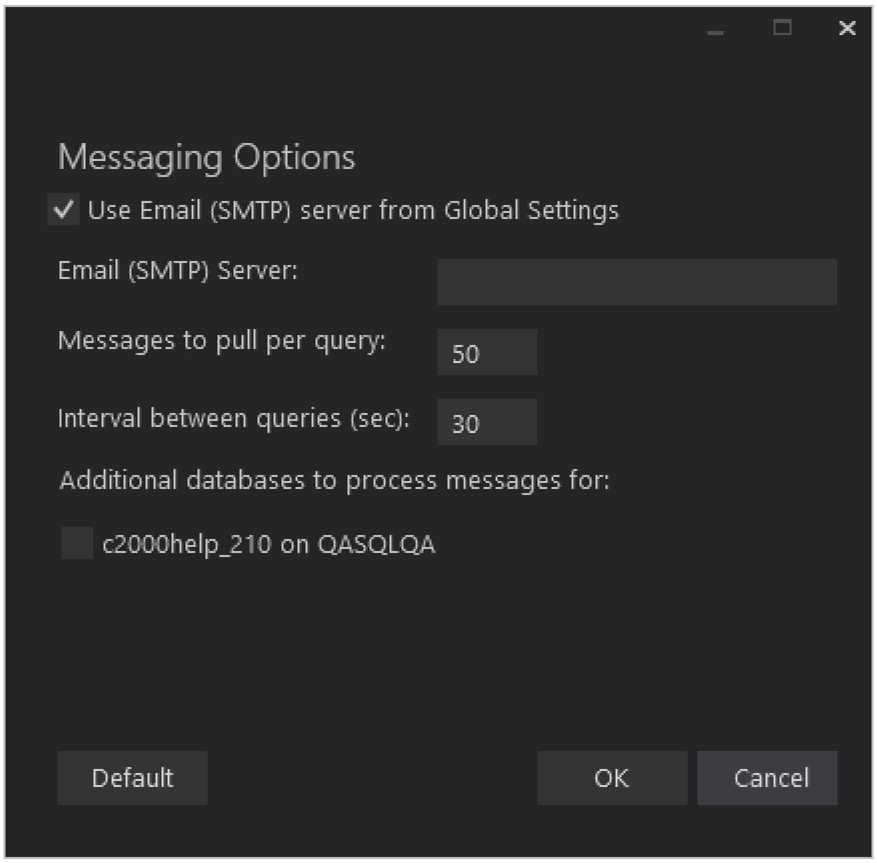
  Select the API database and installed system for configuring Regulatory service components. The Regulatory service needs to be installed for all Anthology Student installations. The service can be installed on any tier (Front End, COM Server, or API) that has access to the API servers. Although many instances of the service can be installed for the enterprise, only one instance of the service can point to one database. This comes in handy when a customer chooses to use one computer to host Regulatory services for multiple environments (QA, UAT, etc.).

- CampusNexus

Select the API database and installed system for configuring components. The service can be installed on any tier (Front End, COM Server, or API) that has access to the API servers. Although many instances of the service can be installed for the enterprise, only one instance of the service can point to one database.

The identity specified to run the service must have **db_owner** permission to the specified Anthology Student database prior to installation. The service account requires access to the Anthology Student database to handle events and activities. Without this access, the service will fail to connect and exceptions will be logged in the log folder (...\C2000\Services\Nexus Event Notification Service <version>\logs\).

Messaging Options



In the Messaging Options window, enter appropriate data as defined in the table below.

— OR —

Click **Default** to use the default settings.

Messaging Options Fields

Field	Description
Use Email (SMTP) server from Global Settings	Select this check box if you want to use the Email (SMTP) server configured on the Global Settings screen. Clear the check box to use a different email server for the Messaging Service.
Email (SMTP) Server	By default Installation Manager uses the Email server from the on the Global Settings screen.
Messages to pull per query	Enter the number of message to pull per query. The default is 50. **Note**: To avoid performance impacts, do not specify more than 500 messages to pull per query.
Interval between queries (sec)	Enter the number of seconds between query intervals to get the next batch of messages to process. The default is 50. **Note**: To avoid performance impacts, do not specify a query interval below 30 seconds.
Additional databases to processes messages for	If you want to provide messaging service to additional databases, select the check box next to the name of the database.

10. Click **OK** to save changes on the Options form. The form is closed.
11. Click to copy a line. Edit the copied line as needed.
12. Click to delete a selected line.
13. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
14. If all tests pass, click .

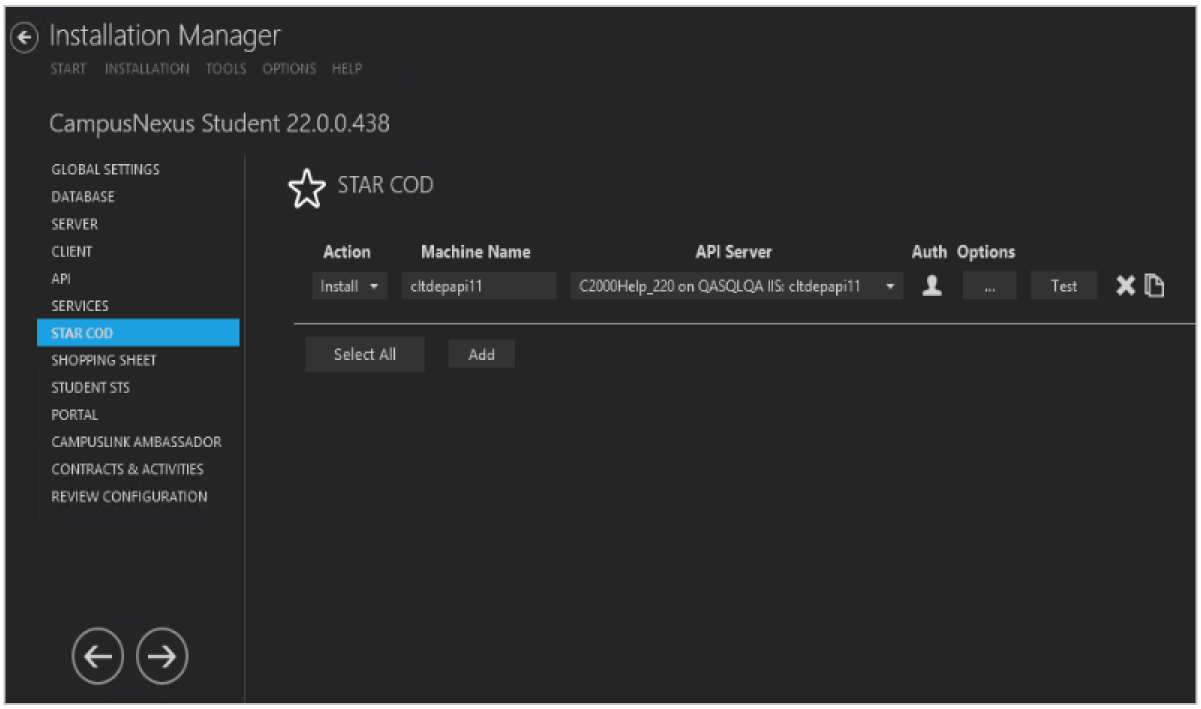
STAR COD

The STAR COD screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and options for transmission and retrieval of STAR COD files to and from Anthology Student.

STAR COD is typically installed on the machine where EDconnect is installed. Keep in mind that EDconnect currently does not support Windows Server 2012.

Set Up STAR COD

1. In the Installation menu, click **STAR COD**. The STAR COD screen for Anthology Student is displayed.



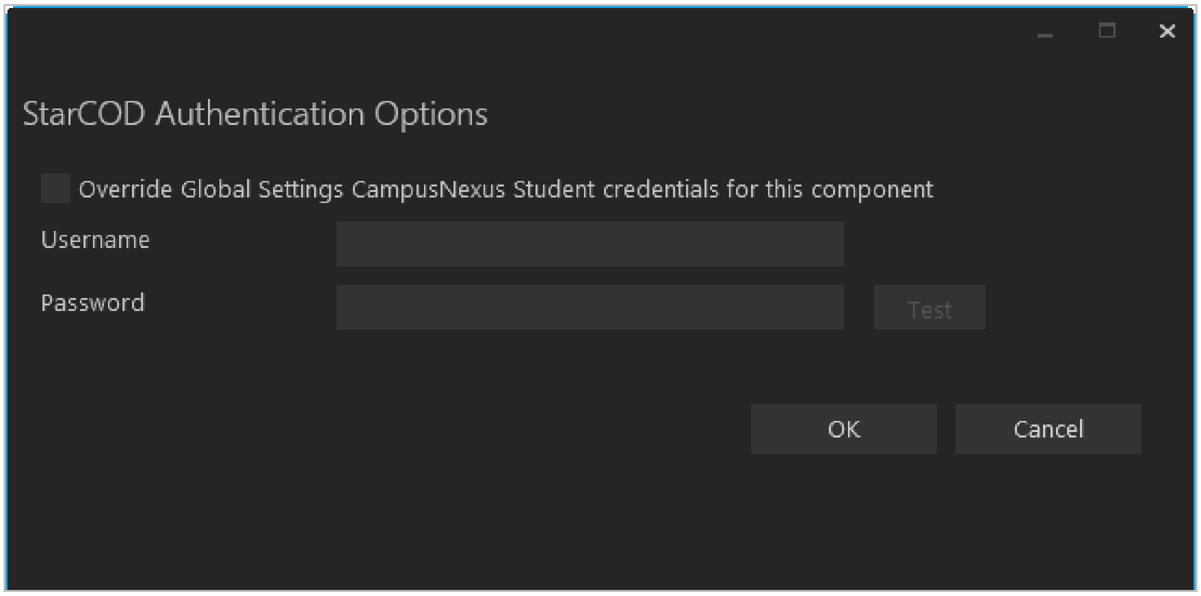
2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

    - **None** – Performs no action.
    - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
    - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

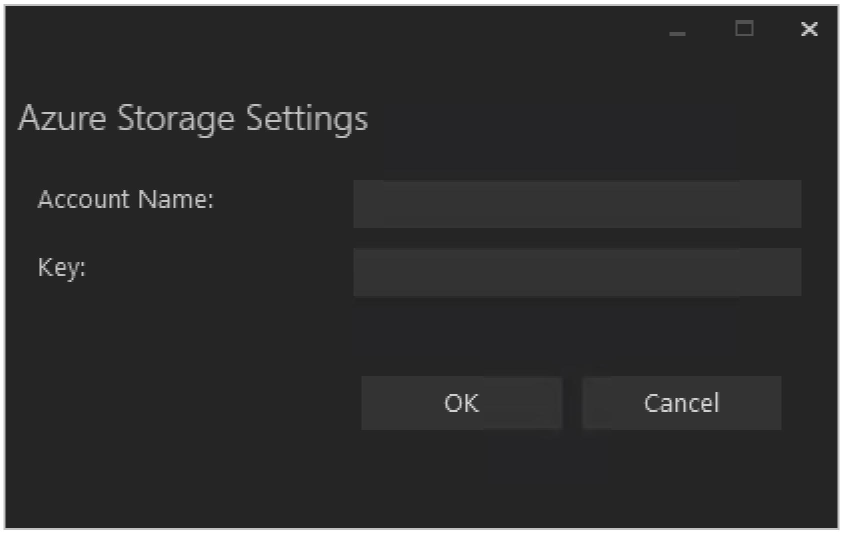
4. Enter the **Machine Name** for the component to be installed.
5. Select the **API Server**. The drop-down list contains all the API Servers for the Anthology Student databases configured in the API settings screen.
6. Click in the **Auth** column if you want to override the authentication options from Global Settings to use alternate Anthology Student credentials on the selected machine. The StarCOD Authentication Options form is displayed.



    a. Select the check box **Override Global Settings Anthology Student credentials for this component** to enable the fields on the form.
    b. Enter the **Username** and **Password** of the Anthology Student account for the selected machine.
    c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
    d. Click **OK** to save changes on the Options form. The form is closed.

7. Click to view and edit the Options form.

In the **Azure Storage Settings** window, specify the **Account Name** and **Key**.



8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Shopping Sheet

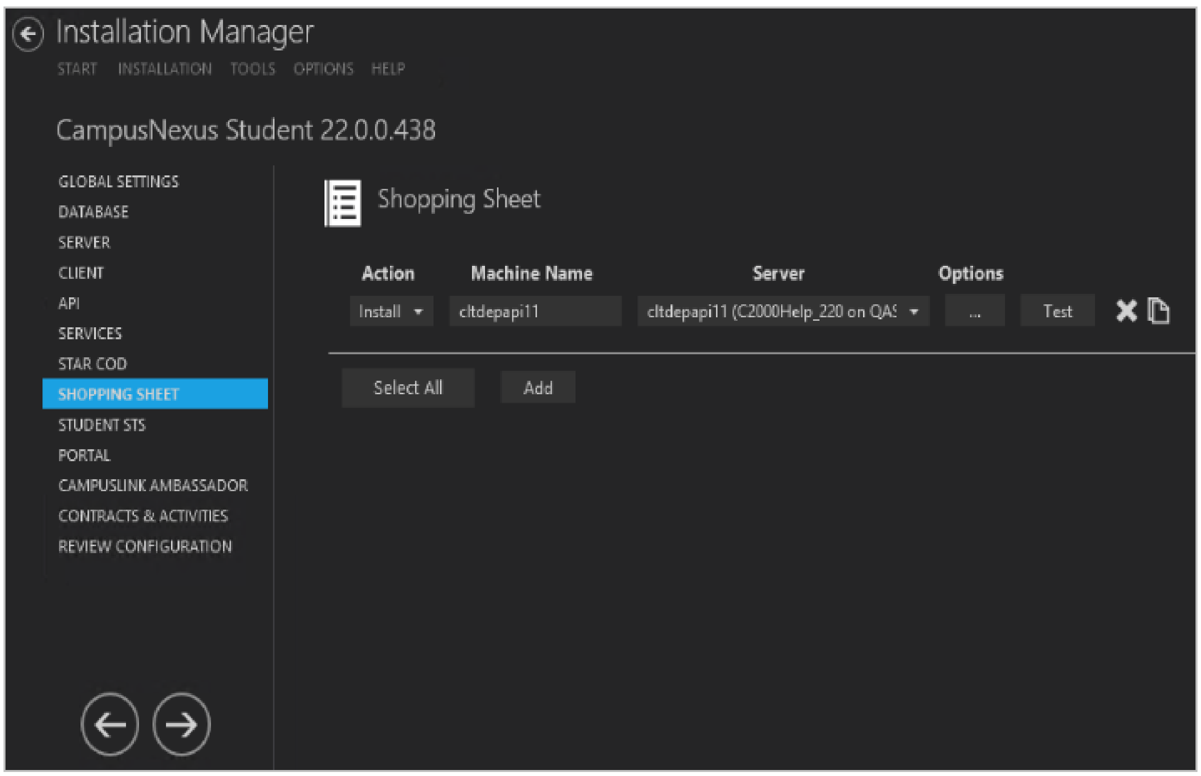
The Shopping Sheet screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and options of the financial aid Shopping Sheet for Anthology Student.

⚠ Shopping Sheet is typically installed on the Portal server.

In award year 2020-2021 and later, the Shopping Sheet is also referred to as the College Finance Plan.

Set Up the Shopping Sheet

1. In the Installation menu, click **Shopping Sheet**. The Shopping Sheet screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.

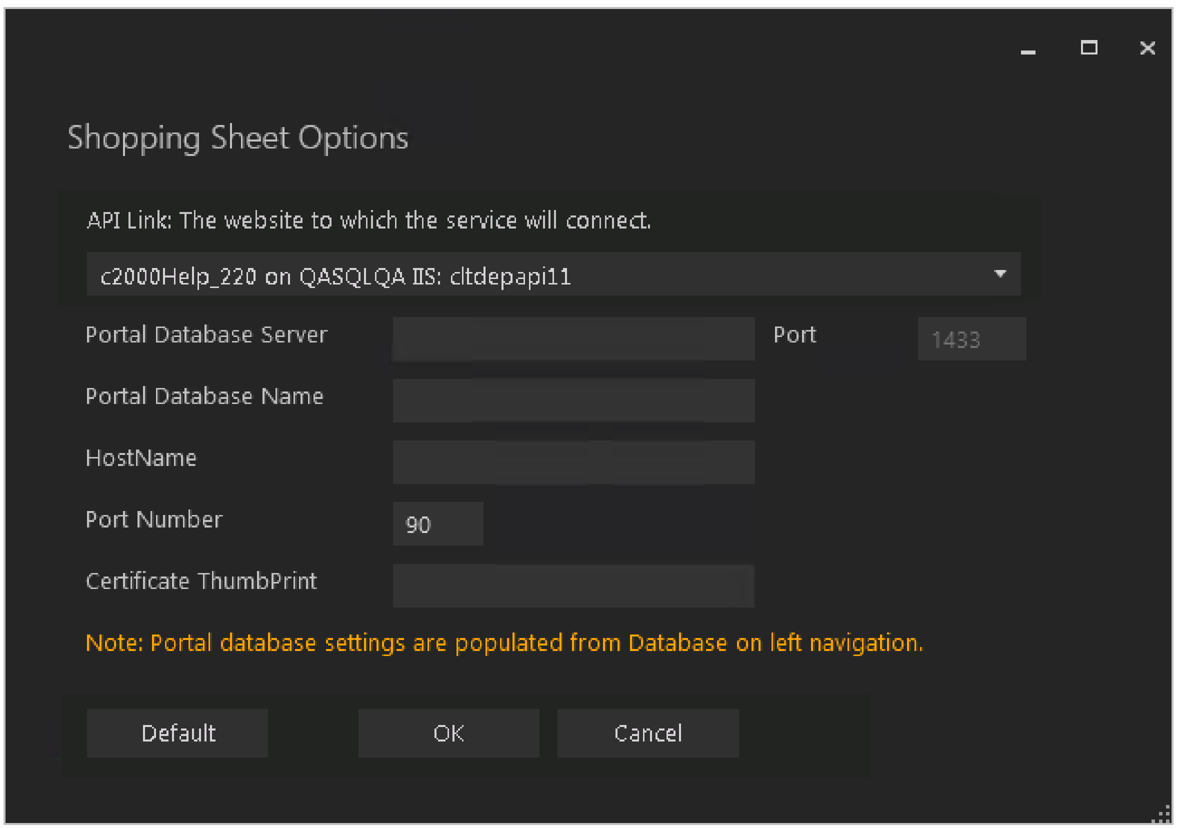
3. Select an appropriate **Action**. The following Action values are available:

- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

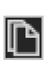
4. Enter the **Machine Name** for the component to be installed.
5. Select the name of a **Server**. The drop-down list contains the servers and Anthology Student databases configured in the Database settings screen.

   Note: Multiple clients can be installed against one server.
6. Click to view and edit the Options form.



Shopping Sheet Options Fields

Field	Description
API Link	Select the database and installed system to be used by the Shopping Sheet component. – OR – Click **Default** to use the API server based on the database selected.
Portal Database Server	Specify the name of the SQL server on which the Portal database resides.
Port	Specify the port number for the Portal or accept the default (1433).
Portal Database Name	Specify the name of the Portal database.
Hostname	Specify the hostname for the Portal URL. It will be added to the IIS bindings of main Portal instance.
Port Number	Specify the port number used by the Portal or accept the default (00).
Certificate Thumbprint	The certificate thumbprint from IIS is required for HTTPS connections. Copy and paste the thumbprint from Portal into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

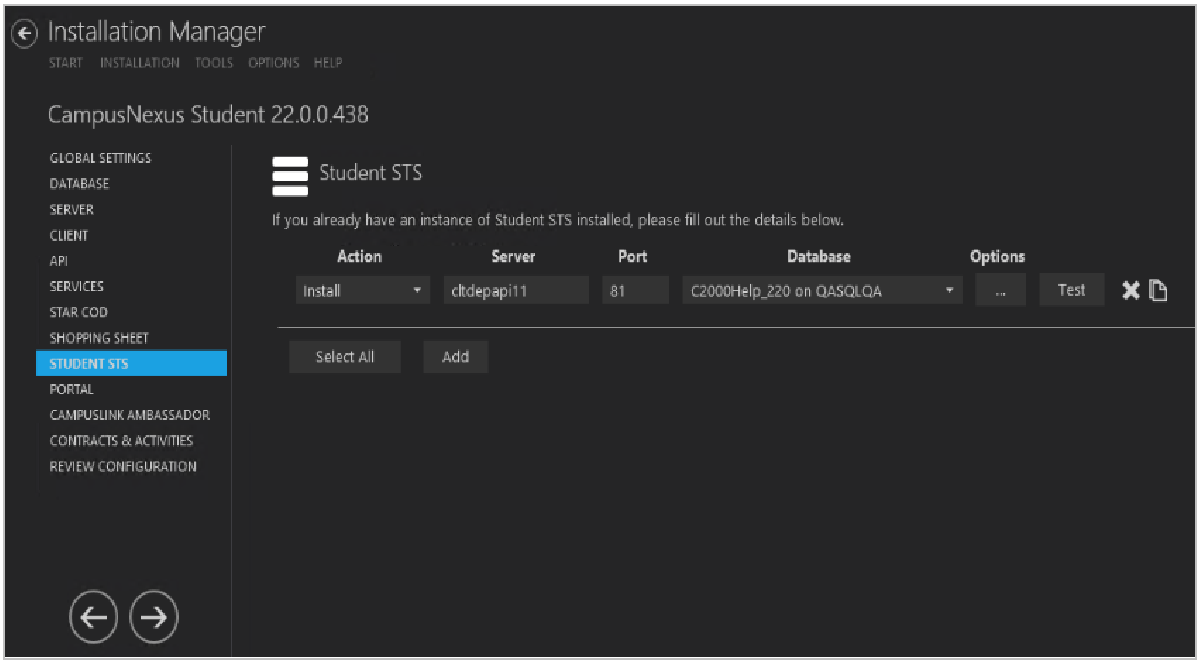
7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Student STS

The Student STS screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database server, and port to be used by the Student Security Token Service (STS). The Student STS provides authentication for applicants, students, and employers logging into Portal. The Student STS is also used by Forms Builder Renderer to allow students to access the Portal via forms created in Forms Builder.

Set Up the Student STS

1. In the Installation menu, click **Student STS**. The Settings screen for Student STS is displayed.

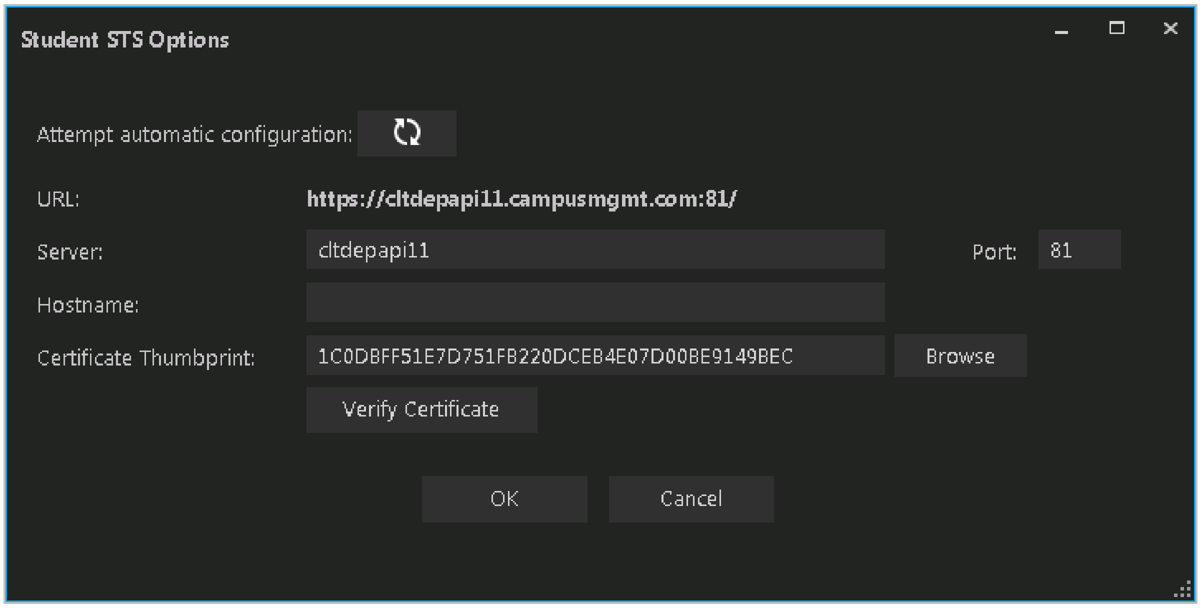


2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. In the **Server** field, enter the name of the machine that hosts the Student STS.
5. In the **Port** field, enter the port number or accept the default (81).

6. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.

7. Click ⋯ to view and edit the Options form.



Student STS Options Fields

Field	Description
Update Settings	Click to attempt an automatic configuration of the Student STS. You must be in the same domain as the Student STS and must have the SQL server permissions for automatic configuration to be successful.
URL	URL name of the Student STS For example: `http://stdsts.campusmgmt.com`
Server	Name of the STS server used to authenticate applicants, student, and employers.
Port	Specify the port number or accept the default (81).
Hostname	This is an optional field. When selected, the web.config file of the Student STS will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port`

Field	Description
Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected. It is not added to the web.config file. This certificate is used only for the Student STS, which provides authentication for Renderer (and Portal) to applicants, students, and employers. Click **Verify Certificate** to make sure the certificate is valid. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

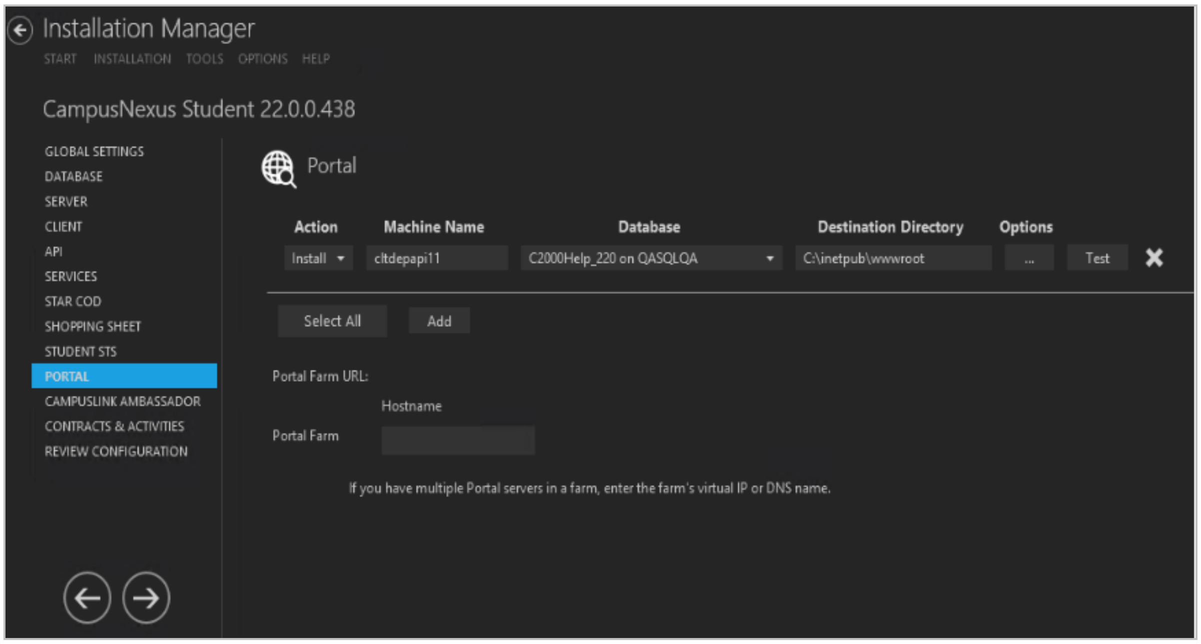
Portal

The Portal screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and options of the web Portal for Anthology Student.

Refer to the Portal Administrator Reference for procedures related to authentication, customization, and branding of Portal version 18.2.0 and later.

Set Up the Portal

1. In the Installation menu, click **Portal**. The Portal screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

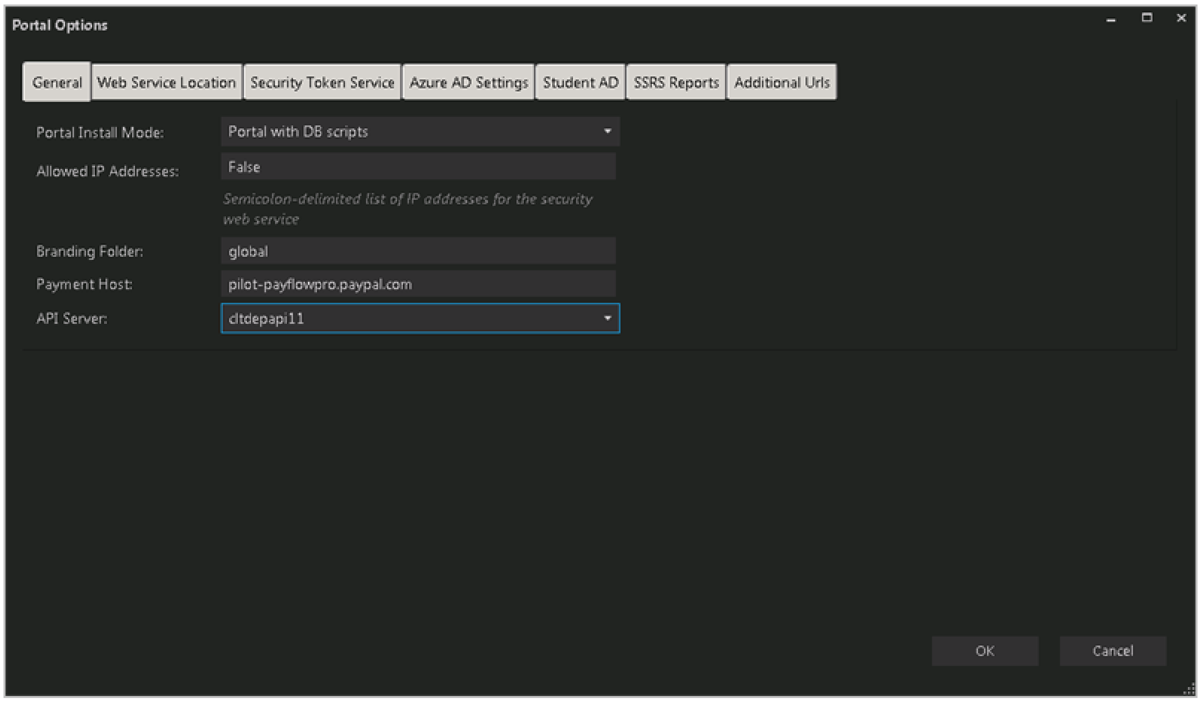
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.

5. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.
6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
7. Click to view and edit the Options form. The form contains the following tabs:

   General Tab

   Use this tab to specify the installation mode, hostname and IP addresses, branding folder, host header, payment host, and API server.



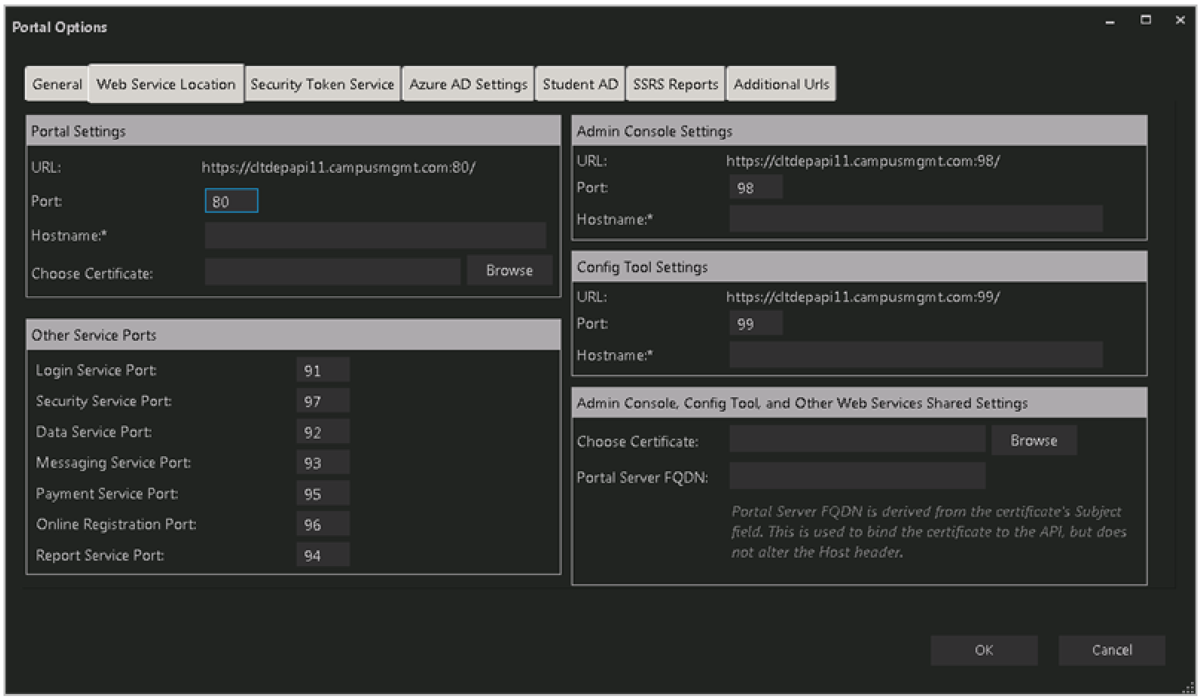
General Tab Fields

Field	Description
Portal Install Mode	Select the Portal Install Mode. The options are: • Portal with DB scripts — This option installs Portal and runs the DB scripts at the same time (default). • Portal without DB scripts — This option installs the Portal websites without running DB scripts. • Portal DB scripts only — This option runs the DB scripts for Portal without installing or reinstalling the Portal websites.

Field	Description
Allowed IP Addresses	List of IP addresses from the Anthology Student database including the IP address of Portal server. Enter up to 15 IP addresses separated by semicolons. Any additional IP addresses entered by the user will be inserted into the Anthology Student database.
Branding Folder	Specify the folder for the campus level branding files or accept the default (global).
Payment Host	Specify the URL of the Payment Host.
API Server	Select the API Server from the drop-down list.

Web Service Location Tab

Use this tab to specify the ports, hostnames, and, if applicable, certificates for the Portal web services.



Web Service Location Tab Fields

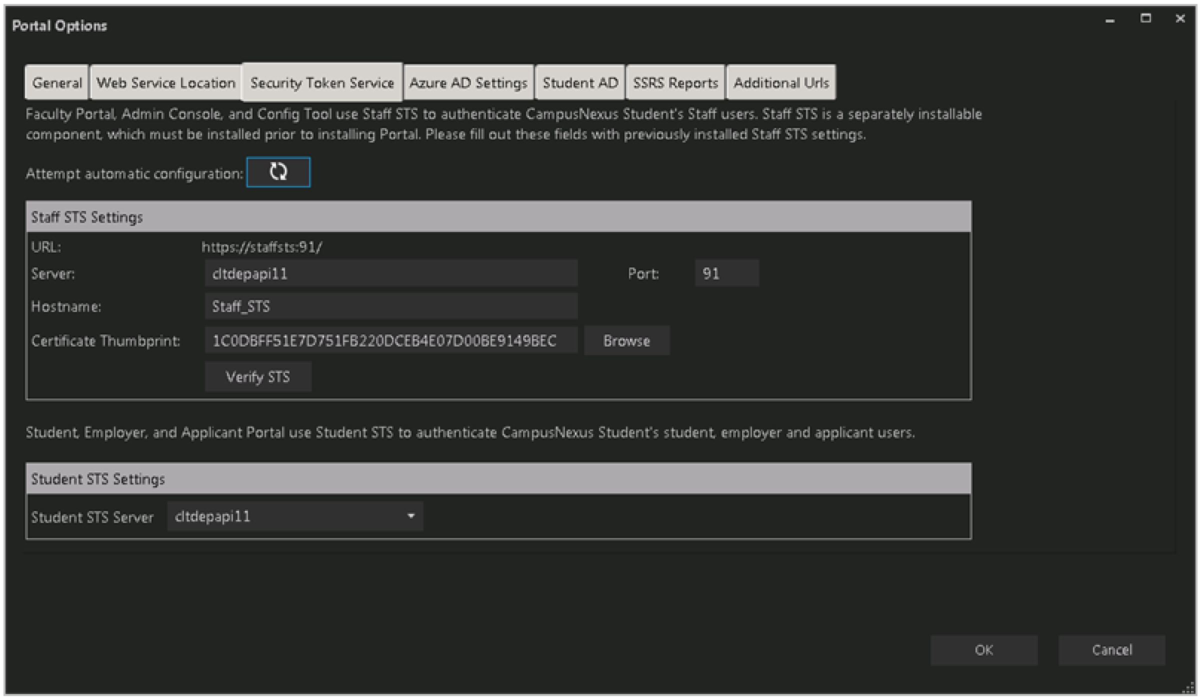
Field	Description
Portal Settings	
URL	URL of the Portal
Port	Specify the port number for the Portal or accept the default (80).
Hostname	This is an optional field. When selected, the web.config file of the Portal will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port`

Field	Description
Use HTTPS	Select this check box if you want Portal to be accessed through HTTPS. When this option is selected, the Choose Certificate field is enabled.
Choose Certificate	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected and is not added to the web.config file. This certificate is used only for Portal. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Other Service Ports	
Login Service Port	Specify the port number of the Login Service or accept the default (91).
Security Service Port	Specify the port number of the Security Service or accept the default (97).
Data Service Port	Specify the port number of the Data Service or accept the default (92).
Messaging Service Port	Specify the port number of the Messaging Service or accept the default (93).
Payment Service Port	Specify the port number of the Payment Service or accept the default (95).
Online Registration Port	Specify the port number of the Online Registration Service or accept the default (96).
Report Service Port	Specify the port number of the Report Service or accept the default (94).
Admin Console Settings	
URL	URL of the Admin Console
Port	Specify the port number for the Admin Console or accept the default (98).

Field	Description
Hostname	This is an optional field. When selected, the web.config file of the Admin Console will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port`
Config Tool Settings	
URL	URL of the Config Tool
Port	Specify the port number for the Config Tool or accept the default (99).
Hostname	This is an optional field. When selected, the web.config file of the Config Tool will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port`
Admin Console & Config Tool Shared Settings	
Choose Certificate	Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Portal Server FQDN	The Portal Server Fully Qualified Domain Name (FQDN) is derived from the certificate's 'Subject' field. It is used to bind the certificate to the API, but does not alter the Host header.

Security Token Service Tab

Use this tab to specify the settings for the Staff STS and Student STS.



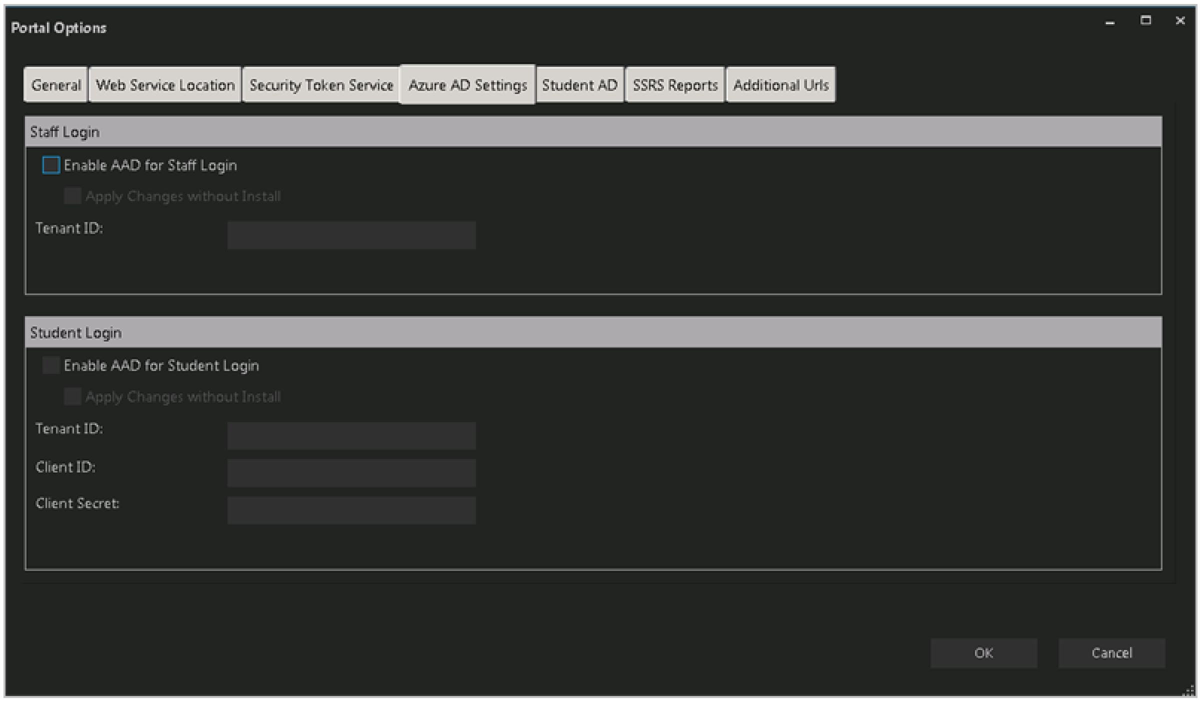
Security Token Service Tab Fields

Field	Description
Update Settings	Click to attempt an automatic configuration of the Security Token Services. You must be in the same domain as the STS and must have the SQL server permissions for automatic configuration to be successful.
Staff STS Settings	
URL	URL of the Staff STS
Server	Specify the name of the Staff STS server.
Port	Specify the port number for the Staff STS or accept the default (91).
Hostname	Hostname of the Staff STS in the format http://<Server-Name>.<certificateName> For example: http://prtl.campusmgmt.com

Field	Description
Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected and is not added to the web.config file. This certificate is used only for Staff STS. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Verify STS	Click **Verify STS** to check that the Staff STS Server is active and that login is successful.
Student STS Settings	
Student STS Server	Select the installed Student STS Server.

Azure AD Settings Tab

Use this tab to specify the Azure Active Directory (AAD) settings for staff and student users logging in to Portal.

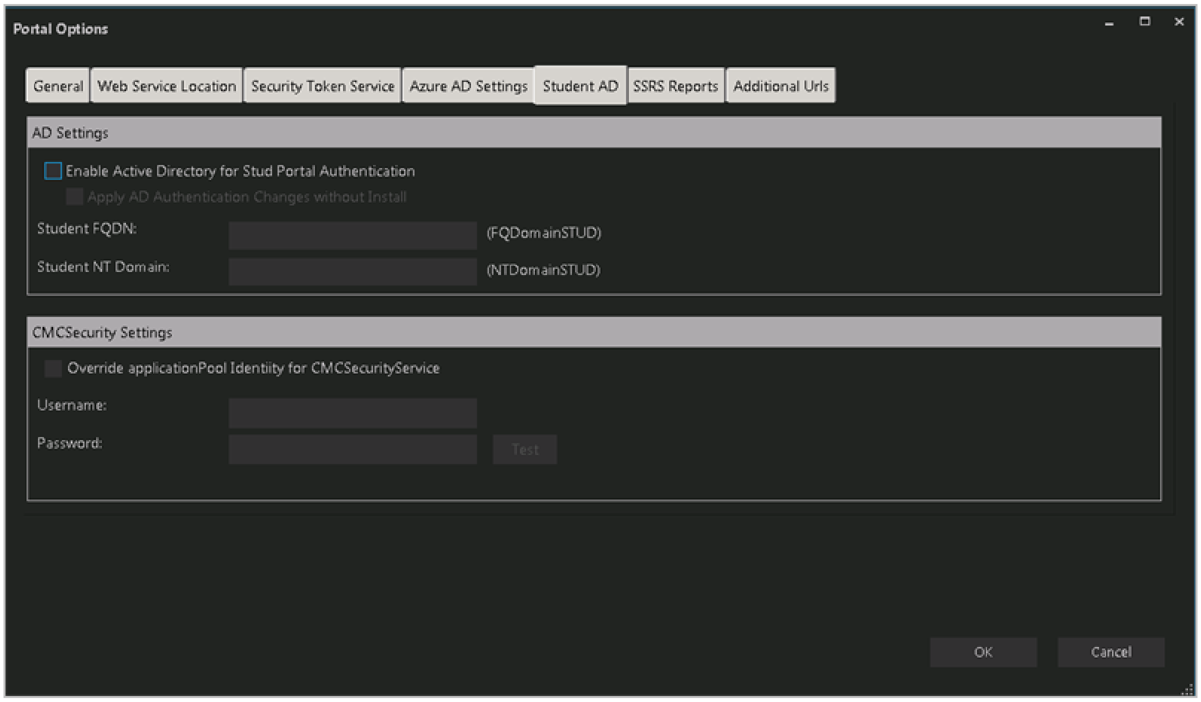


Azure AD Settings Tab Fields

Field	Description
Staff Login	
Enable AAD for Staff Login	Select this check box to enable the Staff Login fields.
Apply Changes without Install	Select this check box if AAD is used without installing Portal.
Tenant ID	Specify the Azure tenant identifier.
Student Login	
Enable AAD for Student Login	Select this check box to enable the Student Login fields.
Apply Changes without Install	Select this check box if AAD is used without installing Portalt.
Tenant ID	Specify the Azure tenant identifier.
Client ID	Specify the Azure client identifier.
Client Secret	Specify the Azure client secret.

Student AD Tab

Use this tab to specify the Active Directory (AD) and Security settings for the Student Portal.



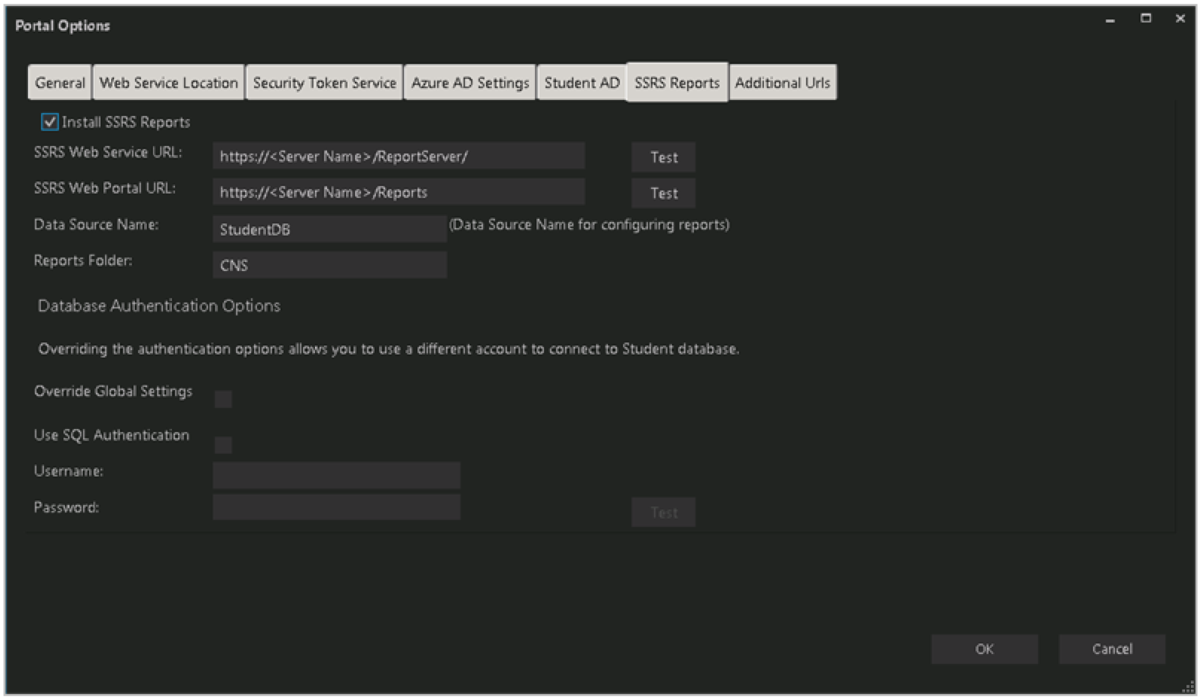
Student AD Tab Fields

Field	Description
AD Settings	
Enable Active Directory for Student Portal Authentication	Select this check box to enable the AD Settings fields.
Apply AD Authentication Changes without Install	Select this check box if AD is used without installing Portal
Student FQDN	Specify the fully qualified domain name (FQDN) for Student Portal.
Student NT Domain	Specify the Windows NT Domain for Student Portal.
CMC Security Settings	
Override Application Pool Identity for CMC Security Service	Select this check box to enable the CMC Security Settings fields.
Username	Specify the user name for the application pool identity override.
Password	Specify the password for the application pool identity override.

SSRS Reports Tab

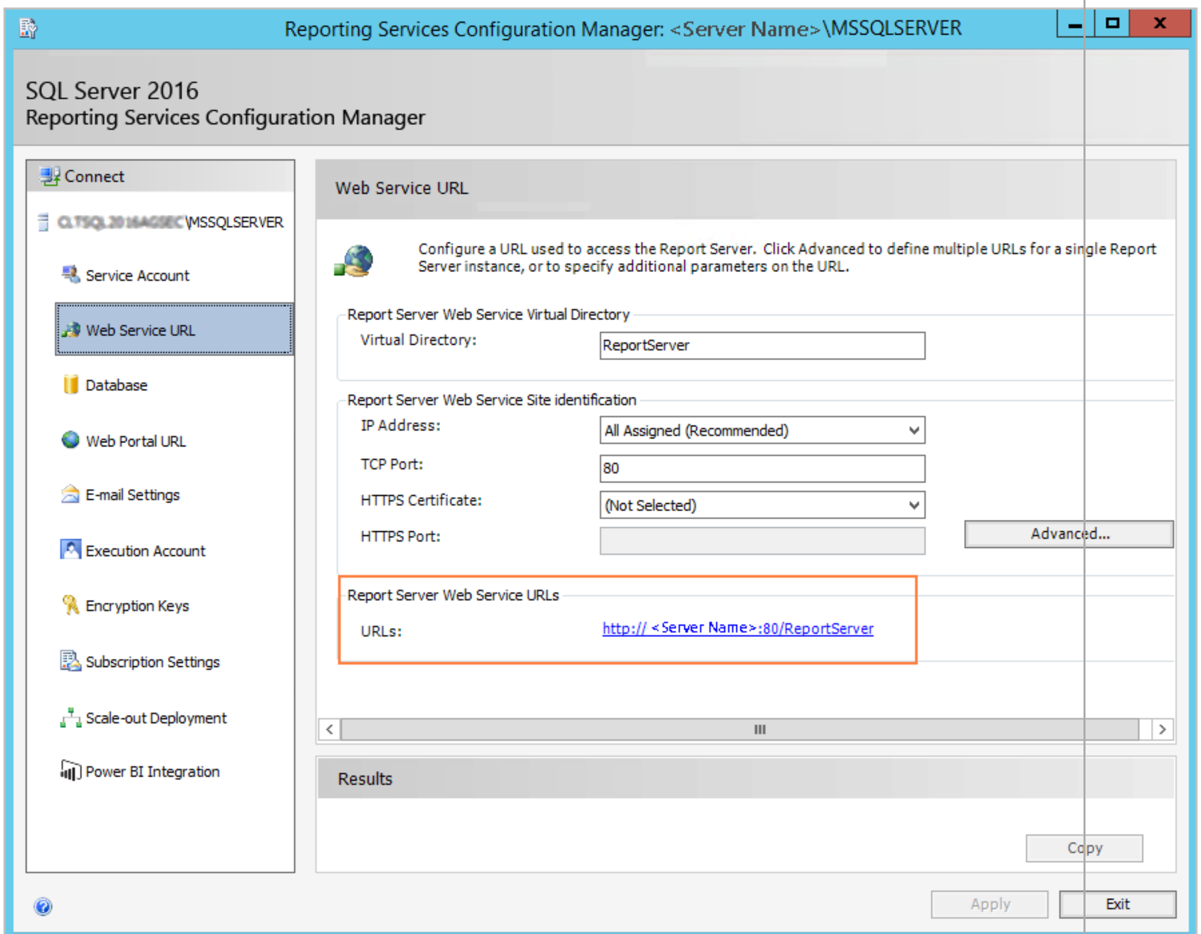
Use this tab to integrate SQL Server Reporting Services (SSRS) 2016, the server-based report generating software system, into the Portal. Settings on this tab are required if Portal uses SSRS reports (instead of Crystal reports).

Examples of SSRS reports are unofficial transcripts (rpt_adTranscriptUnofficial.rpt and rpt_adTranscript_StudentBased.rpt). The unofficial transcripts can be accessed in Portal by students and staff.



SSRS Reports Tab Fields

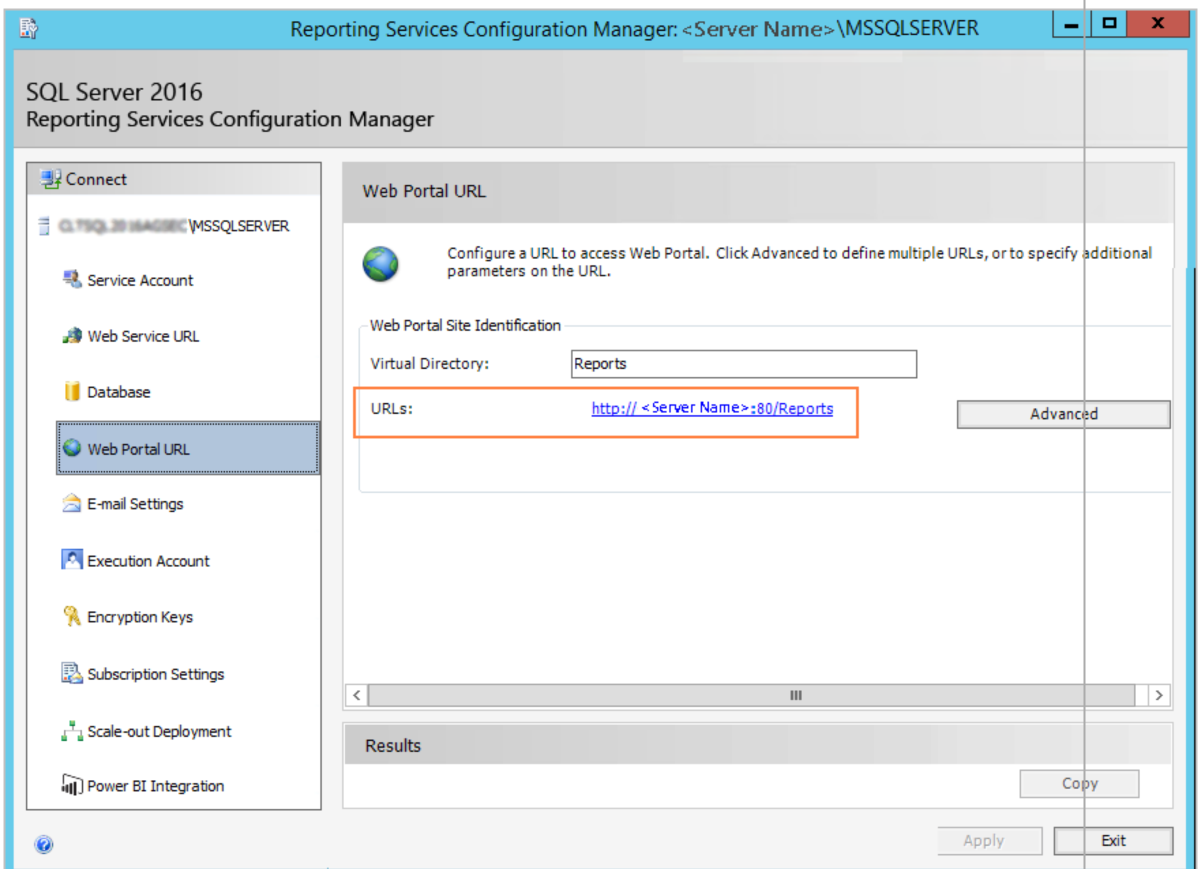
Field	Description
Install SSRS Reports	Select this check box to enable the fields on this tab.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Service URL</td><td>
Specify the Web Service URL configured to access the Report Server. The specified URL will be stored in the web.config file.
This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager.


</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Portal URL</td><td>
Specify the Web Portal URL configured to access the Web Portal. The specified URL will be stored in the web.config file.

This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager page.



</td></tr>
<tr><td>Data Source Name</td><td>Specify the name of the Anthology Student database that is the source for the reports.</td></tr>
<tr><td>Reports Folder</td><td>
Specify the path for the reports folder on the Report Server. A folder will be created if one does not exist. The folder name can be unique to the environment. The reports folder root path will be stored in the web.config file.

Example

`QA/CNS` where `QA` is one folder and `Student_Test` is a folder under `QA`.
</td></tr>
<tr><td colspan="2">Database Authentication Options</td></tr>
<tr><td>Override Global Settings</td><td>Optional: Select this check box to enable the database authentication options.</td></tr>
</table>

Field	Description
Use SQL Authentication	Optional: Select this check box if SQL authentication is applied.
Username	Enter the user name of the account that is given override permissions for the SSRS reports database.
Password	Enter the password of the account that is given override permissions for the SSRS reports database.
Test	Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

In addition to the settings on the SSRS Reports tab in Installation Manager, the setup of reporting services requires configurations in the SQL Server Reporting Services Configuration Manager (see Configure Access to Reports).

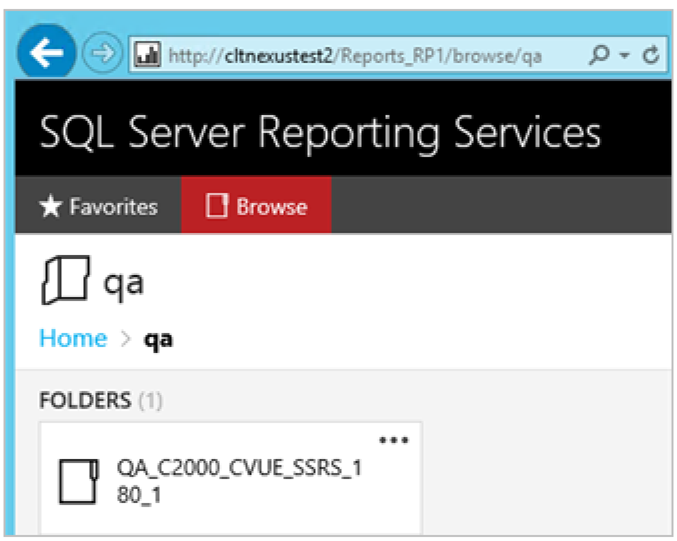
You also need to create folders in the Anthology Student and assign permissions using the Security Console. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Configure Access to Reports

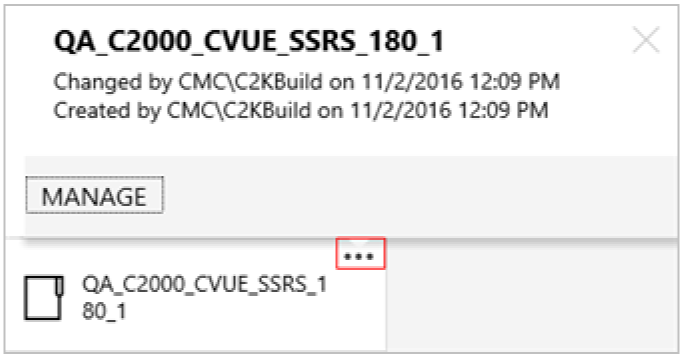
To enable access to the "Reports" menu item in Anthology Student, perform the following steps in the Reporting Services Configuration Manager on the report server:

a. Navigate to the /Reports folder path.

   In the example below the reports folder path is `http://cltnexustest2/Reports_RP1/browse/`**qa**.

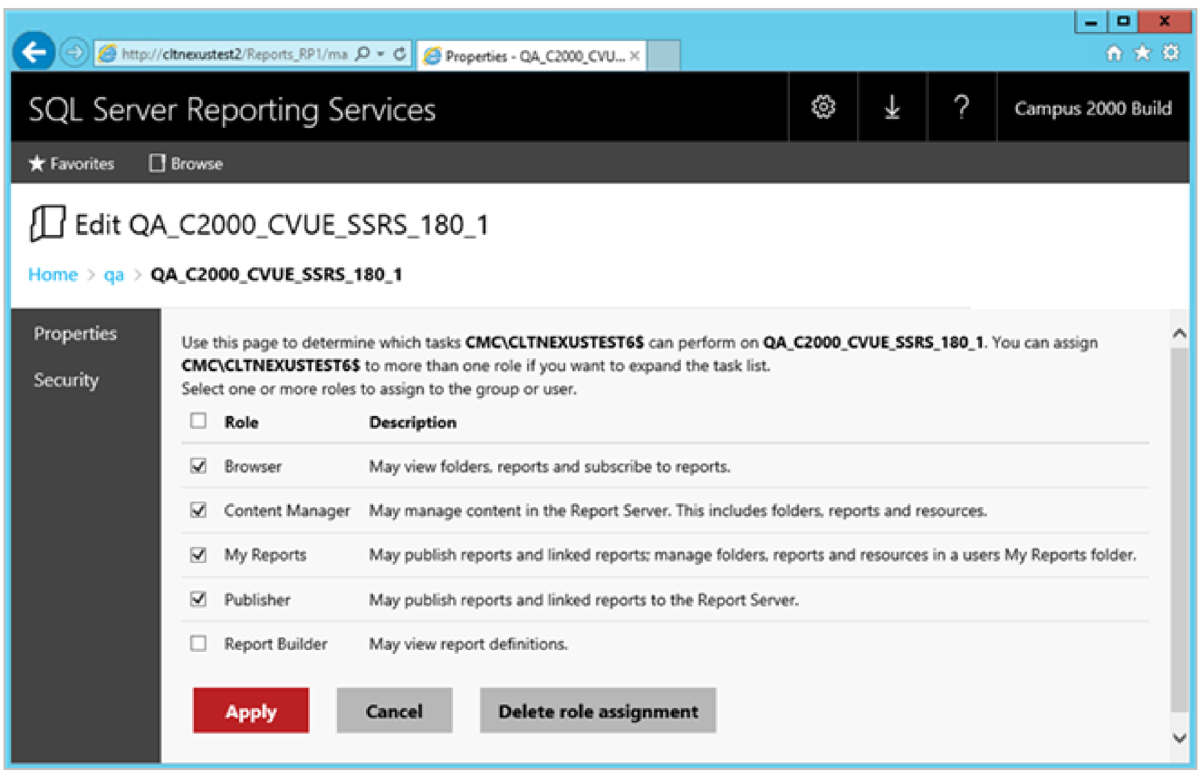
b. Right-click on the ellipsis of the reports folder root and select **Manage**.



c. Select the **Security** tab, click **Customize security**, and click **Add group or user**.

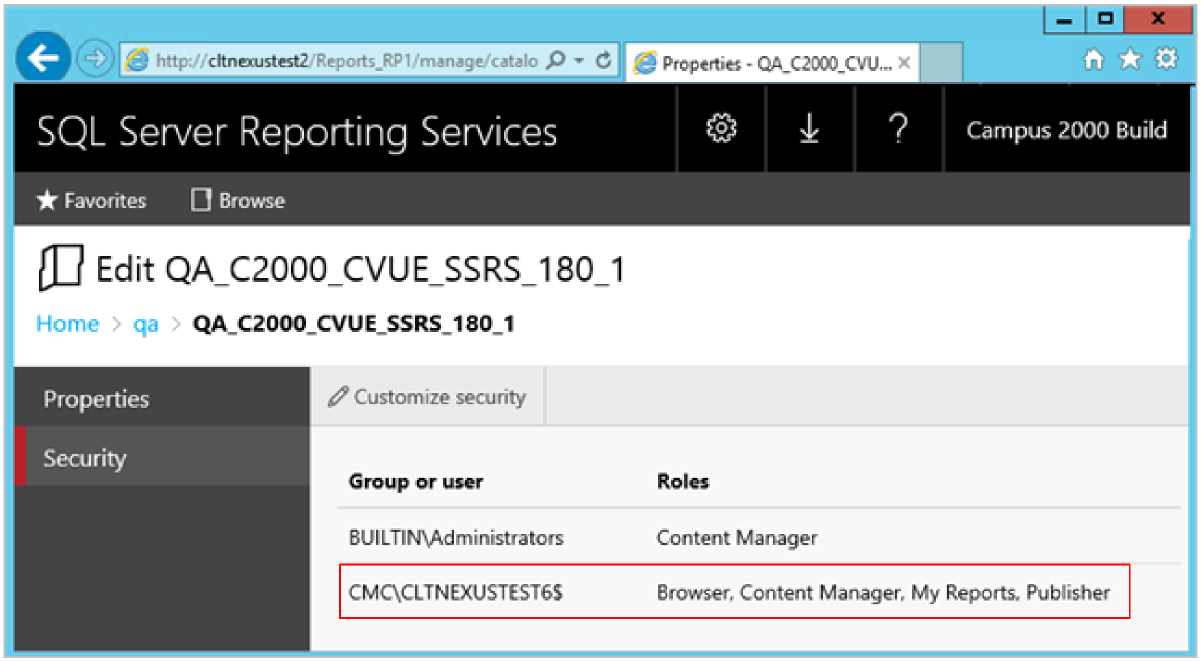
d. Add the **domain\<machine name$>** of Anthology Student and select the following **Roles**:

- Browser
- Content Manager
- My Reports
- Publisher



e. Click **Apply**.

Security for the Reporting Service should be set up as shown below, where CMC\CLTNEXUSTEST6 is the domain\machine name of Anthology Student from which the reports are accessed.



Configure SSRS for HTTPS

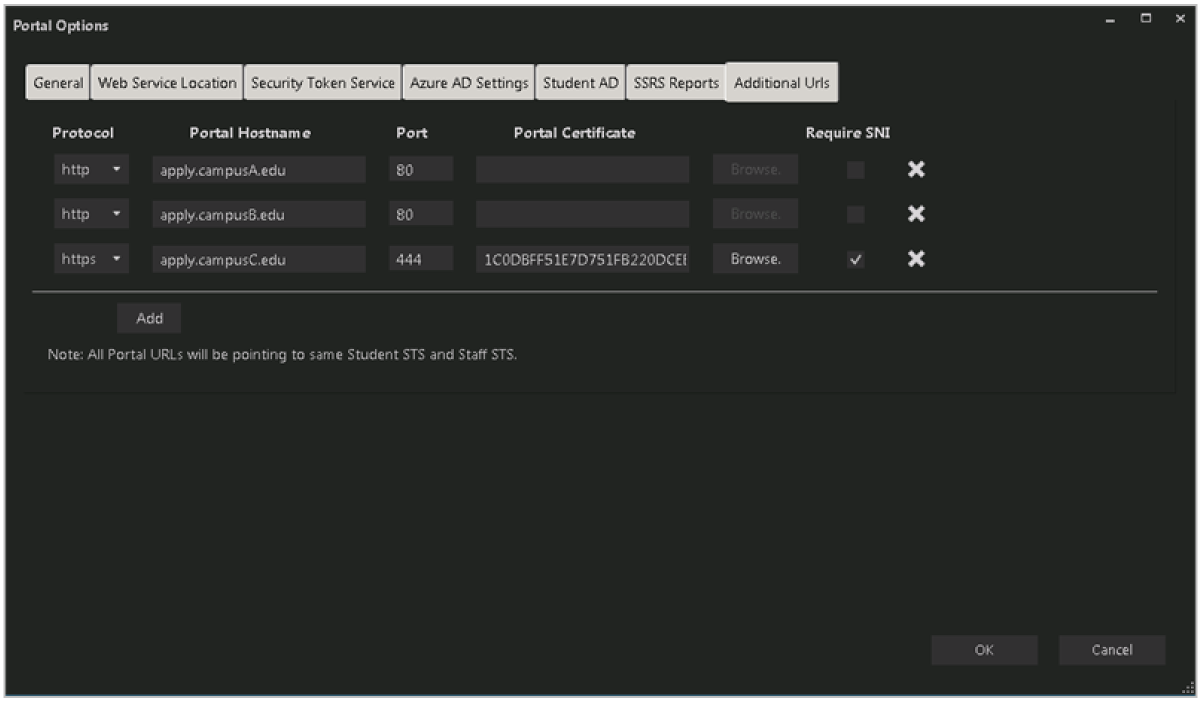
Once the reporting services are installed and configured, test access to the reports in Anthology Student. Select the Reports tile and navigate to any report listed in the menu.

If Anthology Student displays only the title of the report (without any data selection fields), use the browser developer tools (**F12**) and check the **Console** tab. If an error similar to the following is displayed, configure SSRS for secure access with an SSL certificate. For detailed instructions, see https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-ssl-connections-on-a-native-mode-report-server

```
⚠ Mixed Content: The page at 'https://googlesamples.github.io/web-      jquery.js:5562
  fundamentals/samples/discovery-and-distribution/avoid-mixed-content/image-gallery-
  example.html' was loaded over HTTPS, but requested an insecure image
  'http://googlesamples.github.io/web-fundamentals/samples/discovery-and-
  distribution/avoid-mixed-content/puppy.jpg'. This content should also be served
  over HTTPS.
```

Additional Urls Tab

Settings on this tab are required only if the Portal instance is accessed from additional URLs associated with individual campuses. These campuses are served forms from the main Portal instance.



Additional Urls Tab Fields

Field	Description
Add	Click the **Add** button to add a line to the form.
Protocol	Select **HTTP** or **HTTPS** protocol. If HTTPS is selected, the Portal Certificate and Require SNI fields are enabled and must be completed.
Portal Hostname	Specify the hostname for an additional Portal URL. It will be added to the IIS bindings of main Portal instance.
Port	Specify the port number used by the additional Portal URL or accept the default (80).

Field	Description
Portal Certificate	Certificate thumbprint from IIS is required if HTTPS is selected. Copy and paste the thumbprint from Portal into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Require SNI	Server Name Indication (SNI) is required if HTTPS is selected. SNI allows a server to present multiple certificates on the same IP address and TCP port number and hence allows multiple secure websites to be served by the same IP address without requiring all those sites to use the same certificate.

8. Click **OK** to save changes on the Options form. The form is closed.
9. If multiple Portal servers are installed in a server farm (one-to-many NAT), enter the farm's virtual IP address or DNS name in the **Machine Name** field. Installation Manager will display the resulting Portal Farm URL.
10. Click  to delete a selected line.
11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
12. If all tests pass, click .

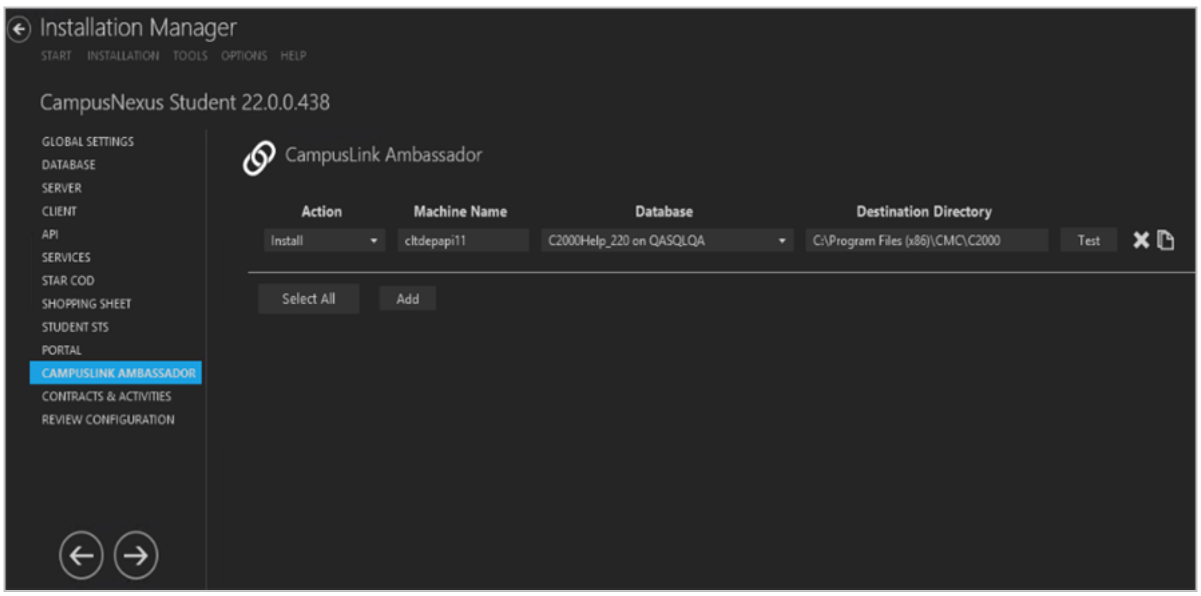
CampusLink Ambassador

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and destination directory for the CampusLink Ambassador (CLA) client tools. The Ambassador Integration WCF Service is installed and configured on the selected machine.

The CLA client tools provide customized integration between Anthology Student and the Ambassador College Books (ACB) application. The ACB application streamlines the book ordering and fulfillment process. CLA enables student information to be automatically sent to ACB and allows all student purchases through ACB systems to appear in the Anthology Student transaction ledger.

Set Up CampusLink Ambassador

1. In the Installation menu, click **CampusLink Ambassador**. The CampusLink Ambassador screen for Anthology Student is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.
6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
7. Click  to copy a line. Edit the copied line as needed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

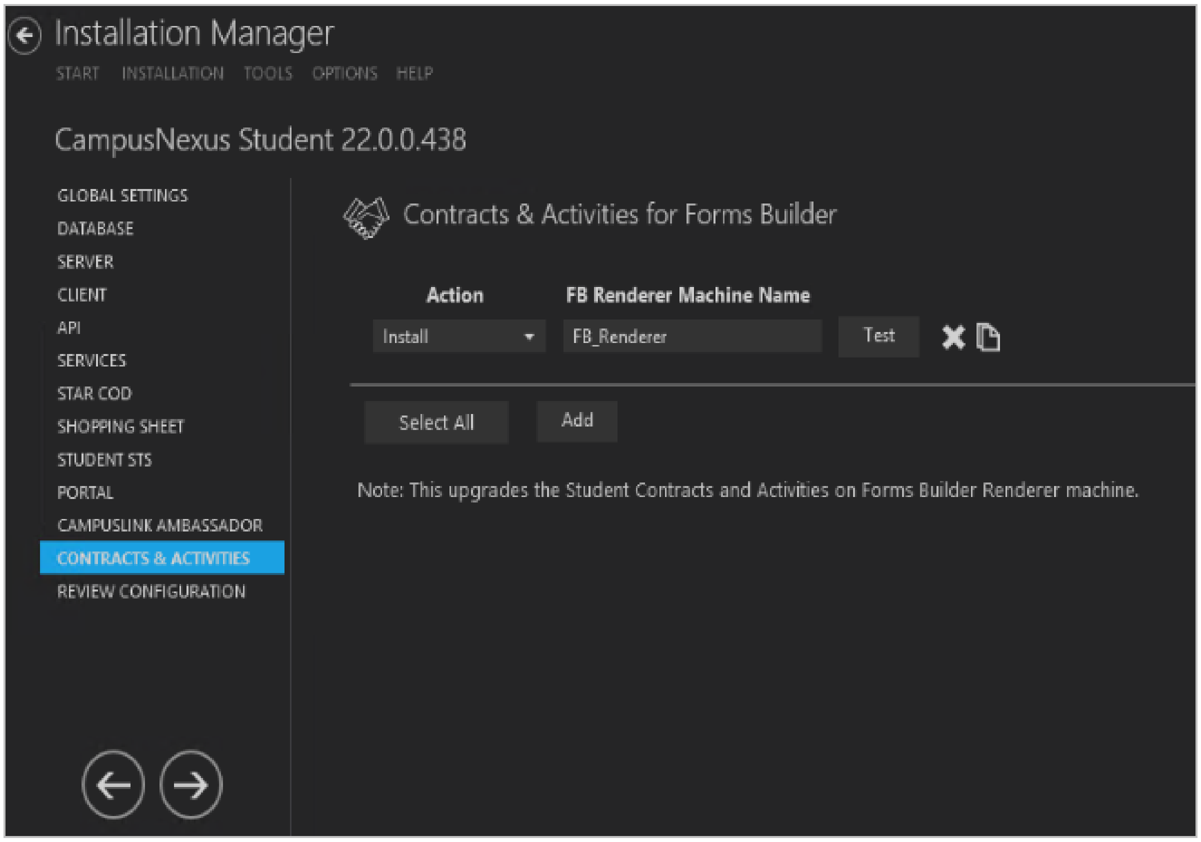
Contracts & Activities

Forms Builder 3.x and later is installed with a base set of Workflow Contracts and Activities. When Anthology Student is upgraded to version 18.2.x, the Anthology Student Contracts and Activities used by Forms Builder need to be upgraded as well.

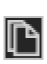
This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name of the Forms Builder Renderer where the Anthology Student Workflow Contracts and Activities for Forms Builder are used.

Set Up the Contracts and Activities for Forms Builder

1. In the Installation menu, click **Contracts & Activities**. The Contracts & Activities for Forms Builder screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter a **Machine Name** of the Forms Builder Renderer where the Contracts & Activities are used.
5. Click  to copy a line. Edit the copied line as needed.
6. Click  to delete a selected line.
7. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

8. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

Review the Configuration and Start Installation

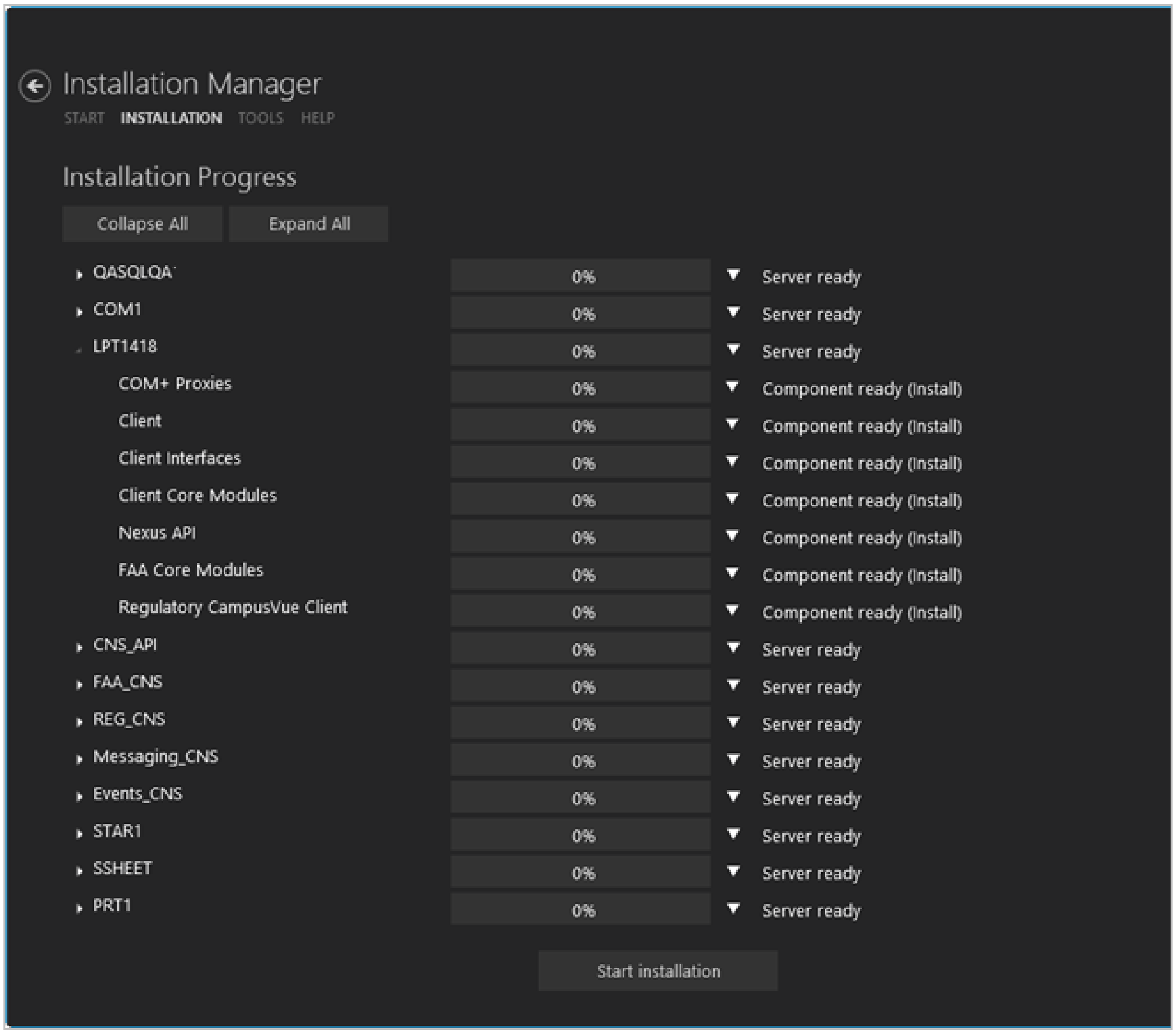
1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

   Indicates that the component passed the prerequisites check.

   Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.
3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.

   Click **Expand All** and scroll through the list of items. Or, click **Collapse All** and then click to expand a section.



4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click ▼ next to a progress bar to access installation logs and other tools (see Installation).

FAA Web App

To add Financial Aid Automation (FAA) to an existing Anthology Student system, use Package Manager to download the Financial Aid Automation installation files for the Student Web App.

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

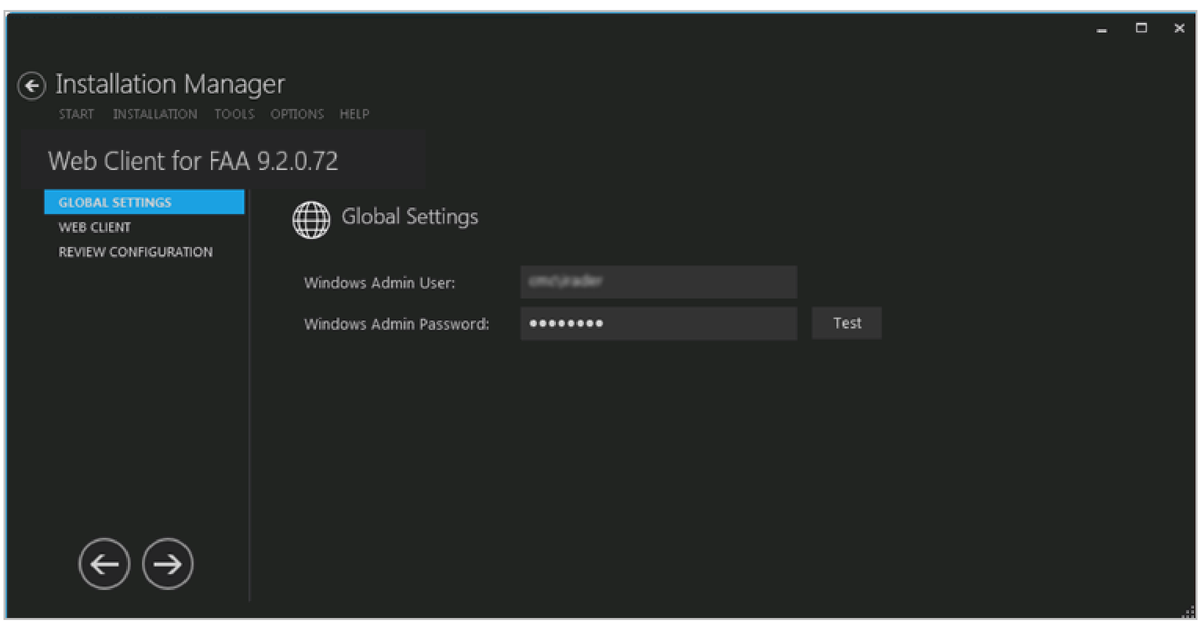
Global Settings

The Global Settings screen contains the Windows Admin user name password used when starting an installation of Financial Aid Automation. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Web Client for Financial Aid Automation** tile. The Global Settings screen is displayed.



2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer where the installation will occur. Depending on your network environment, specify one of the following:

- User name
- Domain\User name
- Email address of Admin User

3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

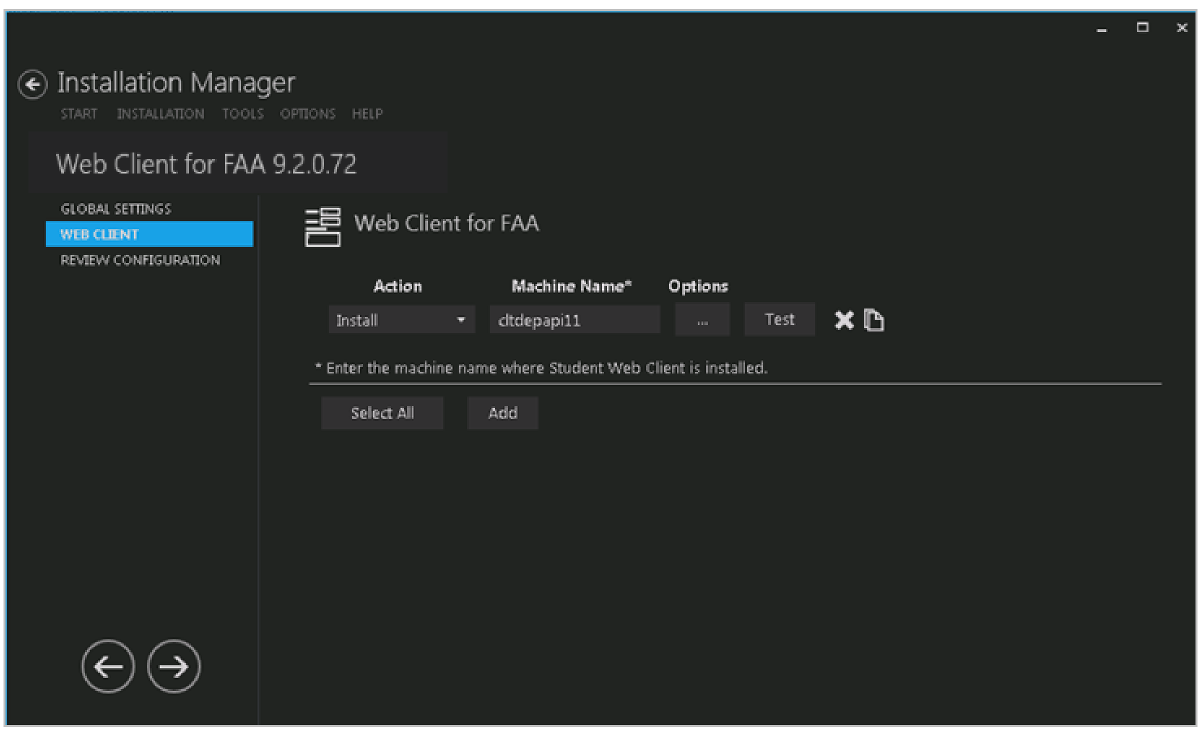
5. If the user is authenticated, click  to continue.

Web Client

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name of the standard interface for Financial Aid Automation and the Anthology Student database.

Set Up the Web Client

1. In the Installation menu, click **Web Client**. The Web Client for FAA screen is displayed.



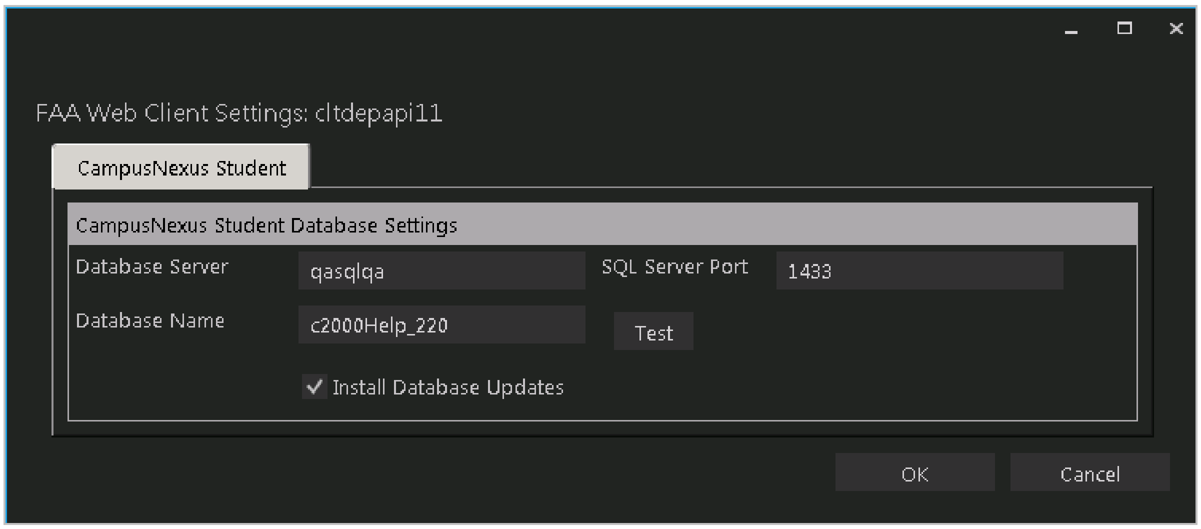
2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Click to view and edit the Options form.



Anthology Student Tab Fields

Anthology Student Database Settings	
Database Server	Name of the SQL server on which the Anthology Student database resides.
SQL Server Port	Specify the port number of the SQL server or accept the default (1433).
Database Name	Name of the Anthology Student SQL database.
Test	Click **Test** to verify the database connection.
Install Database Updates	Select this check box to install updates to the Anthology Student database. Click **Test** to verify the database connection.

6. Click **OK** to save changes on the Options form. The form is closed.
7. Click to copy a line. Edit the copied line as needed.
8. Click to delete a selected line.

9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

   The Test button checks the connectivity of the Admin user to the machine specified in the Server name field.

10. If all tests pass, click .

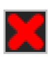
Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

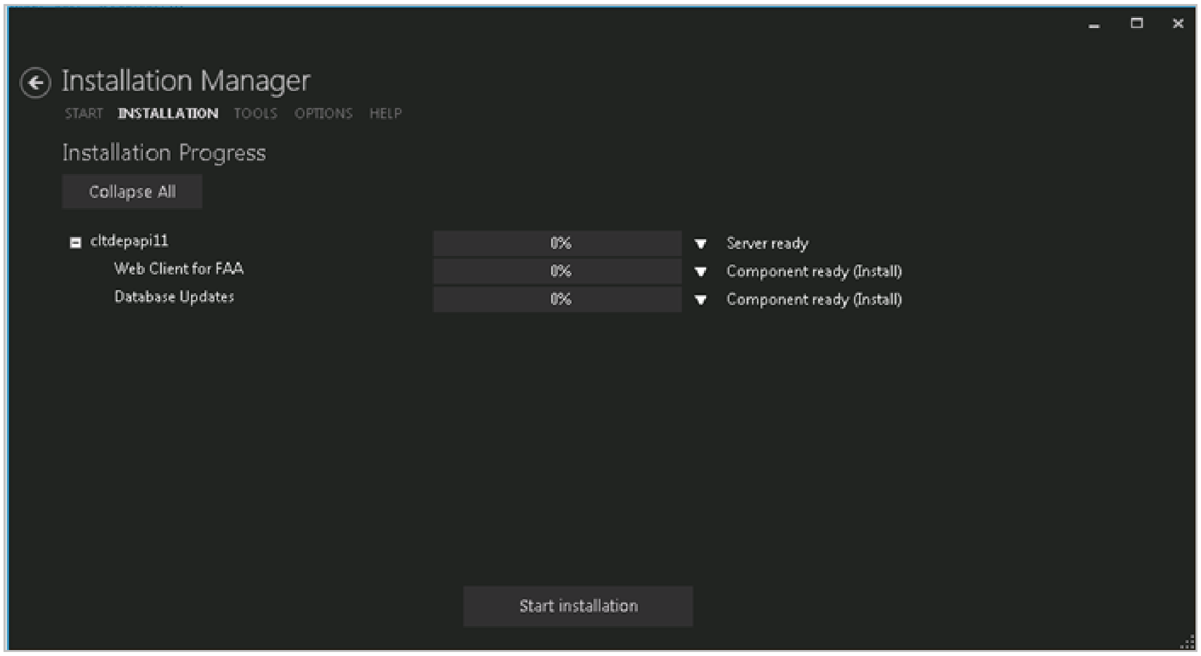
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.
3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.
4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.



Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

FAA Legacy Interface

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

Financial Aid Automation (FAA) is an optional component of Anthology Student. The Automated Processes service can be selected during the initial Anthology Student installation, or it can be added to an existing Anthology Student system.

To add Financial Aid Automation to an existing Anthology Student system, download the Financial Aid Automation installation files using Package Manager, click the Financial Aid Automation tile on the Start screen, and proceed with the installation screens.

Notes:

- Before installing Financial Aid Automation, we recommend that you obtain the customer's EDconnect account so that you can assign administrator permissions on the folders used by EDconnect.
- If Workflow is installed, we recommend that you create separate admin users for Workflow and Financial Aid Automation so that processes run by Workflow and Financial Aid Automation can be easily identified in the logs during troubleshooting. To create separate admin users, use the Auth Options on the Services screen to override the Global Settings.

Global Settings

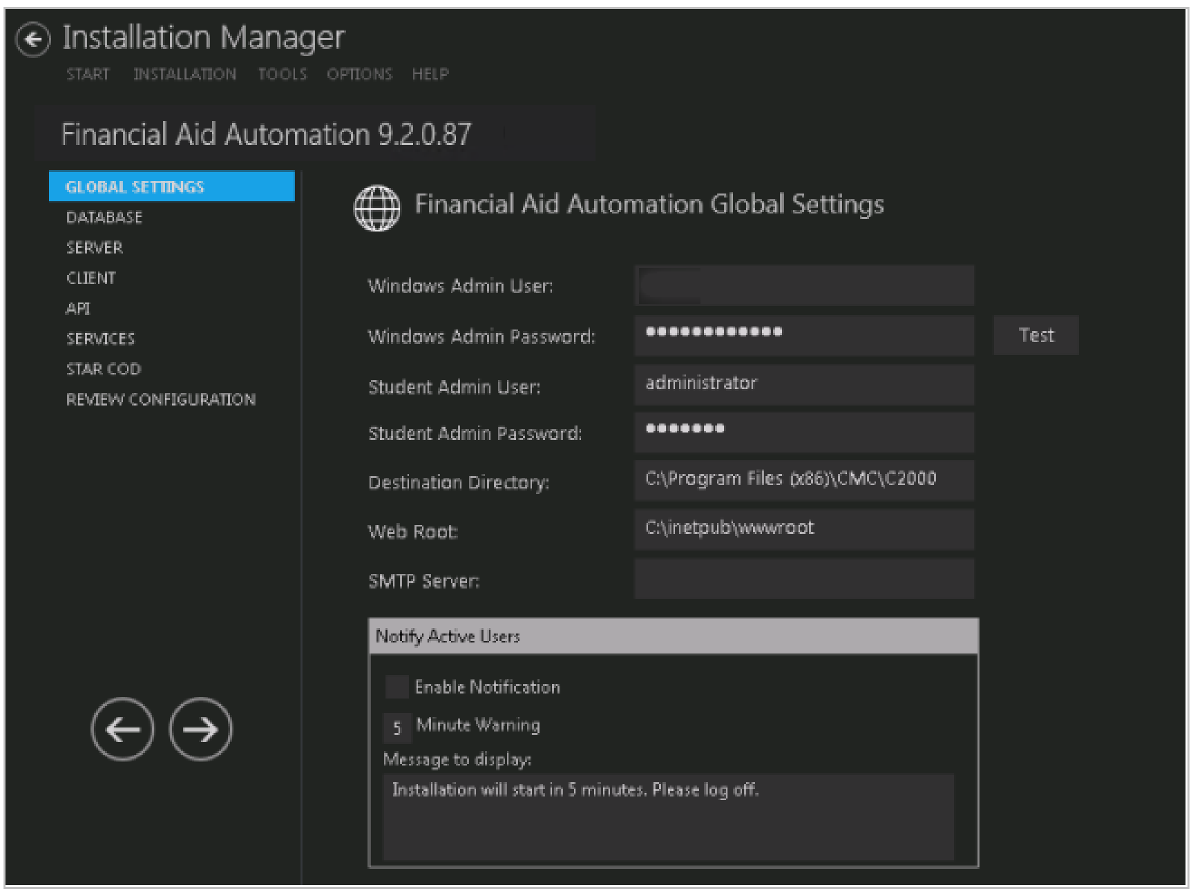
This screen contains the Windows Admin user name password used when starting an installation of Financial Aid Automation for the legacy interface of Anthology Student. Users can also test this information without moving from the screen.

Note: The Global Settings screen for Anthology Student indicates the versions of Financial Aid Automation and Regulatory that are compatible with Anthology Student. Financial Aid Automation and Regulatory can be installed with Anthology Student (see Services for Anthology Student) or added later.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Financial Aid Automation** tile. The Global Settings screen is displayed.



2. Complete the fields on the Global Settings screen as described in the table below.

Global Settings Fields

Field	Description
Windows Admin User	Specify the user name of the user with administrator permissions on the computer where the COM, Windows, and Web Services will run. This account must have administrative access to all the machines being installed to. It must be a sysadmin on the database as integrated security is the only option that will be used. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Windows Admin Password	Specify the password for the Administrator user name. This password is used in the background for other installation steps. **Note**: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.
Student Admin User	Specify the user name of the Anthology Student user with administrator permissions. This is the Anthology Student administrator account that the Windows and Web Services use for Anthology Student access. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Student Admin Password	Specify the password for the Anthology Student Admin User.
Destination Directory	The default directory for the Anthology Student Client and Server is C:\Program Files (x86)\CMC\C2000. You can override the default by choosing another path.
Web Root	The default web root for the APIs to be installed is C:\inetpub\wwwroot. You can override the default by choosing another path.

Field	Description
SMTP Server	Enter the Email (SMTP) Server address used for sending out email notifications by doing the following: a. Determine the desired Email (SMTP) Server IP address and DNS names. b. On the Exchange Server, an entry for an open relay on TCP Port 25 must be allowed and open to receive SMTP traffic from the MTS Server. This traffic must not be routed through a firewall. OSI Layer 7 firewalls can interfere with the service. c. Ping the Email (SMTP) Server from the MTS Server and the SQL Server. d. Telnet to the Email (SMTP) Server on Port 25 and verify successful connection from the MTS Server. e. Enter the IP address in the SMTP Server field.
Notify Active Users	
Enable Notification	Select this check box to enable notification of active Anthology Student users when an installation is about to begin.
Minute Warning	Specify the notification time, that is, the number of minutes until the installation starts.
Message to display	Enter the message to be displayed in the notification window.

3. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

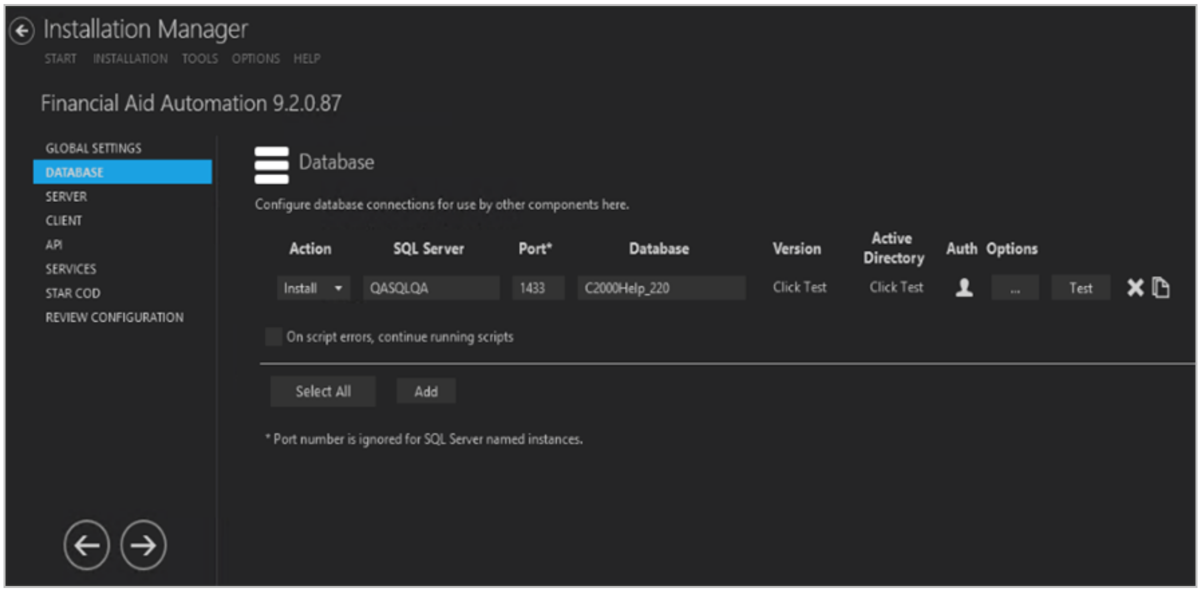
4. If the user is authenticated, click **OK** and click  to continue.

Database

This screen enables you to select the actions to be taken by Installation Manager (e.g., install) and to specify the machine name, the Anthology Student database, and, if applicable, additional databases for Portal and Talisma Fundraising.

Set Up the Database

1. In the Installation menu, click **Database**. The Database screen for Financial Aid Automation is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.

   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the name of the **SQL Server** where the Anthology Student database is installed.

5. Specify the **Port** number for the SQL Server or accept the default (1433).

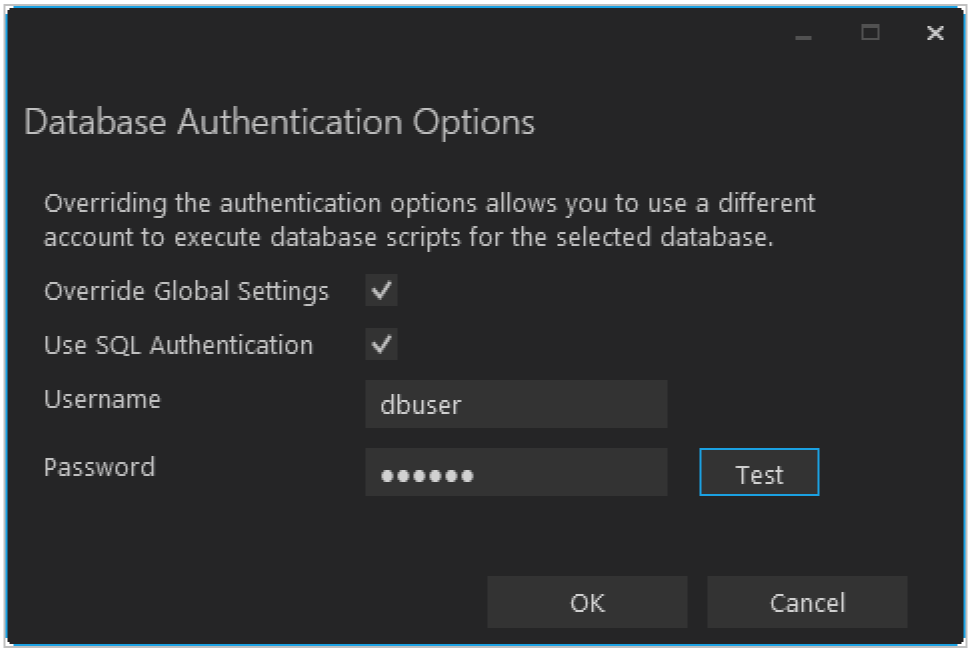
   Note: The port number is ignored for named instances of SQL Server.

6. Specify the name of the **Database** for Anthology Student. The database name must be unique — 'master' is not allowed.

7. The **Version** field is populated when you click the **Test** button.

8. The **Active Directory** field is populated when you click the **Test** button.

9. Click in the **Auth** column if you want to override the authentication options from [Global Settings]() for the selected database, for example, to give another user permissions to execute scripts for the selected database. The Database Authentication Options form is displayed.



   a. Select the **Override Global Settings** check box to enable the fields on the form.

   b. Optional: Select the **Use SQL Authentication** check box if SQL authentication is applied.

      The license checks, version number check, SQL script execution, student admin role check, and MSI parameters will use SQL authentication if selected.

   c. Enter the **Username** and **Password** of the account that is given the override permissions for the selected database.

      The Test buttons in the Options form and in the Database screen will use these credentials if selected.

   d. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

   e. Click **OK** to save changes on the Options form. The form is closed.

10. Select the check box for **On script errors, continue running scripts** if you want the installation process to continue regardless of errors encountered.

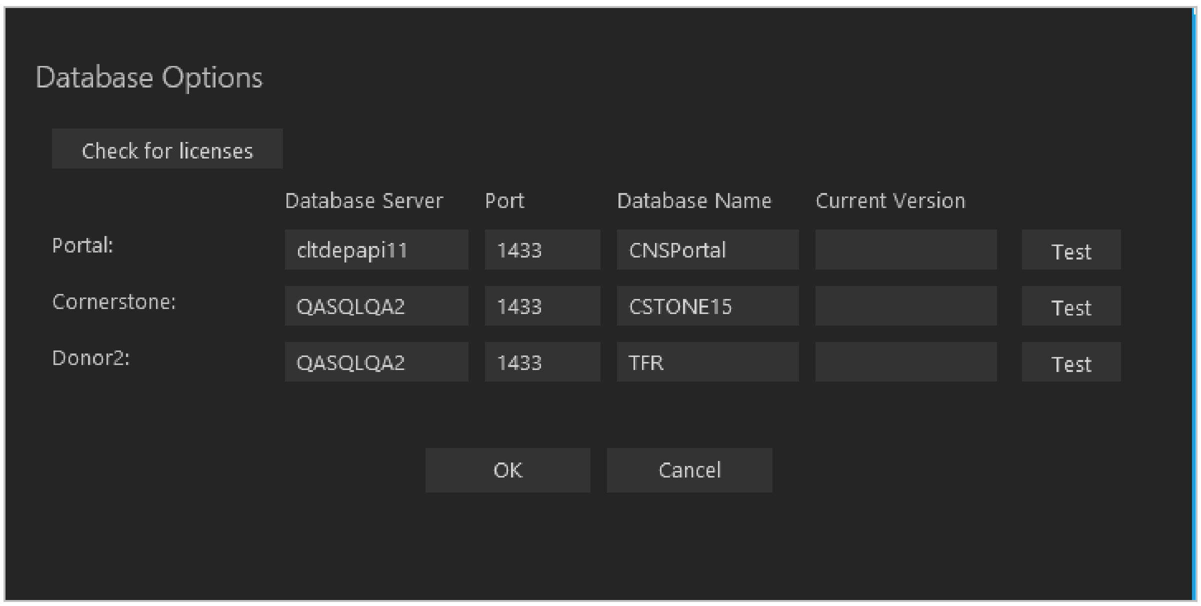
By default, database upgrades will stop if the script encounters any errors. This selection is used if there are custom modifications to the database that are known to cause errors in the upgrade scripts. Selecting this option enables all scripts to be run against the specified database.

Whether the check box is selected or not, any errors are written to a separate error file for each script, which may be investigated after the script execution. Error logs are stored in the following folder: `DatabaseServer\C:\Logs\Output`.

The error log is the name of the script, SQL Server, and database name appended with `_Errors.txt`, for example,
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Errors.txt`)

There is also an output file that has all of the script output:
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Output.txt`

11. Click  to view and edit the Options form.



The Options form is used to specify databases for Portal and Talisma Fundraising. Corresponding licenses are required.

- Entering a Portal database is only necessary for an installation that includes the e-Learning component that has a Portal component and license key associated with Anthology Student.
- The Cornerstone and Donor2 databases are used for Talisma Fundraising in conjunction with the primary Anthology Student database. Installation Manager detects if Talisma Fundraising is enabled in the Anthology Studentt database.

Database Options Fields

Field	Description
Check for Licenses	This button queries the Anthology Student database and checks for product licenses. Based on the licenses found, Installation Manager enables the Portal, Cornerstone, and Donor2 fields. If the licenses are not found, the Licensed? field indicates "False" and the fields remain disabled.
Portal	
Database Server	Name of the SQL server on which the Portal database resides.
Port	Specify the port number for the Portal database or accept the default (1433).
Database Name	Name of the Portal SQL database.
Current Version	This field is populated when you click the **Test** button.
Cornerstone	
Database Server	Name of the SQL Server on which the Cornerstone database resides.
Port	Specify the port number for the Cornerstone database or accept the default (1433).
Database Name	Name of the Cornerstone SQL database.
Current Version	This field is populated when you click the **Test** button.
Donor2	
Database Server	Name of the SQL Server on which the Donor2 database resides.
Port	Specify the port number for the Donor2 database or accept the default (1433).
Database Name	Name of the Donor2 SQL database.
Current Version	This field is populated when you click the **Test** button.

12. Click **OK** to save changes on the Options form. The form is closed.
13. Click to copy a line. Edit the copied line as needed.
14. Click to delete a selected line.
15. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Note: The Test button operates as follows:

    - Queries the database to get the latest version of Anthology Student and populates the current version field.
    - Uses Windows Admin credentials (see Global Settings) and tests connectivity to the SQL server.

- Uses the Student Admin user name (see Global Settings) and checks if it exists in the Anthology Student database.

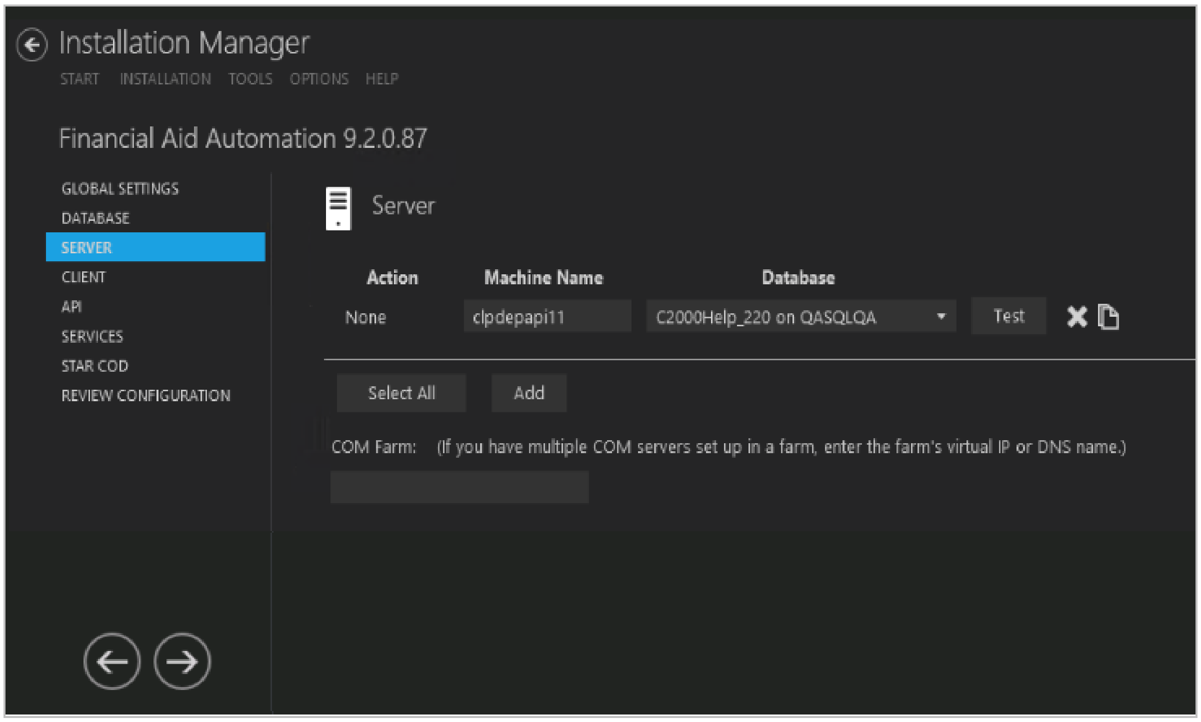
16. If all tests pass, click .

Server

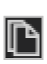
This screen enables you to specify the machine name and select the Anthology Student database accessed by the Financial Aid Automation Server component.

Set Up the Server

1. In the Installation menu, click **Server**. The Server screen for Financial Aid Automation is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** of the Server.
5. Select the Anthology Student **Database** used by Financial Aid Automation.
6. In the **COM Farm** field, enter the farm's virtual IP address or DNS name if you have multiple COM servers set up in a server farm with a load-balancing system.
7. Click  to copy a line. Edit the copied line as needed.

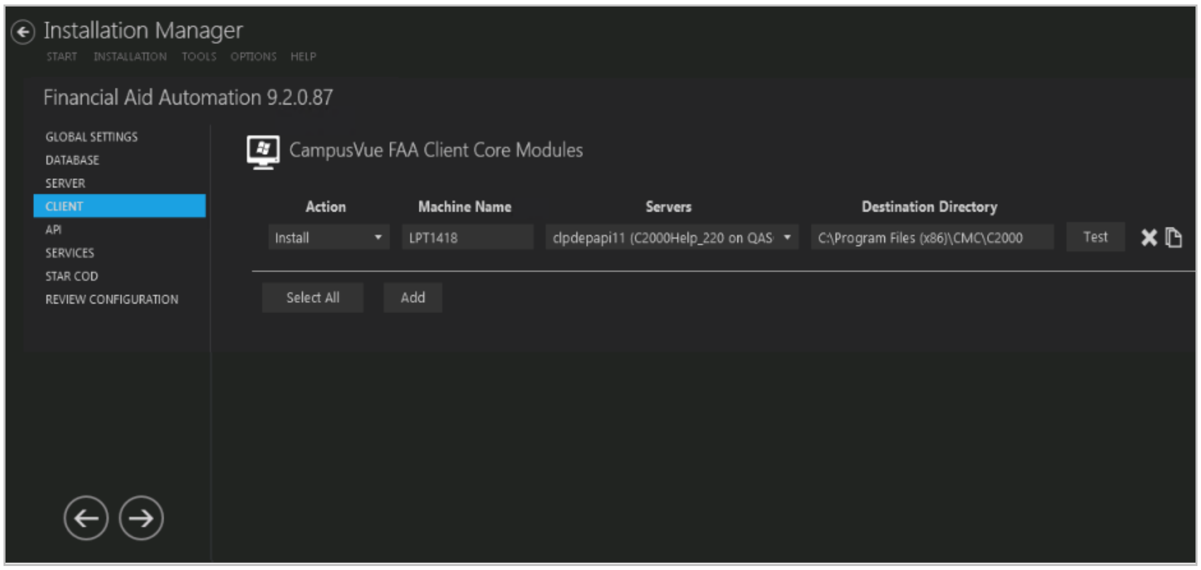
8. Click to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

Client

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name of the legacy interface (desktop client) for Financial Aid Automation.

Set Up the Client

1. In the Installation menu, click **Client**. The Client screen for Financial Aid Automation is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the legacy interface for Anthology Student will be installed.
5. Select the **Server**. The drop-down list displays the values specified on the Server screen.
6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.

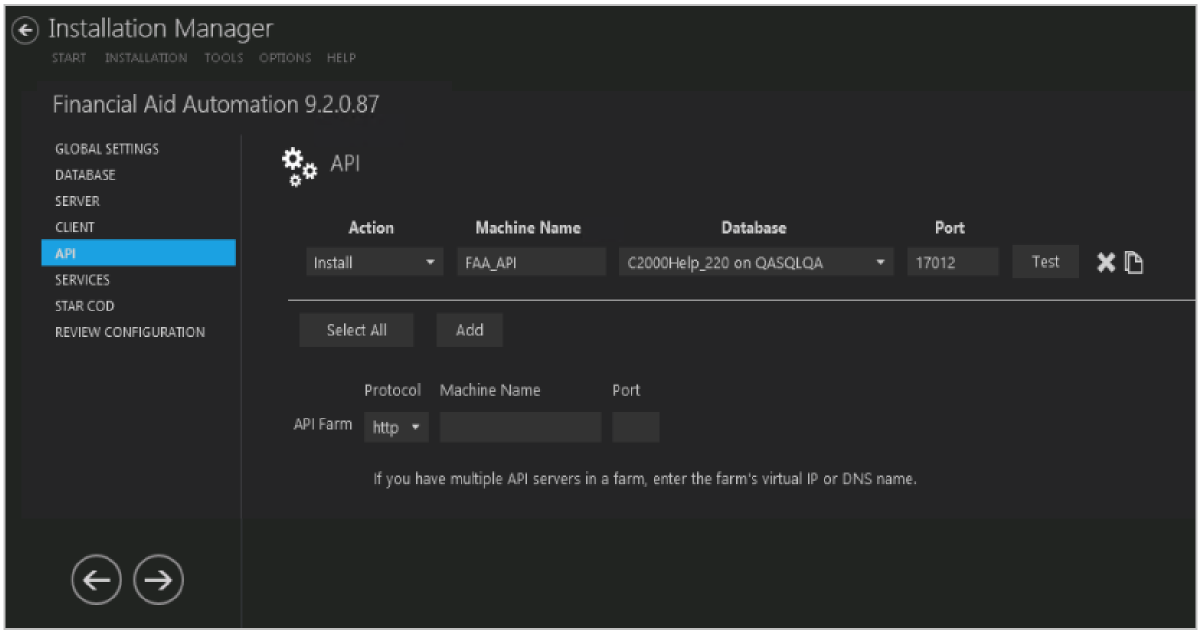
7. Click  to copy a line. Edit the copied line as needed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

API

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database server, and port to be used by the Web Services (APIs) for Financial Aid Automation.

Set Up the APIs

1. In the Installation menu, click **API**. The API screen for Financial Aid Automation is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the APIs for Anthology Student will be installed.

5. In the **Database** field, select a database for Financial Aid Automation. The drop-down contains a list of databases configured in the Database settings screen.
6. In the **Port** field, enter the name of the port where the Web Services will be installed.
7. Click  to copy a line. Edit the copied line as needed.
8. Click  to delete a selected line.
9. If multiple API servers are installed in a server farm:
    a. Select the **Protocol** (http or https).
    b. Enter the farm's virtual IP address or DNS name in the **Machine Name** field.
    c. Specify the **Port** number.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Notes:

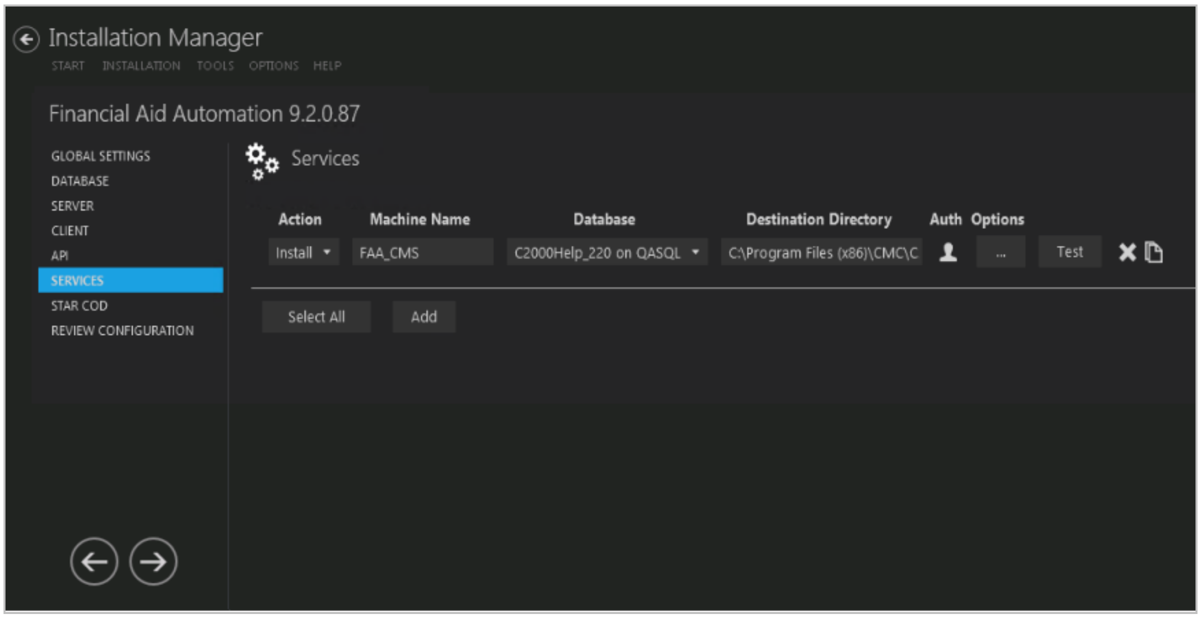
    - The Test button checks if the port number is in use; if so, the user is prompted to enter a different port number.
    - If an upgrade is performed, Installation Manager first checks if the port number is in use by the same Web Service that’s being installed.
11. If all tests pass, click .

Services

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, type, database, and options for the Automated Processes services.

Set Up the Services

1. In the Installation menu, click **Services**. The Services screen for Financial Aid Automation is displayed.

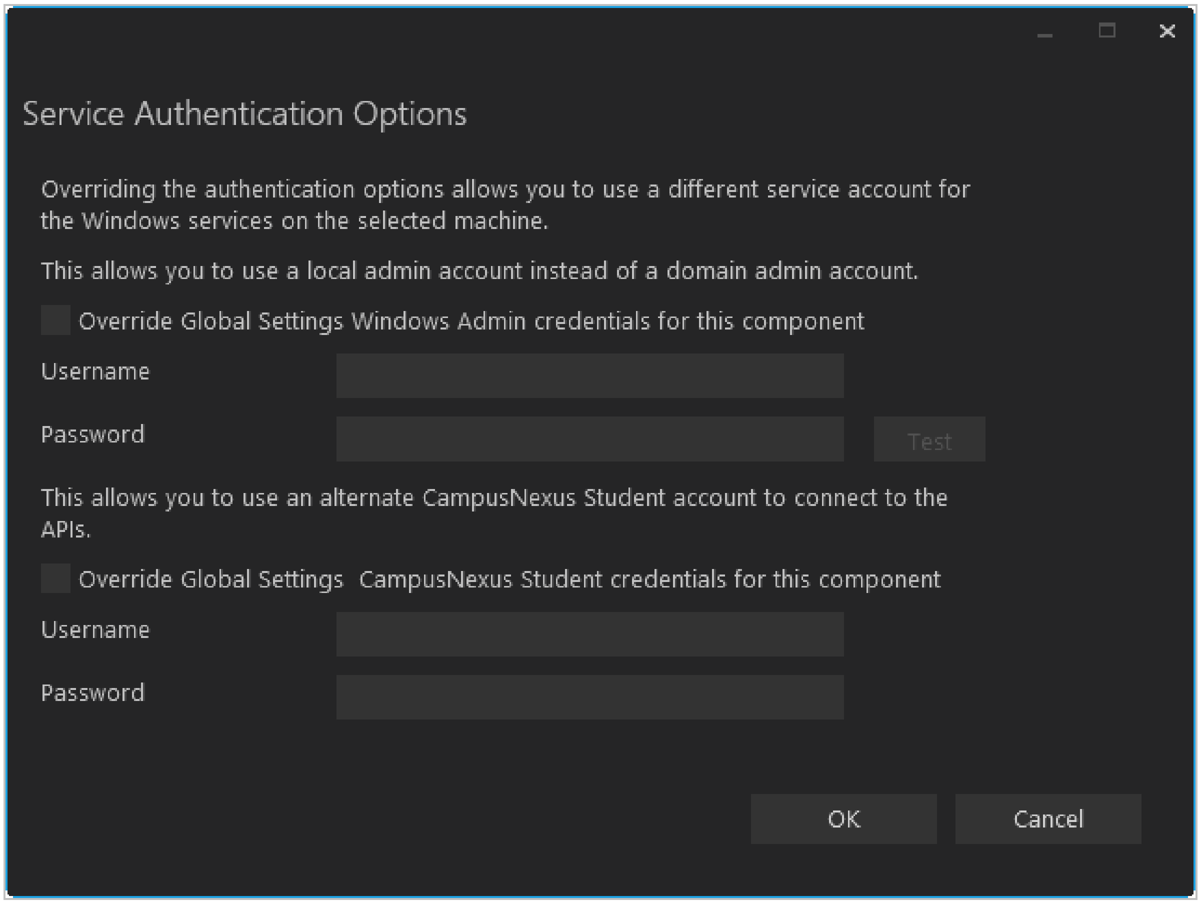


2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.

6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.

7. Click in the **Auth** column if you want to override the authentication options from Global Settings to use a different account for the Windows services and alternate Anthology Student credentials on the selected machine. The Service Authentication Options form is displayed.



   a. Select the check box **Override Global Settings Windows Admin credentials for this component** to enable the associated fields on the form. This option allows you to use a local admin account instead of the domain admin account.

   b. Enter the **Username** and **Password** of the local admin account for the selected machine.

   c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

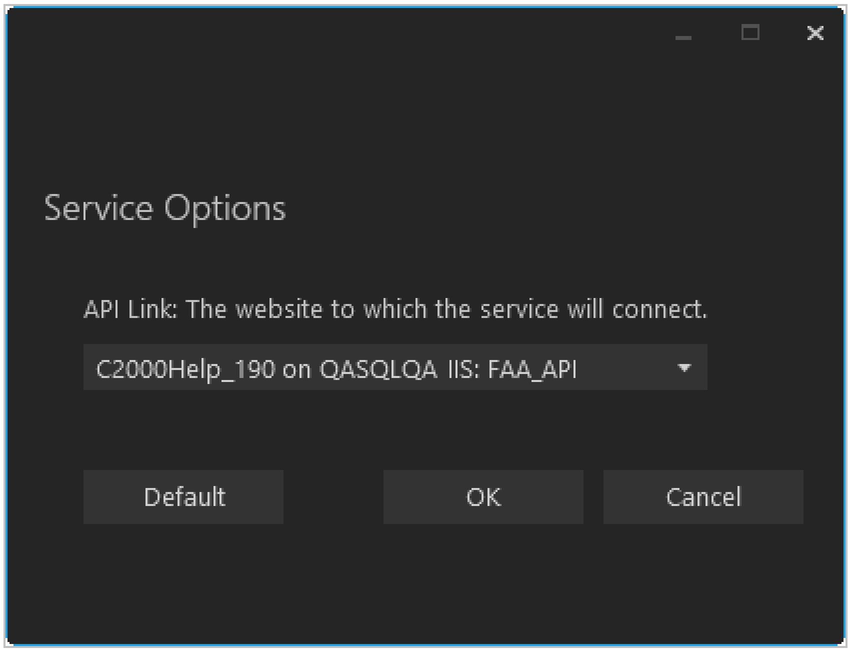
   d. Select the check box **Override Global Settings Anthology Student credentials for this component**.

   e. Enter the **Username** and **Password** of Anthology Student account for the selected machine.

f. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

g. Click **OK** to save changes on the Options form. The form is closed.

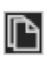
8. Click  to view and edit the Options form.



In the Service Options window, select the database and installed system to be used by the Automated Processes Web Service (API).

— OR —

Click **Default** to use the API server based on the database selected.

9. Click **OK** to save changes on the Options form. The form is closed.
10. Click  to copy a line. Edit the copied line as needed.
11. Click  to delete a selected line.
12. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
13. If all tests pass, click .

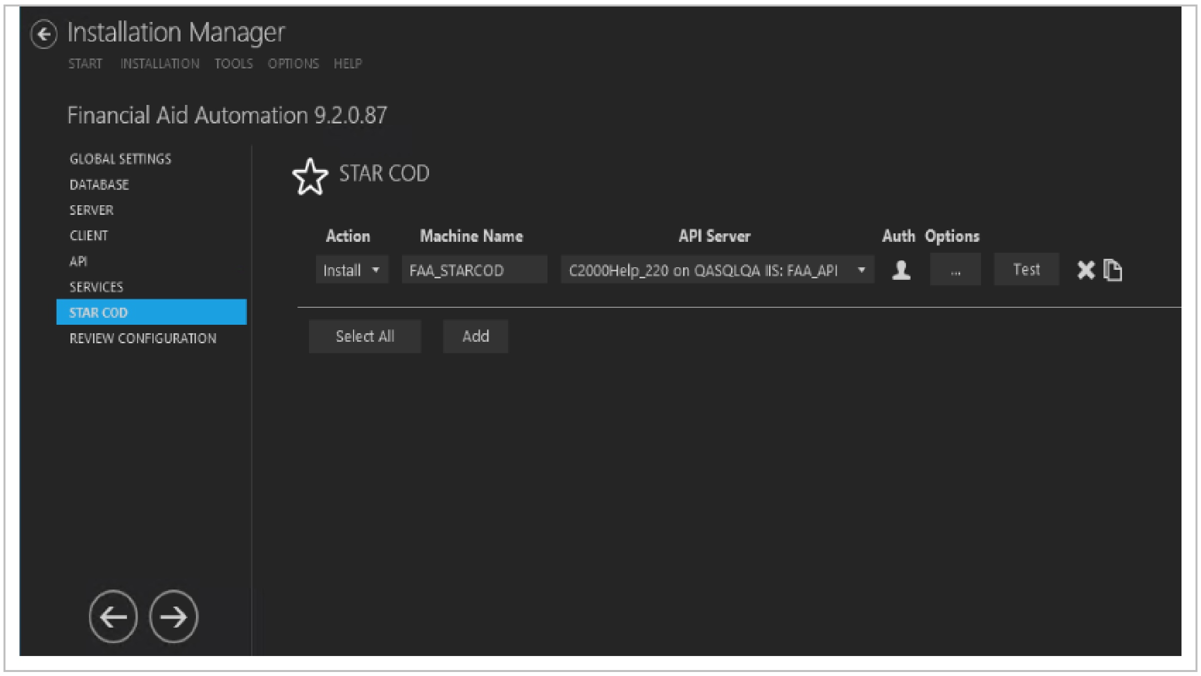
STAR COD

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and options for transmission and retrieval of STAR COD files to and from Anthology Student.

Note: STAR COD is typically installed on the machine where EDconnect is installed. Keep in mind that EDconnect currently does not support Windows Server 2012.

Set Up STAR COD

1. In the Installation menu, click **STAR COD**. The STAR COD screen for Financial Aid Automation is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

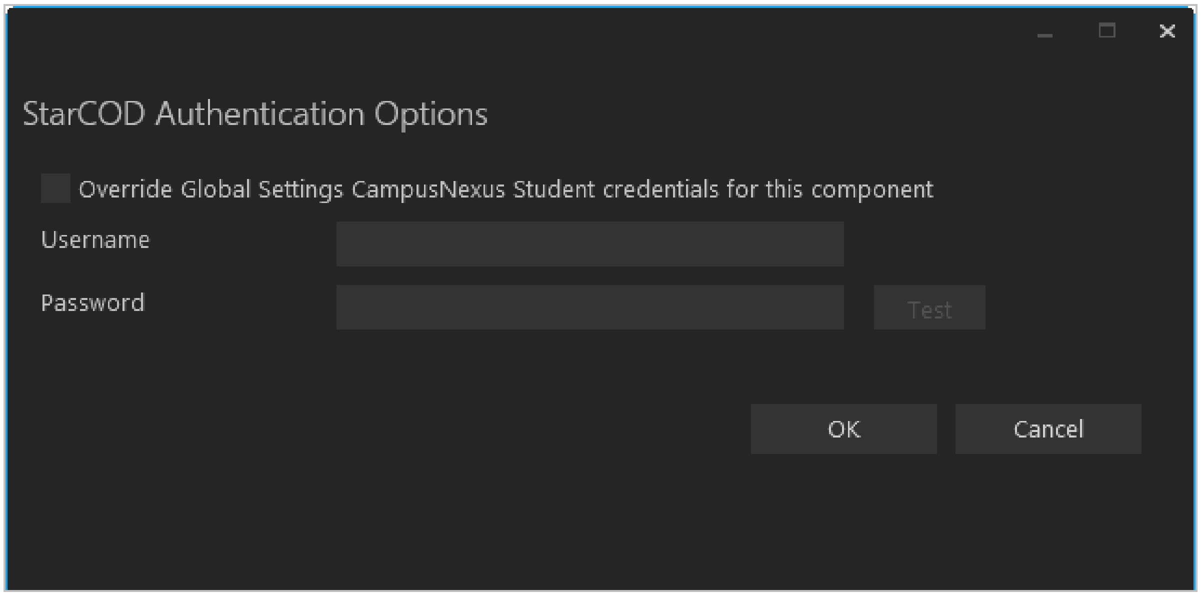
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.

5. Select the **API Server**. The drop-down list contains all the API Servers for the Anthology Student databases configured in the API settings screen.

6. Click in the **Auth** column if you want to override the authentication options from Global Settings to use alternate Anthology Student credentials on the selected machine. The StarCOD Authentication Options form is displayed.



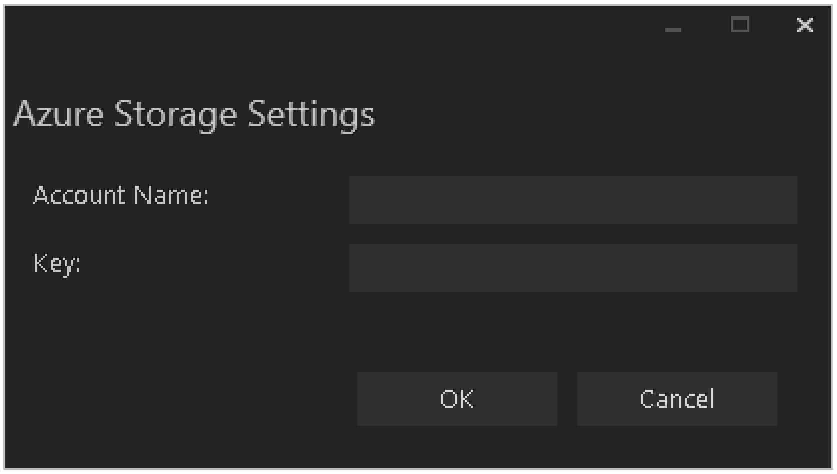
   a. Select the check box **Override Global Settings Anthology Student credentials for this component** to enable the fields on the form.

   b. Enter the **Username** and **Password** of the Anthology Student account for the selected machine.

   c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

   d. Click **OK** to save changes on the Options form. The form is closed.

7. Click to view and edit the Options form.



   a. If you are installing FAA in an Azure environment, specify the **Account Name** and **Key**.

   b. Click **OK** to save changes on the Options form. The form is closed.

8. Click  to copy a line. Edit the copied line as needed.

9. Click  to delete a selected line.

10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

11. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

Review the Configuration and Start Installation

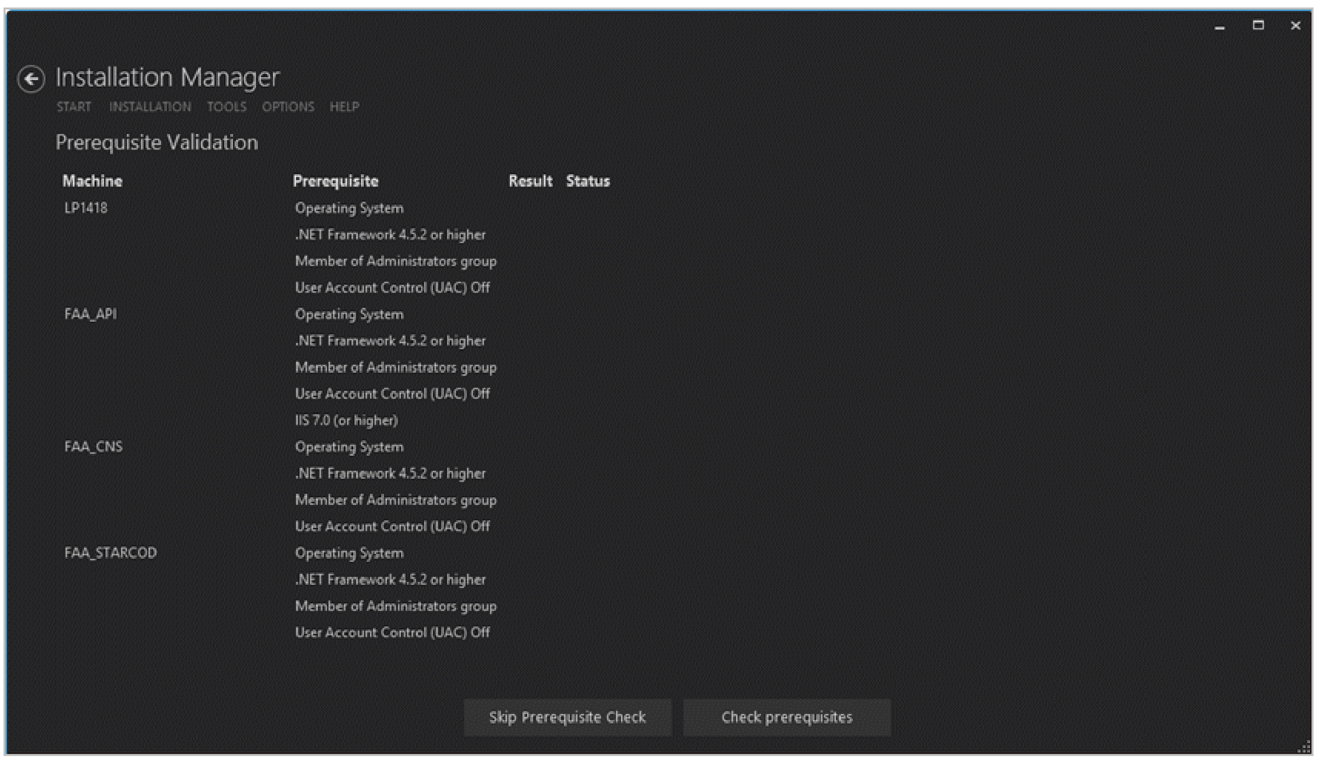
1. Once all setup screens have been properly populated and all lines have been tested and found to be functional, click **Review Configuration** to see all of the information in one screen.

2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.

   Click **Expand All** and scroll through the list of items. Or, click **Collapse All** and then click  to expand a section.

4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click ▼ next to a progress bar to access installation logs and other tools (see Installation).

Regulatory Web App

To add Regulatory to an existing Anthology Student system, use Package Manager to download the Regulatory installation files for the Student Web App.

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

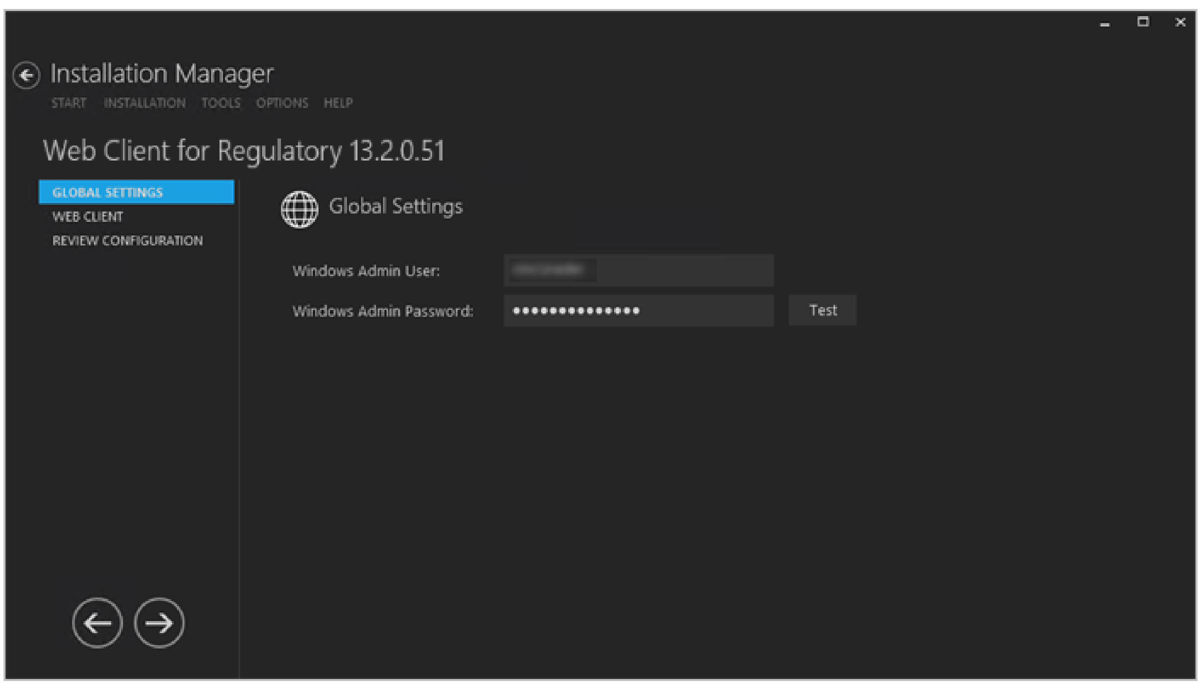
Global Settings

The Global Settings screen contains the Windows Admin user name password used when starting an installation of Regulatory. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the [Start](#) screen of Installation Manager, click the **Web Client for Regulatory** tile. The Global Settings screen is displayed.



2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer where the installation will occur. Depending on your network environment, specify one of

the following:

- User name
- Domain\User name
- Email address of Admin User

3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

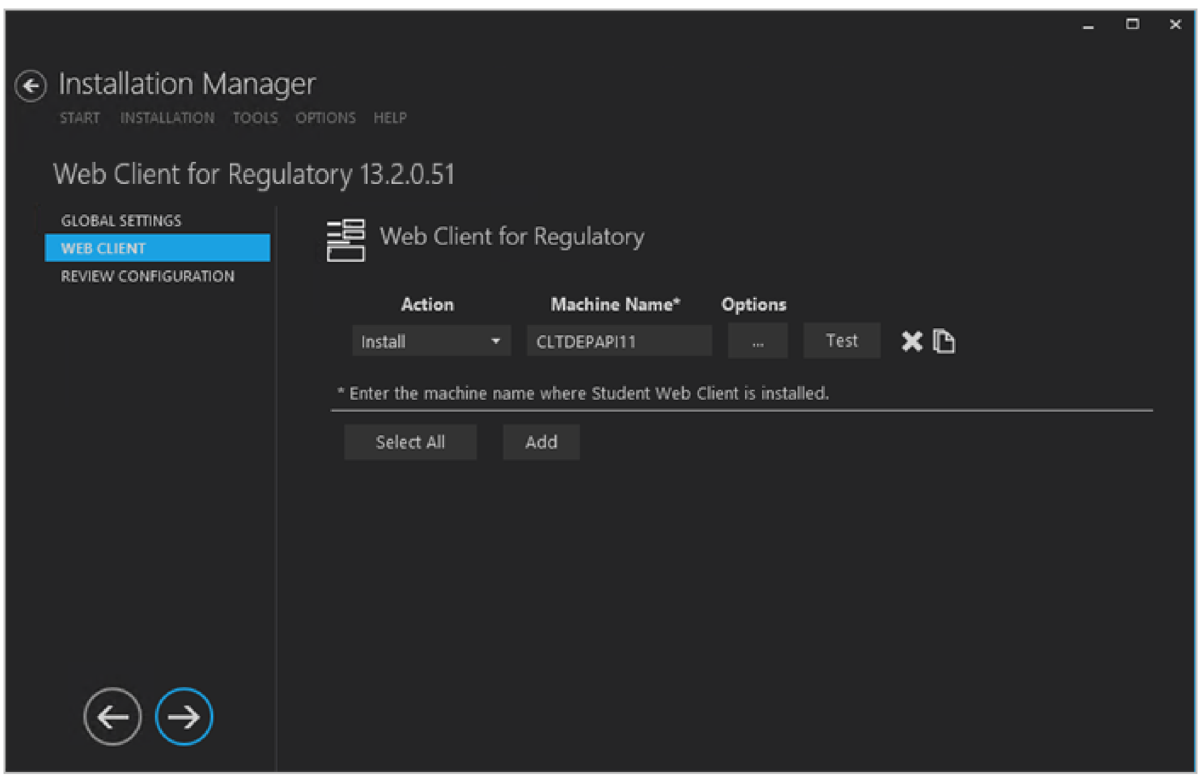
5. If the user is authenticated, click **OK** and click  to continue.

Web Client

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and options of the standard interface (web client) for Regulatory.

Set Up the Web Client

1. In the Installation menu, click **Web Client**. The Web Client for Regulatory screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

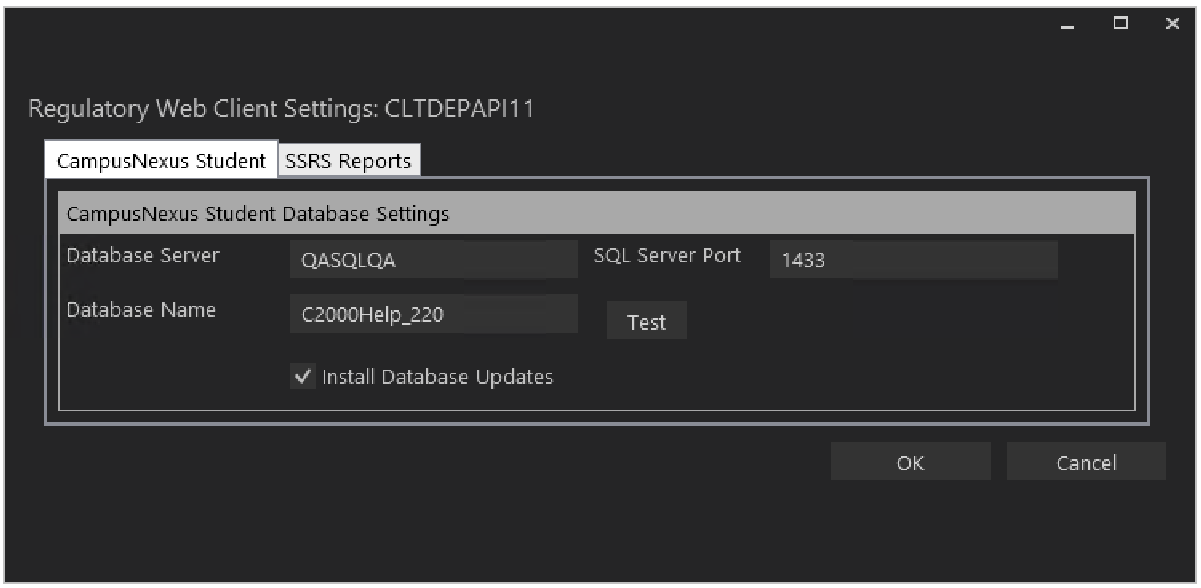
- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Click  to copy a line. Edit the copied line as needed.
6. Click  to view and edit the Options form.

Anthology Student Tab

Use this tab to configure the Anthology Student database connection for use by Regulatory.



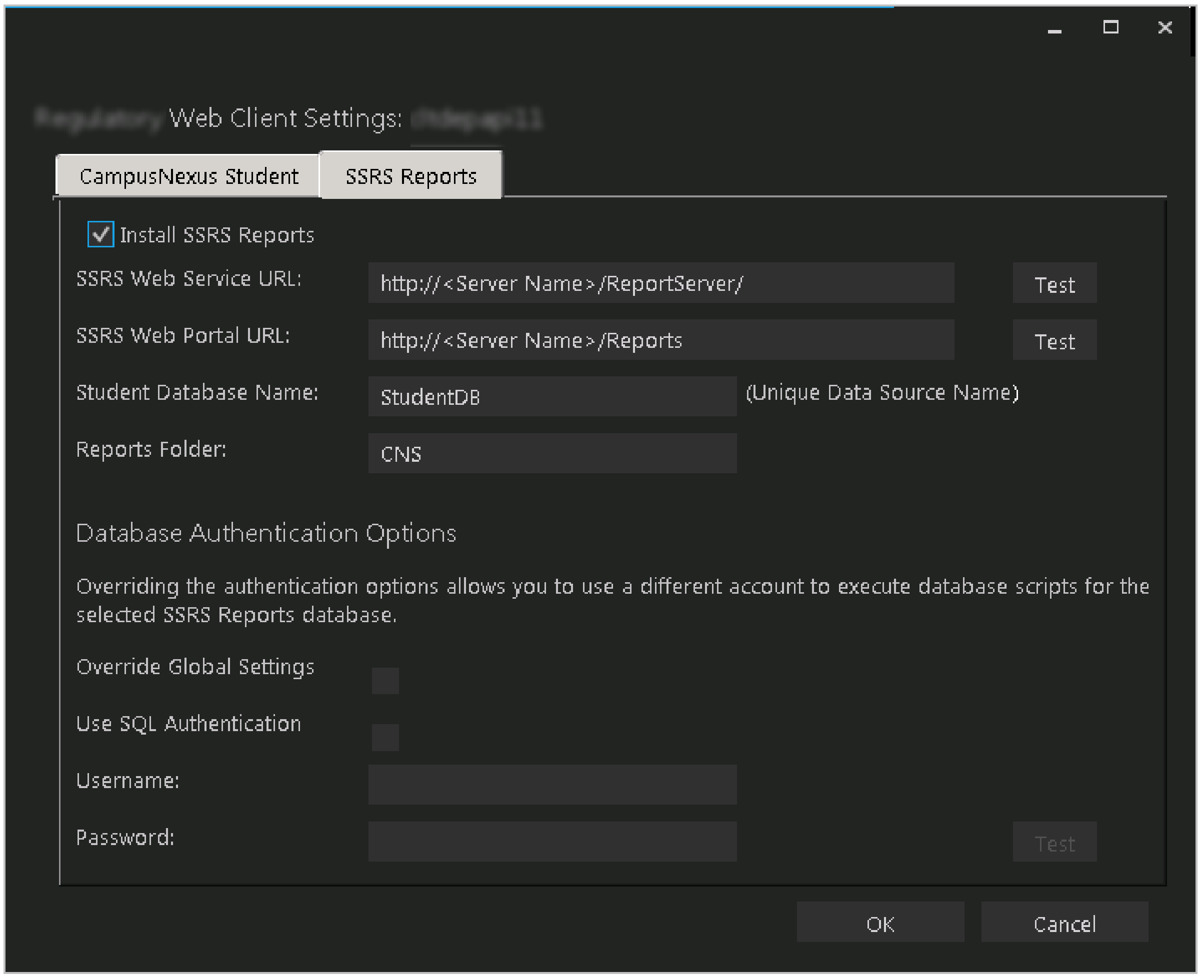
Anthology Student Tab Fields

Field	Description
Anthology Student Database Settings	
Database Server	Name of the SQL server on which the Anthology Student database resides.
SQL Server Port	Specify the port number of the SQL server or accept the default (1433).
Database Name	Name of the Anthology Student SQL database.

Field	Description
Test	Click **Test** to verify the database connection.
Install Database Updates	Select this check box to install updates to the Anthology Student database.

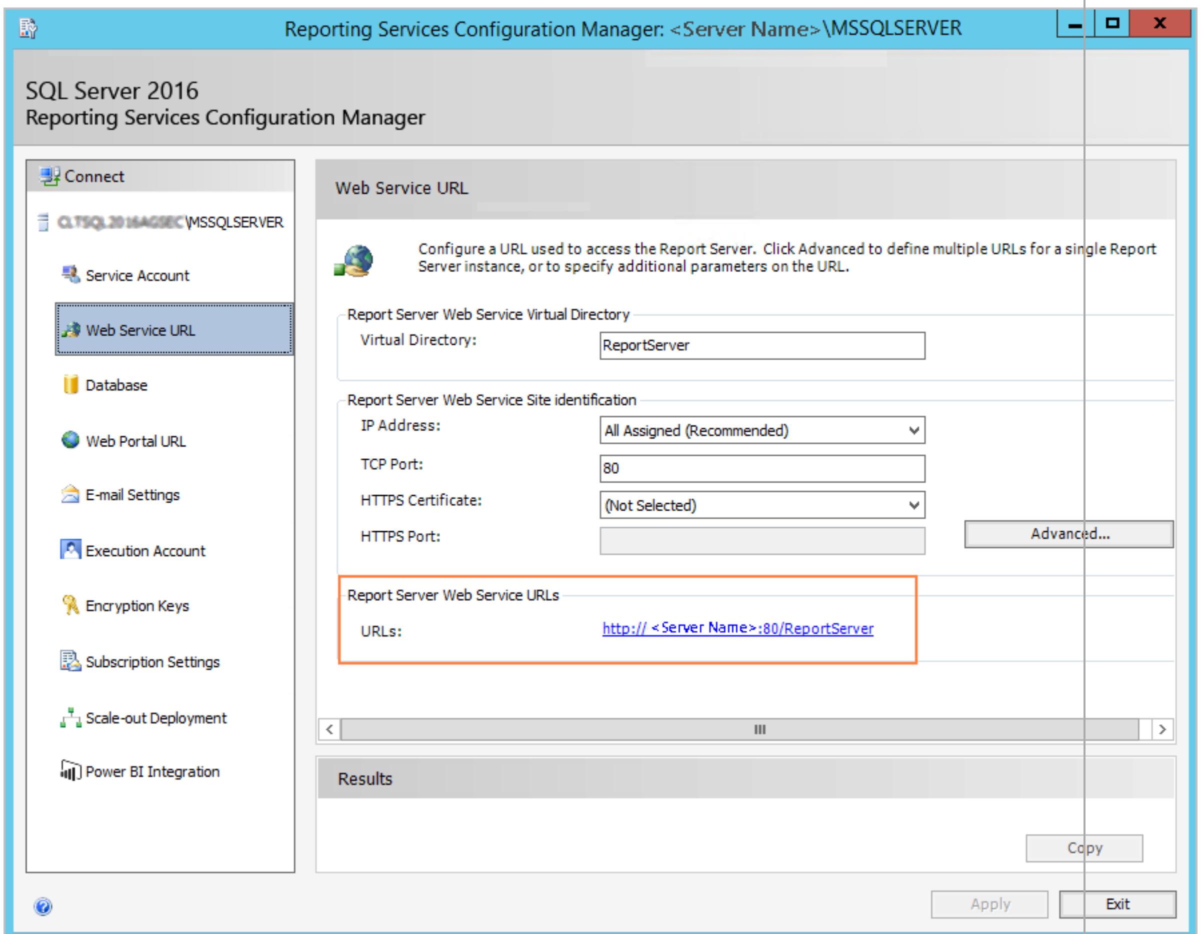
SSRS Reports Tab

Use this tab to integrate SQL Server Reporting Services (SSRS) 2016, the server-based report generating software system, into Regulatory. The SSRS URLs and the Reports Folder Root Path specified on this tab are stored in the web.config file.

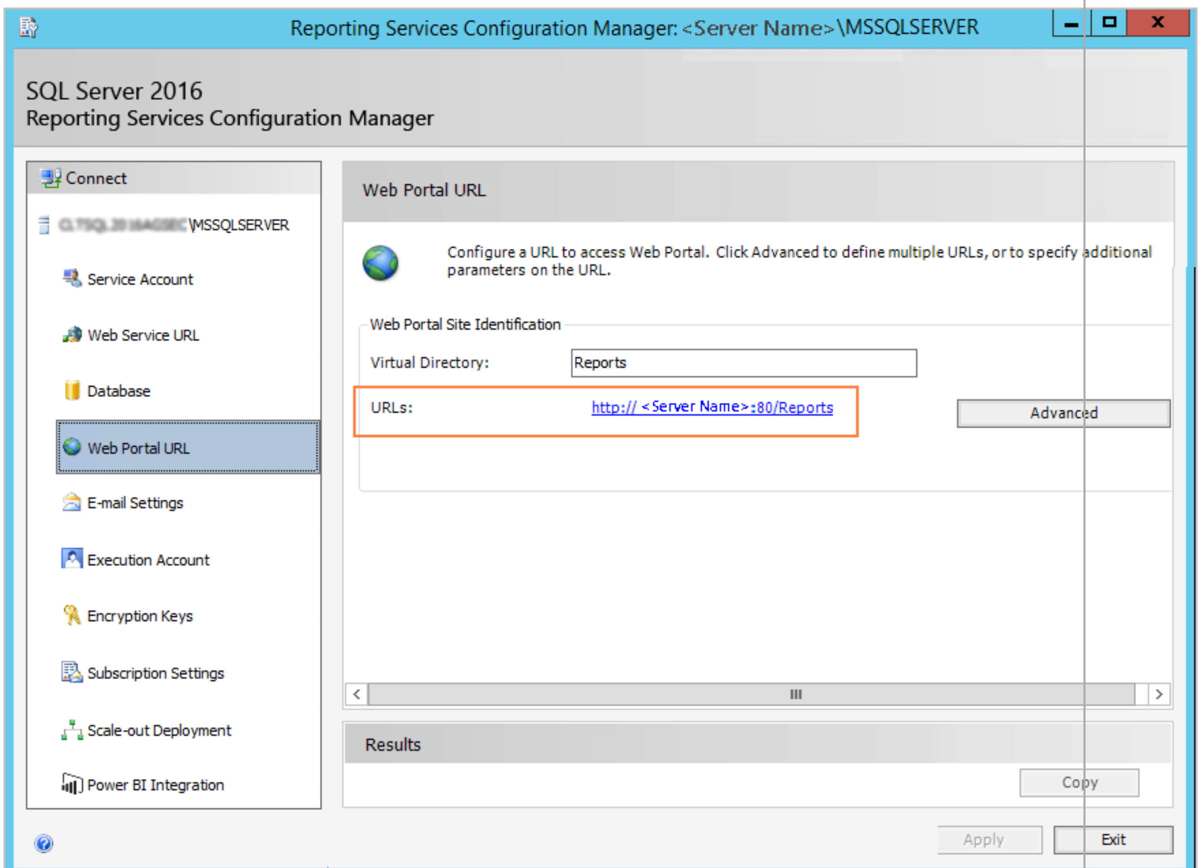


SSRS Reports Tab Fields

Field	Description
Install SSRS Reports	Select this check box to enable the fields on this tab.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Service URL</td><td>
Specify the Web Service URL configured to access the Report Server. The specified URL will be stored in the web.config file.
This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager.


</td></tr>
</table>

Field	Description
SSRS Web Portal URL	Specify the Web Portal URL configured to access the Web Portal. The specified URL will be stored in the web.config file. This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager page. 
Data Source Name	Specify the name of the Anthology Student database that is the source for the reports.
Reports Folder	Specify the path for the reports folder on the Report Server. A folder will be created if one does not exist. The folder name can be unique to the environment. The reports folder root path will be stored in the web.config file. *Example* `QA/CNS` where `QA` is one folder and `Student_Test` is a folder under `QA`.
Database Authentication Options	
Override Global Settings	Optional: Select this check box to enable the database authentication options.

Field	Description
Use SQL Authentication	Optional: Select this check box if SQL authentication is applied.
Username	Enter the user name of the account that is given override permissions for the SSRS reports database.
Password	Enter the password of the account that is given override permissions for the SSRS reports database.
Test	Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

In addition to the settings on the SSRS Reports tab in Installation Manager, the setup of reporting services requires configurations in the SQL Server Reporting Services Configuration Manager (see Configure Access to Reports).

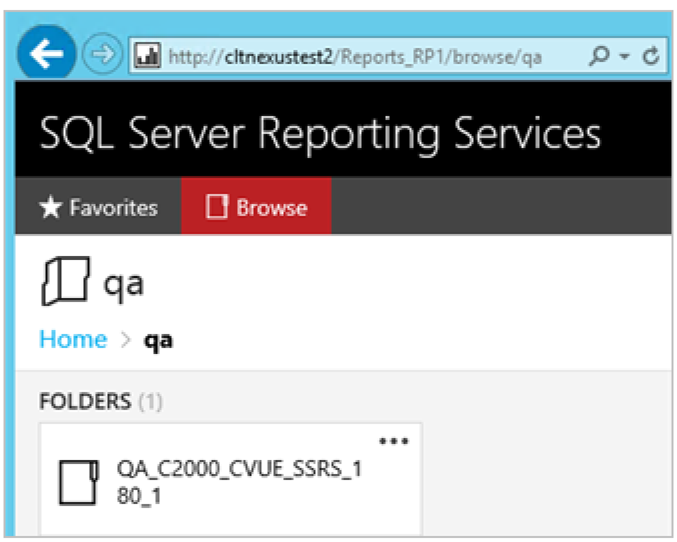
You also need to create folders in the Anthology Student and assign permissions using the Security Console. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Configure Access to Reports

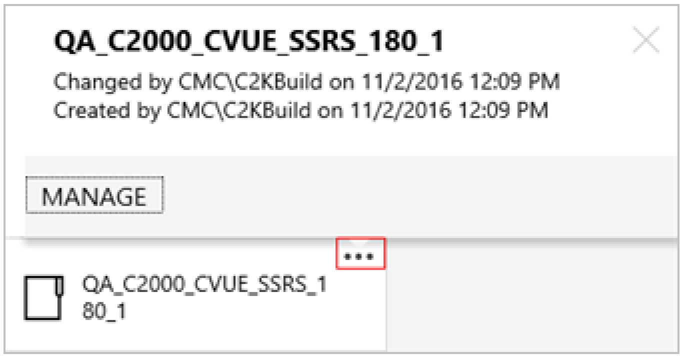
To enable access to the "Reports" menu item in Anthology Student, perform the following steps in the Reporting Services Configuration Manager on the report server:

a. Navigate to the /Reports folder path.

   In the example below the reports folder path is `http://cltnexustest2/Reports_RP1/browse/`**qa**.



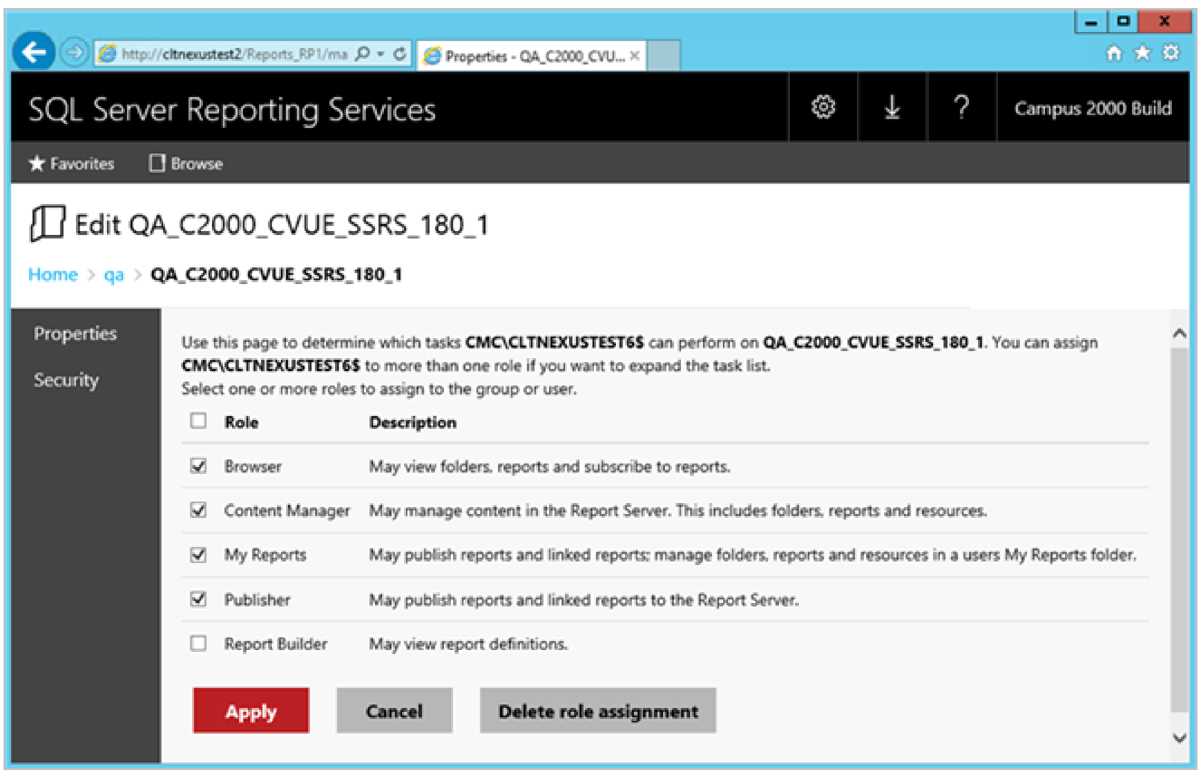
b. Right-click on the ellipsis of the reports folder root and select **Manage**.



c. Select the **Security** tab, click **Customize security**, and click **Add group or user**.

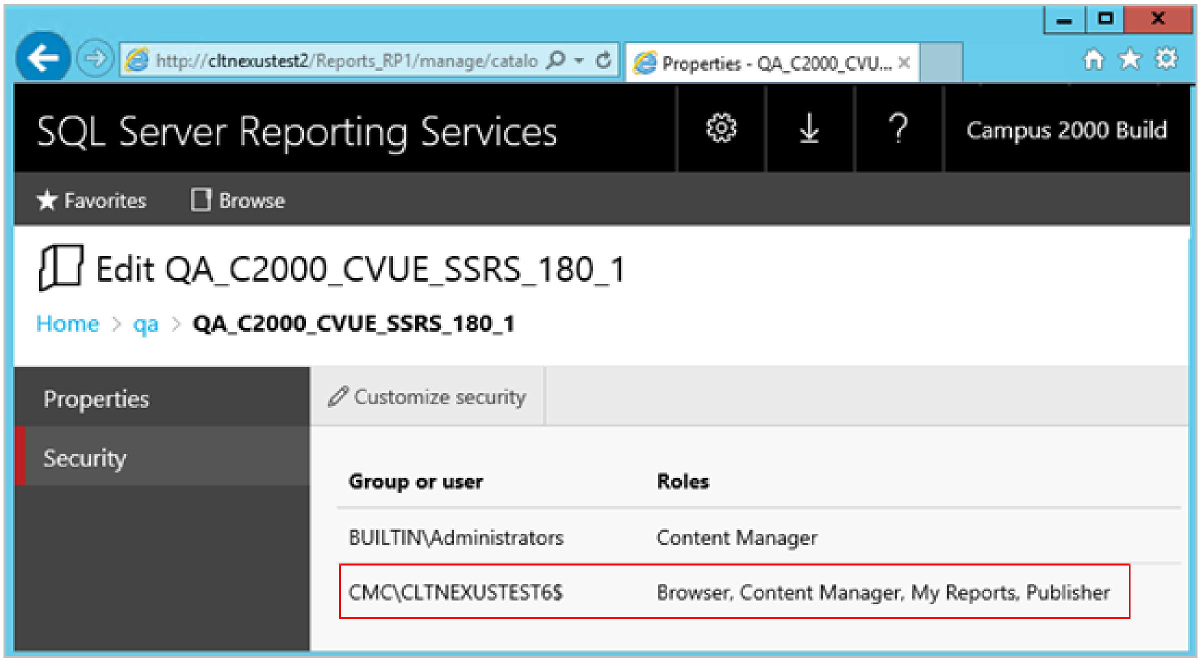
d. Add the **domain\<machine name$>** of Anthology Student and select the following **Roles**:

- Browser
- Content Manager
- My Reports
- Publisher



e. Click **Apply**.

Security for the Reporting Service should be set up as shown below, where CMC\CLTNEXUSTEST6 is the domain\machine name of Anthology Student from which the reports are accessed.



Configure SSRS for HTTPS

Once the reporting services are installed and configured, test access to the reports in Anthology Student. Select the Reports tile and navigate to any report listed in the menu.

If Anthology Student displays only the title of the report (without any data selection fields), use the browser developer tools (**F12**) and check the **Console** tab. If an error similar to the following is displayed, configure SSRS for secure access with an SSL certificate. For detailed instructions, see https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-ssl-connections-on-a-native-mode-report-server

```
⚠ Mixed Content: The page at 'https://googlesamples.github.io/web-      jquery.js:5562
fundamentals/samples/discovery-and-distribution/avoid-mixed-content/image-gallery-
example.html' was loaded over HTTPS, but requested an insecure image
'http://googlesamples.github.io/web-fundamentals/samples/discovery-and-
distribution/avoid-mixed-content/puppy.jpg'. This content should also be served
over HTTPS.
```

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click ✖ to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

   The Test button checks the connectivity of the Admin user to the machine specified in the Server name field.

10. If all tests pass, click ➔.

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

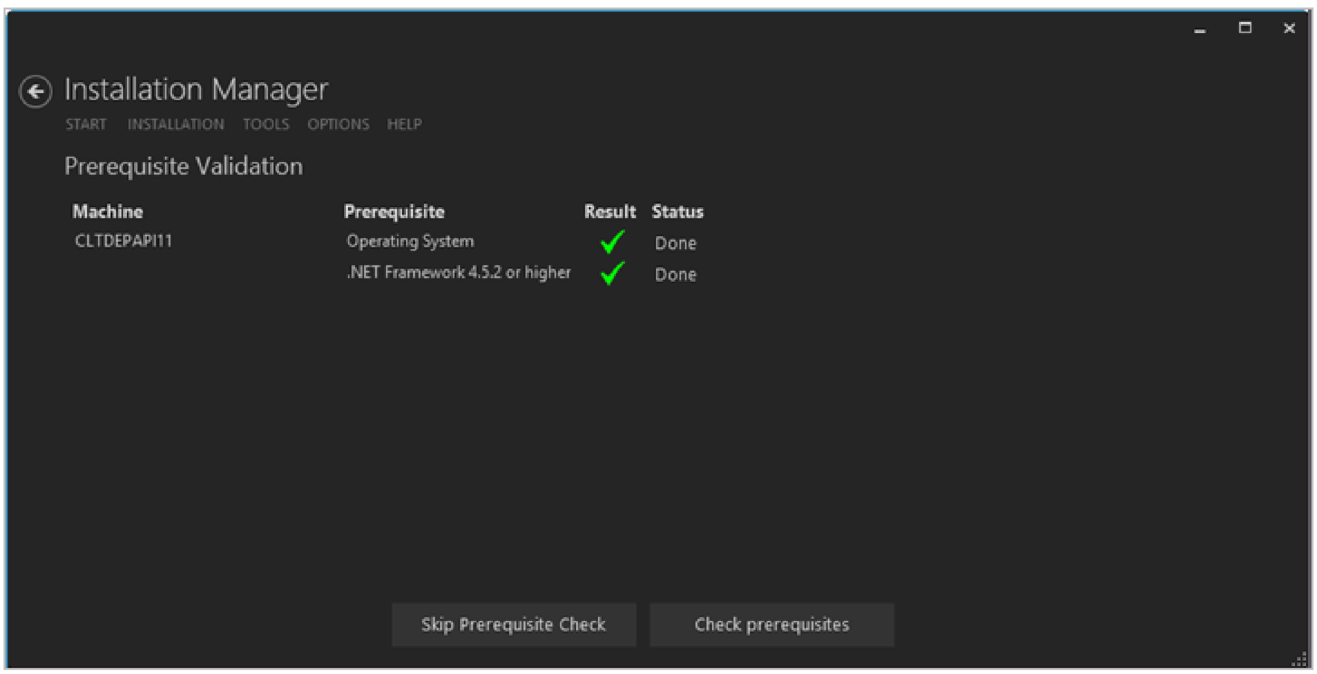
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

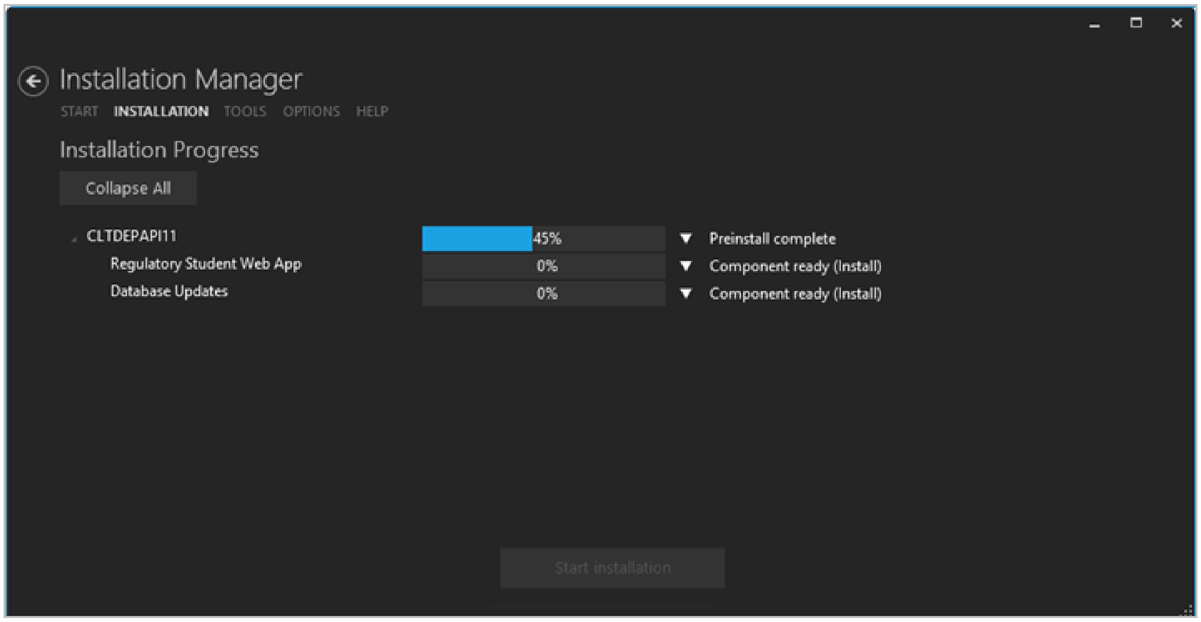
    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.
4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.



Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

Regulatory Legacy Interface

Note: The Anthology Student product interface previously called the "desktop client" is now referred to as the "legacy interface". The product interface previously called the "web client" is now the standard, default product interface and is referred to as the "Student Web App".

Regulatory can be selected during the initial Anthology Student installation, or it can be added to an existing Anthology Student system.

To add Regulatory to an existing Anthology Student system, use Package Manager to download the Regulatory installation files, click the Regulatory tile on the Start screen, and proceed with the installation screens.

Global Settings

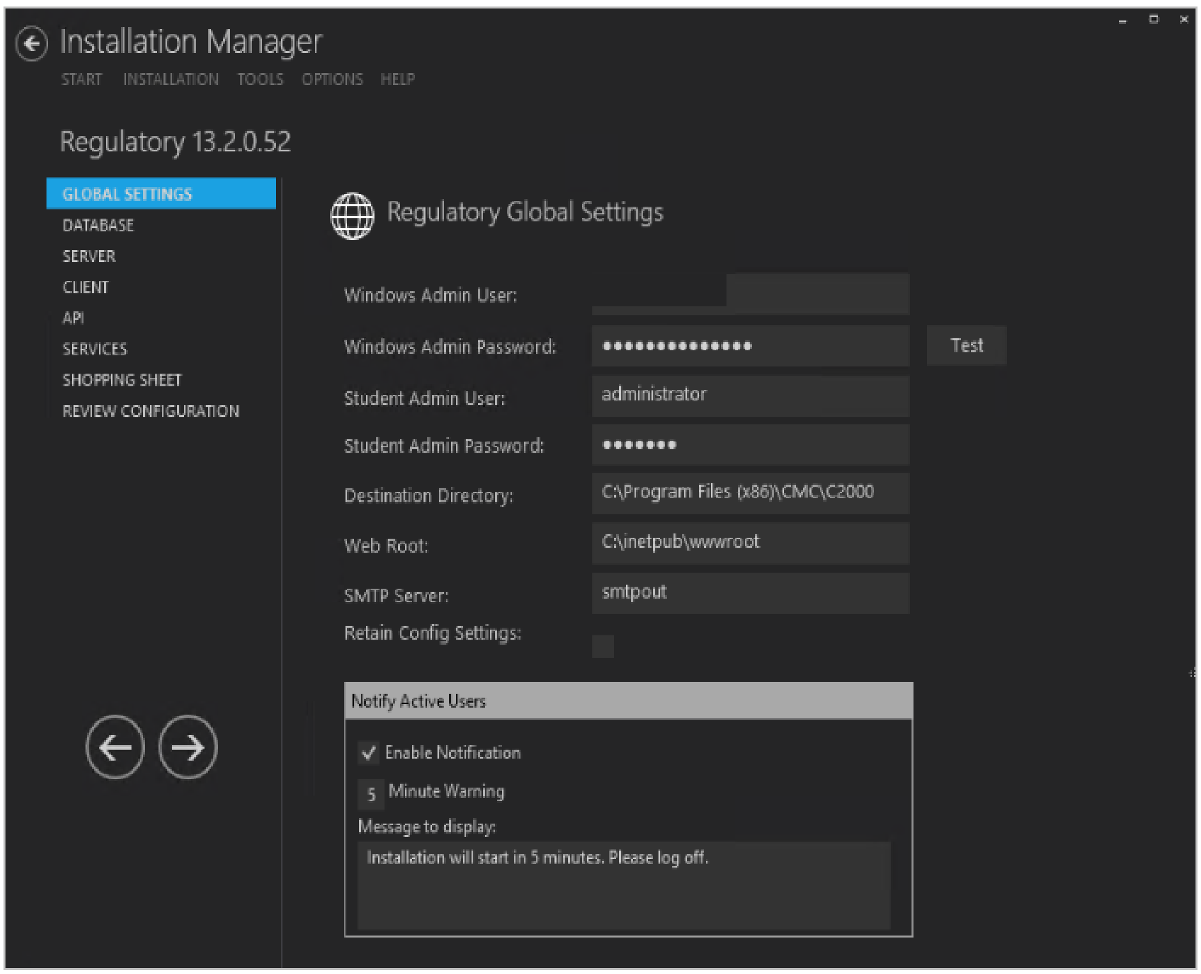
The Global Settings screen contains the Windows Admin user name password used when starting an installation of Regulatory for Anthology Student. Users can also test this information without moving from the screen.

Note: The Global Settings screen for Anthology Student indicates the versions of Financial Aid Automation and Regulatory that are compatible with Anthology Student. Financial Aid Automation and Regulatory can be installed with Anthology Student (see Services for Anthology Student) or added later.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Regulatory** tile. The Global Settings screen is displayed.



2. Complete the fields on the Global Settings screen as described in the table below.

Regulatory Global Settings Fields

Field	Description
Windows Admin User	Specify the user name of the user with administrator permissions on the computer where the COM, Windows, and Web Services will run. This account must have administrative access to all the machines being installed to. It must be a sysadmin on the database as integrated security is the only option that will be used. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Windows Admin Password	Specify the password for the Administrator user name. This password is used in the background for other installation steps. **Note**: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.
Student Admin User	Specify the user name of the Anthology Student user with administrator permissions. This is the Anthology Student administrator account that the Windows and Web Services use for Anthology Student access. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Student Admin Password	Specify the password for the Anthology Student Admin User.
Destination Directory	The default directory for the legacy interface (desktop client) of Anthology Student and server is C:\Program Files (x86)\CMC\C2000. You can override the default by choosing another path.
Web Root	The default web root for the APIs to be installed is C:\inetpub\wwwroot. You can override the default by choosing another path.

Field	Description
SMTP Server	Enter the Email (SMTP) Server address used for sending out email notifications by doing the following: a. Determine the desired Email (SMTP) Server IP address and DNS names. b. On the Exchange Server, an entry for an open relay on TCP Port 25 must be allowed and open to receive SMTP traffic from the MTS Server. This traffic must not be routed through a firewall. OSI Layer 7 firewalls can interfere with the service. c. Ping the Email (SMTP) Server from the MTS Server and the SQL Server. d. Telnet to the Email (SMTP) Server on Port 25 and verify successful connection from the MTS Server. e. Enter the IP address in the SMTP Server field.
Retain Config Settings	Select the Retain Config Settings check box if you want to deploy the latest web.config file and also run a config merge that will merge any settings that were set outside of the install process. If Retain Config Setting is not selected, the install process will not retain and will not merge any configuration settings that were set outside of install process.
Notify Active Users	
Enable Notification	Select this check box to enable notification of active Anthology Student users when an installation is about to begin.
Minute Warning	Specify the notification time, that is, the number of minutes until the installation starts.
Message to display	Enter the message to be displayed in the notification window.

3. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

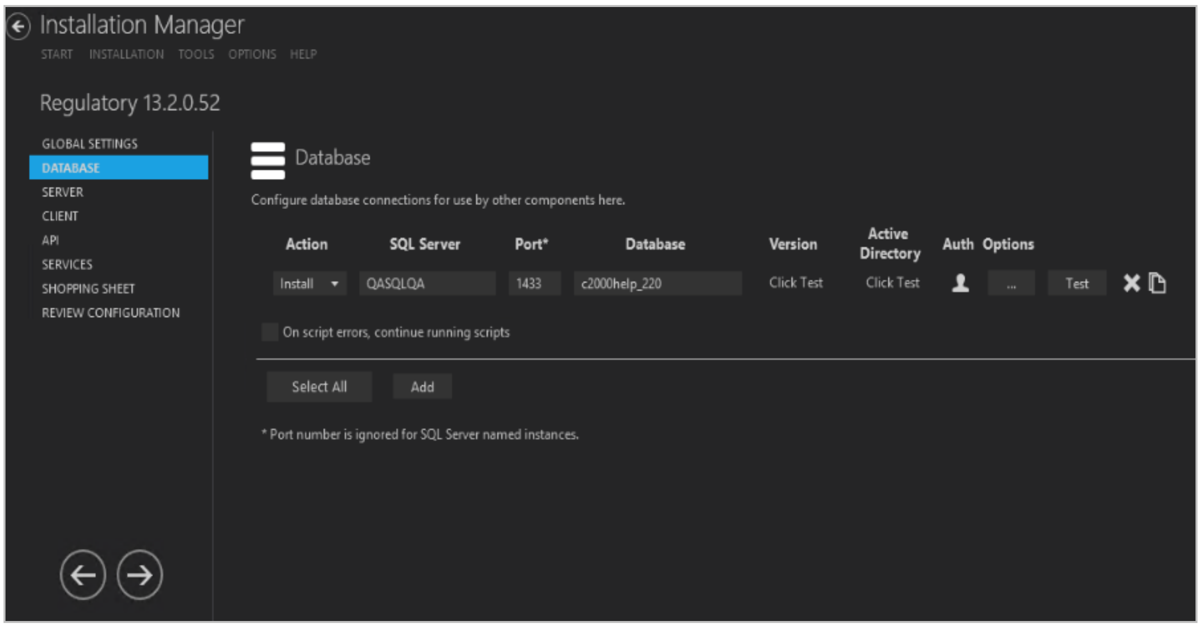
4. If the user is authenticated, click **OK** and click  to continue.

Database

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install) and to specify the machine name, the Anthology Student database, and additional databases for Portal and Talisma Fundraising.

Set Up the Database

1. In the Installation menu, click **Database**. The Database screen for Regulatory is displayed.

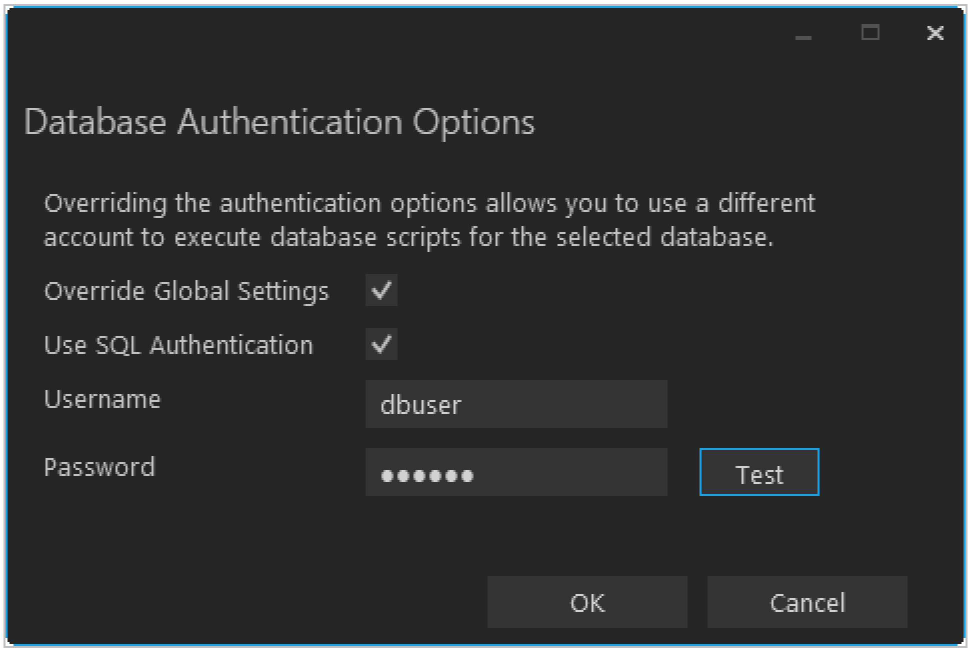


2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the name of the **SQL Server** where the Anthology Student database is installed.
5. Specify the **Port** number for the SQL Server or accept the default (1433).

   Note: The port number is ignored for named instances of SQL Server.
6. Specify the name of the **Database** for Anthology Student. The database name must be unique — 'master' is not allowed.

7. The **Version** field is populated when you click the **Test** button.
8. The **Active Directory** field is populated when you click the **Test** button.
9. Click  in the **Auth** column if you want to override the authentication options from Global Settings for the selected database, for example, to give another user permissions to execute scripts for the selected database. The Database Authentication Options form is displayed.



   a. Select the **Override Global Settings** check box to enable the fields on the form.
   b. Optional: Select the **Use SQL Authentication** check box if SQL authentication is applied.

      The license checks, version number check, SQL script execution, student admin role check, and MSI parameters will use SQL authentication if selected.
   c. Enter the **Username** and **Password** of the account that is given the override permissions for the selected database.

      The Test buttons in the Options form and in the Database screen will use these credentials if selected.
   d. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
   e. Click **OK** to save changes on the Options form. The form is closed.
10. Select the check box for **On script errors, continue running scripts** if you want the installation process to continue regardless of errors encountered.

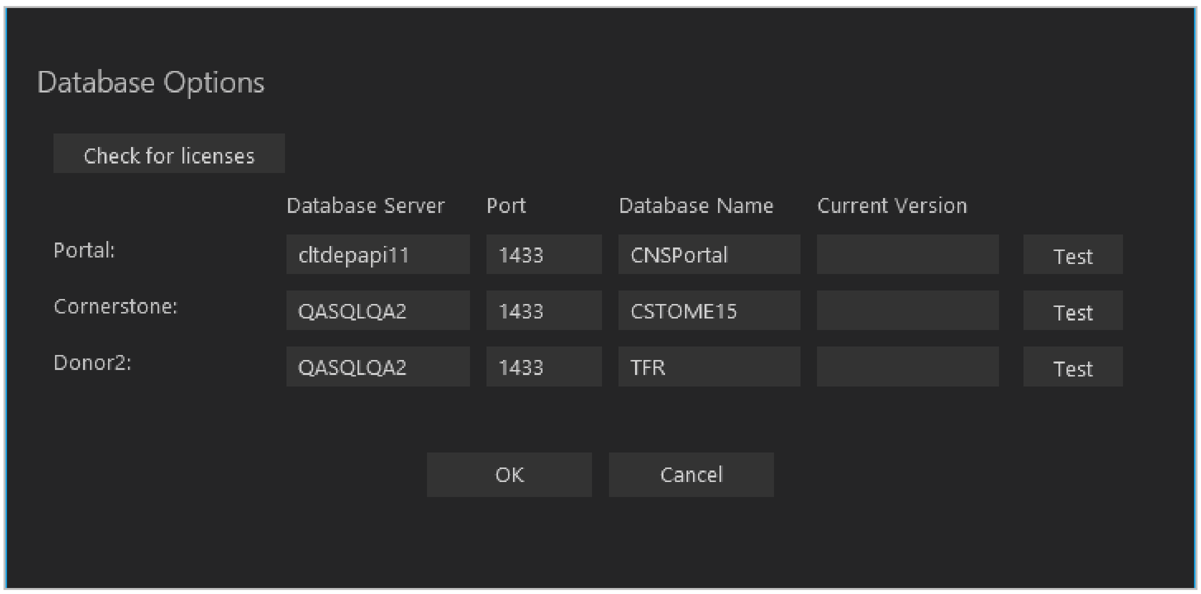
By default, database upgrades will stop if the script encounters any errors. This selection is used if there are custom modifications to the database that are known to cause errors in the upgrade scripts. Selecting this option enables all scripts to be run against the specified database.

Whether the check box is selected or not, any errors are written to a separate error file for each script, which may be investigated after the script execution. Error logs are stored in the following folder: `DatabaseServer\C:\Logs\Output`.

The error log is the name of the script, SQL Server, and database name appended with `_Errors.txt`, for example,
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Errors.txt`)

There is also an output file that has all of the script output:
`CampusVue_17.1.00xx_{SQL Server}_{database_name}_Output.txt`

11. Click  to view and edit the Options form.



The Options form is used to specify databases for Portal and Talisma Fundraising. Corresponding licenses are required.

- Entering a Portal database is only necessary for an installation that includes the e-Learning component that has a Portal component and license key associated with Anthology Student.
- The Cornerstone and Donor2 databases are used for Talisma Fundraising in conjunction with the primary Anthology Student database. Installation Manager detects if Talisma Fundraising is enabled in the Anthology Student database.

Regulatory Database Options Fields

Field	Description
Check for Licenses	This button queries the Anthology Student database and checks for product licenses. Based on the licenses found, Installation Manager enables the Portal, Cornerstone, and Donor2 fields. If the licenses are not found, the Licensed? field indicates "False" and the fields remain disabled.
Portal	
Database Server	Name of the SQL server on which the Portal database resides.
Port	Specify the port number for the Portal database or accept the default (1433).
Database Name	Name of the Portal SQL database.
Current Version	This field is populated when you click the **Test** button.
Cornerstone	
Database Server	Name of the SQL Server on which the Cornerstone database resides.
Port	Specify the port number for the Cornerstone database or accept the default (1433).
Database Name	Name of the Cornerstone SQL database.
Current Version	This field is populated when you click the **Test** button.
Donor2	
Database Server	Name of the SQL Server on which the Donor2 database resides.
Port	Specify the port number for the Donor2 database or accept the default (1433).
Database Name	Name of the Donor2 SQL database.
Current Version	This field is populated when you click the **Test** button.

12. Click **OK** to save changes on the Options form. The form is closed.
13. Click to copy a line. Edit the copied line as needed.
14. Click to delete a selected line.
15. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Note: The Test button operates as follows:

    - Queries the database to get the latest version of Anthology Student and populates the current version field.
    - Uses Windows Admin credentials (see Global Settings) and tests connectivity to the SQL server.

- Uses the Student Admin user name (see Global Settings) and checks if it exists in the Anthology Student database.

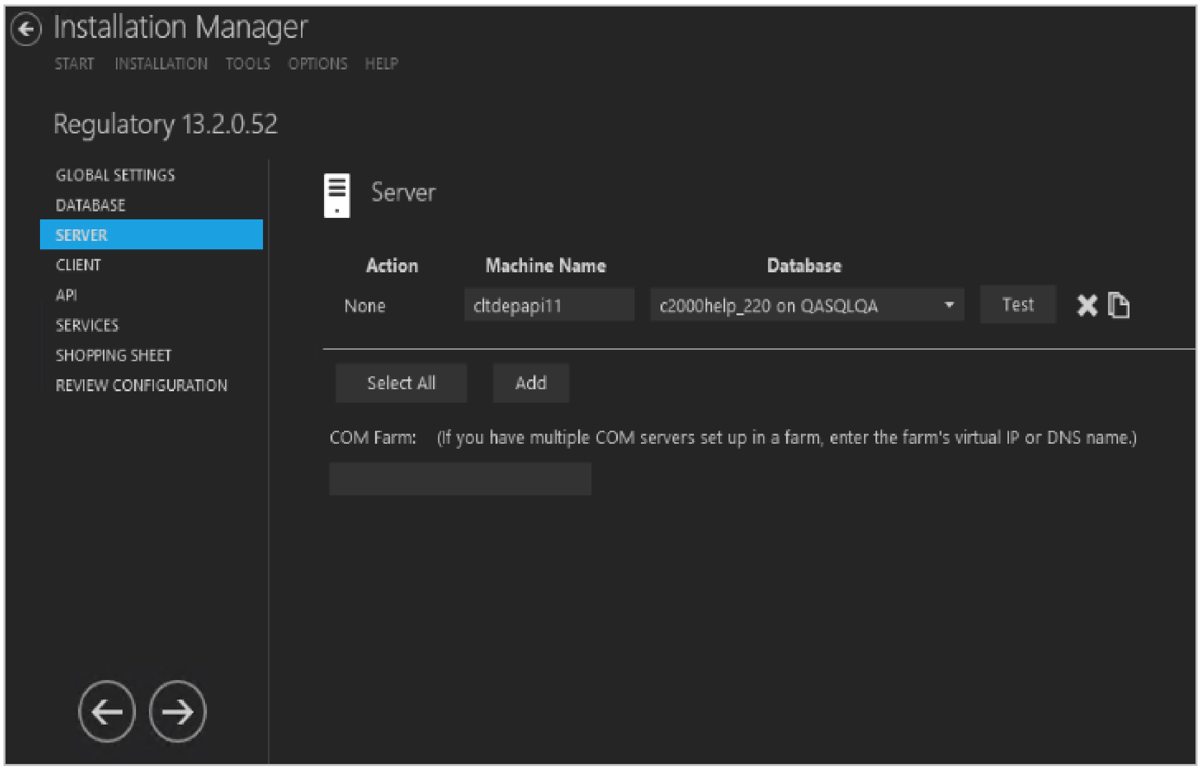
16. If all tests pass, click .

Server

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and database connection of the COM Server for Regulatory.

Set Up the Server

1. In the Installation menu, click **Server**. The Server screen for Regulatory is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the COM server for Anthology Student will be installed.
5. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.

   Notes:

- Only one Server can be installed against one database.
- Multiple Servers can be installed against different databases.

6. Click to copy a line. Edit the copied line as needed.
7. In the **COM Farm** field, enter the farm's virtual IP address or DNS name if you have multiple COM servers set up in a server farm with a load-balancing system.
8. Click to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

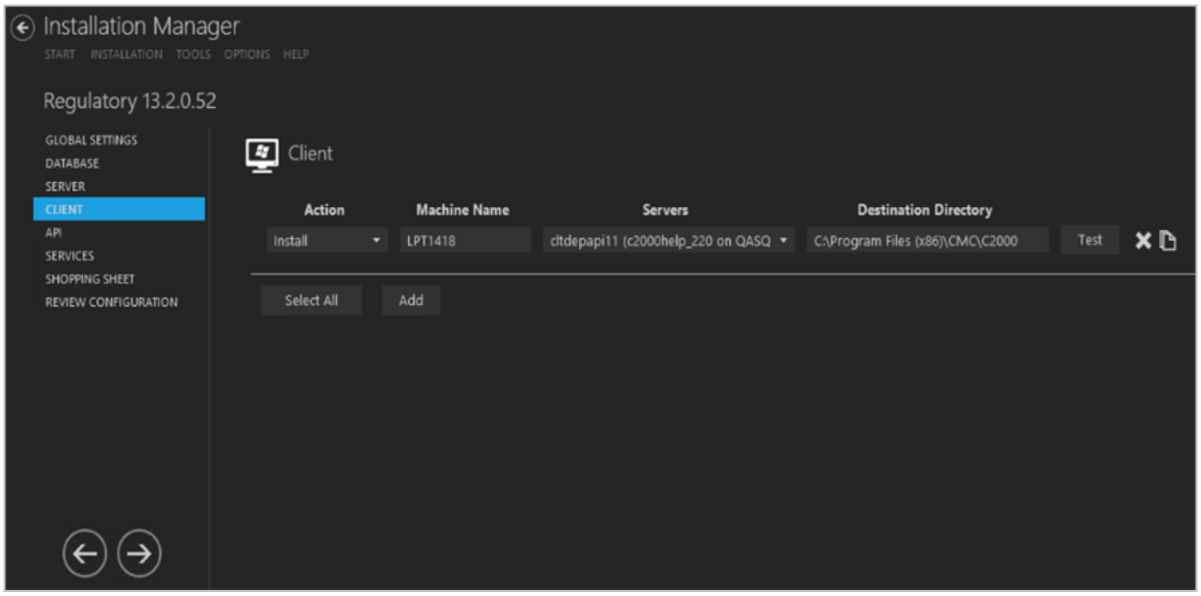
   Note: The Test buttons uses the Windows Admin credentials (see Global Settings) to test connectivity to the machine specified in the Machine Name field on the Server screen (this screen).
10. If all tests pass, click .

Client

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name of the legacy interface (desktop client) for Regulatory.

Set Up the Client

1. In the Installation menu, click **Client**. The Client screen for Regulatory is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed. This is the machine where the desktop client for Anthology Student will be installed.

5. Select the name of a **Server**. The drop-down list contains the servers and Anthology Student databases configured in the Database settings screen.

   Note: Multiple Clients can be installed against one server.

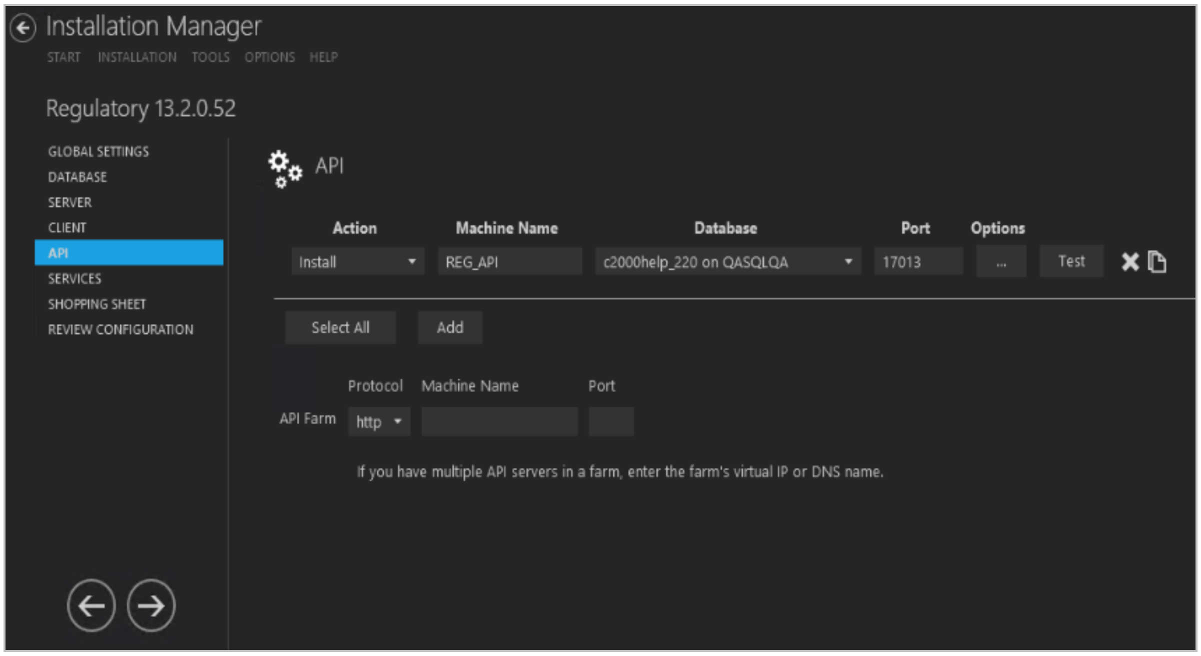
6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.
7. Click  to copy a line. Edit the copied line as needed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

API

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database server, and port to be used by the Web Services (APIs) for Regulatory.

Set Up the APIs

1. In the Installation menu, click **API**. The API screen for Regulatory is displayed.



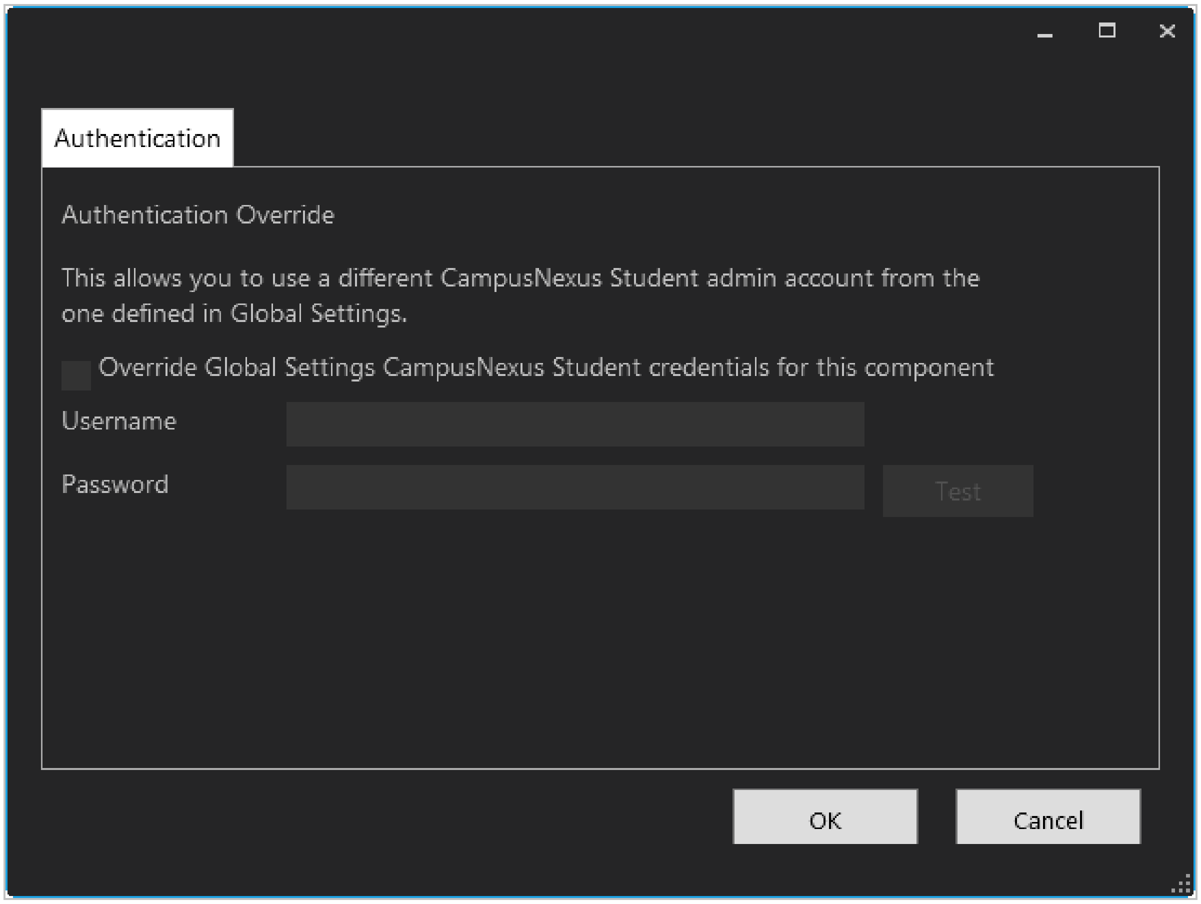
2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This is the machine where the APIs for Anthology Student will be installed.

5. In the **Database** field, select a database for Regulatory. The drop-down contains a list of databases configured in the Database settings screen.

6. In the **Port** field, enter the name of the port where the Web Services will be installed.

7. Click ... to view and edit the Options form. The Authentication Override form is displayed.



   a. Select the check box **Override Global Settings Anthology Student credentials for this component** to enable the fields on the form.

   b. Enter the **Username** and **Password** of the Anthology Student account for the selected machine.

   c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

   d. Click **OK** to save changes on the Options form. The form is closed.

8. Click to copy a line. Edit the copied line as needed.

9. Click to delete a selected line.

10. If multiple API servers are installed in a server farm:

   a. Select the **Protocol** (http or https).
   b. Enter the farm's virtual IP address or DNS name in the **Machine Name** field.
   c. Specify the **Port** number.

11. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Notes:

    - The Test button checks if the port number is in use; if so, the user is prompted to enter a different port number.
    - If an upgrade is performed, Installation Manager first checks if the port number is in use by the same Web Service that’s being installed.

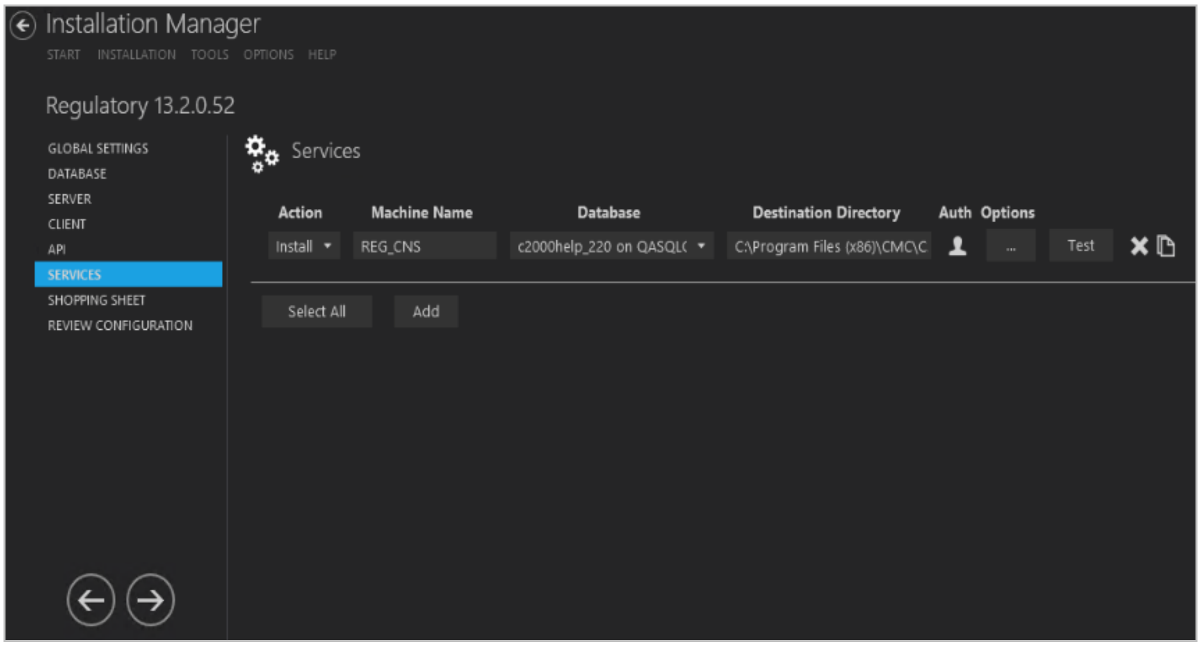
12. If all tests pass, click .

Services

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, type, database, and options for the Regulatory Service.

Set Up the Services

1. In the Installation menu, click **Services**. The Services screen for Regulatory is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

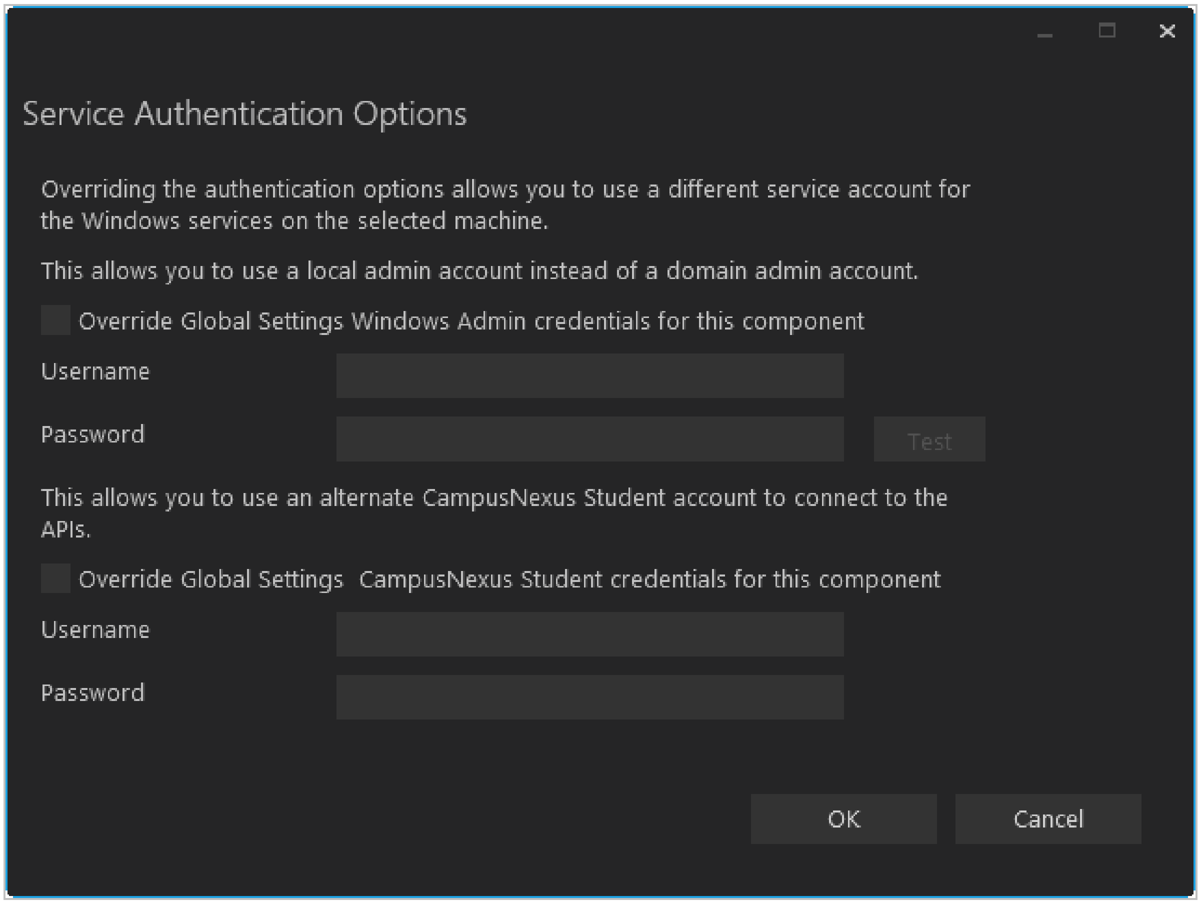
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.

5. Select the name of a **Database** for Anthology Student. The drop-down list contains all the Anthology Student databases configured in the Database settings screen.

6. Specify the **Destination Directory** if you want to override the default directory set on the Global Settings screen.

7. Click in the **Auth** column if you want to override the authentication options from Global Settings to use a different account for the Windows services and alternate Anthology Student credentials on the selected machine. The Service Authentication Options form is displayed.



   a. Select the check box **Override Global Settings Windows Admin credentials for this component** to enable the associated fields on the form. This option allows you to use a local admin account instead of the domain admin account.

   b. Enter the **Username** and **Password** of the local admin account for the selected machine.

   c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

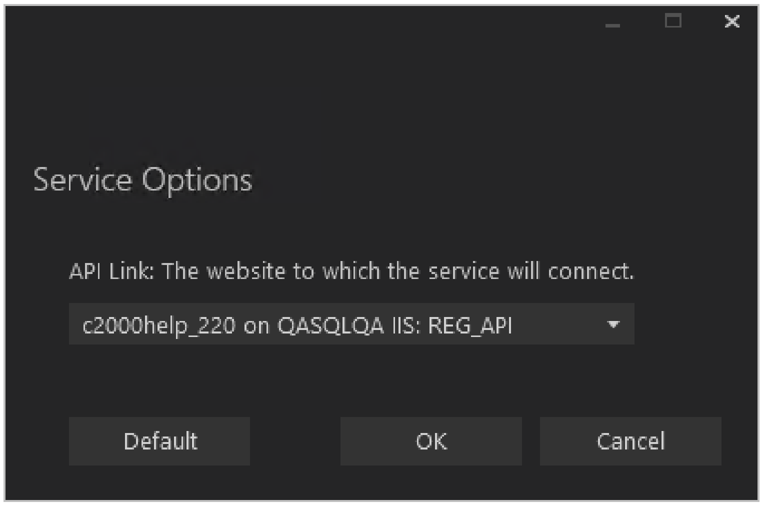
   d. Select the check box **Override Global Settings Anthology Student credentials for this component**.

   e. Enter the **Username** and **Password** of Anthology Student account for the selected machine.

f. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

g. Click **OK** to save changes on the Options form. The form is closed.

8. Click to view and edit the Options form.



In the Service Options window, select the database and installed system to be used by the Regulatory Web Service (API).

— OR —

Click **Default** to use the API server based on the database selected.

9. Click **OK** to save changes on the Options form. The form is closed.

10. Click to copy a line. Edit the copied line as needed.

11. Click to delete a selected line.

12. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

13. If all tests pass, click .

Shopping Sheet

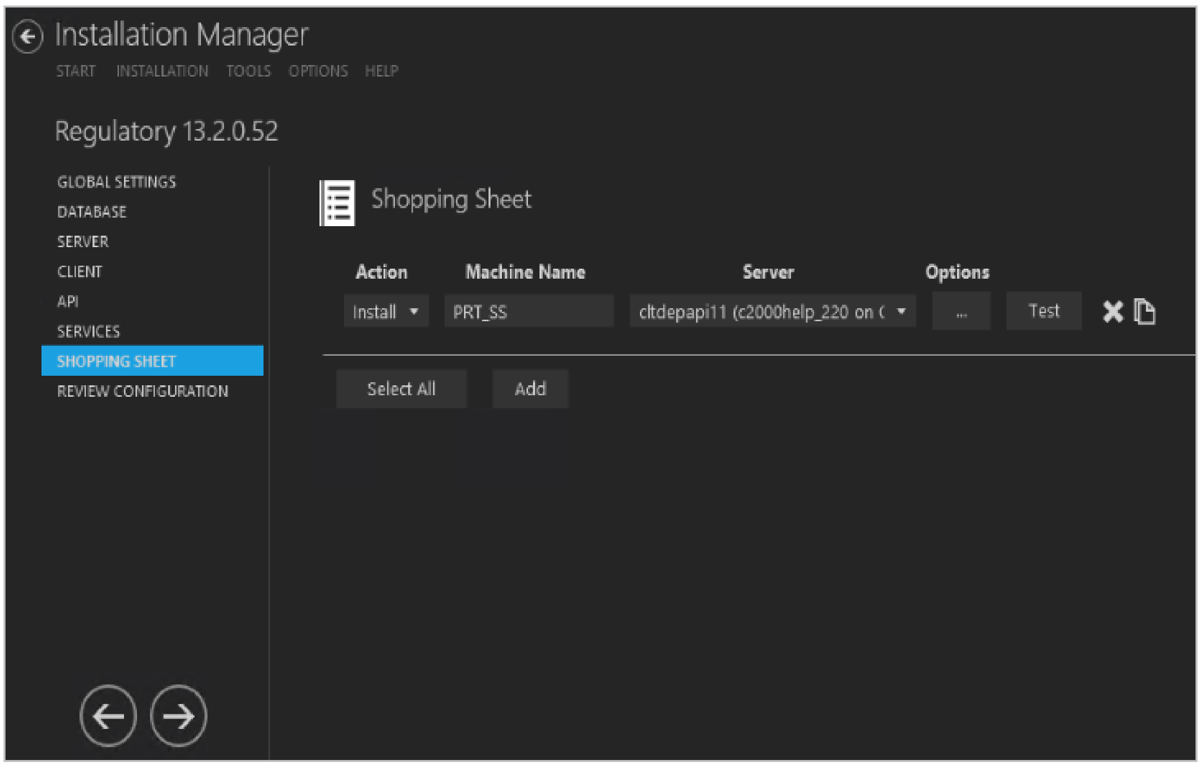
This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name, database, and options of the financial aid Shopping Sheet for Regulatory.

> ⚠ Shopping Sheet is typically installed on the Portal server.

In award year 2020-2021 and later, the Shopping Sheet is also referred to as the College Finance Plan.

Set Up the Shopping Sheet

1. In the Installation menu, click **Shopping Sheet**. The Shopping Sheet screen for Regulatory is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

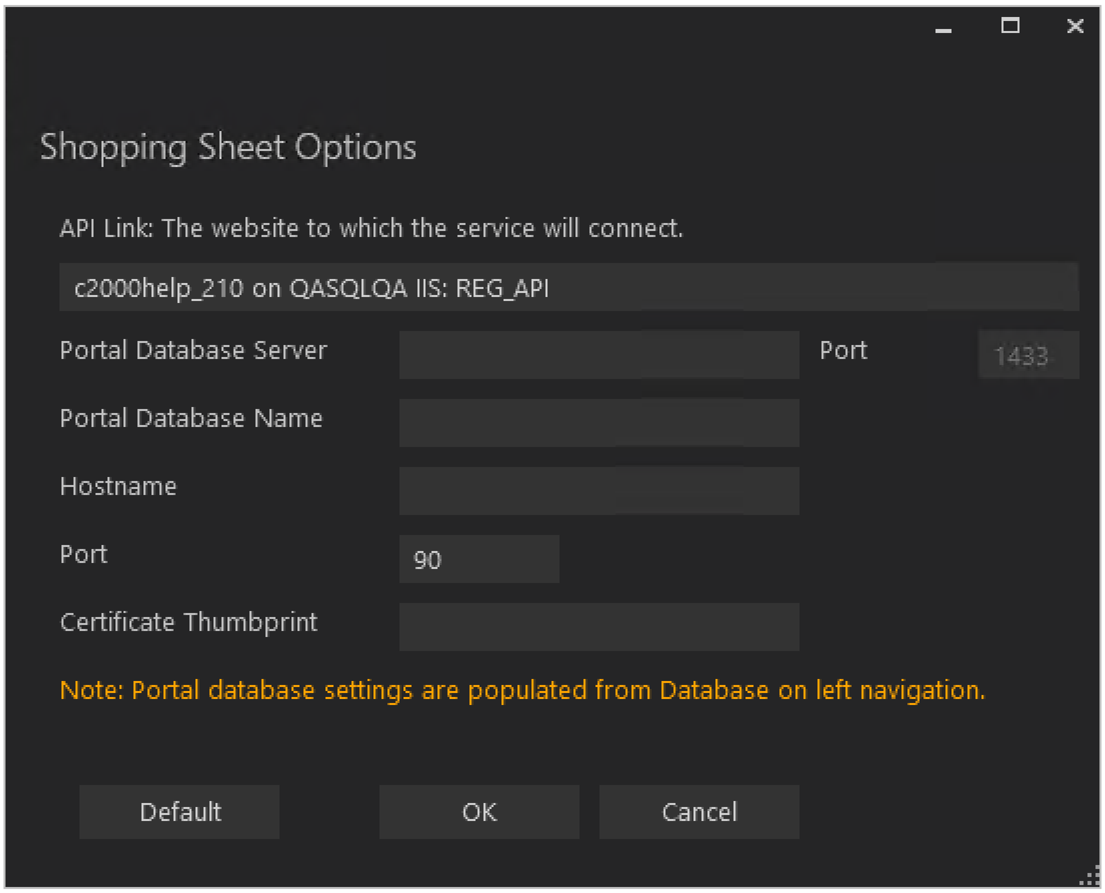
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Select the name of a **Server**. The drop-down list contains the servers and Anthology Student databases configured in the Database settings screen.

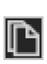
   Note: Multiple clients can be installed against one server.

6. Click ... to view and edit the Options form.



Shopping Sheet Options Fields

Field	Description
API Link	Select the database and installed system to be used by the Shopping Sheet component. – OR – Click **Default** to use the API server based on the database selected.
Portal Database Server	Specify the name of the SQL server on which the Portal database resides.
Port	Specify the port number for the Portal or accept the default (1433).
Portal Database Name	Specify the name of the Portal database.
Hostname	Specify the hostname for the Portal URL. It will be added to the IIS bindings of main Portal instance.
Port Number	Specify the port number used by the Portal or accept the default (00).
Certificate Thumbprint	The certificate thumbprint from IIS is required for HTTPS connections. Copy and paste the thumbprint from Portal into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to copy a line. Edit the copied line as needed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

Review the Configuration and Start Installation

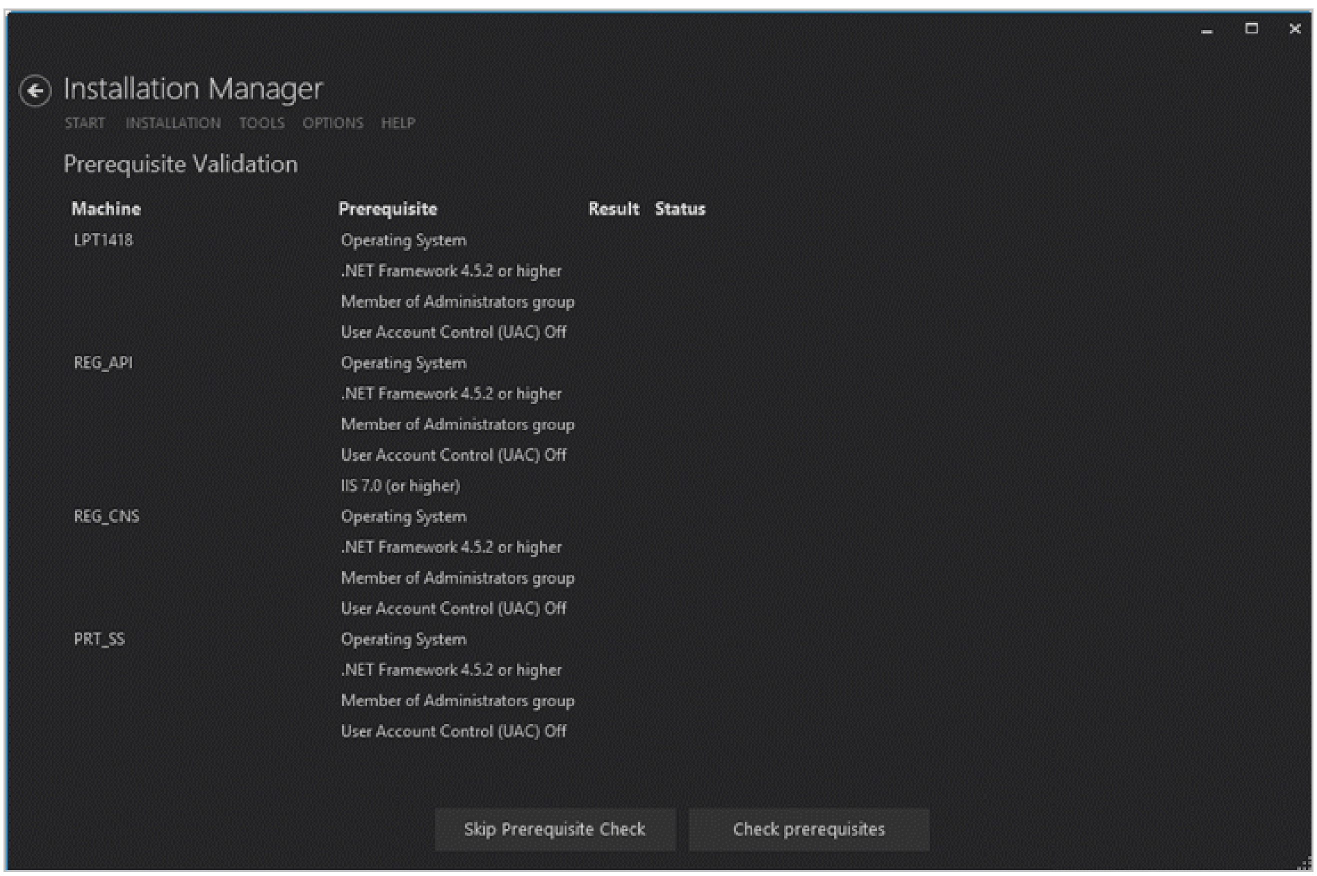
1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.

2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

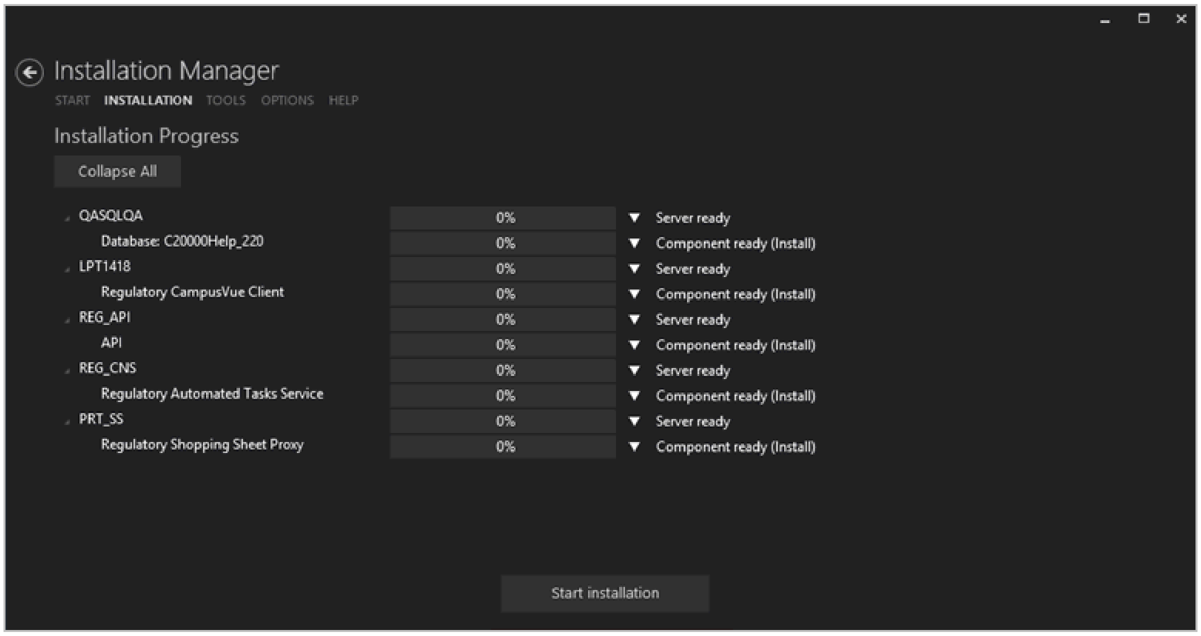
    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.

Click **Expand All** and scroll through the list of items. Or, click **Collapse All** and then click to expand a section.



4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

Regulatory 1098-T Processing Utility

The Regulatory 1098-T Processing Utility gathers 1098-T tax reporting data configured, collected, and stored in the Anthology Student database. Institutions must provide 1098-T forms to students or parents of dependent students each year by January 31 so that eligible students and families can receive educational tax credits. 1098-T forms contain information used by the Federal Government to calculate these credits. The 1098-T processing utility determines which students need to be reported on the 1098-T form.

To add the Regulatory 1098-T Processing Utility to an existing Anthology Student system, download the installation files using Package Manager, click the Regulatory 1098-T Processing Utility tile on the Start screen, and proceed with the installation screens.

The functionality of the 1098-T Processing Utility has been migrated to the standard interface (web client) for Anthology Student 20.0.2 or higher. For the tax reporting year 2019 and 2020, you can use either the stand-alone 1098-T Processing Utility client, the standard interface of Anthology Student, or both.

To add the 1098-T functionality to Anthology Student, complete Regulatory 1098-T Web App install screen. To view the 1098-T utility forms once the installation is complete, in Anthology Student navigate to **Processes > IRS 1098-T**.

Prerequisites

The installation prerequisites for the Regulatory1098-T Processing Utility must match the installed Anthology Student system.

To use the 1098-T functionality via the Student Web App, customers must be on Anthology Student 20.0.2 or higher.

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

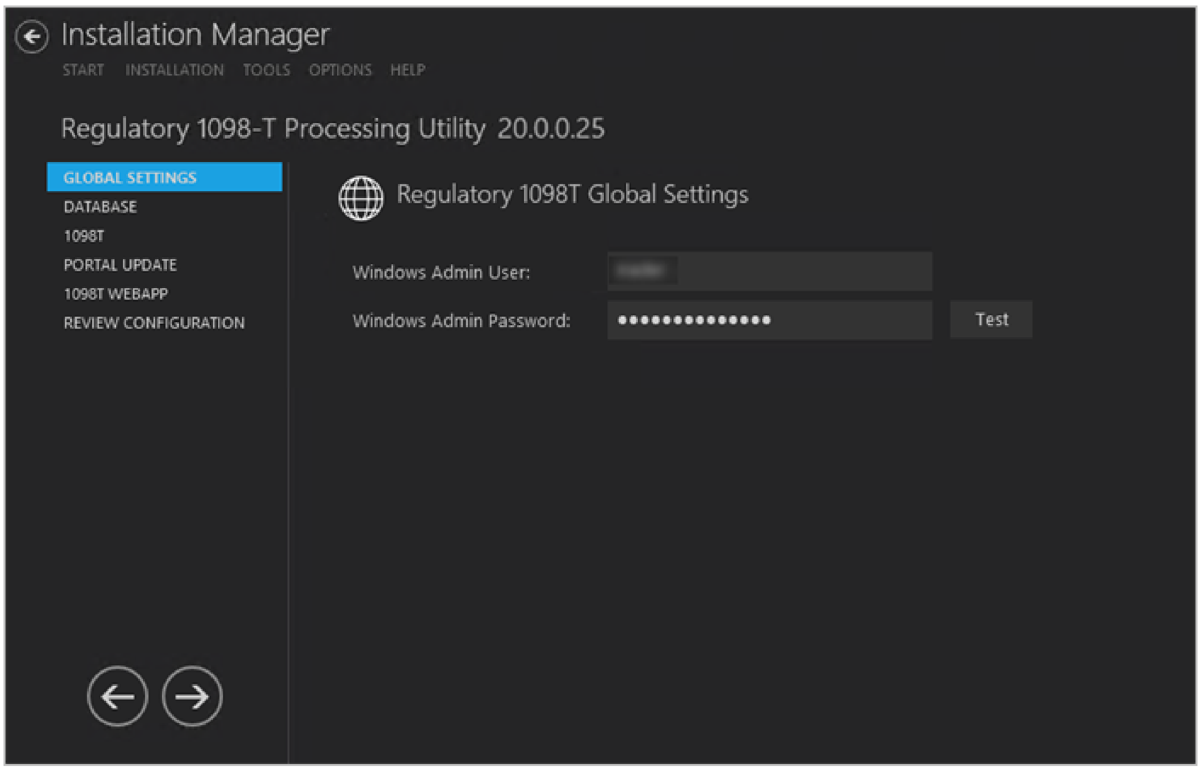
Global Settings

This screen contains the Windows Admin user name password used when starting an installation of the Regulatory 1098-T Processing Utility. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Regulatory 1098-T Processing Utility** tile. The Global Settings screen is displayed.



2. Complete the fields on the Global Settings screen as described in the table below.

Global Settings Fields

Field	Description
Windows Admin User	Specify the user name of the user with administrator permissions on the computer where the COM, Windows, and Web Services will run. This account must have administrative access to all the machines being installed to. It must be a sysadmin on the database as integrated security is the only option that will be used. Depending on your network environment, specify one of the following: • User name • Domain\User name • Email address of Admin User
Windows Admin Password	Specify the password for the Administrator user name. This password is used in the background for other installation steps. **Note**: The Application Pool for Security Token Service will use the Windows Admin credentials provided here.

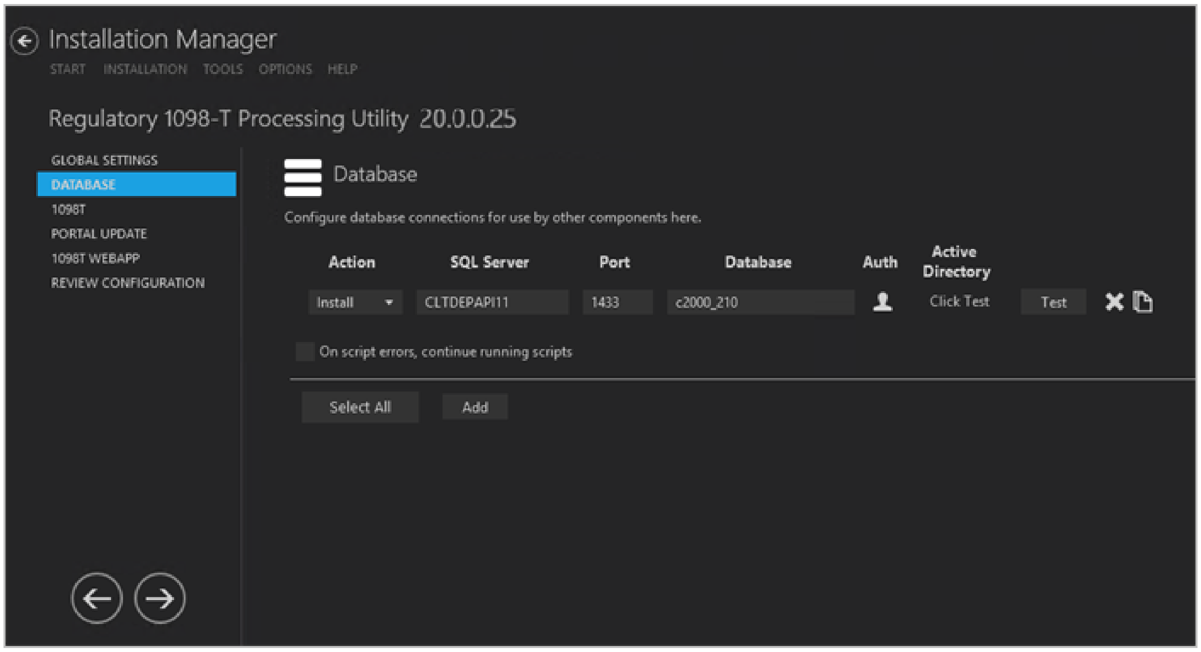
3. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
4. If the user is authenticated, click **OK** and click  to continue.

Database

This screen enables you to select the actions to be taken by Installation Manager (e.g., install) and to specify the machine name, the Anthology Student database, and the authentication options.

Set Up the Database

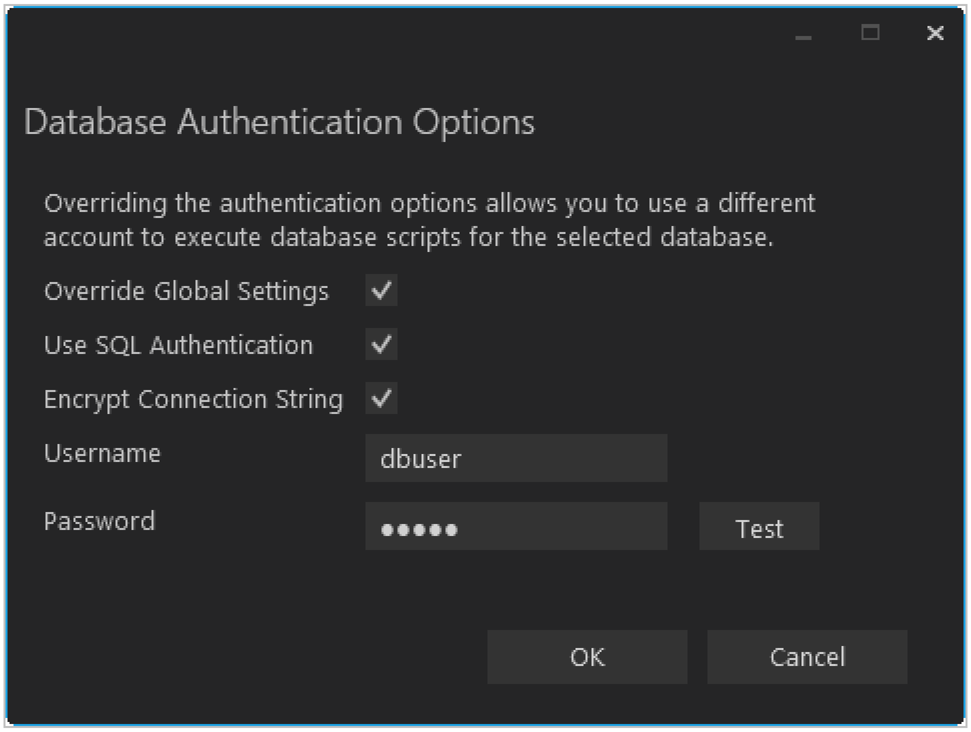
1. In the Installation menu, click **Database**. The Database screen for the Regulatory 1098-T Processing Utility is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the name of the **SQL Server** where the Anthology Student database is installed.
5. Specify a **Port** number or accept the default SQL port (1433).
6. Specify the name of the **Database** for Anthology Student.

7. Click  in the **Auth** column if you want to override the authentication options from Global Settings for the selected database, for example, to give another user permissions to execute scripts for the selected database. The Database Authentication Options form is displayed.



   a. Select the **Override Global Settings** check box to enable the fields on the form.

   b. Select the **Use SQL Authentication** check box if SQL authentication is applied.

      When SQL Authentication is selected, the Encrypt Connection String, Username, and Password are enabled.

      The SQL username and password must be used to execute the database scripts.

   c. The **Encrypt Connection String** check box is selected be default when SQL Authentication is selected. You can clear this option if necessary.

   d. Enter the **Username** and **Password** of the account that is given the override permissions for the selected database.

      The Test buttons in the Options form and in the Database screen will use these credentials if selected.

   e. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

   f. Click **OK** to save changes on the Options form. The form is closed.

8. The **Active Directory** field is populated when you click the **Test** button.

9. Select the check box for **On script errors, continue running scripts** if you want the installation process to continue regardless of errors encountered.

   By default, database upgrades will stop if the script encounters any errors. This selection is used if there are custom modifications to the database that are known to cause errors in the upgrade scripts. Selecting this option enables all scripts to be run against the specified database.

   Whether the check box is selected or not, any errors are written to a separate error file for each script, which may be investigated after the script execution. Error logs are stored in the following folder: `DatabaseServer\C:\Logs\Output`.

   The error log is the name of the script, SQL Server, and database name appended with `_Errors.txt`, for example, `CampusVue_18.3.00xx_{SQL Server}_{database_name}_Errors.txt`)

   There is also an output file that has all of the script output: `CampusVue_18.3.00xx_{SQL Server}_{database_name}_Output.txt`

10. Click  to copy a line. Edit the copied line as needed.

11. Click  to delete a selected line.

12. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

    Note: The Test button operates as follows:

    - Queries the database to get the latest version of Anthology Student.
    - Uses Windows Admin credentials (see Global Settings) and tests connectivity to the SQL server.
    - Uses the Student Admin user name (see Global Settings) and checks if it exists in the Anthology Student database.

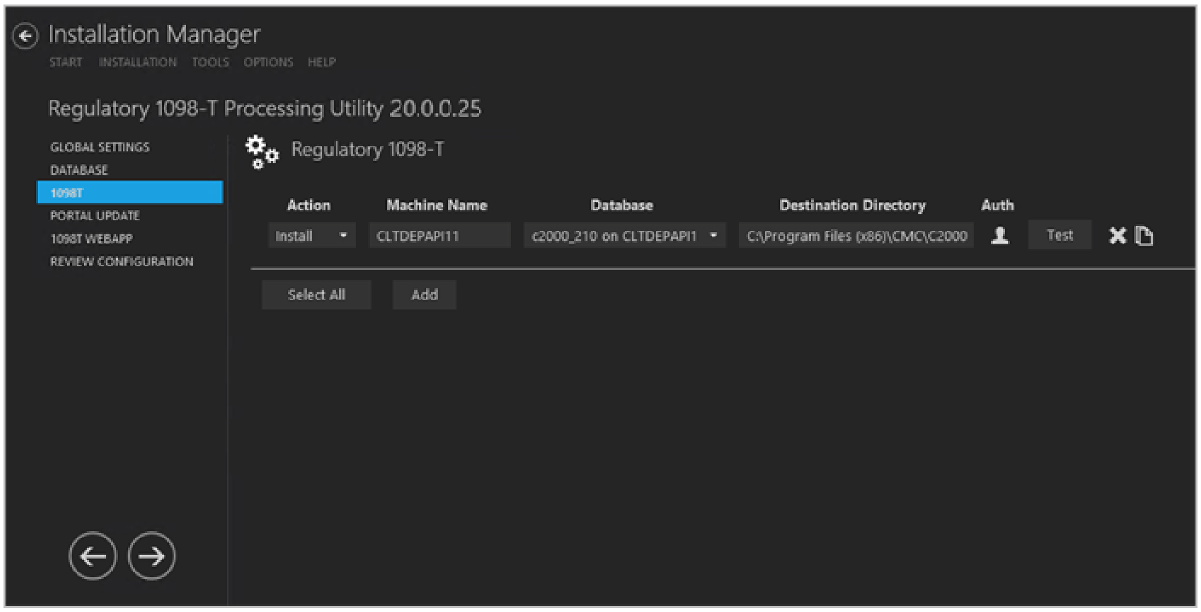
13. If all tests pass, click .

1098-T Client

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name of the client for the Regulatory 1098-T Processing Utility.

Set Up the 1098-T Client

1. In the Installation menu, click **1098T**. The Regulatory 1098T settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

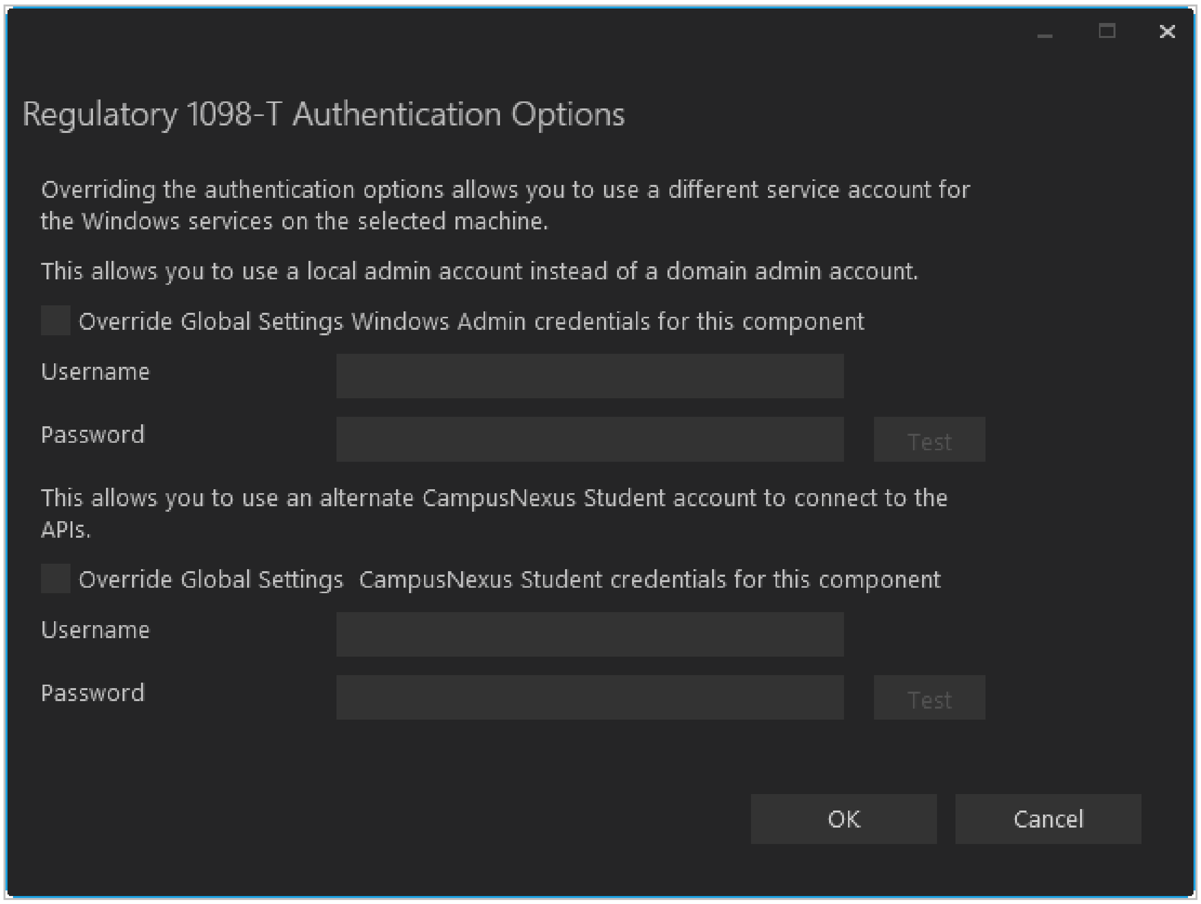
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed. This is the machine where the client for the 1098-T Processing Utility will be installed.

5. In the **Database** field, select a database for Anthology Student. The drop-down contains a list of databases configured in the Database settings screen.

6. Specify the **Destination Directory** if you want to override the default directory set on the [Global Settings](#) screen. Installation Manager searches the machine for an existing \C2000 share folder. It automatically uses the \C2000 share folder as the Destination path to install to, if found. Otherwise, it uses the Destination Path from the Global Settings.

7. Click  in the **Auth** column if you want to override the authentication options from [Global Settings](#) to use a different account for the Windows services and alternate Anthology Student credentials on the selected machine. The Service Authentication Options form is displayed.



   a. Select the check box **Override Global Settings Windows Admin credentials for this component** to enable the associated fields on the form. This option allows you to use a local admin account instead of the domain admin account.

   b. Enter the **Username** and **Password** of the local admin account for the selected machine.

   c. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

d. Select the check box **Override Global Settings Anthology Student credentials for this component**.

e. Enter the **Username** and **Password** of Anthology Student account for the selected machine.

f. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

g. Click **OK** to save changes on the Options form. The form is closed.

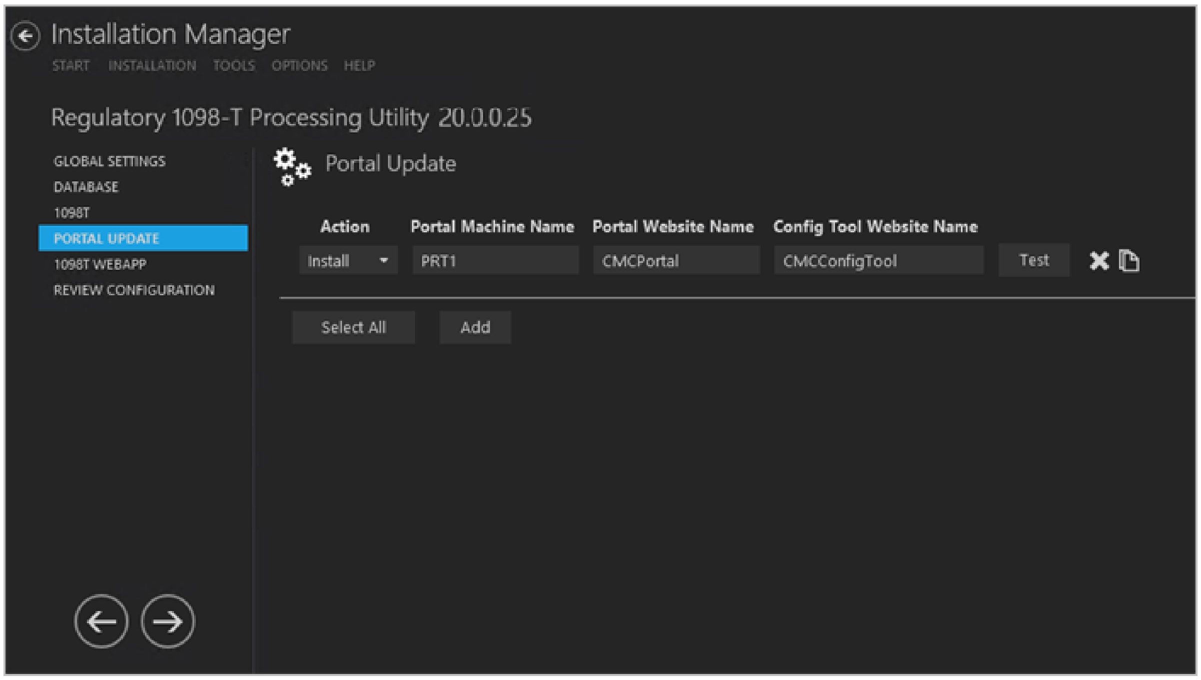
8. Click to copy a line. Edit the copied line as needed.
9. Click to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Portal Update

For campuses that have configured their Portal to display 1098-T forms, students can navigate to the Student Portal to view, accept, decline, or print their 1098-T forms. This screen enables you to install the updates that enable students to view their 1098-T forms in the Student Portal.

Set Up the Portal Link

1. In the Installation menu, click **Portal Update**. The Portal Update screen for the 1098-T Processing Utility is displayed.

2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Portal Machine Name**.

Installation Manager searches for an instance of the Portal and fills in the Portal Website Name and ConfigTool Website Name as they are found.

5. Enter the **Portal Website Name** if you want to override the value populated by Installation Manager.
6. Enter the **Config Tool Website Name** if you want to override the value populated by Installation Manager.
7. Click  to copy a line. Edit the copied line as needed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

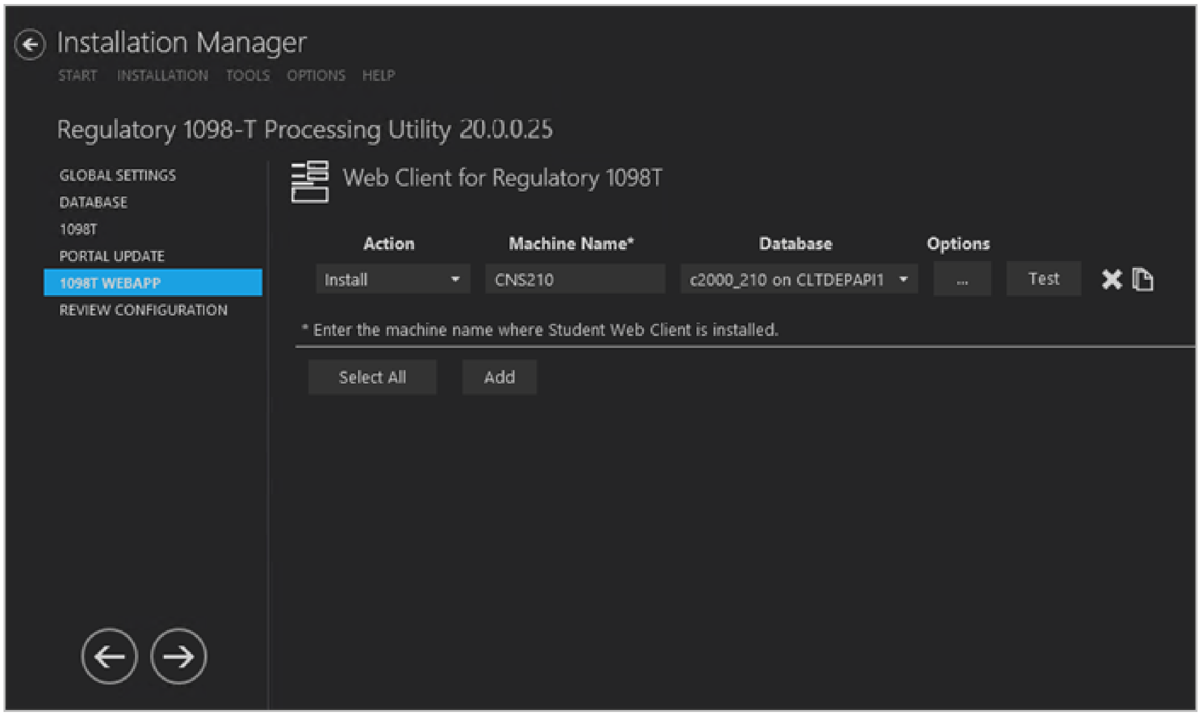
Regulatory 1098-T Web App

The functionality of the 1098-T Processing Utility is available in Anthology Student Web App version 20.0.2 or higher. To view the 1098-T forms in Anthology Student once the installation is complete, navigate to **Processes > IRS 1098-T**.

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and options of the 1098-T Processing Utility.

Set Up the 1098-T Web App

1. In the Installation menu, click **1098T Webapp**. The Web Client for Regulatory 1098T screen is displayed.



2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:

   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

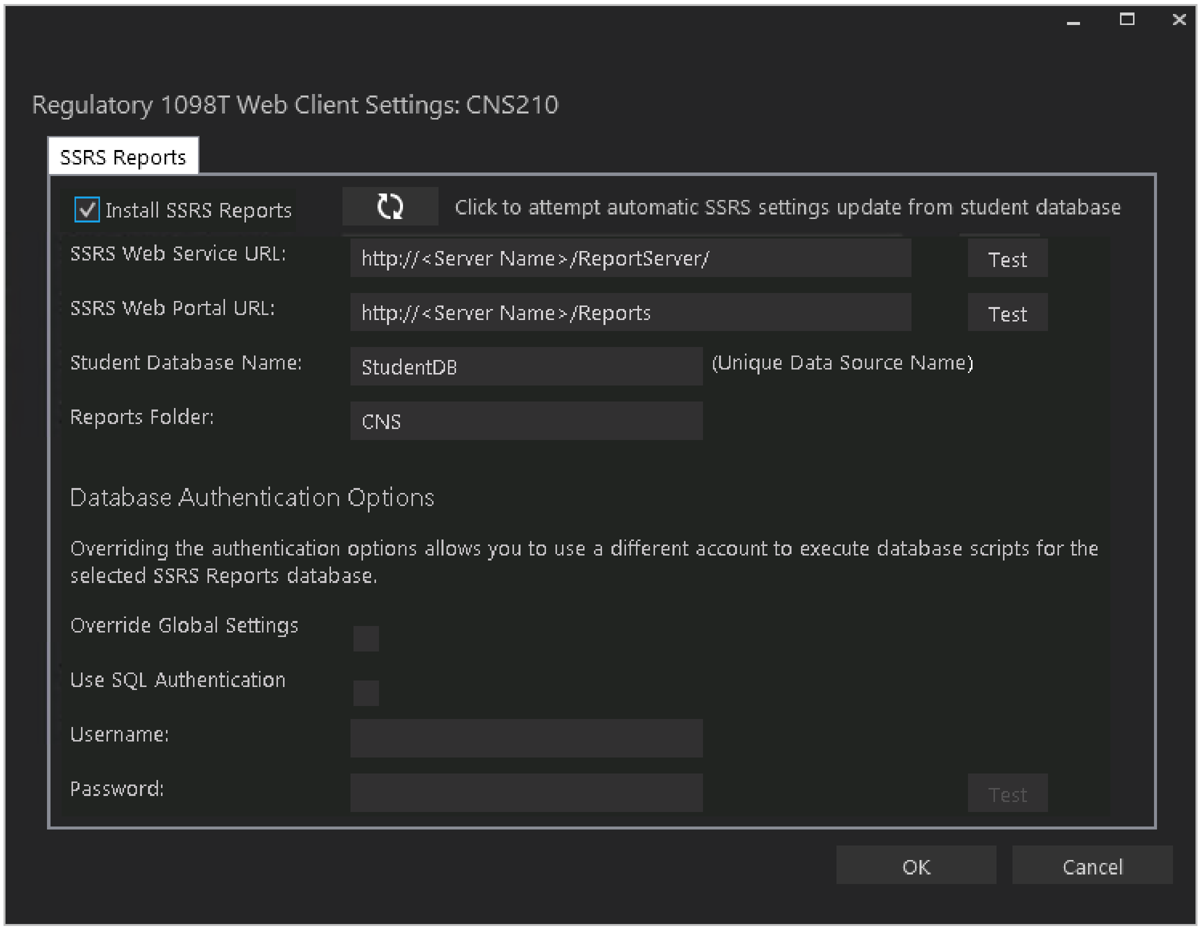
4. Enter the **Machine Name** for the component to be installed.

5. Click to copy a line. Edit the copied line as needed.

6. Click ... to view and edit the Options form.

SSRS Reports Tab

Use this tab to integrate SQL Server Reporting Services (SSRS) 2016, the server-based report generating software system, into the Regulatory 1098T. The SSRS URLs and the Reports Folder Root Path specified on this tab are stored in the web.config file.

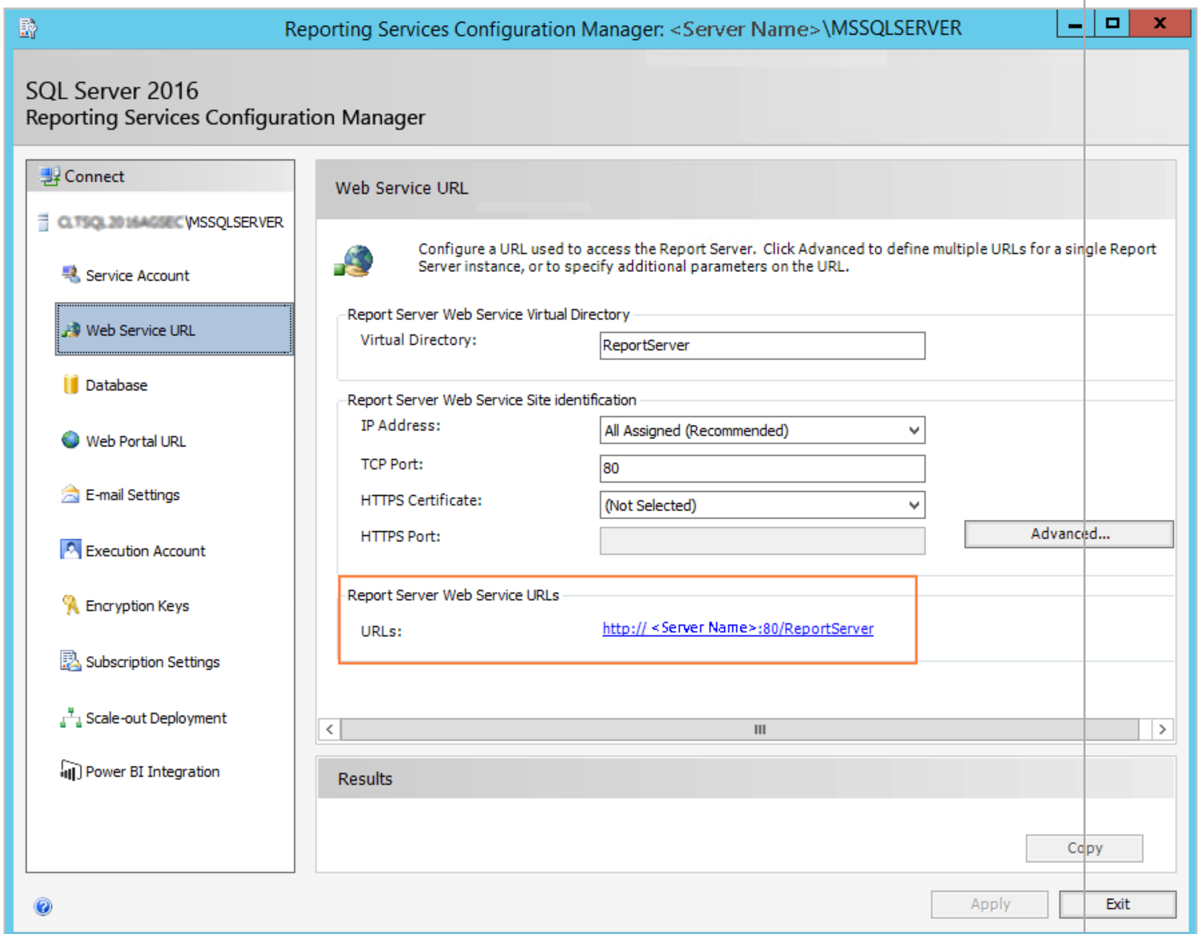


SSRS Reports Tab Fields

Field	Description
Install SSRS Reports	Select this check box to enable the fields on this tab.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Service URL</td><td>
Specify the Web Service URL configured to access the Report Server. The specified URL will be stored in the web.config file.

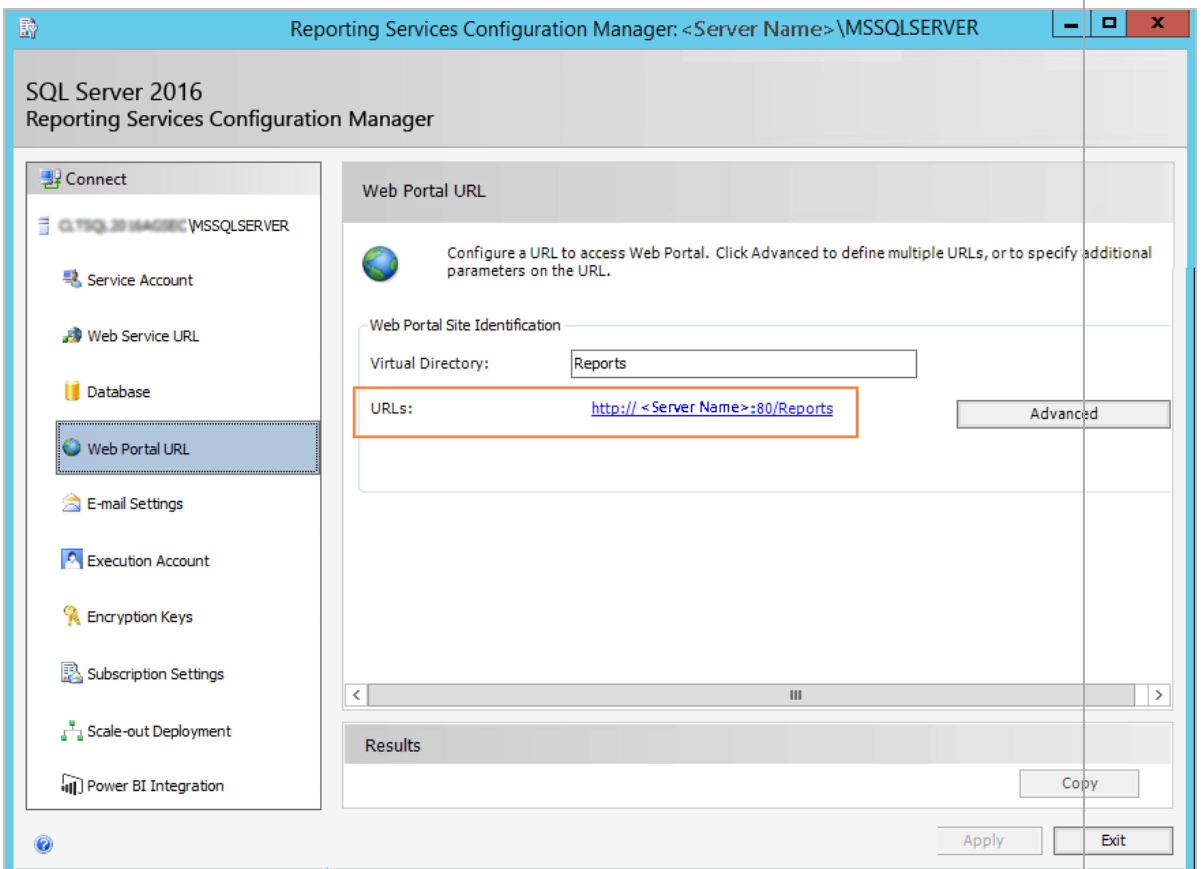
This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager.



</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Portal URL</td><td>Specify the Web Portal URL configured to access the Web Portal. The specified URL will be stored in the web.config file.

This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager page.


</td></tr>
<tr><td>Data Source Name</td><td>Specify the name of the Anthology Student database that is the source for the reports.</td></tr>
<tr><td>Reports Folder</td><td>Specify the path for the reports folder on the Report Server. A folder will be created if one does not exist. The folder name can be unique to the environment. The reports folder root path will be stored in the web.config file.

Example

<code>QA/CNS</code> where <code>QA</code> is one folder and <code>Student_Test</code> is a folder under <code>QA</code>.</td></tr>
<tr><td colspan="2">Database Authentication Options</td></tr>
<tr><td>Override Global Settings</td><td>Optional: Select this check box to enable the database authentication options.</td></tr>
</table>

Field	Description
Use SQL Authentication	Optional: Select this check box if SQL authentication is applied.
Username	Enter the user name of the account that is given override permissions for the SSRS reports database.
Password	Enter the password of the account that is given override permissions for the SSRS reports database.
Test	Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

In addition to the settings on the SSRS Reports tab in Installation Manager, the setup of reporting services requires configurations in the SQL Server Reporting Services Configuration Manager (see Configure Access to Reports).

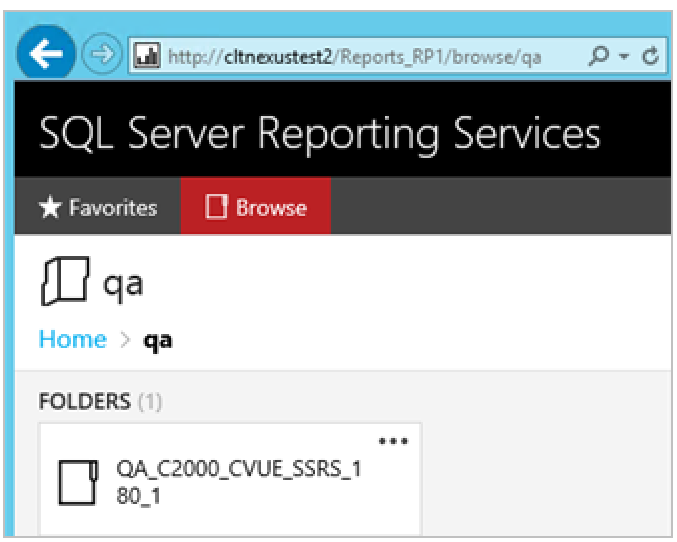
You also need to create folders in the Anthology Student and assign permissions using the Security Console. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Configure Access to Reports

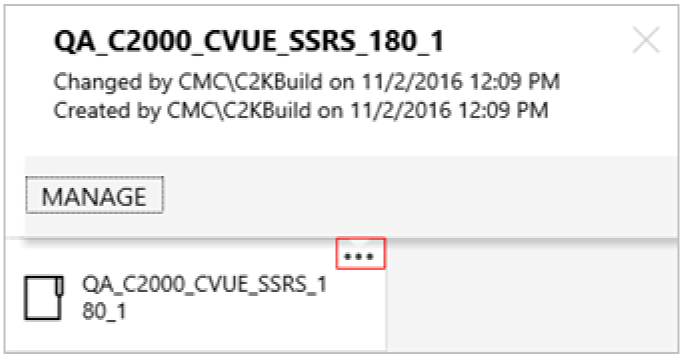
To enable access to the "Reports" menu item in Anthology Student, perform the following steps in the Reporting Services Configuration Manager on the report server:

a. Navigate to the /Reports folder path.

   In the example below the reports folder path is `http://cltnexustest2/Reports_RP1/browse/`**qa**.



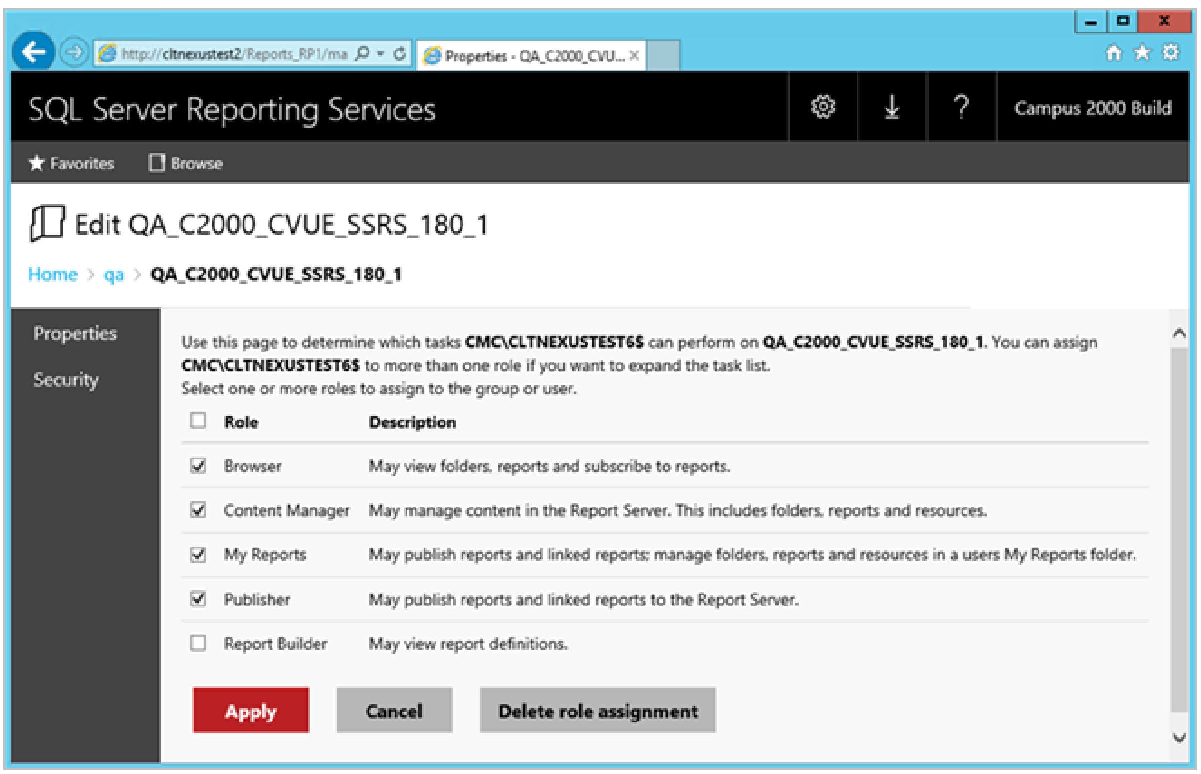
b. Right-click on the ellipsis of the reports folder root and select **Manage**.



c. Select the **Security** tab, click **Customize security**, and click **Add group or user**.

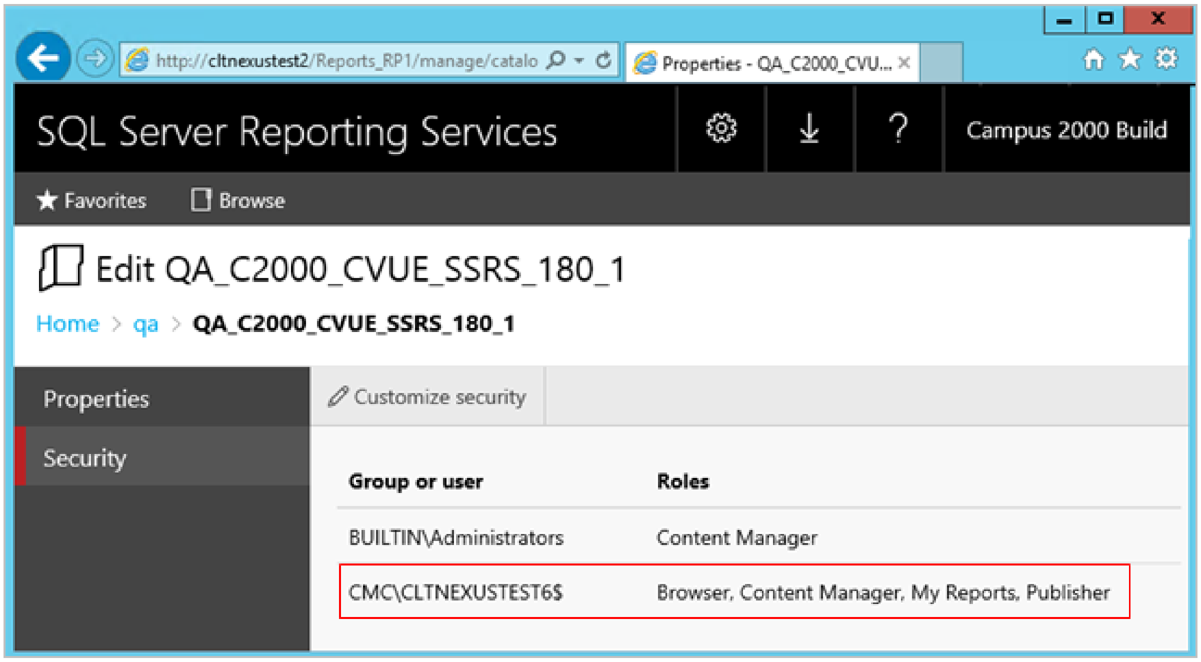
d. Add the **domain\<machine name$>** of Anthology Student and select the following **Roles**:

- Browser
- Content Manager
- My Reports
- Publisher



e. Click **Apply**.

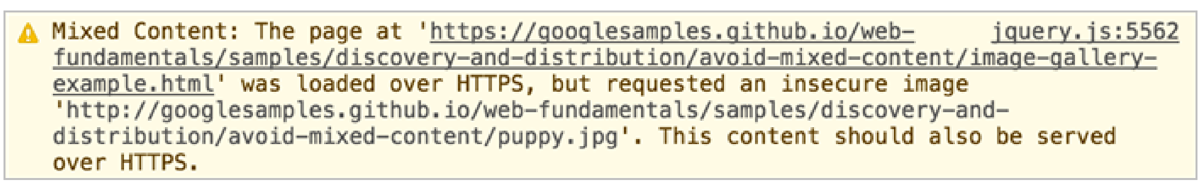
Security for the Reporting Service should be set up as shown below, where CMC\CLTNEXUSTEST6 is the domain\machine name of Anthology Student from which the reports are accessed.



Configure SSRS for HTTPS

Once the reporting services are installed and configured, test access to the reports in Anthology Student. Select the Reports tile and navigate to any report listed in the menu.

If Anthology Student displays only the title of the report (without any data selection fields), use the browser developer tools (**F12**) and check the **Console** tab. If an error similar to the following is displayed, configure SSRS for secure access with an SSL certificate. For detailed instructions, see https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-ssl-connections-on-a-native-mode-report-server



7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

   The Test button checks the connectivity of the Admin user to the machine specified in the Server name field.
10. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

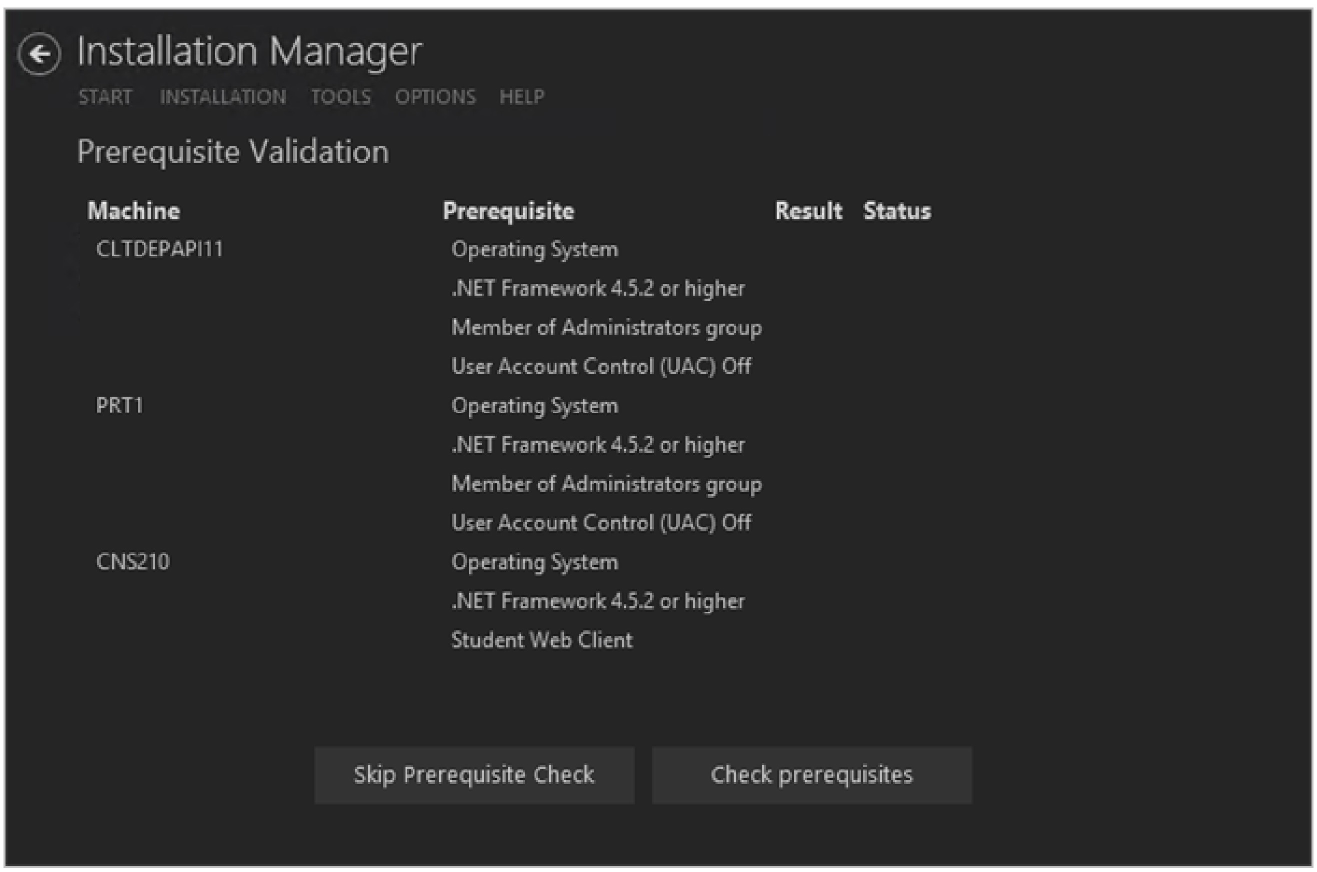
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

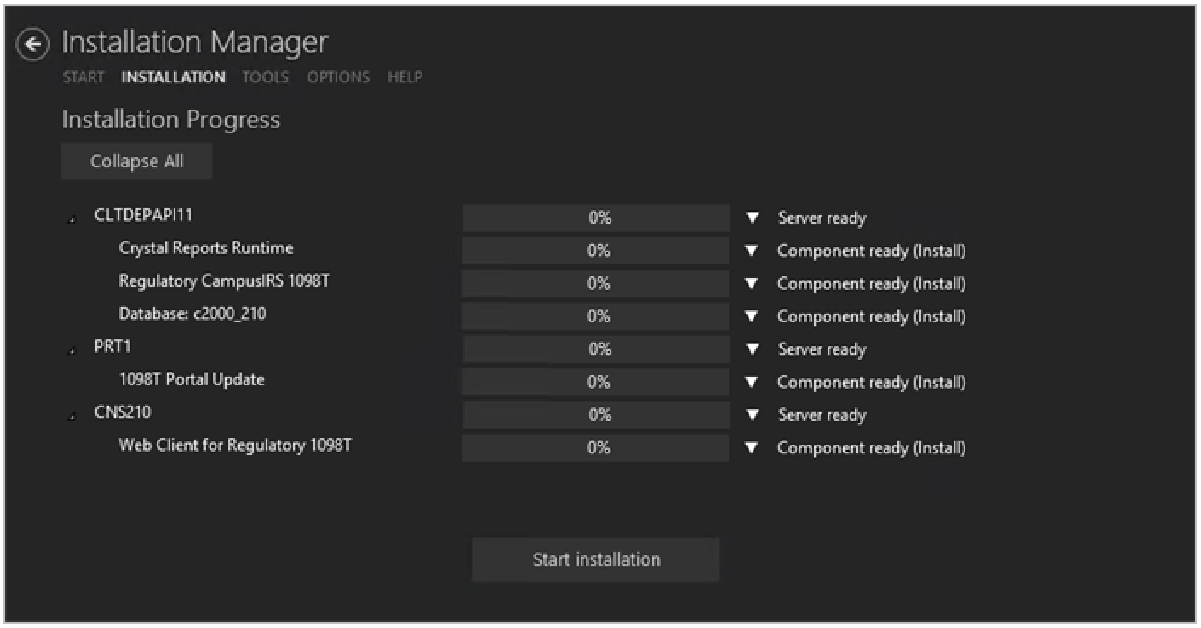
    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.

Click **Expand All** and scroll through the list of items. Or, click **Collapse All** and then click to expand a section.



4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

Faculty Workload Management

You can use the Faculty Workload Management (FWM) module in Anthology Student to automate:

- Workload validation for instructors to ensure they do not exceed their limits at your institution
- Pay generation for instructors (such as part-time and adjunct faculty)

To add Faculty Workload Management to an existing Anthology Student system, use Package Manager to download the installation files for Web Client for Workload Management.

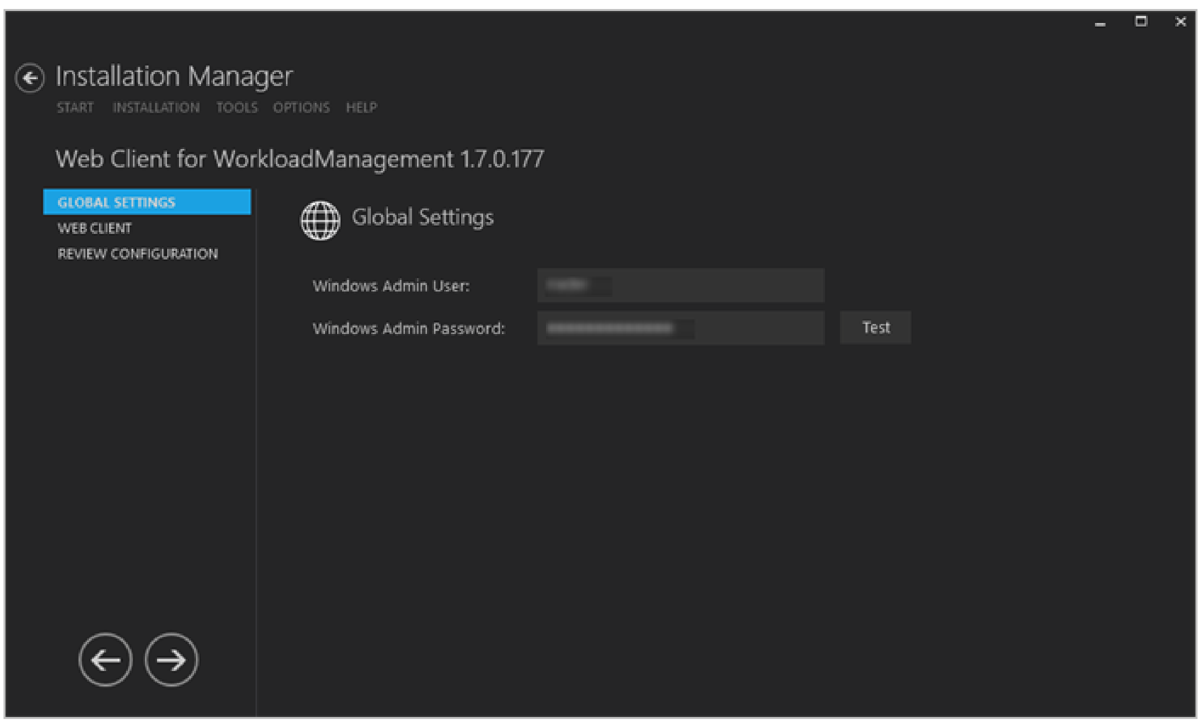
Global Settings

The Global Settings screen contains the Windows Admin user name password used when starting an installation of Faculty Workload Management. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Web Client for Workload Management** tile. The Global Settings screen is displayed.



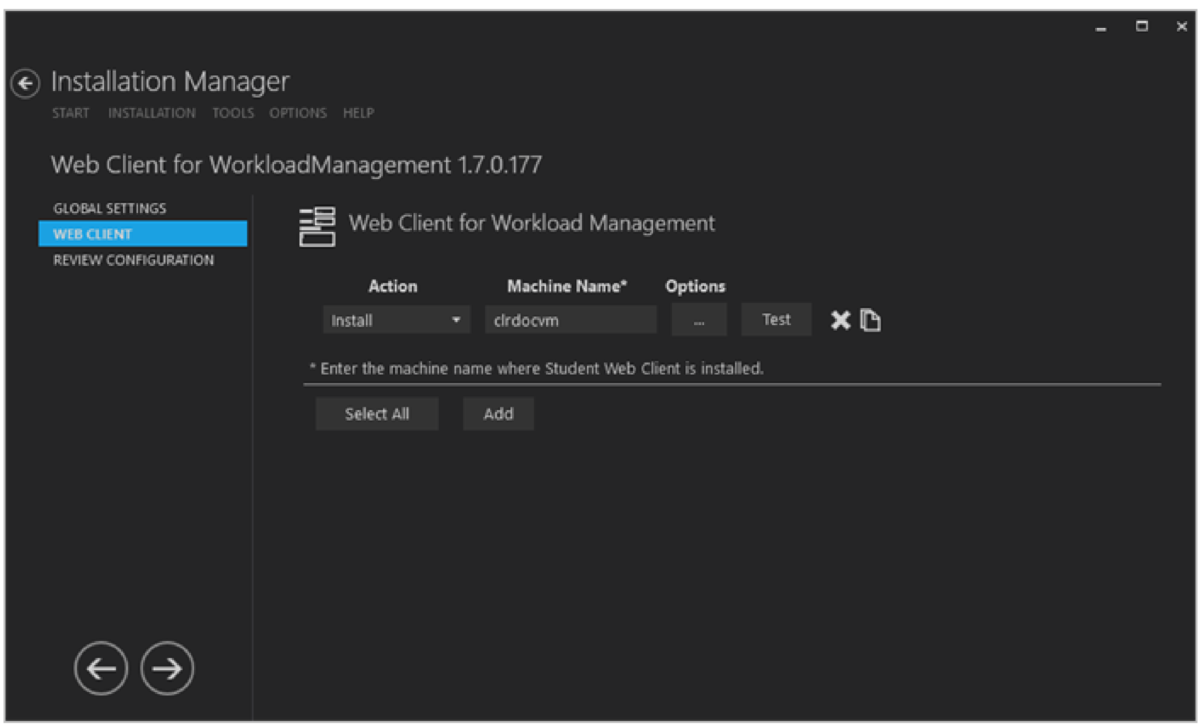
2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer where the installation will occur. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.
4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
5. If the user is authenticated, click **OK** and click  to continue.

Web Client

This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and options for Faculty Workload Management.

Set Up the Web Client

1. In the Installation menu, click **Web Client**. The Web Client for Workload Management screen is displayed.



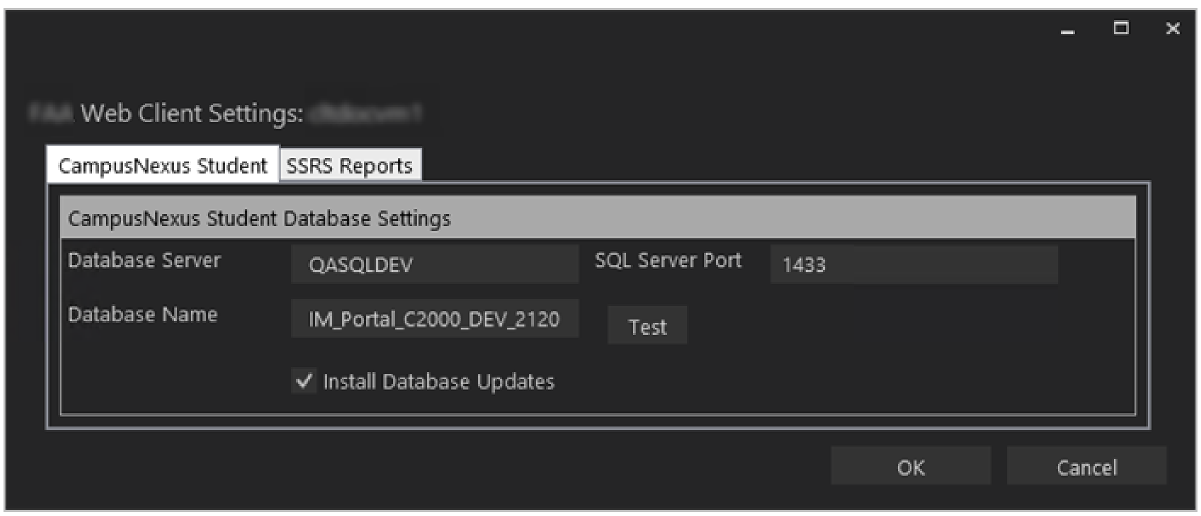
2. Click **Add** to add a line to the Settings screen.

3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed.
5. Click to copy a line. Edit the copied line as needed.
6. Click to view and edit the Options form.

   Anthology Student Tab

   Use this tab to configure the Anthology Student database connection for use by Regulatory.



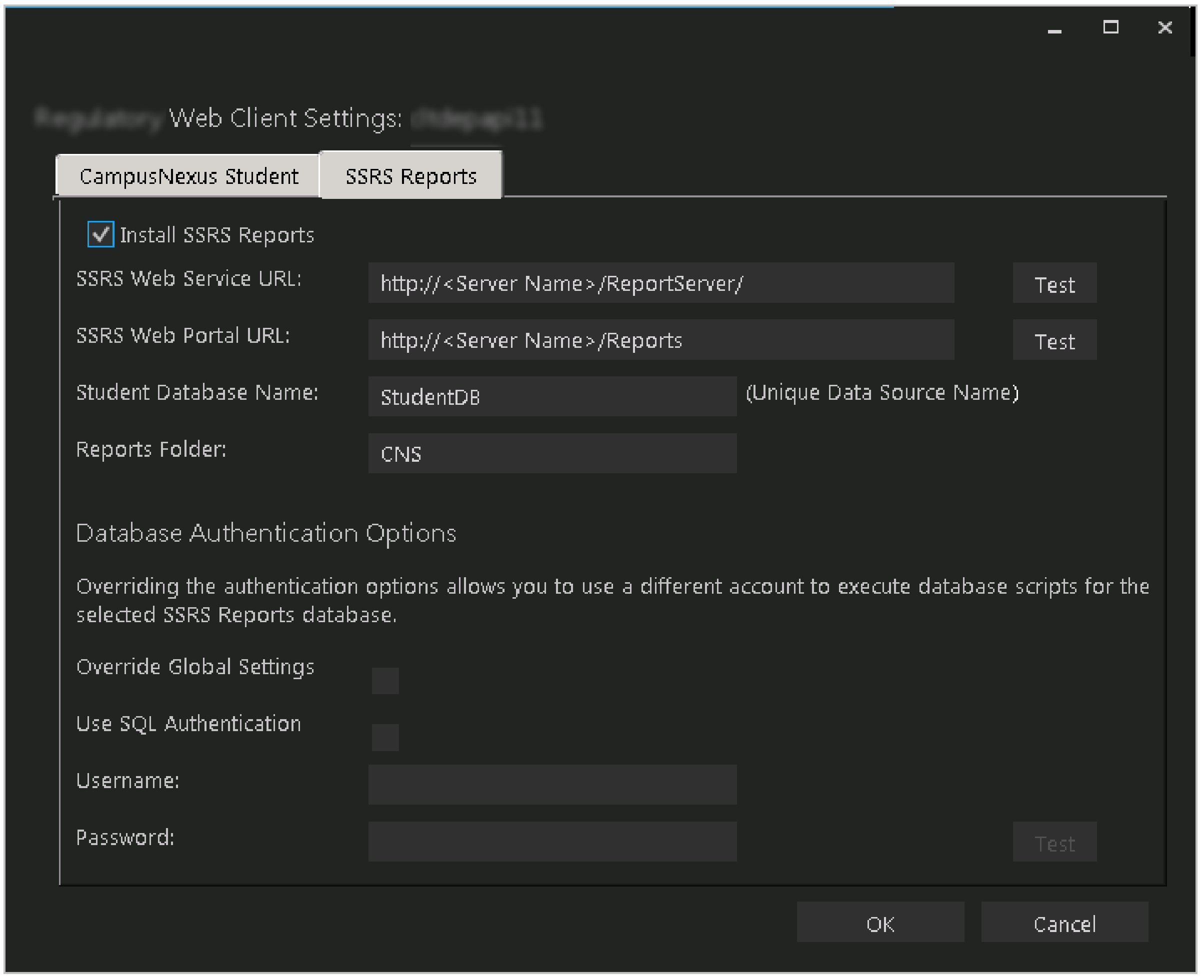
Anthology Student Tab Fields

Field	Description
Anthology Student Database Settings	
Database Server	Name of the SQL server on which the Anthology Student database resides.
SQL Server Port	Specify the port number of the SQL server or accept the default (1433).
Database Name	Name of the Anthology Student SQL database.

Field	Description
Test	Click **Test** to verify the database connection.
Install Database Updates	Select this check box to install updates to the Anthology Student database.

SSRS Reports Tab

Use this tab to integrate SQL Server Reporting Services (SSRS) 2016, the server-based report generating software system, into Faculty Workload Management. The SSRS URLs and the Reports Folder Root Path specified on this tab are stored in the web.config file.



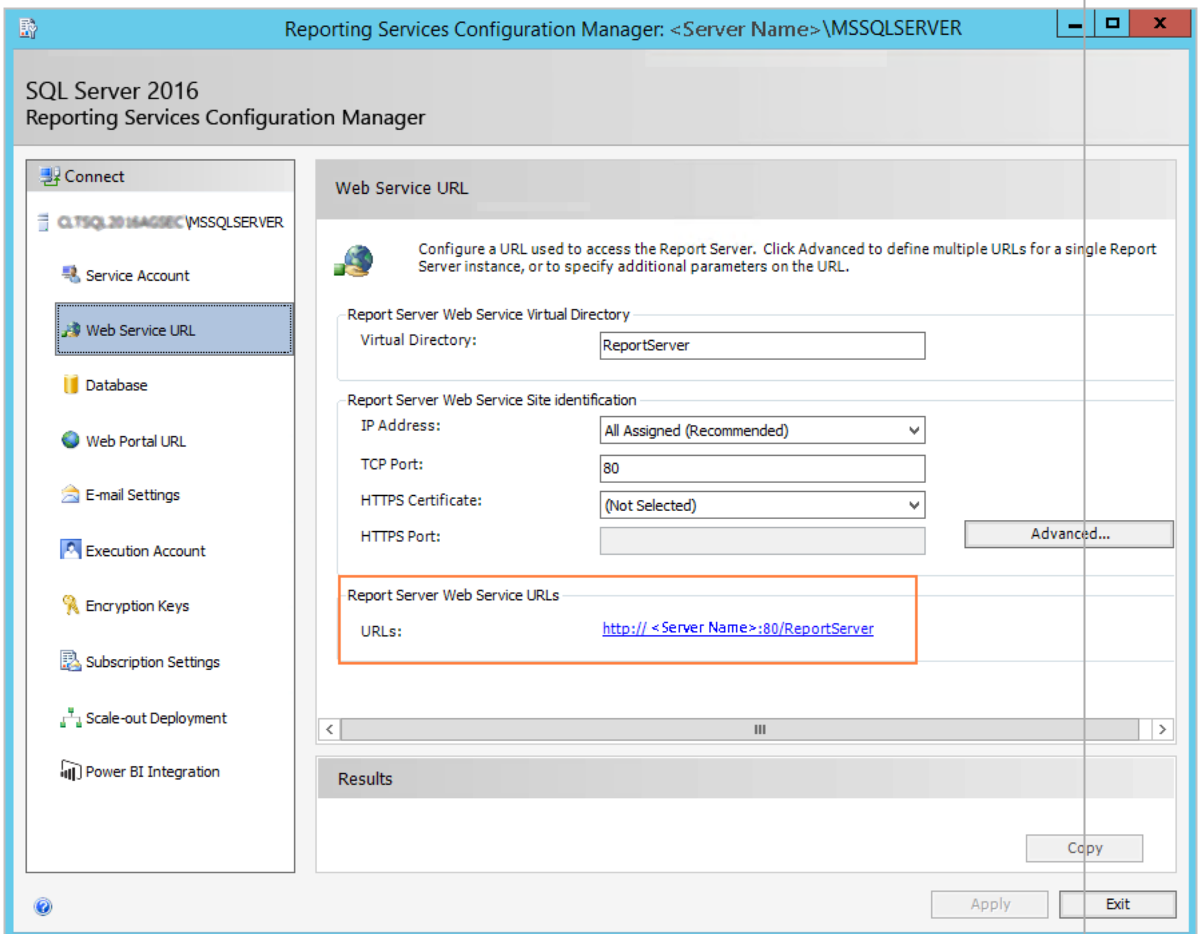
SSRS Reports Tab Fields

Field	Description
Install SSRS Reports	Select this check box to enable the fields on this tab.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Service URL</td><td>

Specify the Web Service URL configured to access the Report Server. The specified URL will be stored in the web.config file.

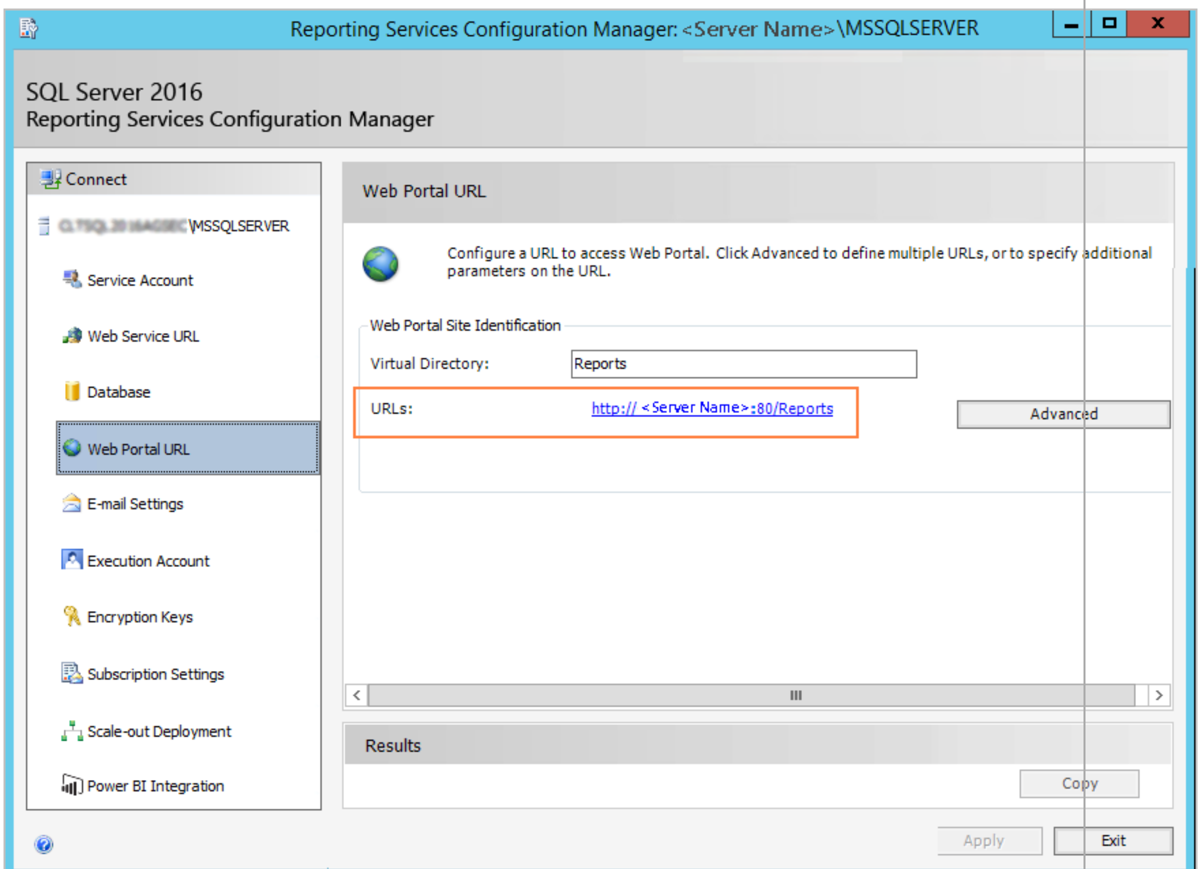
This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager.



</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>SSRS Web Portal URL</td><td>Specify the Web Portal URL configured to access the Web Portal. The specified URL will be stored in the web.config file.

This URL is set while configuring the reporting service and can be found in Reporting Services Configuration Manager page.


</td></tr>
<tr><td>Data Source Name</td><td>Specify the name of the Anthology Student database that is the source for the reports.</td></tr>
<tr><td>Reports Folder</td><td>Specify the path for the reports folder on the Report Server. A folder will be created if one does not exist. The folder name can be unique to the environment. The reports folder root path will be stored in the web.config file.

Example

<code>QA/CNS</code> where <code>QA</code> is one folder and <code>Student_Test</code> is a folder under <code>QA</code>.</td></tr>
<tr><td colspan="2">Database Authentication Options</td></tr>
<tr><td>Override Global Settings</td><td>Optional: Select this check box to enable the database authentication options.</td></tr>
</table>

Field	Description
Use SQL Authentication	Optional: Select this check box if SQL authentication is applied.
Username	Enter the user name of the account that is given override permissions for the SSRS reports database.
Password	Enter the password of the account that is given override permissions for the SSRS reports database.
Test	Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

In addition to the settings on the SSRS Reports tab in Installation Manager, the setup of reporting services requires configurations in the SQL Server Reporting Services Configuration Manager (see Configure Access to Reports).

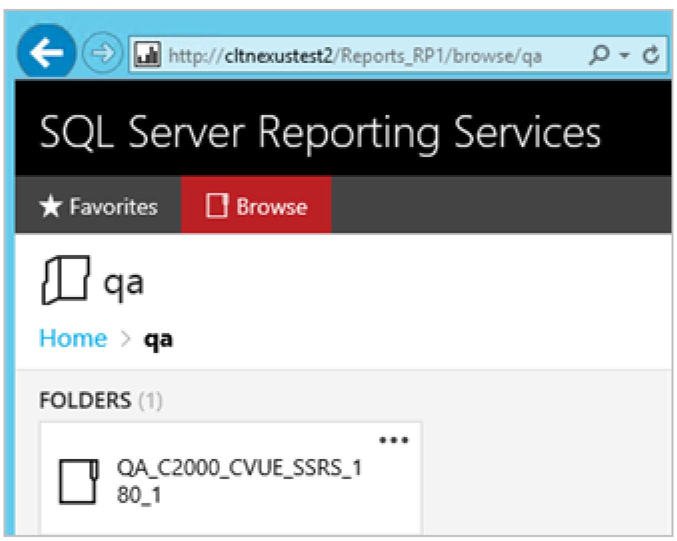
You also need to create folders in the Anthology Student and assign permissions using the Security Console. Refer to the *Administration and Configuration Help* for Anthology Student at the Product Information site.

Configure Access to Reports

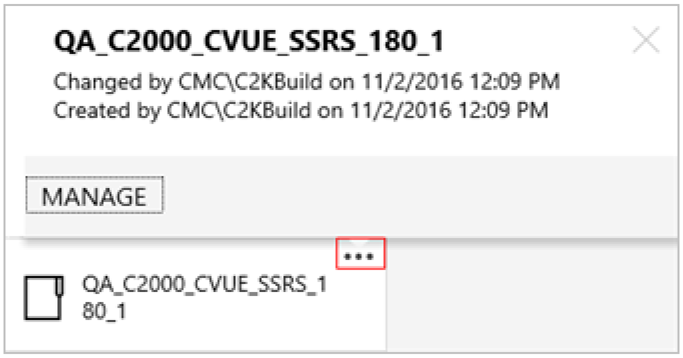
To enable access to the "Reports" menu item in Anthology Student, perform the following steps in the Reporting Services Configuration Manager on the report server:

a. Navigate to the /Reports folder path.

   In the example below the reports folder path is `http://cltnexustest2/Reports_RP1/browse/`**qa**.



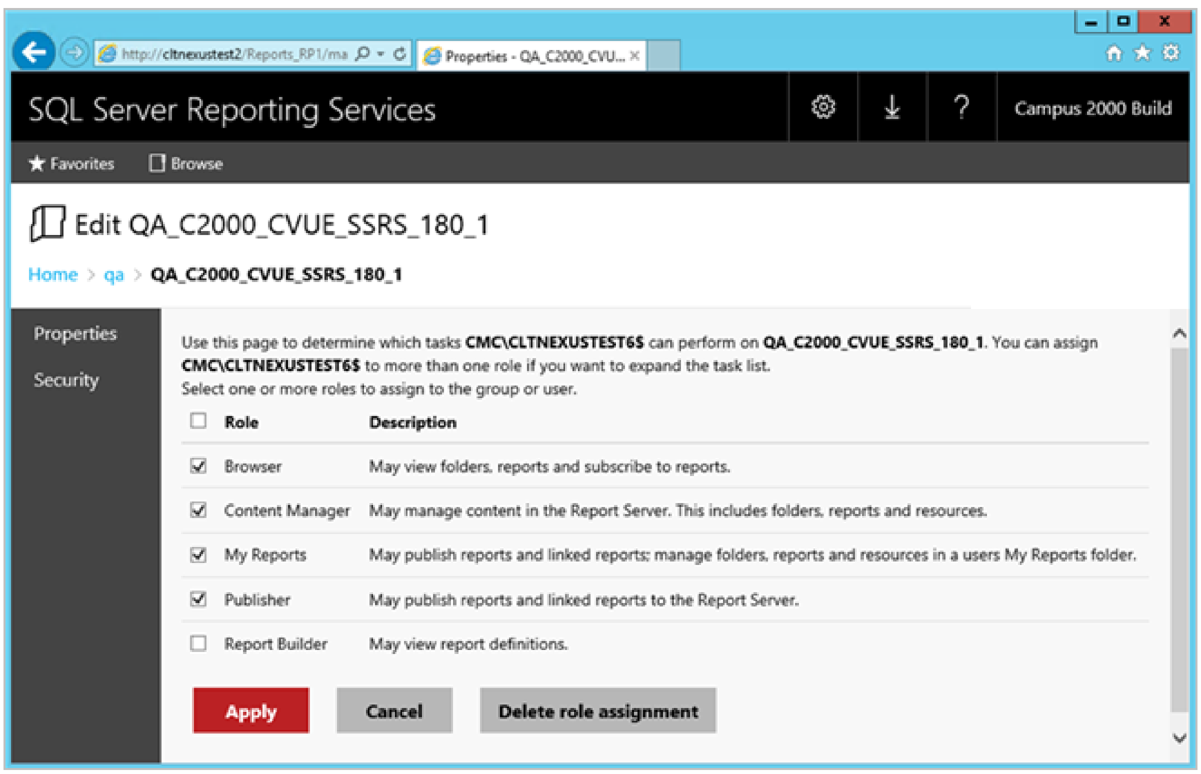
b. Right-click on the ellipsis of the reports folder root and select **Manage**.



c. Select the **Security** tab, click **Customize security**, and click **Add group or user**.

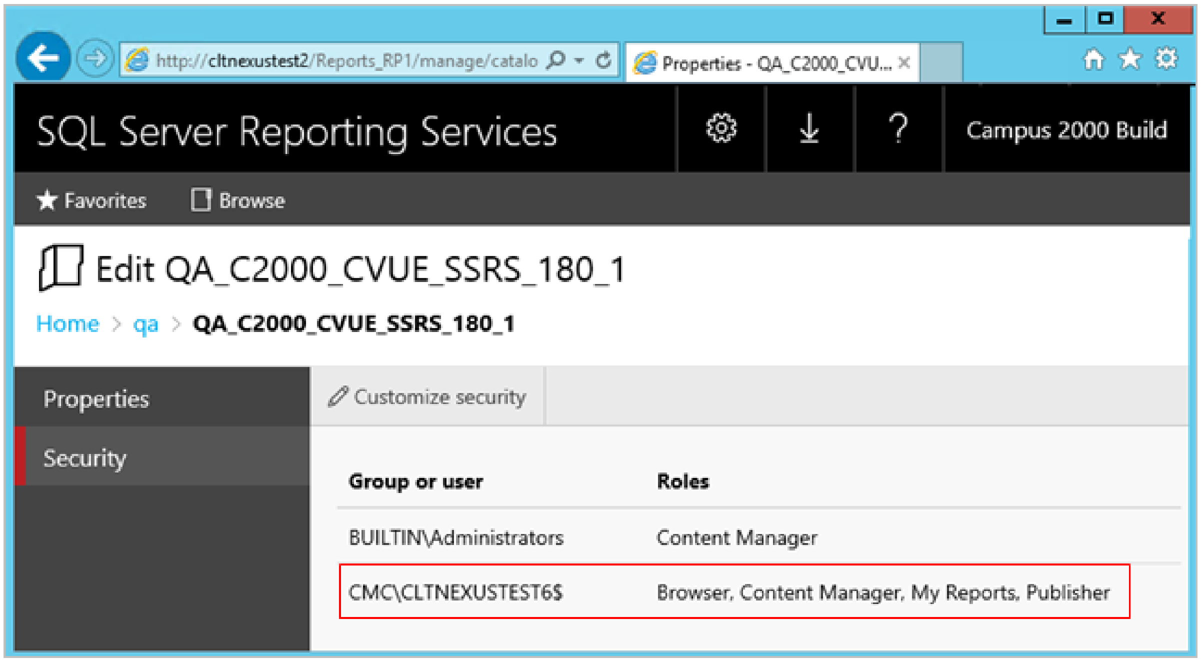
d. Add the **domain\<machine name$>** of Anthology Student and select the following **Roles**:

- Browser
- Content Manager
- My Reports
- Publisher



e. Click **Apply**.

Security for the Reporting Service should be set up as shown below, where CMC\CLTNEXUSTEST6 is the domain\machine name of Anthology Student from which the reports are accessed.



Configure SSRS for HTTPS

Once the reporting services are installed and configured, test access to the reports in Anthology Student. Select the Reports tile and navigate to any report listed in the menu.

If Anthology Student displays only the title of the report (without any data selection fields), use the browser developer tools (**F12**) and check the **Console** tab. If an error similar to the following is displayed, configure SSRS for secure access with an SSL certificate. For detailed instructions, see https://docs.microsoft.com/en-us/sql/reporting-services/security/configure-ssl-connections-on-a-native-mode-report-server

```
⚠ Mixed Content: The page at 'https://googlesamples.github.io/web-      jquery.js:5562
fundamentals/samples/discovery-and-distribution/avoid-mixed-content/image-gallery-
example.html' was loaded over HTTPS, but requested an insecure image
'http://googlesamples.github.io/web-fundamentals/samples/discovery-and-
distribution/avoid-mixed-content/puppy.jpg'. This content should also be served
over HTTPS.
```

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click ✖ to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

   The Test button checks the connectivity of the Admin user to the machine specified in the Server name field.

10. If all tests pass, click ➔.

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

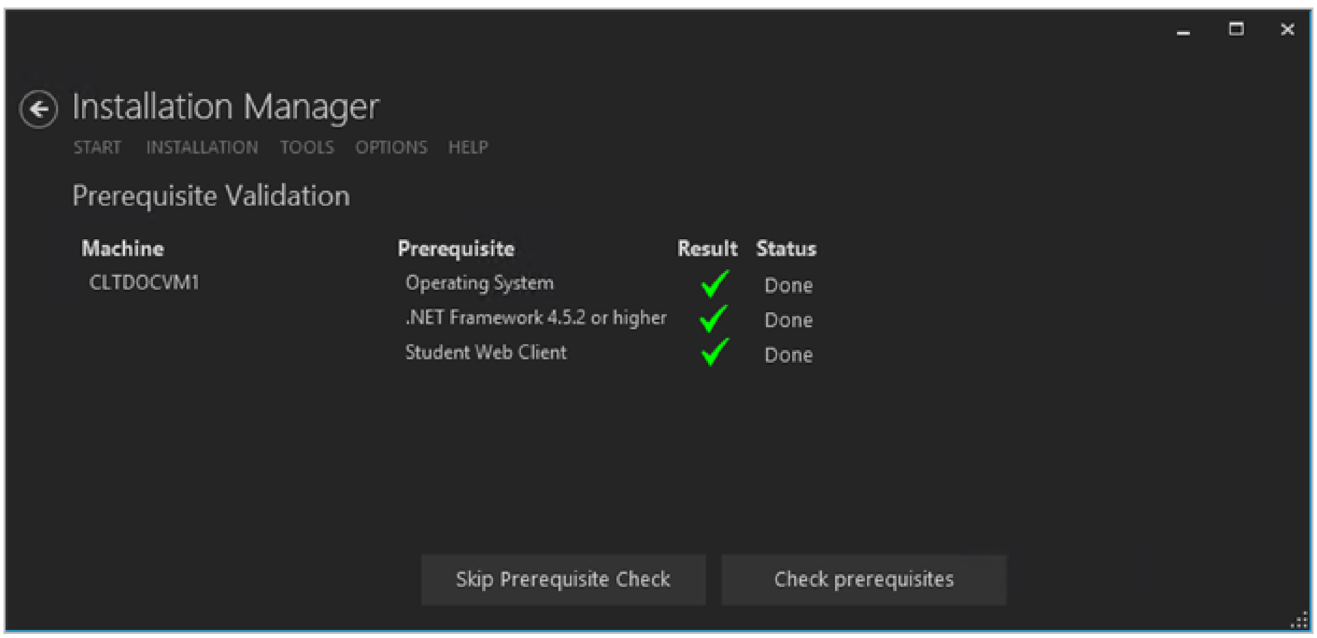
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

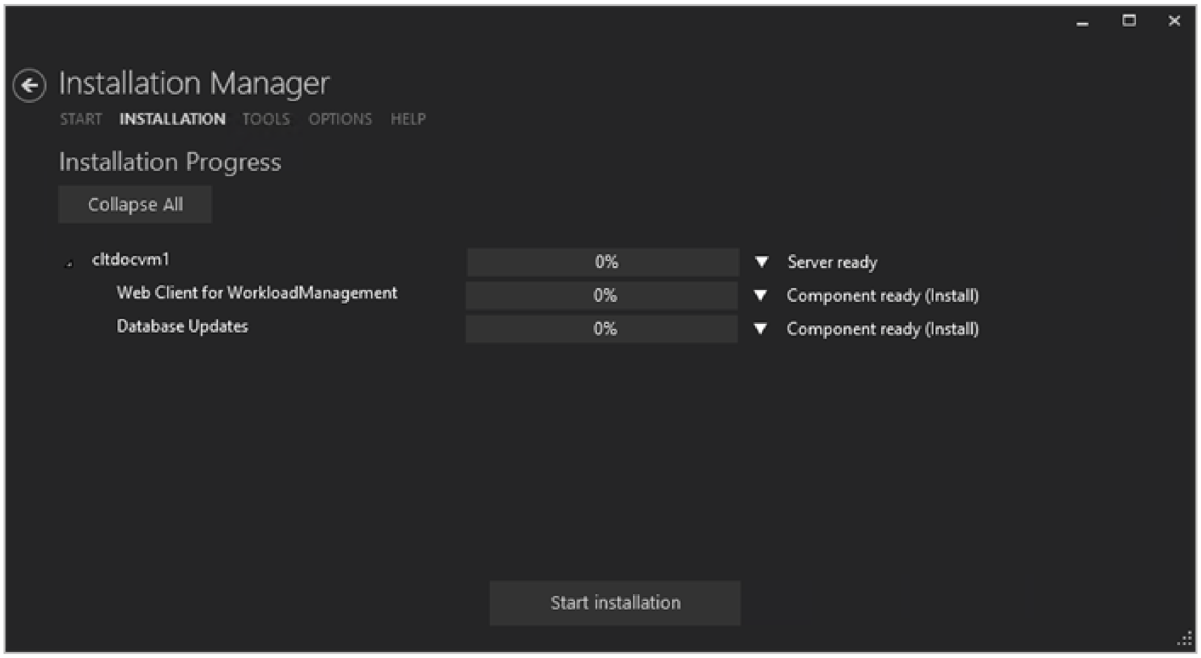
    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.
4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.



Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

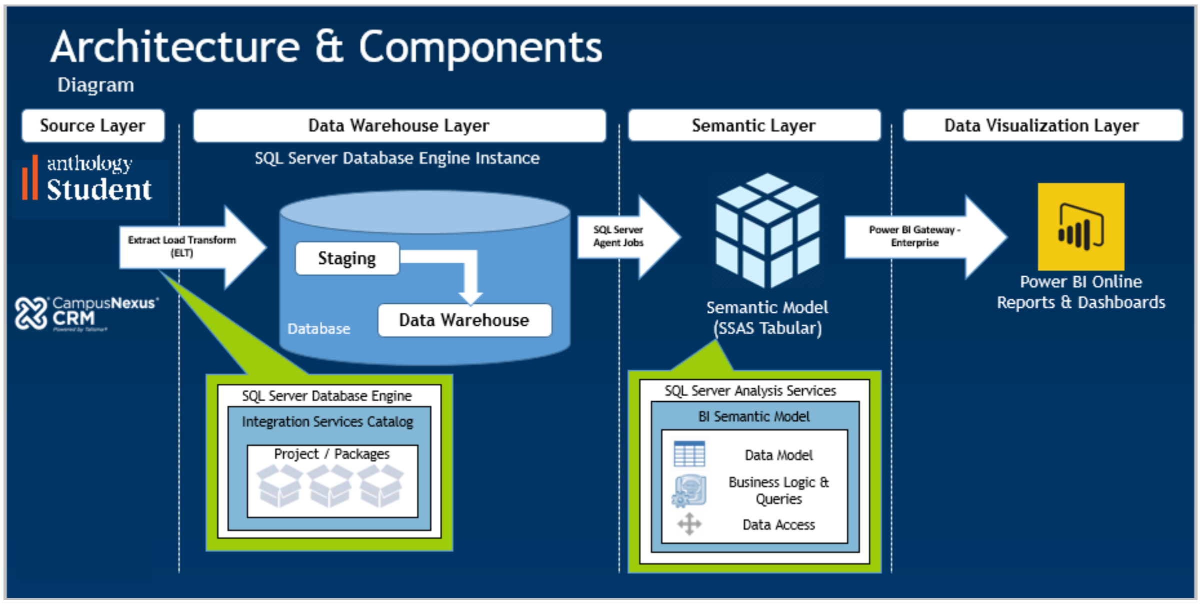
6. To verify or troubleshoot the installation, click ▼ next to a progress bar to access installation logs and other tools (see Installation).

Analytics

The current Business Intelligence (BI) offering for Anthology Student and CampusNexus CRM is Student Analytics. It is installed using Installation Manager.

Architecture

The design of Student Analytics is based on a four-layer architecture.



- Source Layer:

  The Anthology Student and/or CampusNexus CRM databases serve as the data sources throughout Student Analytics; all day-to-day changes made to the databases (insert, update, and delete operations) are tracked and the changes are fetched by the Extract Load Transform (ELT) process.

- Data Warehouse Layer:

  The ETL process uses the SQL Server Integration Services (SSIS) platform and SSIS Catalog framework for data extraction and for updating the dimension and fact tables.

- Semantic Layer:

  Student Analytics has a semantic tabular model deployed on the SQL Server Analysis Services (SSAS) platform and is configured to process and contain the data from the data warehouse. This semantic model consists of dimensions and facts from the data warehouse (data access) and various measures applied across the facts (business logic and queries), facilitating data analysis from various perspectives.

- Data Visualization Layer:

The data visualization layer leverages Microsoft Power BI, enabling users to connect to the semantic model (as a dataset) and create rich visualizations which can be organized on a canvas to build Reports or pinned to build Dashboards and shared across the enterprise.

For more information, refer to Student Analytics Help.

Supported Databases

Student Analytics version 4.x and later supports subsets of data from the Anthology Student and/or CampusNexus CRM databases.

- For Anthology Student versions 20.0 through 21.0, Student Analytics is limited to data associated with the following modules:
  - Academics
  - Admissions
  - Career Services
  - Financial Aid
  - Student Account
  - Contact Manager
- For CampusNexus CRM versions 13.x, Student Analytics is limited to the Campaign module consisting of Campaign Mail, URL Click, and Campaign SMS statistics only. Also, Analytics for CampusNexus CRM is further limited to Contact and Lead based campaigns.

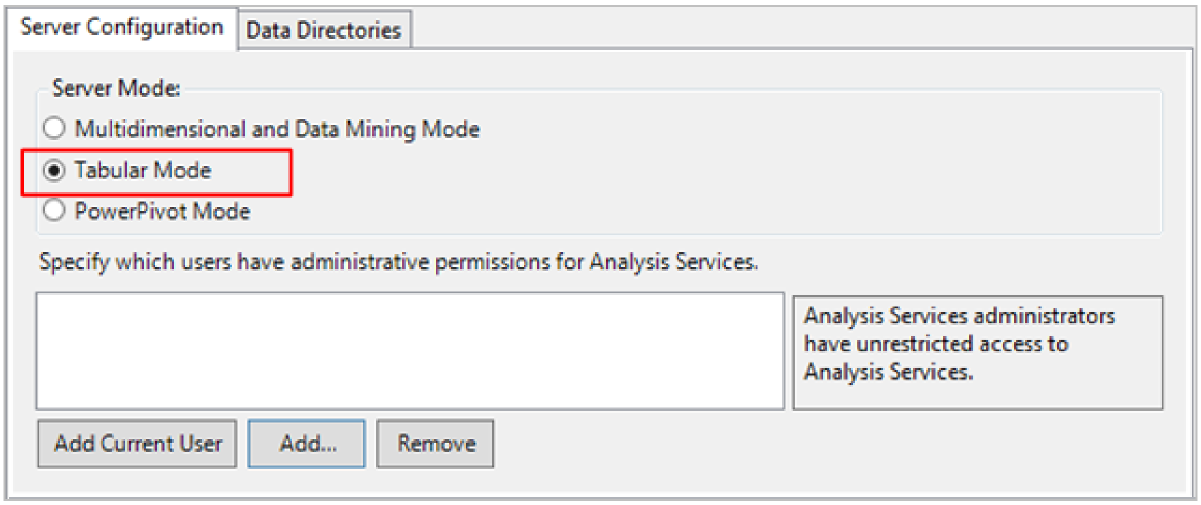
Prerequisites and Requirements

Prerequisites

The prerequisites for the installation of Student Analytics are as follows:

A. SQL Server components including:
   - Database Engine
   - SQL Server Analysis Services (SSAS)

   Important: SSAS must be installed in Tabular Mode.

   For more details on the SQL Server versions, see Hardware/Software Requirements. These requirements apply to all three layers located on-premises (source layer, data warehouse, and semantic layer).

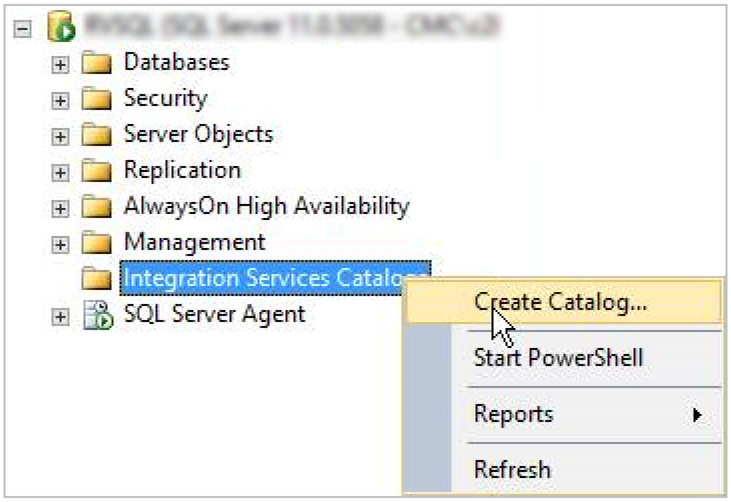
B. Student Analytics 5.2 and later requires "SQL Server 2017 CU 23" or higher on the SQL server where the Anthology Student database is installed.

   Installation Manager checks the CU version of the SQL server against the Data Warehouse line item for the Anthology Student database. Installation Manager does not check the CU version against CampusNexus CRM database.

C. Initial SSISDB catalog on the same server as the data warehouse.

   To create the initial SSISDB catalog:

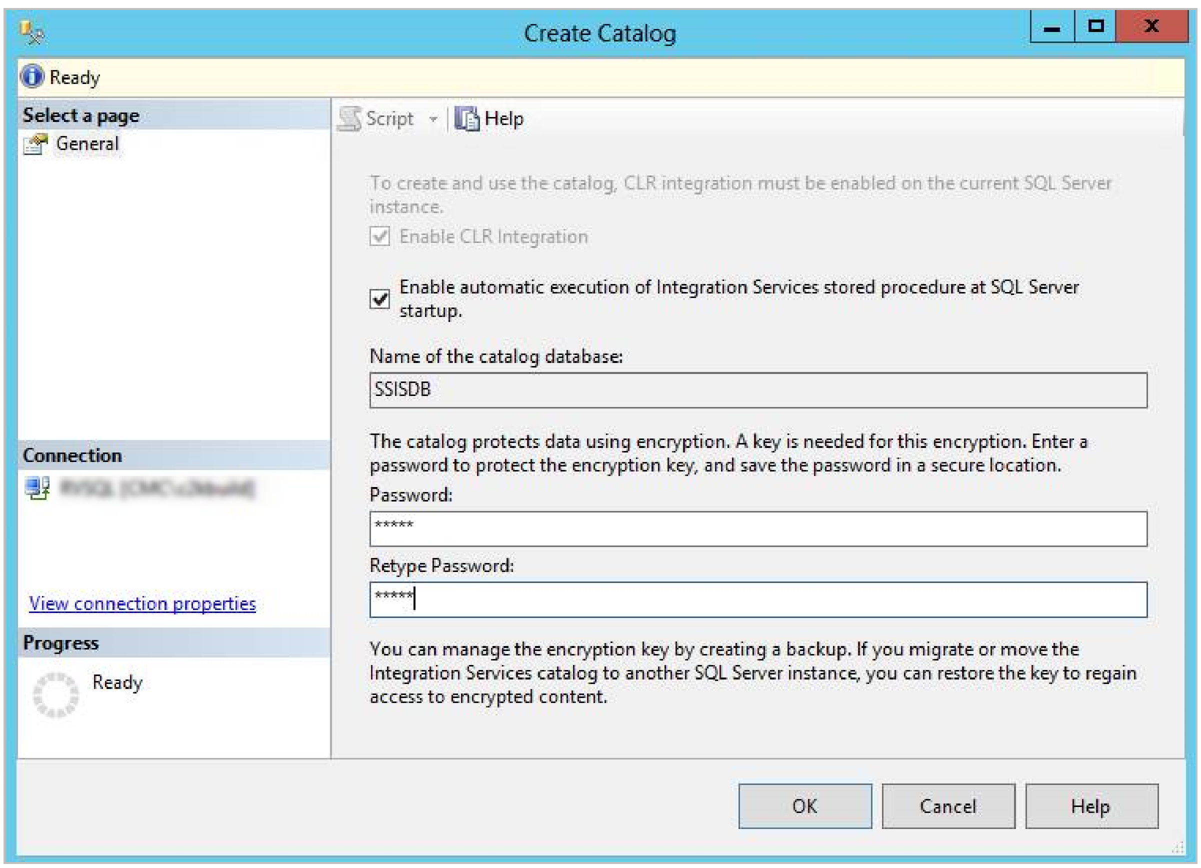
   1. Open **SQL Server Management Studio** and connect to the data warehouse server.
   2. Right-click on **Integration Services Catalog** and select **Create Catalog**.



3. Select **Enable automatic execution of Integration Services stored procedure at SQL Server startup**.

4. Specify the **Name** of the catalog database.

5. Enter the **Password** and click **OK**.



If an error related to the common language runtime (CLR) component occurs, run this script at the server level:

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE;
GO
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

D. Power BI Desktop (free authoring tool from Microsoft; see https://powerbi.microsoft.com/en-us/desktop).

E. Power BI Pro subscription with tenant and initial user. See Power BI Subscription.

   The Microsoft Power BI Reporting layer requires that customers first purchase an appropriate Power BI license through Microsoft. Customers are encouraged to contact their Account Manager if they are interested in implementing Power BI for Student Analytics reporting.

F. Microsoft On-Premises Data Gateway (enables Power BI to connect to on-premises SQL Server Analysis Services instances; see https://powerbi.microsoft.com/en-us/downloads).

G. Adequate drive space for the data warehouse.

   We recommend using separate servers for each of the three layers located on-premises (source layer, data warehouse, and semantic layer). This ensures that the resources required to support each layer do not compete with each other.

H. If CampusNexus CRM is the source database, install the Higher Education Foundation Pack (see Higher Ed) **and enable Campaign Support for the Lead Object** (see CampusNexus CRM product documentation). Also refer to the Port Matrix attached to Ports Used by CRM.

Permissions

The user installing Student Analytics must have:

- Administrator permissions on all machines where Student Analytics components are installed
- An account with sysadmin rights on all SQL Service instances associated with the Student Analytics installation

Installing Student Analytics enables the “Change Data Capture” feature on the Student DB and creates a user “cdc” and assigns the db_owner group level permission. The user “cdc” should be member of the db_owner group.

The following SQL Server services should be configured to run under the context of a **domain** account:

- SQL Server
- SQL Server Agent
- SQL Server Analysis Services
- SQL Server Integration Services

Service Account	Access to Source Database Required	Access to Data Warehouse database (DW) Required	Access to Semantic Model Required
SQL Server (DW)		Yes, db_owner	
SQL Server Agent (DW)	Yes, db_owner	Yes, db_owner	Yes, Server Administrator
SQL Server Analysis Services	No	Yes	Yes
SQL Server Integration Services	Yes, db_owner	Yes, db_owner, ssis_admin on SSISDB	No

Note: The SSIS packages are deployed in the Integration Services Catalog, and they are executed in the context of the SQL Server Agent Service Account. Therefore, ensure that the SQL Server Agent Service Account has permissions to execute the packages.

Hardware/Software Requirements

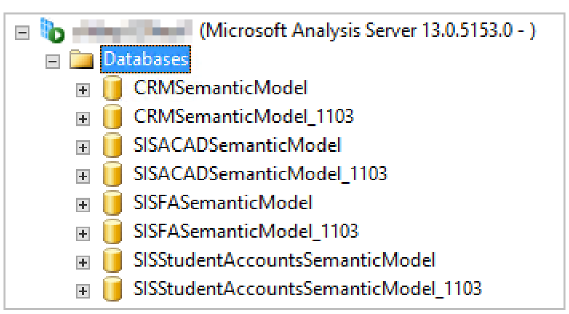
Use the Analytics 5.5.0 Size Estimation Worksheet.xlsx to determine the minimum hardware requirements, amount of disk space, and RAM required for your installation of Student Analytics. The spreadsheet is also available on the FTP site.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Database Renaming During Upgrade to Analytics 3.3 and Later

During the installation of Student Analytics 3.3 and later, if the compatibility level of the SQL database is less than 1200, existing Analysis database(s) will be renamed by appending the old compatibility level to the database name, and new Analysis database(s) will be created.

Example:



As part of the installation process, the roles and permissions will be migrated from the old database to the new database.

Customers need to review the old database(s) for any customizations and migrate them to new database before dropping the old database(s).

Global Settings

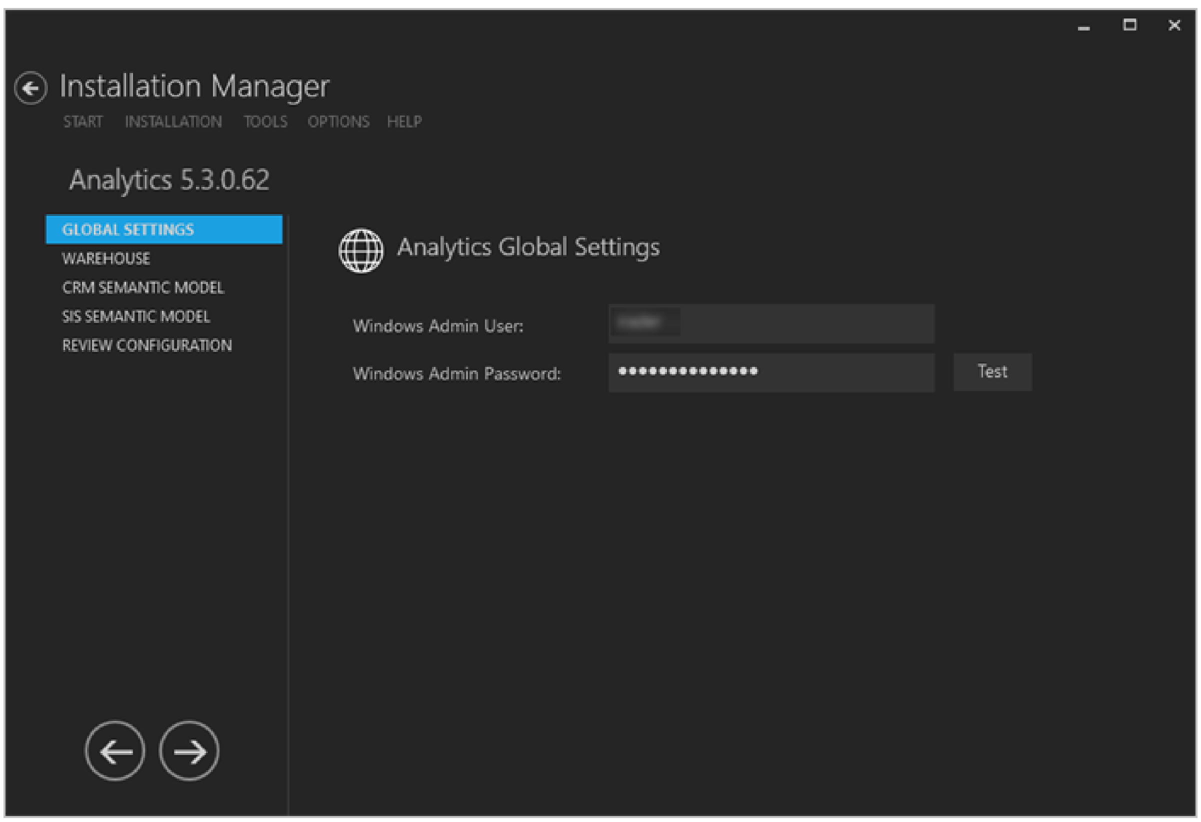
The Global Settings screen contains the user name and password of the system administrator performing the Student Analytics installation. This user must have:

- Administrator permissions on all machines where Analytics components are installed
- An account on all databases associated with the Analytics installation
- Sysadmin rights on all databases associated with the Analytics installation.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

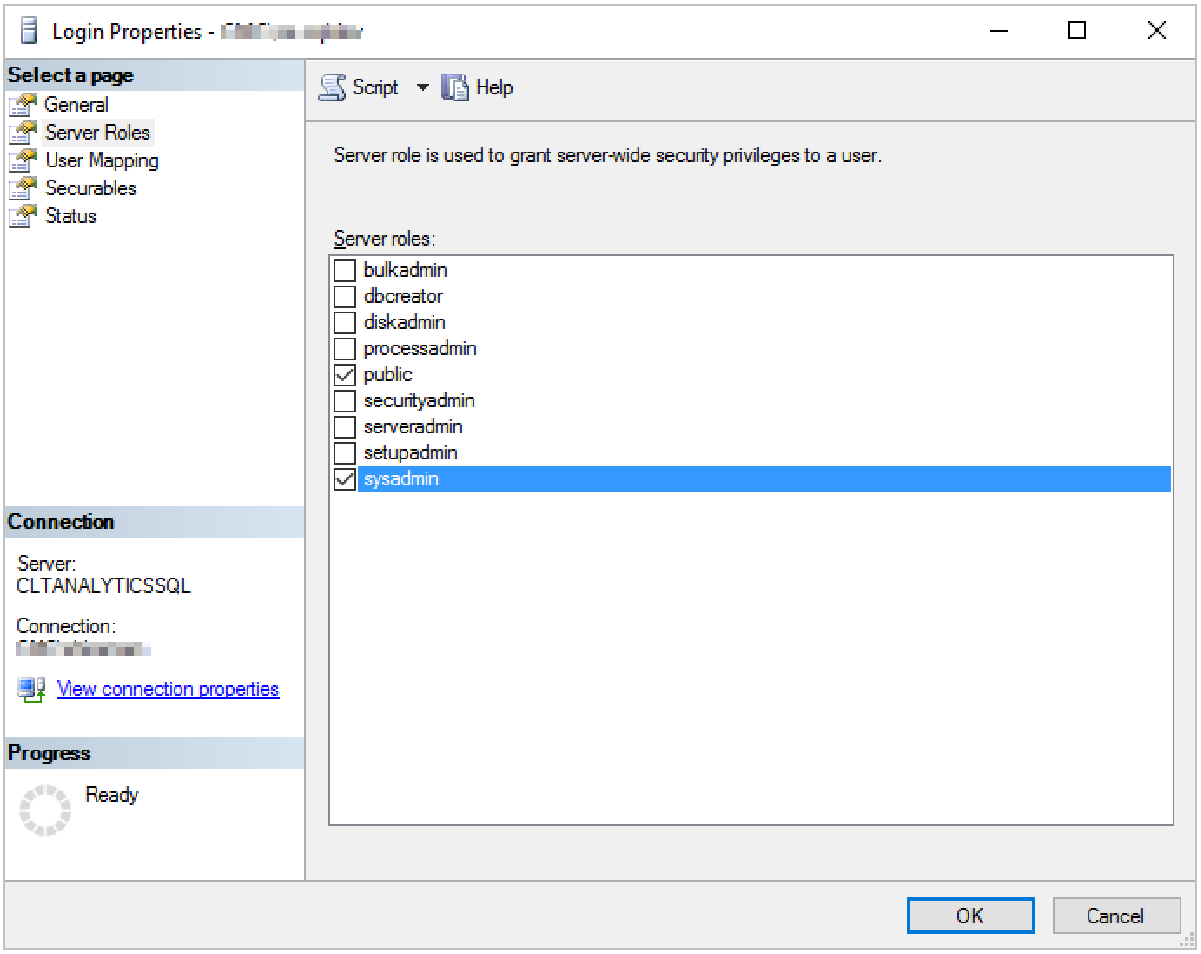
1. In the Start screen of Installation Manager, click the **Analytics** tile. The Analytics Global Settings screen is displayed.



2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer where the installation will occur. Depending on your network environment, specify one of the following:

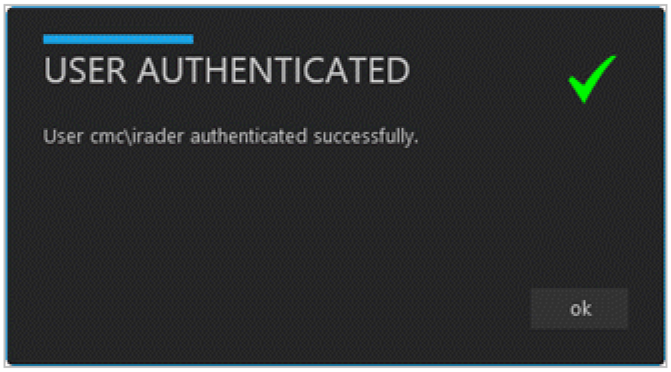
- User name
- Domain\User name
- Email address of Admin User

Important: This user must have sysadmin permissions on the SQL Server instances / SQL Server Analysis Services where warehouse databases and semantic model databases are installed. To check permissions, access SQL Server Management Studio, select the database, and navigate to **Security > Logins > Properties > Server Roles**. Ensure that the **sysadmin** role is selected.



3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.



5. If the user is authenticated, click **OK** and click  to continue.

Warehouse

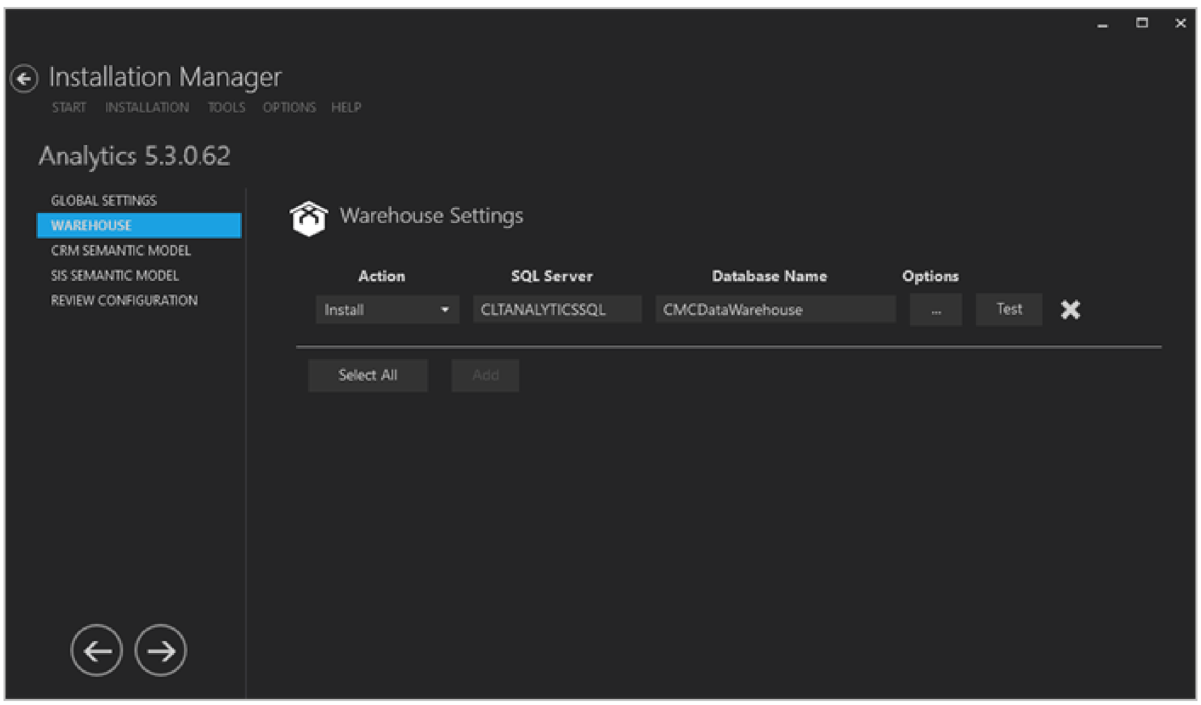
This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the database and configuration options for the Student Analytics Warehouse. The Warehouse assembles data dispersed in various data sources by combining all relevant data. SQL Server Analysis Services (SSAS) connects to the Warehouse database containing the denormalized data from the source database and allows Student Analytics users to query and view the data from many different angles.

The SQL Server Integration Services (SSIS) Catalog is installed with the Warehouse. The SSIS Catalog is the place where you manage SSIS projects and packages, including the configuration and monitoring of Integration Services server operations. SSIS Catalog objects (projects, packages, parameters, environments, and operational history) are stored in the SSISDB.

Note: The initial SSISDB catalog must be created before installing the Warehouse. See Prerequisites and Requirements.

Set Up the Warehouse

1. In the Installation menu, click **Warehouse**. The Warehouse Settings screen is displayed.

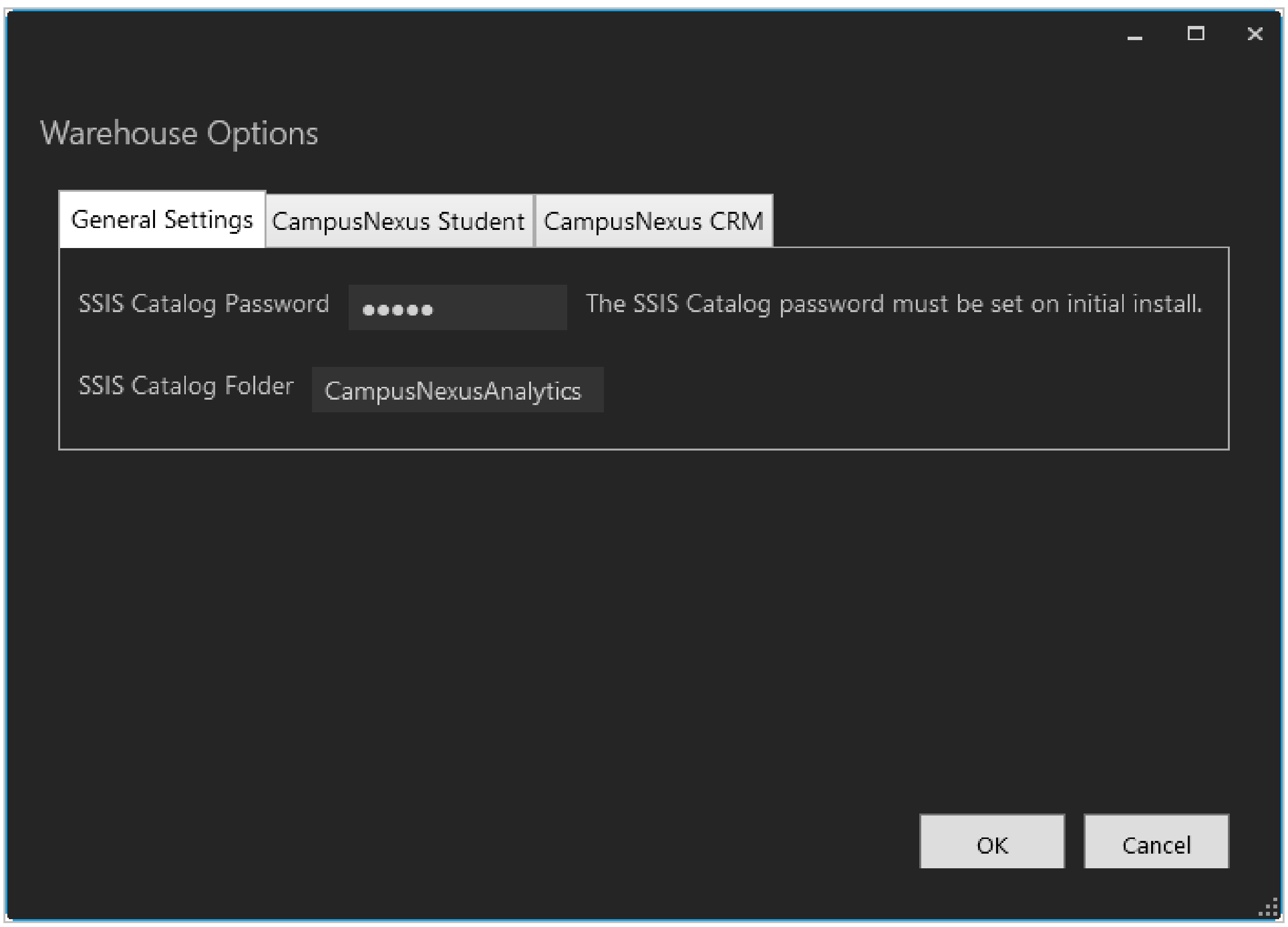


2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:

- **None** – Performs no action.
- **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

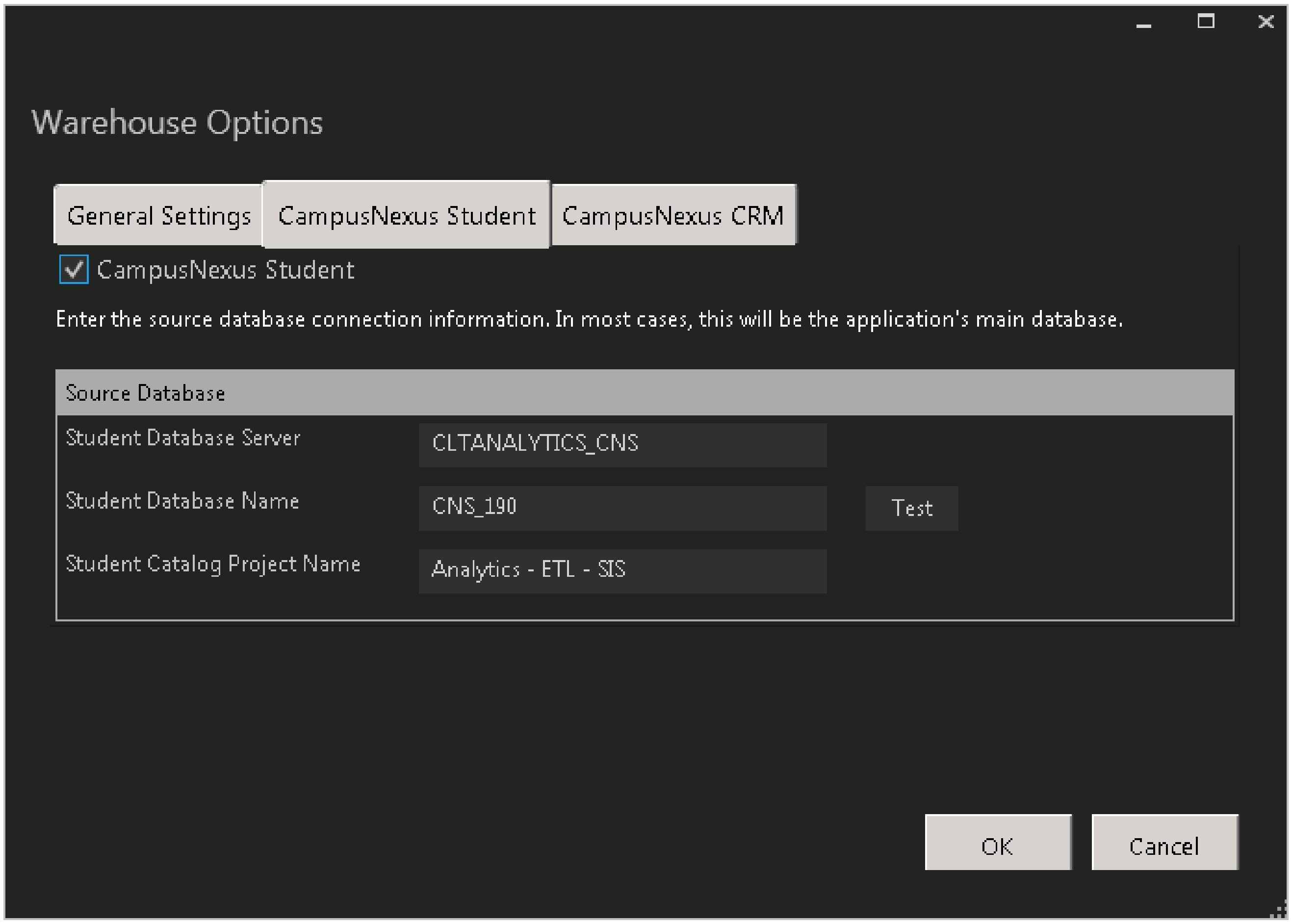
Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. In the **Database Server** field, enter the SQL server name. If the database server contains multiple SQL server instances, also specify the instance name, e.g., <server name\instance>.
5. Specify the **Database Name** of the Warehouse database to be created or upgraded.
6. Click  to view and edit the Options form.



Warehouse Options - General Settings Tab

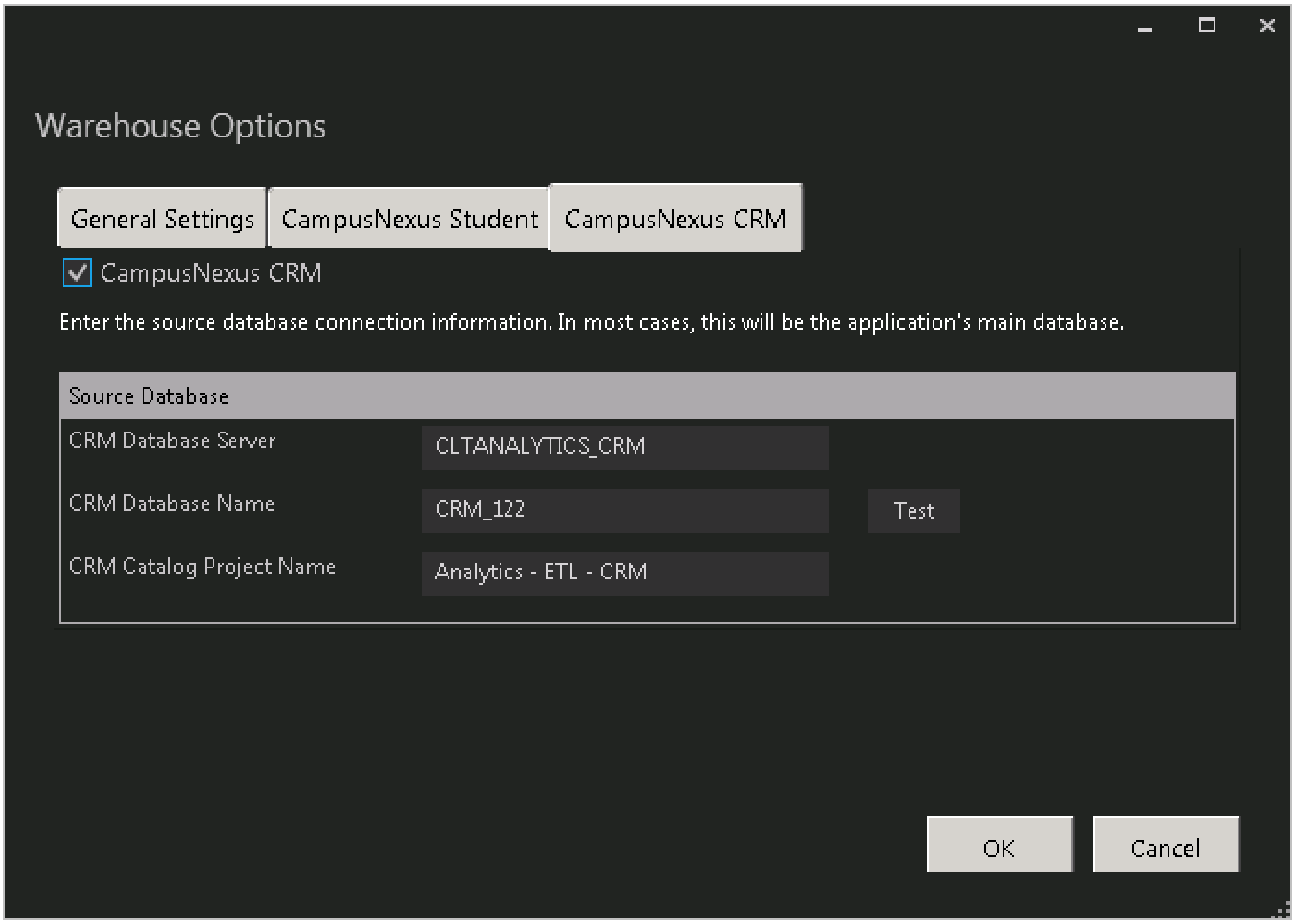
Field	Description
SSIS Catalog Password	Password of the SQL Server Integration Services (SSIS) Catalog.
SSIS Catalog Folder	Name of the folder to be created that will hold the SSIS packages and projects. Specify unique names if multiple projects are deployed on the same SQL Server instance.



Warehouse Options - Anthology Student Tab

Field	Description
Anthology Student	Select this check box if the source database is an Anthology Student database. The associated fields are enabled.
Student Database Server	Name of the Anthology Student database server used by Student Analytics. Student Analytics 5.2 and later requires "SQL Server 2017 CU 23" or higher on the SQL server where the Anthology Student database is installed.
Student Database Name	Name of the Anthology Student database used by Student Analytics. Click **Test** to verify access to the database.

Field	Description
Student Catalog Project Name	Name of the Anthology Student Catalog Project which holds the SSIS packages, for example, Analytics - ETL - SIS.



Warehouse Options - CampusNexus CRM Tab

Field	Description
CampusNexus CRM	Select this check box if the source database is a CampusNexus CRM database. The associated fields are enabled.
CRM Database Server	Name of the CampusNexus CRM database server used by Analytics.
CRM Database Name	Name of the CampusNexus CRM database used by Analytics. In most cases this will be the application's main database. Click **Test** to verify access to the database.
CRM Catalog Project Name	Name of the CampusNexus CRM Catalog Project which holds the SSIS packages, for example, Analytics - ETL - CRM.

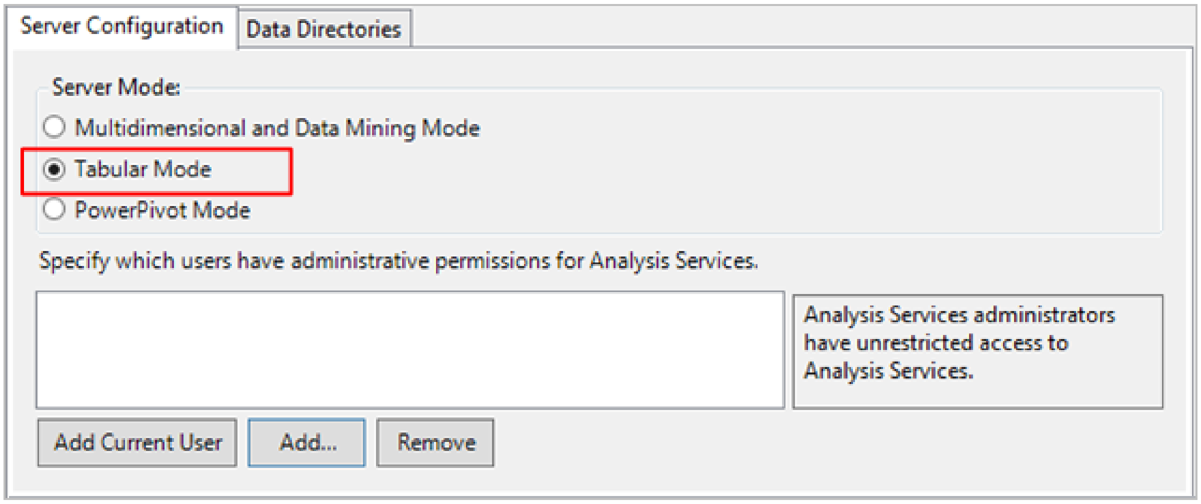
7. Click **OK** to save changes on the Options form. The form is closed.

8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

CRM Semantic Model

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and configuration options for the Semantic Model used by Analytics.

Important: SSAS must be installed in Tabular Mode.



Set Up the CRM Semantic Model

Compatibility Level for Semantic Model Databases

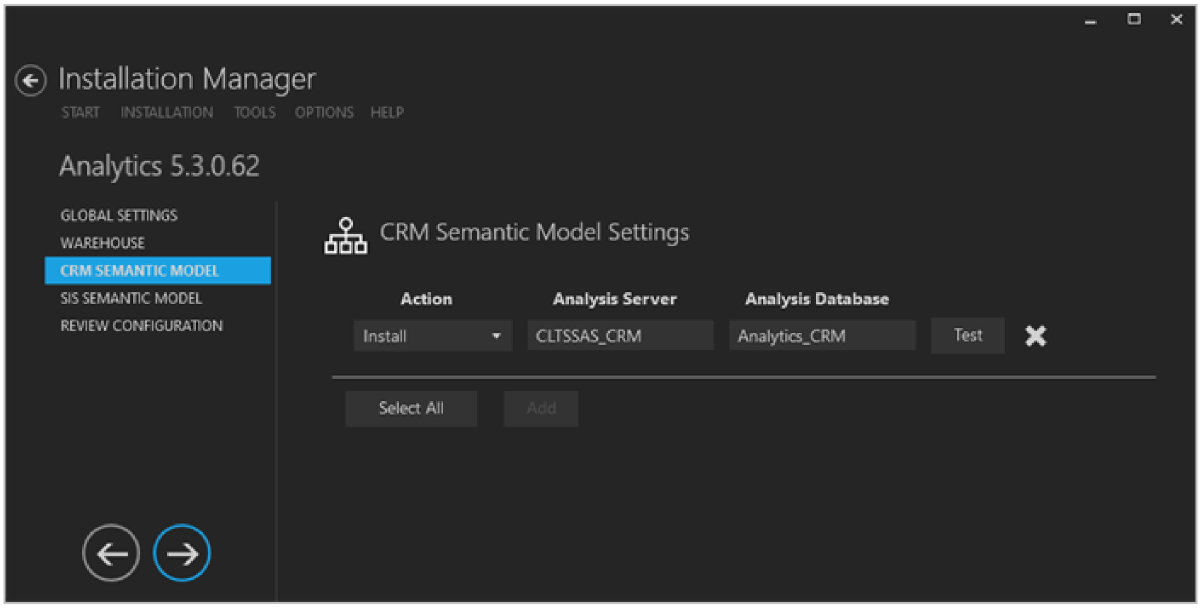
The SQL Server Analysis Server compatibility level for all the semantic model databases in the prior versions of Analytics, 3.2.x and earlier, was 1103 (SQL Server 2012 SP1).

When upgrading earlier versions of Analytics to 3.3 or later, you need to install new semantic model databases.

Or, to upgrade the exiting semantic model databases, first change the compatibility level manually to 1200 (SQL Server 2016 or SQL Server 2017 for Analytics 4.0) using SQL Server Data Tools (SSDT), and then upgrade to Analytics 3.3 or later using Installation Manager.

Before upgrading to Analytics 3.3 or later, please review Database Renaming During Upgrade to Analytics 3.3 and Later.

1. In the Installation menu, click **CRM Semantic Model**. The CRM Semantic Model Settings screen is displayed.



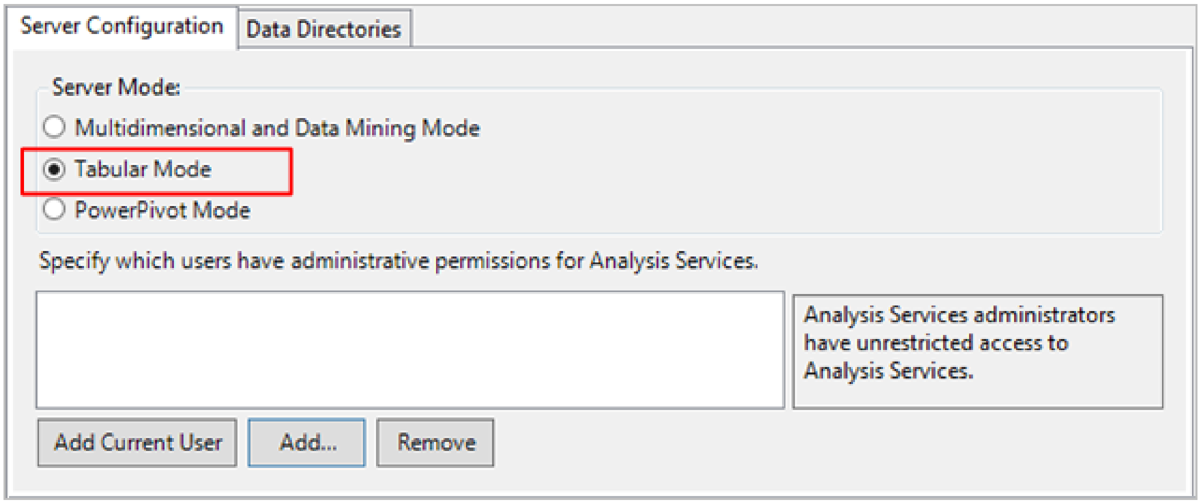
2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. In the **Analysis Server** field, enter the SSAS server name. If the database server contains multiple SSAS server instances, specify the instance name, e.g., <server name\instance>.
5. In the **Analysis Database** field, enter the name of the database to be created or upgraded in the SQL Server Analysis Service.
6. Click  to delete a selected line.
7. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
8. If all tests pass, click .

SIS Semantic Model

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and configuration options for the Semantic Model used by Analytics.

Important: SSAS must be installed in Tabular Mode.



Set Up the SIS Semantic Model

Compatibility Level for Semantic Model Databases

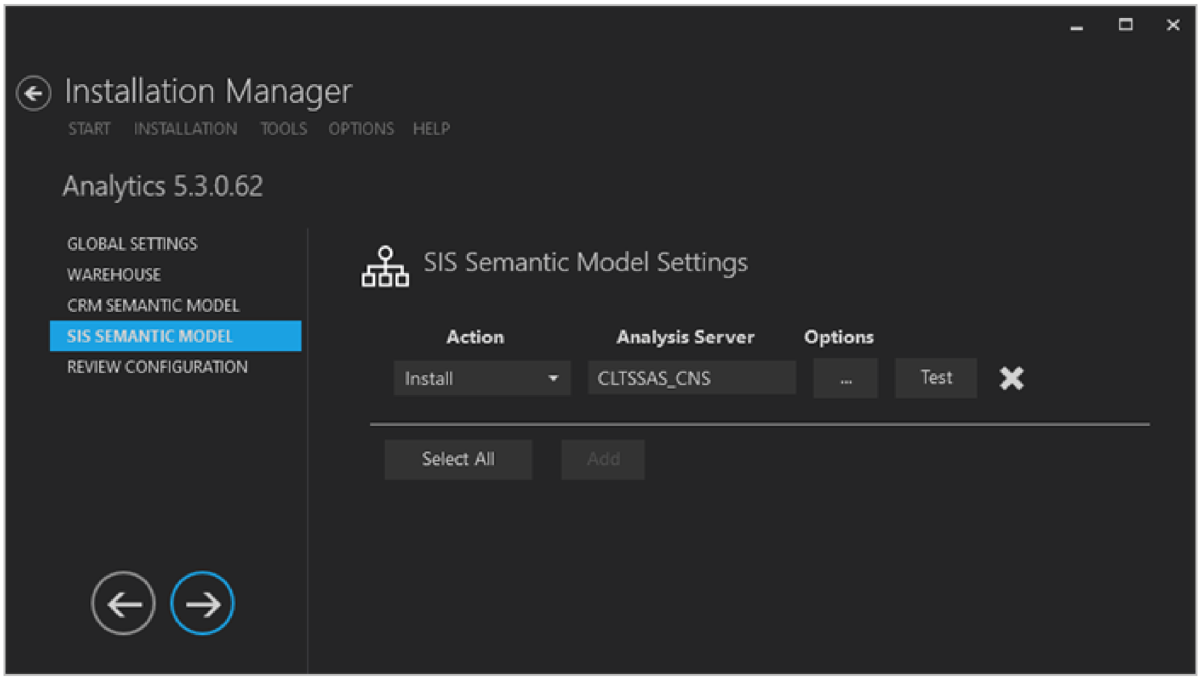
The SQL Server Analysis Server compatibility level for all the semantic model databases in the prior versions of Analytics, 3.2.x and earlier, was 1103 (SQL Server 2012 SP1).

When upgrading earlier versions of Analytics to 3.3 or later, you need to install new semantic model databases.

Or, to upgrade the exiting semantic model databases, first change the compatibility level manually to 1200 (SQL Server 2016 or SQL Server 2017 for Analytics 4.0) using SQL Server Data Tools (SSDT), and then upgrade to Analytics 3.3 or later using Installation Manager.

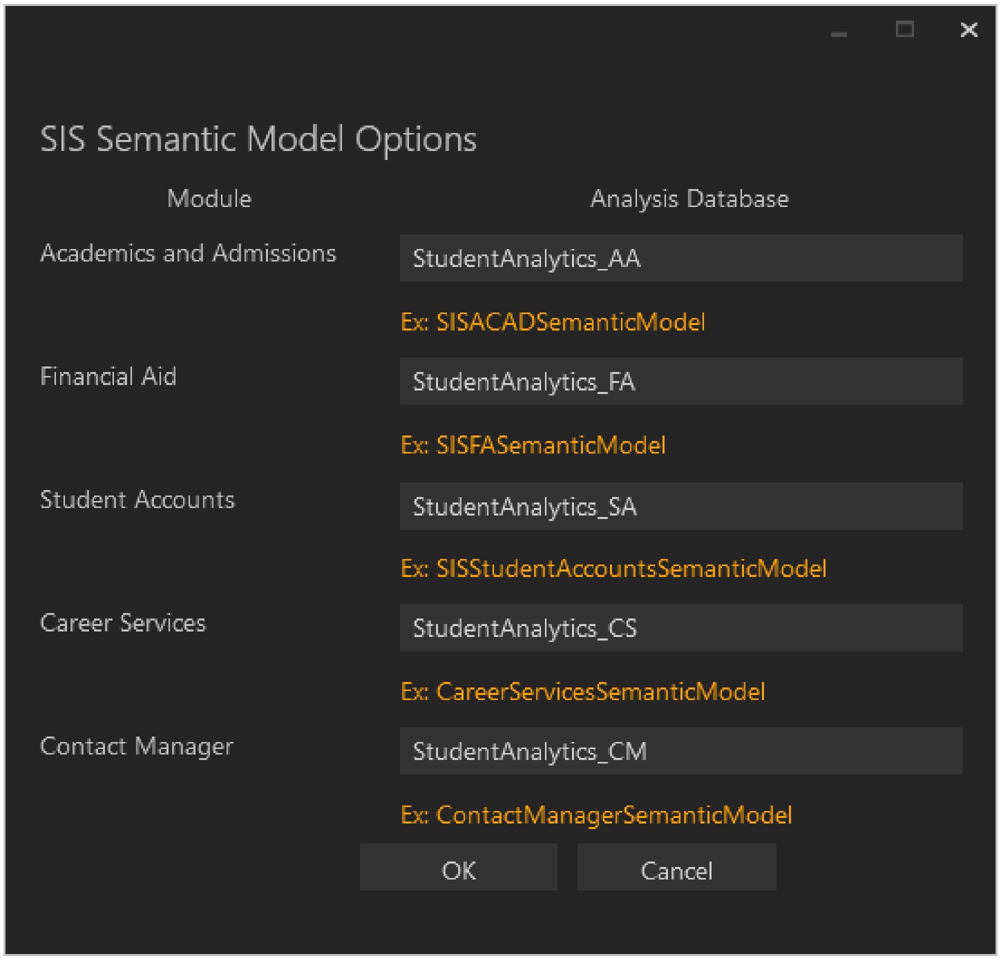
Before upgrading to Analytics 3.3 or later, please review Database Renaming During Upgrade to Analytics 3.3 and Later.

1. In the Installation menu, click **SIS Semantic Model**. The SIS Semantic Model Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. In the **Analysis Server** field, enter the SSAS server name. If the database server contains multiple SSAS server instances, specify the instance name, e.g., <server name\instance>.
5. In the **Analysis Database** field, enter the name of the database to be created or upgraded in the SQL Server Analysis Service. The Analysis Database name should be different from the name of the database specified for CRM Semantic Model.
6. Click  to delete a selected line.
7. Click  to view and edit the Options form. The SIS Semantic Model Options form is displayed.



Specify the names of the analysis databases for the following Anthology Student modules:

- Academics and Admissions
- Financial Aid
- Student Accounts
- Career Services
- Contact Manager

8. Click **OK** to save changes on the Options form. The form is closed.

9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

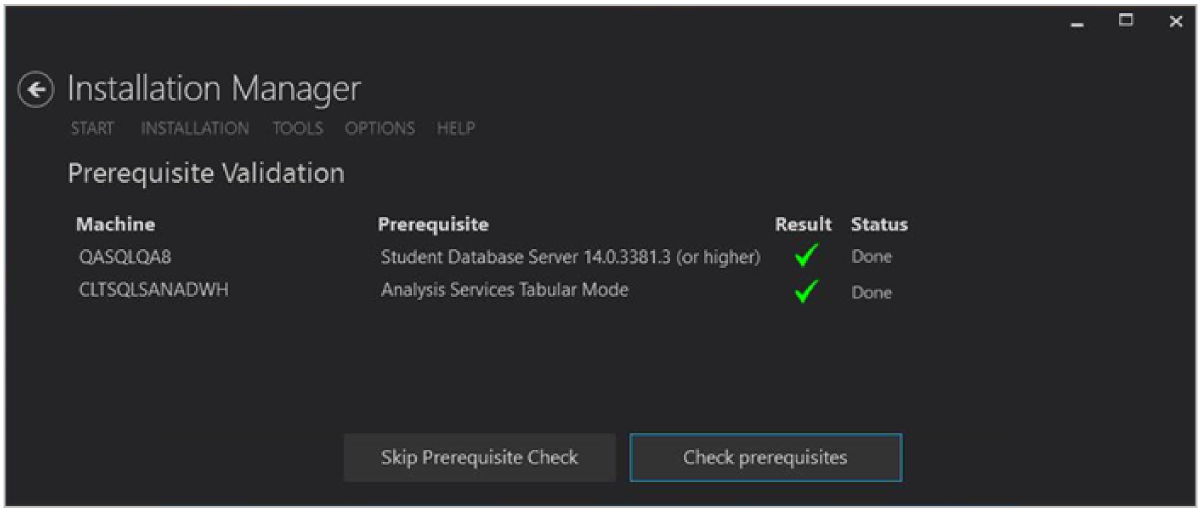
10. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

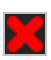
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.



2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

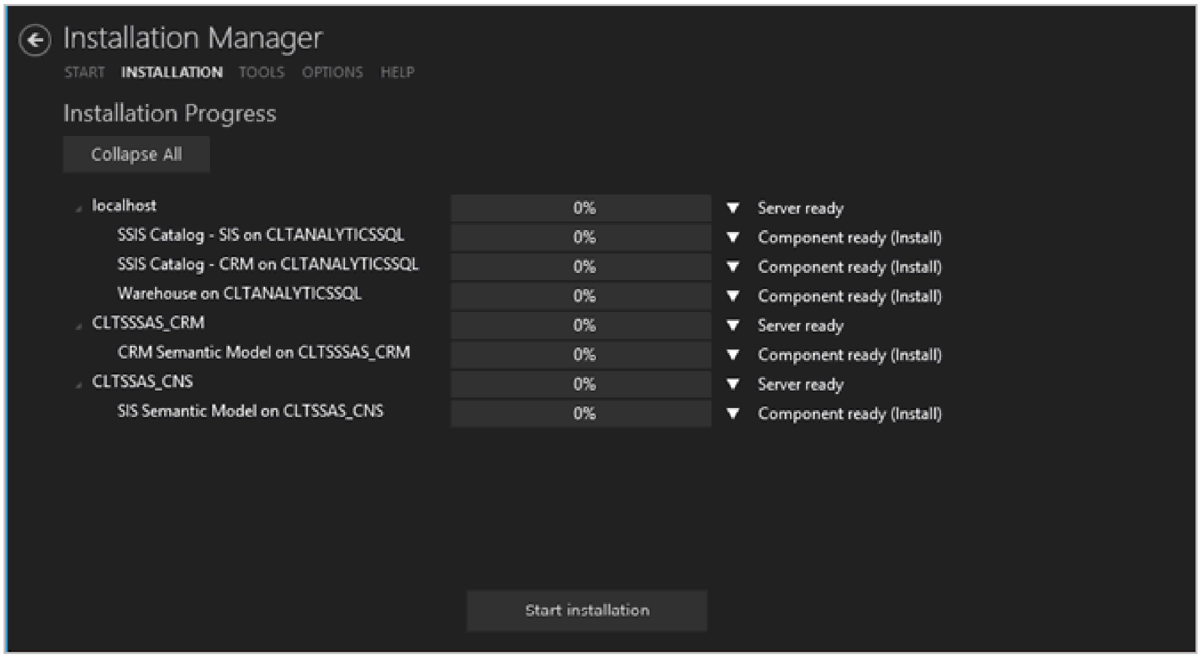
    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.

3. Click **Start Installation** on the Installation Progress screen. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.



4. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

5. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

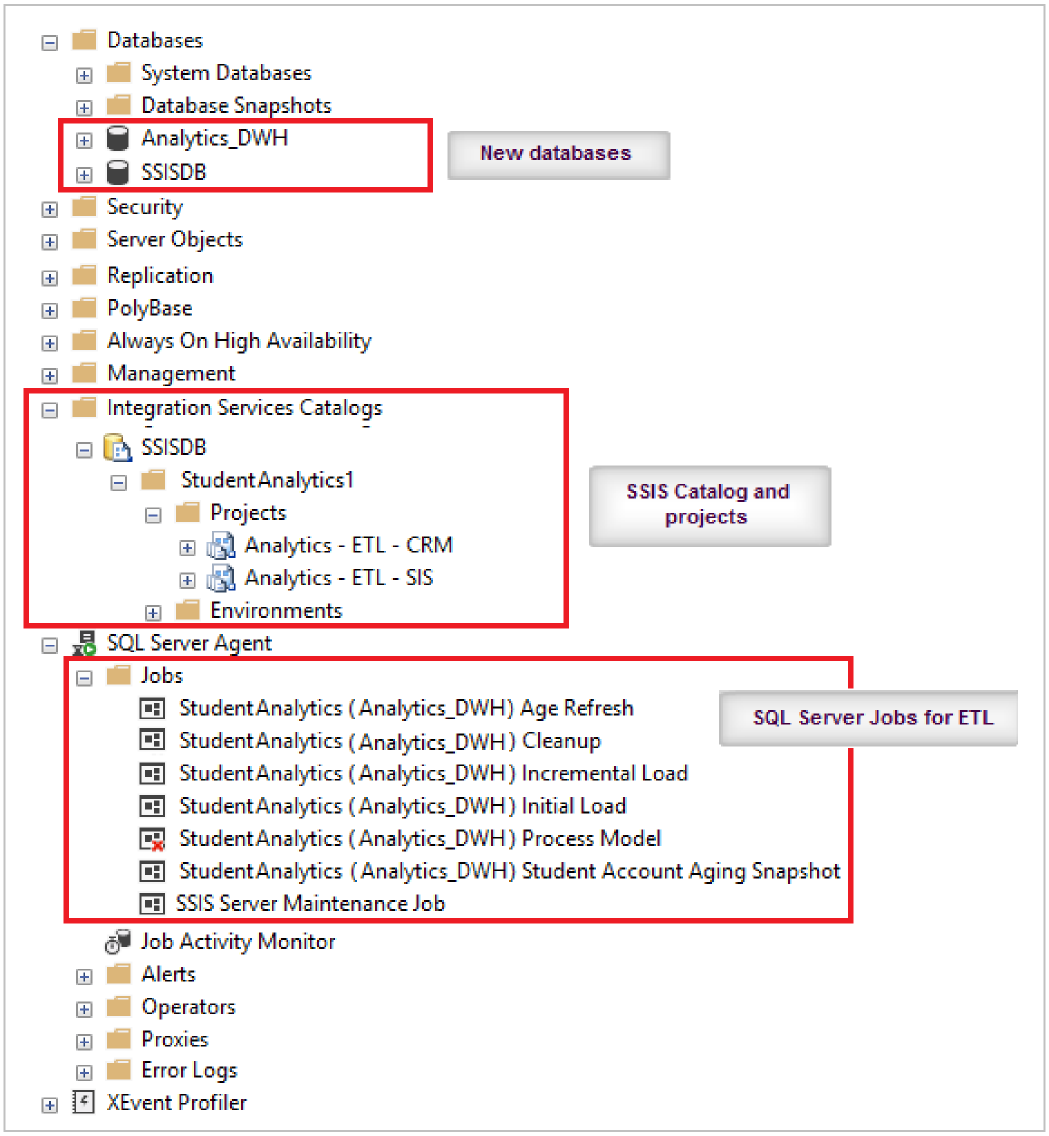
Installation Result

The Analytics installation result described in this example is as follows:

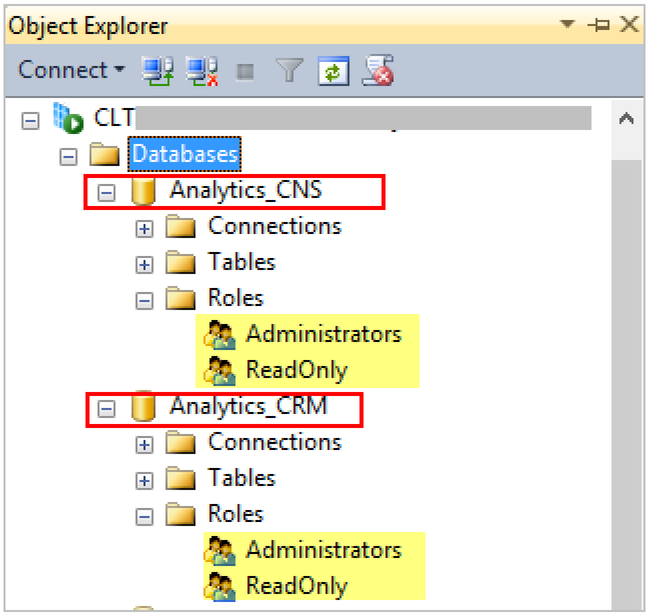
- The **Warehouse** and the **Integration Services Catalog** are installed on server CLTANALYTICSSQL. The figure below shows the following objects were created:
  - Warehouse database
  - SSISDB database (SSIS Catalog database)
  - SIS and CRM catalog projects under the SSIS Catalog folder that contain the SSIS packages

    In this example, 'CampusNexusAnalytics' was the SSIS Catalog folder name specified. The SIS and CRM catalog projects were specified as 'Analytics – ETL – CRM' and 'Analytics – ETL – SIS'.
  - SQL Server Jobs for the ETL process

    Analytics 4.2 enables all jobs upon creation except the "StudentAnalytics (<data_warehouse_name>) Process Model", because processing of Semantic Model databases is now part of the Incremental Load job. The Process Model job can be used to manually process Semantic Model databases when needed.

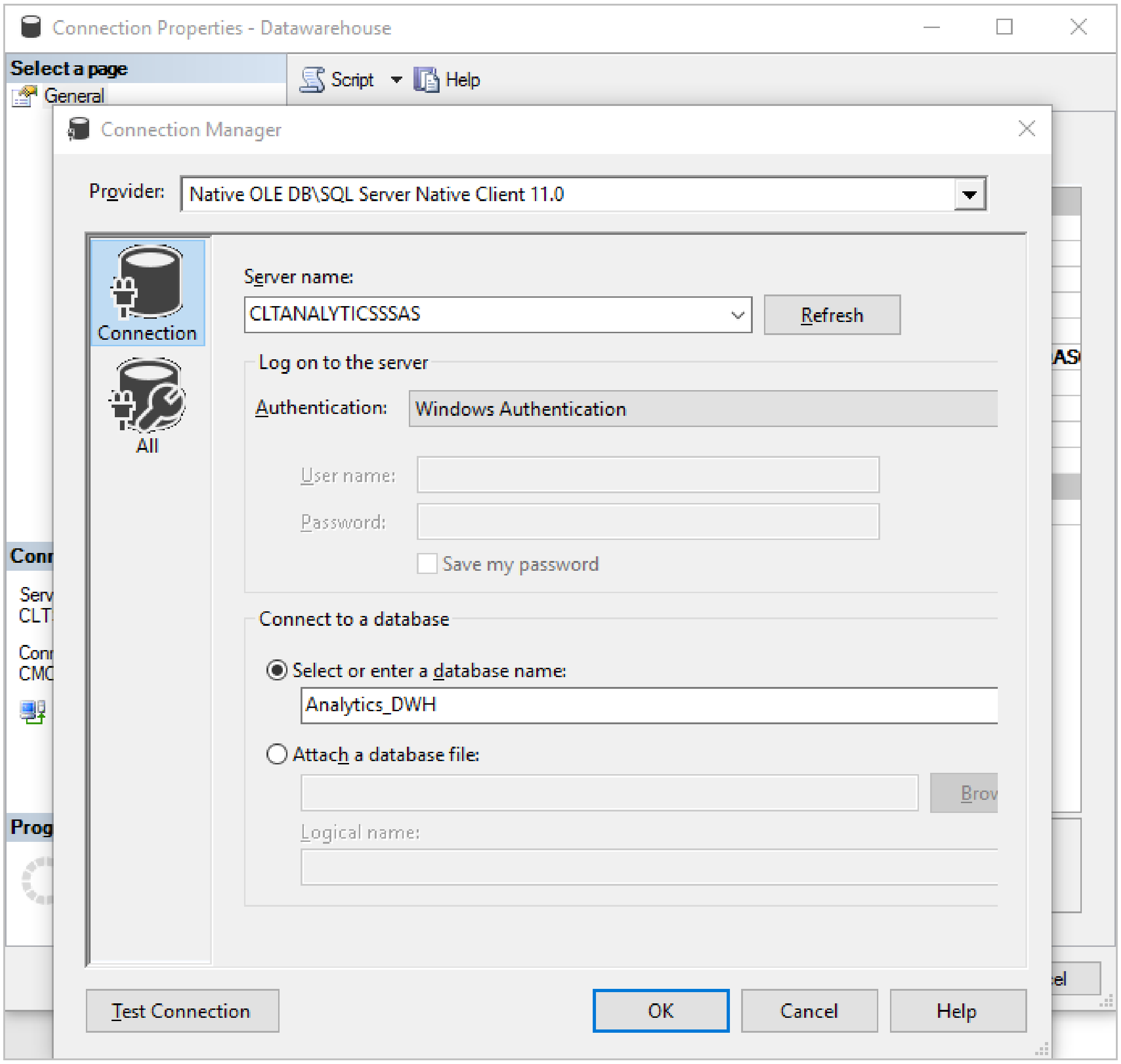


- The **Semantic Models** are installed on server CLTANALYTICSSSAS. The figure below shows two such semantic model databases:



- The Analysis Service on CLTANALYTICSSSAS contains a connection string that points to the Warehouse database: CMC\BusinessAnalystGroup.

  Navigate to **Connections > DataWarehouse > Properties** and click the **ellipsis** in the Connection field to view the connection string in the Connection Manager window.



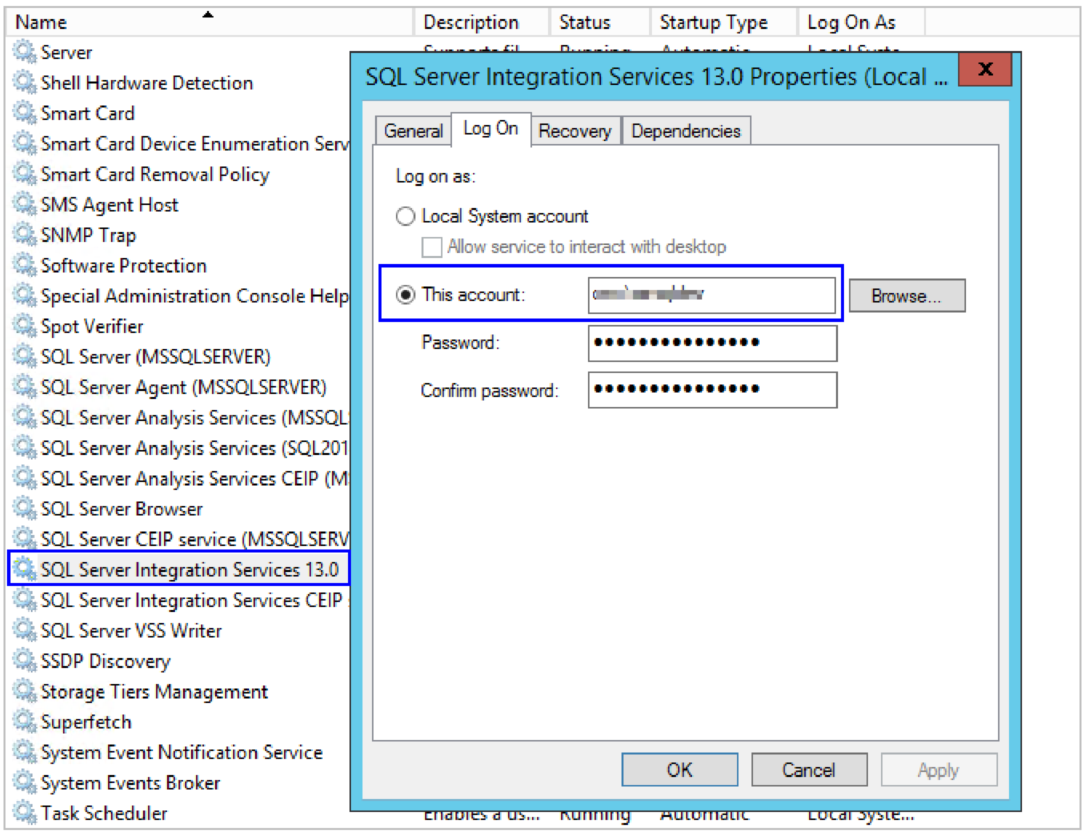
- To view the installation log, refer to View Logs.

ETL User Permissions

After completing the installation of Analytics, set permissions for the SQL Server Integration Services (SSIS) and SQL Server Agent Services (SSAS) service accounts.

SSIS Service Account Permissions

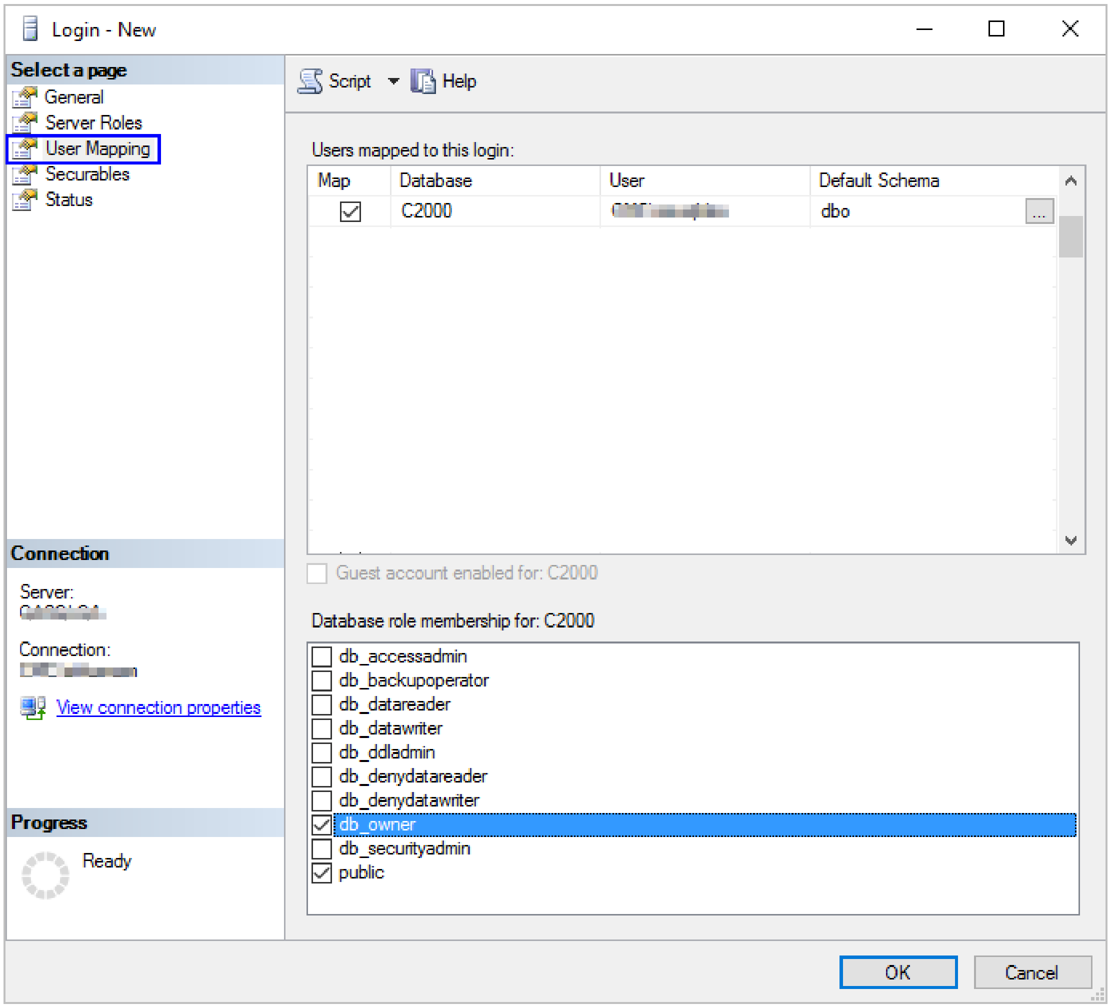
1. Open **Windows Services Manager** on the Data Warehouse machine. Identify the service account configured for SQL Server Integration Services from the Properties window as shown in the following image:



2. Open **SQL Server Management Studio** and connect to source database server (SIS and/or CRM).

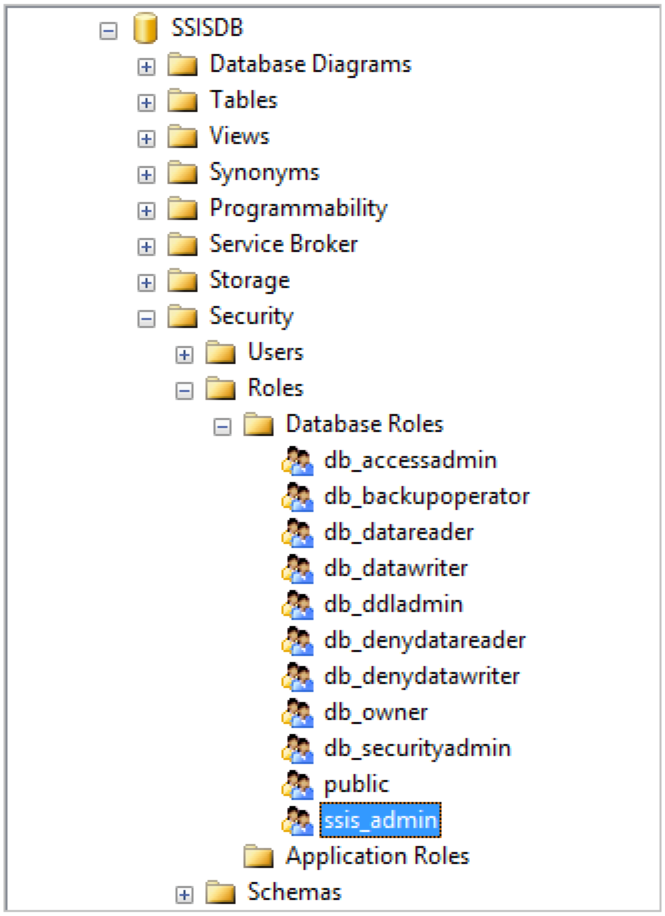
3. Navigate to **Security >> Login**.

4. Right-click **Login** and click **New Login** to create a user with the service account identified in the step 1. Set **dbo_owner** permission to the source database (SIS/CRM) as shown below. If the login already exists, make sure that a minimum of db_owner permission is set on all source databases (SIS and/or CRM).



5. Similarly, follow the steps 2, 3 and 4 for the Data Warehouse database on the Data Warehouse SQL Server instance.

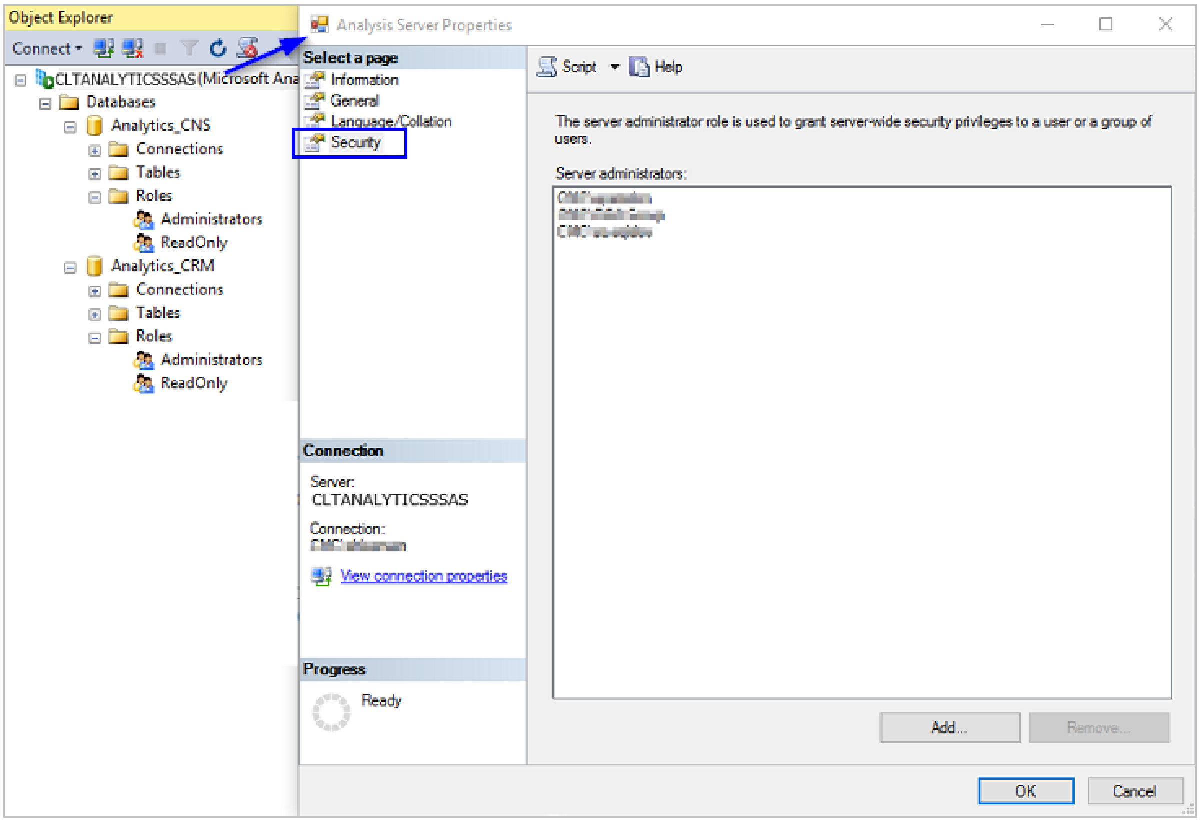
6. Navigate to the SSISDB database and set the SQL Server Integration Services Account, SQL Server Agent Services Service Account to the **ssis_admin** role.



SSAS Service Account Permissions

1. Ensure that the SQL Server Agent Services logon account on the data warehouse server has sufficient privileges to log on to and process the semantic model database on the Analysis Services instance. If the SQL Server Agent Services logon account and SQL Server Analysis Services logon account are not the same, add the SQL Server Agent Services logon account to the Server Administrator role in the Analysis Server Properties, Security page:

a. Open SQL Server Management Studio and connect to the **SQL Server Analysis Services** instance.



b. Right-click the server name and select **Properties** to open the Analysis Server Properties window.

c. Navigate to the Security page and click **Add** to enter the SQL Server Agent Services logon account.

d. Click **OK**.

2. Open the SQL Server Management Studio and connect to source database server (SIS and/or CRM).

3. Navigate to **Security >> Login**.

4. Right-click **Login** and click **New Login** to create a user with the SQL Server Agent Service account. Set **dbo_owner** permission to the source database (SIS/CRM). If the login already exists, make sure that a minimum of db_owner permission is set on all source databases (SIS and/or CRM).

Postinstallation Tasks

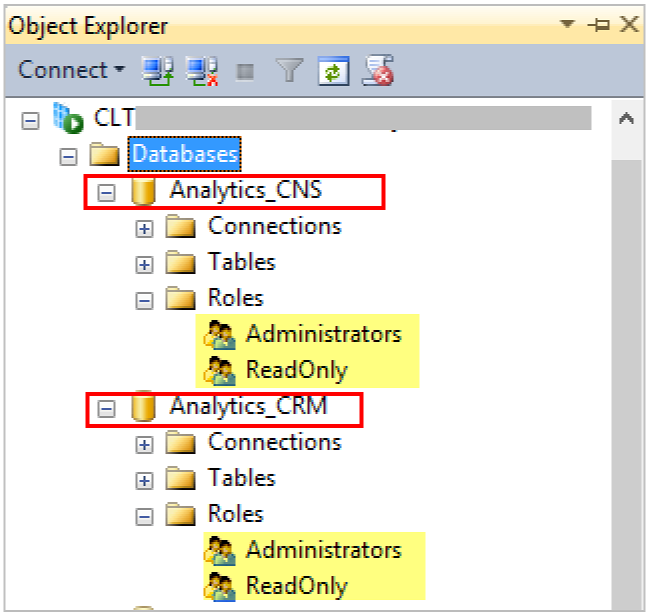
After completing the installation of Analytics and setting up the SSIS and SSAS service accounts, perform the postinstallation tasks.

Assign Roles and Permissions for Analytics Users and Groups

Assign roles and permissions in the Semantic Model database to enable users to access the Semantic Model databases from the Analytics client interface (i.e., Power BI).

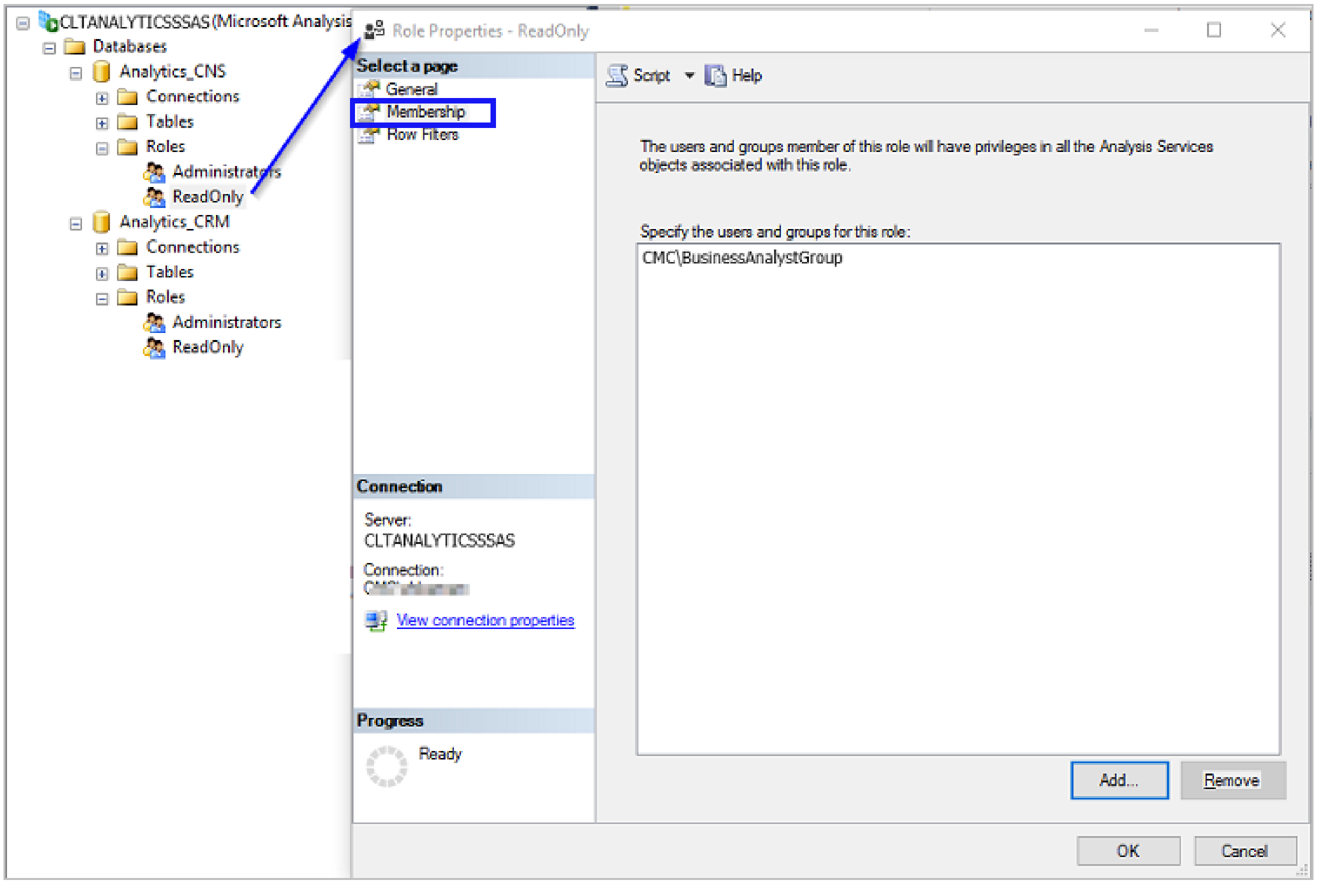
1. Launch **Microsoft SQL Server Management Studio** on the server that runs the SQL Server Analysis Services (SSAS).

2. Navigate to **Databases >***[SIS/CRM Semantic Model name]* **> Roles**.

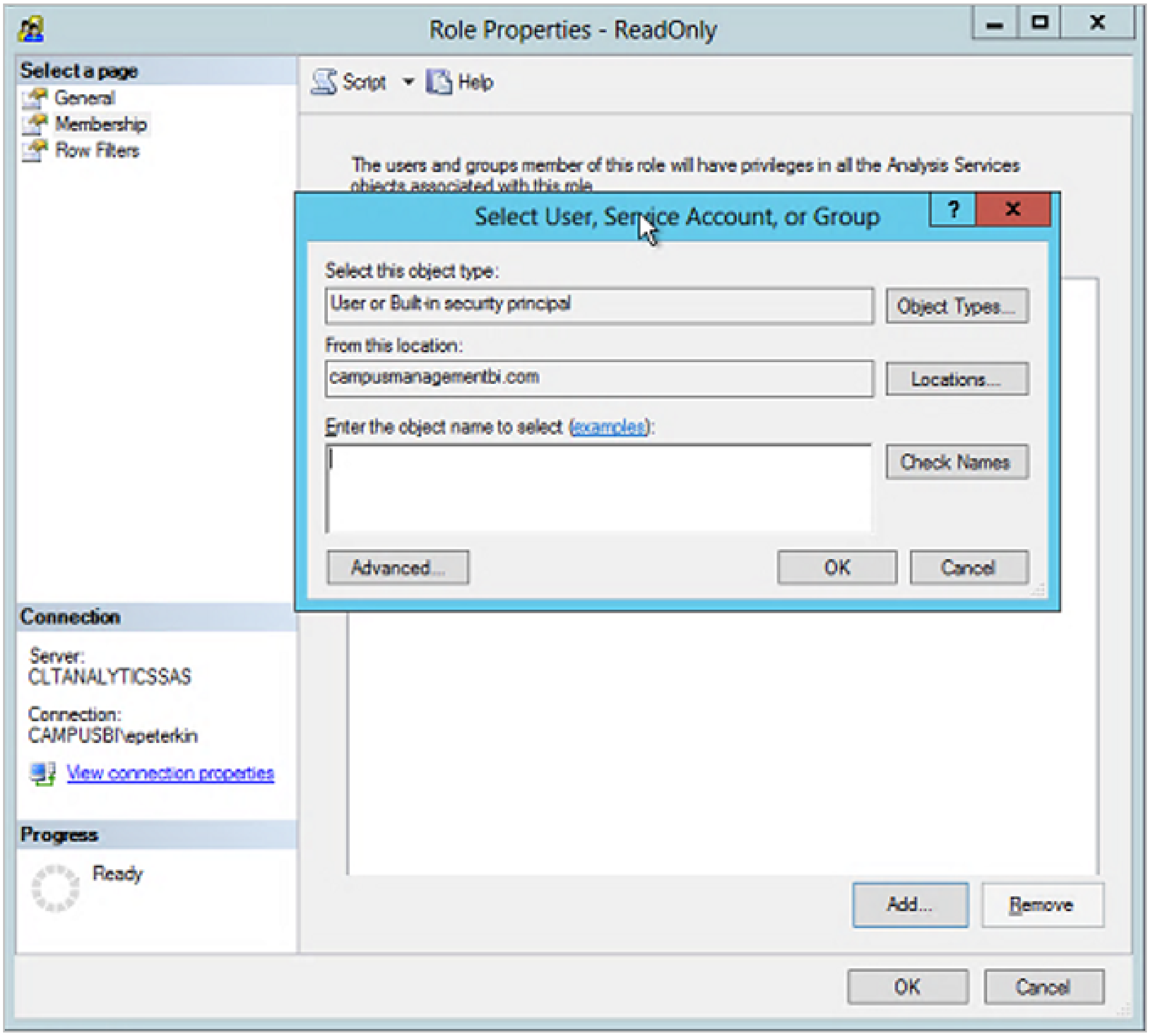
   

   The *Administrators* and *ReadOnly* roles are created by default. Add users to these roles as required. Users with *ReadOnly* roles can view data using Power BI but cannot make administrative changes to the SSAS database. Instead of creating individual users, you can create an Active Directory group and then add users to that group.

3. Right-click a role, select **Properties**, select the **Membership** page, and click **Add** to add the Windows group and user accounts that require access.



4. In the Select Users or Groups window, enter the name of an Analytics user, and click **Check Names**. Click **OK** to add the users or groups.



5. Repeat the previous steps for each Analytics user.

Configure AcademicYearOffset, FiscalPeriodMonthOffset, and CleanupRetentionDays

AcademicYearOffset

Use this configuration to set the Academic Year definition of an educational institution in the Date dimensions of the Datawarehouse. The AcademicYearOffset value is the month offset from January to the beginning of the Academic Year month. For example, if the Academic year begins with September, the AcademicYearOffset value is 8 (calculated as Begin Month Number minus 1). By default, the value of AcademicYearOffset value is set to 8 in the configuration table when the Analytics Datawarehouse is installed. The AcademicYearOffset value must be set correctly based on the Academic Year definition of an educational institution after the Analytics Datawarehouse installation or upgrade (Post Installation steps).

To change the AcademicYearOffset value and update the Date dimensions records, execute the below script on the Datawarehouse database. The script can also be executed after running the “StudentAnalytics <datawarehouse database name> Initial Load” SQL Server job.

Along with configuring Academic Year offset, configure the “**Months in Academic Year Semesters**”. The default configuration is 2 semesters in an Academic Year and each semester will be of 6 months. If the educational institution has unequal semesters, use the below configurations to set the semesters in the Academic year. Up to three semesters can be configured for an Academic Year. For example, if the academic year has 3 semesters where the first semester is of 5 months, second semester is of 4 months and third semester is of 3 months, then set the **MonthsInFirstAcademicYearSemester** value to 5, **MonthsInSecondAcademicYearSemester** value to 4 and **MonthsInThirdAcademicYearSemester** value to 3.

Please note that the sum of months in all semesters should be 12. Value 0 for **MonthsInThirdAcademicYearSemester** indicates that there is no third semester. The intermediate semester cannot be skipped.

```
DECLARE @ConfigKey NVARCHAR(255)   = ''
      ,@ConfigValue NVARCHAR(255) = ''

--AcademicYearOffset
SET @ConfigKey   = 'AcademicYearOffset'
SET @ConfigValue = '8' ---<<Change value in quotes>>
UPDATE [core].[Configuration] SET ConfigValue = @ConfigValue WHERE ConfigKey = @ConfigKey

--MonthsInFirstAcademicYearSemester
SET @ConfigKey   = 'MonthsInFirstAcademicYearSemester'
SET @ConfigValue = '6' ---<<Change value in quotes>>
UPDATE [core].[Configuration] SET ConfigValue = @ConfigValue WHERE ConfigKey = @ConfigKey

--MonthsInSecondAcademicYearSemester
SET @ConfigKey   = 'MonthsInSecondAcademicYearSemester'
```

```
SET @ConfigValue = '6' ---<<Change value in quotes>>
UPDATE [core].[Configuration] SET ConfigValue = @ConfigValue WHERE ConfigKey = @ConfigKey

--MonthsInThirdAcademicYearSemester
SET @ConfigKey   = 'MonthsInThirdAcademicYearSemester'
SET @ConfigValue = '0' ---<<Change value in quotes>>
UPDATE [core].[Configuration] SET ConfigValue = @ConfigValue WHERE ConfigKey = @ConfigKey

EXEC [dbo].[usp_UpdateDimDate]
GO
```

FiscalPeriodMonthOffset

Use this configuration to set the Fiscal Period definition of an educational institution in the Date dimensions of the Datawarehouse. The FiscalPeriodMonthOffset value is the month offset from January to the beginning of the Fiscal Year month. For example, if the Fiscal year begins with July, the FiscalPeriodMonthOffset value is 6 (calculated as Begin Month Number minus 1). By default, the value of FiscalPeriodMonthOffset value is set to 6 in the configuration table when the Analytics Datawarehouse is installed. FiscalPeriodMonthOffset value must be set correctly based on the Fiscal Year definition of an educational institution after the Analytics datawarehouse installation or upgrade (Post Installation steps).

To change the FiscalPeriodMonthOffset value and update the Date dimensions records, execute the below script on the Datawarehouse database. The script can also be executed after running the “StudentAnalytics <data warehouse database name> Initial Load” SQL Server job.

```
DECLARE @ConfigKey NVARCHAR(255) = 'FiscalPeriodMonthOffset'
      ,@ConfigValue NVARCHAR(255) = '6' ---<<Change value in quotes

UPDATE [core].[Configuration]
SET ConfigValue = @ConfigValue
WHERE ConfigKey = @ConfigKey

EXEC [dbo].[usp_UpdateDimDate]
GO
```

CleanupRetentionDays

Use this configuration to set the retention period that identifies the duration of time for which the data in the staging (*_CT) tables should be maintained for any troubleshooting or verification purposes, before it is deleted.

Suppose the institution decides to store the staging data for 2 days, the CleanupRetentionDays value would be set to 2. Any staging data that is older than 2 days will be will be deleted when the StudentAnalytics <data warehouse database name> Cleanup SQL Server job is run.

The default value of CleanupRetentionDays key is 2. To change the CleanupRetentionDays value, execute the below script on the Datawarehouse database.

```
DECLARE @ConfigKey NVARCHAR(255) = 'CleanupRetentionDays'
      ,@ConfigValue NVARCHAR(255) = '2' ---<<Change value here

UPDATE [core].[Configuration]
SET ConfigValue = @ConfigValue
WHERE ConfigKey = @ConfigKey
```

Run the Initial ETL Job

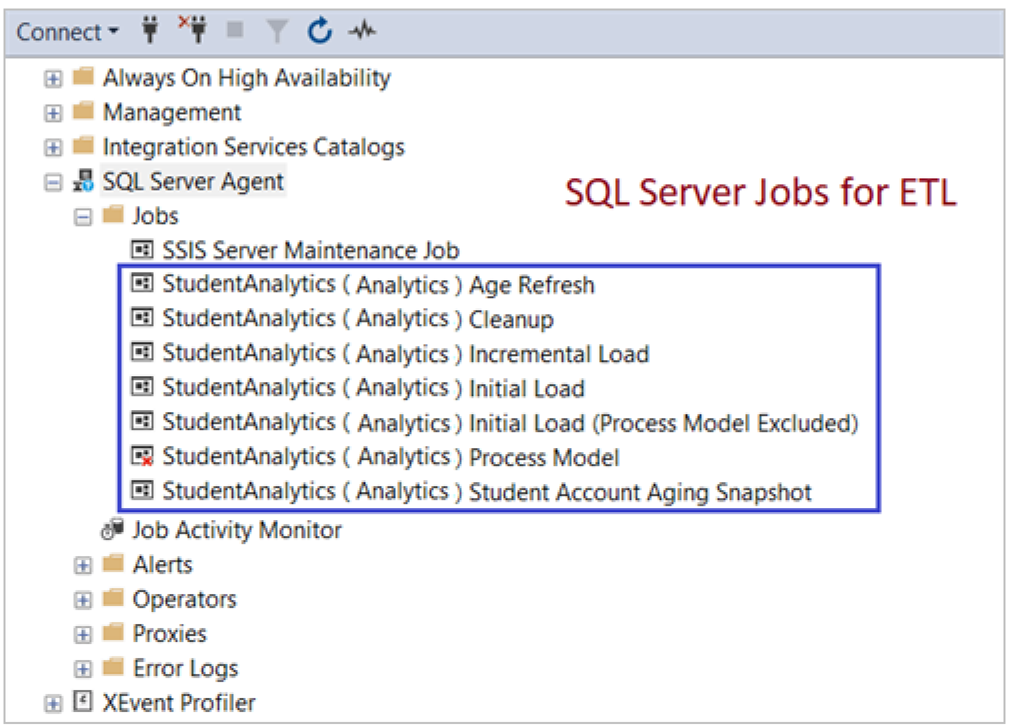
In the following steps you will connect to the Data Warehouse SQL Server instance and run the initial Extraction, Transformation & Loading (ETL) SQL Server job "*StudentAnalytics <data warehouse database name> Initial Load*" to move data from the source database to the warehouse and process the Semantic Model databases.

Student Analytics 5.3.0 provides an option to run the initial load process in two steps:

- First, the *"StudentAnalytics (Data warehouse database name) Initial Load (Process Model Excluded)"* job can be run to load data up to data warehouse.
- Later. the *"StudentAnalytics (Data warehouse database name) Process Model"* job can be run to process the analysis model database.

This will reduce the application downtime during the upgrade process.

1. Launch **Microsoft SQL Server Management Studio** on the server where the SSIS Catalog is installed.
2. Navigate to **SQL Server Agent > Jobs > StudentAnalytics (<Data warehouse database name>) Initial Load**.



The "Age Refresh" job is scheduled to run at 12.00.00 am on the first day of every month. This job updates all Student, Prospect, CRM Contact, and Lead age data.

Analytics 4.1 adds the “**Student Account Aging Snapshot**” job, which is scheduled to run every day at 12.00.00 a.m. This job creates monthly Student Account Aging Snapshots for current and past 1 year and a snapshot for the current month.

3. Right-click and select **Start Job at step**, select **Step 1** in the Start Jobs window, and click **Start**.

   Depending on the size of the database, this job may take minutes or hours. Observe the **Status** value while the process is running. Upon completion of the job, the Start Jobs window displays a *Success* message.

   You can also view reports on the execution of the ETL packages by navigating to **Integration Services Catalogs > SSISDB > <Catalog Folder Name>**. Right-click **<Catalog Folder Name>**, then navigate to **Reports > Standard Reports > All Executions**. Here ‘StudentAnalytics’ is the SSIS Catalog folder name specified during installation. The reports provide error messages and associated details that are useful to troubleshoot any issues with the ETL packages. There are packages for each of the tables that are synchronized between the source and the warehouse.

4. After the initial ETL job completes successfully, disable the initial Load job and make sure the following jobs are enabled:

   - StudentAnalytics <*data warehouse database name*> Age Refresh
   - StudentAnalytics <*data warehouse database name*> Cleanup
   - StudentAnalytics <*data warehouse database name*> Incremental Load
   - StudentAnalytics <*data warehouse database name*> Student Account Aging Snapshot

   Leave the StudentAnalytics <*data warehouse database name*> Process Model job in disabled mode, because processing Semantic Model databases is now part of the Incremental Load job. The Process Model job can be used to manually process Semantic Model databases when needed.

Incremental updates from the source database to the warehouse are performed automatically based on the schedule on these jobs. The default schedule is daily once at 1.00.00 a.m.

Manage Jobs

Enable/Disable Jobs

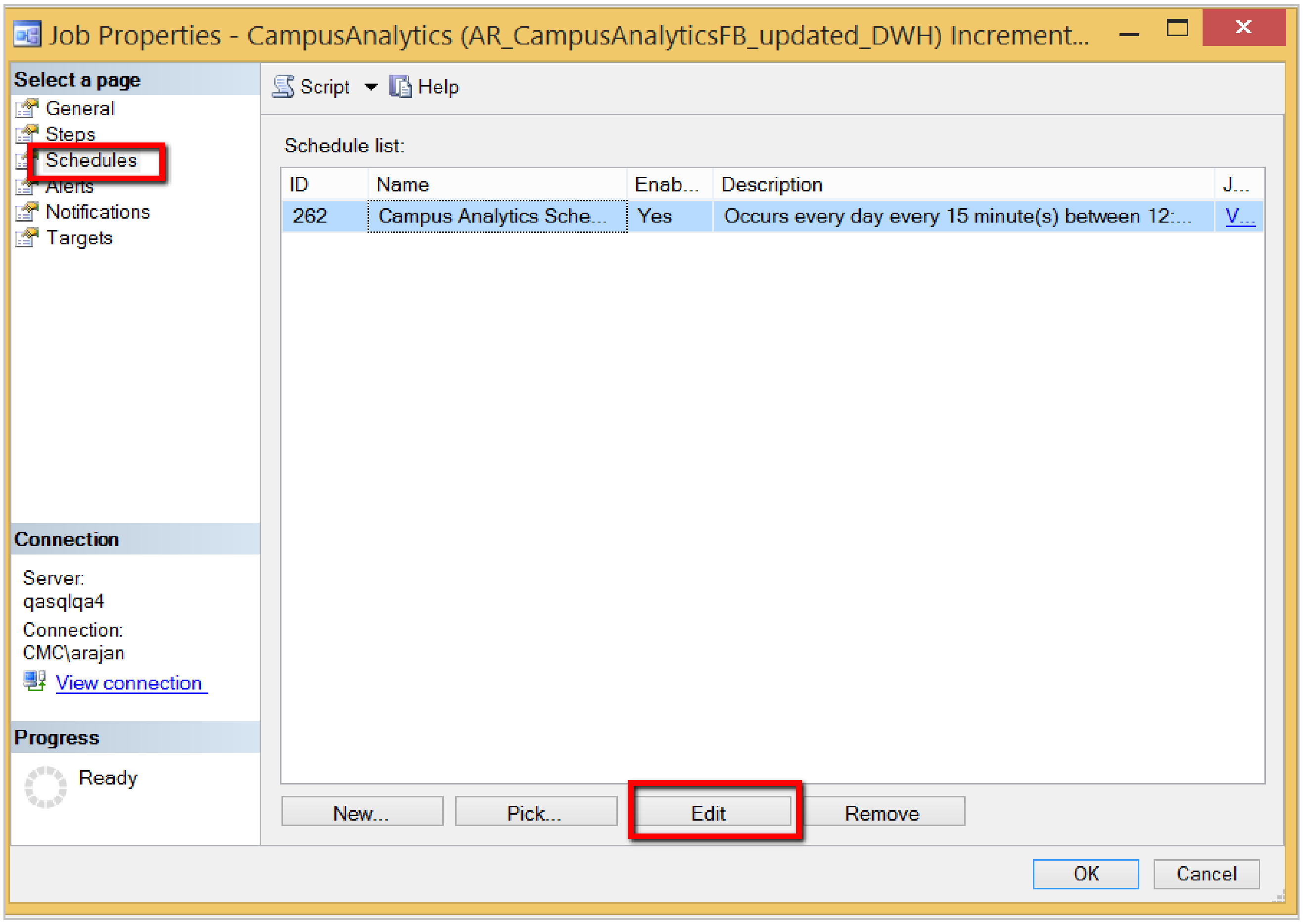
1. Launch **Microsoft SQL Server Management Studio** on the server where the SSIS Catalog is installed.
2. Navigate to **SQL Server Agent > Jobs**
3. Upon successful completion of the job “StudentAnalytics (<Data warehouse database name>) Initial Load”, right-click and disable the Initial Load job.
4. Make sure the following jobs are enabled:
    - StudentAnalytics <data warehouse database name> Age Refresh
    - StudentAnalytics <data warehouse database name> Cleanup
    - StudentAnalytics <data warehouse database name> Incremental Load
    - StudentAnalytics <data warehouse database name> Student Account Aging Snapshot

    If any of the above listed job are not enabled, right-click and enable them.
5. After the initial ETL job completes successfully, verify the Job schedules and if required modify. Upgrading to Analytics 4.2 or higher version will not modify customized job schedules.

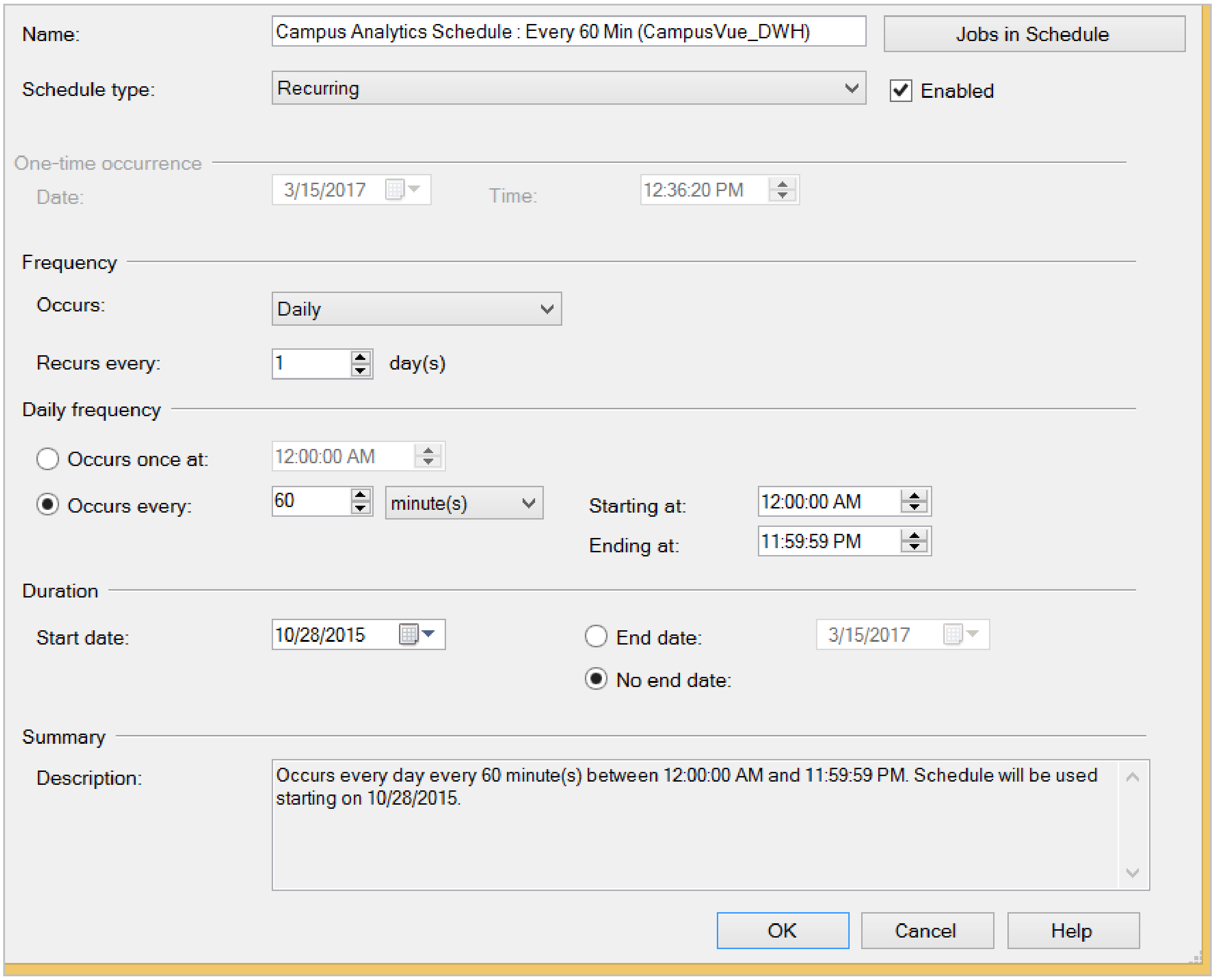
    Please follow the next section to change the Job schedule.

Change the Job Schedule

1. Navigate to **SQL Server Agent > Jobs**.
2. Right-click on the Job and click on **Properties**.
3. Select the **Schedules** tab as show below and click **Edit**.



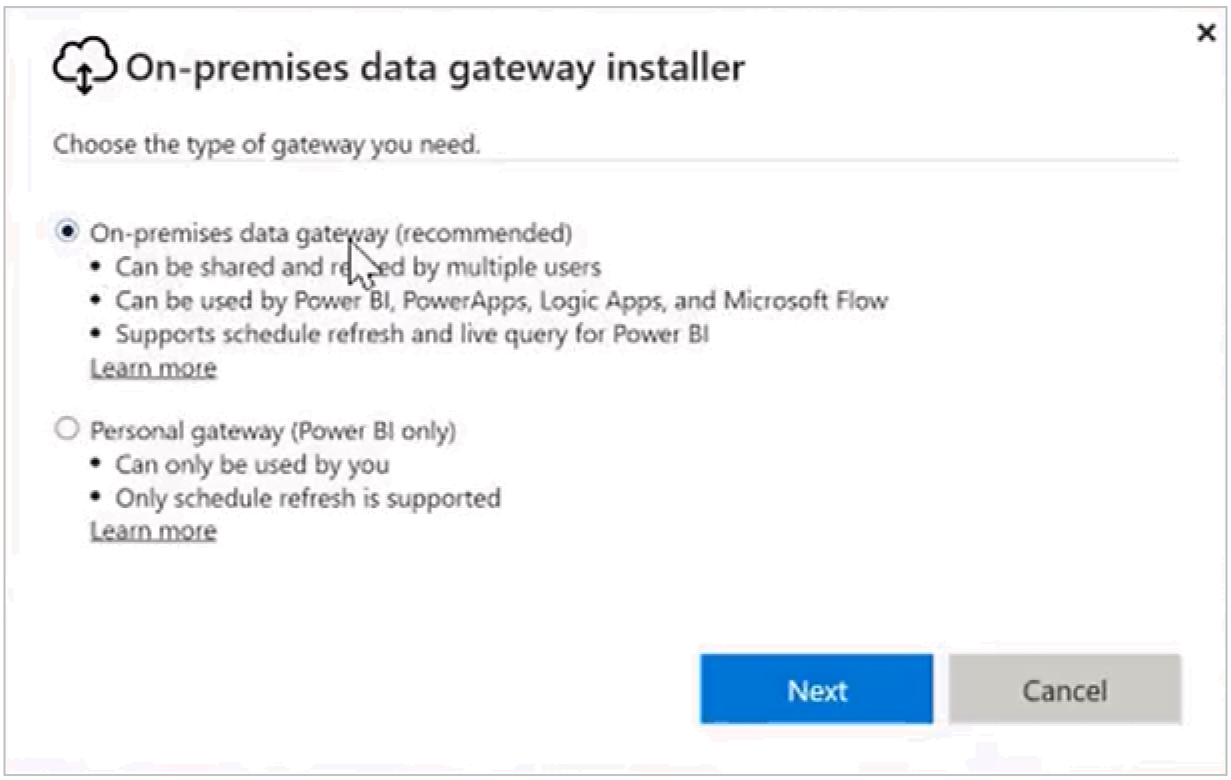
4. Select a schedule that suits your business needs.


Name:
Campus Analytics Schedule : Every 60 Min (CampusVue_DWH)
Jobs in Schedule
Schedule type:
Recurring
Enabled
One-time occurrence
Date:
3/15/2017
Time:
12:36:20 PM
Frequency
Occurs:
Daily
Recurs every:
1
day(s)
Daily frequency
Occurs once at:
12:00:00 AM
Occurs every:
60
minute(s)
Starting at:
12:00:00 AM
Ending at:
11:59:59 PM
Duration
Start date:
10/28/2015
End date:
3/15/2017
No end date:
Summary
Description:
Occurs every day every 60 minute(s) between 12:00:00 AM and 11:59:59 PM. Schedule will be used starting on 10/28/2015.
OK
Cancel
Help

Set Up the Microsoft On-Premises Data Gateway

We recommend that you install this gateway on a server that is running the data source you will be connecting to. While you can install it on a different machine, you will reduce potential network latency by having it on the same machine.

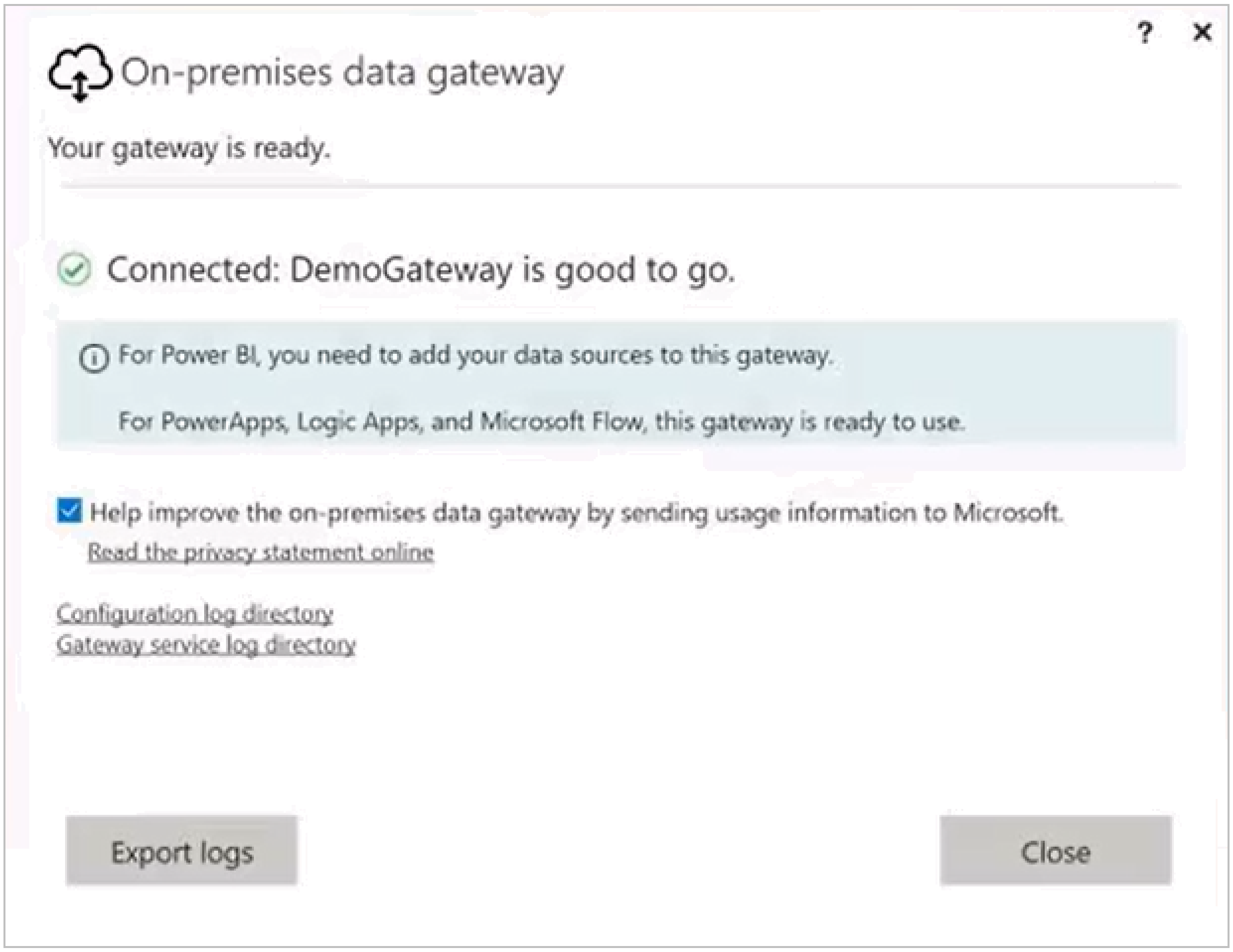
1. Go to https://powerbi.microsoft.com/en-us and click the **See all downloads** link at the bottom of the page.
2. Click the **Download** button for the **Microsoft on-premises data gateway** and complete the setup steps.
3. When the download is complete, install the on-premises data gateway on your desktop. Click **Next**.
4. Select the option to install the **On-premises data gateway** (do not select the "Personal gateway"). Click **Next** to start the download.



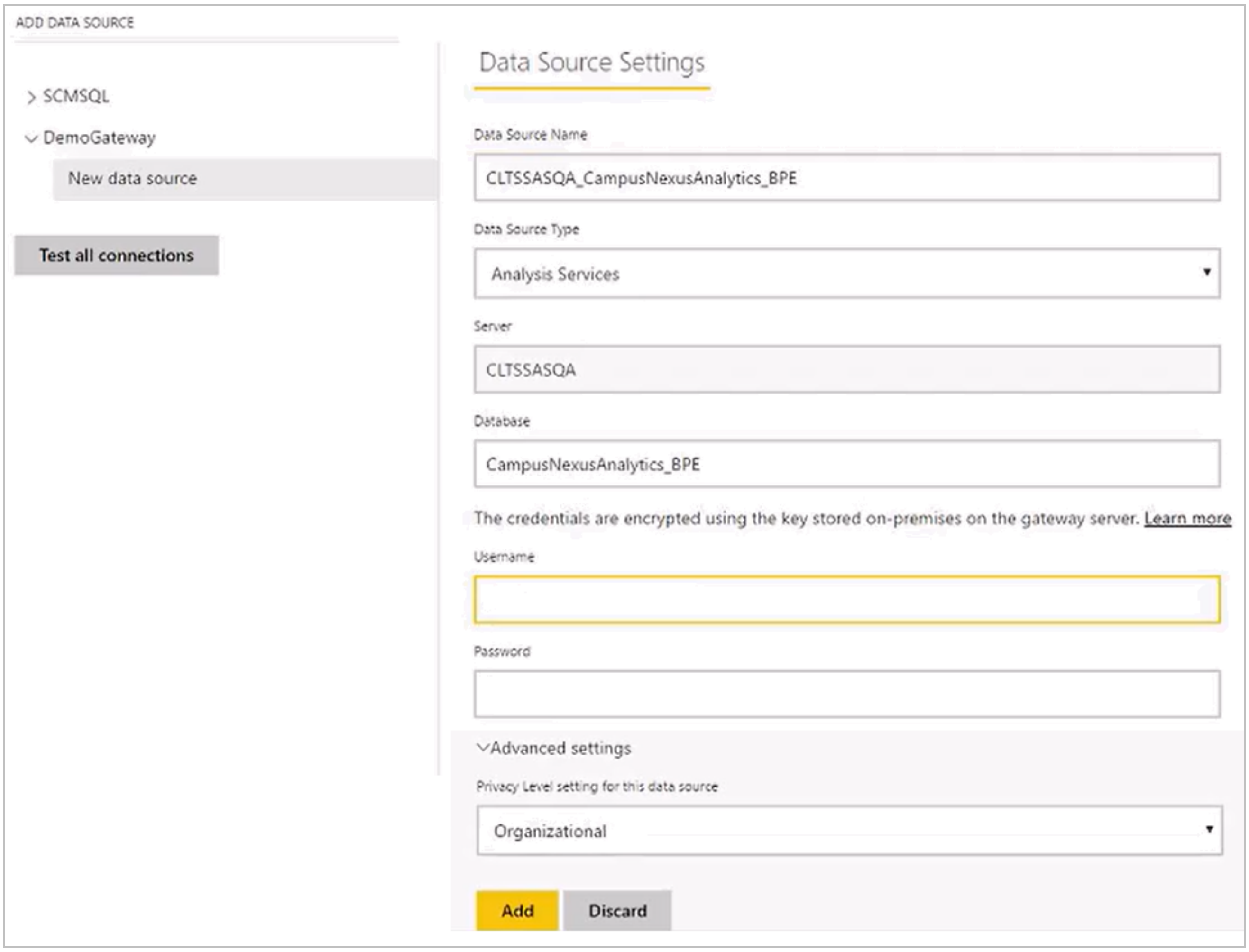
5. Note that the gateway should be installed on a computer that is always on and not asleep. Click **Next**.
6. Select a location for the gateway to be installed, accept the terms of use and privacy statement, and click **Install**.
7. When prompted, enter the email address of the account set up within the Power BI tenant. This should be a generic (not personal) email address, e.g., PowerBi@campusmgmt.com.
8. Select your Power BI email address to sign in to the gateway at **Microsoft Azure**.

9. When you are signed in and ready to register the gateway, select **Register a new gateway on this computer** and click **Next**.
10. Specify the **Gateway name** and **Recovery key** and click **Configure**.

    Note: The recovery key is a password used to restore the gateway.
11. A confirmation message is displayed. Click **Close**.



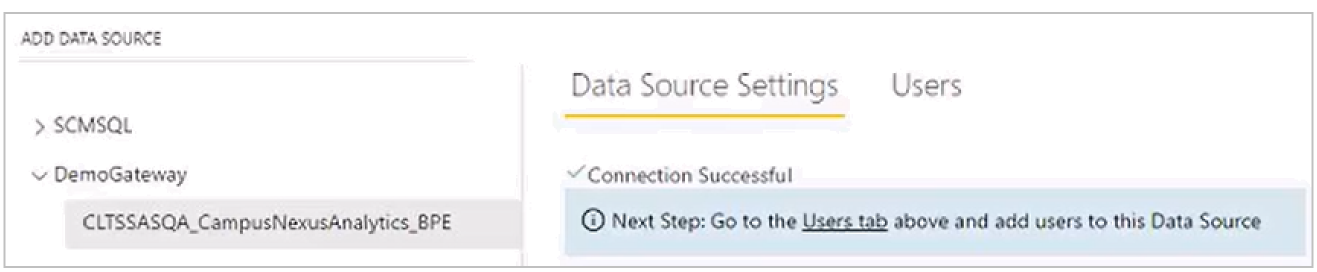
12. Now we need to add data sources to this gateway. To do so, go to https://powerbi.microsoft.com/en-us and click **Sign in**.
13. In Power BI, click  and select **Manage gateways**.
14. Select the gateway you just added and click **Add data sources to use this gateway**.
15. Complete the "Data Source Settings" form and click **Add**.



Notes:

- A naming convention for the Data Source Name could be <server>_<database>
- The user specified on this form must have permissions to the database.
- Click **Advanced Settings** and verify that the privacy level is set to **Organizational**.

16. The message *Connection successful!* is displayed. The data source is now created under the new gateway. The data source is ready for use for any pbix files that are created for this data source.



Manage the Size of the SSISDB (Catalog Database)

The SSISDB (Catalog Database) is installed as part of the catalog configuration. With the default installation Operation cleanup is enabled, and the Retention window is set for 365 days, which means the operation records are maintained for 365 days.

With a higher Retention window, the SSISDB can grow over time and may create performance issues. To manage the size of the SSIDB, we recommend changing the retention window to a smaller value based on the business requirements.

- Check the following catalog properties.

  ```
  SELECT *
  FROM SSISDB.catalog.catalog_properties
  WHERE property_name IN
              (
                  'RETENTION_WINDOW'
                , 'VERSION_CLEANUP_ENABLED'
                , 'OPERATION_CLEANUP_ENABLED'
              }
  ```

- If VERSION_CLEANUP_ENABLED is set to FALSE, enable it.

  ```
  EXEC catalog.configure_catalog VERSION_CLEANUP_ENABLED, TRUE
  EXEC catalog.configure_catalog OPERATION_CLEANUP_ENABLED, TRUE
  ```

- Update the RETENTION_WINDOW to the number best suited for business. For example, if the business requirement is to retain the operation maintenance records for 100 days, update the RETENTION_WINDOW property to 100.

  ```
  EXEC catalog.configure_catalog RETENTION_WINDOW, 100
  ```

Monitor SSISDB growth for a few months to determine if a change is required in the retention window. Since SSISDB is shared by all SSIS packages installed in the database, the growth of SSISDB depends on the number of packages installed on the server and the frequency of execution.

For more details, see [Managing the size of the SQL Server SSIS catalog database]

Analytics for On-Prem and PaaS

This section applies only to Student Analytics. Please confirm if this is applicable for your installation.

Before publishing the reports, make sure that the SSAS server name URL and database name are available. If not, create a service request for the details.

Analytics for On-Prem Prerequisite

- Microsoft On-Premises Data Gateway is installed.

Analytics for PaaS Prerequisites

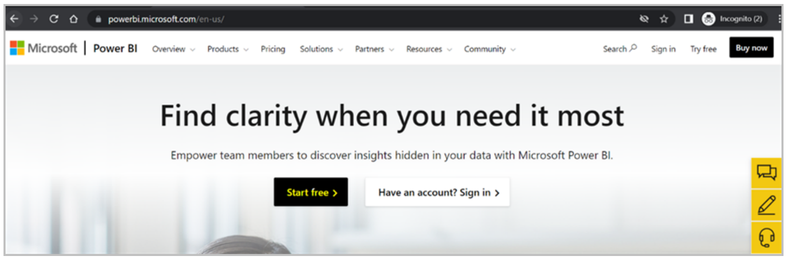
- Customer AAD users must be synced up to the Cloud domain as guest users.
- The Anthology Student database should be on the Cloud with Azure SQL database.

Power BI Subscription

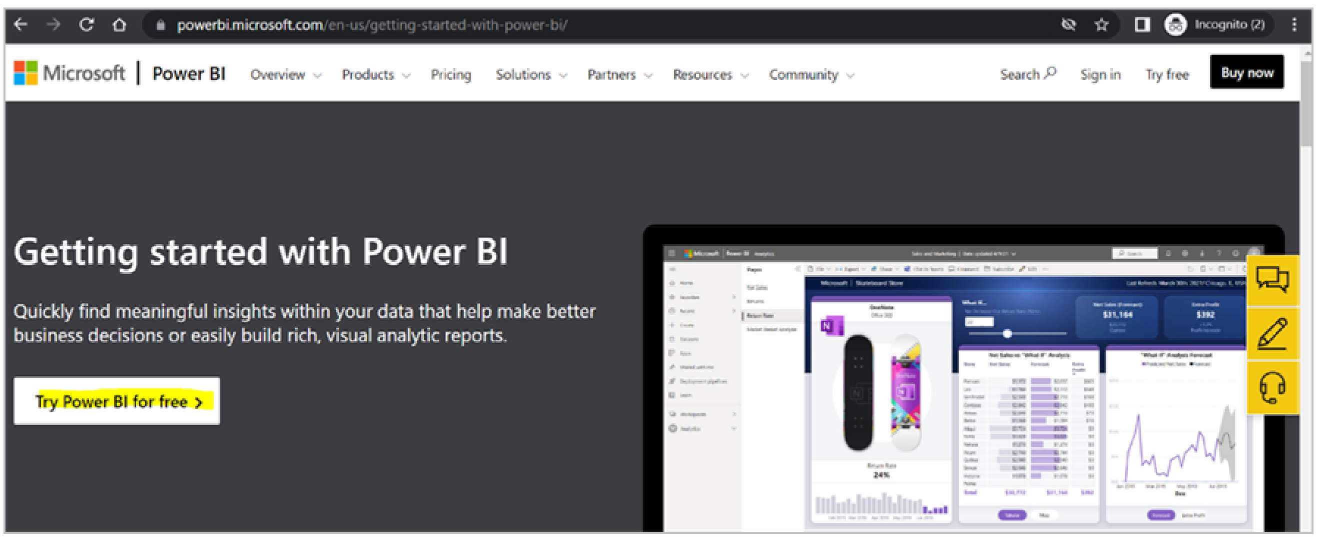
An administrator must subscribe to the Power BI cloud offering from Microsoft and set up a tenant to leverage data visualization in Power BI, enabling users to connect to the Student Analytics semantic model. The tenant is the container for your institution's users, domains, subscriptions, and so on.

Create a Power BI Tenant and Initial User

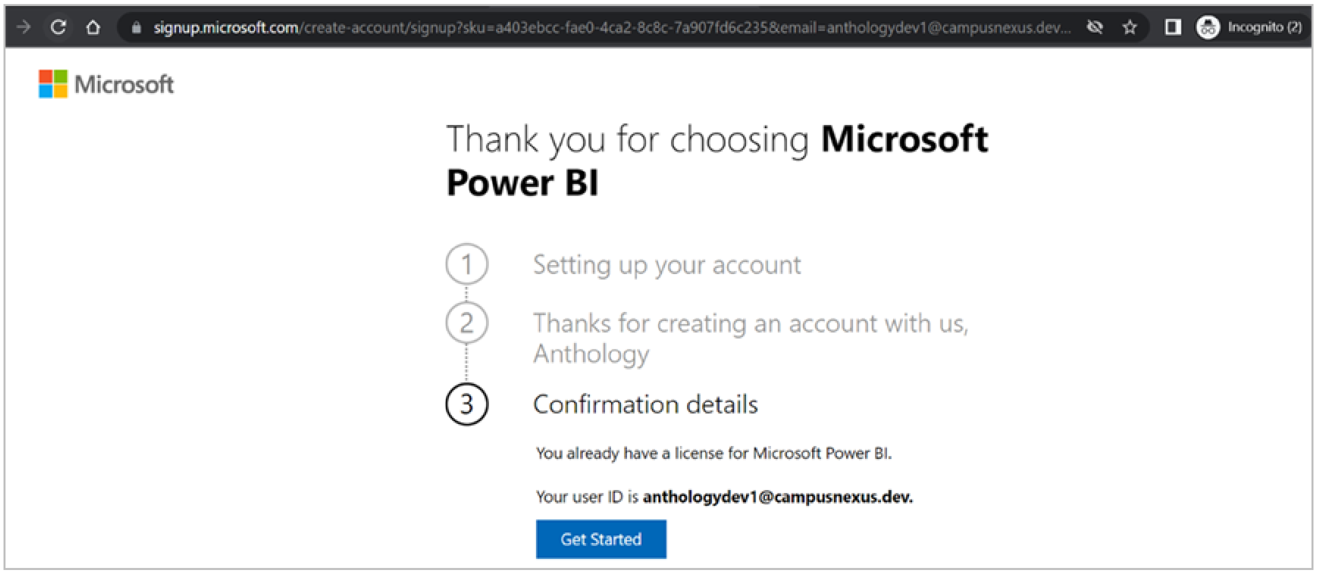
1. Go to https://powerbi.microsoft.com/en-us and click **Start free**.



2. Click **Try Power BI for free**.



3. Specify the required confirmation details and click **Get Started**.



When this is done for the first time, Microsoft creates an Azure Active Directory in the back end and completes all the provisioning steps for a tenant. The first person in your organization that signs up for Power BI creates a tenant in Power BI (see https://powerbi.microsoft.com/en-us/blog/what-is-a-tenant/).

Note: We suggest creating the initial account without a personal name, for example, PowerBI@<yourdomain> so that the account is not tied to a person and the password is not changed. After the initial account is created, additional personal accounts can be created.

If you already have an account with another Microsoft service, your email address will be recognized and you will be prompted to sign in.

4. After you have confirmed your identity, the Welcome to Power BI screen is displayed, the tenant is set up, and a user is created.

Set Up the Microsoft On-Premises Data Gateway

> ⚠ This section applies only when you are installing Analytics on-premises. When you are installing Analytics for PaaS, you do not need to set up the Microsoft On-Premises Data Gateway.

Power BI connects to Analytics using the Microsoft Data Gateway. The gateway provides a secure connection from the Power BI Service to Analysis Services data sources for Analytics. Establishing a connection to Analysis Services through the gateway is required to publish and view Power BI reports for Analytics.

Prerequisites

Review the prerequisites to ensure they are met before moving forward.

You must have:

- A Power BI Pro account with admin access to register and manage the Microsoft Data Gateway. This account should be a generic account not linked to an actual user (for example, PowerBIadmin@yourdomain.com).
- If you are self-hosted, a machine to host the gateway (see server requirements)
- Credentials for a Service Account with server administrator access to the Analysis Services server
- Data Source settings information to connect to the Analysis Services data models:
    - Server Name
    - Data Model Names
    - Service Account credentials

We recommend that you install this gateway on a server that is running the data source you will be connecting to. While you can install it on a different machine, you will reduce potential network latency by having it on the same machine.

Power BI connects to Analysis Services via the Microsoft On-Premises Data Gateway. The gateway is installed and registered to the customer tenant as part of the post installation tasks for Analytics. This enables the Microsoft Power BI service to connect reports to the Analysis Services data models.

Cloud customers will have the gateway installed and registered as part of the post installation process after Analytics is installed.

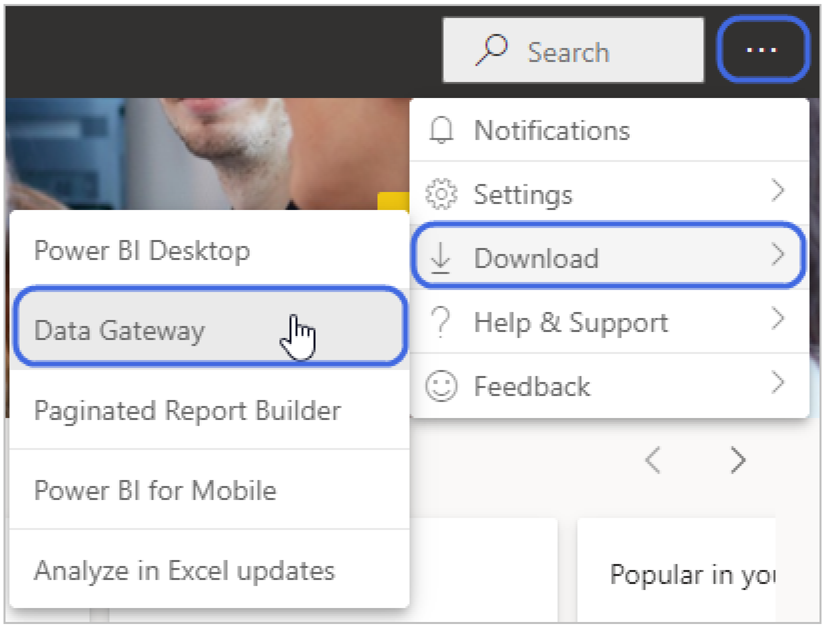
The steps outlined below are required to install and register the data gateway if you are self-hosted.

Note: The minimum screen resolution supported for the on-premises data gateway is 1280 x 800.

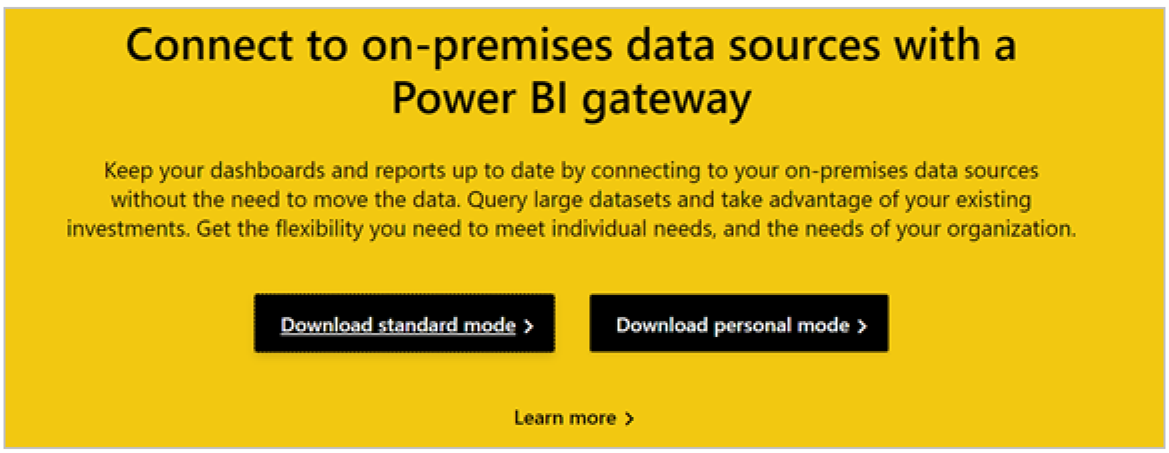
Download and Install the Gateway

1. On the machine where you will install the gateway, visit https://app.powerbi.com/ (**Power BI Service**) and **sign in** using the **Power BI Pro Account**.

2. Click the options **(...)** at the top right, select **Downloads** and select **Data Gateway**.

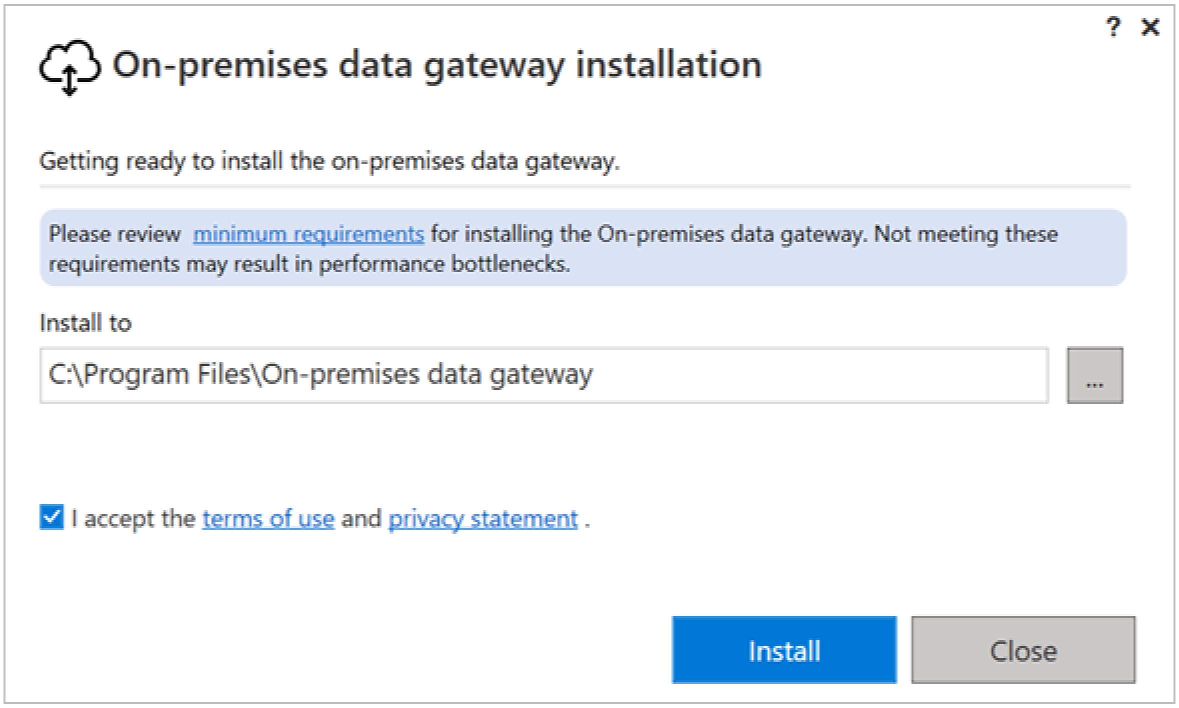


3. Click **Download standard mode** and install the GatewayInstall.exe file.

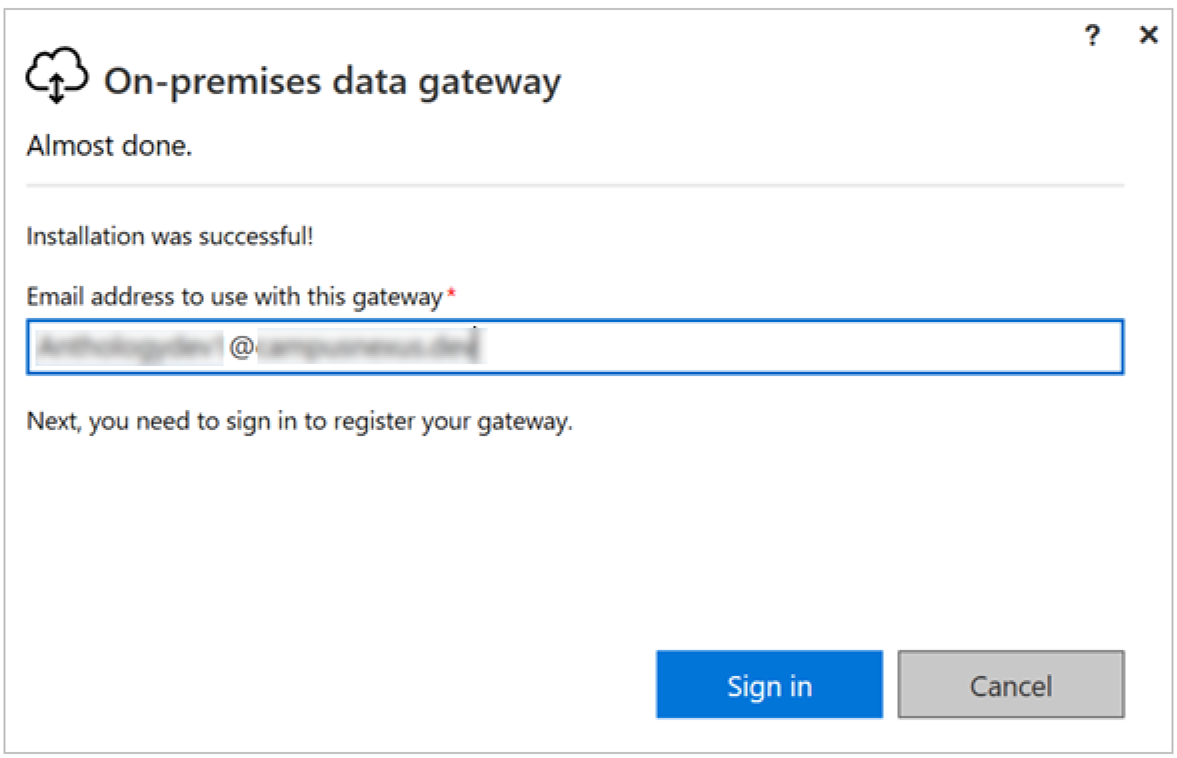


4. When the download is complete, install the on-premises data gateway on your desktop.

   In the gateway installer, keep the default installation path, accept the terms of use, and then select **Install**.



5. Enter the email address for your Office 365 organization account and then select **Sign in**.

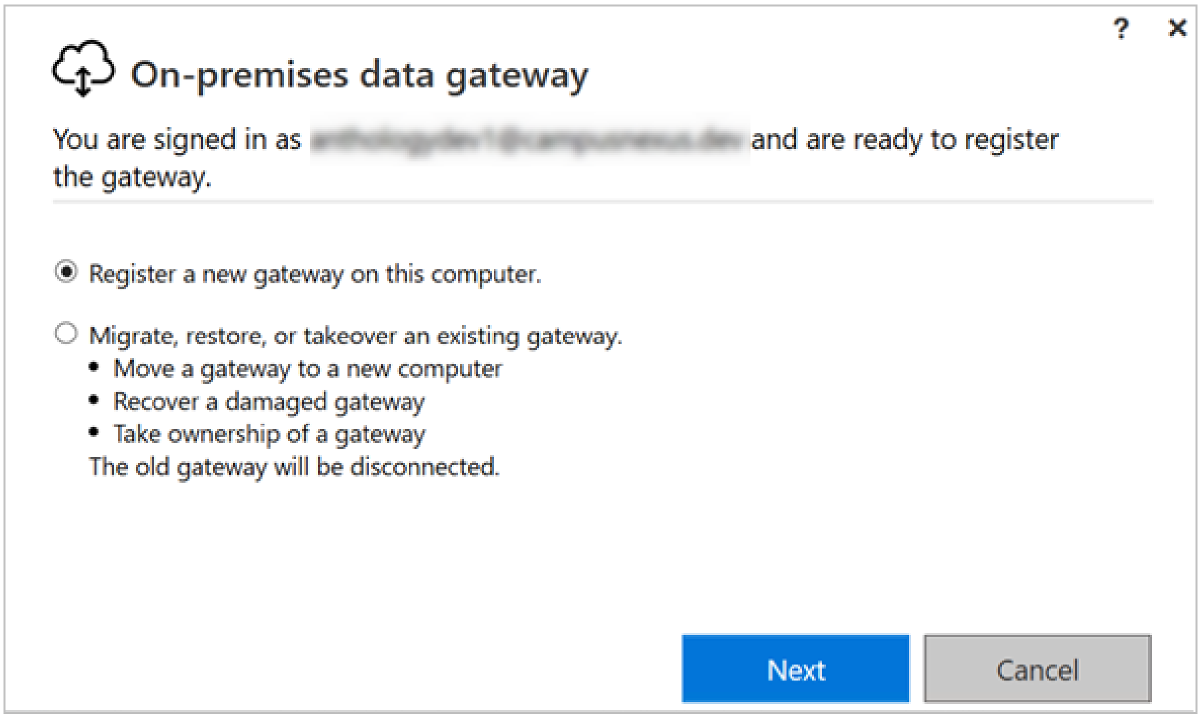


Note: You need to sign in with either a work account or a school account. This account is an organization account. If you signed up for an Office 365 offering and didn't supply your work email address, your address might look like nancy@contoso.onmicrosoft.com. Your account is stored within a tenant in Azure AD. In most cases, your Azure AD account's User Principal Name (UPN) will match the email address.

The gateway is associated with your Office 365 organization account. You manage gateways from within the associated service.

You're now signed into your account.

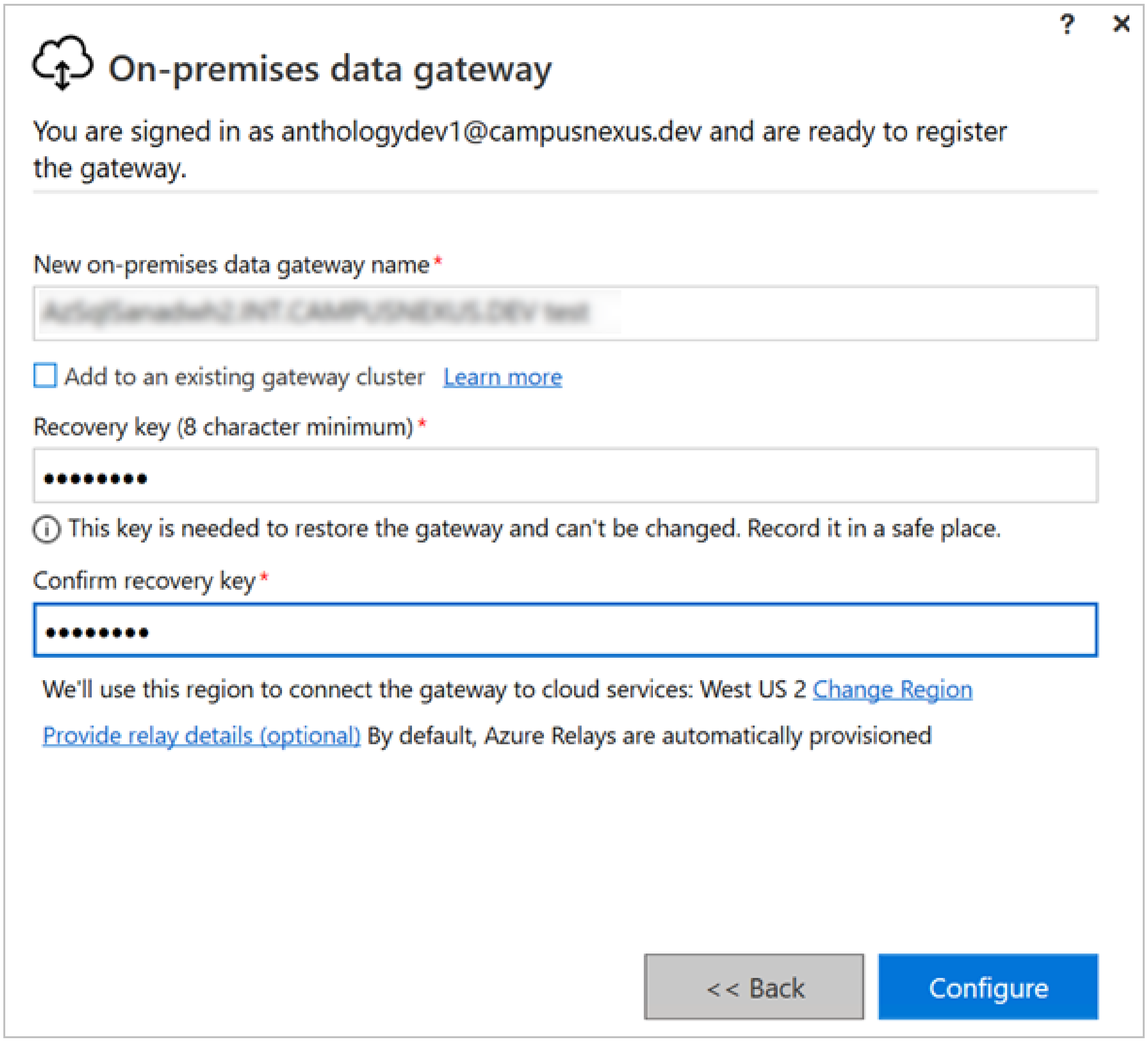
6. Select **Register a new gateway on this computer** and click **Next**.



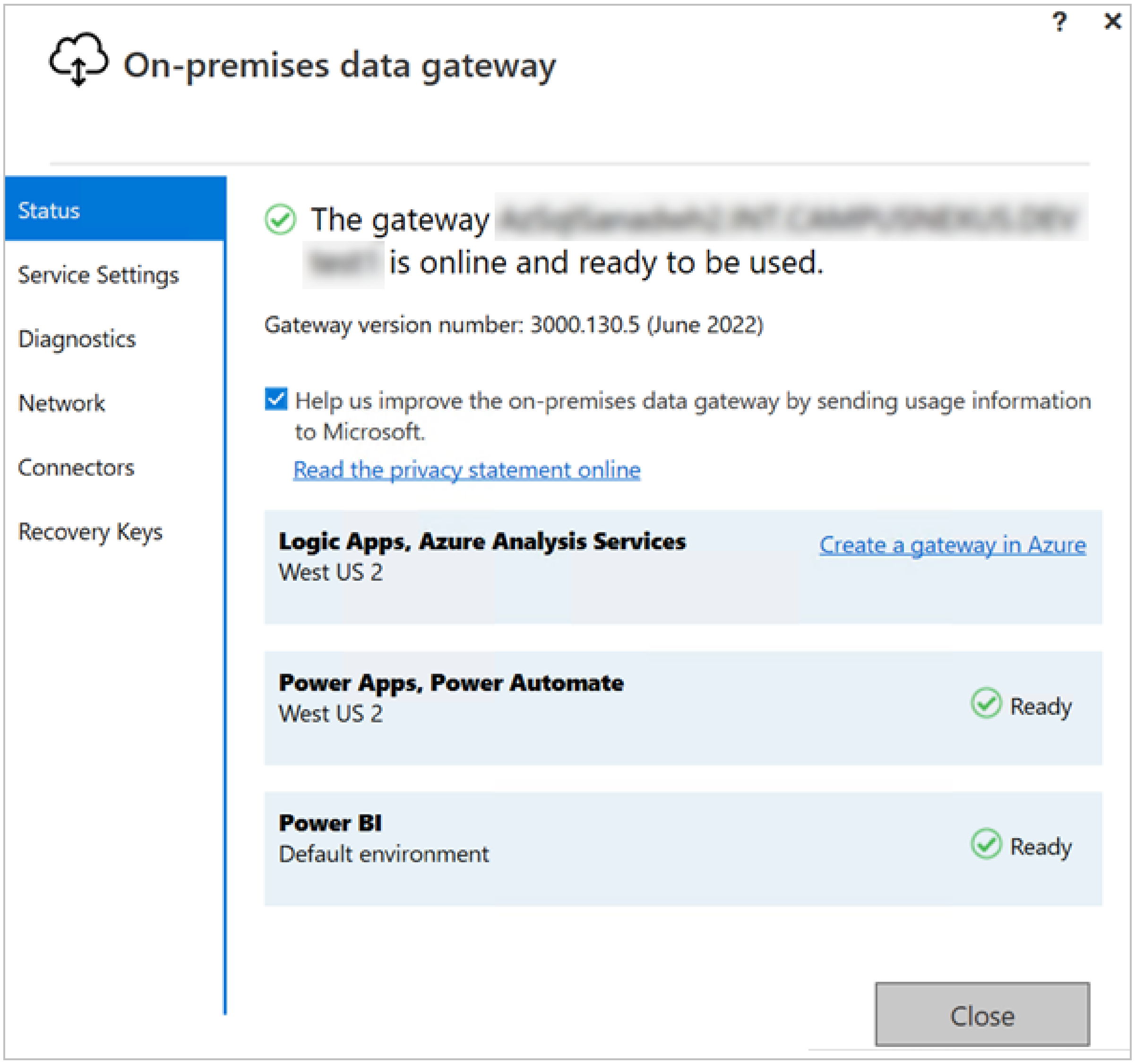
7. Enter a **name** for the gateway. The name must be unique across the tenant.

   Also enter a **recovery key**. You'll need this key if you ever want to recover or move your gateway.

   Select **Configure**.



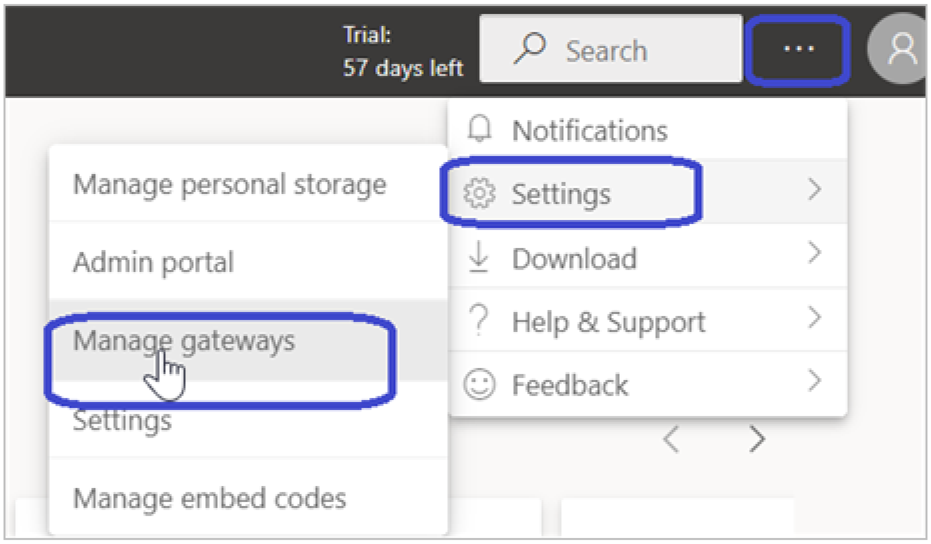
8. Review the information in the final window. Because this example uses the same account for Power BI, Power Apps, and Power Automate, the gateway is available for all three services. Select **Close**.



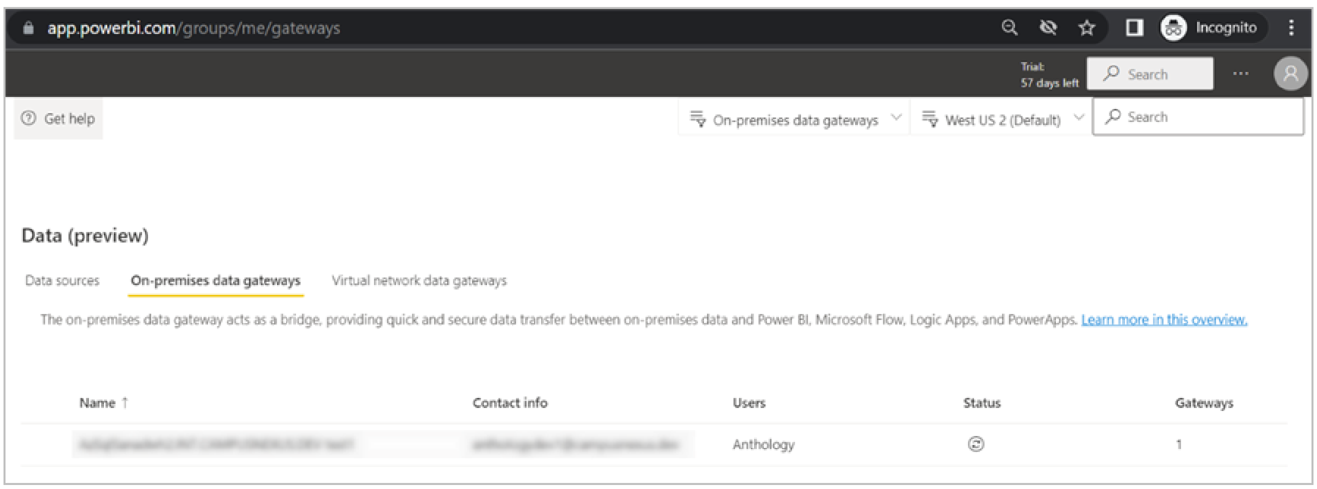
Verify the Gateway Connection

Note: Manage gateways will not show up until you're the admin of at least one gateway. You become an admin either by being added as an admin or because you installed and configured a gateway.

1. Log in to Power BI Service (https://app.powerbi.com/) with the tenant account used to register the gate-way.
2. Click options **(...)** at the top right, select **Settings**, and select **Manage gateways**.



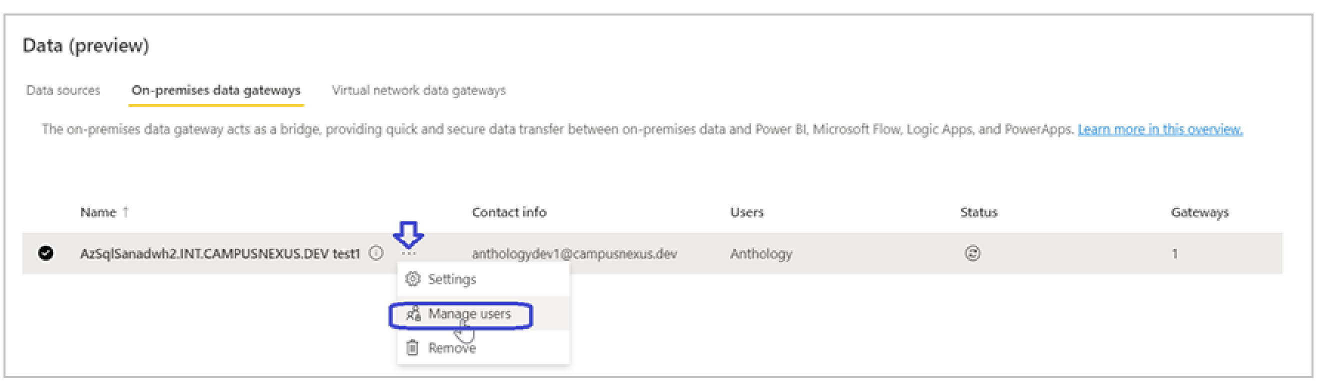
3. Verify the gateway is available on the **On-Premises data gateways** tab.



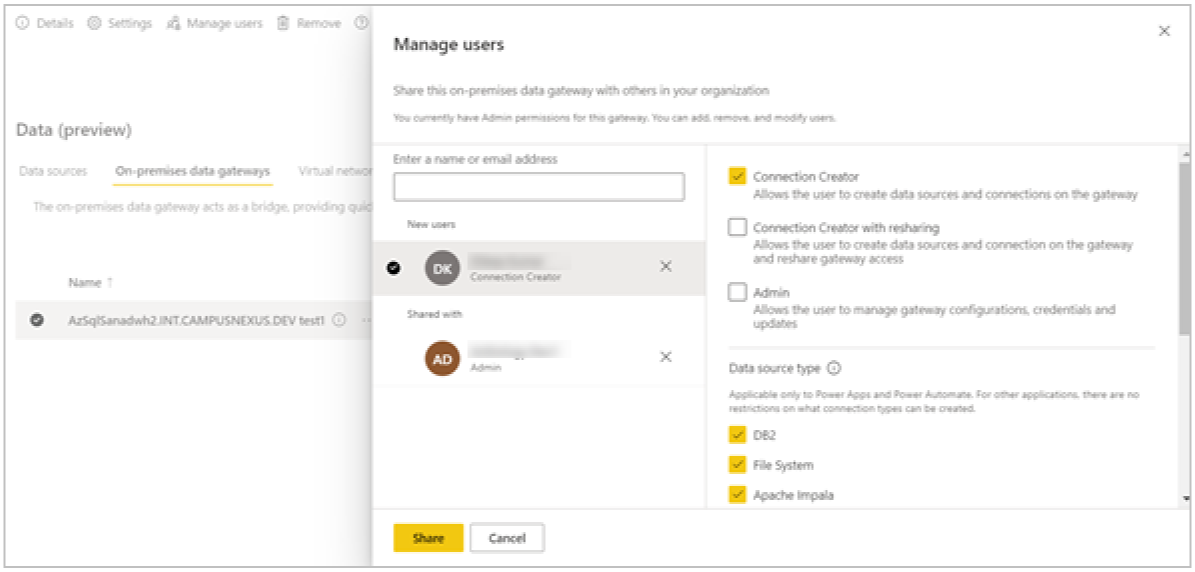
Provision Gateway Administrators

After the Power BI gateway is installed and verified, provision other users' access to administer the data gateway. Users provisioned as an Administrator on the gateway will be able to manage the gateway in Power BI.

1. Select the **Gateway** that was created for **Analysis Services**. Click options **(...)** and select **Manage users**.



2. Enter the **email address** for the user and click **Add**. Repeat this step for all users who will have access to administer the gateway.



Set Up Gateway Data Sources

After the gateway is installed, you will need to add the Analysis Services data sources that will be used by the gateway for Analytics. It should now be available in Power BI as an available gateway cluster. To connect the gateway to the Analytics data models, administrators need to add the Analysis Services data models to the gateway in Power BI.

Anthology Student Data Sources:

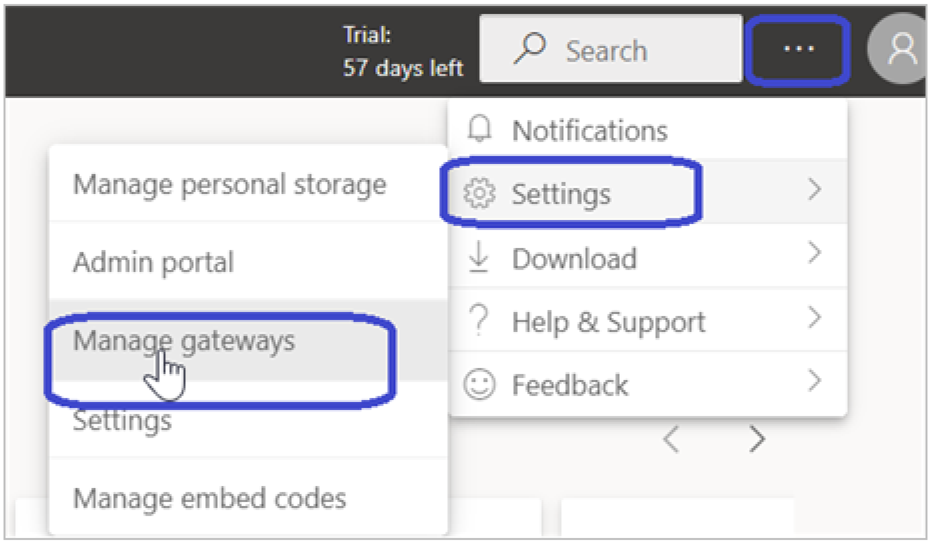
- Academic & Admissions Model (for example, SISACADSemanticModel)
- Financial Aid Model (for example, SISFASemanticModel)
- Student Accounts Model (for example, SISStudentAccountsSemanticModel)
- Career Services Model (for example, SISCSSemanticModel)
- Contact Manger Model (for example, SISCMSemanticModel)

CampusNexus CRM Data Sources:

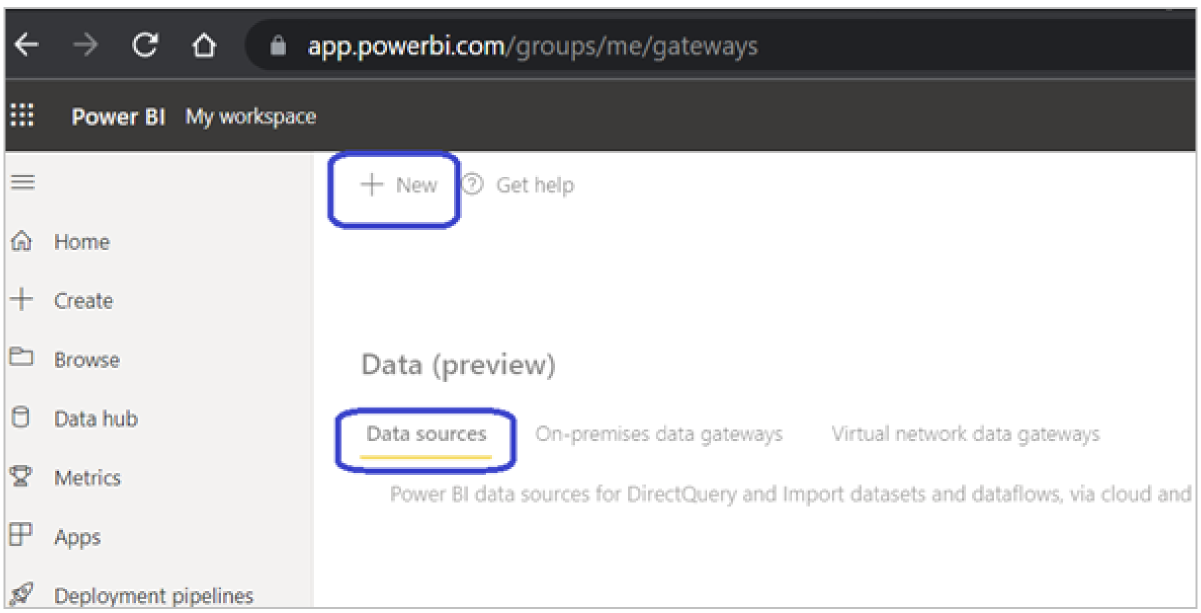
- CRM Model (if applicable)

Add Analysis Services Data Sources to the Gateway

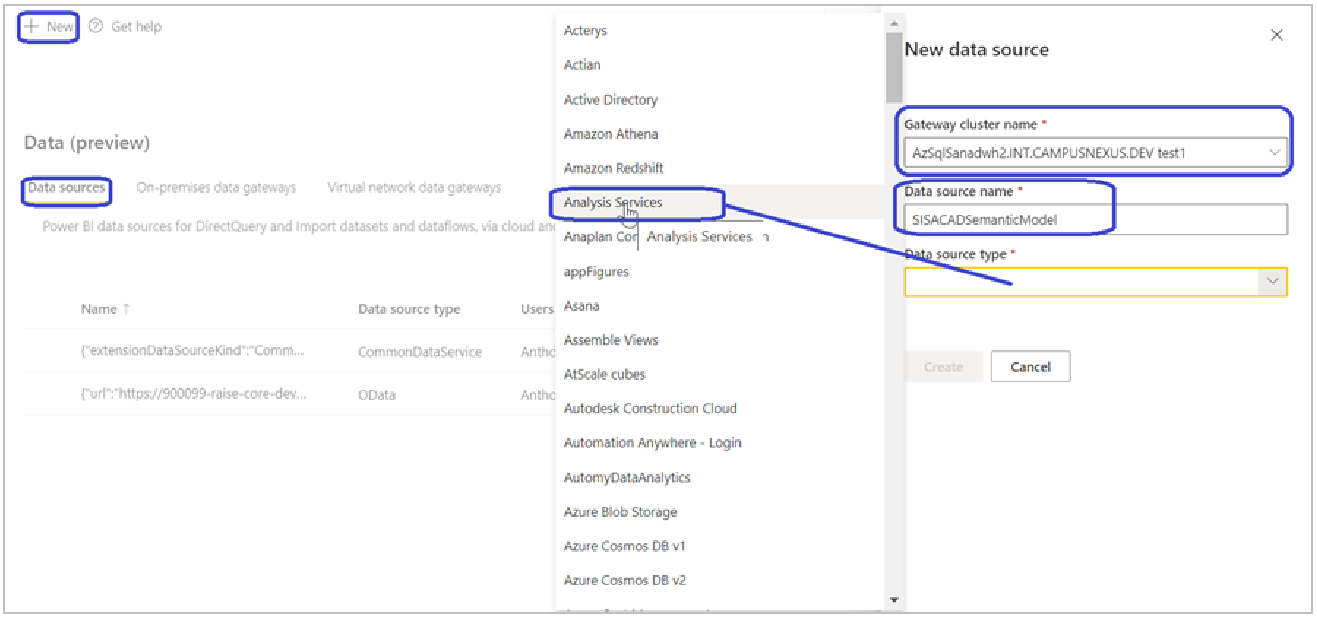
1. Log into https://app.powerbi.com/ with the Microsoft Power BI account used to register the gateway to verify the gateway has been added.
2. Select options **(...)** at the top right, select **Settings**, and select **Manage gateways**.



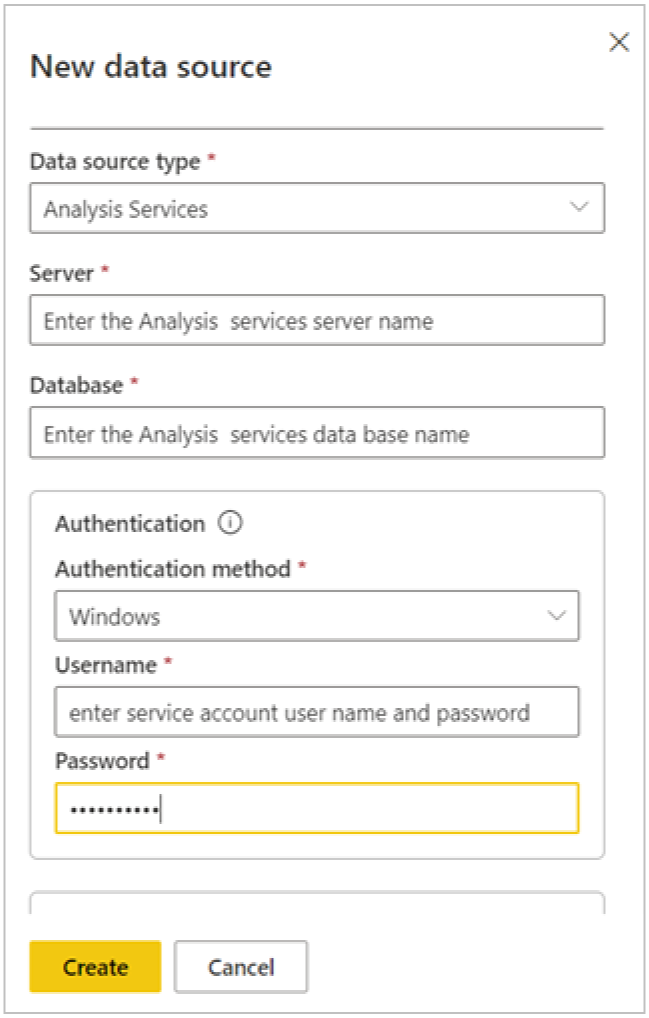
3. Go to **Data sources** and click **New**.



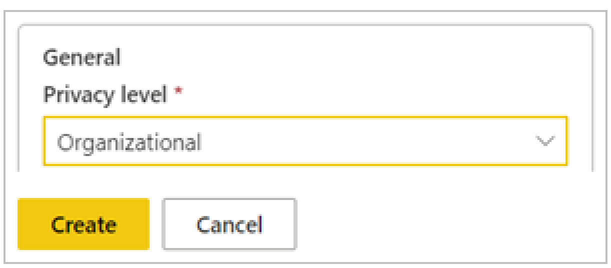
4. Select **Gateway cluster name**, add **Data source name**, and select **Analysis Service**.



5. Configure **Analysis Services Data Source Settings** as shown in the image below.



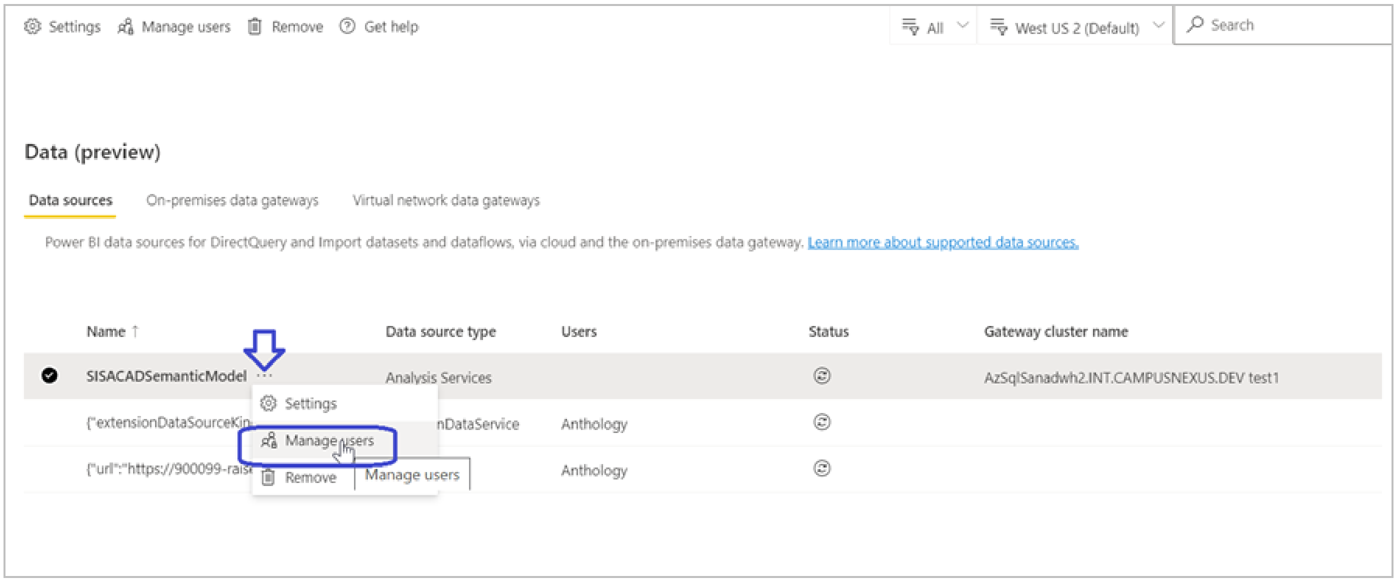
6. Expand **Settings**, select **Organizational**, and click **Create**.

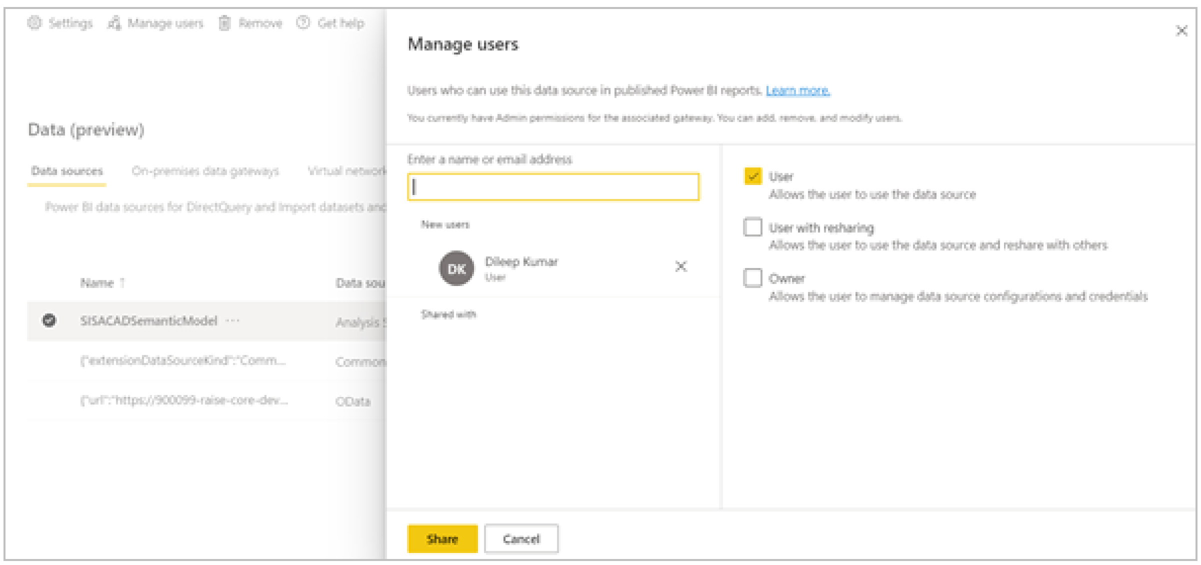


7. Repeat same data source creation steps to add the remaining Analysis Services data models (depends on the Analysis Service data sets that need to be created for each model).

Provision Gateway Data Source User Access

After the Power BI data source is set up and connected successfully, provision users access to the data source. Users provisioned as a User on the data source will be able to manage the data within the source in Power BI.





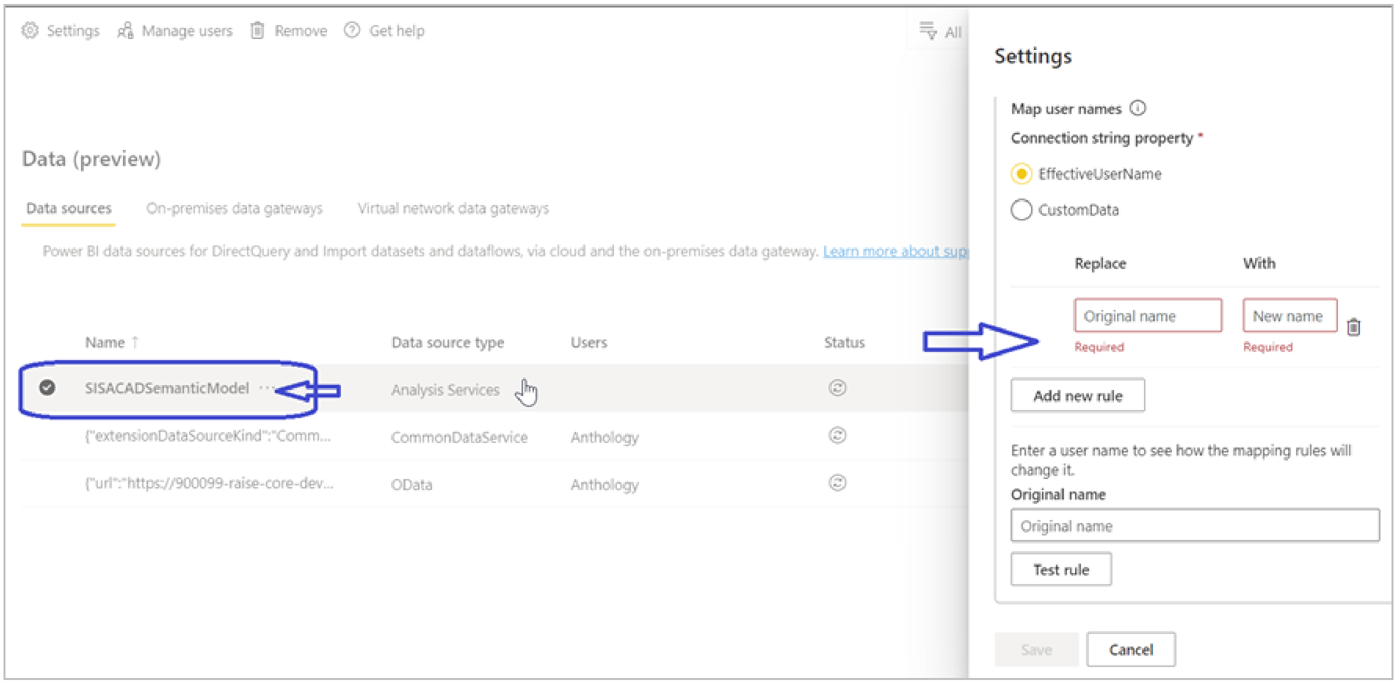
Repeat this step for remaining Analysis Services data source users.

Mapping User Names

In some cases, the user names or emails used to log into Power BI may differ from the logon account name used in AD or AAD to provision access to Analysis Services data models. In these scenarios, user names mappings are needed. The scenario below outlines a case where Mapping Usernames may be necessary.

- Power BI account is: *jdoe@yourdomain.com*
- Local AD account used to access Anthology products is: *jdoe@campusnet.local*

A user name mapping can be created to have the user authenticate through the gateway using the Local AD Account. If mapping user names is used, it will need to be added to each data source.



Synchronize On-premises Active Directory with Azure Active Directory

- You want each of your on-premises Active Directory accounts to match an Azure AD account, because the UPN for both accounts must be the same.
- The cloud services know only about accounts within Azure AD. It doesn't matter if you add an account in your on-premises Active Directory. If the account doesn't exist in Azure AD, it can't be used.
- There are different ways to match your on-premises Active Directory accounts with Azure AD.
    - Add accounts manually to Azure AD.
    - Create an account on the Azure portal or within the Microsoft 365 admin center. Make sure the account name matches the UPN of the on-premises Active Directory account.
- Use the Azure Active Directory Connect tool to synchronize local accounts to your Azure AD tenant.
- The Azure AD Connect tool provides options for directory synchronization and authentication setup. These options include password hash sync, pass-through authentication, and federation. If you're not a tenant admin or a local domain admin, contact your IT admin to get Azure AD Connect configured.

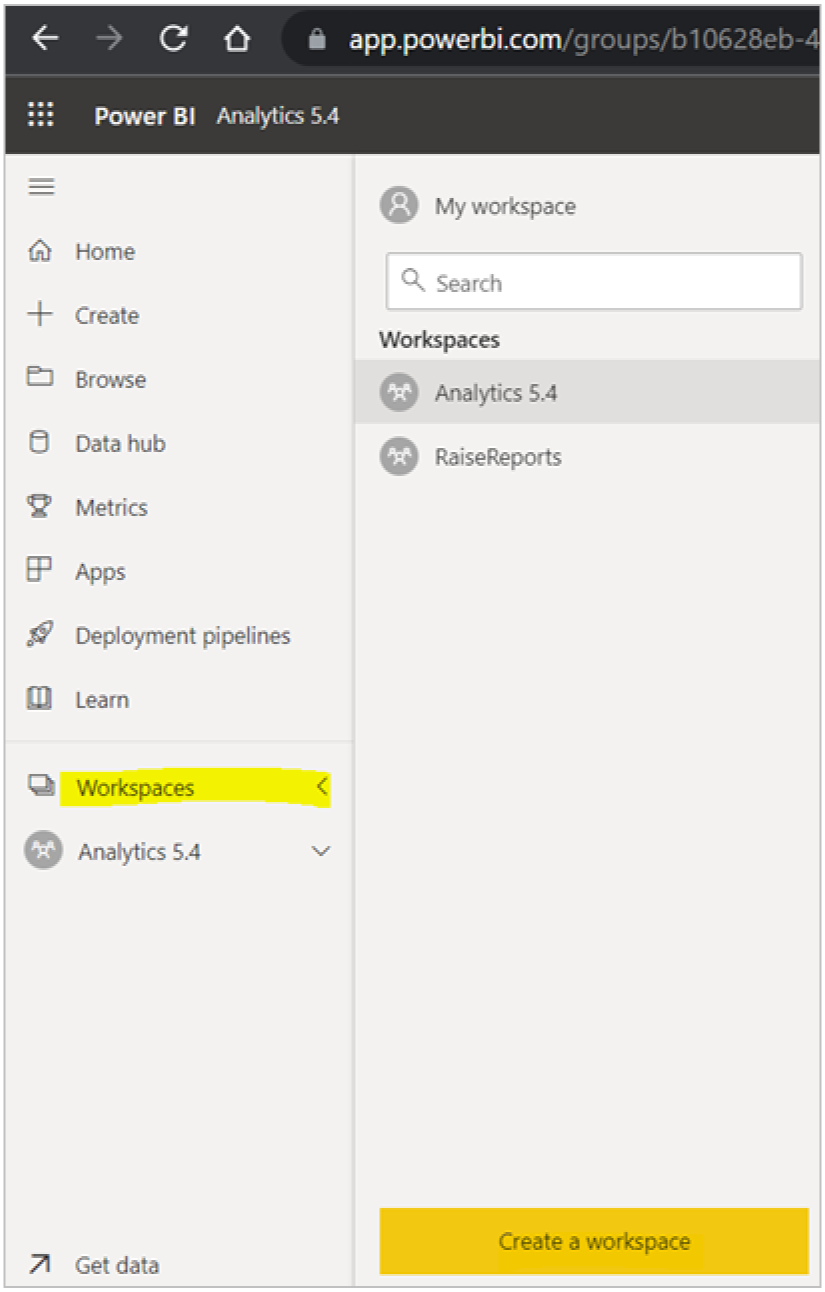
Azure AD Connect ensures that your Azure AD UPN matches your local Active Directory UPN. This matching helps if you're using Analysis Services live connections with Power BI or single sign-on (SSO) capabilities.

User name examples:

- *CustomerForms@Customer.edu* is a Power BI Pro user.
- *CustomerForms@100569cust.campusnexus.cloud* is a service account user which has Analysis Service server access.

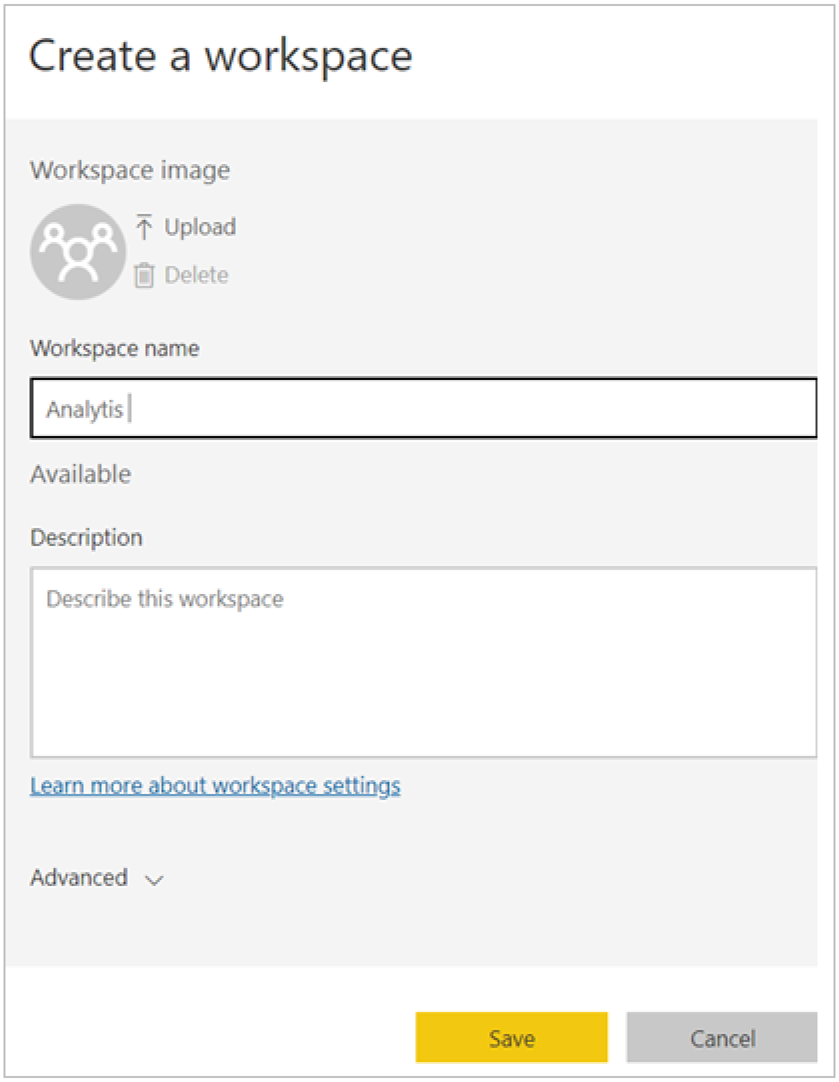
Create an App Workspace

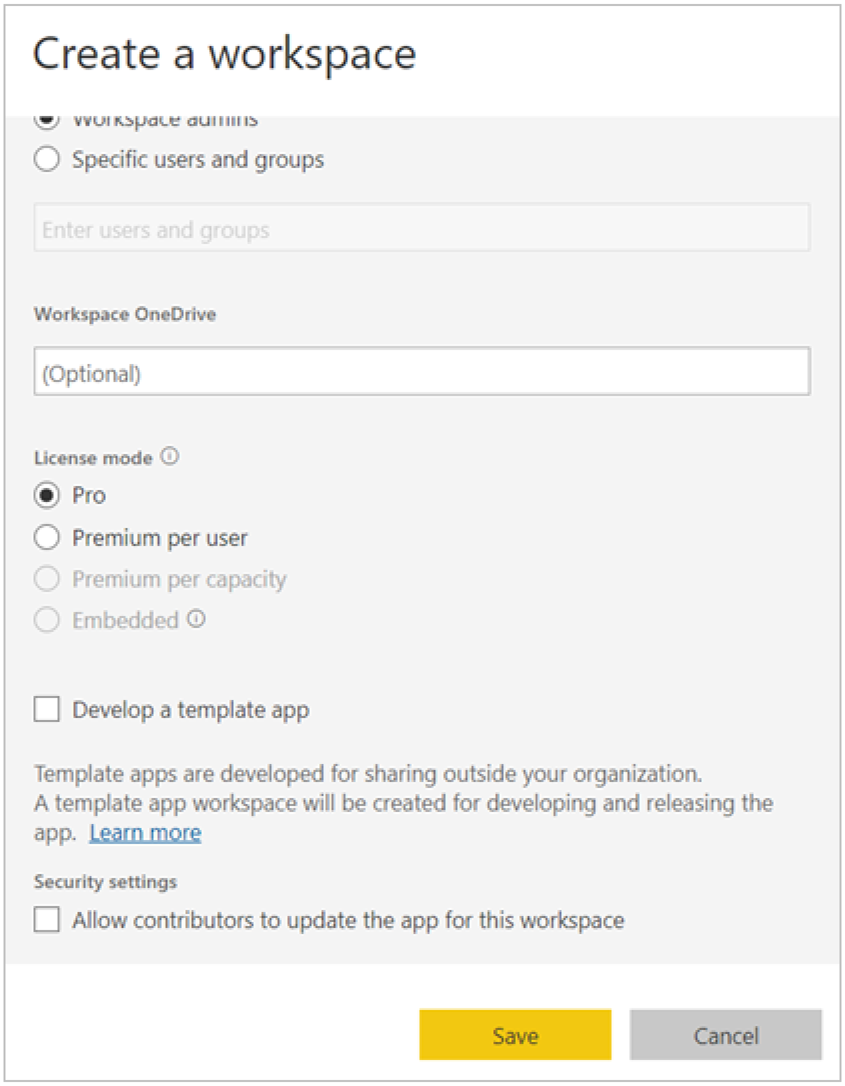
1. Log in to https://app.powerbi.com/ and select **Workspaces** > **Create a workspace**.



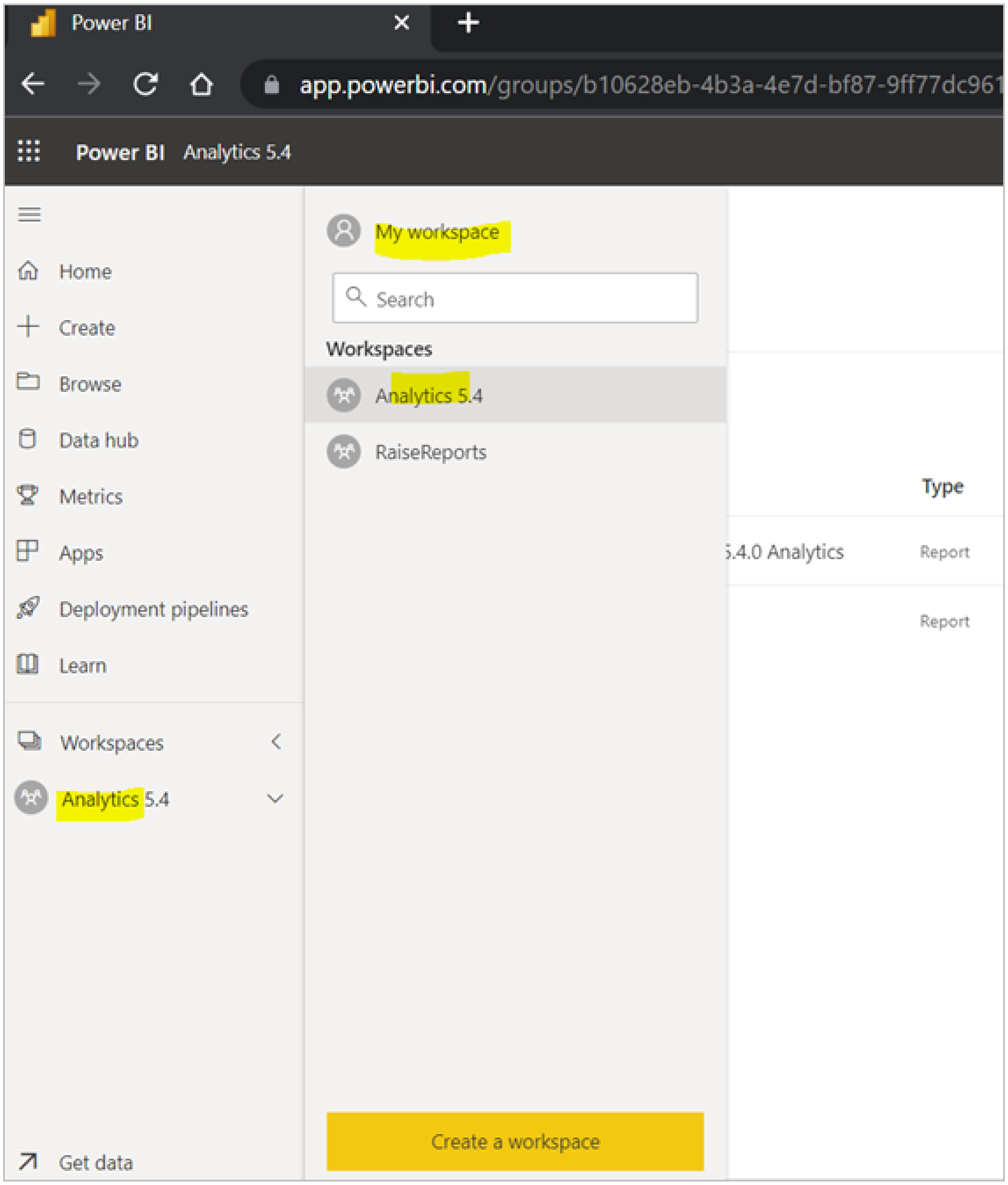
2. Specify the following app workspace properties:
   - **Workspace name**
   - **Description**

- **Contact list** — Add the email addresses of people you want to collaborate with in creating the app.





3. Click **Save** to save the app workspace. Power BI creates the workspace and opens it. It appears in the list of workspaces.



Initially, the app workspace is empty. Adding content is just like adding content to your personal workspace (My Workspace), except the other people in the workspace can work on it too.

Note: You can only publish an app from an app workspace. You cannot use My Workspace to publish apps.

Publish Report Definitions

With every release of Analytics, Power BI report files (PBIX files) are made available to customers who use Power BI for analytics reporting. The report files provide out-of-the-box visualizations and can be published to the Power BI Service workspaces via the Power BI Desktop application. Once published, these reports can be shared and viewed by others using Power BI. Power BI Desktop is where most reports will be created and modified, then published to the Power BI Service for sharing and collaboration.

Prerequisites

Review the prerequisites to ensure they are met before moving forward.

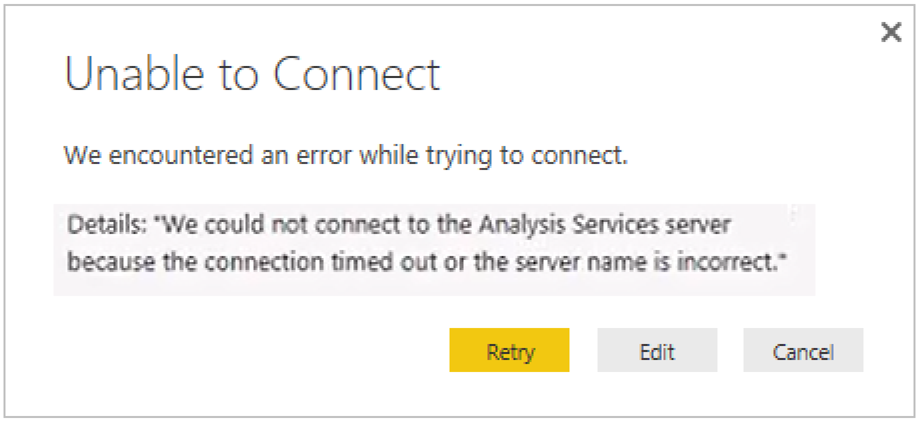
Users must:

- Have access to the latest version of Power BI Desktop
- Have access to the Analytics PBIX files
- Have a valid Power BI Pro license
- Be in the “CS_Analytics_Admin” group in Active Directory
- Be added as a user on the gateway data source
- Have access to Data Source Connection Information:
    - Server Name
    - Analysis Services Data Model Names

Download and Publish a PBIX File

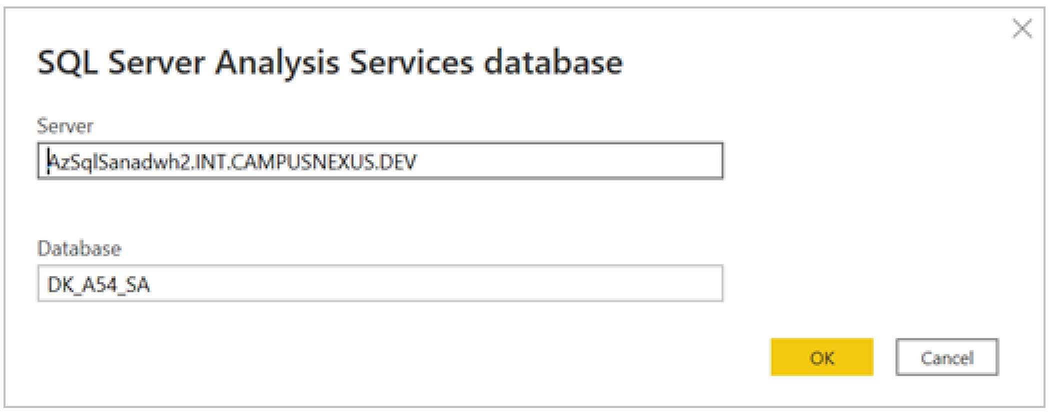
1. Install the Power BI Desktop if you have not done so previously.
    a. Go to https://powerbi.microsoft.com/en-us.
    b. Download Power BI Desktop and complete the setup steps as prompted.
2. Launch Power BI Desktop.
3. Download the PBIX file from the Anthology FTP site, for example, *Student Accounts 5.4.0 Analytics.pbix*.
4. In Power BI Desktop, select **File** > **Open** and browse to the downloaded **PBIX** file.

   The message *"Unable to Connect"* is displayed. The reason for this message is that the PBIX file does not have the connection information for the Analysis Services database that is used as the source.



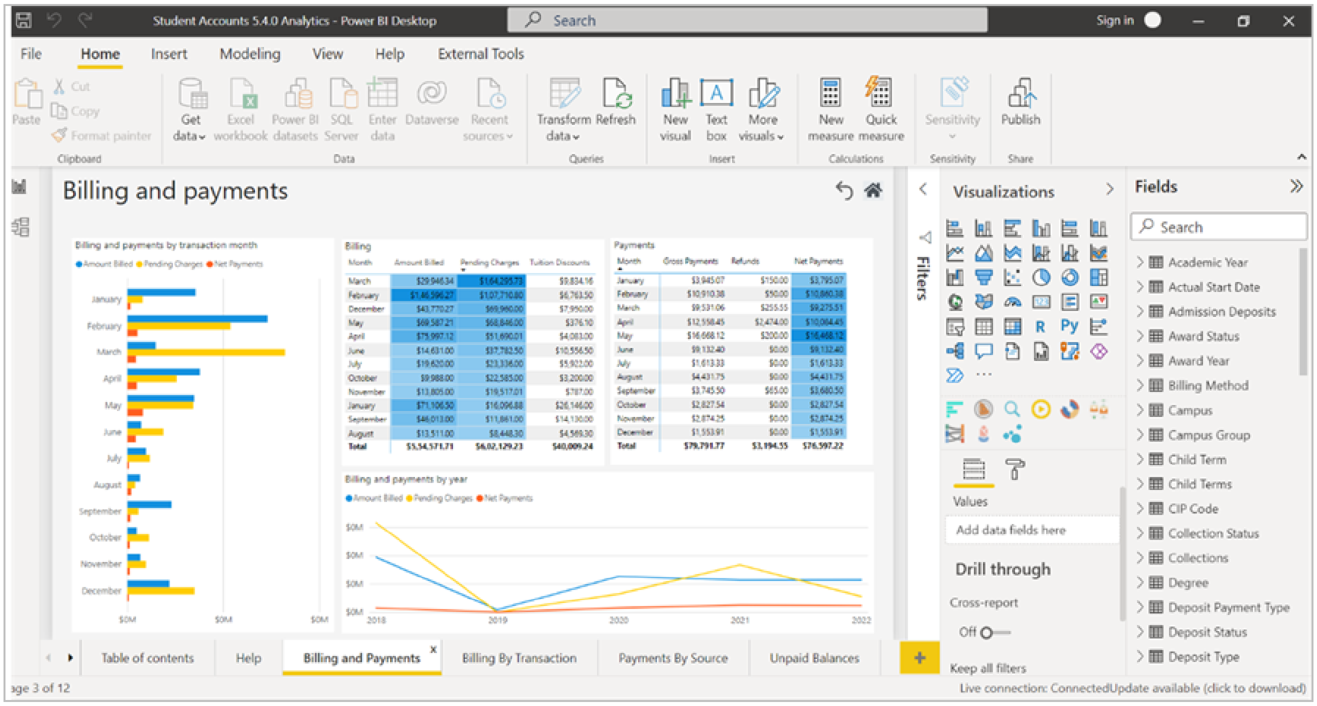
5. Click **Edit** on the *"Unable to Connect"* message. The SQL Server Analysis Services Database form is displayed.
6. Enter the name of your **SSAS Server**, specify the **Database**, and click **OK**.

   Note: The data source of the PBIX file in the example below is the DK_A54_SA.

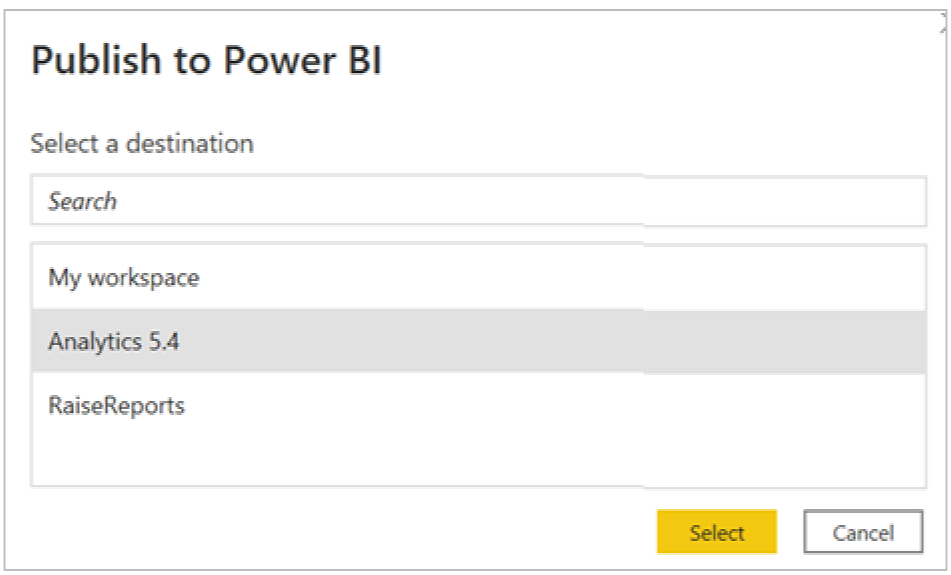


7. The PBIX file will now be loaded to the new database. Power BI Desktop points to the new data source, that is, the Analysis Services database which was just installed.

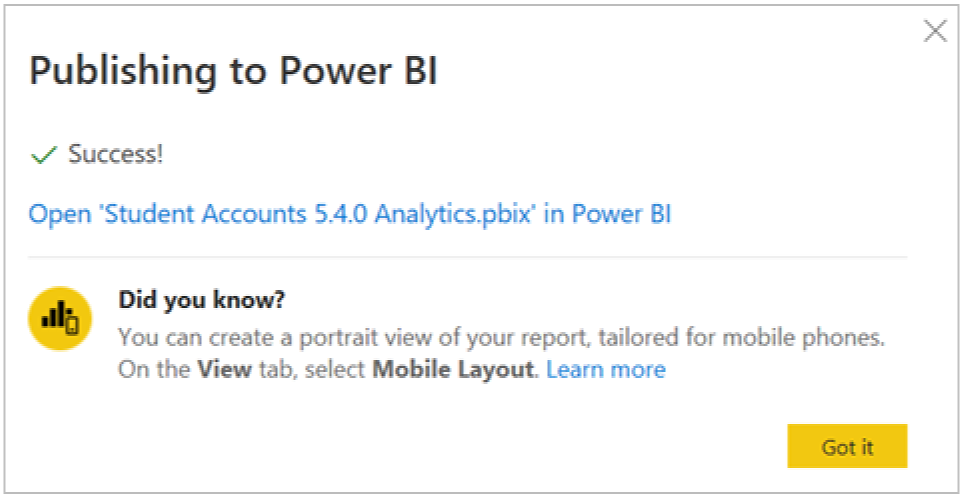
   Click the **tabs** at the bottom of the screen to view the sample reports provided with the product.



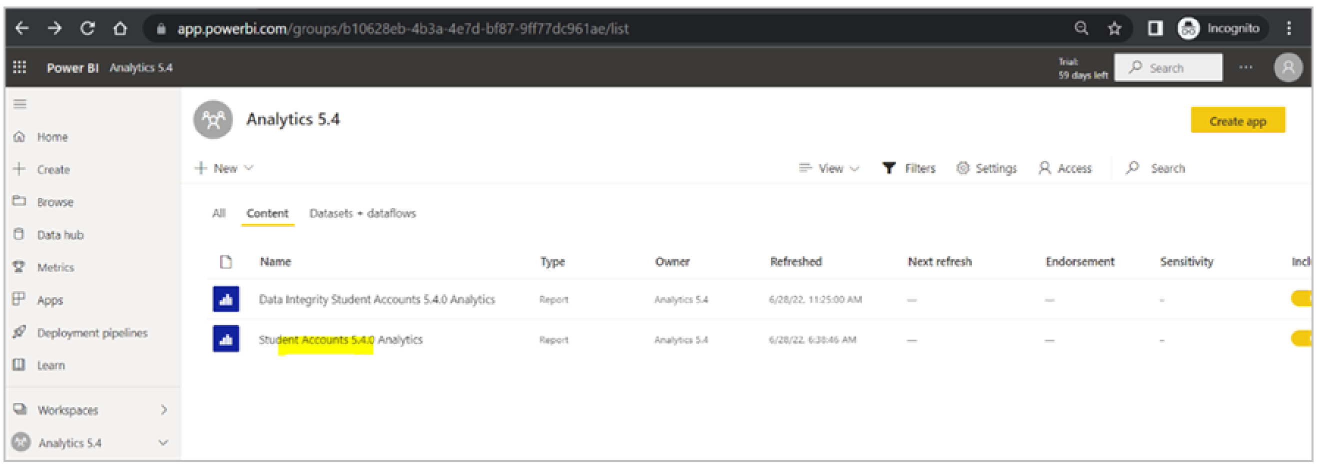
8. Once you have created an app workspace, Power BI prompts you to select the **destination** to publish to. The default is "My workspace". Select the app workspace created above. In our example the app workspace is Analytics 5.4.



9. Click **Got it** on the publishing success message. The PBIX in our example contains a report and a data set that were published to the Analytics 5.4 app workspace.

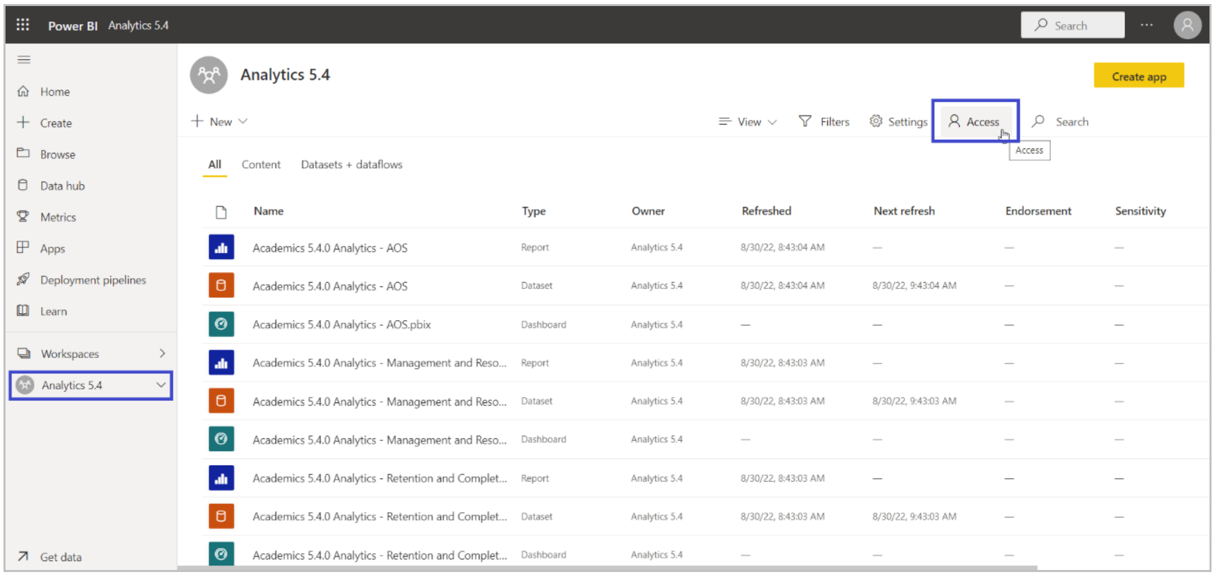


10. The Power BI service now shows that the Analytics 5.4 Reports (Content) and Datasets(Datasets+Dataflows) have been published.

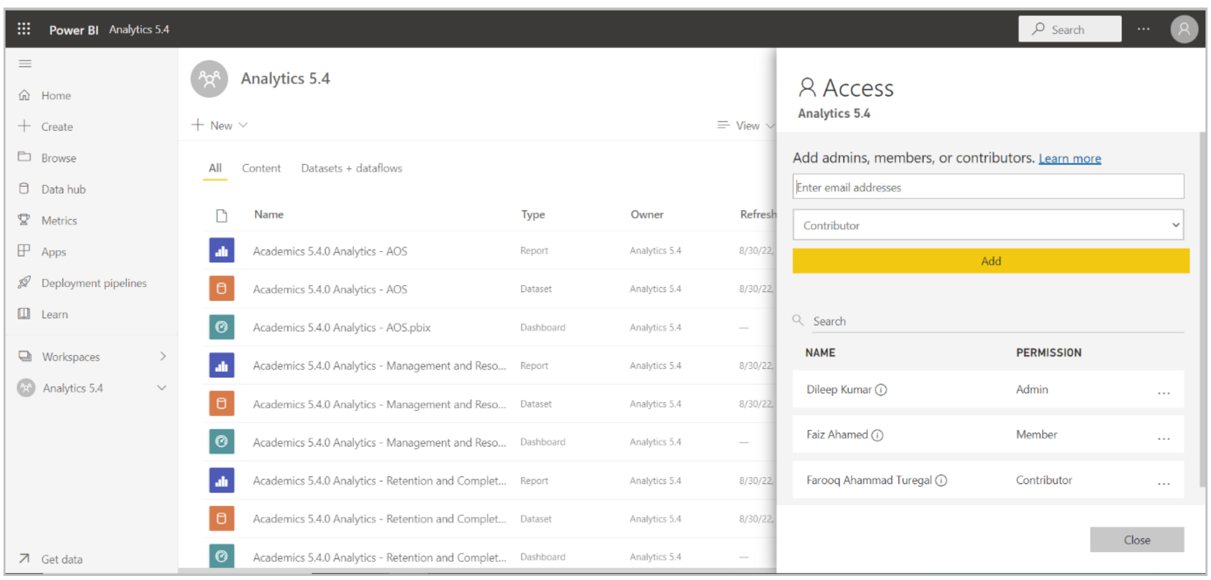


Add Admins, Members, and Contributors to your Workspace

1. Navigate to your workspace and click on **Access**.



2. Add Admins, Members, Contributors, and Viewers to your workspace.

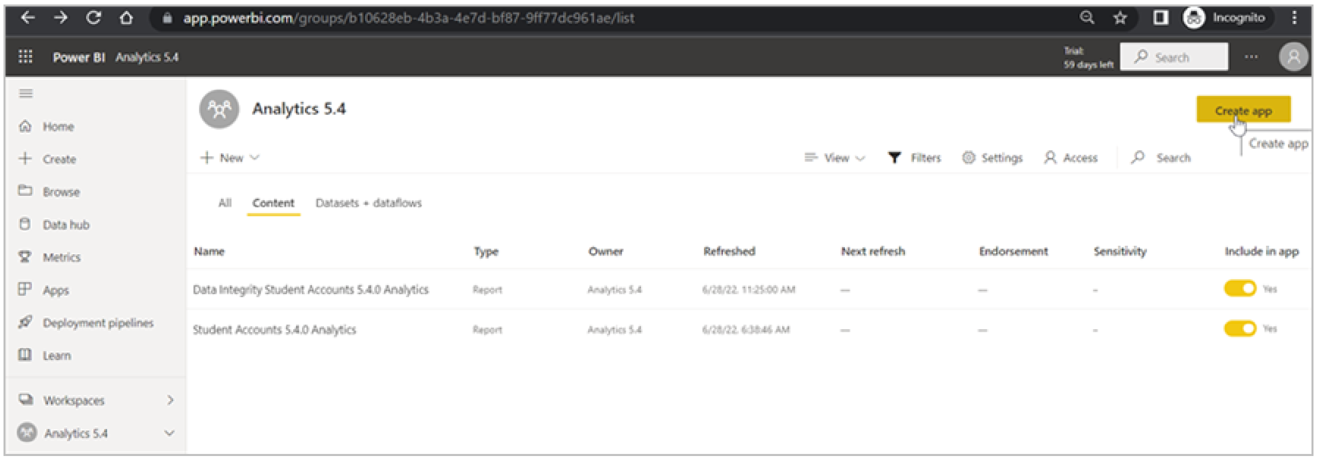


Publish an App

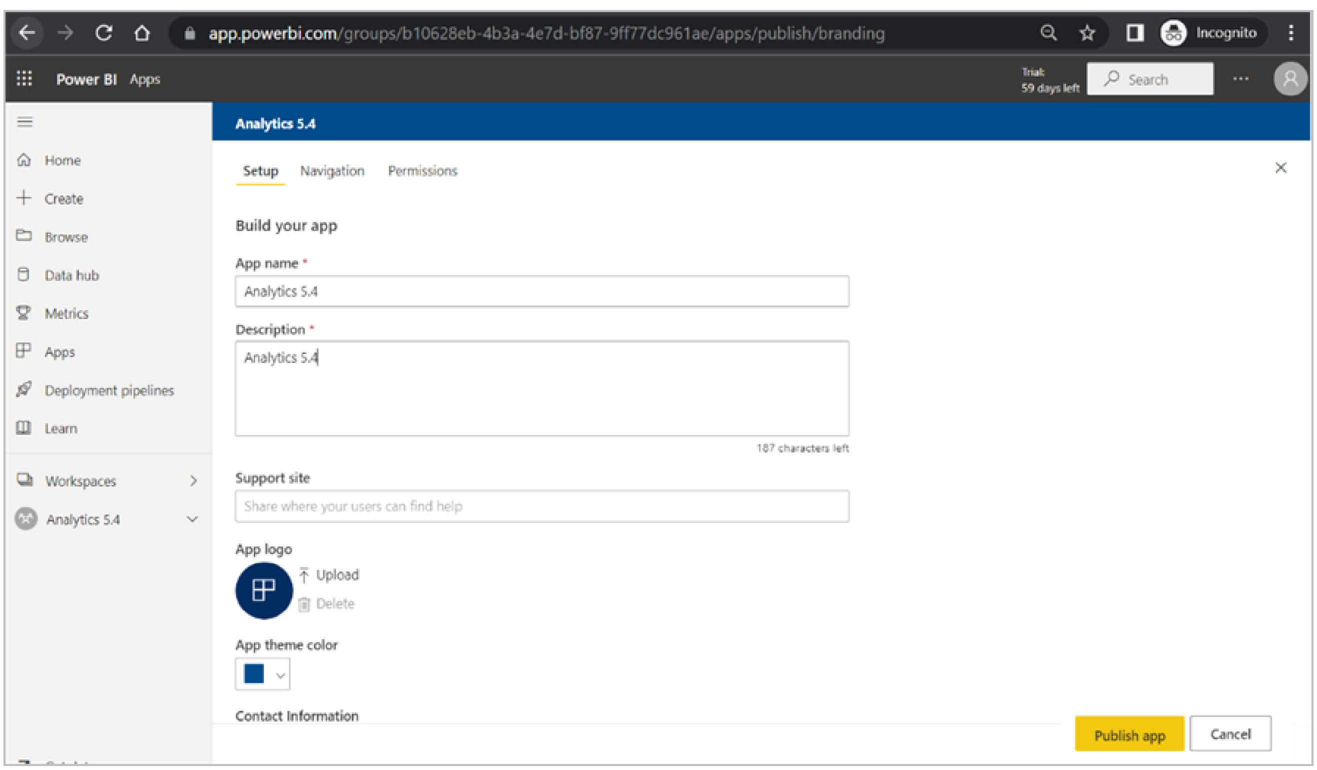
Nothing from the app workspace is available to the business end users until the content moves from the work-space to become an actual app.

1. To create an app, select the Reports tab or Datasets tab and click **Create app**.

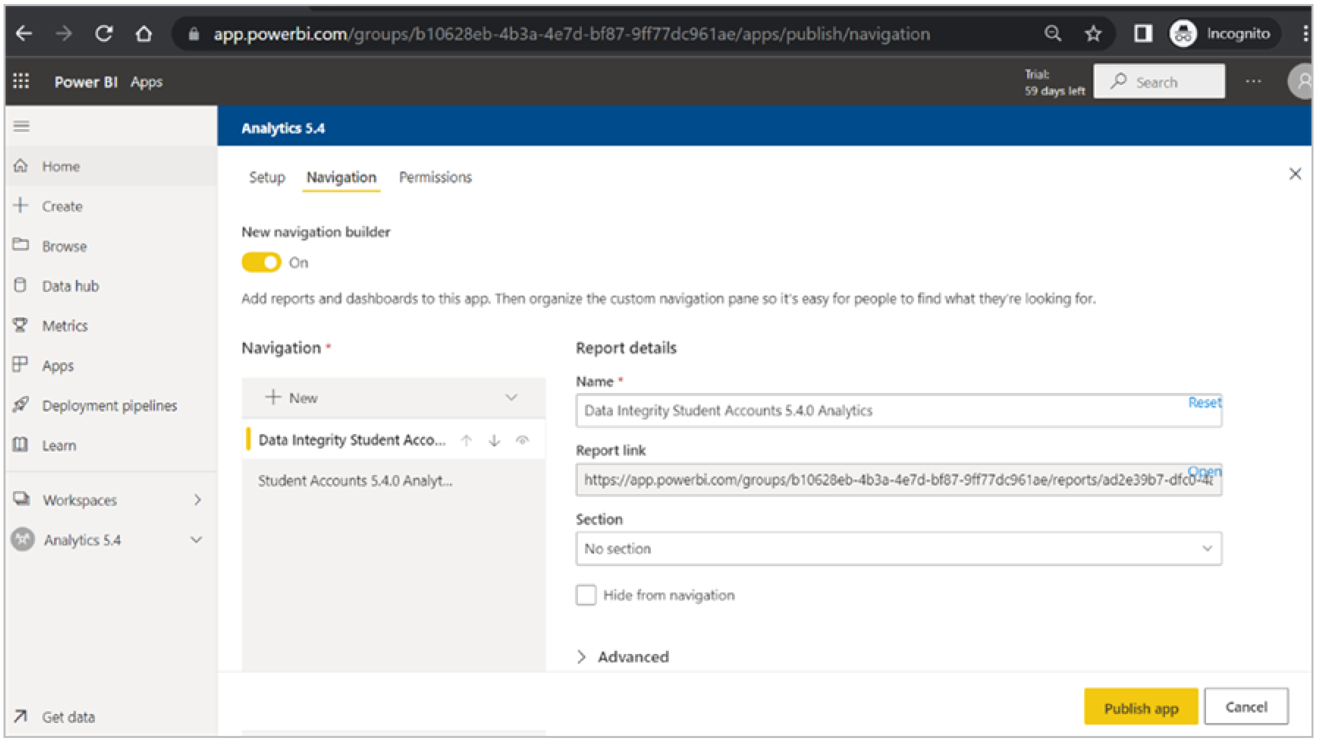
   Note: Use the “Include in app” option to include only the required reports in the app.

2. On the Setup tab, provide a **Description** of the app.

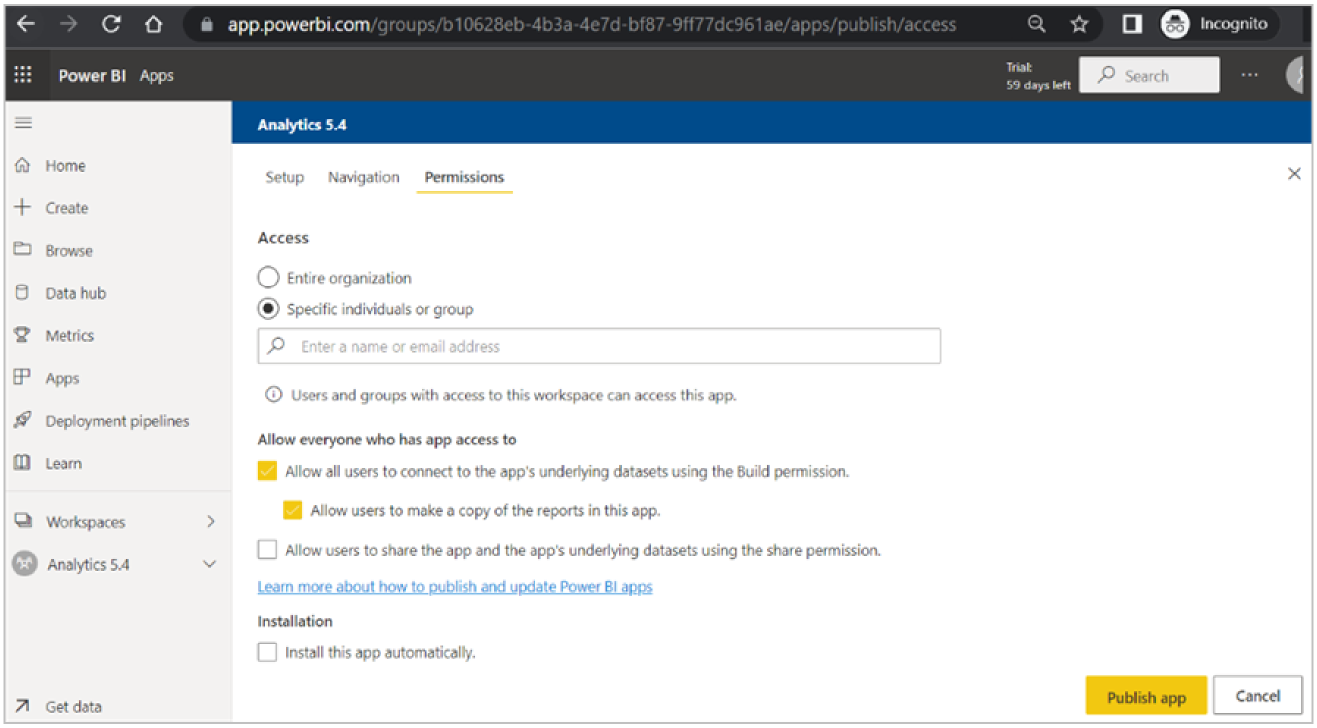
3. On the Navigation tab, select the **Report** that will be published.



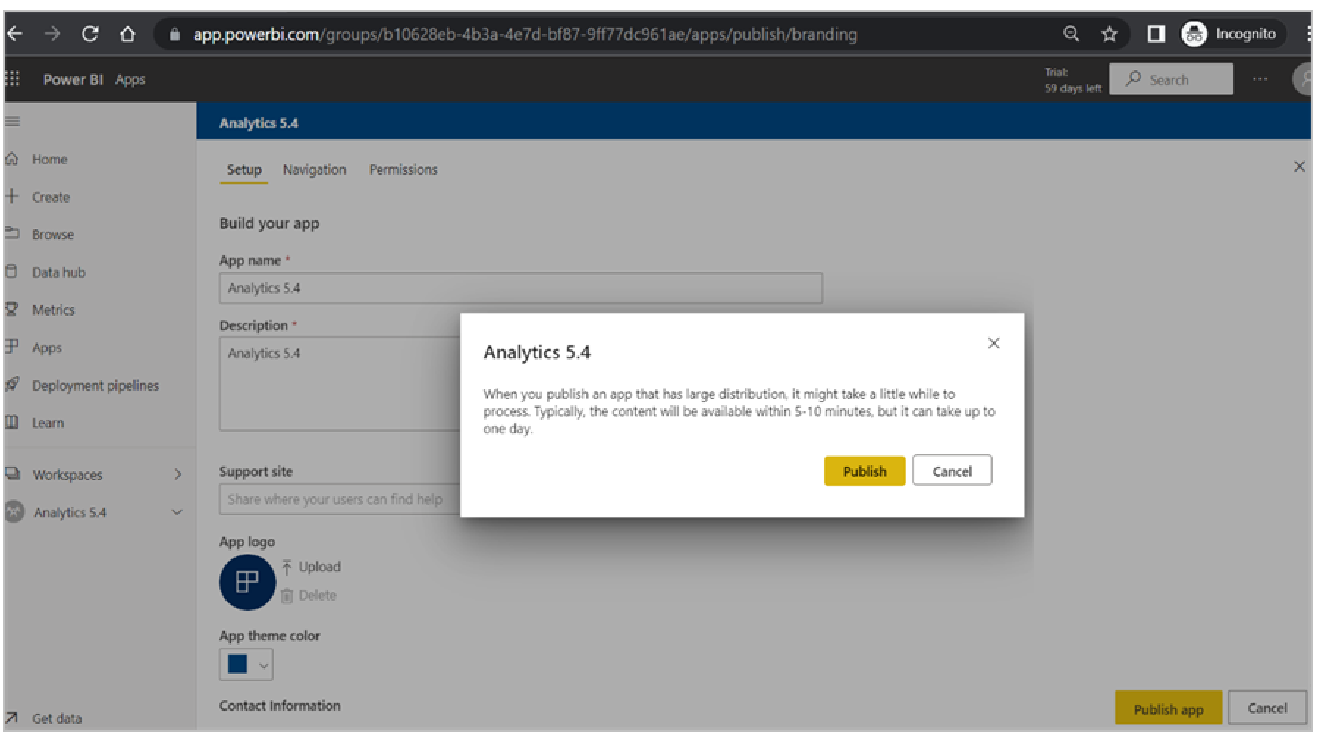
4. On the Permissions tab, select the **Access** for the app. You can choose the entire organization or specific individuals or groups. Click on **Publish**.

   Note: If Power BI is configured within Anthology Student and users want to access the Analytics Reports from this app workspace, they need to first get this app by logging in to their https://app.powerbi.com/ account.

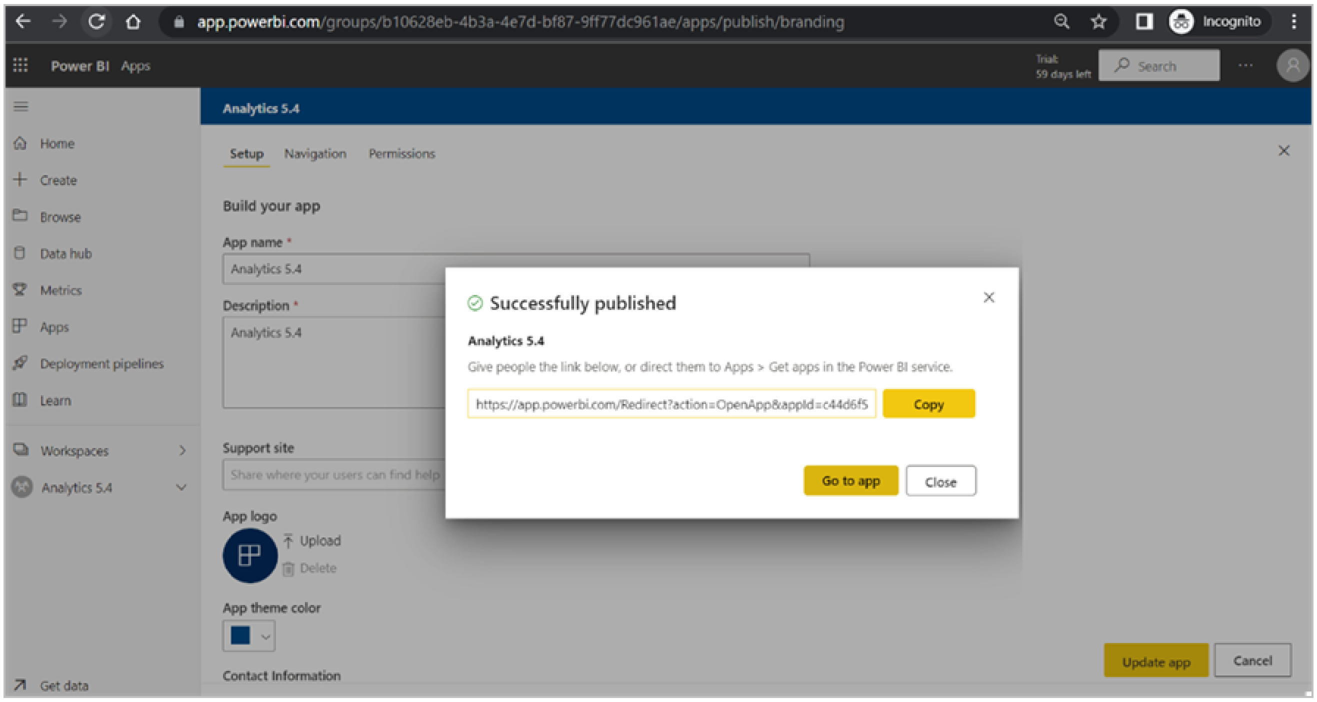
   The option "Install this app automatically" is available. When it is selected, the app will be automatically installed for those who have permission to this app.



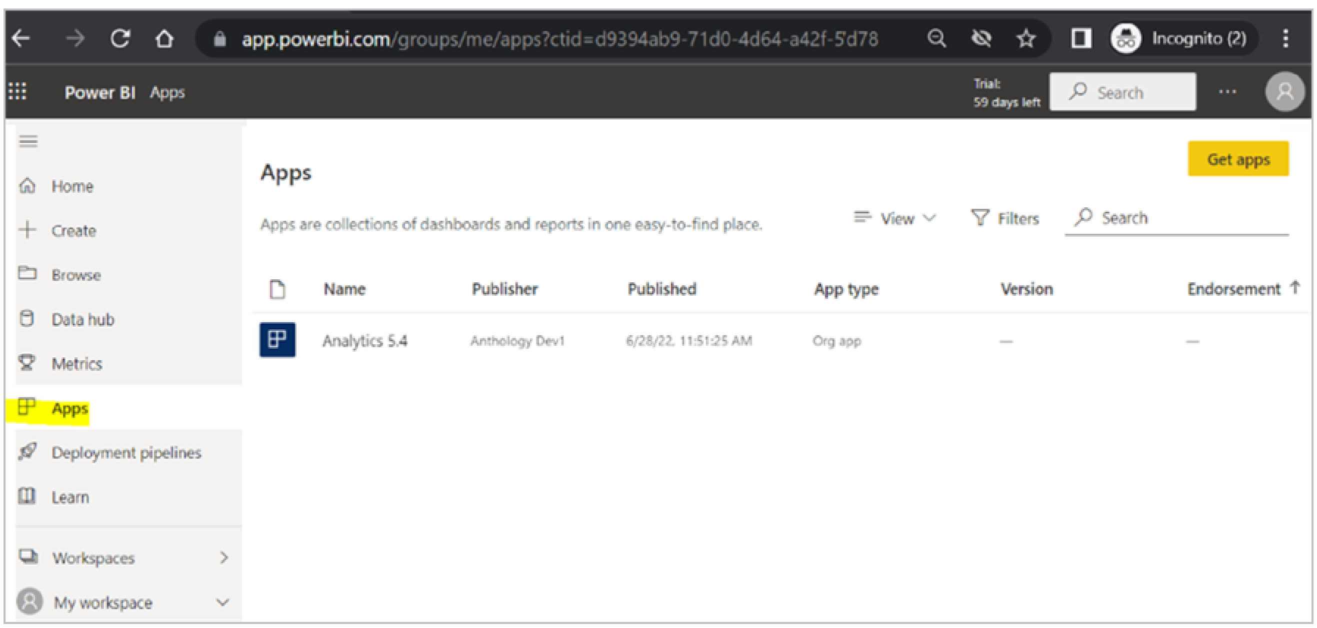
5. Click **Publish** on the Ready to publish dialog.



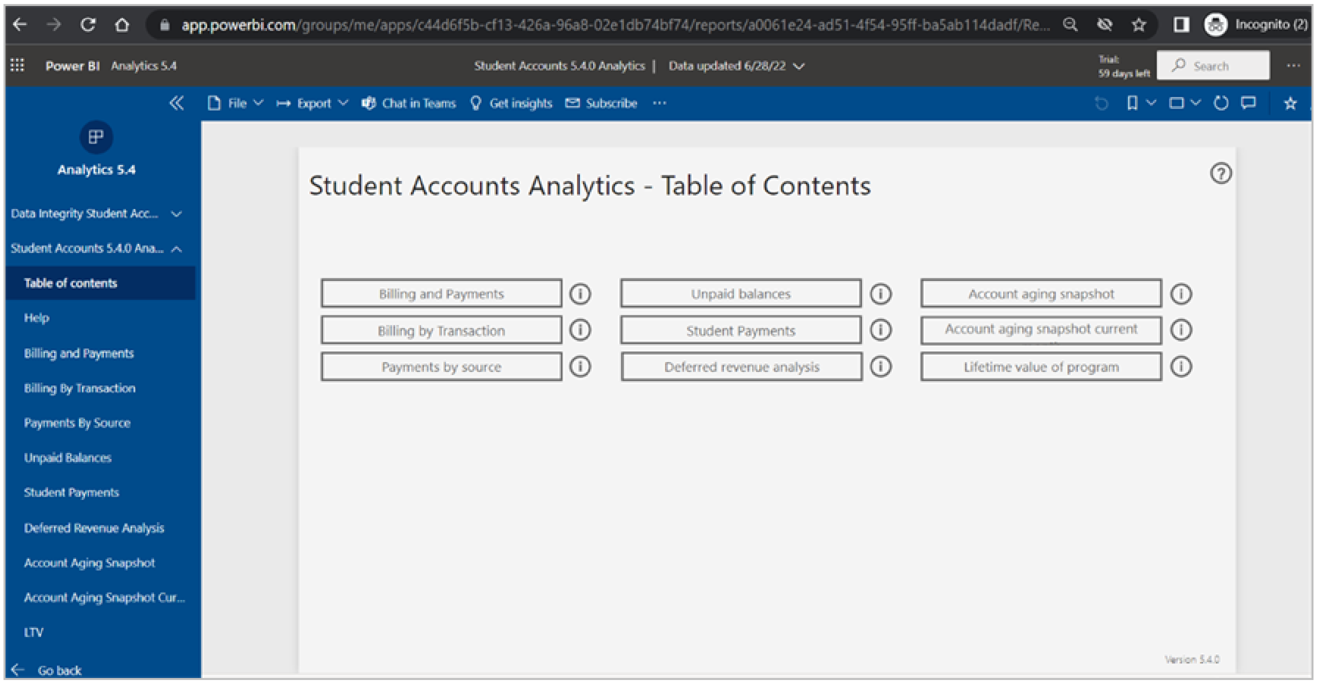
6. The *Successfully Published* message provides a URL that can be shared with anyone who has been given permissions to use the app. Click **Copy** to copy the URL to clipboard and click **Go to app**.



7. Select the **Apps** menu to view the app.



In our example, the landing page for the app is the report selected above ("Student Accounts").


app.powerbi.com/groups/me/apps/c44d6f5b-cf13-426a-96a8-02e1db74bf74/reports/a0061e24-ad51-4f54-95ff-ba5ab114dadf/Re...
Incognito (2)
Power BI Analytics 5.4
Student Accounts 5.4.0 Analytics | Data updated 6/28/22
Trial: 59 days left
Search
File
Export
Chat in Teams
Get insights
Subscribe
Analytics 5.4
Data Integrity Student Acc...
Student Accounts 5.4.0 Ana...
Table of contents
Help
Billing and Payments
Billing By Transaction
Payments By Source
Unpaid Balances
Student Payments
Deferred Revenue Analysis
Account Aging Snapshot
Account Aging Snapshot Cur...
LTV
Go back
Student Accounts Analytics - Table of Contents
Billing and Payments
Unpaid balances
Account aging snapshot
Billing by Transaction
Student Payments
Account aging snapshot current
Payments by source
Deferred revenue analysis
Lifetime value of program
Version 5.4.0

Forms Builder

Installation Manager supports the installation of multiple versions of Forms Builder. Forms Builder 2.x and Forms Builder 3.x and later can be installed side by side. Forms Builder 3.x and later is a new product; it is not an upgrade of Forms Builder 2.x. The installation steps for each version are different.

Select the appropriate link to continue:

- Forms Builder 2.x
- Forms Builder 3.x and Later

Forms Builder 2.x

You can use Installation Manager to install the Forms Builder application. Forms Builder is an easy-to-use, web-based application for the creation, design, publication, and management of electronic form workflows. It enables organizations to quickly customize complex processes without the need for expensive programming, custom web design, or service costs. Forms Builder enables users to create forms for every constituent at the institution: new applicants, existing students, faculty, and staff.

Prerequisites

Note: Installation Manager checks for the prerequisites to be installed. It does not install them.

For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Installation Manager installs the following components:

- Forms Builder
- Security Token Service (STS)

  > ⚠ Forms Builder version 2.3.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

- If you are using Anthology Student and Workflow with Forms Builder, the Forms Builder Contracts and Activities are required. Go to the **Start** screen and select **Package Manager**. Download the **Forms Builder Contracts and Activities** package and install it.

Software Prerequisites

Microsoft .NET Framework 4.5.1

Accounts, Permissions, and Other Prerequisites

- Only Integrated Authentication for SQL can be used to install Forms Builder.
- If a Forms Builder database does not exist, a blank Forms Builder database must be created prior to installing Forms Builder.
- All Forms Builder web applications use ApplicationPoolIdentity for authentication. To avoid errors during the Forms Builder installation, ensure that the following permissions are set up:

  If Forms Builder and Database are on different machines, ensure that Domain\Form-sBuilderMachineName$ has db_owner permission to the Forms Builder, Anthology Student, Portal, or CampusNexus CRM database before starting the installation.

If Forms Builder is on same machine as the SQL server, ensure NT Authority\system and NT Authority\Network Service has db_owner permission to the Forms Builder, Anthology Student, Portal, or CampusNexus CRM database before starting the installation.

Postinstallation steps when Forms Builder and Database are on the same server

- If Forms Builder and SQL are on the same machine, then after Forms Builder is installed, the application pools for all Forms Builder web applications need to change from ApplicationPoolIdentity to built-in NetworkService account.
- In a few instances, the Forms Builder CRM Adapter, Designer and Renderer websites may need to be running under the service account to launch Forms Builder Designer.
- The application pools that are installed as part of Forms Builder must be added to the database as db_owner.

  For example, the following accounts need to be added to Anthology Student, Portal, or CampusNexus CRM and Forms Builder databases:

  - IIS AppPool\CMCPortalSTSAppPool
  - IIS AppPool\CMCFormsBuilderAdapterAppPool
  - IIS AppPool\CMCFormsBuilderDesignerAppPool
  - IIS AppPool\CMCFormsRendererAppPool
  - IIS AppPool\CMCDataServiceAppPool
  - IIS AppPool\CRMFormsBuilderAdapterAppPool

Forms Builder License

Please contact Support to get a license script.

Forms Builder for CampusNexus CRM

- The Forms Builder machine needs to have access db_owner permission to the CampusNexus CRM Main database.

  Domain\FormsBuilderMachine$ has to be added to SQL security with db_owner rights.

- Forms Builder uses the Security Token Service package delivered with CampusNexus CRM Web Client. Therefore, the installation of Web Client is a prerequisite for Forms Builder when Forms Builder is intended for use with CampusNexus CRM.
- CampusNexus CRM Application Server is a prerequisite for installing Forms Builder.

If Forms Builder is being installed to a machine where the CampusNexus CRM Application Server is not installed, an instance of Application Server has to be installed before installing Forms Builder. Alternatively, Forms Builder can be installed on the Application Server machine.

- CampusNexus CRM 10.1 should be installed before installing Forms Builder 2.1.
- Forms Builder 2.0 cannot be installed on CampusNexus CRM 10.1.

Forms Builder for Anthology Student

- Forms Builder uses Student API and Portal web services to log in. Therefore, the installation of Anthology Student and Portal is a prerequisite for Forms Builder when Forms Builder is intended for use with Anthology Student.
- The Forms Builder machine needs to have access db_owner permission to the Anthology Student database as well as the Portal database.
- Domain\FormsBuilderMachine$ has to be added to SQL Security with db_owner rights.
- Student Portal web services must be accessible from the server where Forms Builder is installed.

Conditional Postinstallation Step for Forms Builder

If Forms Builder is being installed on a Windows Server 2012 that has SharePoint Foundation 2013 installed, the following script must be executed to avoid errors when rendering a Form.

%windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/globalModules /[name='SPNativeRequestModule'].preCondition:integratedMode,bitness64

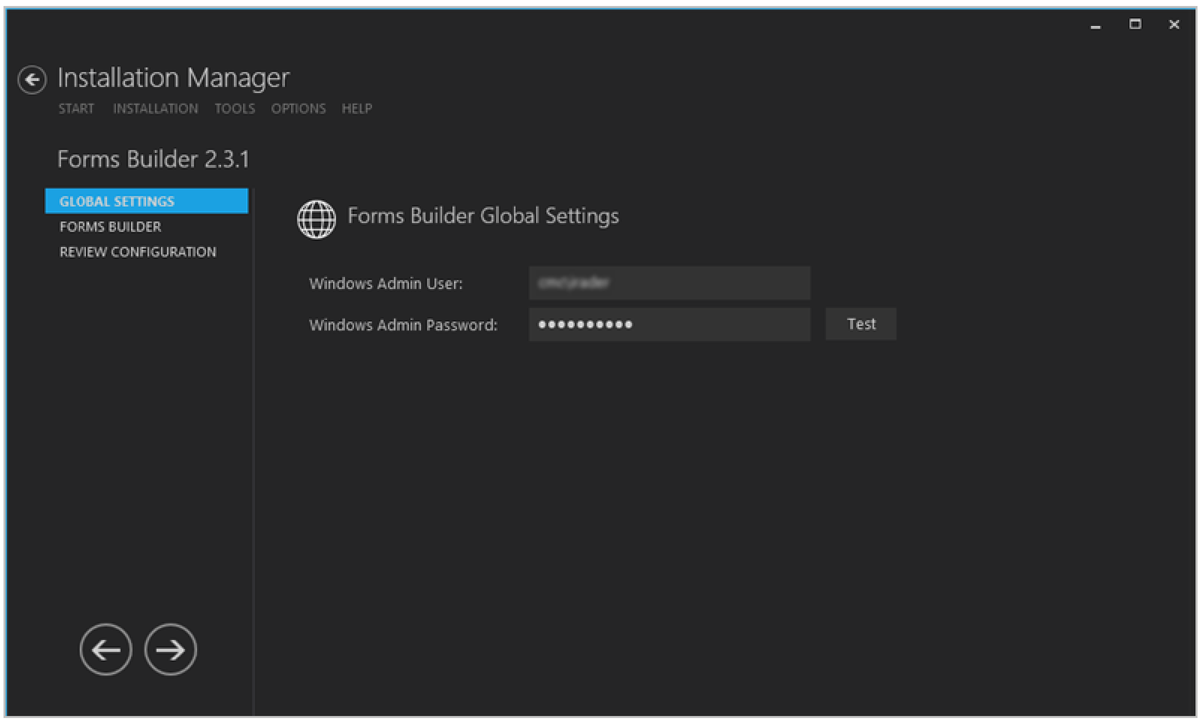
Global Settings

The Global Settings screen contains the user name and password used when starting a Forms Builder installation. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click **Forms Builder**. The Forms Builder Global Settings screen is displayed.



2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer on which the installation will occur. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.
4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

5. If the user is authenticated, click **OK** and click  to continue.

Forms Builder

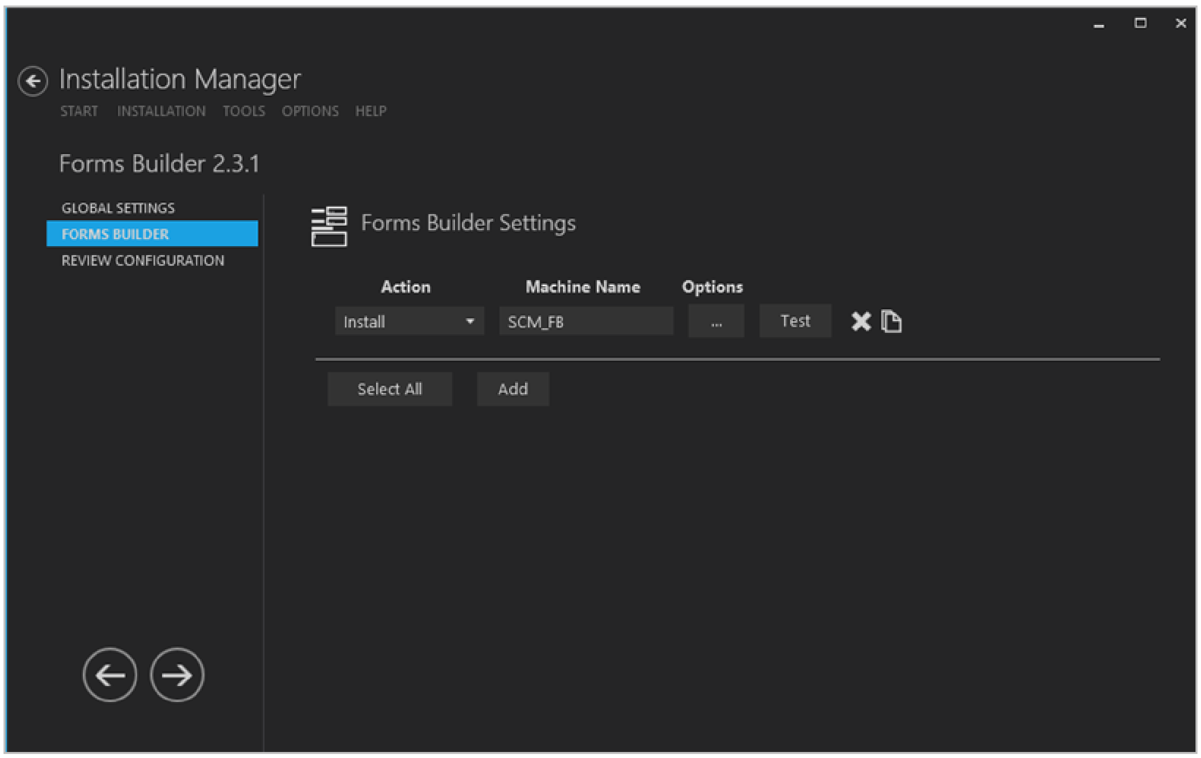
This Settings screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and configuration options for Forms Builder.

Prerequisites

Forms Builder version 2.3.0 or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

Set Up Forms Builder

1. In the Installation menu, click the **Forms Builder** 2.x tile. The Forms Builder Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.

- **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

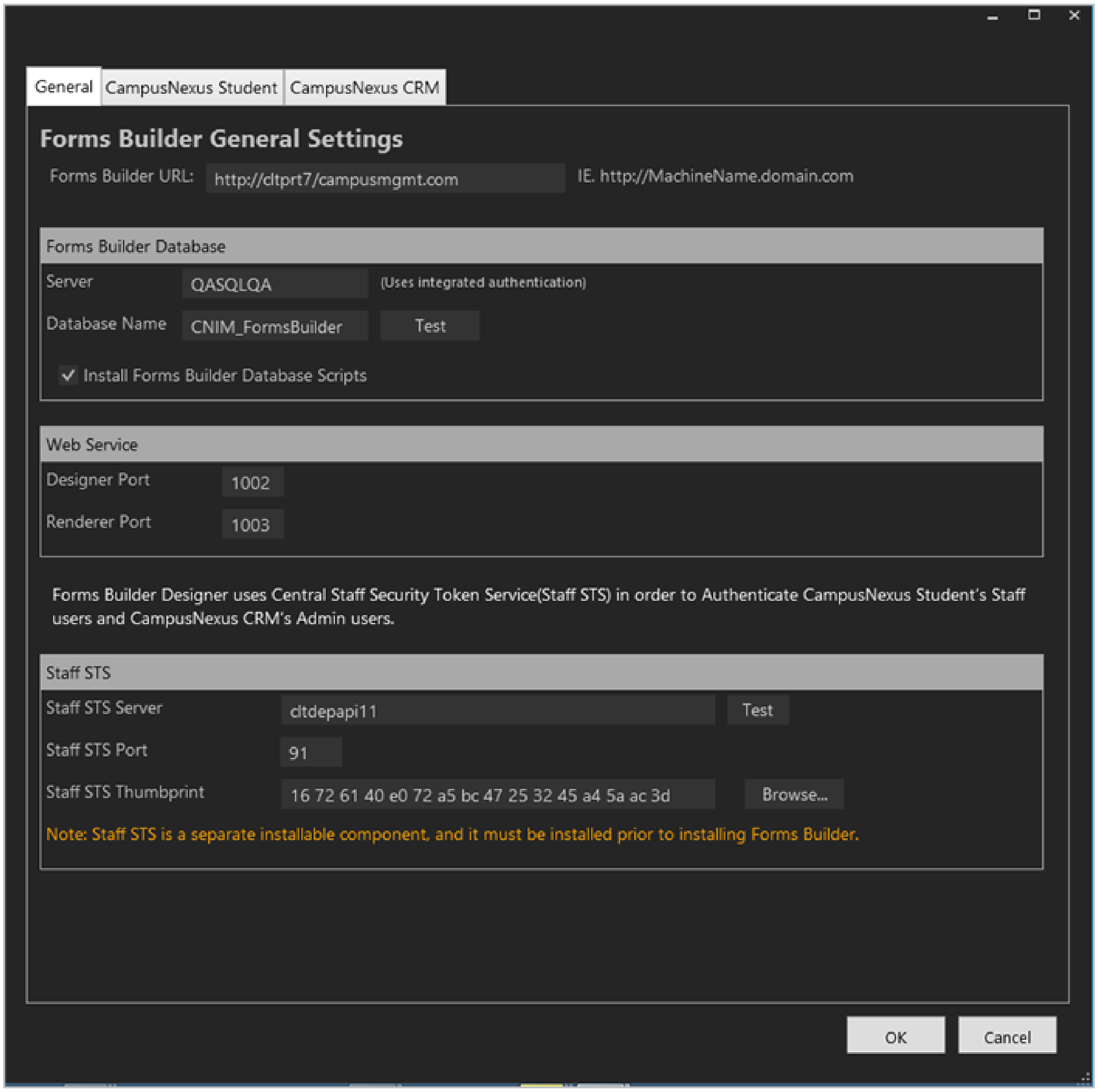
  Note: The Uninstall option does not completely revert the environment, for example, the Forms Builder database is not removed.

Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.

4. Enter the **Machine Name** for the component to be installed.
5. Click to copy a line. Edit the copied line as needed.
6. Click to view and edit the Options form for the Forms Builder Settings. The form contains the following tabs:

   General Tab

   Settings on this tab are required and common to all components of Forms Builder.



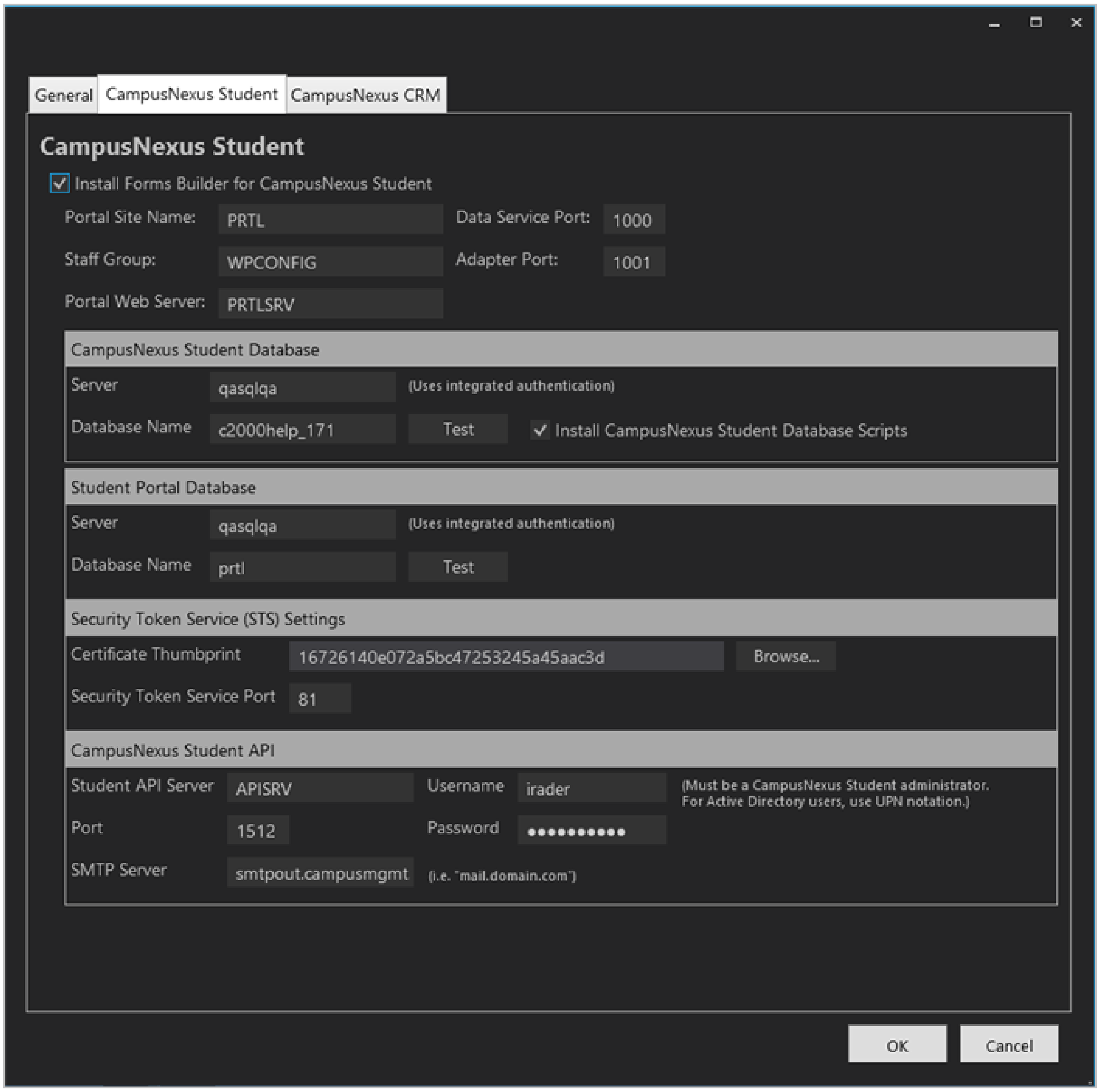
General Tab Fields

Field	Description
Forms Builder URL	Website where the Forms Builder application will be accessed by end users. Format: `http://MachineName.domain.com`
Forms Builder Database	
Server	Name of the Forms Builder SQL database server. The Server uses integrated authentication. For a fresh installation, a new blank database needs to be created.
Database Name	Name of the Forms Builder SQL database.
Test	Click **Test** to verify the database connection.

Field	Description
Install Forms Builder Database Scripts	Clear this check box if you do not want to install the Forms Builder database scripts.
Web Service	
Designer Port	Specify the port number of the Forms Builder Designer port or accept the default (1002).
Renderer Port	Specify the port number of the Forms Builder Renderer port or accept the default (1003).
Staff STS	
Staff STS Server	Specify the name of the Staff STS Server. The Staff STS Server must have been previously installed. See Staff STS.
Test	Click **Test** to verify the STS connection.
Staff STS Port	Specify the port number of the installed Staff STS server or accept the default (91).
Staff STS Thumbprint	Certificate thumbprint from IIS. The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

Anthology Student Tab

Settings on this tab are required if Forms Builder for Anthology Student is installed.



Anthology Student Tab Fields

Field	Description
Install Forms Builder for Anthology Student	Select this check box to install Forms Builder for Anthology Student. The related fields are enabled.
Portal Site Name	Site Name configured for the Portal ('legacy' portal) login page. The Portal SiteName is PRTL by default. The Portal Site Name value is found in the web.config file under Appsettings of Portal ('legacy'). The SiteName value is used for Anthology Student STS and Anthology Student Adapter.
Staff Group	Specify the Staff Group name. The Staff Group is WPCONFIG by default. The Staff Group is appended in the Forms Builder Designer web config file.

Field	Description
Portal Web Server	Specify the Portal Web Server name. The SySiteSettings of the Anthology Student database will be modified with Portal Server Name in the Portal WebService URLs. For a Load Balanced Portal environment, enter the load balancer server.
Data Service Port	Specify the port number for the Data Service port or accept the default (1000). The Data Services are of the latest version of Anthology Student services.
Adapter Port	Specify the port number for the Anthology Student Adapter port or accept the default (1001).
Anthology Student Database	
Server	Name of the Anthology Student SQL database server. The Server uses integrated authentication.
Database Name	Name of the Anthology Student SQL database.
Test	Click **Test** to verify the database connection.
Install Anthology Student Database Scripts	This option is selected by default. It installs scripts for the Anthology Student database. The related fields are enabled.
Student Portal Database	
Server	Name of the Student Portal SQL database server. The Server uses integrated authentication. The SySiteSettings of the Anthology Student database are modified with Portal Server Name in the Portal WebService URLs. For a Load Balanced Portal environment, enter the load balancer server.
Database Name	Name of the Student Portal SQL database.
Test	Click **Test** to verify the database connection.
Security Token Service (STS) Settings	

Field	Description
Certificate Thumbprint	Certificate thumbprint from IIS. Copy and paste the thumbprint into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Security Token Service Port	Specify the port number of the STS server or accept the default (81).
Anthology Student API	
Student API Server	Name of the Anthology Student API server.
Port	Specify the port number of the Anthology Student API.
SMTP Server	Specify the SMTP Server address in the format "mail.domain.com". This setting populates or overwrites the mailSettings under System.net in the Web.config file. This setting is required for some Workflow activities when Forms Builder is integrated with Anthology Student.
Username	User name or account used to create workflows for Forms Builder. The user must be an Anthology Student administrator. For Active Directory users, use the user principal name (UPN) notation.
Password	Password used to by the Anthology Student admin user.

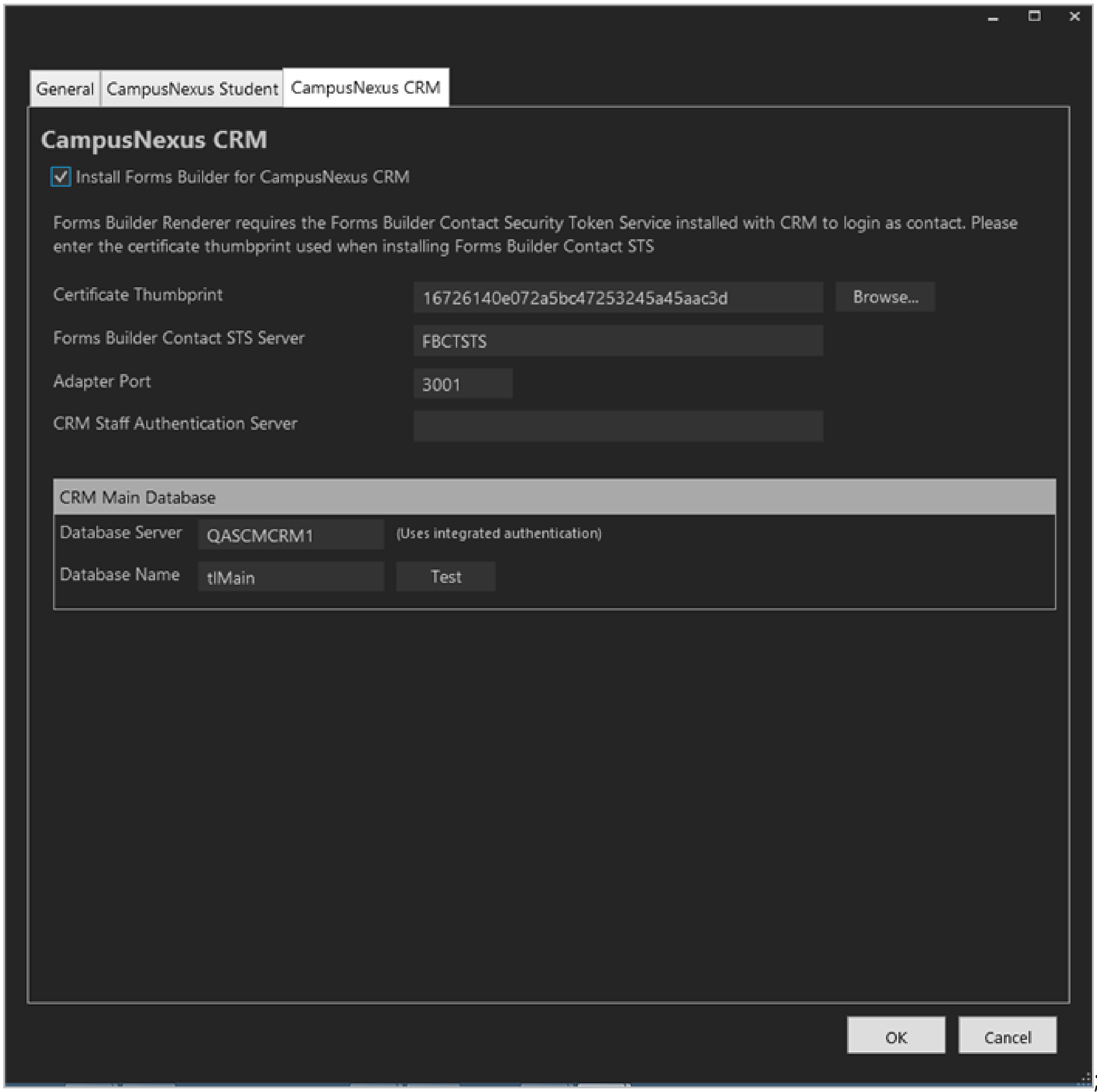
CampusNexus CRM Tab

Settings on this tab are required if Forms Builder for CampusNexus CRM is installed.

Notes:

- Forms Builder uses the STS package delivered with Forms Builder Contact STS. Therefore, the installation of Forms Builder Contact STS is a prerequisite when Forms Builder is intended for use with CampusNexus CRM.

- An instance of CRM Application Server needs to be installed on the machine where Forms Builder is being installed.



;

CampusNexus CRM Tab Fields

Field	Description
Install Forms Builder for Cam-pusNexus CRM	Select this check box to install Forms Builder for CampusNexus CRM. The CRM Main Database fields are enabled.

Field	Description
Certificate Thumbprint	Certificate thumbprint used when installing the Forms Builder Contact STS. Copy and paste the thumbprint into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Forms Builder Contact STS	Name of the Forms Builder Contact STS host.
Adapter Port	Specify the port number of the adapter for CampusNexus CRM or accept the default (3001).
CRM Staff Authentication Server	If applicable, enter the name of the server where the CRM Staff Authentication Service is installed. Installation Manager will construct the complete URL based on the Server name. `http://StaffAuthenticationServiceServer/Cmc.NexusCrm.WebServices` The CRMStaffAuthenticationServiceURL will be inserted into the syregistry table in the Anthology Student database.
CRM Main Database	
Database Server	Name of the server that hosts the Main database for CampusNexus CRM. The Server uses integrated authentication.
Database Name	Name of the Main database for CampusNexus CRM.
Test	Click **Test** to verify the database connection.

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.

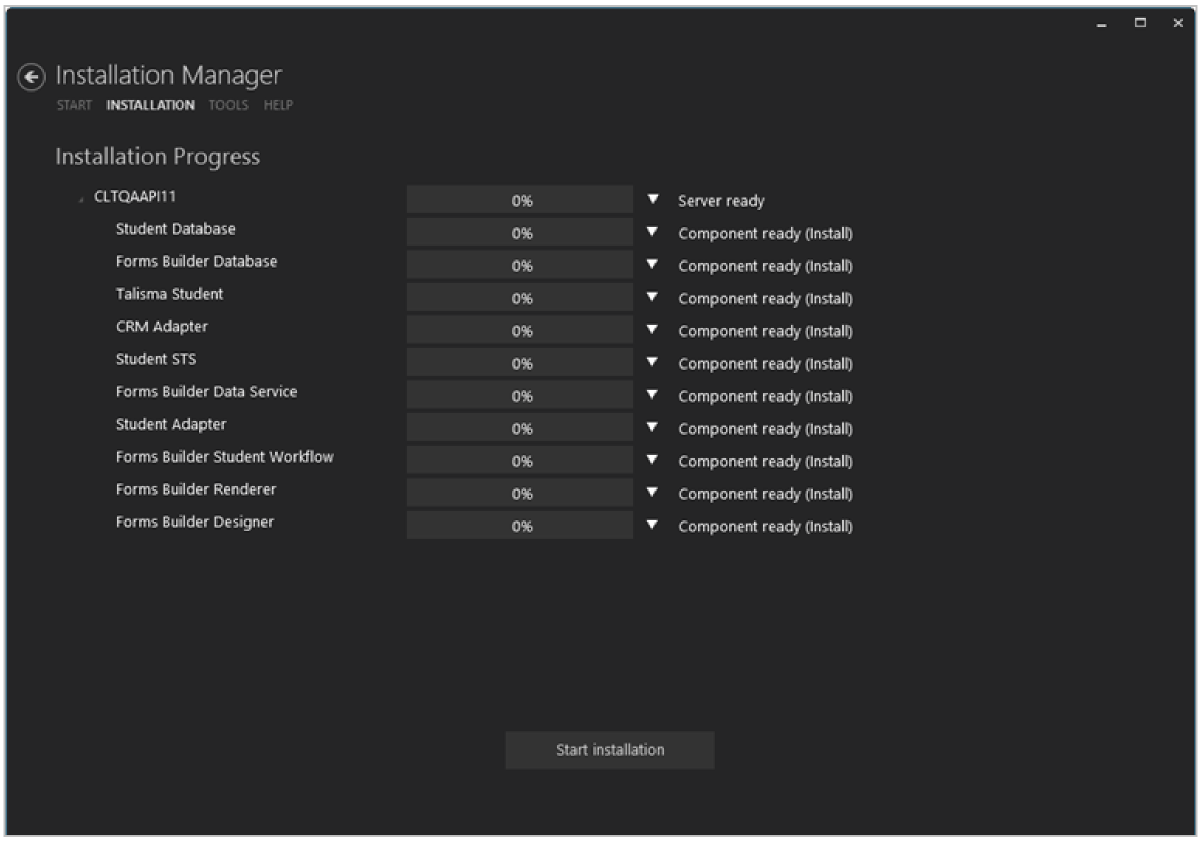
10. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

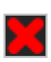
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.

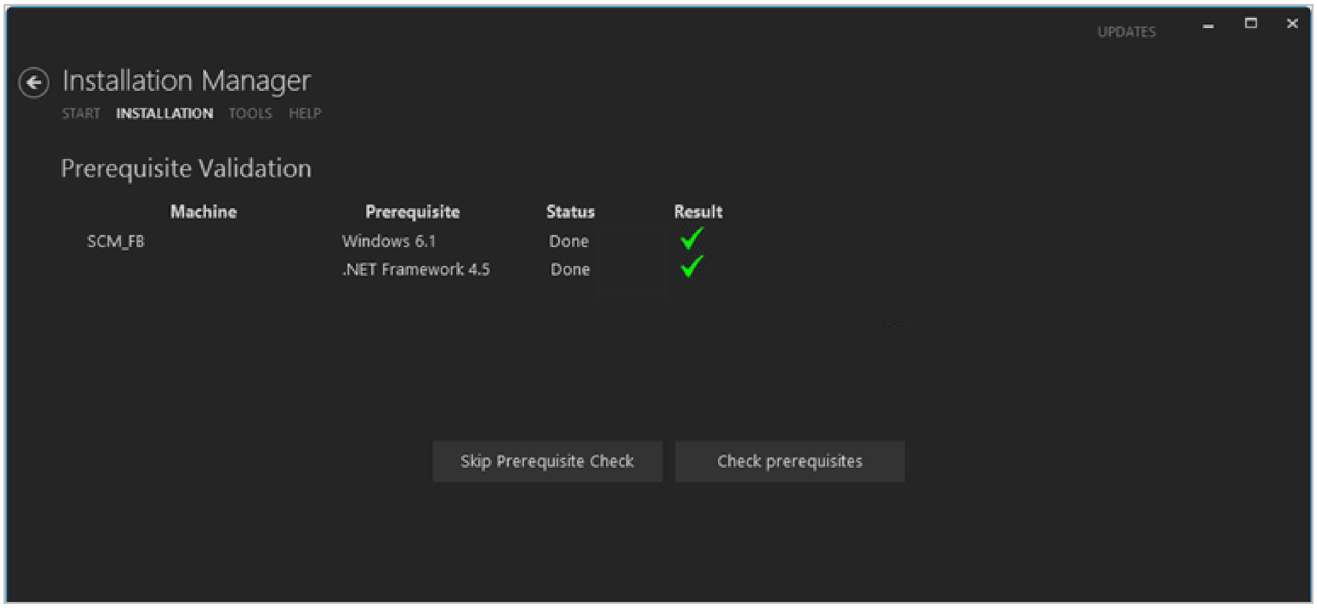


2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

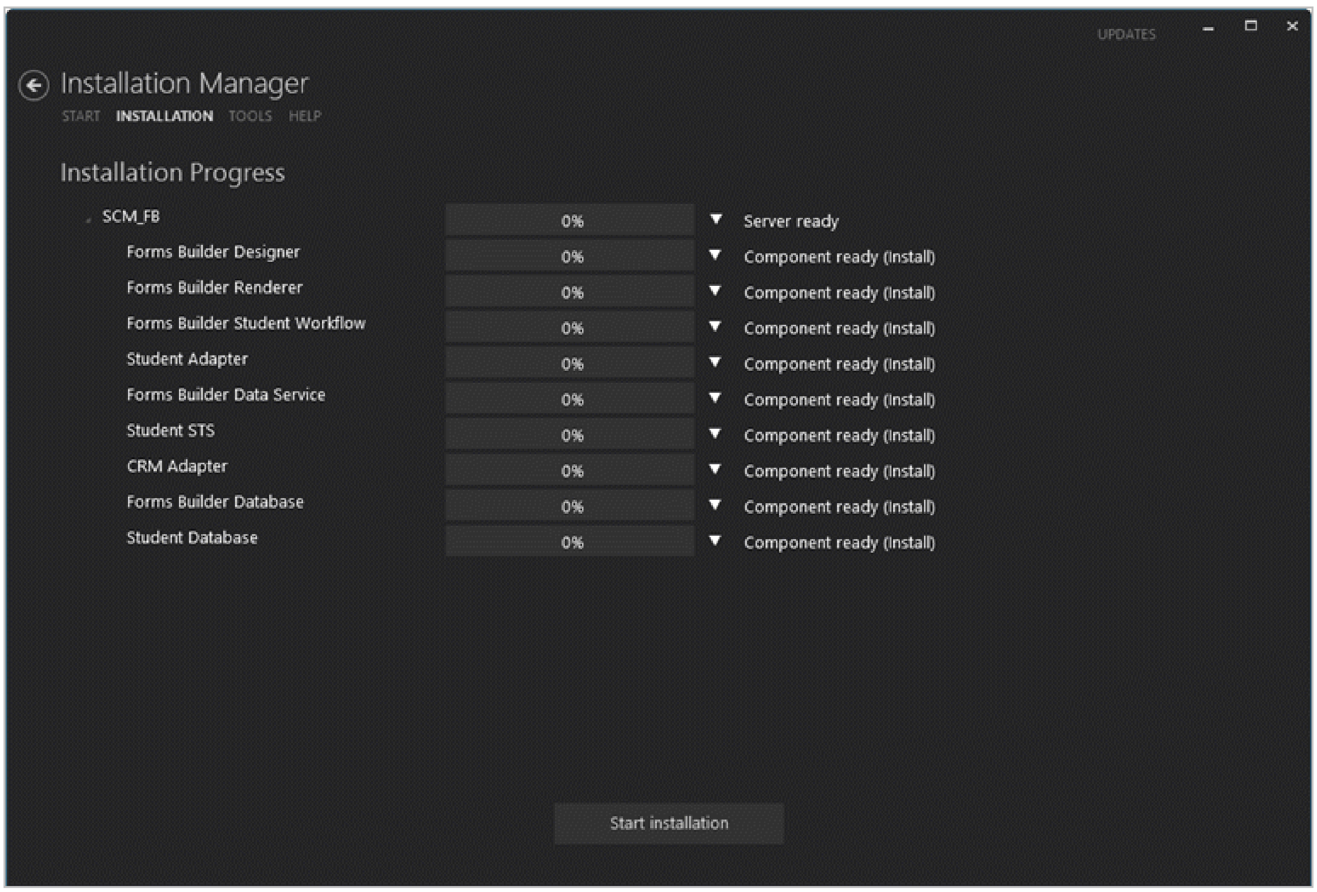
 Indicates that the component passed the prerequisites check.

 Indicates that the component failed the prerequisites check.

Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.



3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.



4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.
6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

Postinstallation Steps

Depending on your environment, the following postinstallation steps may be necessary.

- Postinstallation steps when Forms Builder and Database are on the same server.
- Conditional Postinstallation Step for Forms Builder (if Forms Builder is installed on a Windows Server 2012 that has SharePoint Foundation 2013 installed).

Verify the Forms Builder Installation

To ensure that Forms Builder is successfully installed:

1. Navigate to `http://<FormsBuilder URL>:1002` to invoke the Forms Builder application.
2. For Anthology Student, log on to Forms Designer as a staff member to ensure that all the fields are populated.
3. Click **Configuration** and make sure the link points to the correct `CvueFBAdapterService.svc`. Verify the following items:
   a. The Fields grid in the Forms Builder Toolbox is populated.
   b. Click the **Configuration** link in the Toolbox. The URL on the Adapter tab should return a WCF response.

      If the Forms Builder license is not applied on the Forms Builder Database, the Configuration dialog will not be displayed.
   c. The correct version number is displayed in the status bar.
4. Verify that the Forms Builder Renderer page can be opened at the following URL:

   `http://<FormsBuilder URL>:1003//Home/PublishedSequences`

Forms Builder 3.x and Later

In version 3.x, the Forms Builder application has been redesigned and architecturally reengineered to take advantage of the Anthology object model. The new generation of Forms Builder uses OData (Open Data Protocol) to access and expose data from various data sources. The Adapter for queries from the CampusNexus CRM or Anthology Student databases is no longer required.

Forms Builder 3.x and later can be installed to connect to the Anthology Student database, the CampusNexus CRM database, or both giving Forms Builder access to the associated database entities and fields. Forms Builder 3.x does not have its own database; it uses the database schema that is part of the CampusNexus object model.

Forms Builder 3.x and later provides greater flexibility to the user and enables integration with Workflow (“Form Flow”). Each new sequence that is created and saved automatically creates a corresponding workflow definition that can be further customized/edited using the Workflow Composer.

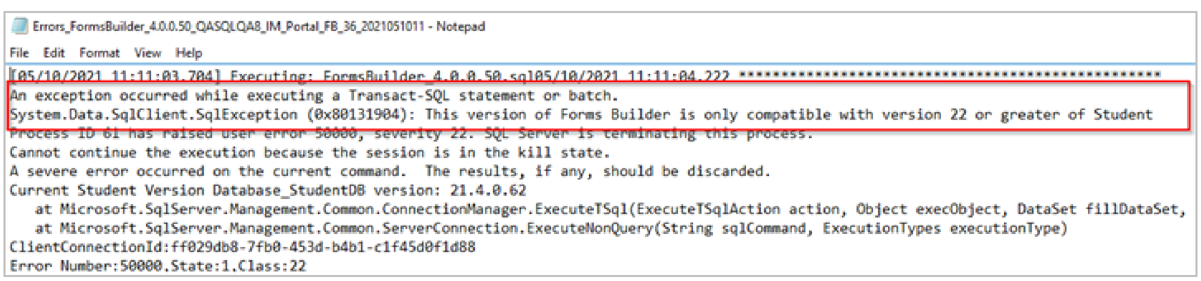
Forms Builder 3.x and later uses the Staff STS for Designer logins and CMCPortalSTS/FB Contact STS for Renderer logins.

Prerequisites

Note: Installation Manager checks for the prerequisites to be installed. It does not install them. For information on compatibility with operating platforms and other products, see Platform Compatibility and Product Compatibility (logon required).

Due to significant architectural changes needed to support cloud deployments, Forms Builder 4.0 is only compatible with Anthology Student 22.0, Workflow Composer 4.0, and CampusNexus CRM 13.0 and higher.

If Anthology Student 22.0 or higher is not found during the installation of Forms Builder 4.x, an exception occurs and is displayed in the log.


Errors_FormsBuilder_4.0.0.50_QASQLQA8_IM_Portal_FB_36_2021051011 - Notepad

File Edit Format View Help

```
[05/10/2021 11:11:03.704] Executing: FormsBuilder_4.0.0.50.sql05/10/2021 11:11:04.222 ***************************************************
An exception occurred while executing a Transact-SQL statement or batch.
System.Data.SqlClient.SqlException (0x80131904): This version of Forms Builder is only compatible with version 22 or greater of Student
Process ID 61 has raised user error 50000, severity 22. SQL Server is terminating this process.
Cannot continue the execution because the session is in the kill state.
A severe error occurred on the current command.  The results, if any, should be discarded.
Current Student Version Database_StudentDB version: 21.4.0.62
   at Microsoft.SqlServer.Management.Common.ConnectionManager.ExecuteTSql(ExecuteTSqlAction action, Object execObject, DataSet fillDataSet,
   at Microsoft.SqlServer.Management.Common.ServerConnection.ExecuteNonQuery(String sqlCommand, ExecutionTypes executionType)
ClientConnectionId:ff029db8-7fb0-453d-b4b1-c1f45d0f1d88
Error Number:50000.State:1.Class:22
```

Installation Manager installs the following components:

- Forms Builder
- Security Token Service (STS)

> ⚠ Forms Builderversion 3.x or later requires the Staff STS component to be installed. Go to the **Start** screen and select **Package Manager**. Download the **Staff STS** package and **install it**. For more details, see Staff STS.

- Student Web App
- Web Client for CampusNexus CRM if Forms Builder Designer connects to the CampusNexus CRM database
- Forms Builder Contact STS if Forms Builder Designer connects to the CampusNexus CRM database (see Web Components)
- Workflow Composer

  After installing Workflow Composer, download the Forms Builder Contracts 3.x.x and the Anthology Student and/or CampusNexus CRM Activities and Contracts using the Package Manager within Workflow Composer.
- Workflow Tracking Database

  When you install the Workflow Tracking Database, ensure that the domain\FormsBuilderMachine$ account has db_owner permission to the Workflow Tracking Database.

Upgrade Notes

Forms Builder **3.7**

- Installation Manager installs .NET 4.8.

Forms Builder **3.6**

- "CrmConnection" string was added to the Renderer web.config file. For more details, see Renderer Connection Strings in Forms Builder help.
- Installation Manager configures IIS as follows:
  - Application pools for Forms Builder and Anthology Student: *StartMode* is set to *AlwaysRunning*
  - Site setting: *Preload Enabled* is set to *True*.

  For more details, see Application Initialization in Forms Builder help.
- Installation Manager installs .NET 4.7.2.

Postinstallation Tasks

A. Perform the appropriate steps described in Set Up the Database Environment.

B. When all setup steps are completed, verify the installation by accessing Forms Builder Designer and Renderer.

- **Forms Builder Designer** is installed on port 9002 by default. Access your Forms Builder with this port number to view the home page of Forms Builder.

  `http://<server>.<domain>:9002/`

- **Forms Builder Renderer** is installed on port 9003 by default. Access your Forms Builder URL with this port number and append `/#/Sequencelist` to view the Sequence List.

  `http://<server>.<domain>:9003/#/Sequencelist`

Notes:

- The port numbers can be customized during the Forms Builder installation.
- Forms Builder Designer and Renderer can be installed with HTTPS.
- Forms Builder Designer and Renderer can be installed using custom host names. An IIS binding will be added to the websites and all the configuration files will be updated with the Custom URL.
- The web.config file for Forms Renderer determines if the Sequence List is displayed or not. Change this setting to "true" if you do not want your users to view the Sequence List at this URL. The default is: `<add key="DisableSequenceList" value="false"/>`
- An API key is installed for Anthology Inc. products released in April 2018 and later. If you are using Forms Builder 3.4 and later with earlier versions of CampusNexus CRM and/or Anthology Student, you may need to configure matching API keys. For more details, see API Keys.

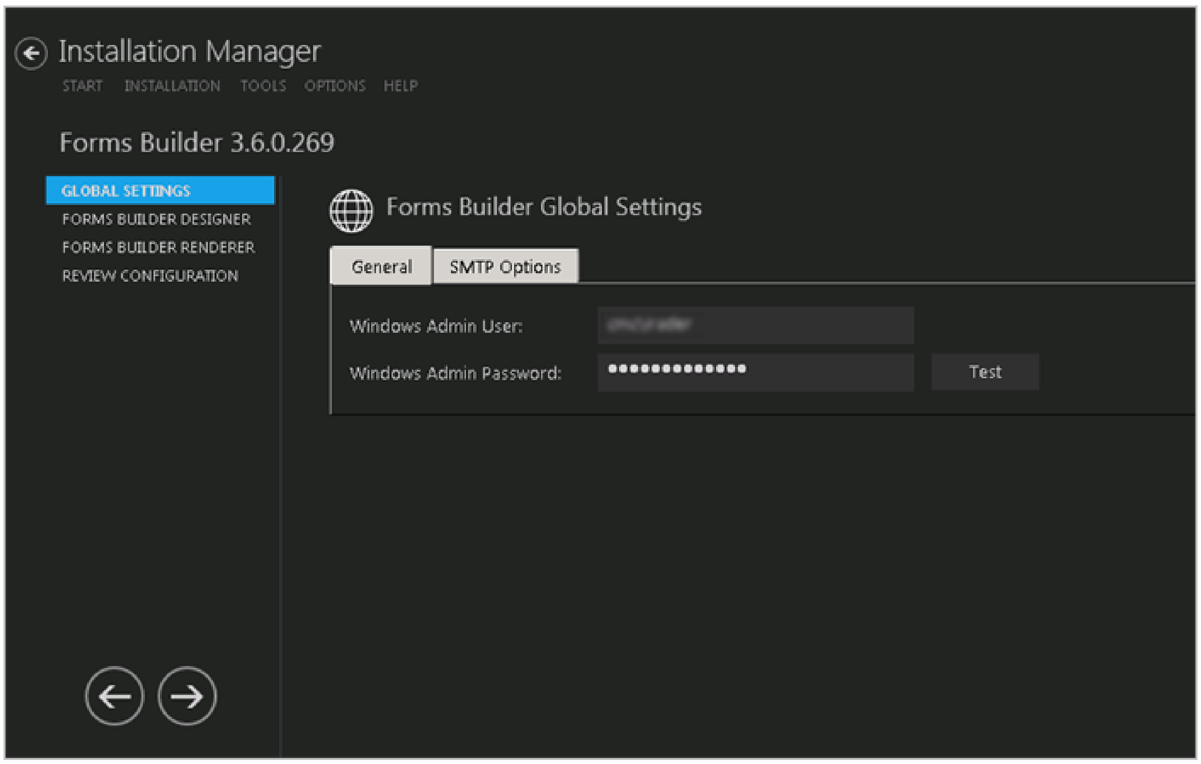
Global Settings

This screen contains the user name and password used when starting a Forms Builder installation. Users can also test this information without moving from the screen.

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Forms Builder** 3.x tile. The Forms Builder Global Settings screen is displayed.



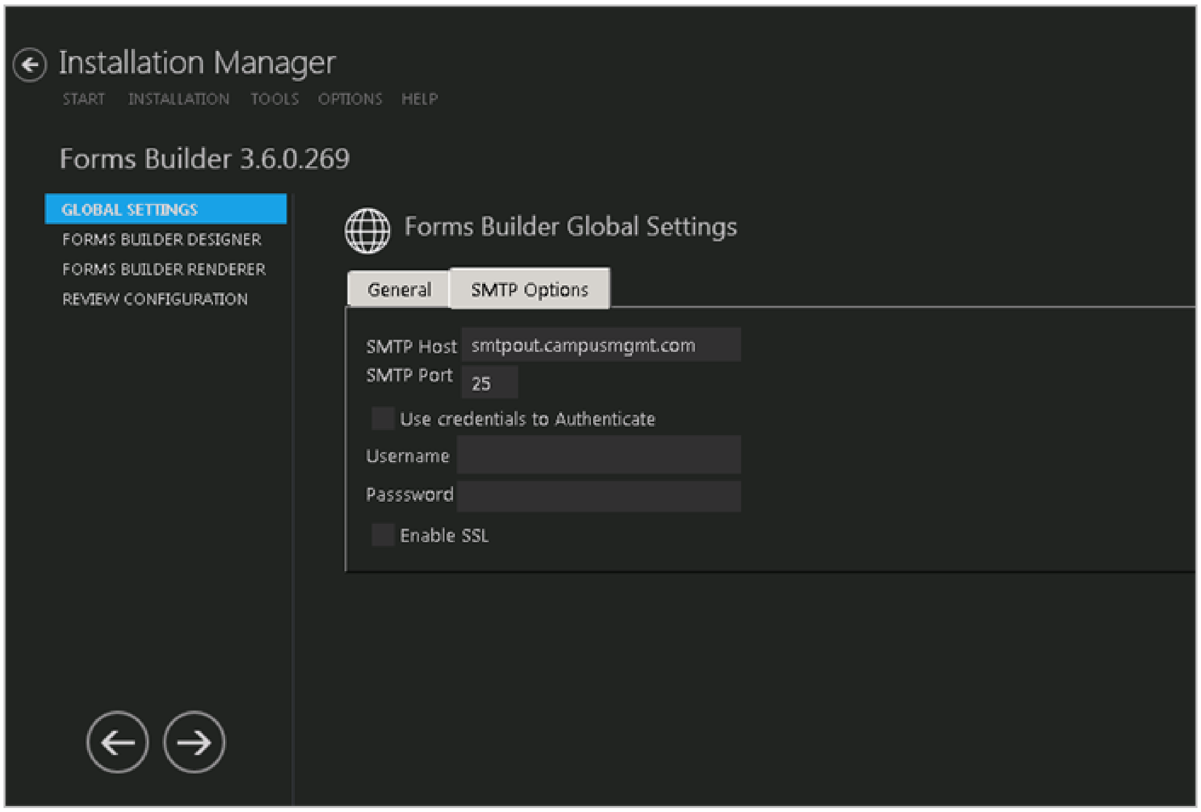
2. On the General tab, in the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer on which the installation will occur. Depending on your network environment, specify one of the following:

   - User name
   - Domain\User name
   - Email address of Admin User

3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.

5. On the SMTP Options tab, provide the following information:
   - In the **SMTP Host** field, enter the domain address of the SMTP host used for sending out email notifications from Forms Builder.
   - Specify the **SMTP Port** number.
   - Select **Use credentials to Authenticate** and enter the **Username** and **Password** of the sender's email account.
   - If applicable, select **Enable SSL**. Installation Manager will check for a valid certificate.



6. If the user is authenticated, click **OK** and click  to continue.

Forms Builder Designer

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and configuration options for Forms Builder Designer.

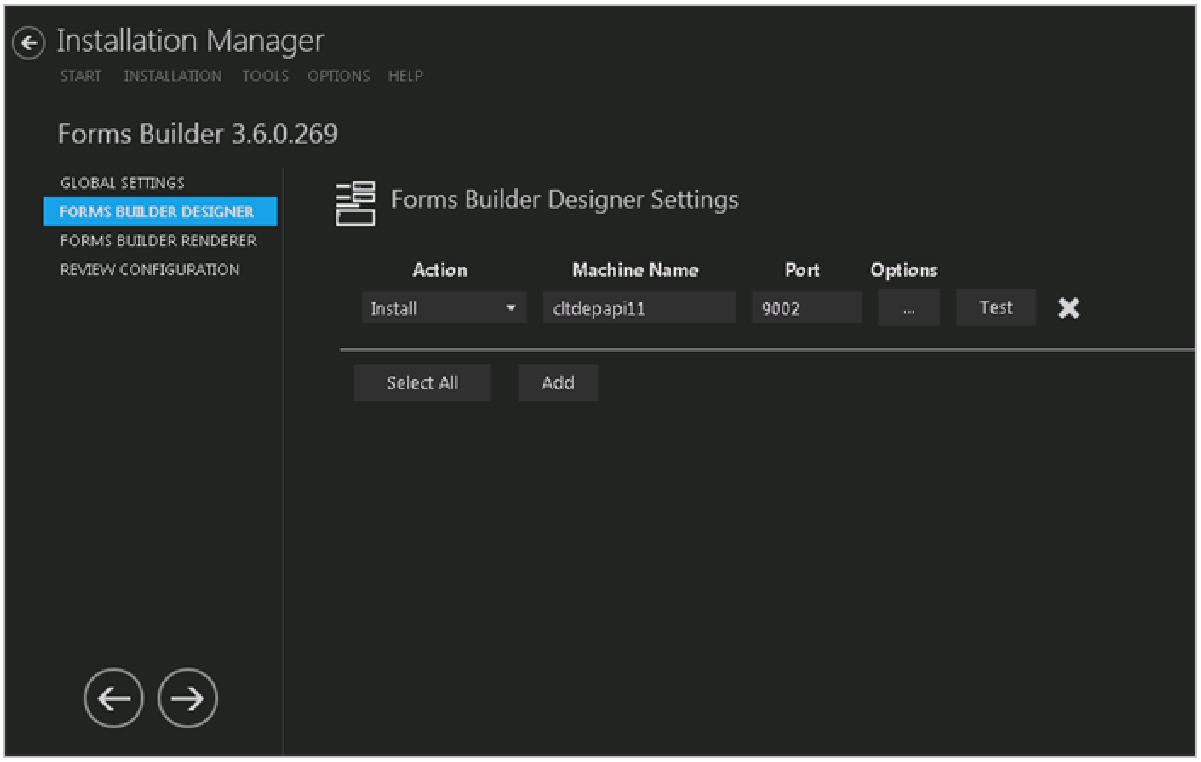
Prerequisites

Forms Builder version 3.x requires the following to be installed:

- Staff STS
- Student Web App if Forms Builder Designer connects to the Anthology Student database
- Web Client for CampusNexus CRM if Forms Builder Designer connects to the CampusNexus CRM database
- Forms Builder Staff Authentication Service if Forms Builder Designer connects to the CampusNexus CRM database (see Web Components)
- Forms Builder Contact STS if Forms Builder Designer connects to the CampusNexus CRM database (see Web Components)
- Workflow Composer
- Workflow Tracking Database

Set Up Forms Builder Designer

1. In the Installation menu, click **Forms Builder Designer**. The Forms Builder Designer Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This can be a local or remote machine.
5. Specify the port number of the Forms Builder Designer port or accept the default (9002).
6. Click  to view and edit the Options form.

   General Tab

   Settings on this tab are common to all components of Forms Builder Designer.

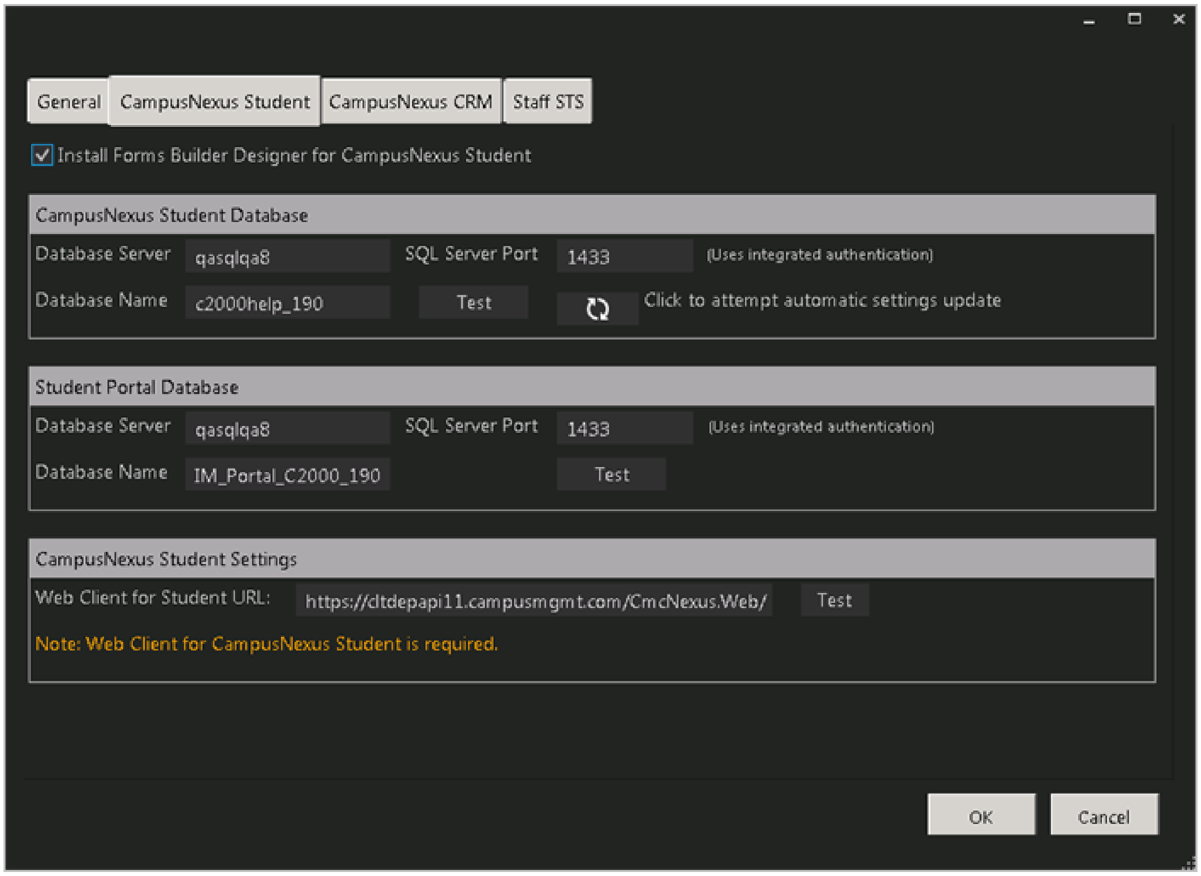
General Tab Fields

Field	Description
Forms Builder Designer URL	This is a friendly URL to access Forms Builder Designer. The default port for Designer is 9002. The default format is: `http(s)://machinename.domain.com:port`
Hostname	This is an optional field. When selected, the host header will be added to the Forms Builder Designer website, and the web.config file of Designer will be updated with the custom host URL. If this field is left blank, the URL for Designer accessed by end users and the URL in the config files will be `http(s)://machinename.domain.com:port`
Use HTTPS	Select this check box if you want the Forms Builder Designer to be accessed through HTTPS. When this option is selected, the Designer Certificate Thumbprint field is enabled.

Field	Description
Designer Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected and is not added to the web.config file. This certificate is used only for Forms Builder Designer. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

Anthology Student Tab

Settings on this tab are required if Forms Builder for Anthology Student is installed.



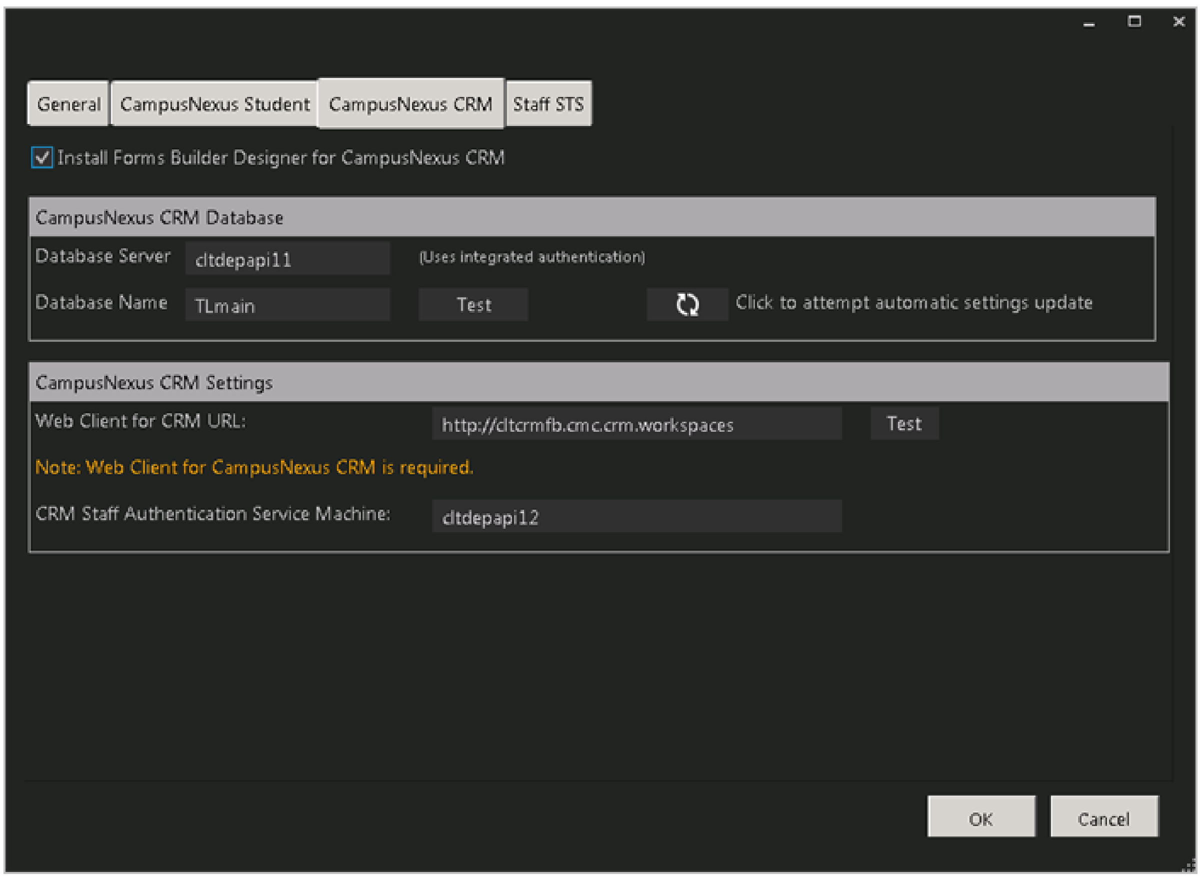
Anthology Student Tab Fields

Field	Description
Install Forms Builder Designer for Anthology Student	Select this check box to install Forms Builder Designer for Anthology Student. When this option is selected, entries in the remaining fields on this tab are required.
Anthology Student Database	
Database Server	Name of the Anthology Student SQL database server. The Server uses integrated authentication.
Database Name	Name of the Anthology Student SQL database.
SQL Server Port	Specify the port number of the installed SQL server or accept the default (1433).
Test	Click **Test** to verify connectivity to the Anthology Student database and to check if the Workflow Tracking database is installed.
Update Settings	Click  to update the settings by querying the database. (Syregistry table in the Anthology Student database)
Student Portal Database	

Field	Description
Database Server	Name of the Student Portal SQL database server. The Server uses integrated authentication.
Database Name	Name of the Student Portal SQL database.
SQL Server Port	Specify the port number of the installed SQL server or accept the default (1433).
Test	Click **Test** to verify connectivity to the Student Portal database.
Anthology Student Settings	
Web Client for Student URL	The URL of Anthology Student is displayed.
Test	Click **Test** to verify that Anthology Student is active.

CampusNexus CRM Tab

Settings on this tab are required if Forms Builder for CampusNexus CRM is installed.

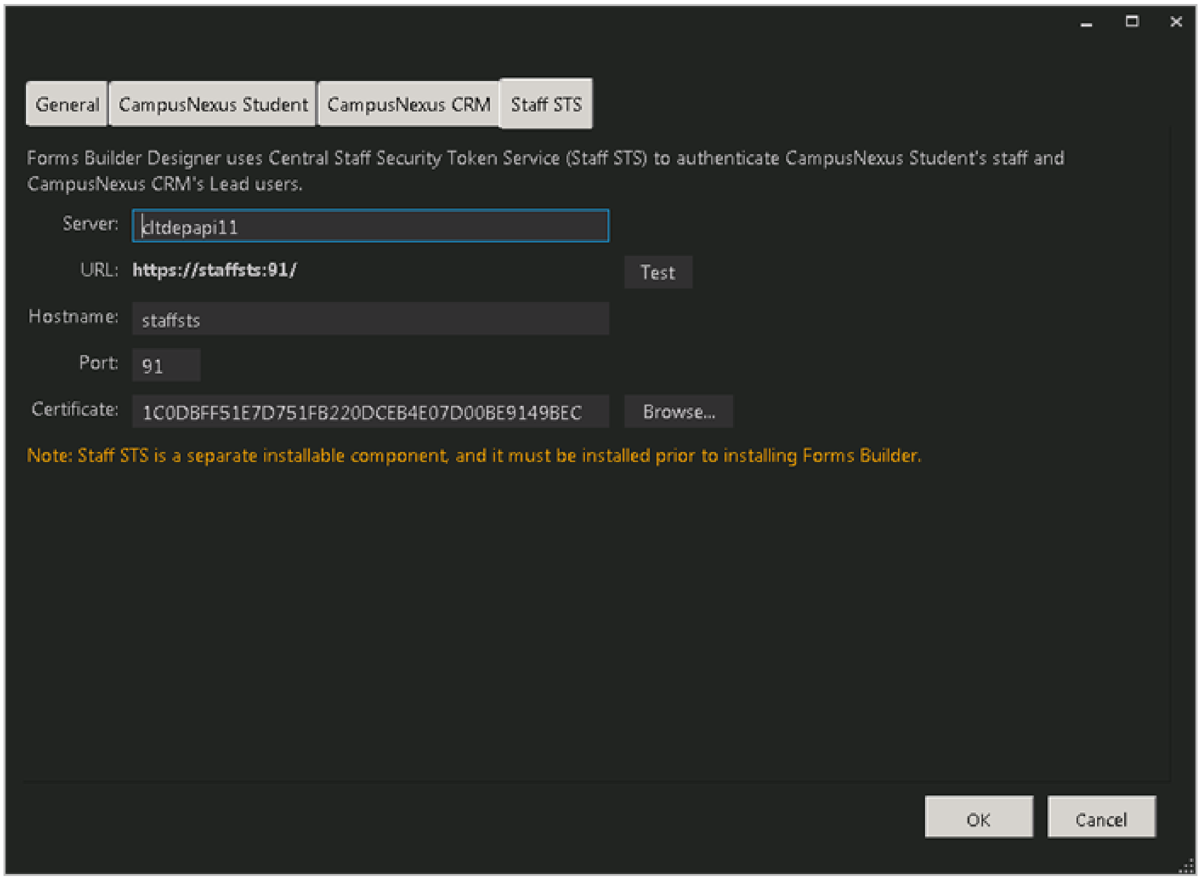


CampusNexus CRM Tab Fields

Field	Description
Install Forms Builder Designer for CampusNexus CRM	Select this check box to install Forms Builder Designer for CampusNexus CRM. When this option is selected, entries in the remaining fields on this tab are required.
CampusNexus CRM Database	
Database Server	Name of the CampusNexus CRM SQL database server. The Server uses integrated authentication.
Database Name	Name of the CampusNexus CRM SQL database.
Test	Click **Test** to verify connectivity to the CampusNexus CRM database and to check if the Workflow Tracking database is installed.
Update Settings	Click  to update the settings by querying the database.
CampusNexus CRM Settings	
Web Client for CRM URL	The URL of the Web Client for CampusNexus CRM is displayed.
Test	Click **Test** to verify that Web Client for CRM is active.
CRM Staff Authentication Service Machine	Name of the machine where the CRM Staff Authentication Service is installed (see Web Components).

Staff STS Tab

Settings on this tab are required if Forms Builder for Anthology Student and/or CampusNexus CRM is installed.



Staff STS Tab Fields

Field	Description
Server	Specify the machine name of the Staff STS Server. The Staff STS Server must have been previously installed. See Staff STS.
URL	This is a friendly URL to access the Staff STS. The default port for Designer is 91. The default format is: `http(s)://machinename.domain.com:port`
Test	Click **Test** to verify that the Staff STS Server is active and that login is successful.
Hostname	This is an optional field. If you have configured Staff STS on a custom host, specify the Staff STS hostname here. Otherwise, this field must be left blank and the default URL for Staff STS will be used in the Forms Builder Designer web.config file.
Port	Specify the port number of the installed Staff STS server or accept the default (91).

Field	Description
Certificate	Certificate thumbprint from IIS. The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

7. Click **OK** to save changes on the Options form. The form is closed.
8. Click  to delete a selected line.
9. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
10. If all tests pass, click .

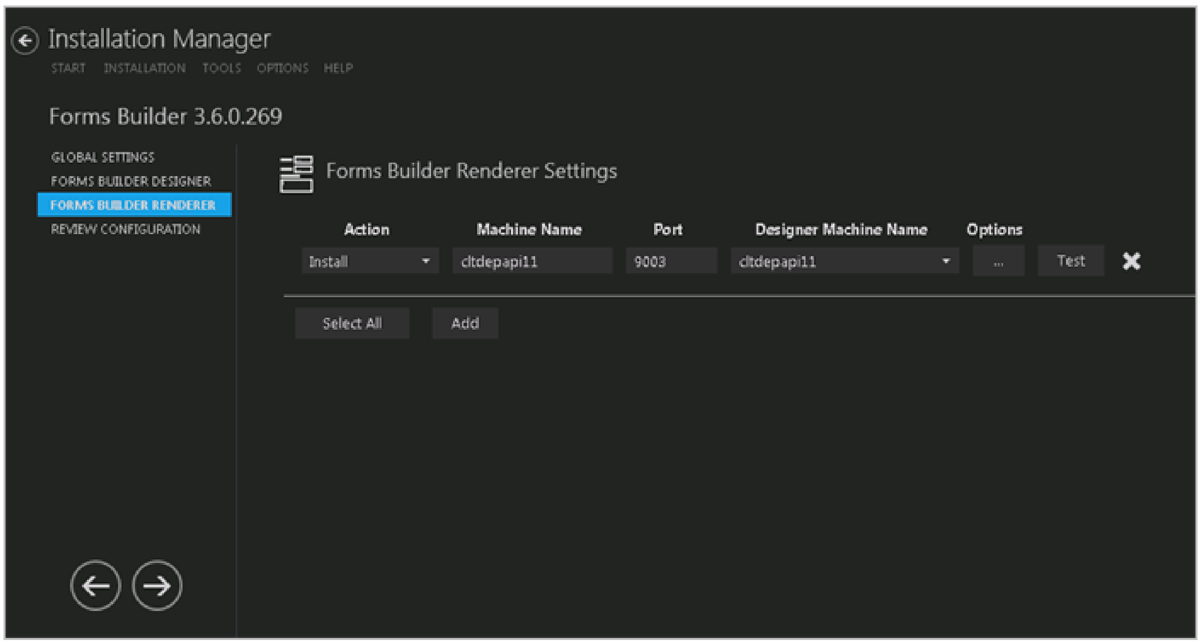
Forms Builder Renderer

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the machine name and configuration options for Forms Builder Renderer.

Note: Forms Builder Designer and Renderer can be installed on the same machine or on different machines.

Set Up Forms Builder Renderer

1. In the Installation menu, click **Forms Builder Renderer**. The Forms Builder Renderer Settings screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

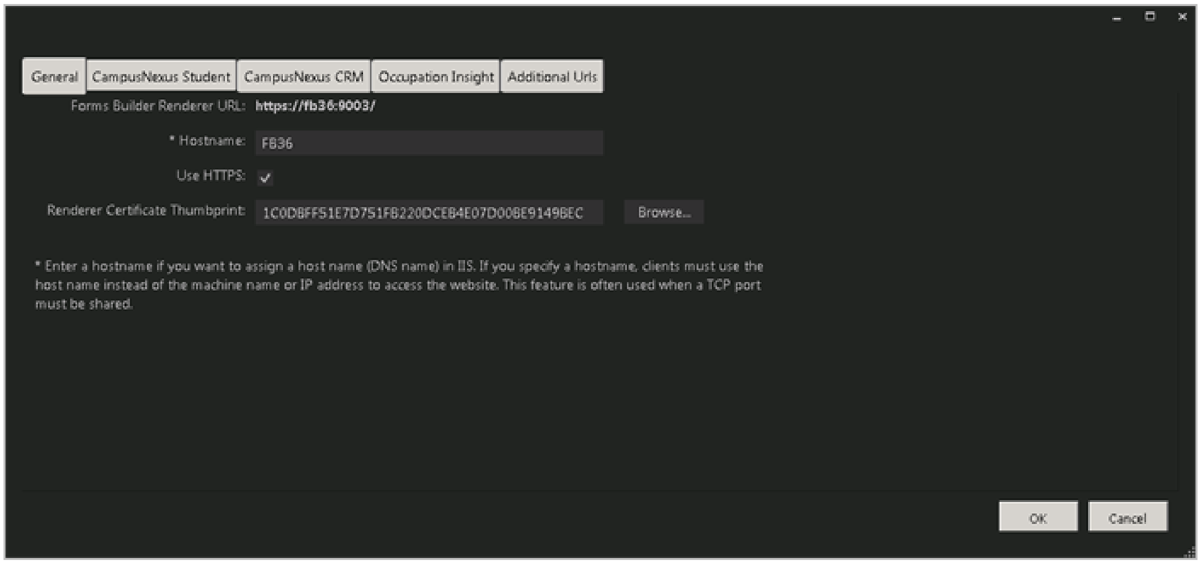
   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. Enter the **Machine Name** for the component to be installed. This can be a local or remote machine.
5. Specify the **Port** number of the Forms Builder Renderer or accept the default (9003).

6. Select the **Designer Machine Name** in the drop-down list.

7. Click ... to view and edit the Options form.

   General Tab

   Settings on this tab are required and common to all components of Forms Builder Renderer.



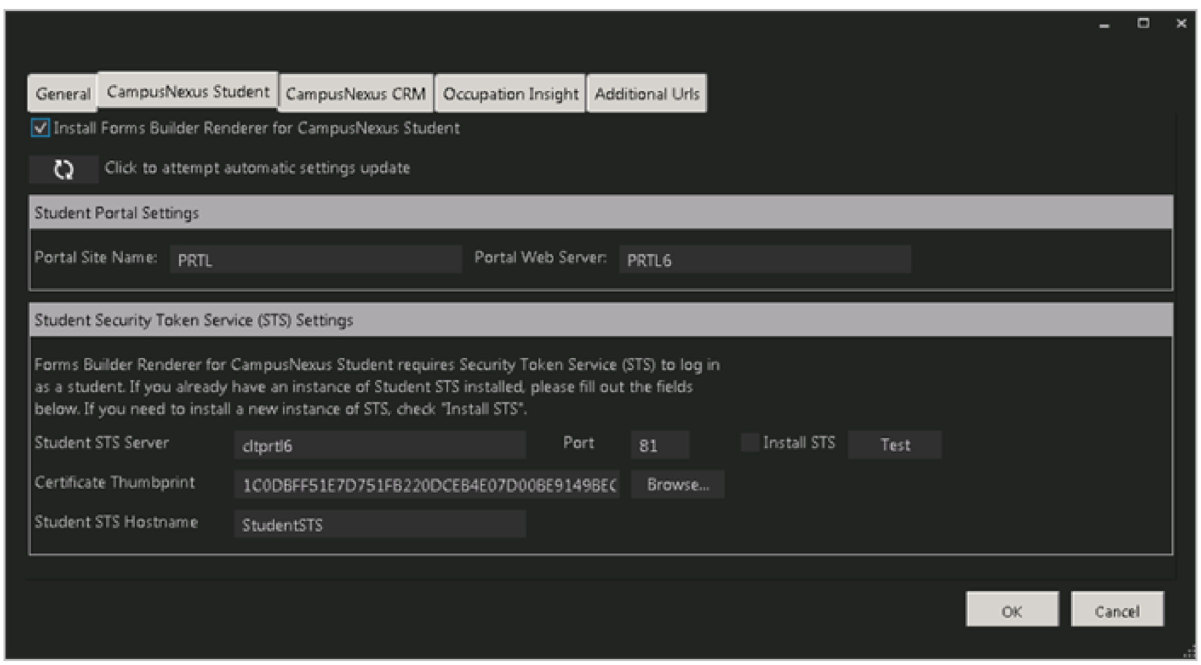
General Tab Fields

Field	Description
Forms Builder Renderer URL	This is a friendly URL to access Forms Builder Renderer. The default port for Renderer is 9003. The default format is: `http(s)://machinename.domain.com:port`
Hostname	This is an optional field. When selected, the host header will be added to the Forms Builder Renderer website, and the web.config file of Renderer will be updated with the custom host URL. If this field is left blank, the URL for Renderer accessed by end users and the URL in the config files will be `http(s)://machinename.domain.com:port`
Use HTTPS	Select this check box if you want the Forms Builder Renderer to be accessed through HTTPS. When this option is selected, the Renderer Certificate Thumbprint field is enabled.

Field	Description
Renderer Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected and is not added to the web.config file. This certificate is used only for Forms Builder Renderer. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**

Anthology Student Tab

Settings on this tab are required if Forms Builder for Anthology Student is installed.



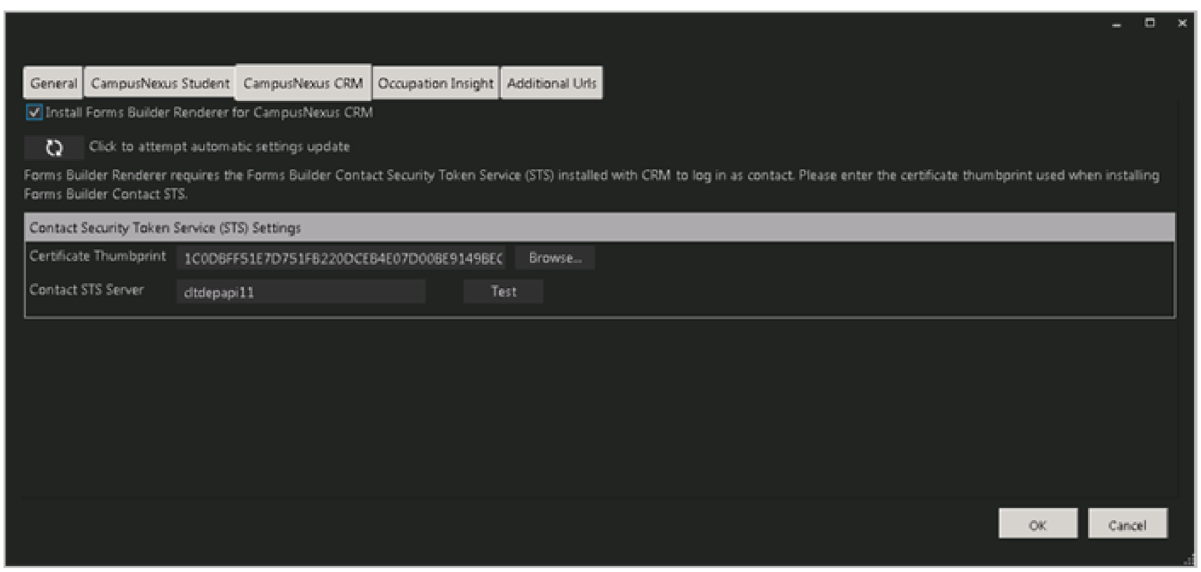
Anthology Student Tab Fields

Field	Description
Install Forms Builder Renderer for Anthology Student	Select this check box to install Forms Builder Renderer for Anthology Student.
Update Settings	Click  to update the settings by querying the database. (Syregistry table in the Anthology Student database)
Student Portal Settings	
Portal Site Name	Site Name configured for the Portal ('legacy' portal) login page. The Portal Site Name is PRTL by default. It changes to PRTL1, PRTL2 so on when multiple Portals are installed on single IIS server. The Portal Site Name value is found in the web.config file under Appsettings of Portal ('legacy'). The Site Name value is used for Anthology Student STS.
Portal Web Server	Specify the Portal Web Server name. The SySiteSettings of the Anthology Student database will be modified with Portal Server Name in the Portal WebService URLs. For a Load Balanced Portal environment, enter the name of load balancer server.
Student Security Token Service (STS) Settings	
Student STS Server	Name of the STS server used to authenticate applicants, students, and employers.
Port	Specify the port number of the installed Student STS server or accept the default (81).
Install STS	Select this check box if you want to install a new Student STS instance.
Test	Click **Test** to verify that the Student STS is active and that login is successful.

Field	Description
Certificate Thumbprint	Certificate thumbprint from IIS. This certificate is required only when HTTPS is selected. It is not added to the web.config file. This certificate is used only for the Student STS, which provides authentication for Renderer (and Portal) to applicants, students, and employers. Click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Student STS Hostname	This is an optional field. When selected, the web.config file of the Student STS will be updated with the custom host URL. If this field is left blank, the URL in the config files will be `http(s)://machinename.domain.com:port`

CampusNexus CRM Tab

Settings on this tab are required if Forms Builder for CampusNexus CRM is installed.

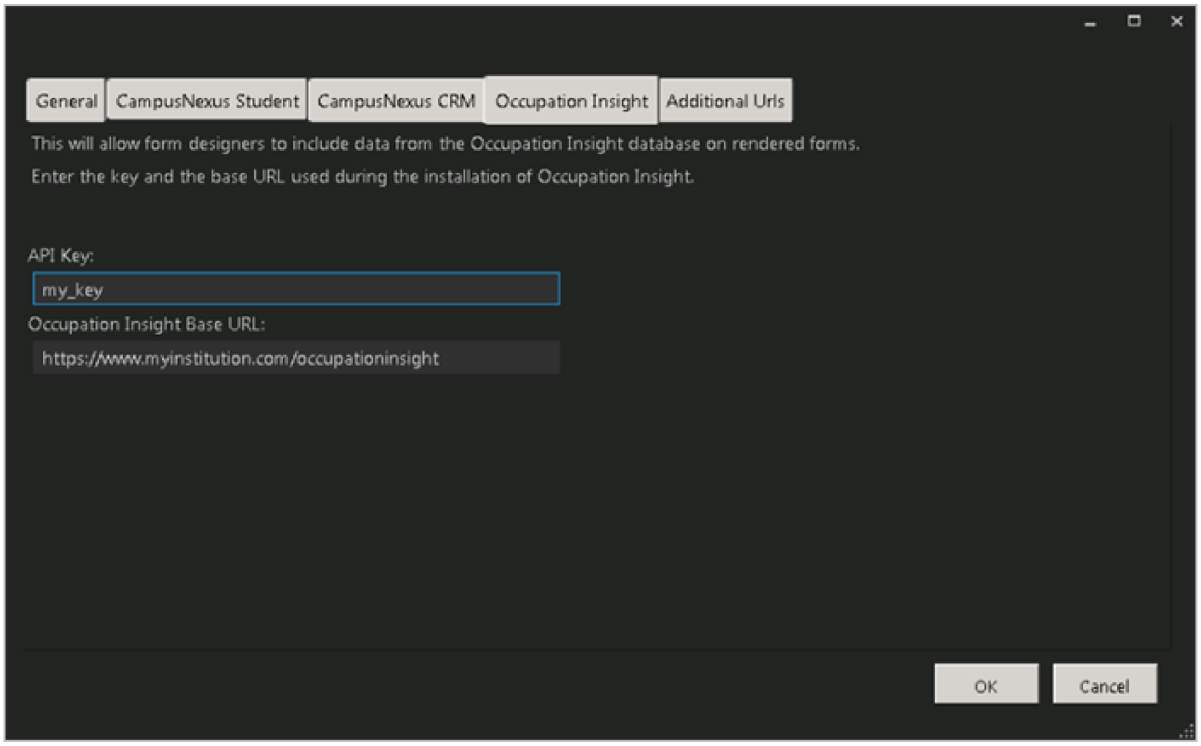


CampusNexus CRM Tab Fields

Field	Description
Install Forms Builder Renderer for CampusNexus CRM	Select this check box to install Forms Builder Renderer for CampusNexus CRM.
Update Settings	Click  to update the settings by querying the database.
Contact Security Token Service (STS) Settings	
Certificate Thum-bprint	Certificate thumbprint from IIS. The same certificate thumbprint that is used on the Staff STS must be used here. Copy and paste the thumbprint from the Staff STS into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Designer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File...** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Contact STS Server	Specify the machine name of the Contact Security Token Service (STS) Server.
Test	Click **Test** to verify that the Contact STS Server is active and that login is successful.

Occupation Insight Tab

Settings on this tab are required only if Occupation Insight is used as a database source for Forms Builder. The settings are stored in the Forms Builder Renderer web.config file.

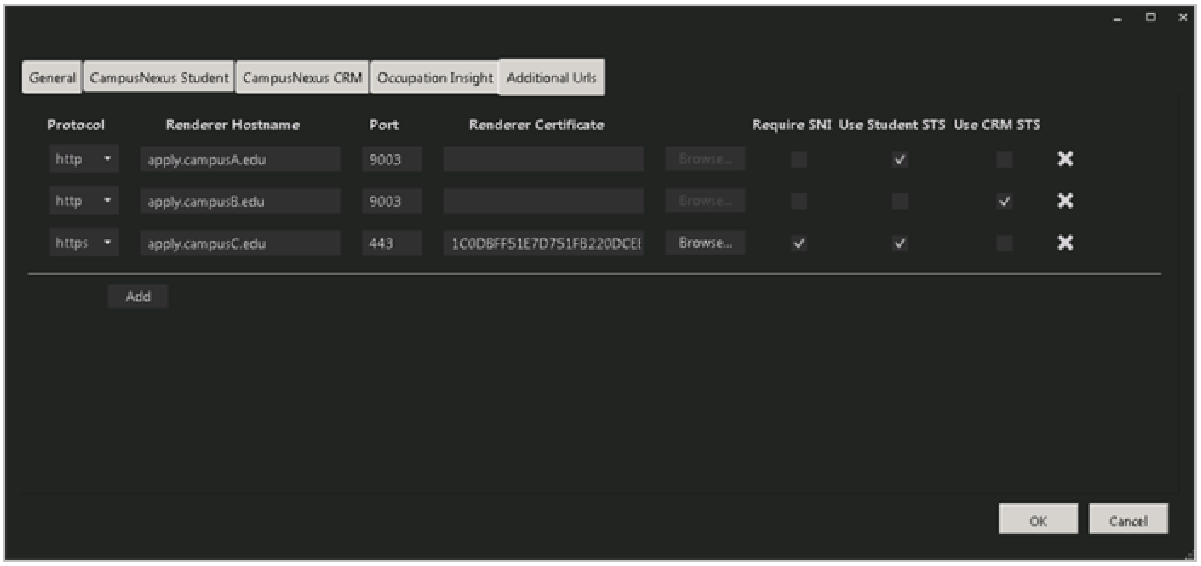


Occupations Insight Tab Fields

Field	Description
API Key	Enter the API key used during the installation of Occupation Insight. See [Occupation Insight](). **Note**: This is a specific key for the Occupation Insight APIs. It is not the same as the API key used for the framework APIs.
Occupation Insight Base URL	This URL is used by Forms Builder to access Occupation Insight data through OData queries.

Additional Urls Tab

Settings on this tab are required only if the Renderer instance is accessed from additional URLs associated with individual campuses. These campuses are served forms from the main Renderer instance, however, the forms use branding and authentication services that are specific to individual campuses. To provide authentication for users accessing the rendered forms from the additional URLs, Installation Manager creates redirect URLs for the STS services. The STS service used depends on whether Forms Builder accesses Anthology Student, CampusNexus CRM, or both products. The settings are stored in the Forms Builder Renderer web.config file.



Additional Urls Tab Fields

Field	Description
Add	Click the **Add** button to add a line to the form.
Protocol	Select **HTTP** or **HTTPS** protocol. If HTTPS is selected, the Renderer Certificate and Require SNI fields are enabled and must be completed.
Renderer Host-name	Specify the hostname for an additional Renderer URL. This hostname will the url value in the <realms> section of the Renderer web.config file (see below). It will be added to the IIS bindings of main Renderer instance.
Port	Specify the port number used by the additional Renderer URL or accept the default (9003).

Field	Description
Renderer Cer-tificate	Certificate thumbprint from IIS is required if HTTPS is selected. Copy and paste the thumbprint from Renderer into this field, or click **Browse** to navigate to the IIS Server Certificates to select the thumbprint. The thumbprint is added to the Renderer web.config file. **To extract a .CER file from IIS:** a. Open Internet Information Services (IIS) Manager and choose the certificate to be used from **Server Certificates**. b. **Double-click** to open the certificate properties. c. Select **Root** level and in the **Details** tab, click the **Copy to File…** button. d. Click **Next**. Select **No, do not export the private key**, and click **Next**. e. Select **DER encoded binary X.509 (.CER)** and click **Next**. f. Specify a file path and name (root) to export to and click **Next**. g. Click **Finish**
Require SNI	Server Name Indication (SNI) is required if HTTPS is selected. SNI allows a server to present multiple certificates on the same IP address and TCP port number and hence allows multiple secure websites to be served by the same IP address without requiring all those sites to use the same certificate.
Use Student STS	Select this check box if the Student STS is used to authenticate Anthology Student users.
Use CRM STS	Select this check box if the Contact STS is used to authenticate CampusNexus CRM users.

The settings specified on the Additional Urls tab are written to the <authenticationConfigSection> section in the Renderer web.config file.

- The `<realms>` section contains a key and value for each additional incoming Renderer URL.
- The `<issuers>` section contains a key and value for the authentication services, i.e., Student STS and CRM STS.
- The `<mappings>` section contains the mapping between realm keys and STS keys.

```
<authenticationConfigSection>
  <!-- incoming urls -->

  <realms>
    <!-- <url key="" value="" /> -->
    <url key="CampusA" value="http://apply.CampusA.edu/" />
    <url key="CampusB" value="http://apply.CampusB.edu/" />
```

```
    <url key="CampusC" value="http://apply.CampusC.edu/" />
  </realms>

  <!-- STS redirect urls -->

  <issuers>
    <!-- <url key="" value="" /> -->
    <url key="CampusASTS" value="https://studentsts.CampusA.edu:81"/>
    <url key="CampusBSTS" value="https://crmsts.CampusB.edu:81"/>
    <url key="CampusCSTS" value="https://studentsts.CampusC.edu:81"/>
    <url key="Student STS" value="https://<server>.campusmgmt.com:811"/>
    <url key="CRM STS" value="https://<server>.campusmgmt.com/cmc.crm.sts/"/>
  </issuers>

  <mappings>
    <!-- <mapping realmKeys=" comma separated realm keys or * for wildcard match "
                product=" name of the product or * for wildcard match "
               issuerKey=" url key of the issuer " /> -->

    <mapping realmKeys="CampusA" product="Student" issuerKey="CampusASTS"/>
    <mapping realmKeys="CampusB" product="CRM" issuerKey="CampusBSTS"/>
    <mapping realmKeys="CampusC" product="Student" issuerKey="CampusCSTS"/>
    <mapping realmKeys="*" product="Student" issuerKey="Student STS"/>
    <mapping realmKeys="*" product="CRM" issuerKey="CRM STS"/>
  </mappings>

 </authenticationConfigSection>
```

8. Click **OK** to save changes on the Options form. The form is closed.
9. Click  to delete a selected line.
10. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
11. If all tests pass, click .

Review Configuration

The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

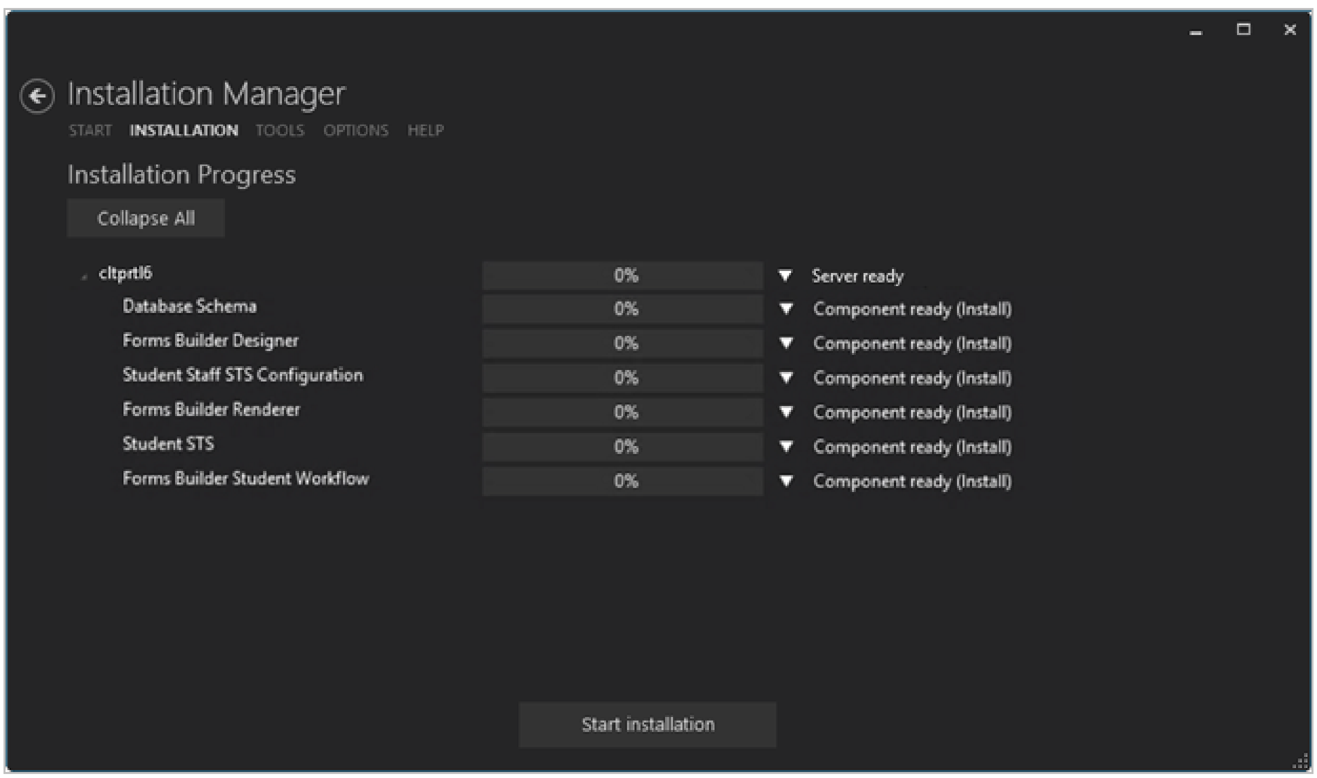
Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.
2. Click **Check prerequisites** to validate the configuration. The check results are displayed.

    Indicates that the component passed the prerequisites check.

    Indicates that the component failed the prerequisites check.

   Correct any issues for failed components and run the prerequisites check again. Proceed with the next step after all components pass the check.
3. Click **Skip Prerequisites Check**. The Installation Progress screen is displayed.

4. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

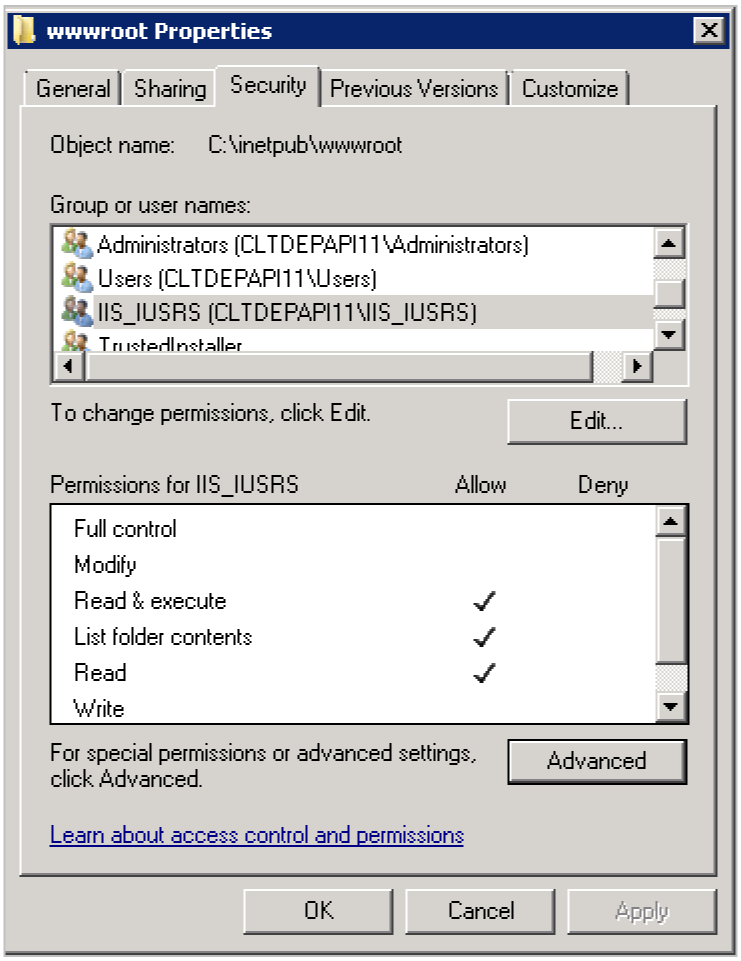
5. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.
6. To verify or troubleshoot the installation, click next to a progress bar to access installation logs and other tools (see Installation).

After you have completed the installation, assign Full Control Permissions for IIS_IUSRS in the Forms Builder Designer and Renderer web applications.

Full Control Permissions for IIS_IUSRS

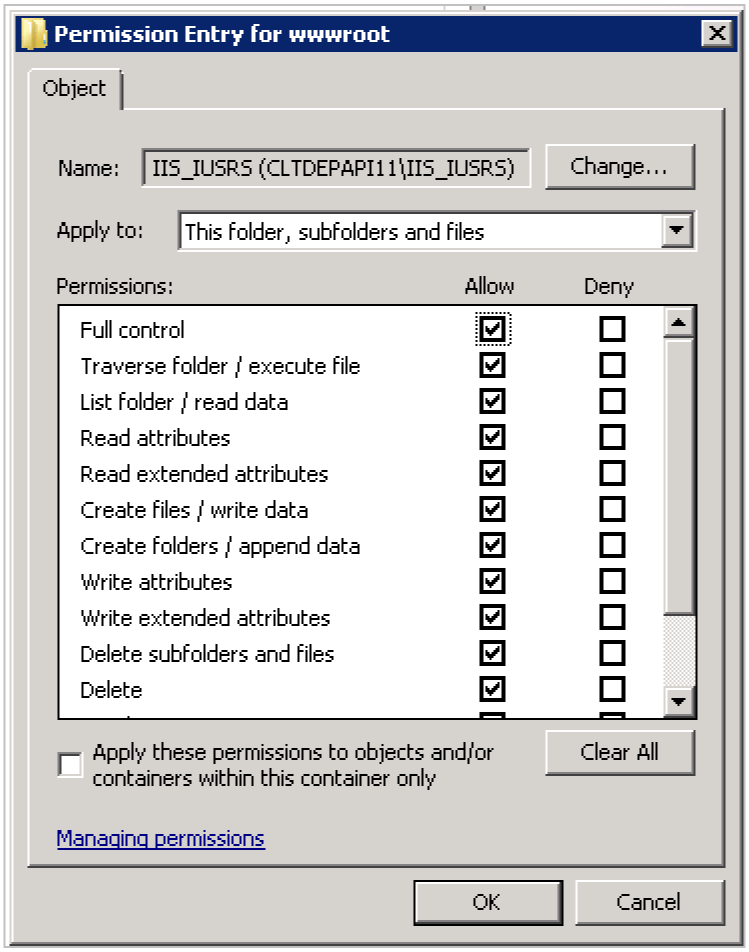
Anthology web applications use application pool identity. To enable the applications to create logs under their physical folders in IIS, it is necessary to grant the IIS_IUSRS group full control permissions. This applies to the Forms Builder Designer and Forms Builder Renderer applications.

1. On the IIS, open Windows Explorer, and select the directory of the web application.
2. Right-click and select **Properties**.
3. Select the **Security** tab.



4. Select the **IIS_IUSRS** user and click **Advanced**.

5. Select **Full control** permission and click **OK**.



Set Up the Database Environment

Forms Builder can be used with the databases of CampusNexus CRM, Anthology Student, or both. In addition, the Workflow Composer along with appropriate packages for contracts and activities is required.

For details about the supported product version combinations, refer to the Product Compatibility Matrix (logon required).

Depending on the database environment, perform the following integration and verification steps.

CampusNexus CRM Environment

1. Use Installation Manager to install **CampusNexus CRM** (including the Web Client).
2. On the machine where the Web Client for CampusNexus CRM is installed:
   a. Navigate to **\inetpub\wwwroot\cmc.crm.workspaces**.
   b. In CampusNexus CRM version 11.1, open the **NexusCRM.config** file.

      In CampusNexus CRM version 12.0 or later, open the **web.config** file.
   c. Find "EdmModelGeneration" and make sure that BuildMode is enabled.

```
<EdmModelGeneration BuildMode="Enabled">
  <!--
Allowed Values for BuildMode
  - "Enabled" - For generating model using the latest meta from database
  - "CompileSourceFile" - For generating model using the Source Files. Used only for troubleshooting.
  - "Disabled" - For disabling model generation
"Faulted" and "CompileSucceeded" values are for internal usage
-->
</EdmModelGeneration>
```

3. Use Installation Manager to install **Workflow Composer**.
4. Open Workflow Composer, click **Package Manager**, and verify that the activities and contracts packages for your product versions are installed.

   For example, if you are using Forms Builder 3.5 with CampusNexus CRM 12.1, install the following packages:

   - Forms Builder Contracts 3.5.0 (3.5.0.xxx)
   - Activities and Contracts (CRM) 12.1.0 (12.1.0.xxx)

   Remove the packages for older versions when you install new versions.
5. Log in to the **Web Client** for CampusNexus CRM.
6. Open File Explorer, navigate to **\inetpub\wwwroot\Cmc.Crm.Workspaces\bin**, and copy the **Cmc.NexusCrm.Contracts.dll** file.
7. Paste the **Cmc.NexusCrm.Contracts.dll** file into the following locations:

- On the machine that hosts Forms Builder: **\inetpub\wwwroot\CMCFormsRenderer_V3\bin**
- On the machine where Workflow Composer is installed: **\Program Files (x86)\CMC\Workflow**

Every time you build new custom fields/entities in CampusNexus CRM, copy the Cmc.NexusCrm.Contracts.dll to these locations.

> ⚠ **Do not copy the Cmc.NexusCrm.Contracts.dll to the \bin folder of Forms Builder Designer.**

Verify the Setup

After Forms Builder has been installed:

1. Log in to Forms Builder Designer.
2. In Form Designer, create a form that collects data for a **Contact**.
3. In Sequence Designer, create and save the sequence, and then click **Open Workflow**.
4. In Workflow Composer, add a **CreateEntity<ContactEntity>** activity to the Entry of the first form and a **SaveEntity<ContactEntity>** activity in the final transition.
5. Publish the updated workflow definition.
6. In the Sequence List, open and fill out the rendered form.
7. In the Desktop for CampusNexus CRM, verify that the new Contact is created.

Note: In this environment, workflow definitions for sequences are saved in the database of CampusNexus CRM.

For more details, see CampusNexus CRM Integrations.

Anthology Student Environment

1. Use Installation Manager to instal **Anthology Student** (including the Web Client).
2. Use Installation Manager to install **Workflow Composer**.
3. Open Workflow Composer, click **Package Manager**, and verify that the activities and contracts packages for your product versions are installed.

   For example, if you are using Forms Builder 3.5 with Anthology Student 19.0.4, install the following packages:

   - Forms Builder Contracts 3.5.0 (3.5.0.xxx)
   - Activities and Contracts (V1) 19.0.4 (19.0.4.xxx)
   - Activities and Contracts (V2) 19.0.4 (19.0.4.xxx)

   Remove the packages for older versions when you install new versions.

Verify the Setup

After Forms Builder has been installed:

1. Log in to Forms Builder.
2. In Form Designer, create a form that collects data for a **Student**.
3. In Sequence Designer, create and save the sequence, and then click **Open Workflow**.
4. In Workflow Composer, add a **CreateEntity<Studententity>** activity to the Entry of the first form and a **SaveEntity<StudentEntity>** activity in the final transition.
5. Publish the updated workflow definition.
6. In the Sequence List, open and fill out the rendered form.
7. In the Web Client for Anthology Student, verify that the new Student is created (or check the syStudent table in the database).

Note: In this environment, workflow definitions for sequences are saved in the database of Anthology Student.

CampusNexus CRM and Anthology Student Environment

If you are using both CampusNexus CRM and Anthology Student, perform all of the steps described above.

Note: In this environment, workflow definitions for sequences are saved only in the database of Anthology Student.

CampusNexus CRM Integrations

Integrate Forms Builder with CampusNexus CRM 11.1 or Later

1. The **Higher Ed** and **Web Client** components must be installed.
2. If you're using CampusNexus CRM 11.1:

   > In the Web Client installation folder, in the **NexusCrm.config** file, set the value of the **EdmModelGeneration BuildMode** parameter to **Enabled**, and then restart the Cmc.Crm.Workspaces application pool.

   If you're using CampusNexus CRM 12.0:

   > In the Web Client installation folder, in the **web.config** file, set the value of the **EdmModelGeneration BuildMode** parameter to **Enabled**, and then restart the Cmc.Crm.Workspaces application pool.

3. Copy the **Cmc.NexusCrm.Contracts.dll** file from the \bin folder of Web Client to the installation folder of Workflow Composer and Forms Renderer.

   All operational and reference objects are wrapped in this file Cmc.NexusCrm.Contracts.dll. When new properties are created in CampusNexus CRM or an existing property definition (metadata) is changed, this file is regenerated. For example, it is regenerated when creating or updating an object, a tab, a property or a relationship.

   The regenerated file needs to be copied to the installation folder of **Workflow Composer** and to the \bin folder of **Forms Renderer**.

   > ⚠ **Do not copy the Cmc.NexusCrm.Contracts.dll to the \bin folder of Forms Builder Designer.**

4. Clients using Anthology Student and CampusNexus CRM can use a single installation of Workflow Composer and Forms Builder 3.x to work with both applications.
5. In CampusNexus CRM, a maximum of 1024 properties can be published for use with Forms Builder 3.x. If additional properties are needed, unpublish previously published properties and then publish new properties. The maximum count of 1024 properties cannot be exceeded. For more information about publishing and unpublishing object properties, see the description of the sproc_GetPropertiesPublishStatusForObject and sproc_SetPropertiesPublishStatusForObject stored procedures in the CampusNexus CRM Integration guide.
6. CampusNexus CRM 11.1:

   > To consume events triggered from Web Client and iServices in Workflow Composer, set the value of the **Workflow Integrated** parameter to “True” in the **NexusCRM.config** file in the Web Client installation folder. By default, its value is “False”.

CampusNexus CRM 12.0:

> To consume events triggered from Web Client and iServices in Workflow Composer, set the value of the **Workflow Integrated** parameter to “True” in the **web.config** file in the Web Client installation folder. By default, its value is “False”.

Integrate Workflow Composer with CampusNexus CRM 11.1 or Later

1. In Workflow Composer, download and install the Activities and Contracts (CRM) package corresponding to the installed version.
2. Copy the **Cmc.NexusCrm.Contracts.dll** and **Cmc.NexusCrm.WcfProxy.dll** files from the \bin folder of Web Client to the installation folder of Workflow Composer and to the \bin folder of Forms Renderer.

   Do not copy the Cmc.NexusCrm.Contracts.dll to the \bin folder of Forms Builder Designer.

3. In the installation path of Workflow Composer, open the **WorkflowComposer.exe.config** file using a text editor (e.g., Notepad) and navigate to the **<appSettings>** tag.
4. Verify that the value of the **ConfigureCampusNexusWcfProxy** key is “true”. Change its value to “true” if a different value is set.
5. Add a new key, **CmcNexusCrmWebUrl**, and specify the Web Client URL as its value.

   Updated code in the <appSettings> tag will now be as follows:

```
<appSettings>
<add key=”ConfigureCampusNexusWcfProxy” value=”true”/>
<add key=”CmcNexusCrmWebUrl” value=”<Web Client URL>”/>
</appSettings>
```

6. Save and close the WorkflowComposer.exe.config file.

Run an OData Query in the Web Client

System integrators can view the results of a lookup query that is available in the Web Client for CampusNexus CRM. Prior to integrating with CampusNexus CRM, this functionality helps an integrator to verify the list of values that will be displayed in their query.

View Lookup Query Results

1. Suffix the Web Client URL as follows: **http://<web client url>/nexuscrmodata/$metadata**.

   The web page that is displayed includes lookup queries that are available by default.

2. Search for the text “lookup” and then navigate to the query that you want to run.

   Example

You want to run the following query to verify the list of available Account types:

LookupQueryName="EnumAccountAccountTypes?$select=Id,DisplayValue&$filter=IsActive eq 1&$orderby=DisplayOrder"

a. Copy the following text from the query:

   EnumAccountAccountTypes?$select=Id,DisplayValue&$filter=IsActive eq 1&$orderby=DisplayOrder

b. Append the copied text to the Web Client URL as follows:

   http://<Web Client URL>/nex-uscrmodata/EnumAc-countAccountTypes?$select=Id,DisplayValue&$filter=IsActive%20eq%201&$orderby=DisplayOrder

c. Press ENTER.

3. The list of values available in the Account Type property is displayed.

API Keys

To enhance the security of Anthology Inc. products, API keys were added to the products released in May 2018 and later. An API key is a secret token that is submitted with a web service request to identify the origin of the request. The key for the consumer of the service needs to match the key of provider of the service, otherwise access to the service is rejected. The API key is unique for each customer.

The API key is an AppSetting in the web.config files of applications built on the CampusNexus framework. It uses the following syntax:

```
<add key="apiKey" value=""/>
```

The API key is the same key that is used in the Package Manager screen of Installation Manager.

Installation Manager 1.18 and later automatically adds the key value to the web.config files during installation of the following product versions:

- CampusNexus CRM **12.0** and later
- Anthology Student **19.0** and later
- Contracts & Activities **19.0** and later
- Portal **19.0** and later
- Regulatory **10.1** and later
- Financial Aid Automation **6.2** and later
- Workflow Composer **2.6** and later

Using Earlier Product Versions

If you are using products with lower versions in combination with any of the above listed versions, the API key must be manually added to the web.config file of the older version.

If there is no key defined in the web.config file, a default key that exists in the authentication provider will be used.

Depending on the product and version, you may need to overwrite the default key with your customer-specific key value.

— OR —

If the `appSettings` section does not contain the <add key="apiKey" value=""/> line, add the line and specify your key value.

The following is a snippet of a web.config file for Forms Builder Renderer 3.4:

```
<appSettings>
  <add key="ConfigureCampusNexusWcfProxy" value="true" />
  <add key="ConfigureCVueNexusWcfProxy" value="true" />
  <!-- Following will be populated when Crm is enabled for Forms Builder -->
  <add key="CmcNexusCrmWebUrl" value="http://<server:port>/" />
  <add key="PaymentProvider" value="pilot-payflowpro.paypal.com" />
  <add key="AuxiliaryServiceBaseUrl" value="" />
  <!-- Following should be set to true only in Azure environments where the Auxiliary service is installed and
required. -->
  <add key="UseRemotePDFConverterService" value="false" />
  <!-- Following sets a time before conversion to PDF starts. Default 500, increase if blank documents on a
slow server. -->
  <add key="ViewCreatorDefaultStartConversionTimerInMilliseconds" value="" />
  <add key="ApiKey" value="<Your API key value>" />
</appSettings>
```

> ⚠ If the API keys are not set up correctly, an "Access denied" error will be seen in the Renderer log, for example, when a Forms Builder workflow calls an Anthology Student activity.

Occupation Insight

Occupation Insight is a multi-tenant Software as a Service (SaaS) solution hosted by Anthology Inc.

Occupation Insight integrates Anthology Student program data with workforce market data and can be used as a data source for real-time analytics about the job market in Forms Builder 3.4 and later.

The service interacts with the Anthology Inc. applications via the Sync API and the Power BI API. Institutions using the service need to obtain keys for the APIs and install the Sync Agent for Anthology Student locally.

Important: If you are upgrading to Occupation Insight 2.1 and later and have installed previous versions of the Sync Agent, you must uninstall the previous versions.

Integration with Forms Builder 3.4 and Later

If Occupation Insight is used with Forms Builder, the API Key and Base URL for Occupation Insight need to be configured in the Renderer options. For more details, see Forms Builder Renderer.

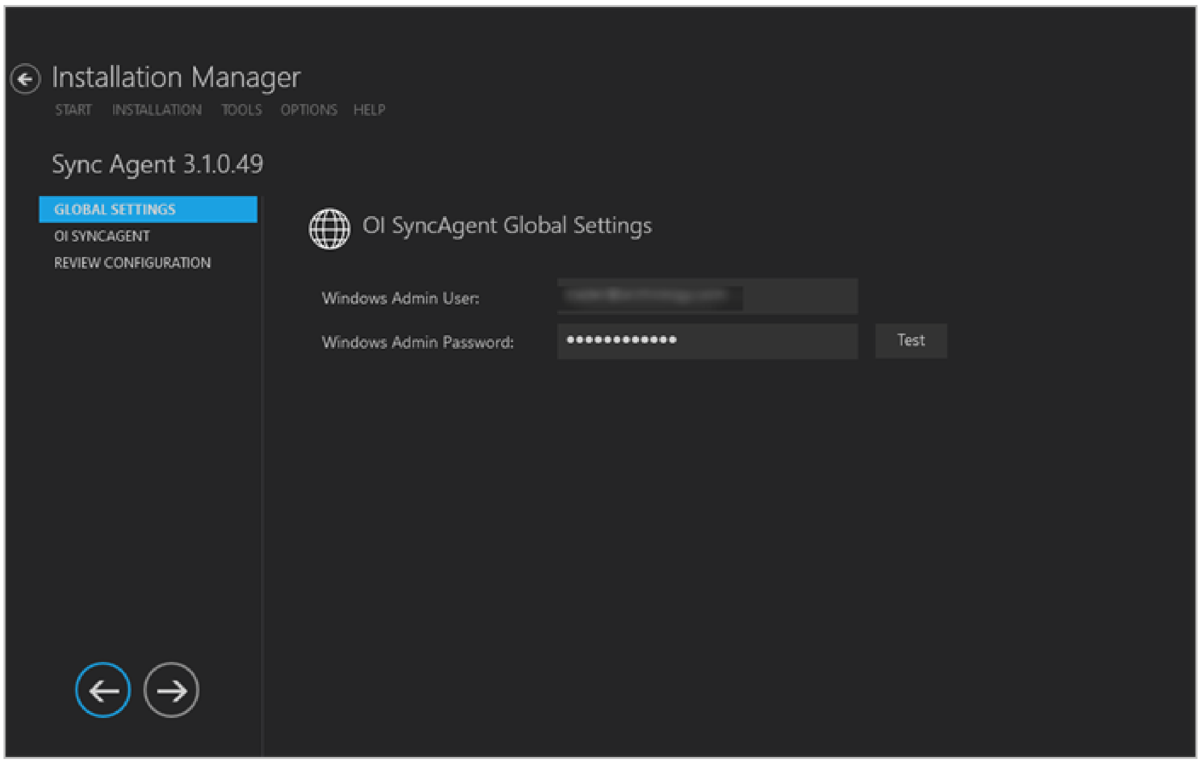
Global Settings

The Global Settings screen contains the user name and password of the system administrator performing the Occupation Insight Sync Agent installation. This user must have:

Important: Information on all Installation Manager screens is not saved until you exit the screen by clicking  or by clicking another component on the navigation menu.

Specify the Global Settings

1. In the Start screen of Installation Manager, click the **Sync Agent** tile. The Sync Agent Global Settings screen is displayed.

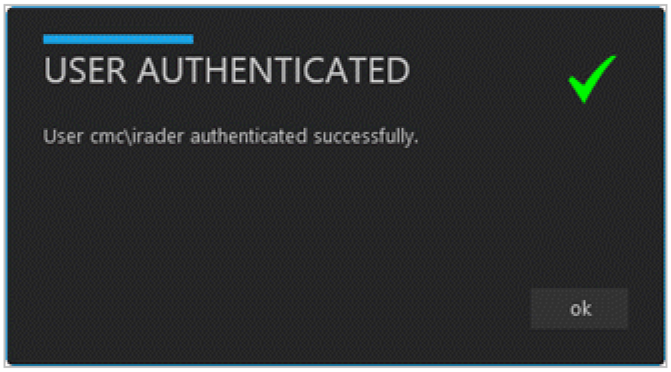


2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer where the installation will occur. Depending on your network environment, specify one of the following:

    - User name
    - Domain\User name
    - Email address of Admin User

3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.

4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.



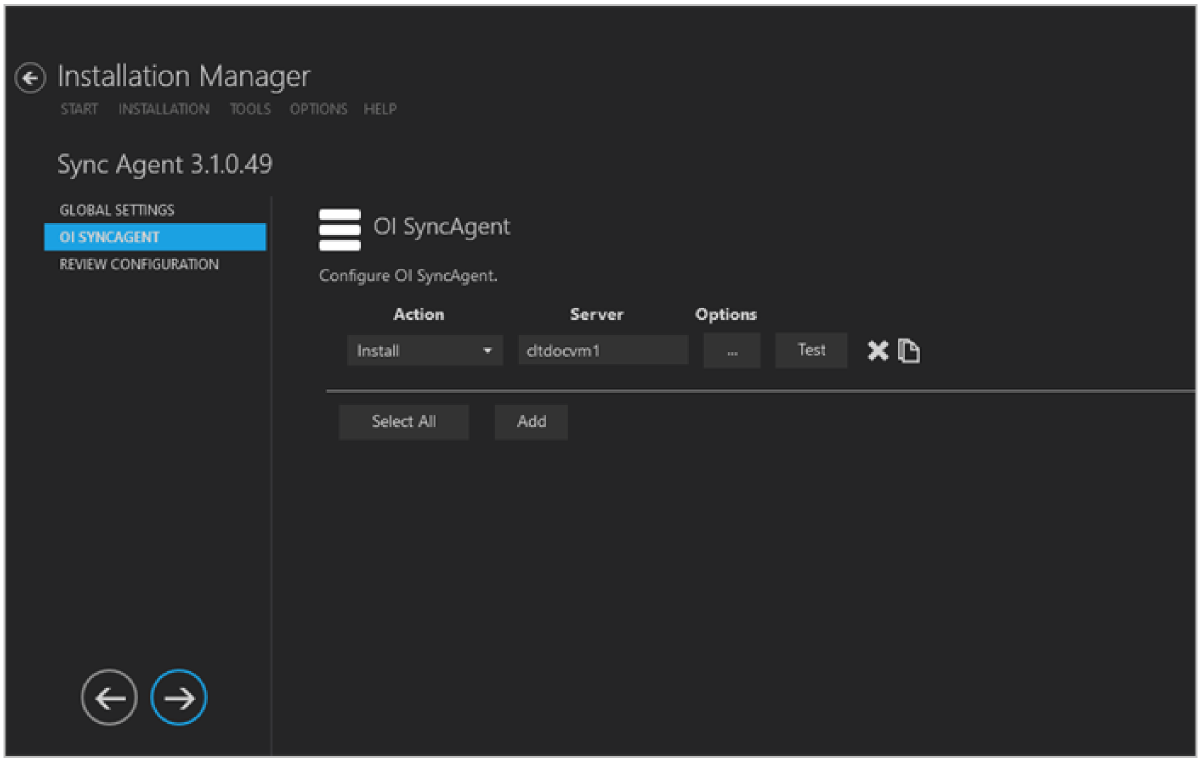
5. If the user is authenticated, click **OK** and click  to continue.

OI Sync Agent

This screen enables you to select the actions to be taken by Installation Manager (e.g., install, uninstall) and to specify the database and configuration options for the Occupation Insight Sync Agent.

Set Up the OI Sync Agent

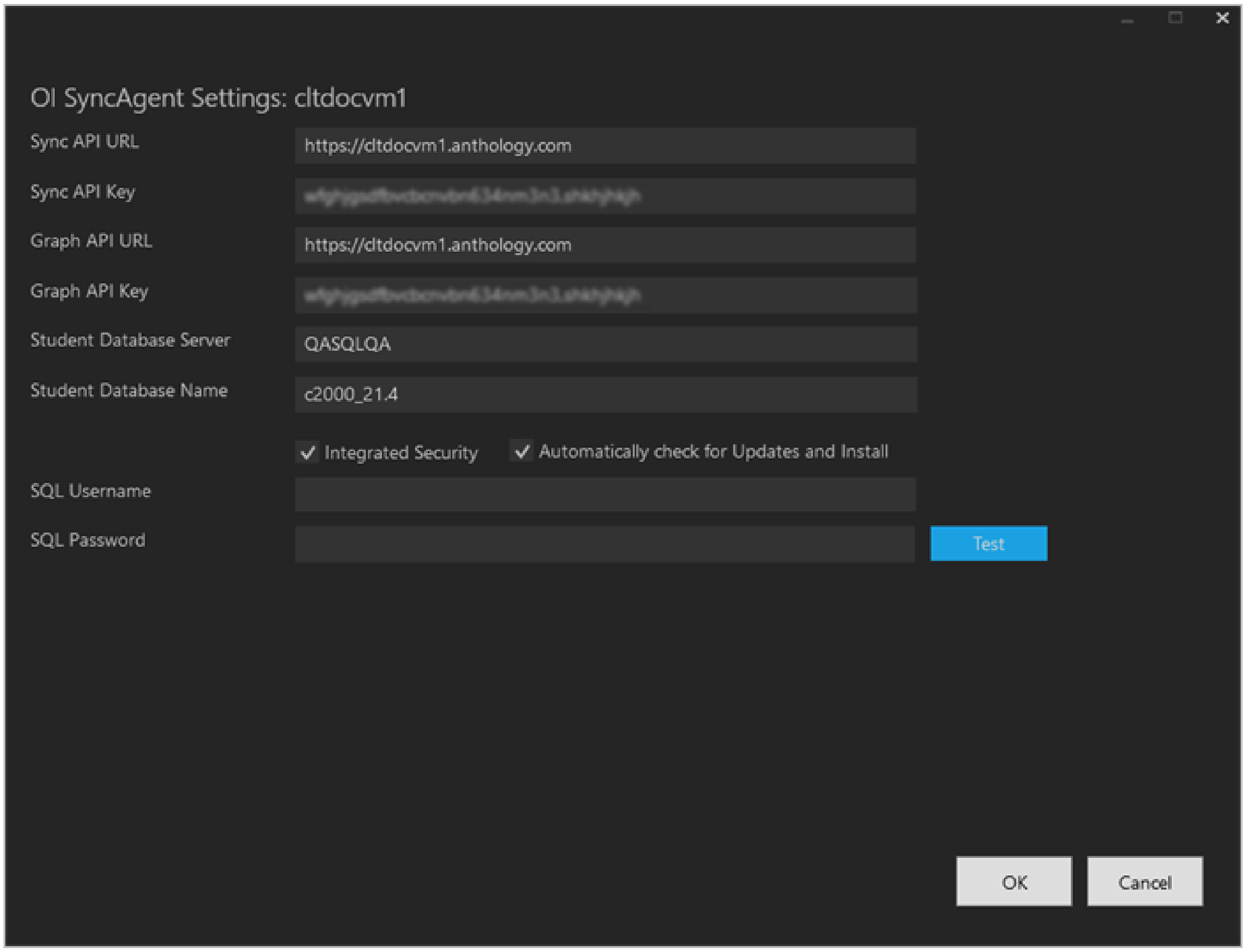
1. In the Installation menu, click **OI Sync Agent**. The OI Sync Agent configuration screen is displayed.



2. Click **Add** to add a line to the Settings screen.
3. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
4. In the **Server** field, enter the name of the server that hosts the Occupation Insight Sync Agent.

5. Click  to view and edit the Options form.



OI Sync Agent Settings

Field	Description
Sync Api URL	Specify the URL for the Occupation Insight Sync API.
Sync Api Key	Enter the key used access the Occupation Insight Sync API.
Graph API URL	Specify the URL for the Occupation Insight Graph API.
Graph API Key	Enter the key used access the Occupation Insight Graph API.
Student Database Server	Name of the Anthology Student database server used by Occupation Insight.
Student Database Name	Name of the Anthology Student database used by Occupation Insight. Click **Test** to verify access to the database.
Integrated Security	Select the Integrated Security check box or specify the SQL Username and Password in the fields below.

Field	Description
Automatically check for Updates and Install	This option is selected by default. It enables the Occupation Insight Sync Agent to check for and install updates. The auto update option streamlines the upgrade process for customers who utilize the agent in their on-premises Anthology Cloud 1.x or Anthology Cloud 2.x environments. If a customer wants to opt out of the auto update functionality, clear the check box while installing the Sync Agent for that customer. **Note**: If the auto-update option is cleared while installing Sync Agent 3.1, and the customer later wants auto update switched **on**, the Sync Agent will need to be uninstalled and reinstalled with the auto-update option selected.
SQL Username	Specify the user name for the Anthology Student database.
SQL Password	Specify the password for the Anthology Student database.

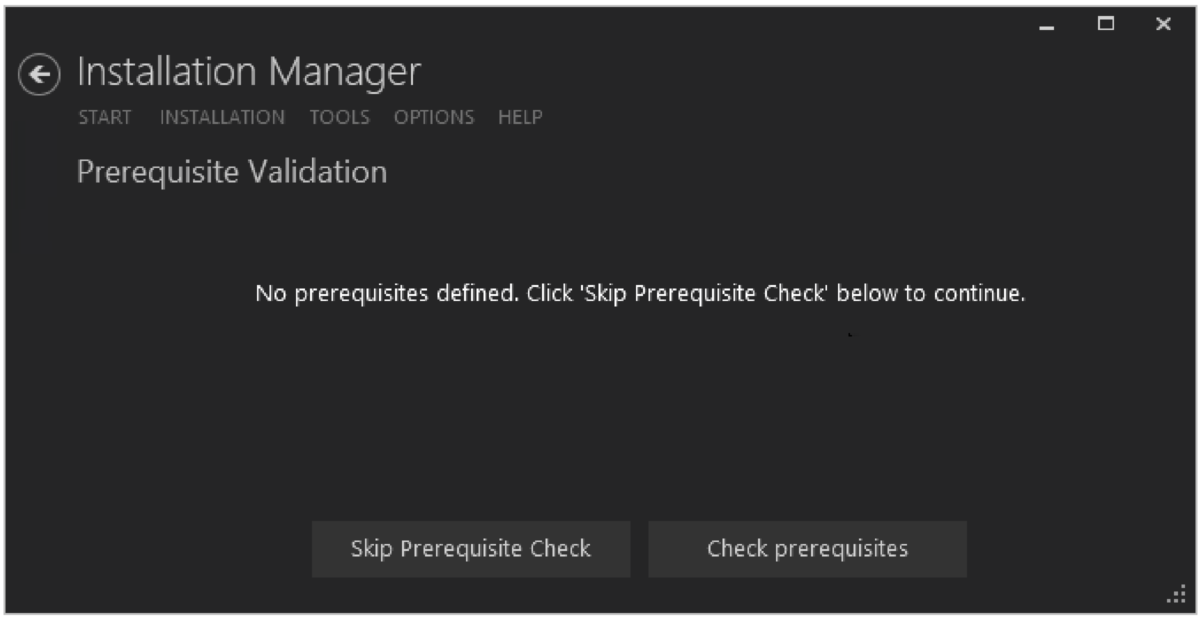
6. Click **OK** to save changes on the Options form. The form is closed.
7. Click  to delete a selected line.
8. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
9. If all tests pass, click .

Review Configuration

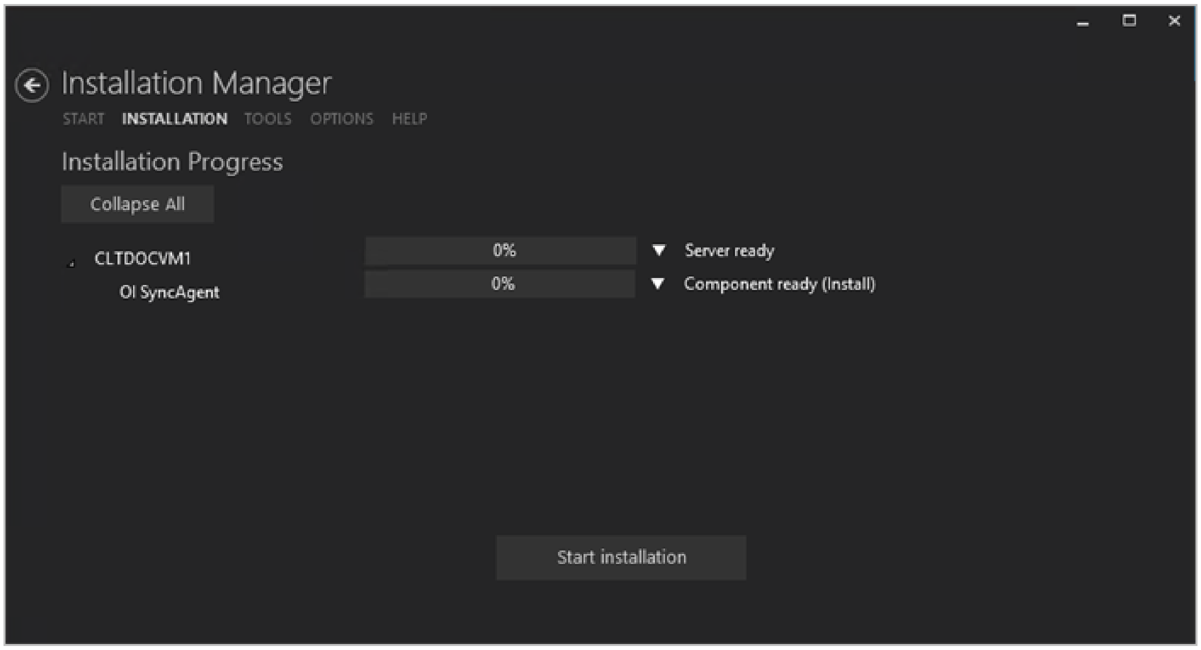
The installation supports multiple setup configurations depending upon the business needs. All of this information is displayed in the Review Configuration screen.

Review the Configuration and Start Installation

1. Once all setup screens have been properly populated and all lines have been tested and found to be functional on each component screen, click **Review Configuration** to see all of the information in one screen.



2. Since there is no prerequisites check for the Occupation Insight Sync Agent, proceed to click **Skip Prerequisites Check**. The Installation Progress screen is displayed.



3. Click **Start Installation**. Progress bars display the percentage progress of the components that are being installed.

   Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

4. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

5. To verify or troubleshoot the installation, click ▼ next to a progress bar to access installation logs and other tools (see Installation).

Workflow

Anthology products are based on an event-driven architecture in which a software element executes in response to receiving one or more event notifications. The main components in this architecture are the event broker and workflows. Events are used in workflows to perform specific activities in response to the events. Each event can be used to trigger one or more activities. Workflows are discrete tasks based on business rules and requirements. Workflow Composer provides activities, that is, 'chunks of code', for power users to compose tasks that are meaningful in a specific environment.

The workflow components include the Workflow Composer application with the built-in Package Manager and the Workflow Tracking Database. The installation of Workflow Composer is mandatory for users of Forms Builder version 3.x and later. The installation of the Tracking Database is optional.

Upgrade Notice for Workflow Composer

Anthology Student

All customers that upgrade Anthology Student must upgrade to the highest version of Workflow Composer that is compatible with the release they are upgrading to. If a customer is already on a lower version of Workflow Composer and is not upgrading Anthology Student, it is also recommended for customers to move to the latest version of Workflow Composer to ensure any changes introduced are adopted.

CampusNexus CRM

All customers that upgrade CampusNexus CRM must upgrade to the highest version of Workflow Composer that is compatible with the release they are upgrading to. If a customer is already on a lower version of Workflow Composer and is not upgrading CampusNexus CRM, it is also recommended for customers to move to the latest version of Workflow Composer to ensure any changes introduced are adopted.

If a CampusNexus CRM customer is upgrading to Anthology Student 21.0, the customer must upgrade to CampusNexus CRM 13.0 and upgrade to Workflow Composer 3.x or 4.x

Workflow Composer 3.x requires **Microsoft .NET Framework 4.7.2**. For more details, see

- https://support.microsoft.com/en-us/help/4054531/microsoft-net-framework-4-7-2-web-installer-for-windows
- https://support.microsoft.com/en-us/help/4054530/microsoft-net-framework-4-7-2-offline-installer-for-windows

Workflow Composer 4.x requires **Microsoft .NET Framework 4.8**. For more details, see

- https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer
- https://support.microsoft.com/en-us/help/4503548/microsoft-net-framework-4-8-offline-installer-for-windows

For detailed installation instructions, see:

- Workflow Composer
- Workflow Tracking Database

The remaining topics in this section are for reference only. The information about Logging, Event Logs, and Service Module Host may be helpful when troubleshooting issues related to workflows.

Workflow Composer

A single instance of Workflow Composer can be used to work with Anthology Student, CampusNexus CRM, and Forms Builder.

To enable this behavior in CampusNexus CRM:

1. In the **Web.config** file of CampusNexus CRM Web Client, change the database details of the '**dbconnection**' key of Workflow Composer to the value that's set in Anthology Student:

   <add name="dbConnection" providerName="System.Data.SqlClient" connectionString="**data Source**=<Name of the Anthology Student database>;**initial catalog**=<Name of the CampusNexus CRM database>;Integrated Security=SSPI;Persist Security Info-o=False;Pooling=True;MultipleActiveResultSets=True;Application Name=Workflow Composer;"/>

2. Make the same change in the **Web.config** file of the following iServices:

   - Account Iservice
   - Cof Iservice
   - Contact Iservice
   - HEFoundation Iservice
   - Report Iservice
   - Portal Iservice
   - Utils Iservice
   - Interaction Iservice

3. Ensure that Application Pool Identity Users of CampusNexus CRM Web Client and iServices are available in Anthology Student's database. They must have login permissions in Anthology Student and read permissions to its database. For more information, see Application Pool Identity and Integrated Security.

4. To consume events triggered from Web Client and iServices in Workflow Composer, set the value of the **Workflow Integrated** parameter to **True** in the Web.config file (Web Client and iServices). By default, its value is False.

Workflow Composer Updates

Workflow Composer 3.x or later:

- Is required with Activities and Contracts for Anthology Student 21.0 and later.
- Is deployed via Installation Manager and ClickOnce.
- Requires users to configure connections. For more details, see Configure Workflow Composer.

Prerequisites

- Due to significant architectural changes needed to support cloud deployments, Workflow Composer 4.x is only compatible with Anthology Student 22.0, Forms Builder 4.0, and CampusNexus CRM 13.0 and higher.
- With the releases of Anthology Student 22.0 and Forms Builder 4.0, V1 workflow activities will no longer be supported and should be replaced with V2 activities. A message will be displayed if V1 activities are detected. Workflows created against V1 contracts will still work and will be supported. Details about required actions are provided in Workflow help.
- Workflow Composer 4.x requires Microsoft .NET Framework 4.8. For more details, see
  - https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer
  - https://support.microsoft.com/en-us/help/4503548/microsoft-net-framework-4-8-offline-installer-for-windows
- If Workflow Composer is configured to connect directly to the database, **Insert** and **Update** permissions for the following database tables are required:
  - WorkflowDefinition
  - WorkflowDefinitionVersion

  The permissions are required for the logged in user when using integrated security and for the login credentials (user name and password) specified if installing via Installation Manager and integrated security is not used.
- If Workflow Composer is configured to use the Workflow Web API, users will need to be associated with either the **Reader** or **Contributor** role for the Workflow Web API enterprise application in the Anthology Cloud 2.0 Azure Active Directory.

Install Workflow Composer

Install Using Installation Manager

Anthology Cloud 1.2 and on-premises customers install Workflow Composer from Installation Manager.

1. Click the **Package Manager** tile in the Start screen of Installation Manager.
2. Download the package for **Workflow Composer**.
3. When the download is completed, return to the Start screen of Installation Manager.
4. Click the **Workflow** tile in the Start screen. File Manager displays the SetupFiles folder containing the Workflow Setup.exe file.

After retrieving the installer, you can run the Workflow Setup.exe directly or copy and distribute it to other users within your organization.

5. Double-click the **Workflow Setup.exe** file. The Workflow Setup screen is displayed.
6. Click **Install**. The Setup Progress screen is displayed. You are notified if a previous installation of Workflow Composer is detected.
7. Click **Next** to continue. The API key and database settings screen is displayed.
8. In the API key database settings screen, specify the following:
    - **Api Key (Package Manager Customer Key)** - This is the same key that is used in the Package Manager screen of Installation Manager.
    - **Database Server**
    - **Database**

    Select **Use Integrated Security** or specify the **Username** and **Password** for the database.

    Click **Test** to verify database access. If the test was successful, click **Next** to continue.
9. (Optional) In the SMTP settings screen, specify the following if you want the application to be able to send emails to the intended recipients:
    - **SMTP Server**
    - **SMTP Port** (default: 25)
    - If applicable, select **Use credentials to authenticate** and specify the **Username** and **Password**.
    - If applicable, select **Enable SSL**.
10. Click **Next**. The installation process starts. Click **Close** when Workflow Composer has been successfully installed.
11. Click the **Workflow** icon on your desktop to open Workflow Composer. Note that the status bar at the bottom left indicates the Workflow Composer version and database connection.

Install Using ClickOnce

Anthology Cloud 2.0 customers install Workflow Composer using a ClickOnce application. ClickOnce allows self-updating Windows-based applications to be installed and run with minimal user interaction. Users install Workflow Composer with one click on the **Install** button or **launch** it from a website.

For details about the ClickOnce URL and login credentials, refer to **https://filetransfer.campusmgmt.com** > **softwareupdates** > **Workflow Composer** > **WF_ComposerInstallationSteps.pdf**.

> ⚠ Depending on the settings and antivirus/malware software installed on your machine and your corporate policies, you may see a warning when installing Workflow Composer and its Activities and Contracts packages.

Run Workflow Composer. Upon startup, Workflow Composer 4.0.1 and later displays the Configuration window.

Continue with Configure Workflow Composer and then Install Activities and Contracts.

Configure Workflow Composer

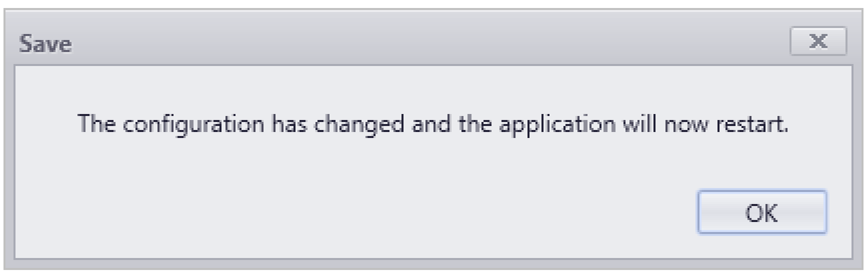
Once Workflow Composer is installed, you need to specify whether it accesses the databases via direct connections or via a Workflow Web API.

- In an Anthology Cloud 2.0 environment, configure the Workflow Web API Connection. The Workflow Web API replaces the Citrix connections used previously in cloud environments.
- In on-premises or Azure (non-Anthology Cloud 2.0) environments, configure Direct Database Connections.

The configuration needs to be done only once when Workflow Composer is installed the first time. The settings are retained during upgrades.

Workflow Composer 4.0.1 introduces the option to change the configuration upon launching the application. You can choose to **Connect** to the previously configured environment or change the configuration to access a different environment.

If you change the configuration, the following message appears. When you click **OK**, Workflow Composer will restart and connect to the newly configured host. It will take a few seconds to start.



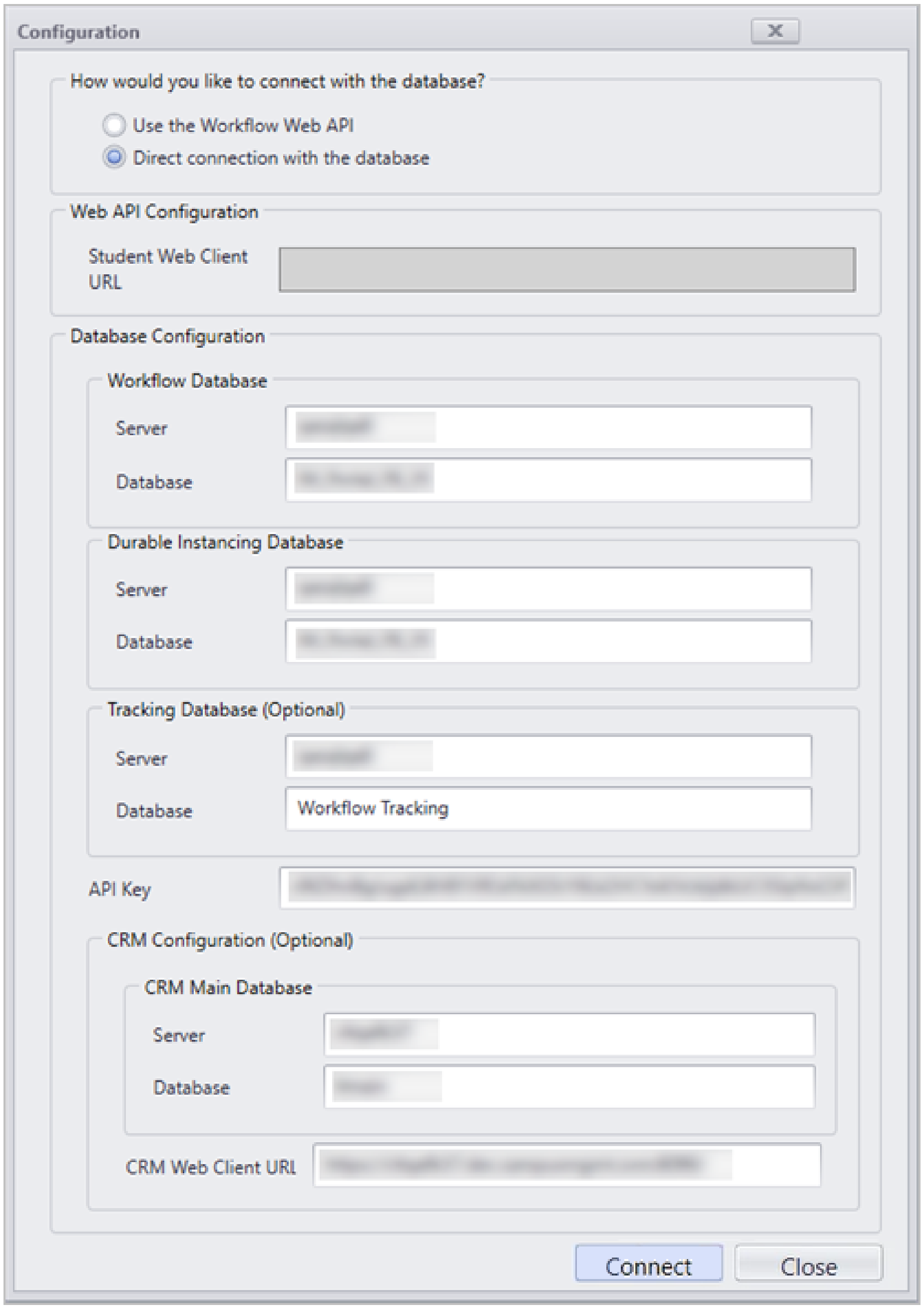
If you click the  button at the top of the Configuration window, you can open the Configuration window again and change the configuration details again.

The System tab in the ribbon of Workflow Composer provides a **Configuration** option that enables you to change the initial configuration.

Direct Database Connections

If you are using Workflow Composer with on-premises databases connections:

1. Select **Direct connection with the database**.



2. Specify the server names and database names for your database connections.

   - The **Workflow Database** is the database that supplies values to your workflow activities. It can be the Anthology Student or CampusNexus CRM database.
   - The **Durable Instancing Database** typically uses the same server and database as the Workflow Database.

- (Optional) The **Tracking Database** is named "WorkflowTracking" by default. It can be on the same server as the Workflow Database and the Durable Instancing Database.

3. In the **API Key** field, specify the key you use to access Anthology Activities and Contracts packages.
4. (Optional) In the **CRM Configuration** section, specify the following:
   - CRM Main Database **Server** and **Database**
   - **CRM Web Client URL**

   By default, the CRM Configuration section will be blank.

   Integrated security will be used for the connection information.

   When the Server and Database are populated under the CRM Main Database, a connection string will be created in the Workflow configuration file named CRMdbconnection.

```
  <connectionStrings>
    <clear />
    <add name="LocalSqlServer" connectionString="data source-
e=.\SQLEXPRESS;Integrated Secur-
ity=SSPI;AttachDBFilename=|DataDirectory|aspnetdb.mdf;User Instance=true"
      providerName="System.Data.SqlClient" />
    <add name="dbConnection" connectionString="Data Source=<server>;Initial Cata-
log=<database>;Integrated Security=True;Application Name=&quot;Workflow Com-
poser&quot;"
      providerName="System.Data.SqlClient" />
    <add name="WorkflowDurableInstancingConnection" connectionString="Data Source-
e=<server>;Initial Catalog=<database>;Integrated Secur-
ity=True;Pooling=True;MultipleActiveResultSets=True;Application
Name=&quot;Workflow Composer&quot;"
      providerName="System.Data.SqlClient" />
    <add name="WorkflowTrackingConnection" connectionString="Data Source-
e=<server>;Initial Catalog=&quot;Workflow Tracking&quot;;Integrated Secur-
ity=True;Persist Security
Info=False;Pooling=True;MultipleActiveResultSets=True;Application Name-
e=&quot;Workflow Composer&quot;"
      providerName="System.Data.SqlClient" />
    <add name="CrmDbConnection" connectionString="Data Source=<server>;Initial
Catalog=<database>;Integrated Security=True;Persist Security Info-
o=False;Pooling=True;MultipleActiveResultSets=True;Application Name-
e=&quot;Workflow Composer&quot;"
      providerName="System.Data.SqlClient" />
  </connectionStrings>
```

   When the CRM Web Client URL is populated, an additional appSettings key will be added in the Workflow configuration file.

```
  <appSettings file="">
    <clear />
    <add key="DataMapperAssembly" value="Cmc.CampusLink.BusinessEntities,
```

```
Culture=neutral, PublicKeyToken=<token>" />
    <add key="ConfigureCampusNexusWcfProxy" value="true" />
    <add key="ConfigureCVueNexusWcfProxy" value="true" />
    <add key="apiKey" value="<key>" />
    <add key="StudentWebClientUrl" value="https://<server>.<domain>:<port>" />
    <add key="CrmWebClientUrl" value="https://<server>.<domain>:<port>/" />
  </appSettings>
```

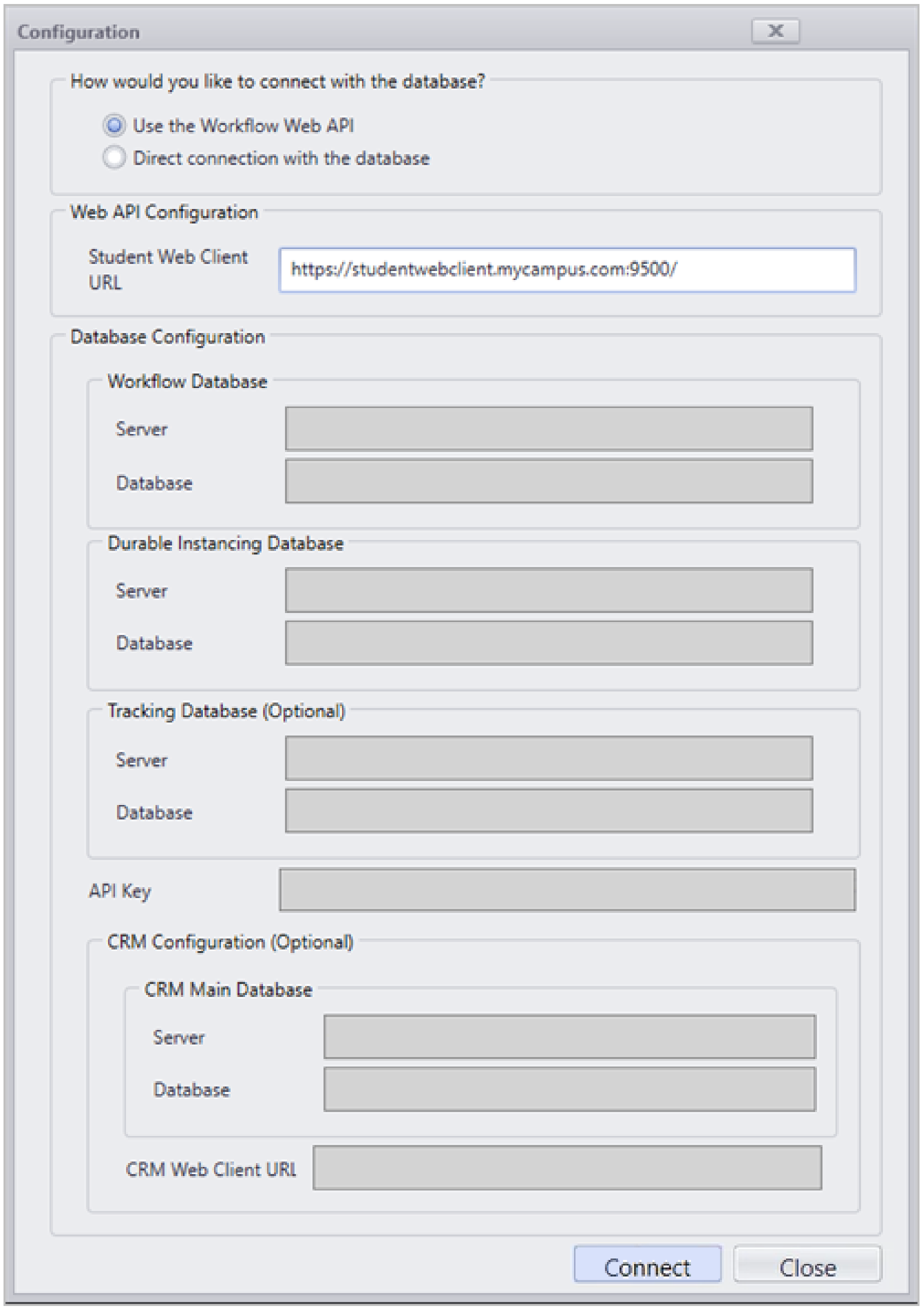
5. Click **Save**.

6. Click **Yes** to confirm that you want to proceed. Workflow Composer will restart.

Workflow Web API Connection

If you are using Workflow Composer in an Anthology Cloud 2.0 environment :

1. Select **Use the Workflow Web API**.



2. Specify your Anthology Student **Web Client URL**, i.e., https://<server>.<domain>:<port>. This URL provides access to the server where the Workflow Web API is deployed.

   The remaining fields are disabled.

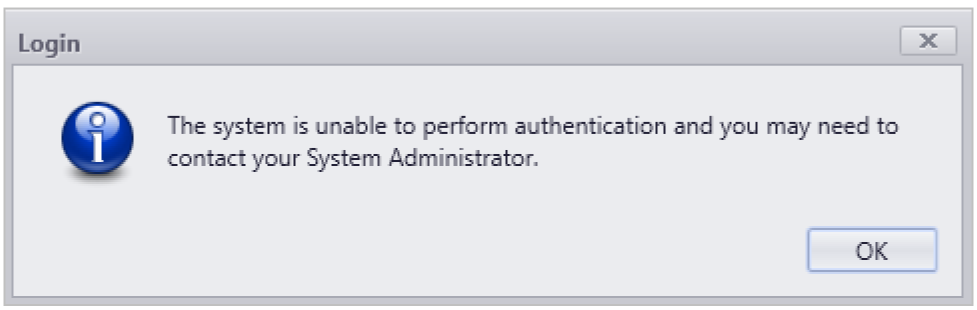
Workflow Composer 3.1 supports dual tenancy in Azure AD. This enables Anthology Inc. support staff to log in to a customer environment to diagnose an issue. CMC staff append **account/login/cmc** to the Student Web Client URL value in order to use a different authentication context for the same environment.

Tenant	Student Web Client URL	Sign in Logo
Azure AD Tenant (Customer)	https://<server>.<domain>:<port>.campusnexus.cloud/	Microsoft
Support Tenant (Anthology Staff)	https://<server>.<domain>:<port>.campusnexus.cloud/account/login/cmc	anthology

3. Click **Save**.
4. Click **Yes** to confirm that you want to proceed. Workflow Composer will restart.

When you use the Workflow Web API, you must log in to your Anthology Cloud 2.0 account in the Azure Active Directory (AAD).

In case of a service interruption or incorrect configuration, a message similar to the following will be displayed.



After you click OK, you can launch Workflow Composer again and the Configuration window will be displayed again. You can change the Web API Configuration and log into your account.

Your user profile in the Anthology Cloud 2.0 AAD is associated with a role.

- The **Contributor** role allows you to add/publish, delete, and edit workflows.
- The **Reader** role allows you to view workflows.

  As a Reader, you can modify a workflow and save it to the file system. But you cannot publish it. If you try to publish or delete a workflow or persisted instance, Workflow Composer returns the message: *"You are not authorized to perform this action."*

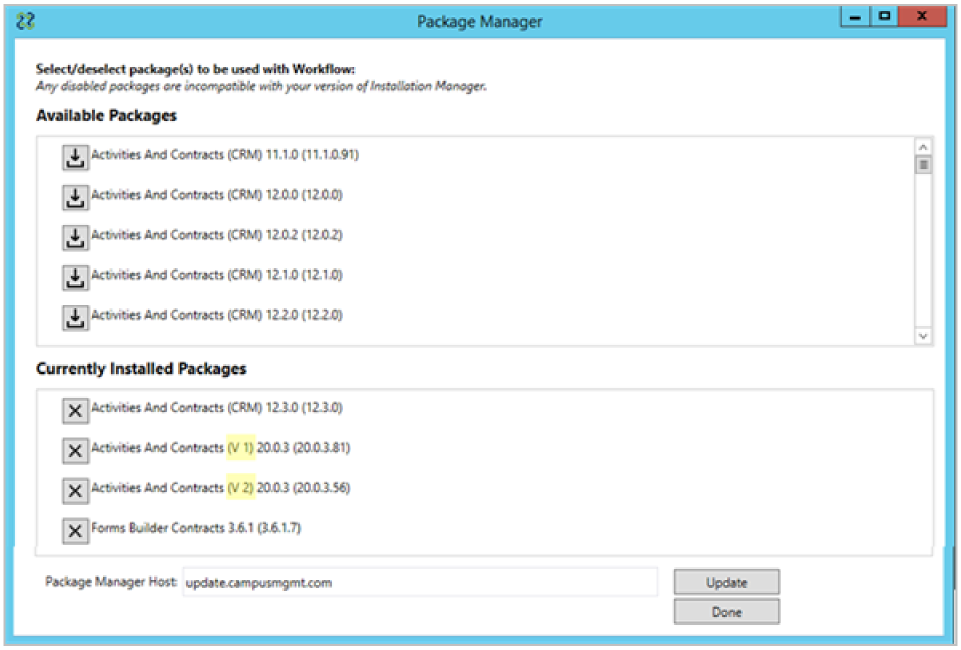
If you are not associated with either role, you will need to contact a System Administrator as you will not have access to the application.

Install Activities and Contracts

After installing Workflow Composer, you need install Activities and Contracts that match the versions of Anthology Student, CampusNexus CRM, and/or Forms Builder in your environment.

Note: If you installed Workflow Composer using ClickOnce with auto update, previously installed packages are removed and need to be reinstalled.

1. In the ribbon of Workflow Composer, click **Package Manager**. Click **Yes** to close Workflow Composer.
2. In the Package Manager screen, check the address of the **Package Manager Host**. If necessary, edit the address and click **Update**.



3. In the *Available Packages* section, locate the Activities and Contracts to be used with Workflow Composer in your environment. The packages are product and version specific.

   You can install only one version of a specific package type. For example, if you installed "Activities and Contracts (CRM) 12.0.0", you cannot have "Activities and Contracts (CRM) 13.0.0" on the same instance of Workflow Composer at the same time. "Activities and Contracts (CRM) 13.0.0" will overwrite "Activities and Contracts (CRM) 12.0.0".

   Anthology Student requires two packages. For example, if your Anthology Student environment is at version 20.0.3, install Activities and Contracts (**V1**) 20.0.3 **and** Activities and Contracts (**V2**) 20.0.3.

   Note: Anthology Student 21.0 (and later) Activities and Contracts are required when using Workflow Composer with Web API connection. Earlier versions of Activities and Contracts are incompatible.

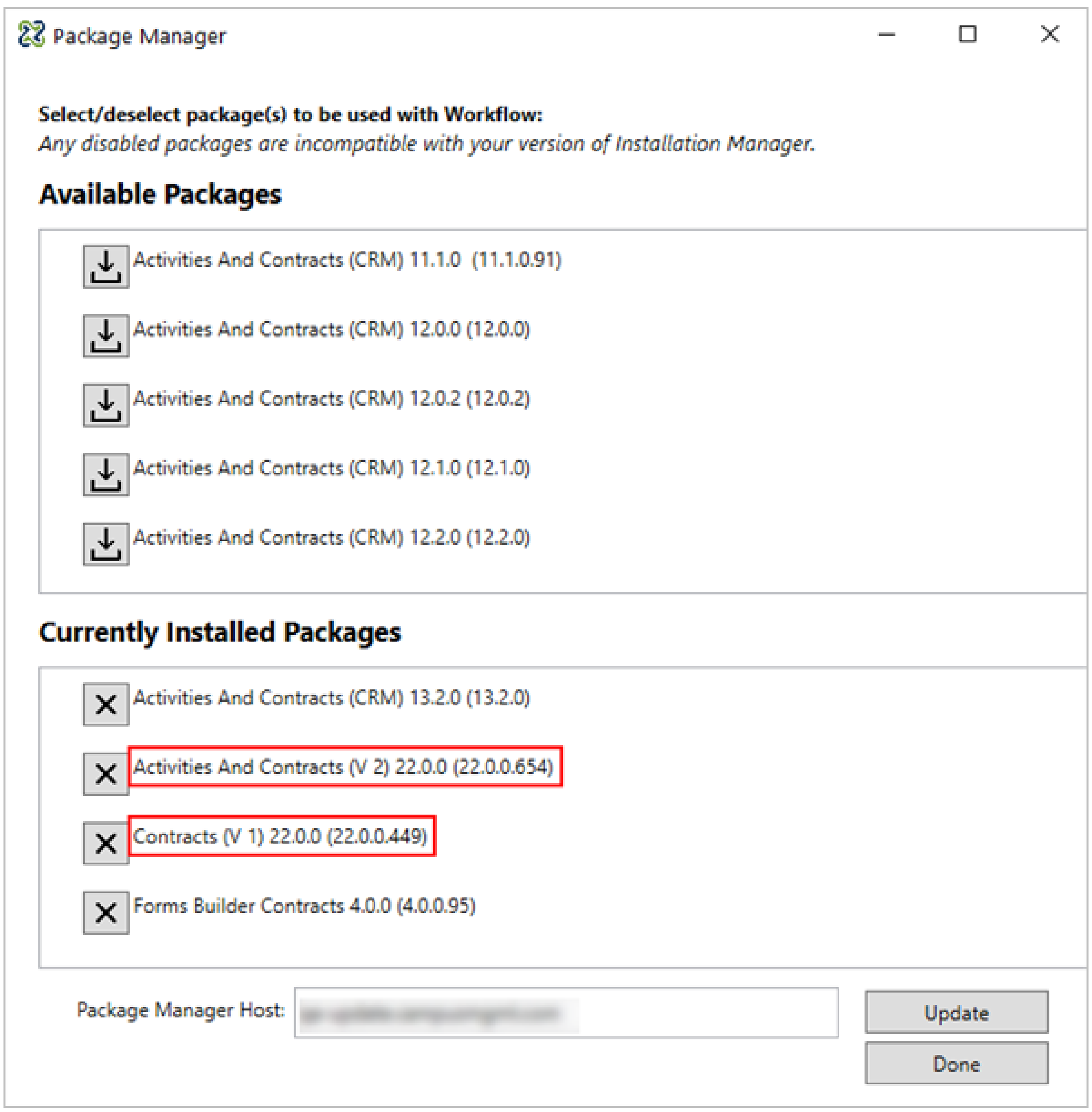
With Workflow Composer 4.x and Anthology Student 22.x and later, you need to install both the V2 Activities and Contracts and the V1 Contract packages.

If you have workflows with V1 Activities, warning messages will be displayed when you select or run a workflow. See Run Time Messages About V1 Activities in Workflow Help.

If workflows that contain V1 Activities have not been updated prior to upgrading to Anthology Student 22.x and installing 22.x Activities and Contracts packages, perform the following steps:

1. Uninstall the V1 and V2 packages for 22.x.
2. Import an earlier version of V1 and V2 packages (e.g., 21.x).
3. Update the workflows to replace the V1 activities.
4. Re-import the 22.x packages.

The packages for Anthology Student 22.x and later will only contain the V1 Contracts and not the Activities.



4. Click to install each package. The installed packages will be listed in the *Currently Installed Packages* section.

   To remove a package, click in the *Currently Installed Packages* section.

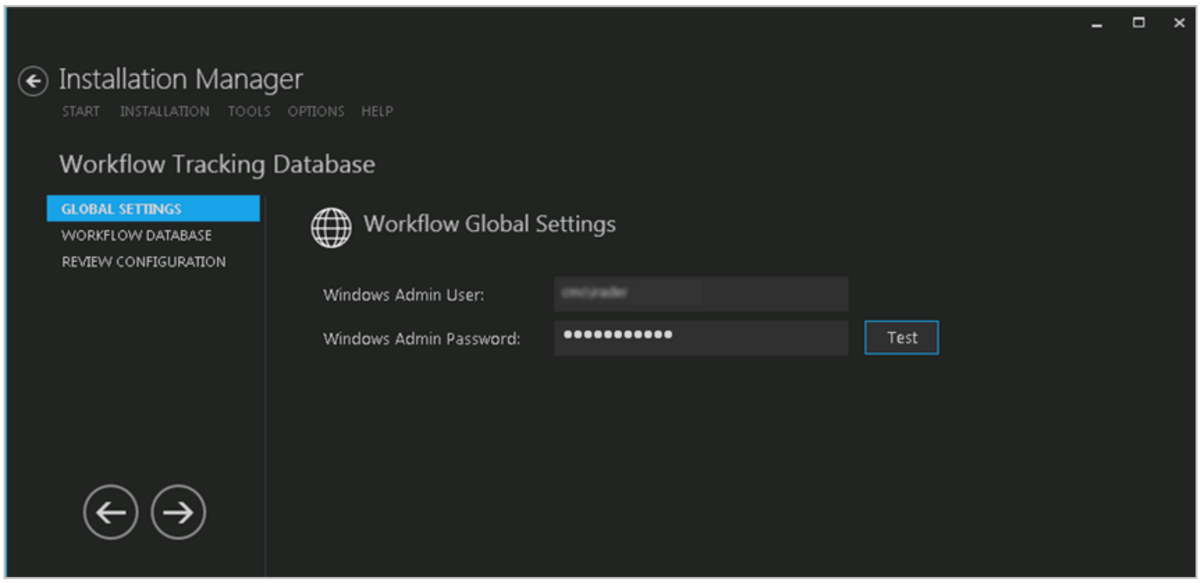
5. Click **Done** to close Package Manager.

Workflow Tracking Database

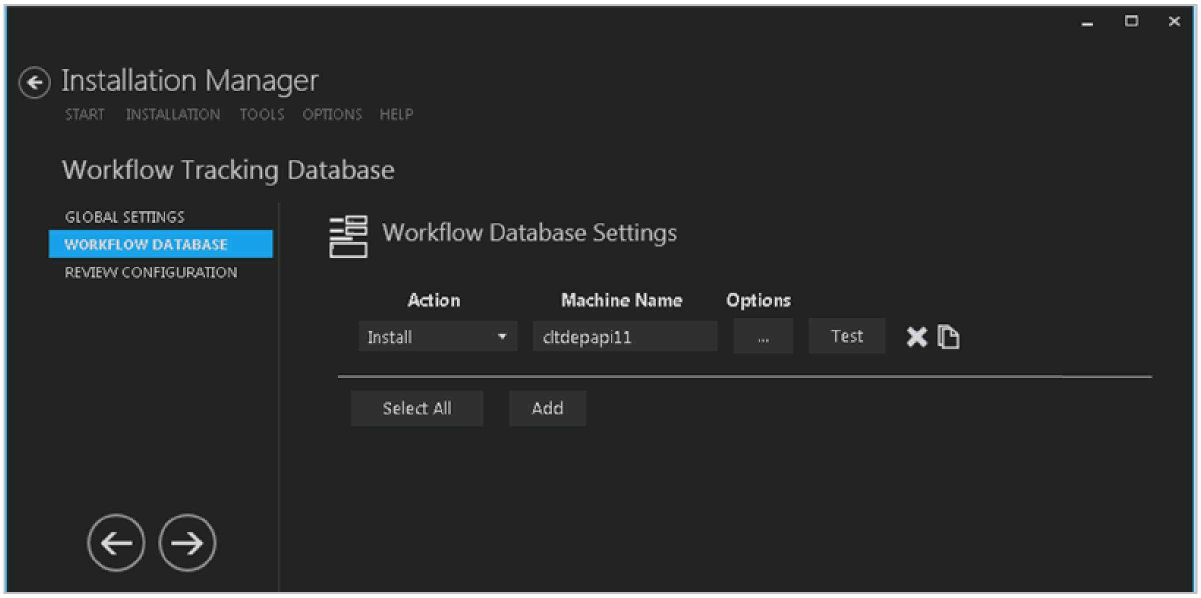
The installation of the Workflow Tracking Database is **optional**. If it is needed, click the Package Manager tile in the Start screen of Installation Manager and download the package for the Workflow Tracking Database.

Set Up the Workflow Tracking Database

1. In the Start screen of Installation Manager, click **Workflow Tracking Database**. The Workflow Global Settings screen is displayed.



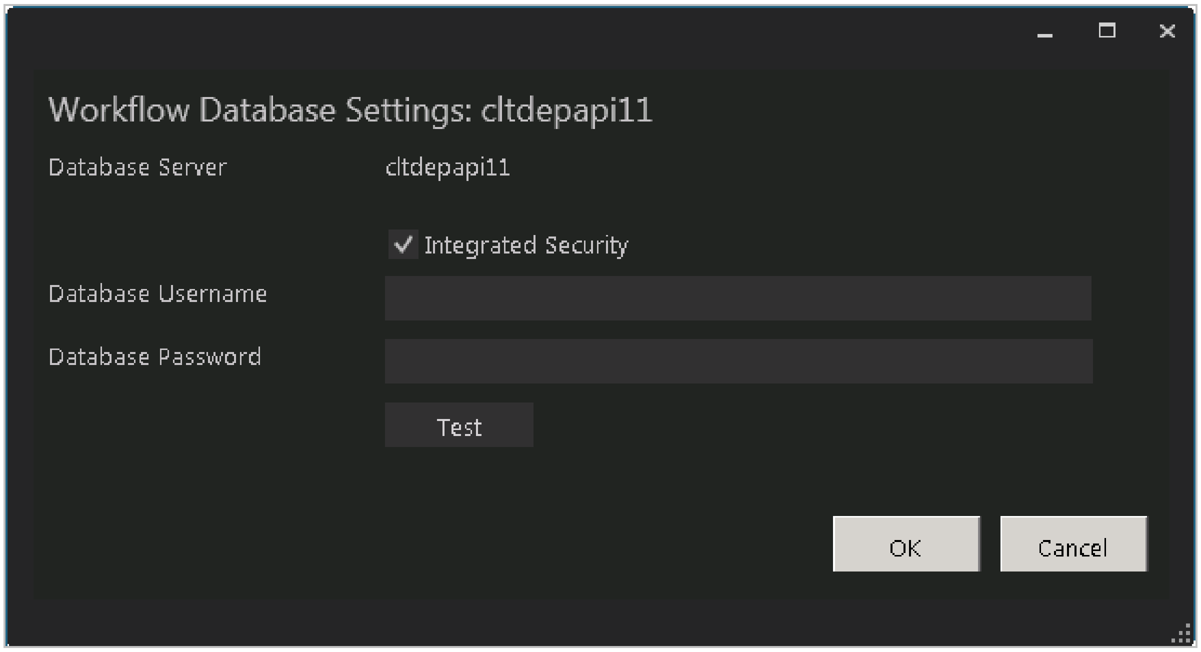
2. In the **Windows Admin User** field, specify the user name of the user with Administrator permissions on the computer on which the installation will occur. Depending on your network environment, specify one of the following:
   - User name
   - Domain\User name
   - Email address of Admin User
3. In the **Windows Admin Password** field, specify the password for the Administrator user name. This password is used in the background for other installation steps.
4. Click **Test** to ensure the user authentication settings are correct. A confirmation message is displayed.
5. If the user is authenticated, click **OK** and click  to continue.
6. In the Installation menu, click **Workflow Database**. The Workflow Database Settings screen is displayed.



7. Click **Add** to add a line to the Settings screen.
8. Select an appropriate **Action**. The following Action values are available:
   - **None** – Performs no action.
   - **Install** – Performs a fresh installation or upgrade of a component. You can install or upgrade multiple components at the same time.
   - **Uninstall** – Removes all subcomponents on that machine and uninstalls the component from Programs and Features.

   Optional: Click **Select All** to set the Action field to **Install** for all components listed on this screen. Click **Unselect All** to set the Action field to **None**.
9. Enter the SQL Server where the *WorkflowTracking* database will be installed.

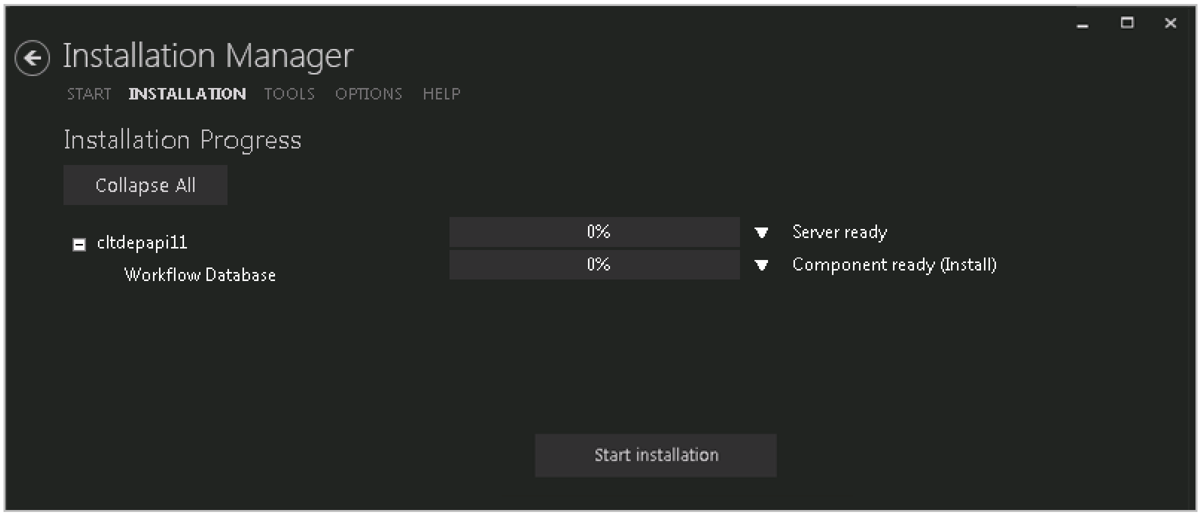
   Note: Installation Manager does not provide an option to enter the name for this database because the name will always be *WorkflowTracking*.
10. Click to copy a line. Edit the copied line as needed.
11. Click to view and edit the Options for Workflow Database Settings. This form is used to specify the database where the workflows are stored.



Options Fields

Field	Description
Database Server	Name of the Workflow Tracking Database server.
Database User-name	User name or account that will be used to connect to the Workflow Tracking Database when Integrated Security is not used. Can be left blank.
Database Pass-word	Password used to connect to the Workflow Tracking Database when Integrated Security is not used. Can be left blank.
Integrated Secur-ity	Select the Integrated Security check box to use this feature and click **Test** to verify the connection. Clear this check box if the database user name and password will be used.

12. Click **OK** to save changes on the Options form. The form is closed.
13. Click  to delete a selected line.
14. Click **Test** to ensure the setup for the corresponding line is correct. If a test on a particular line fails, check all associated fields and click **Test** again.
15. If all tests pass, click . The Prerequisite Validation screen is displayed.
16. In the Prerequisite Validation screen, click **Skip Prerequisite Check**.



17. Click **Start Installation** on the Installation Progress screen. Progress bars display the percentage progress of the components that are being installed.

    Note: The Start Installation button is disabled while the installation is in progress and upon successful installation of all components. If an error occurs during installation of one or more components, the Start Installation button is enabled again.

18. Once the progress bars have reached 100%, a message is displayed confirming the installation, or an error message is displayed.

19. To verify or troubleshoot the installation, click ▼ next to a progress bar to access installation logs and other tools (see Installation).

NLog

The default logging provider used by Anthology is NLog. NLog allows you to set up log targets, levels, rules, layouts, etc. through configuration.

Configure Logging

To configure logging, modify the `nlog.config` file contained within the application's executing directory. For web applications, this file exists alongside the `web.config` file.

Note: In Workflow Composer 4.0.2 and later, the `nlog.config` file no longer exists. The NLog configuration settings have been placed in the app config file (WorkflowComposer.exe.config).

```
<?xml version="1.0" encoding="utf-8"?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <targets>
    <target name="file" xsi:type="File"
      layout="${longdate} ${threadid:padding=3} ${level:padding=-30} ${logger:padding=-30} ${message} ${exception:format=tostring}"
      fileName="${basedir}logs/${shortdate}.txt"
      keepFileOpen="true" />
    <target name="console" xsi:type="ColoredConsole"
      layout="${date:format=HH\:MM\:ss} ${threadid:padding=3} ${logger:padding=-30} ${message}" />
  </targets>
<rules>
  <logger name="*" minLevel="Error" writeTo="file" />
</rules>
</nlog>
```

Above is an example of a config file that is configured with two targets: file and console. The logging rules define which target is executed based on level (`Trace`, `Debug`, `Information`, `Warning`, `Error`, and `Fatal`). The configuration above logs to a subfolder off the base directory whenever an `Error` or `Fatal` level is logged by the application. To log verbose diagnostic information, you can change the `minLevel` to `Trace`, which will log all levels of diagnostic information.

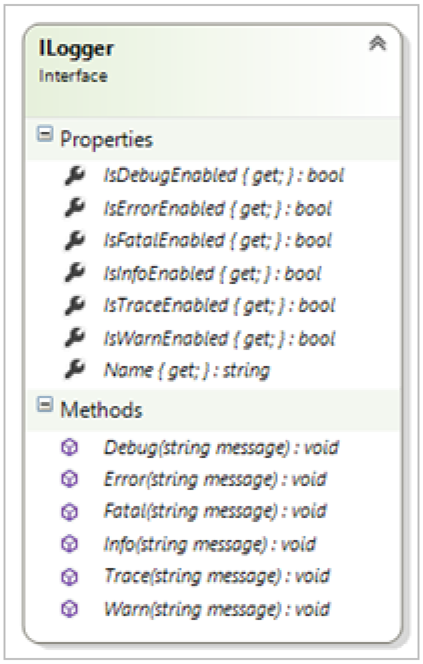
For additional information regarding the configuration file, see https://github.com/nlog/NLog/wiki/Configuration-file.

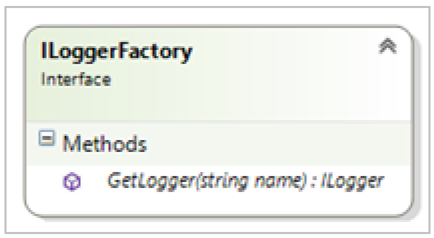
For supported NLog targets, see https://github.com/nlog/NLog/wiki/Targets.

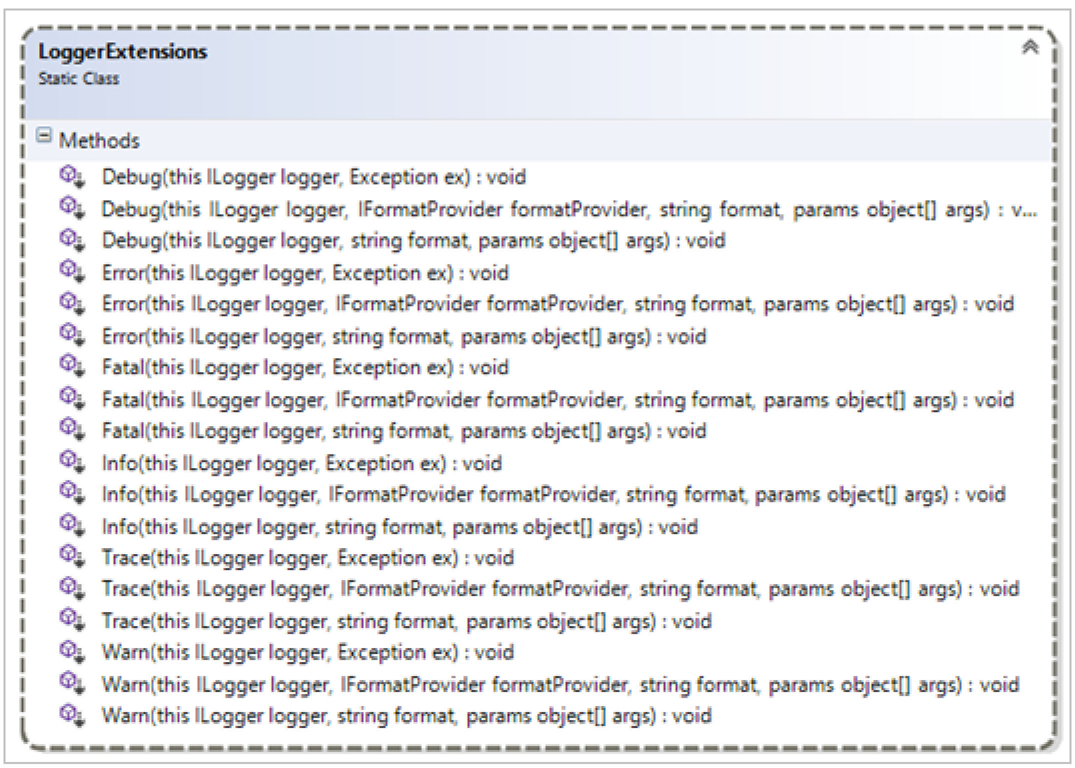
Write Logs

Three public types are associated with the logging framework:

- ILoggerFactory
- ILogger
- LoggerExtensions (extensions methods for ILogger)







There are two ways to enable logging in your class. The preferred way is to receive an ILogger interface as a constructor dependency. The IoC container ensures that this dependency is wired for you.

```
public class MyClass : IMyClass
{
    private readonly ILogger _logger;

    public MyClass(ILogger logger)
    {
        _logger = logger;
        _logger.Debug("ctor");
    }

    public void Foo()
    {
        _logger.Trace("Foo");
        try
        {

        }
        catch (Exception ex)
        {
            _logger.Error(ex);
            throw;
        }
    }
}
```

If your class is a legacy class that does not support DI, you can use the ServiceLocator to retrieve an ILoggerFactory to create the logger.

```
public class MyClass : IMyClass
{
    private readonly ILogger _logger;

    public MyClass()
    {
        _logger = ServiceLocator.Default.GetInstance<ILoggerFactory>().GetLogger(this);
        _logger.Debug("ctor");
    }

    public void Foo()
    {
        _logger.Trace("Foo");
        try
        {

        }
        catch (Exception ex)
        {
            _logger.Error(ex);
            throw;
        }
    }
}
```

Add Log Messages to Classes

Once you have a logger in a class, it is important to add the relevant LOG messages to it that will help us all in debugging and understanding how this class is behaving.

Log Non-Exception Messages

Trace Messages

Use these messages to trace which lines of source code are being executed; they will log what is going on with the code.

Usage: `_log.Trace("Your message.")`

Debug Messages

Use these messages to output the contents or values of variables or properties during the execution of source code; they will log the important values of objects that may affect how the code will execute.

Usage: `_log.Debug("Your message. variable1={0}.", variable1)`

Info Messages

Use these messages to log information that may be useful to know about the normal operation of the application (such as environment variables, paths, etc.).

Usage: `_log.Info("Your message. variable1={0}.", variable1)`

Warning Messages

Use these messages to log messages that we are not sure are acceptable or to track variable/property values that may be close to being out of the acceptable range.

Usage: `_log.Warn("Your message. variable1={0}.", variable1)`

Error Messages

Use these messages to log any exceptions we have that are not being handled. This is typically used in the CATCH of a TRY/CATCH block.

Usage: See Log Exception Messages.

Fatal Messages

Use these messages to log special conditions that indicate that something went terribly wrong in the execution of the code.

Usage: See Log Exception Messages.

Log Exception Messages

To properly log an exception, you should follow one of the patterns shown below. This will allow you to capture the full exception details and also include (if necessary) any other values that may be important for debugging.

Scenario #1. Logging a custom message, some variable value, and the exception

```
string itemToParse = "abc";
try
{
    DateTime.Parse(itemToParse);
}
catch (Exception ex)
{
    _log.Error("[Your message (if any)]. [Variable Name] = '{0}'. {1}", itemToParse, ex);
    throw;
}
```

Result log message:

[Your message (if any)]. [Variable Name] = 'abc'. System.FormatException: The string was not recognized as a valid DateTime. There is an unknown word starting at index 0. at System.DateTime.Parse(String s) at Cmc.UI.Web.EcoSysW3C.------() in \DEV\DEV\Cmc\UI\Web\Cmc.UI.Web.EcoSysW3C\------.cs:line xx

Scenario #2. Logging some variable value, and the exception

```
string itemToParse = "abc";
try
{
    DateTime.Parse(itemToParse);
}
catch (Exception ex)
{
    _log.Error("[Variable Name] = '{0}'. {1}", itemToParse, ex);
    throw;
}
```

Result log message:

[Variable Name] = 'abc'. System.FormatException: The string was not recognized as a valid DateTime. There is an unknown word starting at index 0. at System.DateTime.Parse(String s) at Cmc.UI.Web.EcoSysW3C.------() in \DEV\DEV\Cmc\UI\Web\Cmc.UI.Web.EcoSysW3C\------.cs:line xx

Scenario #3. Logging only the exception

```
string itemToParse = "abc";
try
{
    DateTime.Parse(itemToParse);
}
catch (Exception ex)
{
    _log.Error(ex);
    throw;
}
```

Result log message:

System.FormatException: The string was not recognized as a valid DateTime. There is an unknown word starting at index 0. at System.DateTime.Parse(String s) at Cmc.UI.Web.EcoSysW3C.------() in \DEV\DEV\Cmc\UI\Web\Cmc.UI.Web.EcoSysW3C\------.cs:line xx

Note: You must always inject the exception to the string message using {0}!

If you log an exception as shown below, it will fail to include the exception in the log message. See result of this message below:

```
string itemToParse = "abc";
try
{
    DateTime.Parse(itemToParse);
}
catch (Exception ex)
{
    _log.Error("message.", ex);
    throw;
}
```

Result log message:

message

Read Log Messages to Debug or Troubleshoot

There are three different ways to see your log messages when you wish to debug or troubleshoot an issue:

1. Access the SQL server and get values from the LOGS table (if they are being logged to the DB)
2. Access the local log files being saved in (webroot)/LOGS
3. Use a real-time viewer

You can download the FREE LOG viewer from: http://www.legitlog.com/Products/LegitLogViewer.

Legit Log™

Once you install it, you can use it to:

- Read the log text file, or
- View messages in real-time as they are added to the logger.

To enable real-time logging, follow these steps:

1. Select **Logs >> Live Capture Log**.
2. Select **Start capture global**.

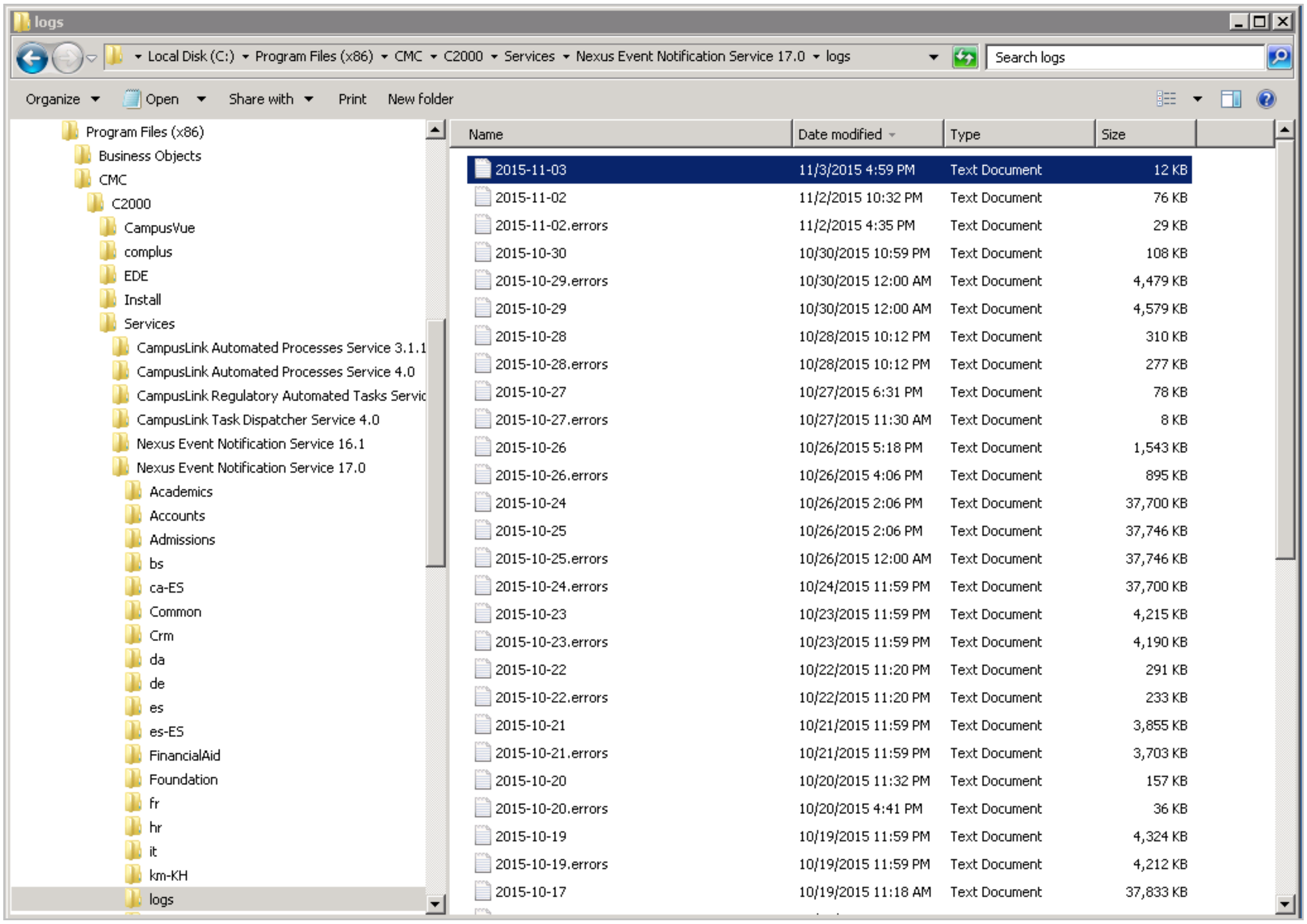
You should now start seeing any log messages as they are added into the logger.

For additional information, see the NLog website: http://nlog-project.org.

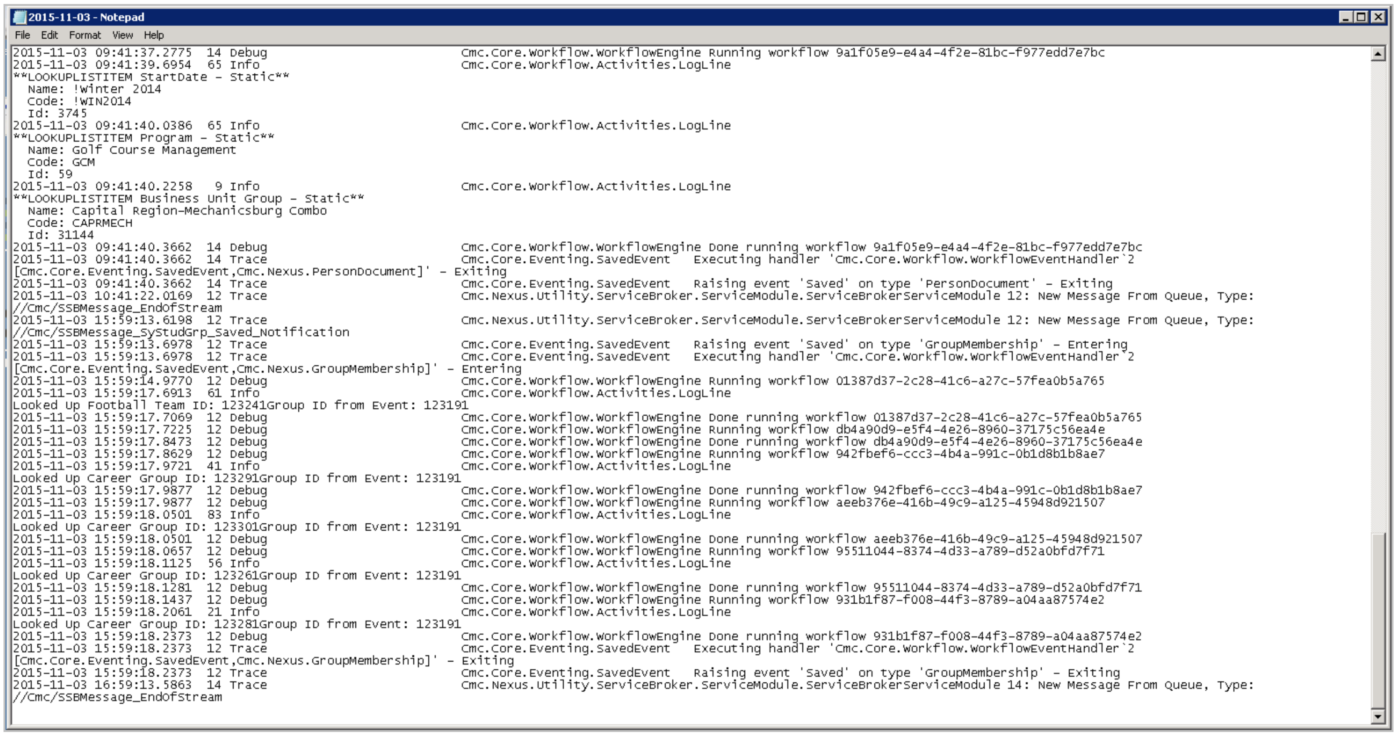
Event Logs

Event logs for workflows that are executed on an Anthology Student server are written to the following folder on the server machine:

```
Program Files (x86)\CMC\C2000\Services\Nexus Event Notification Service
<version>\logs.
```



The logs capture all workflow events including LogLine output, events associated with long running workflows, and errors captured by the Service Module Host.




```
2015-11-03 09:41:37.2775  14 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow 9a1f05e9-e4a4-4f2e-81bc-f977edd7e7bc
2015-11-03 09:41:39.6954  65 Info                           Cmc.Core.Workflow.Activities.LogLine
**LOOKUPLISTITEM StartDate - Static**
  Name: !Winter 2014
  Code: !WIN2014
  Id: 3745
2015-11-03 09:41:40.0386  65 Info                           Cmc.Core.Workflow.Activities.LogLine
**LOOKUPLISTITEM Program - Static**
  Name: Golf Course Management
  Code: GCM
  Id: 59
2015-11-03 09:41:40.2258   9 Info                           Cmc.Core.Workflow.Activities.LogLine
**LOOKUPLISTITEM Business Unit Group - Static**
  Name: Capital Region-Mechanicsburg Combo
  Code: CAPRMECH
  Id: 31144
2015-11-03 09:41:40.3662  14 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow 9a1f05e9-e4a4-4f2e-81bc-f977edd7e7bc
2015-11-03 09:41:40.3662  14 Trace                          Cmc.Core.Eventing.SavedEvent   Executing handler 'Cmc.Core.Workflow.WorkflowEventHandler`2
[Cmc.Core.Eventing.SavedEvent,Cmc.Nexus.PersonDocument]' - Exiting
2015-11-03 09:41:40.3662  14 Trace                          Cmc.Core.Eventing.SavedEvent   Raising event 'Saved' on type 'PersonDocument' - Exiting
2015-11-03 10:41:22.0169  12 Trace                          Cmc.Nexus.Utility.ServiceBroker.ServiceModule.ServiceBrokerServiceModule 12: New Message From Queue, Type:
//Cmc/SSBMessage_EndOfStream
2015-11-03 15:59:13.6198  12 Trace                          Cmc.Nexus.Utility.ServiceBroker.ServiceModule.ServiceBrokerServiceModule 12: New Message From Queue, Type:
//Cmc/SSBMessage_SyStudGrp_Saved_Notification
2015-11-03 15:59:13.6978  12 Trace                          Cmc.Core.Eventing.SavedEvent   Raising event 'Saved' on type 'GroupMembership' - Entering
2015-11-03 15:59:13.6978  12 Trace                          Cmc.Core.Eventing.SavedEvent   Executing handler 'Cmc.Core.Workflow.WorkflowEventHandler`2
[Cmc.Core.Eventing.SavedEvent,Cmc.Nexus.GroupMembership]' - Entering
2015-11-03 15:59:14.9770  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow 01387d37-2c28-41c6-a27c-57fea0b5a765
2015-11-03 15:59:17.6913  61 Info                           Cmc.Core.Workflow.Activities.LogLine
Looked Up Football Team ID: 123241Group ID from Event: 123191
2015-11-03 15:59:17.7069  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow 01387d37-2c28-41c6-a27c-57fea0b5a765
2015-11-03 15:59:17.7225  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow db4a90d9-e5f4-4e26-8960-37175c56ea4e
2015-11-03 15:59:17.8473  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow db4a90d9-e5f4-4e26-8960-37175c56ea4e
2015-11-03 15:59:17.8629  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow 942fbef6-ccc3-4b4a-991c-0b1d8b1b8ae7
2015-11-03 15:59:17.9721  41 Info                           Cmc.Core.Workflow.Activities.LogLine
Looked Up Career Group ID: 123291Group ID from Event: 123191
2015-11-03 15:59:17.9877  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow 942fbef6-ccc3-4b4a-991c-0b1d8b1b8ae7
2015-11-03 15:59:17.9877  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow aeeb376e-416b-49c9-a125-45948d921507
2015-11-03 15:59:18.0501  83 Info                           Cmc.Core.Workflow.Activities.LogLine
Looked Up Career Group ID: 123301Group ID from Event: 123191
2015-11-03 15:59:18.0501  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow aeeb376e-416b-49c9-a125-45948d921507
2015-11-03 15:59:18.0657  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow 95511044-8374-4d33-a789-d52a0bfd7f71
2015-11-03 15:59:18.1125  56 Info                           Cmc.Core.Workflow.Activities.LogLine
Looked Up Career Group ID: 123261Group ID from Event: 123191
2015-11-03 15:59:18.1281  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow 95511044-8374-4d33-a789-d52a0bfd7f71
2015-11-03 15:59:18.1437  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Running workflow 931b1f87-f008-44f3-8789-a04aa87574e2
2015-11-03 15:59:18.2061  21 Info                           Cmc.Core.Workflow.Activities.LogLine
Looked Up Career Group ID: 123281Group ID from Event: 123191
2015-11-03 15:59:18.2373  12 Debug                          Cmc.Core.Workflow.WorkflowEngine Done running workflow 931b1f87-f008-44f3-8789-a04aa87574e2
2015-11-03 15:59:18.2373  12 Trace                          Cmc.Core.Eventing.SavedEvent   Executing handler 'Cmc.Core.Workflow.WorkflowEventHandler`2
[Cmc.Core.Eventing.SavedEvent,Cmc.Nexus.GroupMembership]' - Exiting
2015-11-03 15:59:18.2373  12 Trace                          Cmc.Core.Eventing.SavedEvent   Raising event 'Saved' on type 'GroupMembership' - Exiting
2015-11-03 16:59:13.5863  14 Trace                          Cmc.Nexus.Utility.ServiceBroker.ServiceModule.ServiceBrokerServiceModule 14: New Message From Queue, Type:
//Cmc/SSBMessage_EndOfStream
```

The NLog settings determine the log level and target for event logs.

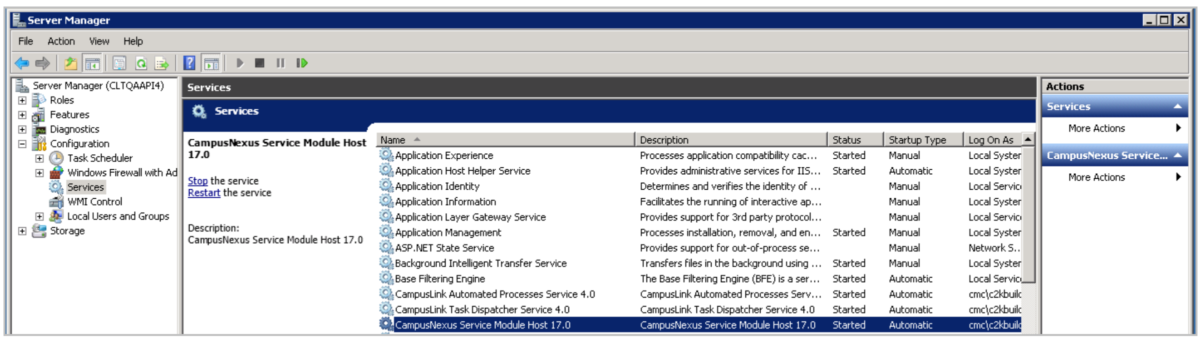
Service Module Host

ServiceModuleHost.exe is a Windows service that allows Saved Events to execute and is responsible for hosting plugin modules to simplify deployment and maintenance of processes that run in the background. Installation Manager sets the services to be started automatically; however, when you are building workflows, it is important to ensure that the Service Module Host is running on the server.

To stop or start the Service Module Host service:

1. On the server where the workflows are executed, select **Start > Administrative Tools > Server Manager**, right-click and select **Run as administrator**.
2. Navigate to **Configuration > Services** and select the **Service Module Host** service.

   By default, the Startup Type of the Service Module Host is set to **Automatic** with a Status of **Started**.

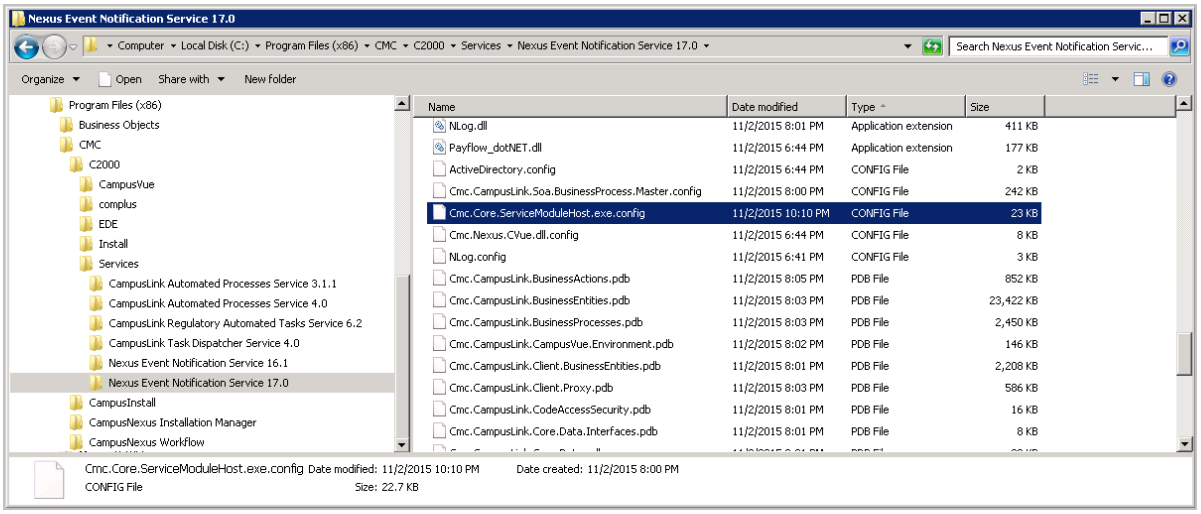
   

3. To stop or restart the service, click **Stop** or **Restart** the service.

Service Module Host Config File

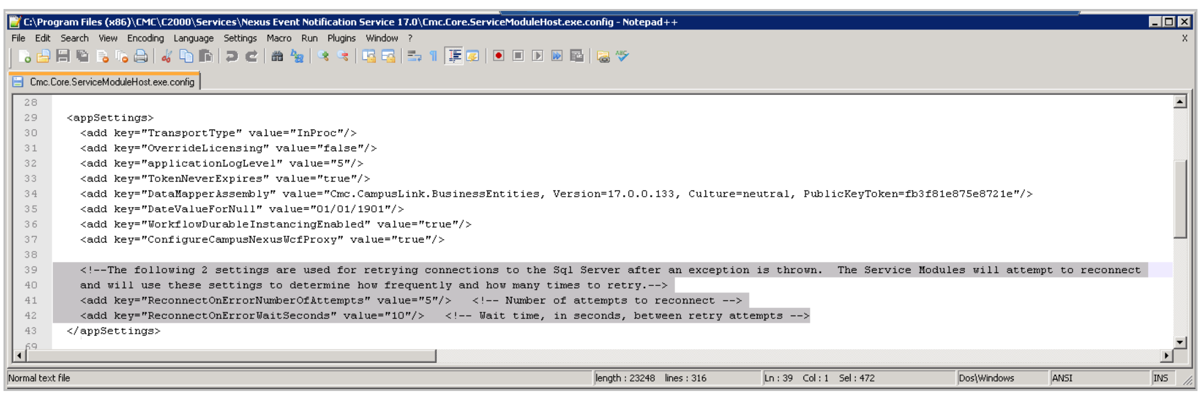
Installation Manager updates the configuration files to ensure that they point to the correct database and contain proper settings. The configuration file for the ServiceModuleHost.exe and normally does not need to be modified; however, you should be aware of the SQL Reconnect Setting and Connection Strings.

The Service Module Host config file is located in `C:\Program Files (x86)\CMC\C2000\Services\Nexus Event Notification Service <version>`.



SQL Reconnect Setting

The Service Module Host service has logic to limit the reconnection attempts when the Service Module Host service senses a connection failure to the SQL database. The time duration is a configured value in seconds that the Service Module Host service uses to attempt the connection again. The settings contain a Number of Retries value indicating how many times to retry the connection.



If, after the number of attempts have been tried and the SQL server is still unavailable, the Service Module Host logs a fatal exception indicating that the Windows service should be restarted after the SQL connection issue has been resolved. The Service Module Host then needs to be stopped and restarted to re-establish the connection (see To stop or start the Service Module Host service:).

The following is an example of an error displayed in the workflow Event Log when the timeout expired and a reconnection was attempted:

2015-08-29 00:00:04.7756 13 Error

Cmc.Nexus.Utility.ServiceBroker.ServiceModule.ServiceBrokerServiceModule System.InvalidOperationException: Timeout expired. The timeout period elapsed prior to obtaining a connection from the pool. This may have occurred because all pooled connections were in use and max pool size was reached.

at System.Data.ProviderBase.DbConnectionFactory.TryGetConnection(DbConnection owningConnection, TaskCompletionSource`1 retry, DbConnectionOptions userOptions, DbConnectionInternal oldConnection, DbConnectionInternal& connection)

at System.Data.ProviderBase.DbConnectionInternal.TryOpenConnectionInternal(DbConnection outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`1 retry, DbConnectionOptions userOptions)

at System.Data.ProviderBase.DbConnectionClosed.TryOpenConnection(DbConnection outerConnection, DbConnectionFactory connectionFactory, TaskCompletionSource`1 retry, DbConnectionOptions userOptions)

at System.Data.SqlClient.SqlConnection.TryOpenInner(TaskCompletionSource`1 retry)

at System.Data.SqlClient.SqlConnection.TryOpen(TaskCompletionSource`1 retry)

at System.Data.SqlClient.SqlConnection.Open()

If errors like this occur frequently and fill up the event logs, you might need to adjust the values for **ReconnectOnErrorNumberOfAttempts** (default value = 5) and **ReconnectOnErrorWaitSeconds** (default value = 10) in the CONFIG file of the Service Module Host.

Connection Strings

The CONFIG file of the Service Module Host contains connection strings for the following databases:

- Anthology Student Database
- Database containing the workflow persistence tables
- Workflow Tracking Database