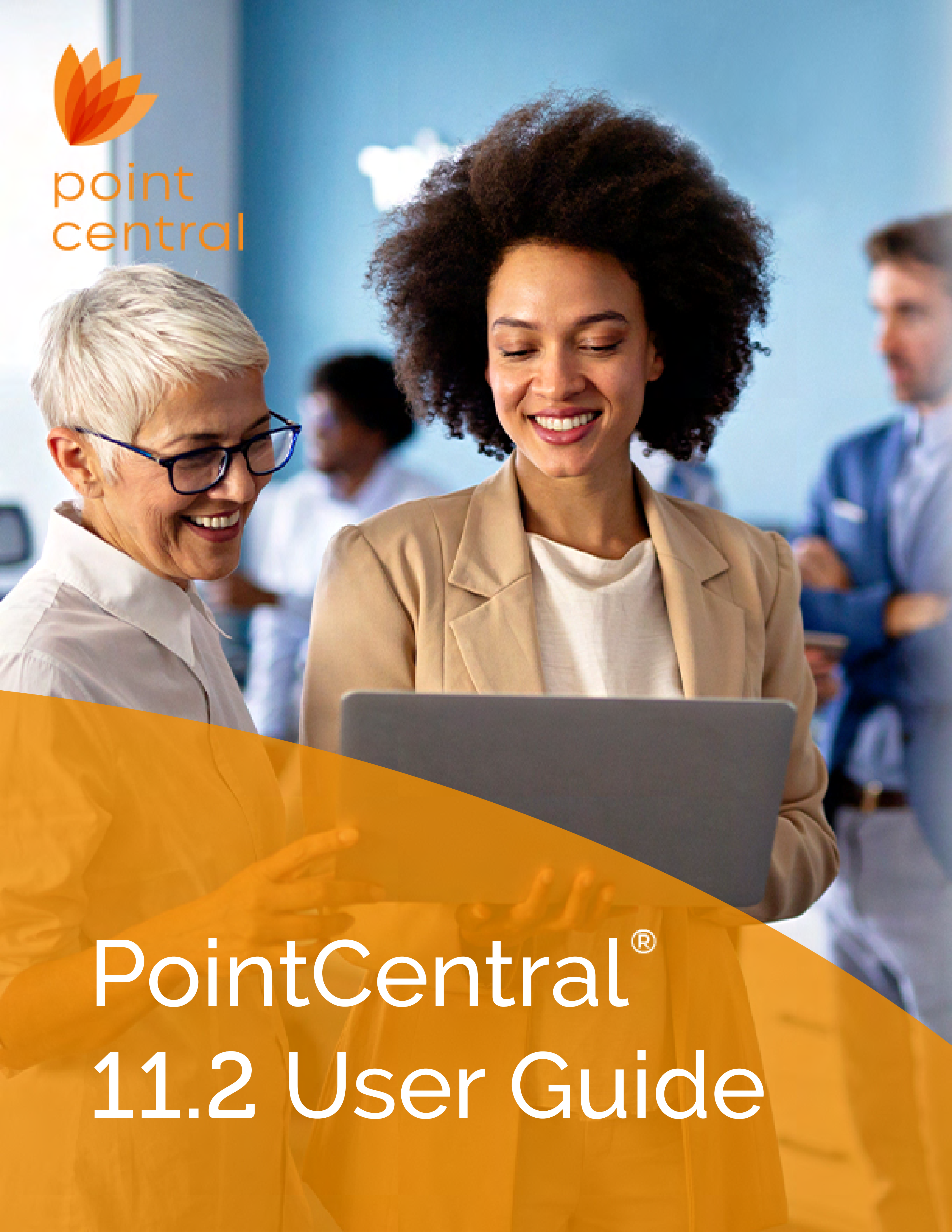


PointCentral®
11.2 User Guide

calyx

6475 Camden Avenue, Suite 207

San Jose, CA 95120

Corporate Office: (408) 997-5525

Dedicated Customer Service: (800) 342-2599

Sales: (800) 362-2599

Change Table

Version	Section	Document Changes
11.2	Edit User Group Access	Added a new section for editing User Group access rights for a Cardex Database.
	Edit User Access Rights	Added a new section for editing User access right for a Cardex Database.
	User Activity Log	Added information related to viewing a user's Activity and were to locate the function.
	Import Resources	The Import Resources section is updated to reflect the changes made to the *Configurations > Import menu*.

Table of Contents

List of Tables

List of Figures

Preface

Product Assistance and Support

The following product support is available.

Table 1: Product Assistance

Contact	Supports
Sales • **Email:** sales@calyxsoftware.com • **Call:** 800-36-CALYX (800-362-2599)–Press 1	• Point • PointCentral • WebCaster account subscription • Website activation and CD-ROM related issues
Dedicated Customer Service • **Email:** customerservice@calyxsoftware.com • **Call:** 800-34-CALYX (800-342-2599)	

Have the following information available when contacting Technical Support:

- Name
- Company name
- Current PointCentral version
- Account ID

Note: Refer to the *Point User Guide* for information about installing the Point client.

Chapter 1 - Overview

PointCentral is a convenient and secure way to share Point files across organizations. Loan data is stored on a central server. The central server makes Point files accessible from any location. Loan originators and processors can instantly access loan files on the central server from Point desktops through an internet connection with the PointCentral performance and speed. Time-consuming operations not possible for large numbers of loans over the limited bandwidth connection to a network branch are available.

File access is centrally administered to provide control over loan data. User access rights to data folders can be granted, modified, or revoked centrally. The **User Group** feature enables grouping Users with similar access requirements. Adding or removing access rights to a data folder for all Users in a User Group is enabled. Users can change passwords at any time without impacting access rights.

Users are defined globally on PointCentral to eliminate the repetitive creation of the same User in every data folder required by conventional Point. View User and group access rights to the following:

- Data folders
- Templates
- Rules
- Cardex

PointCentral manages templates, including:

- Closing cost scenarios
- Loan programs
- Custom forms
- Reports and Marketing documents

PointCentral allows changes to templates that all Point Users are running in the latest versions. PointCentral also manages Cardex databases to decide which Users need to share the same database and know that all Users can access Cardex quickly.

Centralized Data, Security, and Control

Store and manage Point loan files on a secure central server that can be accessed from any location by using Point to log in to internet connections. Copy or delete data files only within Point so data always remains secure.

PointCentral Performance

Search loan files to review task lists and run reports faster than with Point alone. PointCentral compresses the Point files and other information exchanged between Point and PointCentral to speed up all interactions.

Collaboration and Visibility

Share loan files across organizations. Headquarters and branch offices can monitor business by running reports based on loan files stored on PointCentral.

Transparent to Point Users

Loan originators and processors can work with files stored on the PointCentral server.

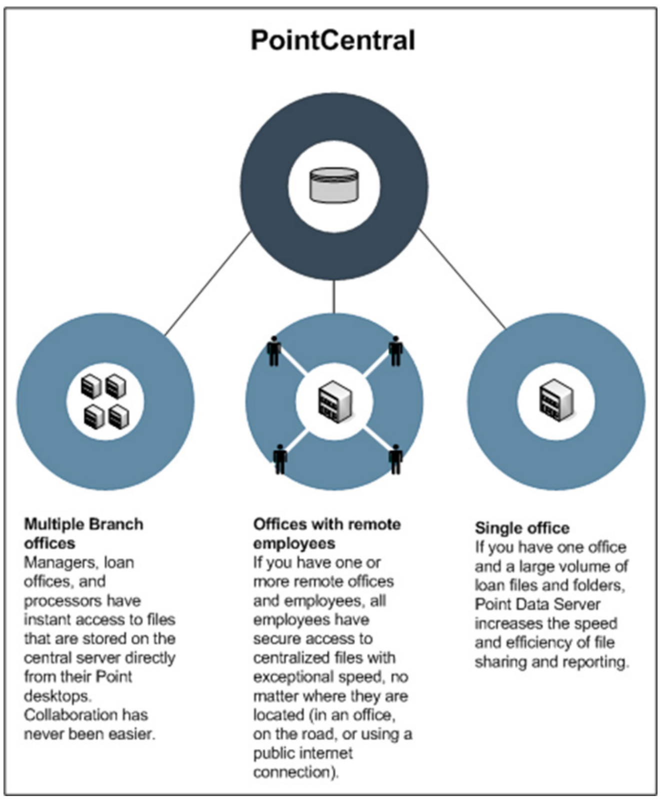


Figure 1: Organization Structure

Architecture

Direct file access in conventional Point requires the following configurations:

- Point and the files to be on the same local area network (LAN).
- Use of a virtual private network (VPN).

Organizations with multiple branches cannot share data across the organization without a VPN. Some common operations in conventional Point are very time-consuming in an environment that contains multiple folders, loans, or a limited bandwidth VPN.

PointCentral eliminates the need for VPN by transferring the Point files over a secure HTTPS connection to the PointCentral server at a central location. The secure HTTPS connection can be made over the public internet. PointCentral maintains a database of common information from Point folders and individual Point files.

The following figure shows how Point accesses conventional data folders over a Windows file share for all operations.

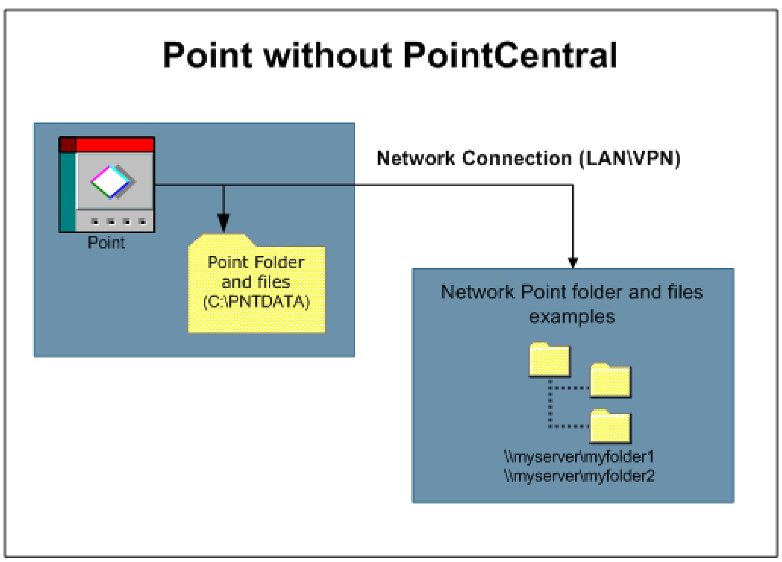


Figure 2: Conventional Point

The following figure shows how Point performs all loan and template access operations by using a secure HTTPS connection to PointCentral.

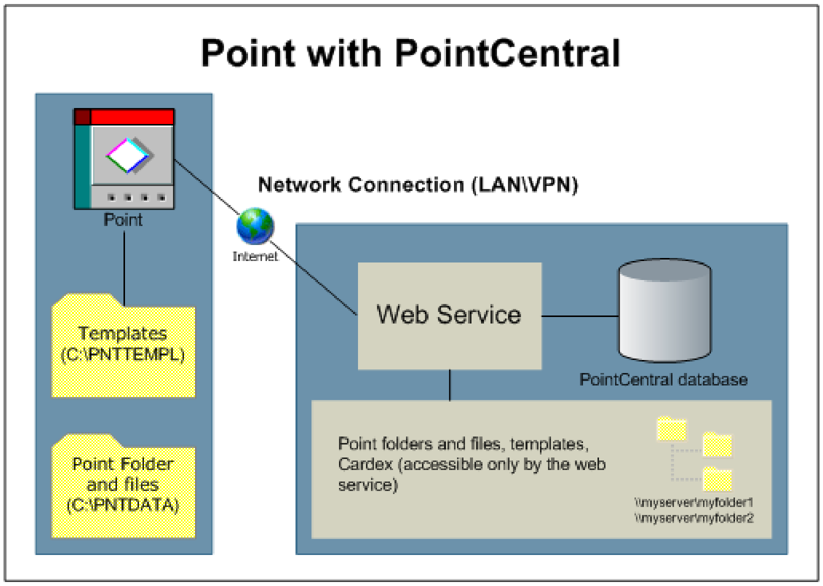


Figure 3: Point with PointCentral

Point uses a secure HTTPS connection to PointCentral through the web service when performing the following loan access operations:

- Opening a loan
- Saving a loan
- Retrieving lists of loans
- Retrieving lists of tasks
- Retrieving lists of reports

The web service accesses the SQL database with no file share. No file share eliminates the VPN and results in faster execution time when accessing the following screens:

- Point Find
- Advanced Find
- List Co-Borrowers
- Search Tasks
- Reports

The SQL database maintains read-only copies of select Point fields to accelerate operations. The Point loan files are stored on PointCentral. Point clients do not access the Point files on PointCentral. The file contents are transferred over the HTTPS internet connection between Point and the PointCentral server. The web service and **FileSync** components transfer the file contents between the HTTPS connection and server. Point does not read or write files to the PointCentral server. The file share is eliminated, and all files are transferred over the HTTPS connection.

Components

PointCentral consists of the following major components:

- Service
- Administration Web Site
- FileSync Windows Service
- SQL database
- Configuration Wizard
- Point loan and data folder access.
- Templates
- Cardex database

The components are shown in the following diagram.

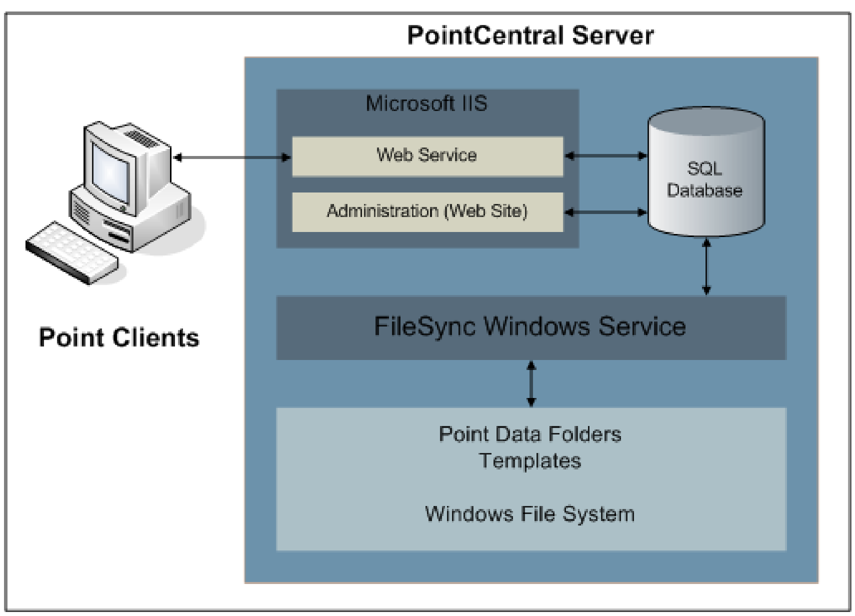


Figure 4: PointCentral Components

Web Service

Point sends requests to the **CalyxPdsService** web service. The Microsoft® Internet Information Services (IIS) web service queries the database and accesses loans or returns lists of results. Conventionally time-consuming operations are returned much faster than the file scanning method used by conventional Point. Operations include:

- Searches
- Advanced searches
- Tasks
- Reports

Administration Website

The *Administration* website is the administrative interface to PointCentral. The system administrator uses the interface to:

- Create Point data folders.
- Create Users
- Create User Groups
- Assign access rights to data folders.
- Configure PointCentral
- Monitor PointCentral
- Manage PointCentral

FileSync Windows Service

The FileSync (CalyxPdsFileSync) Windows Service monitors individual Point files while saving changes through the HTTPS connection to the web service.

FileSync stores loan files on the server file system. The web service reads the loan files from the server file system. The process is invisible to the Point client as the client transmits files over the HTTPS connection to the PointCentral server. Changes detected in the Point files are synchronized to the database to keep the information in the database synchronized with the Point files and ready for query. The FileSync component switches conventional Point data folders to accelerated and vice-versa.

SQL Database

The SQL database stores the common information required for Point to provide:

- Searches
- Tasks

- Reports
- Related operations

PointCentral Configuration Wizard

The PointCentral Configuration Wizard is used to create or upgrade a database. The administrator uses the *Wizard* screens to configure a new system or upgrade a previous version. The Wizard updates the necessary connection strings in the components.

Point Loan and Data Folder Access

PointCentral accesses the PointCentral loan files and data folders through the secure HTTPS connection to the web service. The Windows file share to data folders required by conventional Point is eliminated with PointCentral.

Templates and Cardex

PointCentral manages templates and Cardex databases. Template files are stored on the centralized server and distributed to the Point clients as required.

PointCentral processes requests from Point quickly. The time is used for transmitting the results over the limited bandwidth available through the link between the net branch and headquarters.

Performance Tests

A test environment was created to check the server performance. The following test cases were selected to represent typical environments:

- The environment bandwidth was limited to roughly a DSL connection dedicated to one Point User.
- The environment included a typical LAN environment with network connections of 100Mbps.
- The environment bandwidth was limited to a DSL connection shared by ten Point Users.

The following figure shows the performance advantage of PointCentral acceleration with limited bandwidth (10KB download).

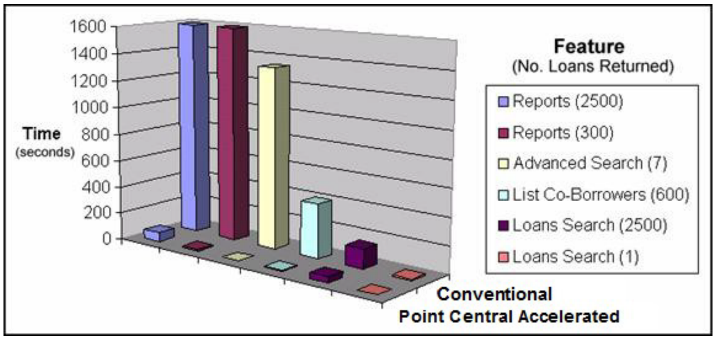


Figure 5: Acceleration Performance

The following table shows the results when the bandwidth was limited to 100KB download (typically a DSL connection).

Table 2: DSL Connection

Point feature	Number of loans returned	Conventional folder	Accelerated folder
Reports	2,500	3 minutes 43 seconds	11 seconds
Reports with a date range	300	3 minutes 38 seconds	2 seconds
Advanced search	7	2 minutes 18 seconds	1 second
List co-borrowers	600	27 seconds	1 seconds
Loans search	2,500	25 seconds	7 seconds
Loans search	1	1 second	1 second

The following table shows the results in a LAN environment (100Mbps).

Table 3: LAN Environment (100Mbps)

Point feature	Number of loans returned	Conventional folder	Accelerated folder
Reports	2,500	1 minutes 43 seconds	9 seconds
Reports with a date range	300	1 minutes 24 seconds	2 seconds
Advanced search	7	15 seconds	1 second
List co-borrowers	600	7 seconds	1 second

Point feature	Number of loans returned	Conventional folder	Accelerated folder
Loans search	2,500	9 seconds	2 seconds
Loans search	1	1 second	1 second

Web Service

The web service completes Point client requests when a Point User is searching for the following:

- Loans
- Tasks
- Opening
- Saving loans
- Generating reports
- Other necessary operations

web services enable programs to communicate between computers transparently over a network.

Web Service Access

Use the following steps to access the web service.

1. Select the **Start** menu.
2. Select **Administrative Tools**.
3. Select **IIS Manager**.

A virtual directory named service is created in the *Microsoft IIS Default* website when PointCentral is installed. A clear improvement in performance is noticeable in the following features:

- Loan Search
- Advanced Search
- List Co-Borrowers
- Folders
- Tasks
- Reports and Marketing Documents

The back-end database is implemented by using Microsoft SQL Server. The following figure illustrates a Point client making a request to the web service through to the PointCentral middle tier. The middle tier accesses the back-end SQL database to retrieve the results. Not all loan information is stored in the PointCentral database. The database contains only the information needed to improve performances, such as:

- Searching
- Opening
- Saving
- Loans
- Tasks

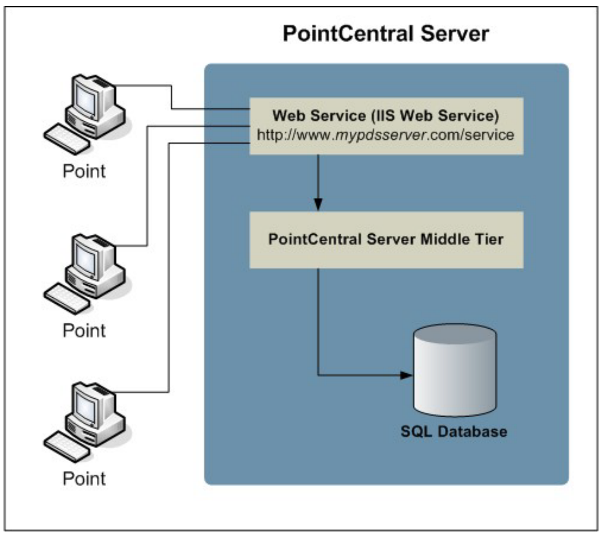


Figure 6: Server Loan Retrieval

Web Service Launch

The Point client and web service exchange is XML (Extensible Markup Language). Verify the web service is properly configured and running to Call the web service directly Point. Open the main web service page through a browser to display a standard HTML page with information about the web service status.

Use the following steps to open the main web service page.

1. Log on to the computer where PointCentral is installed.
2. Select Start.
3. Select **All Programs**.
4. Select **Calyx Software**.
5. Select **PointCentral**.

6. Select **PointCentral Service** to open the local host web site.

Note: Localhost resolves to the IP address 127.0.0.1 to resolve the local server. Point the browser to the web service URL from any server in the network.

See SSL Certificate Backup for more information about the local host service and the SSL certification.

Event Log

The web service logs messages to the Windows **Event Log**. All informational messages, warnings, and errors are written in the Windows **Event Log**.

Use the following steps to start the *Windows Event Viewer*.

1. Select **Administrative Tools** from the *Control Panel*.
2. Select **Event Viewer**.

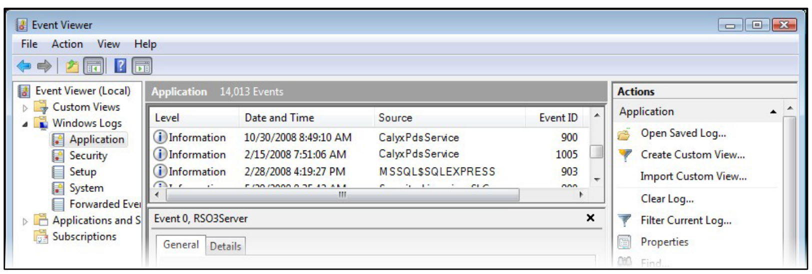


Figure 7: Event Viewer

3. Double-click an event in the list from **CalyxPdsService** to view the event properties.

The web service indicates the event has started in the example. The example includes the major, minor, and build number. The event is created when the first request is made to the web service after previously stopping.

The web service could stop for one of the following reasons:

- PointCentral rebooted.
- Microsoft IIS stopped and restarted.
- The default website in Microsoft IIS stopped and restarted.
- Maintenance message or other value in the web service configuration file changed.
- Version updated.

Note: The first request to the web service may take a few moments to process because the web service is initializing. Subsequent requests are faster.

See Advanced Configuration for more information about changing values in the web service configuration file.

Messages to Point Users

Results are returned to Point in normal requests from clients to the web service. Problems may occur causing a warning or an error message to display. Messages are issued immediately after the results are returned to the Point client.

- See Advanced Configuration for more information about the loan and task maximum capacity.
- See Web Service Errors and Warnings for a list of the possible error codes and messages returned to Point Users and information about unsupported fields.

Multiple Server Deployment

Most organizations that install and configure PointCentral require only one system to centralize folders.

Regional Deployment

A regional deployment can accommodate bandwidth requirements better than a centralized deployment for larger organizations. One server deployed for every region could support a feasible number of branches as shown in the following figure:

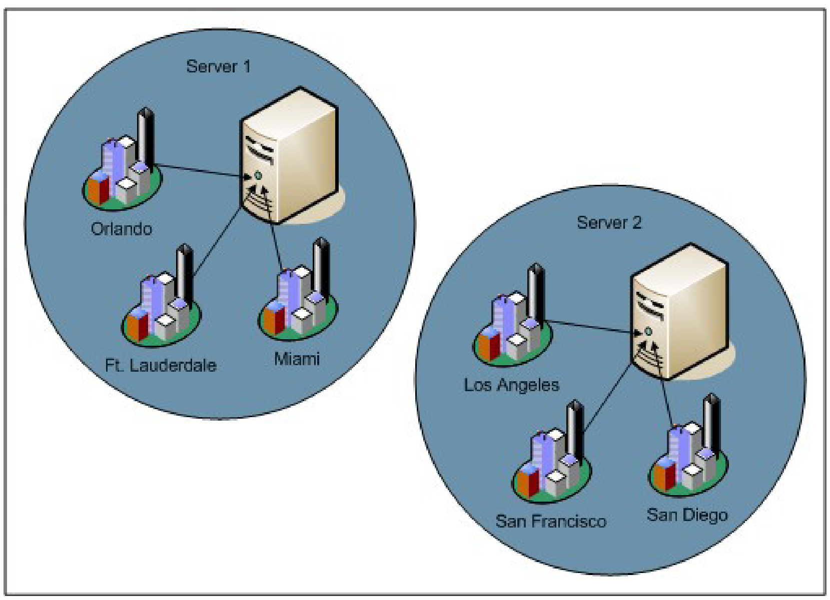


Figure 8: Regional Deployment

Connection to multiple PointCentral servers is not available. The setup assumes the need to run reports across accelerated folders from different servers is not required. A process can be created to transfer data from all PointCentral databases into a centralized database using the SQL Server replication.

Branch Deployment

Organizations might want to set up one server per branch. This configuration provides lower bandwidth requirements such as:

- Faster responses
- Increased flexibility in reporting through the SQL server database

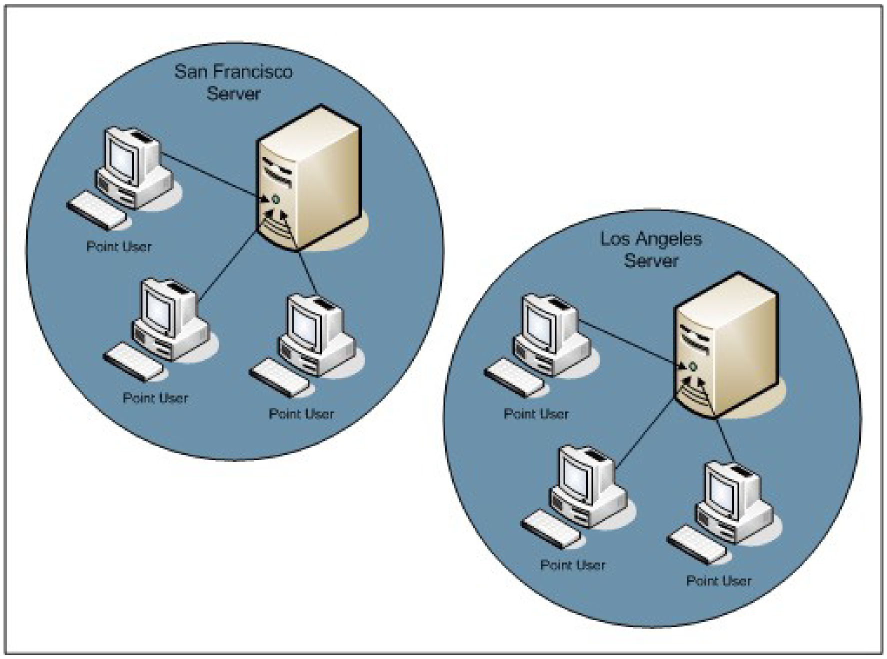


Figure 9: Branch Deployment

Fault Tolerance

SQL Server Backup

Make frequent data backups including the SQL Server data and transaction logs using a warm backup SQL Server that implements SQL Server replication. Switch to the hot backup to minimize downtime if the primary SQL Server fails.

Note: See Microsoft documentation for details about SQL Server replication.

Data Folder Backup

Make frequent data folder backups. Create a process for copying data folders to different PointCentral server created as the hot backup. Install PointCentral on the server, but do not run FileSync until required. Switch to the hot backup to minimize downtime if the primary system fails.

Directories in the warm backup server must match directories used in the live production environment. Accomplish the matched directories by implementing a warm backup server with both SQL Server replication and the method for copying loan and template files.

Increase reliability by using fault tolerant disk configurations such as Redundant Array of Independent (RAID).

The following table describes the RAID levels.

Table 4: RAID Levels

Level	Title	Description
0	Striped disk array without fault tolerance	Provides data striping (spreading out blocks of each file across multiple disk drives) without redundancy. This improves performance but does not deliver fault tolerance. If one drive fails, then all data in the array is lost
1	Mirroring and Duplexing	Provides disk mirroring. Provides twice the read transaction rate of single disks and the same write transaction rate as single disks
2	Error-Correcting Coding	Stripes data at the bit level rather than the block level **Note:** Not a typically used.
3	Bit-Interleaved Parity	Provides byte-level striping with a dedicated parity disk. **Note:** Level 3 cannot service simultaneous multiple requests and is rarely used.
4	Dedicated Parity Drive	Common implementation of RAID Provides block-level striping with a parity disk. Parity data is used to create a replacement disk if a data disk fails. **Note:** Disadvantage is the parity disk can create write bottlenecks.
5	Block Interleaved Distributed Parity	Provides data striping at the byte level and stripe error correction information. Results in excellent performance and good fault tolerance **Note:** Level 5 is one of the most popular RAID implementations.

Level	Title	Description
6	Independent Data Disks with Double Parity	Provides block-level striping with parity data distributed across all disks
0+, 1	A Mirror of Stripes	Creates two RAID 0 stripes and a RAID one mirror is created on top. Used for both replicating and sharing data among disks
10	A Stripe of Mirrors	Creates multiple RAID one mirrors and a RAID 0 stripe is created on top.
7	N/A	Trademark of Storage Computer Corporation that adds caching to Levels 3 or 4.

SSL Certificate Backup

Back up the SSL certificate in IIS for PointCentral with the **Private Key** exported to a safe place. SSL certificate cannot be restored to IIS without the **Private Key**.

Point clients cannot use PointCentral because the valid SSL certificate enables the secure connection between Point and PointCentral if the SSL certificate expires or becomes invalid.

Operating Requirements

The environment must meet the minimum system requirements before installing PointCentral. Several prerequisites must be met before installation.

System Requirements

The following hardware is required to support PointCentral.

Table 5: System Requirements

Component	Requirement
Processor	1.4 GHz, 64-bit processor or equivalent processing power.
Memory	1GB of RAM (2GB recommended).
Disk Space	• 20GB of available hard disk space (depends on Point data folders configuration). • Electronic document storage: 20MB per loan file (on average).

Software Requirements

The following software is required to support PointCentral.

Table 6: Software Requirements

Component	Version
Operating System	• Microsoft Windows Server® 2022, with latest service pack, IIS • Microsoft Windows Server® 2019, with latest service pack, IIS • Microsoft Windows Server® 2016, with latest service pack, IIS • Microsoft Windows Server 2012, with IIS and Application Server Role* **Note:** Calyx does not support the operation of PointCentral on a domain controller or exchange server. Calyx supports PointCentral only with Windows Server Standard, Data Center, or Enterprise editions. Calyx does not support the operation of PointCentral on Microsoft Windows Essentials for 2012.
Microsoft .NET Framework®	Version 4.8
SQL Server	
Large organizations (>50 Users)	• Microsoft SQL Server® 2019 Standard or Enterprise Edition, with latest service pack • Microsoft SQL Server® 2016 Standard or Enterprise Edition, with latest service pack • Microsoft SQL Server® 2014 Standard or Enterprise Edition, with latest service pack
Small organizations (<50 Users)	• Microsoft SQL Server® 2019 Standard or Enterprise Edition, with latest service pack • Microsoft SQL Server® 2016 Express Edition, with latest service pack • Microsoft SQL Server® 2014 Express Edition, with latest service pack

Component	Version
Network Environment	• Domain name • SSL certificate that matches the domain name installed on the IIS default web site. • Static IP address

Additional Requirements

Calyx does not directly support third-party products, including:

- Microsoft .NET Framework
- Internet Information Services (IIS), SQL Server
- SQL Server Express
- Other applications mentioned in this information.

Calyx does not recommend or support the operation of PointCentral on a domain controller or exchange server.

Calyx does not support the operation of PointCentral on Microsoft Windows Essentials.

The Calyx Resolver System can provide a Calyx-hosted domain name.

Chapter 2 – Installation Prerequisites

IMPORTANT! Perform the installation and setup in the following sequence to ensure proper installation and configuration.

Contact the System Administrator to properly set up the IP address. Set up the network to have a fixed external/public IP address available for the server. Use Calyx Resolver to provide a host name and DNS hosting. Review information about SQL log file sizing before beginning the installation.

Note: Calyx Software does not directly support third party products.

Refer to Calyx Resolver for Calyx Resolver details.

Refer to the Microsoft *Shrinking the Transaction Log* article for more information about log file sizing.

IIS Manager

IIS Manager is required to run PointCentral.

Determine IIS Manager Installation

PointCentral requires an IIS installation and specific server roles to be installed prior to the PointCentral install.

IIS hosts the following three components:

- Administration site
- web service
- Calyx Resolver

Select **Administrative Tools** from the **Start** menu to determine if the IIS Manager is already installed. Proceed to Delete Components/Applications.

Install IIS Manager

Administrative privileges on the server are required to install IIS.

Initiate Installation

Use the following steps to install IIS and required server roles.

1. Access the *Windows Start* screen.
2. Select **Server Manager** from the **Windows** taskbar.

3. Select **Add Roles and Features** from the **Manage** menu.

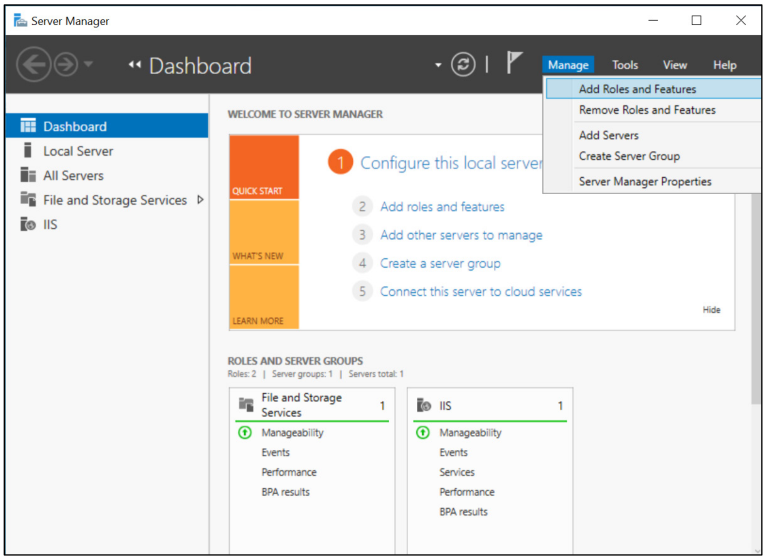


Figure 10: Server Manager Dashboard

4. Verify the destination server and network environment are prepared for the role and feature to install.

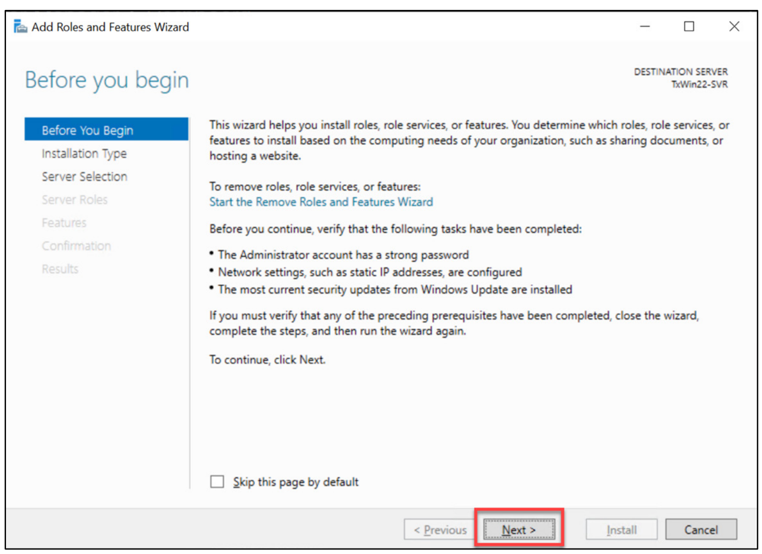


Figure 11: Add Roles and Features Wizard

5. Click **Next**.

6. Select the appropriate radio button to install components for roles or features on a single server.

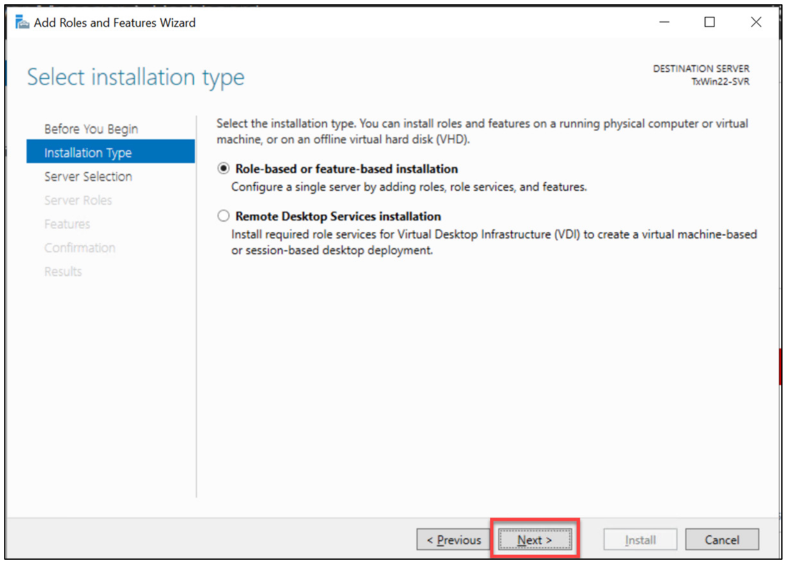


Figure 12: Select Installation Type

7. Click **Next**.
8. Select a server from the **Server Pool**.

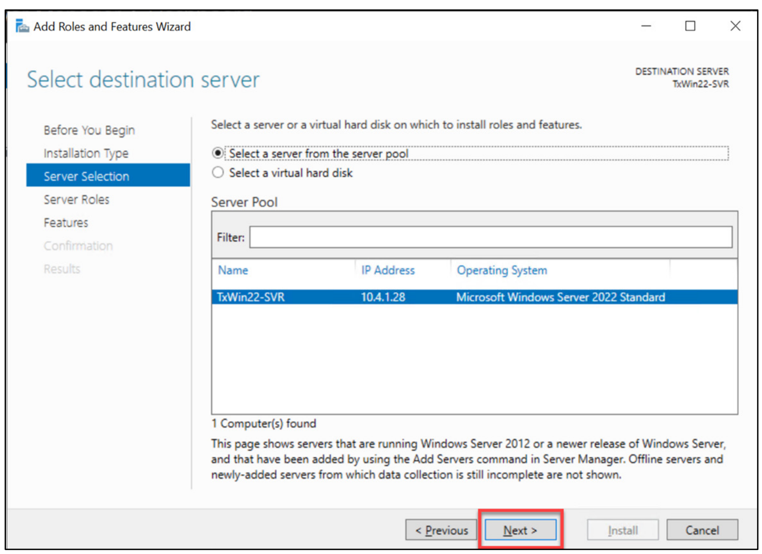


Figure 13: Select Destination server

9. Click **Next**.

10. Select **Application Server** and **Web Server (IIS)**.

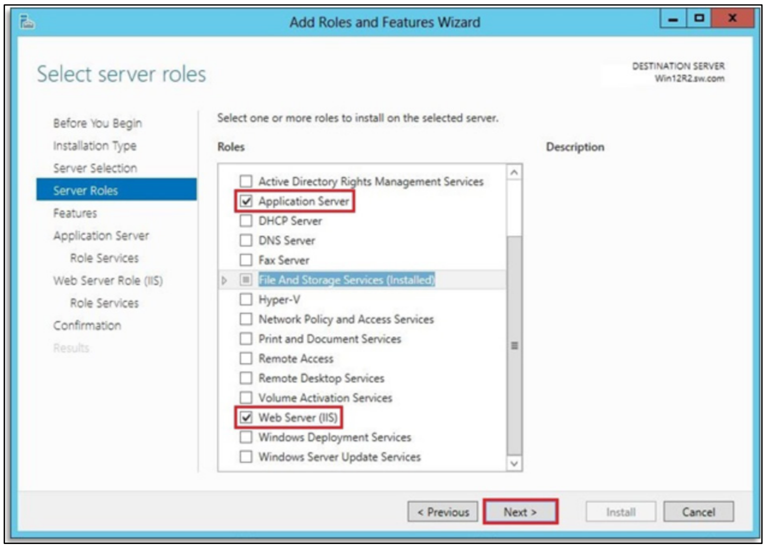


Figure 14: Select Server Roles

11. Click **Next**.

Add Features

Use the following steps to add features if prompted.

Note: Proceed to Complete IIS Manager Installation if the *Add IIS Features* dialog does not open.

1. Click **Add Features** to proceed.

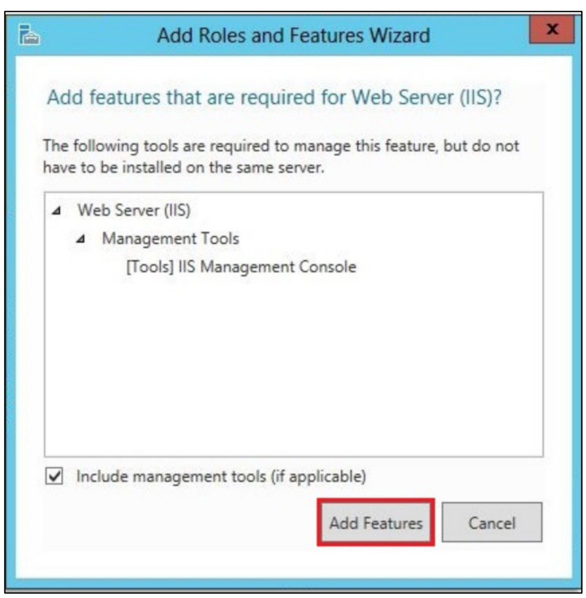


Figure 15: Add IIS Features

2. Select all *.NET Framework 3.5 Features* and required additional features.
3. Select all *.NET Framework 4.8 Features* and required additional features.

Note: Select features except **Named Pipe Activation** for *.NET Framework 4.5 Features*.

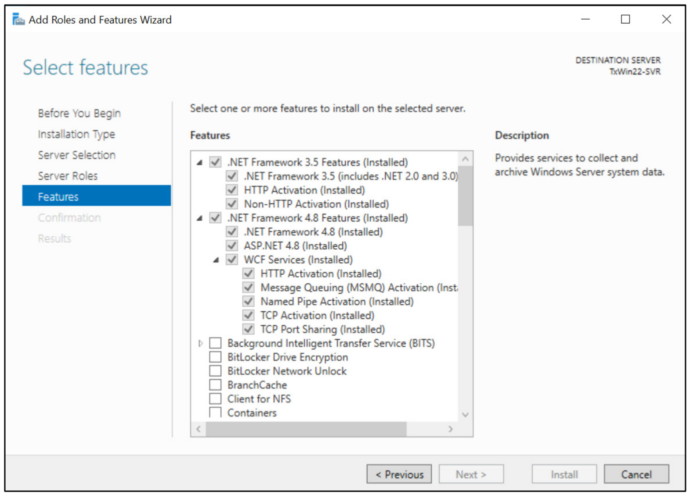


Figure 16: Select Features (.NET 4.8)

4. Click **Next**.
5. Click **Add Features** if a message displays to confirm the additional features.
6. Click **Next**.
7. Proceed to Complete IIS Manager Installation.

Complete IIS Manager Installation

Use the following steps to complete the IIS Manager installation.

1. Click **Next** to proceed to the *Role Services* dialog.

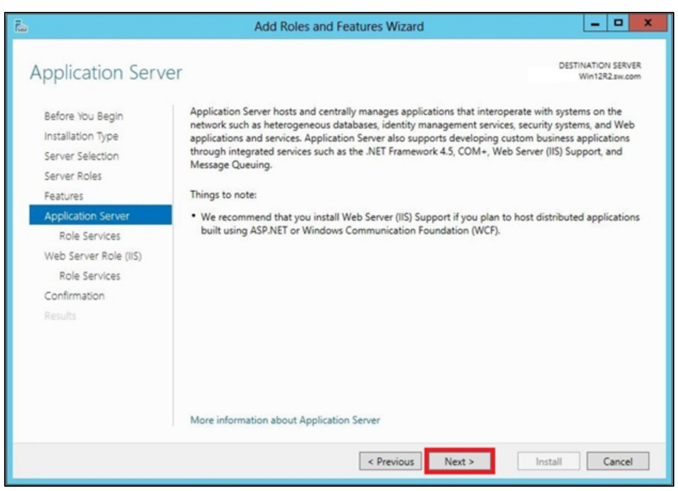


Figure 17: Application Server

2. Verify that .NET Framework 4.8 and Web Server (IIS) Support) are selected.

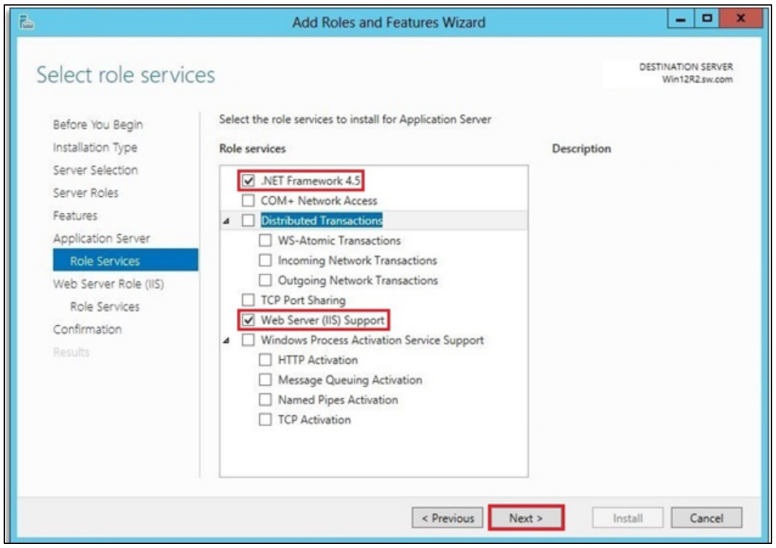


Figure 18: Select Role Services

3. Click **Add Features** if a message displays to confirm the additional features.
4. Click **Next**.

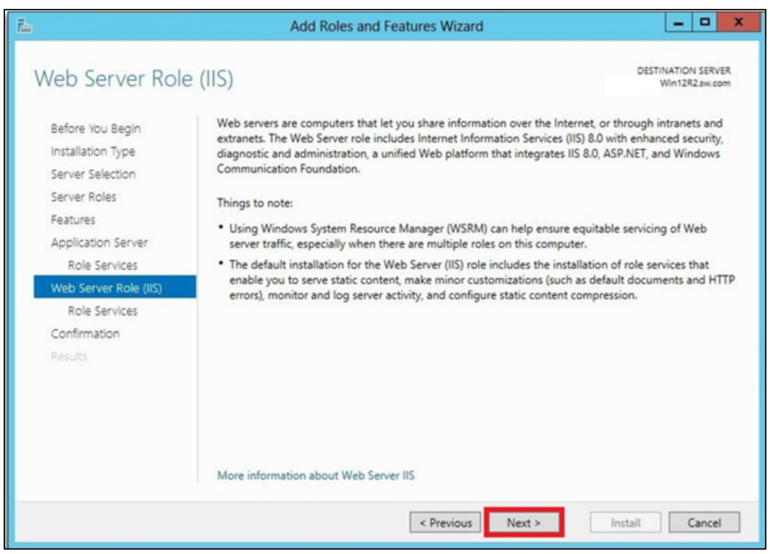


Figure 19: IIS Server Role

5. Save all default selections.

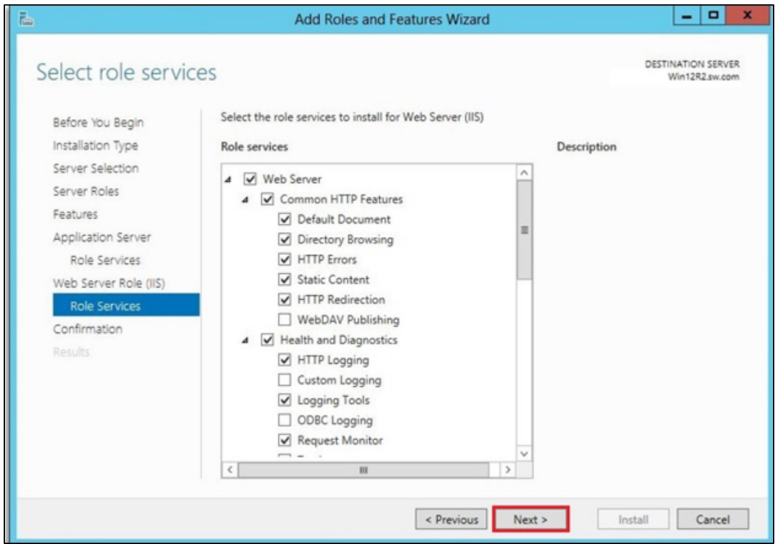


Figure 20: Role Services

6. Click **Next**.
7. Click **Install**.

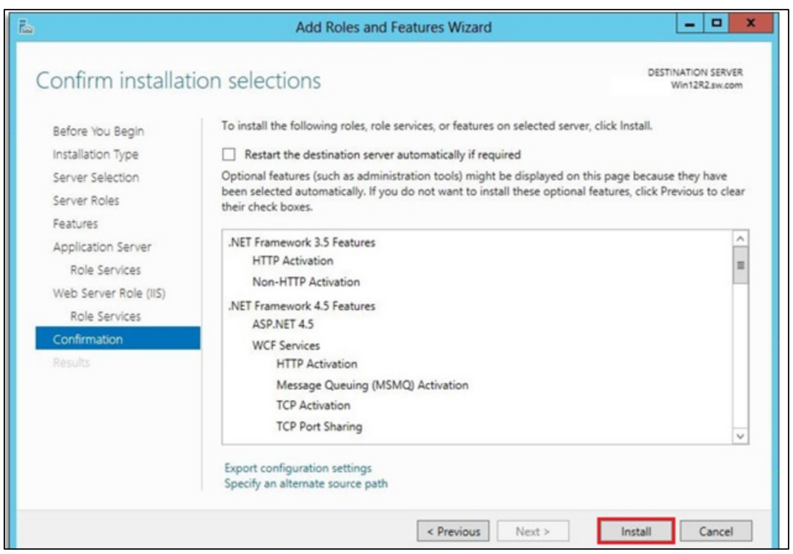


Figure 21: Confirm Installation Selections

8. Click **Close** when the **Installation Succeeded Message** displays.

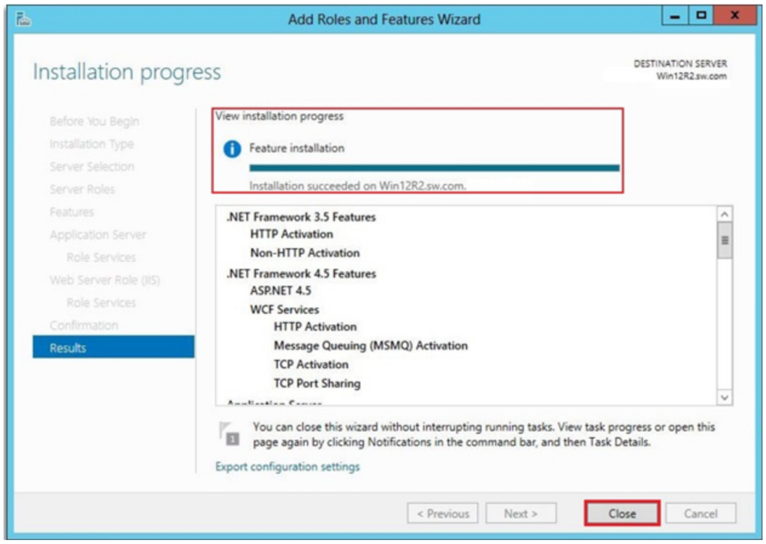


Figure 22: Installation Progress

Delete Components/Applications

The following components may be installed depending on the installation method and Windows version in addition to creating a default website during the IIS installation. Many IIS components/applications are not required. Stop or uninstall the components/applications if not required:

- Default FTP Site
- Administration Web Site
- Default SMTP Virtual Server
- Default NNTP Virtual Server
- FrontPage extensions

Install SQL Server

Microsoft SQL Server, Standard or Enterprise Edition (2012/2014/2016/2019) is recommended for organizations with 50 or more Point Users. Express Edition is recommended for organizations with fewer than 50 Point Users.

Note: Verify that the required .NET Framework version is installed before beginning the installation.

SQL Server Express Edition

Use the following sections to install SQL Server Express Edition.

SQL Server 2019 Express

1. Download the appropriate SQL Server Express Edition.
2. Launch the **.exe** file when the download is complete.
3. Select Installation.

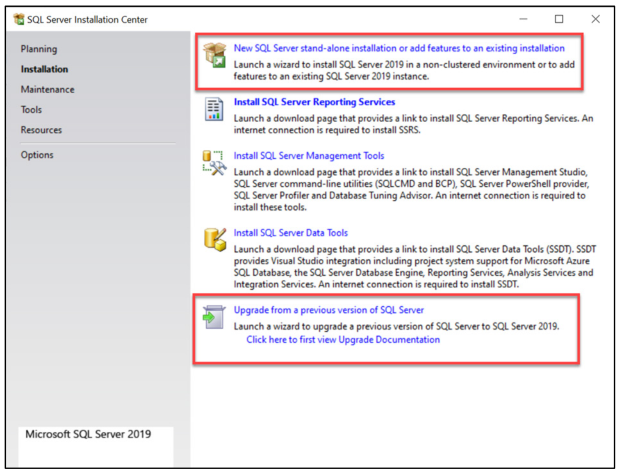


Figure 23: SQL Server Express Installation

4. Select New installation or Upgrade.
5. Select the **I accept the license terms** checkbox.

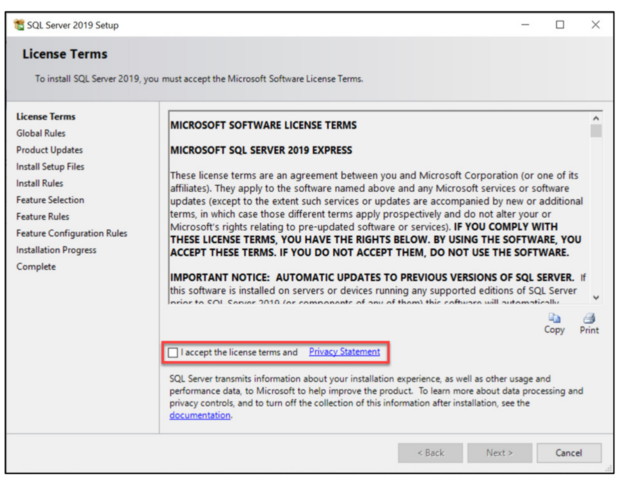


Figure 24: SQL Express License Terms

6. Click **Next**.

7. Click on the **Show details** button to view the details and resolve if any error checks have failed.
8. Click Re-run to run the check again after errors are resolved.
9. Repeat steps 7-8 until all errors are resolved.

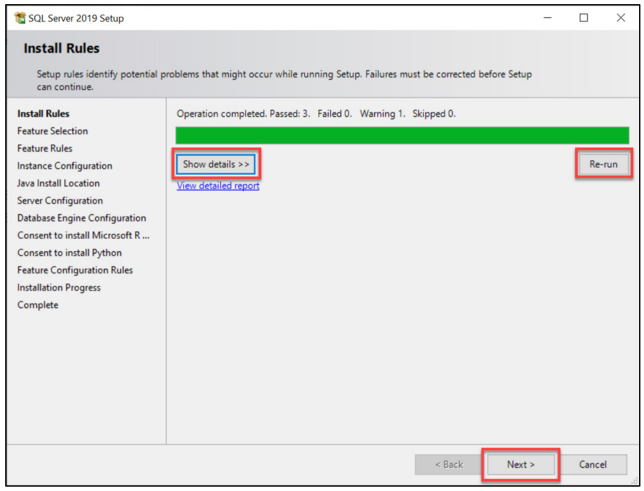


Figure 25: SQL Install Rules

10. Click **Next**.
11. Retain the default settings.

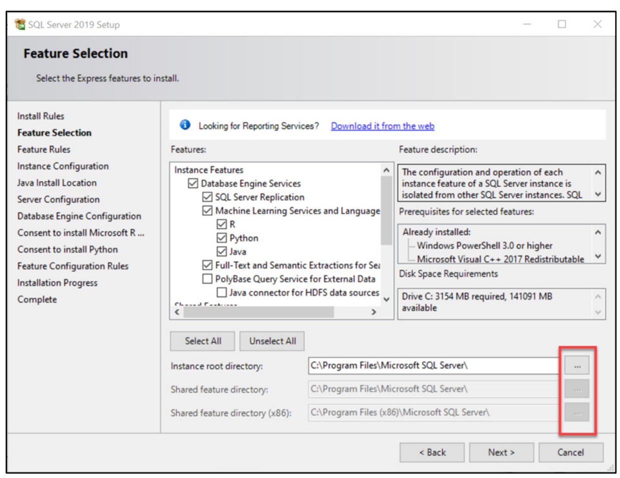


Figure 26: SQL Express Feature Selection

12. If needed, click on the **ellipse** to select a different directory.

Note: Machine Learning services, such as R, Java, and Python require consent before installation.

13. Click **Next**.

14. Rename the SQL instance in the **Named Instance** field to rename.

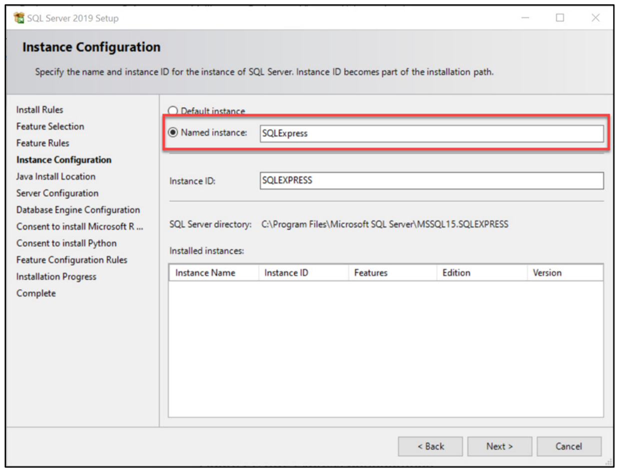


Figure 27: SQL Express Configuration

15. Click **Next**.
16. If using Java, select **Open JRE** or browse for a previous installation of JRE or JDK.
17. Click **Next**.
18. Select the appropriate **Account Name**.

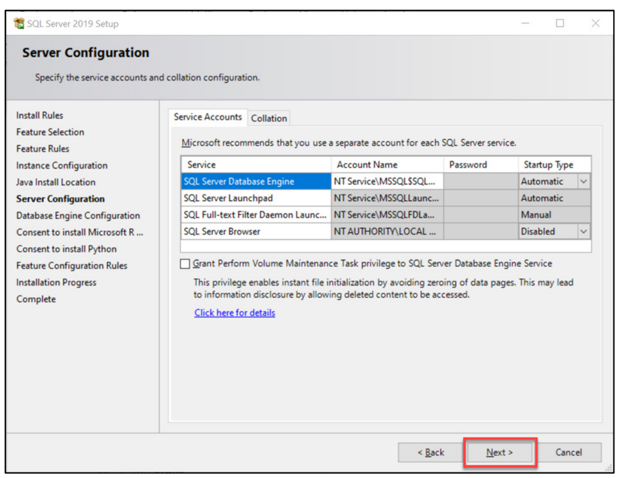


Figure 28: SQL Express Server Configuration

Note: Use the *Network Services* account to avoid issues with the installation.

19. Click **Next**.

20. Select the **Mixed Mode** radio button.

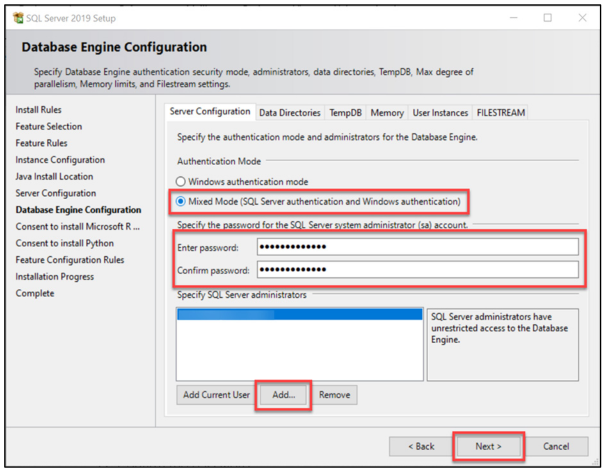


Figure 29: Configure SQL Express Database

21. Enter the password for the SQL Server system administrator account.
22. Confirm the password.
23. Select the **Windows NT** account that applies to the local machine.

Note: The account is typically the domain admin account.

24. Click **Next**.
25. If R and Python services were selected, click on the **Accept** button to install the services.
26. Click **Next** to complete the installation.

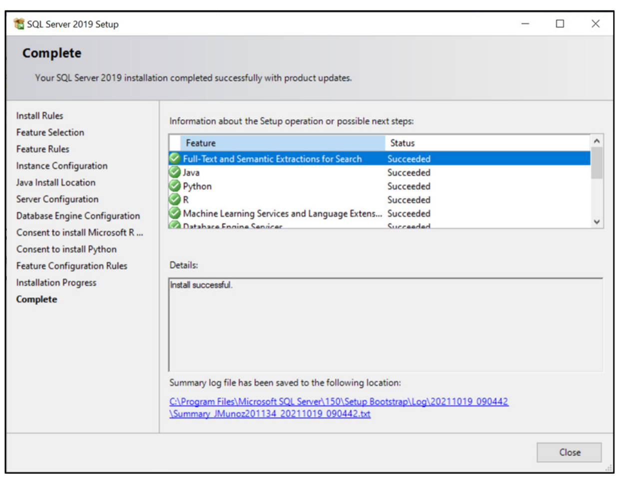


Figure 30: Installation Complete

SQL Server 2012, 2014, and 2016

The following installation is for SQL Server Express Edition 2012. 2014, and 2016. The screens may vary among the versions, but the steps are the same.

1. Download the appropriate *SQL Server Express Edition*.
2. Launch the **.exe** file when the download is complete.
3. Select **Installation**.

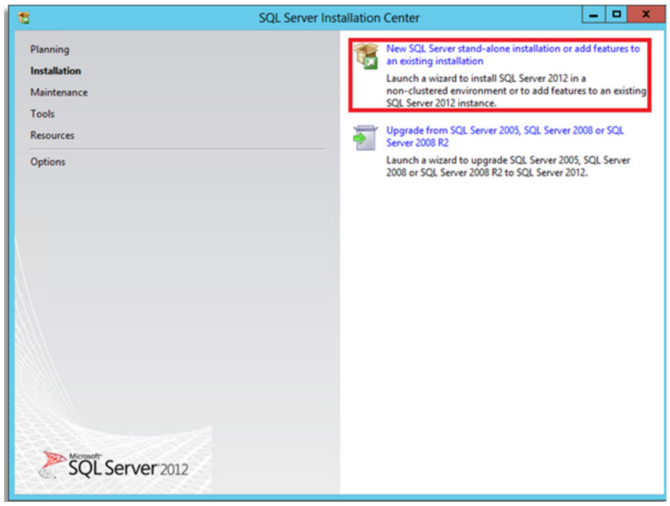


Figure 31: SQL Server Express Installation

4. Select New installation or Upgrade.
5. Select the I accept the license terms checkbox.

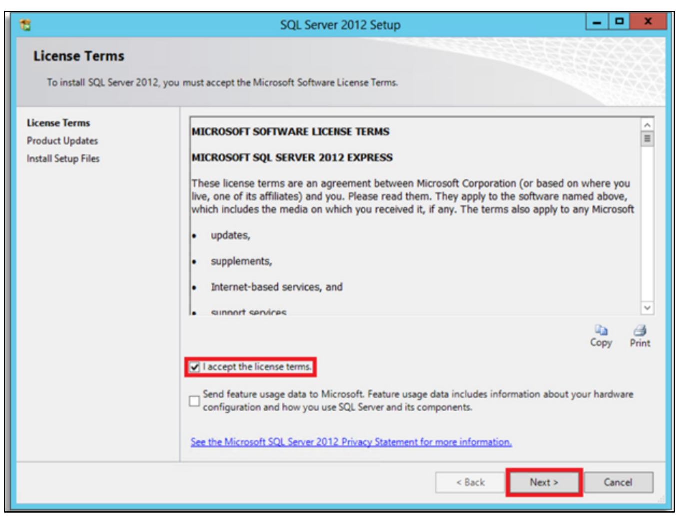


Figure 32: SQL Express License Terms

6. Select the **Send feature usage** checkbox to send information about SQL usage and components.

7. Click **Next**.
8. Click the **Show details** button to view the details and resolve if any error checks have failed.

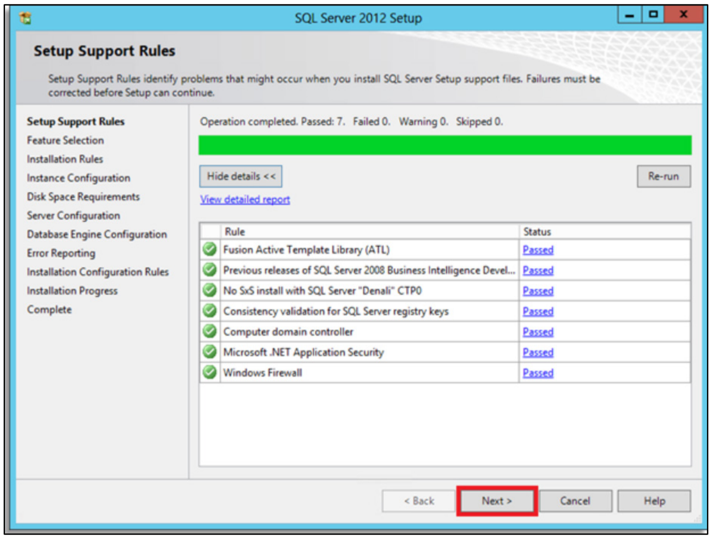


Figure 33: SQL Setup Support Rules

9. Click **Re-run** to run the check again after errors are resolved.
10. Repeat Steps 8 - 9 until all errors are resolved.
11. Click **Next**.

Complete Installation

1. Retain the default settings.

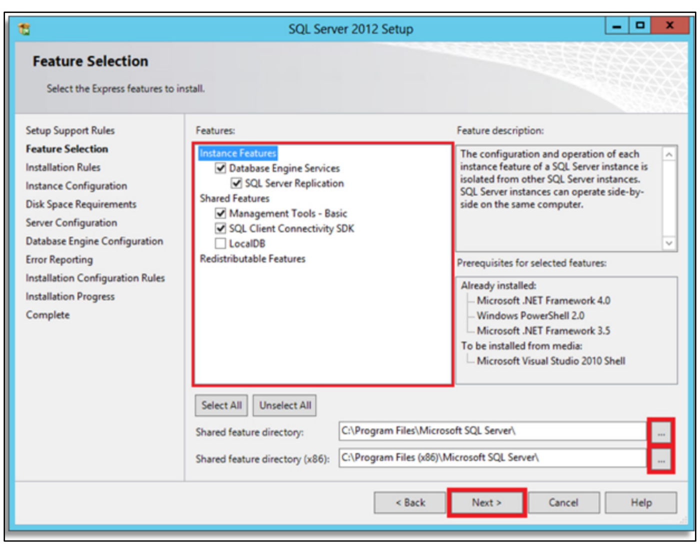


Figure 34: SQL Express Feature Selection

2. Use the **Browse** button to change the *Shared Feature Directory*.
3. Click **Next**.
4. Rename the SQL instance in the **Named Instance** field to rename.

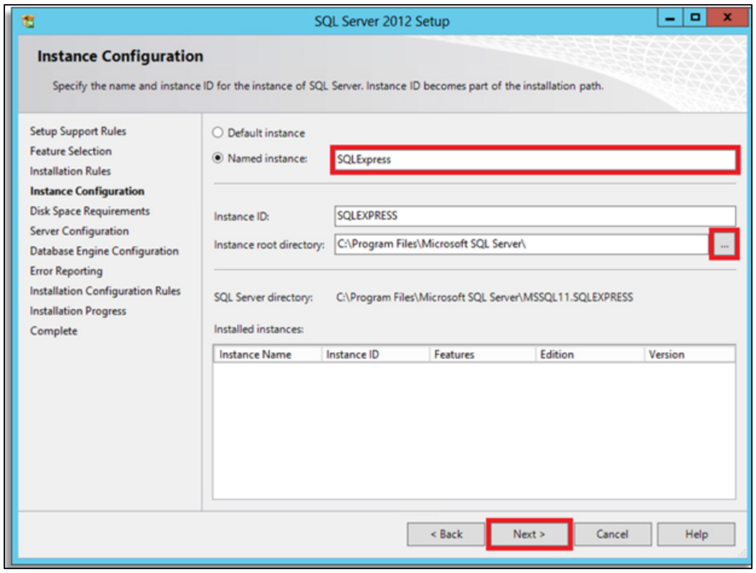


Figure 35: SQL Express Configuration

5. Use the **Browse** button to change the *Instance Root Directory*.
6. Click **Next**.
7. Select the appropriate **Account Name**.

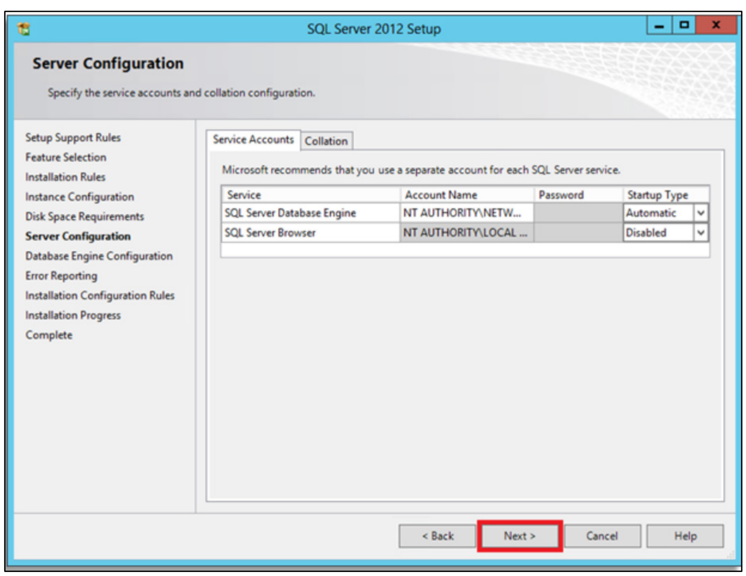


Figure 36: SQL Express Server Configuration

Note: Use the *Network Services* account to avoid issues with the installation.

8. Click **Next**.
9. Select the **Mixed Mode** radio button.

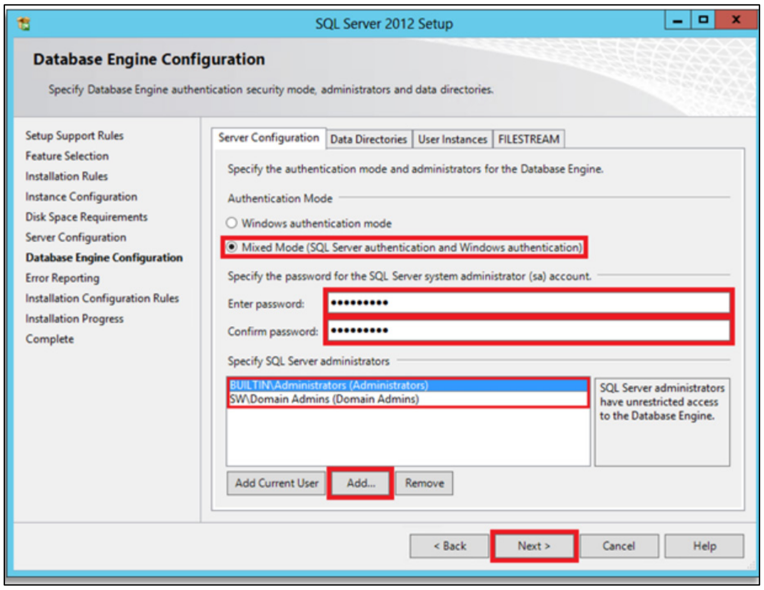


Figure 37: Database Engine Configuration

10. Enter the password for the SQL Server system administrator account.
11. Confirm the password.
12. Select the **Windows NT** account that applies to the local machine.

Note: The account is typically the domain admin account.

13. Select the checkbox to enable sending error reports to Microsoft.

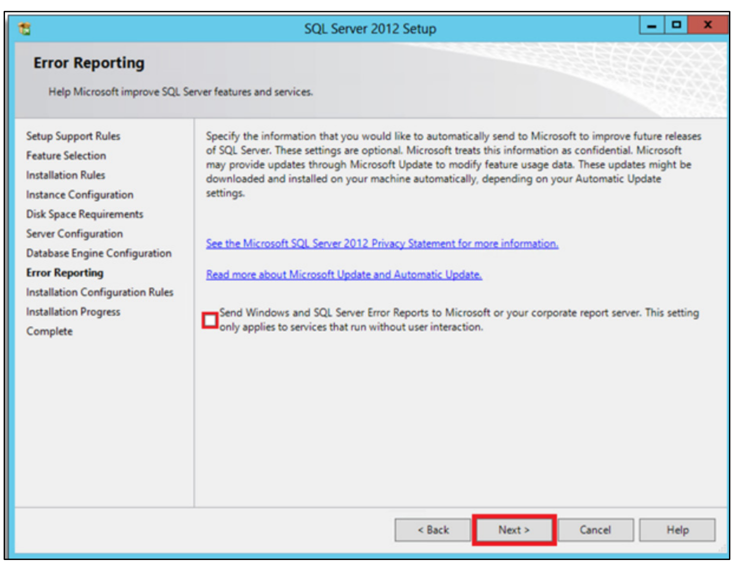


Figure 38: SQL Express Error Reporting

14. Click **Next** to start the installation.
15. Click **Close** when installation is complete.

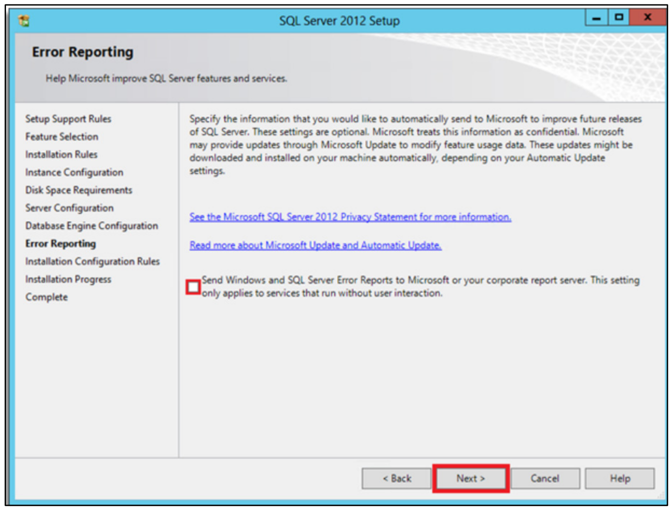


Figure 39: SQL Express Error Reporting

16. Click **Next** to start the installation.
17. Click **Close** when installation is complete.

SQL Server Express Management Tools

Install the **SQL Server Management Tools** for when electing to install the SQL Server Express version.

1. Launch the **.exe** file you downloaded from the Microsoft website or from MyCalyx.com.
2. Select **Install SQL Server Management Tools**.

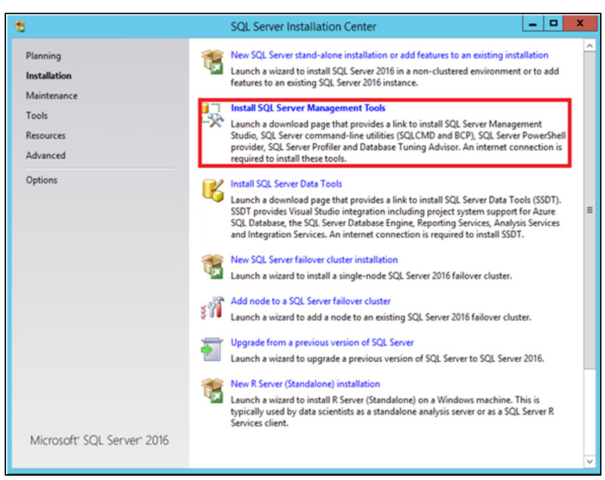


Figure 40: SQL Server Installation Center

3. Select the **SSMS Download** link.

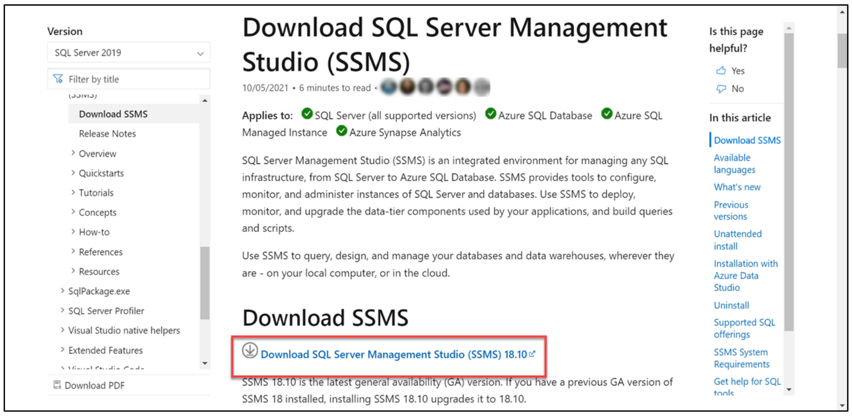


Figure 41: SSMS Download Screen

4. Select **Install** on the *Welcome* screen.

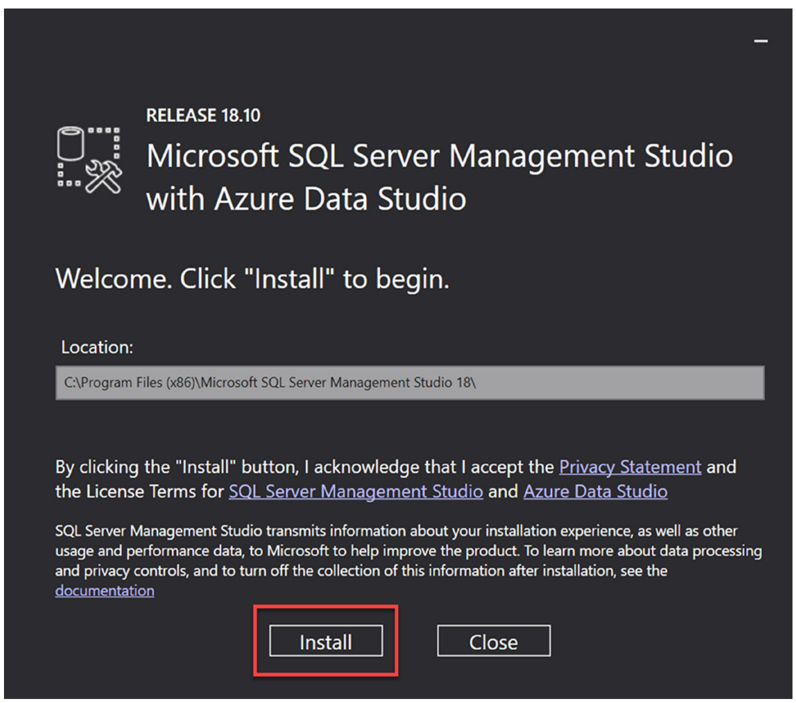


Figure 42: Installation Welcome Screen

5. Click **Close** when installation is complete.

Remove Directories

The InstallShield Wizard creates the following three virtual directories at the IIS root default website during the PointCentral:

- **Virtual Directory Admin:** Points to the administration site installation directory

- **Virtual Directory Service:** Points to the web service installation directory
- **Virtual Directory Resolver:** Points to the Resolver service installation directory

Note: Remove the virtual directories and re-install PointCentral or manually create IIS websites and virtual directories that point to the administration site and web service if the virtual directories admin, service, or Filesync are at the default website.

Refer Chapter 2 – Installation for information about the virtual directories during installation.

Note: Refer to Microsoft documentation for information about how to install and configure IIS.

Domain Name Setup

Preparing your domain to resolve the PointCentral to search, open, or save loans entails the following actions when Calyx Resolver is not used to obtain your domain name.

- Acquiring and registering a domain name.
- Configuring a domain name server.
- Acquiring an SSL certificate.

The network may require setting up a fixed external/public IP address available for the server.

Calyx Resolver

Calyx Resolver is provided by Calyx Software to obtain the following services:

- **Hostname:** Calyx provides up to five hostnames per account ID for the server in the form *.calyxpds.com.
- **DNS Hosting:** All DNS queries for the Calyx-provided hostname are resolved to the IP address.

Calyx Resolver is set up using the PointCentral Configuration Wizard. The machine must have a static private or public IP address.

Continue to use the existing domain name and SSL certificate rather than using Calyx Resolver to set them up if preferred. Switch to Calyx Resolver at any time.

Note: Calyx Resolver is a free service when the PointCentral subscription is up to date.

Configure DNS

Configure the domain name to the correct IP address after purchase when a Point client attempts to access it.

SSL Certificate

All data sent between the Point client and PointCentral is encrypted for security. Install a **Secure Sockets Layer (SSL)** certificate on the IIS server that hosts the administration and web service sites to ensure the data is properly encrypted.

Use the following steps to install and configure the SSL certificate on the PointCentral website:

1. Create the **SSL Certificate Request**.
2. Purchase the **SSL Certificate**.
3. Configure the **SSL Certificate**.
4. Install the **SSL Certificate**.

Chapter 3 - PointCentral Installation

Install PointCentral when all the software and pre-installation requirements are complete.

Make a backup of the data when upgrading the database in the event a restore is required. The installation process supports the installation of new systems and upgrades of systems that run PDS version 10.5 and later (earlier versions not supported).

Administrative privileges are required to install PointCentral to complete installation. Access to the installation executable is through MyCalyx.

Use the following steps to install PointCentral.

Install PointCentral

Use the following steps to install PointCentral.

1. Log in to www.mycalyx.com from the **PointCentral** server.
2. Click **Download Server Software**.
3. Select the latest version.
4. Click **Download**.
5. Click the **Install** or **Upgrade** PointCentral link.
6. Select **Run/Save** on the **Installation** file.
7. Click **Next** on the InstallShield Wizard**.**

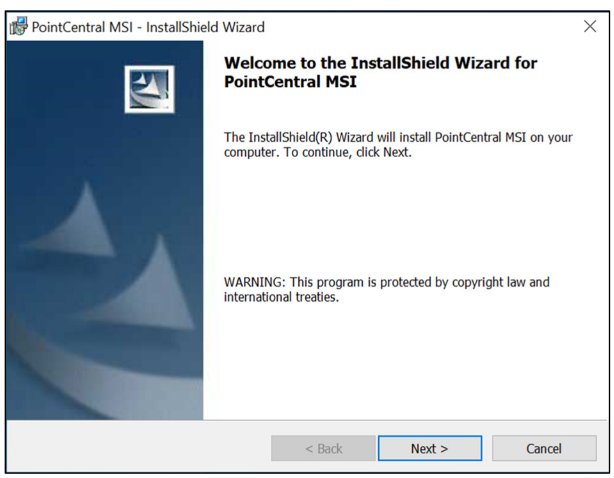


Figure 43: InstallShield Wizard Welcome

8. Read the Software **License Agreement**.

Figure 44: License Agreement

9. Select **I accept the terms in the license agreement**.
10. Click **Next**.

Note: The InstallShield Wizard sets the destination folder to C:\Program Files (x86)\Calyx Software\PointCentral as the root folder path. Upgrades will show in the previous install location.

11. Click **Change** to select another destination folder.

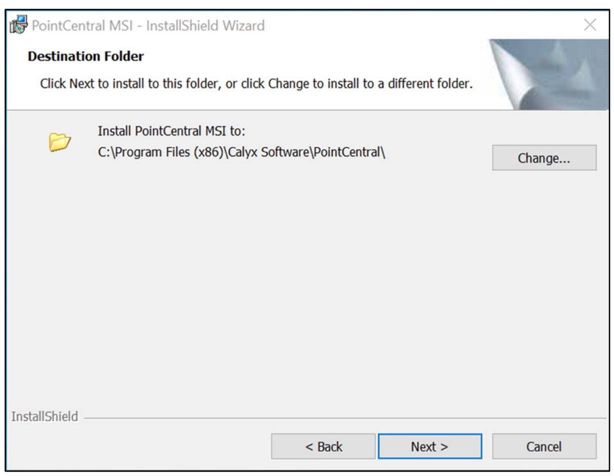


Figure 45: Destination Folder

Note: Select a path with sufficient disk space to accommodate future data folder growth.

12. Click **Next**.

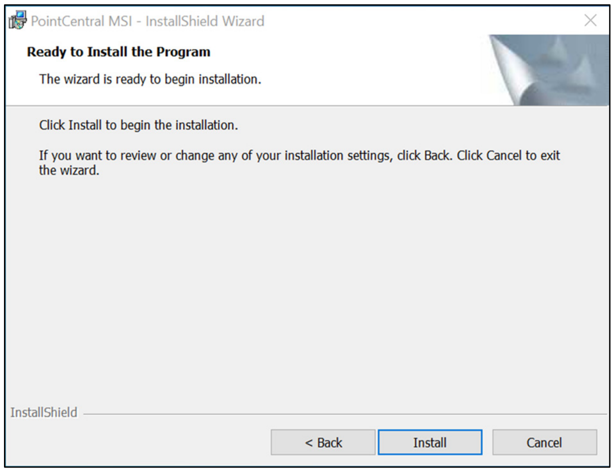


Figure 46: Ready to Install

13. Click **Install**.
14. Click **Finish**.

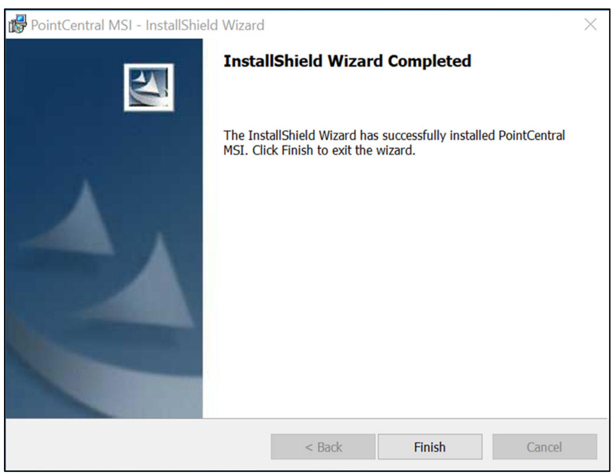


Figure 47: Installation Confirmation

15. Restart the server if prompted.
16. Proceed to Configure PointCentral.

Configure PointCentral

Configure the database after installing PointCentral. The PointCentral Configuration Wizard automates the configuration and performs the following actions:

- Creates the SQL database for new installations.
- Upgrades your SQL database when installing an upgrade.

- Verifies the integrity of your database for previously installed or upgraded databases.

Use the PointCentral Configuration Wizard to set up connections from PointCentral components to PointCentral database.

Obtain the following information before proceeding:

- Domain name
- DNS
- SSL certificate

The PointCentral Configuration Wizard creates new tables and alters the schema of existing tables during an upgrade. The Wizard retains any unchanged data.

The PointCentral Configuration Wizard stops the **FileSync Windows** service prior to installation to prevent PointCentral application access. FileSync stops unwanted errors from being added to the Windows Event Log.

The PointCentral Configuration Wizard places the web service in Upgrade mode while the database upgrades. A message displays to Point Users indicating the Point access has failed when Users attempt to access Point during the upgrade.

Initiate PointCentral Configuration

Launch the PointCentral Configuration Wizard from **C:\Program Files (x86) \Calyx Software\PointCentral\PdsDbCreate.exe** as an administrator if the Wizard does not launch automatically.

Note: Check behind other dialogs if the PointCentral Configuration Wizard is not visible.

1. Select **C:\Program Files (x86) \Calyx Software\PointCentral**.
2. Double-click **PdsDbCreate.exe**.
3. Enter **Company Name** and Calyx **Account ID**.

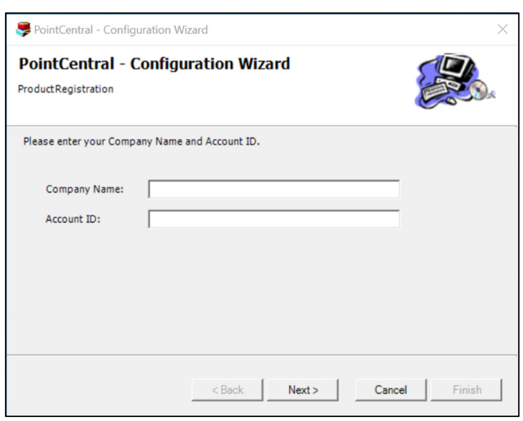


Figure 48: Product Registration

4. Click **Next**.
5. Select the appropriate **SQL Server** radio button.

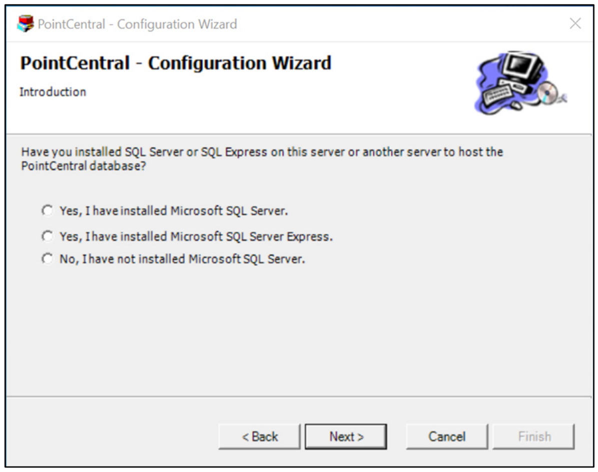


Figure 49: Specify SQL Version

6. Click **Next**.

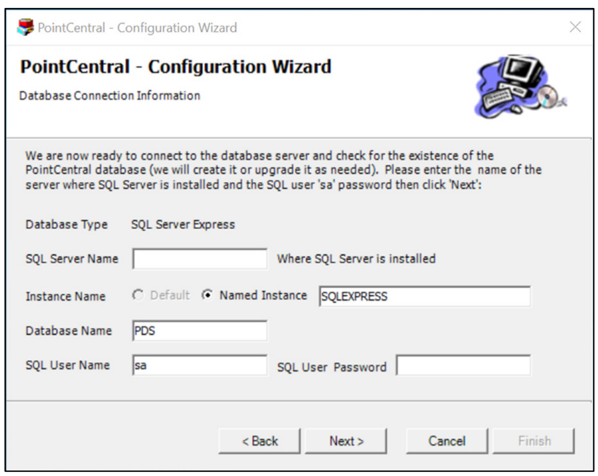


Figure 50: Database Connection Information

Note: The *Database Type* is populated with the server selected on the *Introduction* dialog. (See Figure 91.)

7. Complete the *Database Connection Information* dialog.
8. Enter the server name where Microsoft SQL Server is installed in the **SQL Server Name** field to change the default.
9. Enter the **Database Name** field.
10. Enter the Microsoft SQL Server **User Password**.
11. Click **Next**.

12. Click **Next** on the *Database Upgrade or Creation* dialog to accept the default directory.

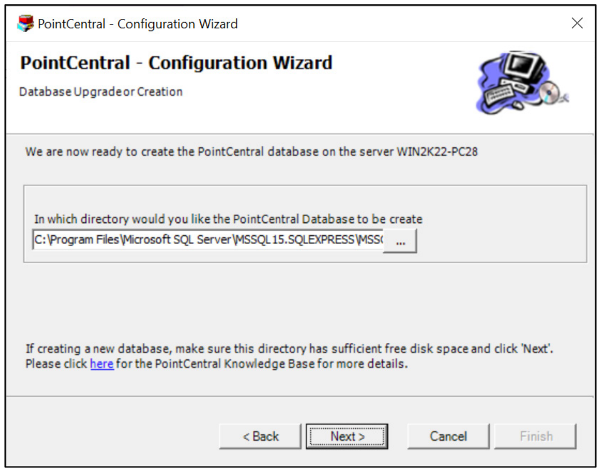


Figure 51: Database Upgrade or Creation

Note: Navigate to the directory to create and store the database files to store in a different location. The default path for remote database creation is used on the remote server (the default path is taken from the data files path for the master database) when creating a database for the first time and SQL Server is on a different server from PointCentral. Use database management tools to move the server from the default directory to a different directory on the remote server when required. The dialog is slightly different when upgrading.

13. Click **Next** to verify the database. For information about database connection issues or about the DNS/SSL certificate, click on the desired link below.

    [Troubleshoot Database Connection]

    [DNS/SSL Certificate Provider]

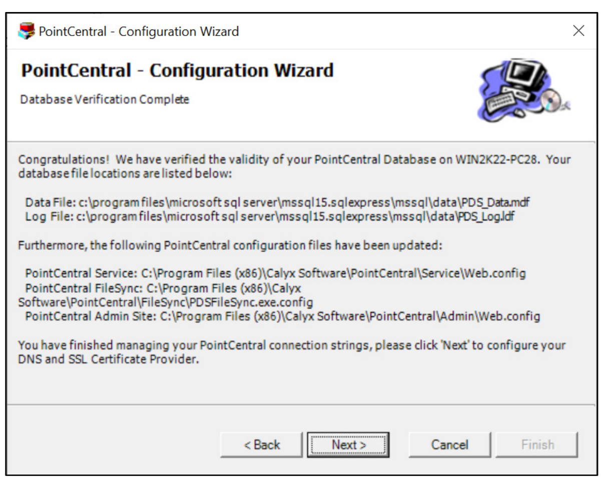


Figure 52: Database Verification

Troubleshoot Database Connection

Check the following if the PointCentral Configuration Wizard is not able to connect to the database.

1. Verify one of the supported **Microsoft SQL Servers** is installed.
2. Verify that **Microsoft SQL Server** is running.
3. Verify that the correct password was entered and matches the password that was defined when **SQL Server** was installed.
4. Verify the correct protocols are enabled for your instance of SQL Server.
5. Click **Next**.
6. Proceed to DNS/SSL Certificate Provider.

DNS/SSL Certificate Provider

The locations of the SQL Server database underlying files and the updated configuration files display one *Database Verification Complete* dialog displays when database configuration is successful.

Note: The paths **C:\Program Files\Microsoft SQL Server\MSSQL\Data** and **C:\Program Files (x86)\Calyx Software\PointCentral** may vary depending on the environment. The current default location for PointCentral is C:\ProgramFiles (x86)\CalyxSoftware\PointCentral.

The PointCentral Configuration Wizard begins FileSync and takes the web service out of Upgrade mode. The *DNS, SSL Certificate Provider* dialog displays when the Wizard is ready to continue.

1. Select the appropriate **DNS and SSL Certificate Provider** radio button.

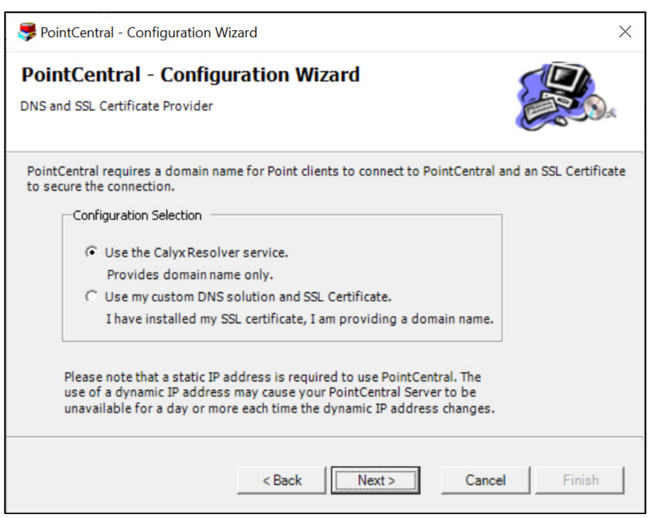


Figure 53: DNS and SSL Certificate Provider

2. Click **Next**.

Note: Click *Finish* when the *Finish* dialog is displayed if you selected to *Use my custom DNS solution and SSL Certificate*.

3. Select the **Change Calyx Resolver Registration** checkbox if applicable to change any network settings.

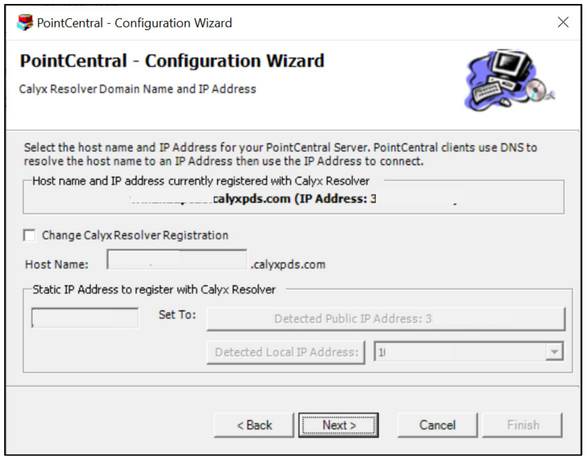


Figure 54: Calyx Resolver Domain Name & IP

4. Enter a **Host Name**.

Note: The host name becomes part of the Service and Admin URLs used to connect to PointCentral.

5. Enter the server **Static IP Address** to enable server over the Internet.

Note: Click the **Detected Local IP Address** button to automatically populate the field with your current local **IP** address to only enable within the local network.

6. Click **Next**.

7. Click **Next** on the Calyx Resolver Name and IP Address Confirmation dialog.

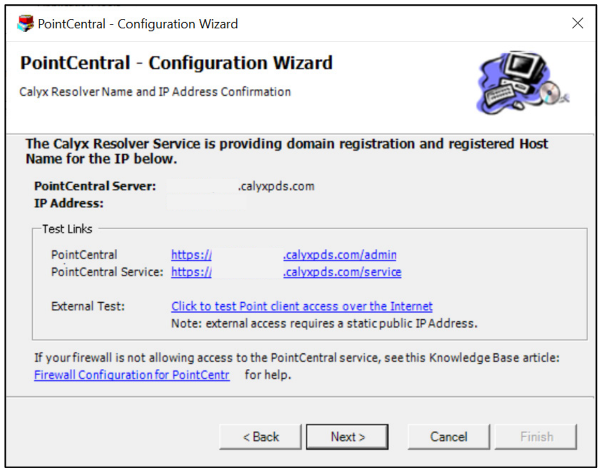


Figure 55: Confirm Calyx Resolver Name & IP

8. Click **Finish**.

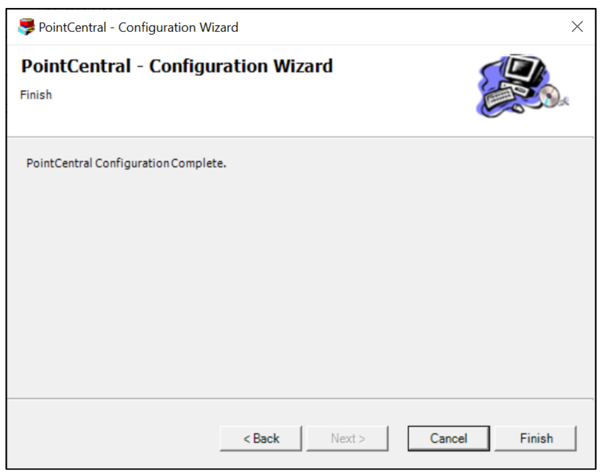


Figure 56: Configuration Complete

Reconfigure PointCentral

Run the PointCentral Configuration Wizard if system changes occur in the future. The Wizard performs the following during the reconfiguration:

- Updates database connection information
- Resets NTFS permissions
- Configures Calyx Resolver

Refer to the PointCentral Knowledge Base for additional troubleshooting information.

[Training | Calyx Customer Portal | Calyx Software]

Uninstall PointCentral

Reverse the configuration that was completed during installation to uninstall.

Reset IIS, FileSync, & SQL Server

Ensure there are no open connections to the database before you delete the database.

Note: Administrator privileges are required to perform these actions.

1. Open a command prompt dialog in **Microsoft Windows** to stop **IIS**.
2. Enter **iisreset /Stop**.
3. Press **Enter**.
4. Access **Administrative Tools** from the **Start** menu to Stop FileSync.
5. Double-click **Services**.
6. Double-click **CalyxPdsFileSync** to open the *CalyxPdsFileSync Properties* dialog box.

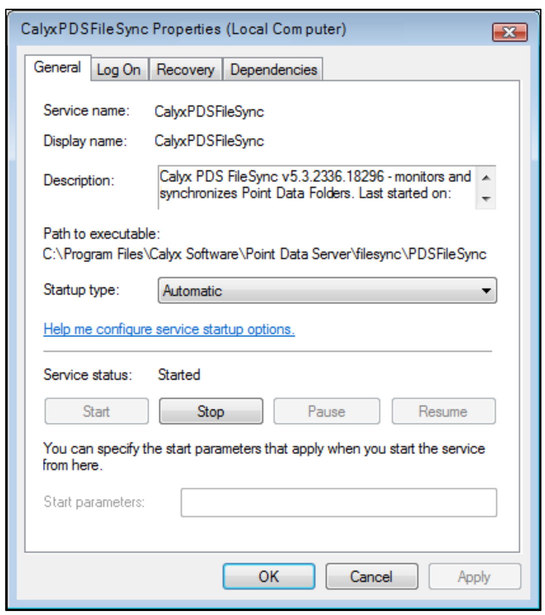


Figure 57: CalyxPDSFileSync Properties

7. Click **Stop**.
8. Click **OK** to close the dialog.
9. Stop and restart **SQL Server**.

Note: Type net stop **CalyxPdsFileSync** in the command prompt dialog to stop FileSync.

10. Open a command prompt dialog in **Microsoft Windows**.

11. Enter **net stop mssql$sqlexpress** if you are running SQL Express.
12. Press **Enter**.
13. Enter **net stop mssqlserver** if running SQL Server.
14. Click **Yes** If you are prompted to stop the **SQL SERVERAGENT** service.
15. Enter **net start** mssql$sqlexpress in the command prompt dialog if running SQL Express.
16. Press **Enter**.
17. Enter **net start mssqlserver** if running SQL Server.

Connections and locks to the SQL Server are reset and ready to delete the PointCentral database.

Delete PointCentral Database

These instructions refer to Microsoft SQL Server 2005 Management Studio Express.

The following is deleted when deleting PointCentral database:

- Users
- User groups
- Cardex databases
- Access rights that exist in the database

Use the following steps to delete a PointCentral database.

1. Open SQL Server Management Studio Express.
2. Expand the **Computer Name Node**.
3. Expand the **Databases** node.
4. Right-click the database name.
5. Select **Delete**.
6. Verify the **Delete backup and restore history information for databases** checkbox is selected.
7. Click **OK**.

Uninstall PointCentral

Uninstall the components after the database is deleted. The InstallShield Wizard contains an uninstall feature to reverse the actions performed during installation.

1. Click **Add** or **Remove** on the *Windows Control Panel*.
2. Select **PointCentral**.
3. Click **Remove**.
4. Click **Yes** on the *Confirmation* dialog.
5. Restart the computer.

Chapter 4 – PointCentral Setup

Configure PointCentral to accept incoming requests after installation.

Configuring PointCentral includes:

- Setting the operational parameters
- Configuring clients
- Setting site parameters
- FileSync parameters
- Service parameters

Note: Create a test environment to test your installation when possible. Create the test environment after completing the configuration steps in this topic.

Initial PointCentral Access

Add the *Administration* site to your **Trusted Sites Zone**. Microsoft Edge prompts with a content blocking message where the site can be added to the **Trusted Sites Zone**.

Create an Administrative User before configuring the following:

- Users
- User groups
- Data folders

Note: Internet Explorer is required to access the *Administration* site.

1. Select **PointCentral Administration** to open https://localhost/admin.

Note: A Security Alert message displays because localhost does not match the name on the SSL certificate.

2. Click **Yes** to proceed.

Note: The localhost resolves to the IP address to the local server.

3. Enter admin in the **Username** field.

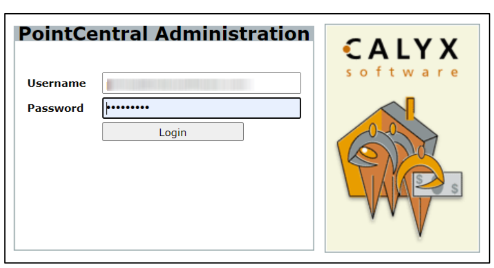


Figure 58: PointCentral Administration Login

4. Leave the **Password** field blank.
5. Click **Login** to display the *Release Notes* screen.
6. Click **Save**.
7. Select the **Do not show these Release Notes again at login** checkbox to prevent the *Release Notes* from displaying again at login.

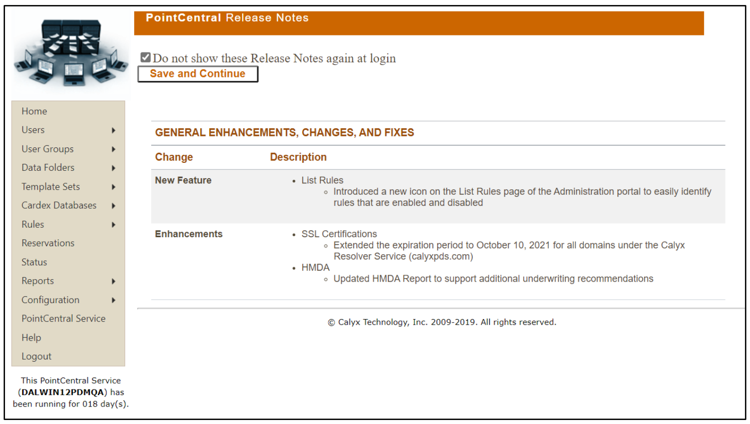


Figure 59: PointCentral Release Notes

8. Click **Save and Continue** to proceed to the *Home* page.

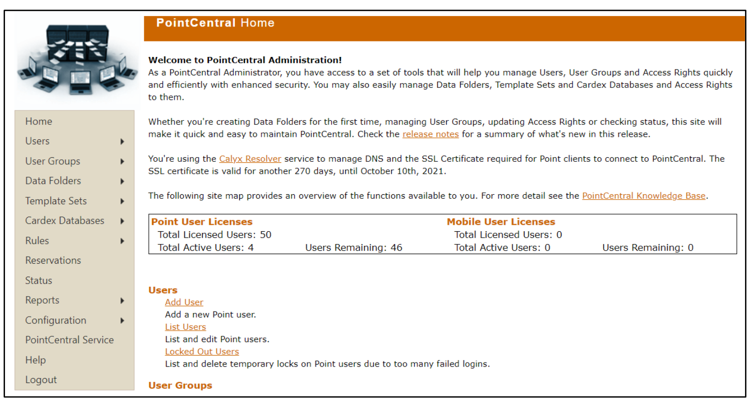


Figure 60: PointCentral Home Page

9. Enter a new **Username** and **Password** In the *First Time Login* dialog.

Note: New login data is required to access the *Administration* site. The PointCentral password must contain a minimum of eight characters and at least three of the following attributes:

- Uppercase alphabetical characters (A-Z)
- Lowercase alphabetical characters (a-z)
- Numeric characters (0-9)
- Special characters (! @, #, $, etc.)

Set Operational Parameters

Use the *Parameters* screen to configure PointCentral. Click **Save** for each line-item change.

Organization Settings

Complete the following organization settings.

1. Select **Parameters** from the *Configuration* menu**.** (See Figure 60.)
2. Enter the **Admin Username**.

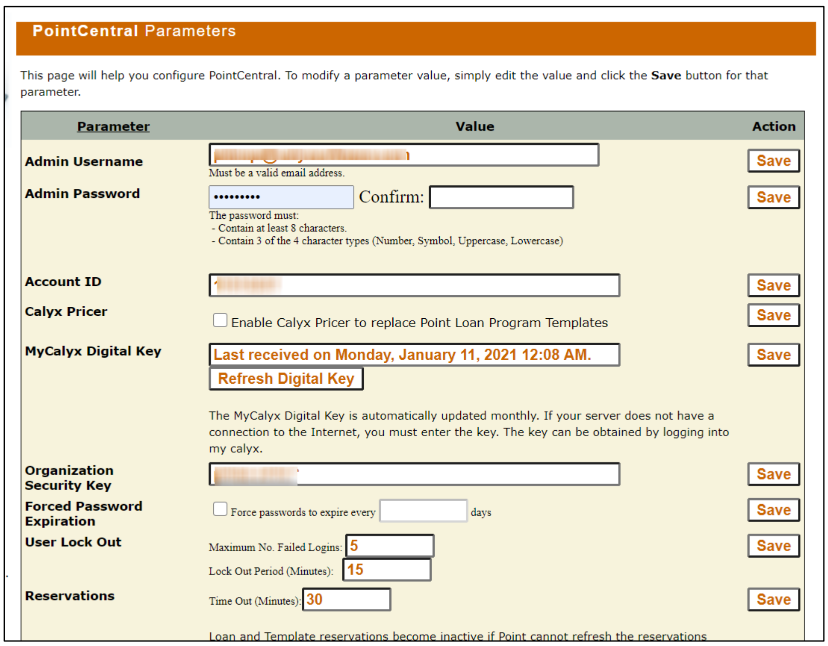


Figure 61: Organization Parameters

3. Enter the **Admin Password**.
4. Confirm the **Admin Password**.
5. Enter the **Account ID**.

Note: The *Account ID* is assigned by Calyx with PointCentral. Contact Sales if the Account ID is unknown.

6. Select the **Enable Calyx Pricer to replace Point Loan Program Templates** checkbox to launch Calyx Pricer automatically when Point Users click the **Loan Program** button.

Note: Users must be assigned a template set in PointCentral to access Calyx Pricer from the *Loan Program* button in Point when Calyx Pricer is enabled. An error occurs for Users who are not assigned a template set. See Template Sets for details.

7. Enter the **MyCalyx Digital Key** field if the site does not have an internet connection.

Note: The *MyCalyx Digital Key* is entered automatically when PointCentral is downloaded from MyCalyx for the first time if the server has an internet connection.

8. Click **Refresh** to view MyCalyx license and User updates and import the information into PointCentral.
9. Verify/enter the **Organization Security Key**.
10. Select the **Forced Password** checkbox to force password changes and enter the password change frequency.
11. Enter the **Maximum Number of Failed Logins** before User lockout.
12. Enter the **Lockout Period** to establish the number of minutes the User must wait before attempting log in again after exceeding the maximum number of failed logins.
13. Enter the **Reservations Time** out.

Note: See Reservations for details.

Template Settings

Complete the template-specific settings. PointCentral compresses and archives all the template files within a template set into one template set archive file before sending templates to Point Users. The compression improves performance and reduces the amount of time a Point User must wait the first time they log in to Point and PointCentral. The second time a Point User logs in, only the files that changed are sent to the Point client when a User accesses a certain template type.

PointCentral can automatically rebuild the template set archives once a day. The rebuild ensures the first time a Point User logs in PointCentral sends all the template files within the User template set without additional calls to the server.

Force the Point client to always download the template set archive from PointCentral when many template files change daily, and the size of template sets is small. The setting improves performance because every Point client does not have to download every template file that changed since the last log in.

Note: Use this feature with caution and set the number of template files that would trigger an automatic download of the template archive appropriately.

Changing the root folder path and root template set path requires the conversion of all data folders to conventional Point and re-importing the folders. Folder Access rights are not preserved when folders are converted to conventional Point. The Users and User Groups remain intact because they are not defined at the folder level in PointCentral. The default value is recommended. FileSync may not start or may generate an error if the **Root Folder Path** field is empty.

The root template set path may only be changed if all template sets were converted to conventional Point and no PointCentral template sets exist. Restart the web service for changes to this value to take effect.

1. Select the **Automatically rebuild of Template Set Archive once a day** checkbox for the daily rebuild.

Figure 62: Template Parameters

2. Enter the **Template Rebuild** time.
3. Select the **Force Point to download the entire Template Set Archive** checkbox enter then the number of template files.
4. Verify the **Root Folder Path** and update if applicable.
5. Verify the **Root Template Set Path** and update if applicable.
6. Use the **Temporary Path Browse** button to establish the temporary file location on the PointCentral server.
7. Select the **Audit Trail** checkbox to enable field changes tracking.
8. Select the **Calyx Experience Improvement Program** checkbox to be included.

Client Configuration

Computers must be configured to work with PointCentral before Users can access PointCentral.

Connect Point Client to PointCentral

Many installations allow access to PointCentral and the data folders from the internet. This feature enables central control access to Point by managing PointCentral Users over the internet. Users can access only Point conventional data folders when Point cannot contact PointCentral.

Use the following steps to connect a Point client to PointCentral.

1. Ensure that Point is closed on the Point client.
2. Select **Point Administrator** from the **Start** menu.

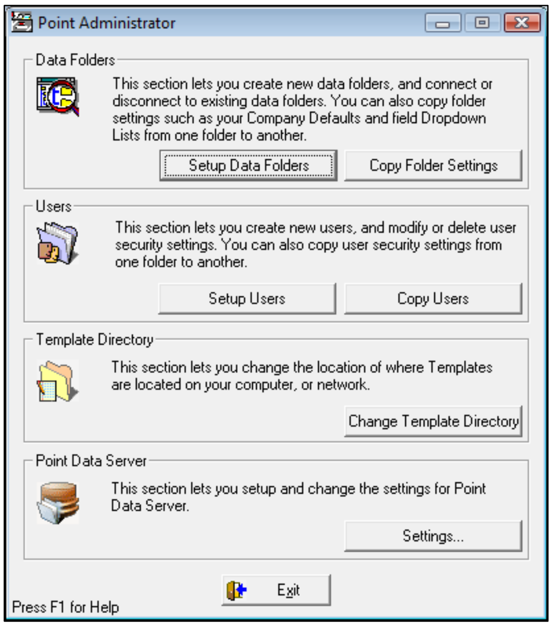


Figure 63: Point Administration

3. Click **Settings** in the Point Data Server section.
4. Select **Enable Point Data Server** checkbox.

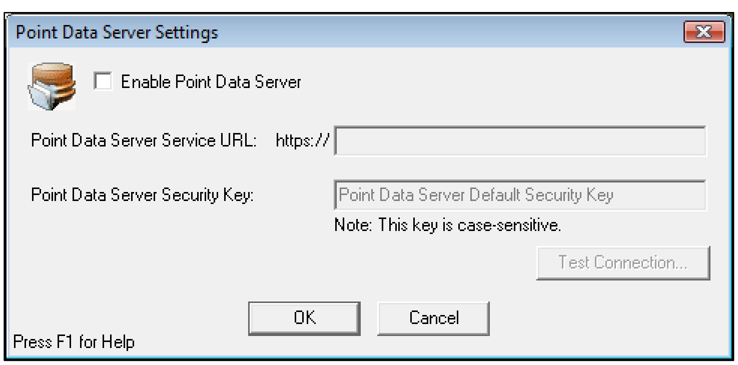


Figure 64: Point Data Server Settings

5. Enter the domain name that is used in the SSL certificate in the **Point Data Server Service URL** field.
6. Append the domain name with **/service**.

Note: Service refers to the web service virtual directory in IIS.

7. Enter the security key used to set the security key parameter in the **Point Data Server Security Key** field. (See Organization Settings for details.)
8. Click **Test Connection**.
9. Enter **User ID** and **Password** in the *Test Login* dialog.

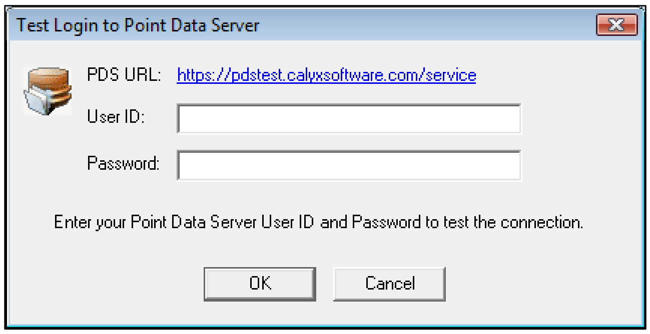


Figure 65: Test Login

Note: Any valid user name and password may be used to test the connection.

10. Click **OK** to test the connection to PointCentral.
11. Click **OK** to dismiss the successful connection message when it appears.
12. Click **OK** to accept the settings.
13. Click **Exit**.

Disable Search Refresh Settings

Navigation Panel Search Results refresh each time the User accesses the **Loans** and **Tasks** tabs in conventional Point by default. The search results are displayed in the Point workspace. Disable the automatic refresh feature on Point clients. Point Users can refresh the **Search Results** at any time by clicking the **Search** button on the client **Loans** or **Tasks** tab.

Note: See the *Point User Guide* for additional details.

1. Open **Point** on the client.
2. Enter the **User ID** and **Password** on the *User Login* dialog.
3. Click **OK**.

4. Select **Search/Display Settings** from the *Utilities* menu.

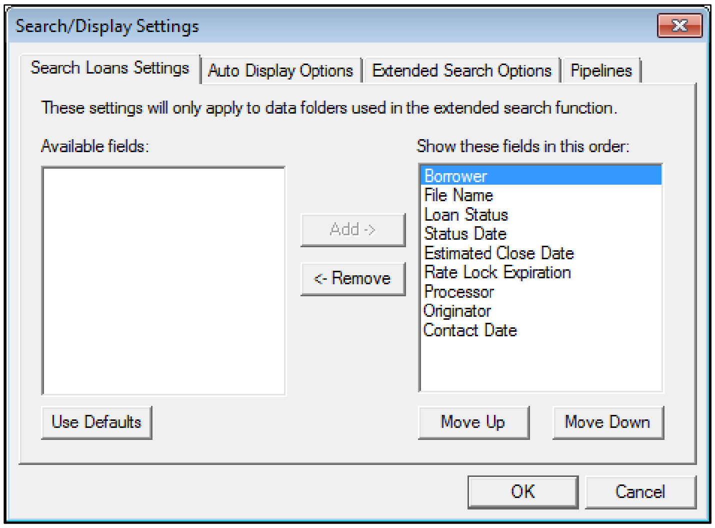


Figure 66: Search/Display Settings Dialog

5. Click the **Auto Display Options** tab.
6. Click **Never in the Auto Display Loan Search Results** section.

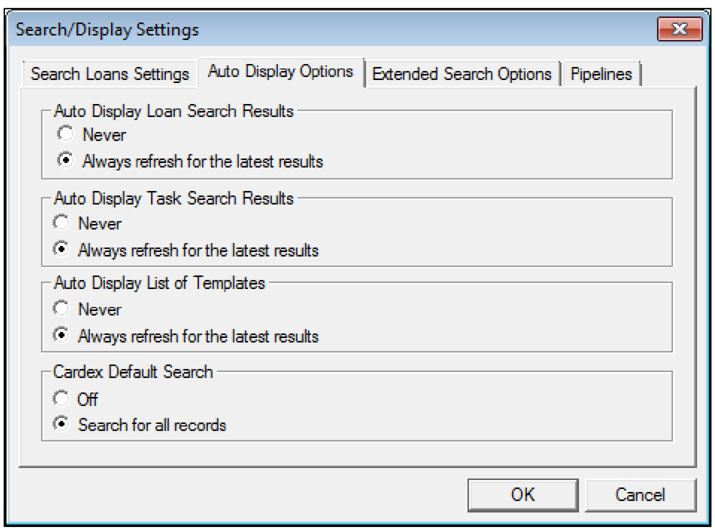


Figure 67: Auto Display Options

7. Click **Never** in the **Auto Display Task Search Results** section.
8. Click **Never** in the **Auto Display List of Templates** section.
9. Click **Off** in the **Cardex Default Search** section.
10. Click **OK** to save the settings.

Reservations

Reservations ensure Users cannot edit a loan or template file while opened by another User. Loans are held open by keeping the file open in the file system in conventional Point data folders. Point transfers the loans and templates over the HTTPS connection while opening and closing when using PointCentral. Reservations to guarantee exclusive access for editing.

Reservations are initiated when a User accesses a loan. The Reservation prevents other Point Users from editing loans until the current User finishes editing and closes the file. Loan packages include the .prs or .brw file and all other files associated with the loan. Loan packages are transferred from PointCentral to the Point User local machine when a User opens a prospect or borrower loan.

Reservation Warnings

An error message displays indicating the file is reserved when another Point User attempts to open a loan or template file. The message includes the current Point User and when the file was reserved.

Note: The Point User has the option of opening the currently reserved file in read-only mode.

Active Reservations

Access the *Reservations* screen to see current reservations.

1. Access PointCentral *Home* page. (See Figure 60.)

2. Select **Reservations** on the *Home* page.

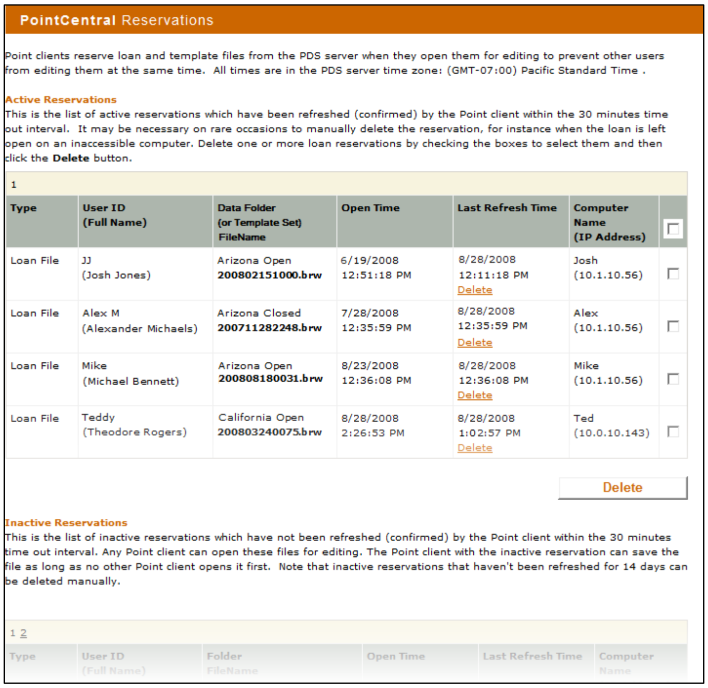


Figure 68: Reservations Screen

Table 7: Reservations Screen Options

Option	Description
File Type	Indicates File Type
User ID	Displays current User name
Data Folder FileName	Indicates Data Folder or Template Set where file resides
Open Time	Indicates when file was opened
Last Refresh Time	Indicates when file was last refreshed
Computer Name	Indicates computer on which file is open

The following occurs when a reservation becomes inactive:

- Inactive reservation file/template is deleted, and new reservation made when a new User attempts to open the file.
- File/template is saved and reservation reactivated when the most recent User accesses the file.

Note: See Set Operational Parameters for details about setting reservation times.

Delete Reservations

Reservations are automatically deleted when the current User closes the file/template. Reservations are also deleted if Point restarts after abnormal termination without closing the file/template.

Use the following steps to manually delete open reservations.

1. Select **Reservations** on the *Home* page. (See Figure 68.)
2. Select the checkbox for the reservation to delete.
3. Click **Delete**.

Check PointCentral Status

The *Status* screen provides the status of requested operations. PointCentral does not complete requests in the sequence received. The *Administration* site queues the requests for FileSync to complete.

Actions are created as the Administrator submits administrative requests. Access the *Status* screen to view feedback about actions.

The following information lists the stages that are involved in processing a request:

- The administrator requests an action.
- Requested action is placed into a queue with a **Pending** status.
- FileSync begins the requested action and updates status to **Progress.**
- Requested action is complete and status updates to **Done.**

PointCentral is more scalable and stable because it can queue requests and complete them one by one using the process above. The *Status* screen is divided into the following two sections:

- Requested Actions: **Pending/In Progress**
- Requested Actions: **Done**

The following table contains a list of possible actions.

Table 8: Possible Actions

Import Data Folder	Create Data Folder	Copy Folder Settings
Copy Folder Access Rights	Update Folder Name	Import Users and Access Rights
Rebuild Additional Fields Table	Rebuild Custom Fields Table	Synchronize Data Folder
Change Root Folder Path	Switch Data Folder to Conventional	Stop/Start Monitoring Folder
Create a Template Set	Rebuild a Template Set	Copy a Template Set
Switch Template Set to Conventional	Delete Cardex Database	Copy Cardex Database
Import Cardex Database	Change Root Template Set Path	Import Users From File

Advanced Configuration

FileSync, the *Administration* site, and the web service are configurable through the *Administration* site and the PointCentral Configuration Wizard for most operations and features supported by PointCentral.

Access more advanced parameters to control system component behavior. System components include a private configuration file containing advanced parameters.

PointCentral Components Configuration Files

All configuration files are XML-formatted text files. Use a text or XML editor to make changes to the advanced parameters.

Note: The default values for the component configuration parameters are adequate for most installations. Make changes to these parameters only when necessary.

The configuration files are stored in the following local installation directory locations.

Table 9: Component Configuration Files

File Name	Location
Admin	...\Calyx Software\PointCentral\admin\Web.config
FileSync*	...\Calyx Software\PointCentral\filesync\PDSFileSync.exe.config
web service	...\Calyx Software\PointCentral\service\Web.config
Admin	...\Calyx Software\PointCentral\admin\dataconfiguration.config

File Name	Location
PDS FileSync	...\Calyx Software\PointCentral\filesync\dataconfiguration.config

Note: The *Admin* and *FileSync* directories also store information about how to connect to the SQL database in a file named *dataconfiguration.config*.

Administration Site Parameters

web.config is the *Administration* site configuration file. The file is a standard ASP.NET configuration file for web sites. The administration advanced parameters are in the **<appSettings>** within **<configuration>**, as shown in the following example:

```
<configuration>
<!-- application specific settings -->
  <appSettings>
    <add key="PdsConnectionString" value="value of PDS database connection string"
    />
    <add key="NumFoldersPerPage" value="20" />
    <add key="DatabaseCommandTimeOut" value="60" />
  </appSettings>
  <system.web>
   ...
  </system.web>
</configuration>
```

The following parameters are on the administration site.

PdsConnectionString

The **PdsConnectionString** parameter is a standard ADO.NET database connection string used to connect the administration site to the PointCentral database.

Note: The *PdsConnectionString* is automatically updated by the PointCentral Configuration Wizard. It is not necessary to edit it manually.

Key: PdsConnectionString

Sample Value:

workstation id=PDSSERVER;packet size=4096;User id=sa; pwd=MyPdsPassword;data source=PDSSERVER;persist security info=False;initial catalog=Pds

NumFoldersPerPage

The **NumFoldersPerPage** parameter sets the number of folders displayed per page on the *Administration* site pages. The *Administration* site splits the list into multiple pages to enable the Administrator to access the pages individually. The multiple page format enables the system to scale and support hundreds of data folders without degradation of performance.

Key: NumFoldersPerPage

Default Value: 20

Minimum Value: 1

The following pages take into consideration the **NumFoldersPerPage** parameter:

- Data Folders/Accelerated
- Data Folders/Conventional
- Folder Monitoring/Enabled
- Folder Monitoring/Disabled
- Synchronization
- Status

DatabaseCommandTimeOut

The **DatabaseCommandTimeOut** parameter sets the maximum time (in seconds) the Administration application waits for a response from the database before timing out. The default is 60 seconds and should be enough for most installations. Increase the value if the system contains many folders, loan files, or tasks and time outs begin occurring.

Key: DatabaseCommandTimeOut

Default Value: 60

Minimum Value: 60

DbVersionNeeded

The **DbVersionNeeded** parameter defines the database that works with the deployed component. This parameter is available in all three components. Do not change the parameters.

Key: DbVersionNeeded

Default Value: Version specific (n.n.n)

Note: Refer to Microsoft documentation for details about ASP.NET configuration.

FileSync Parameters

PDSFileSync.exe.config is the FileSync configuration file. The file is an XML-formatted text file that contains the advanced FileSync parameters.

The following parameters are in the **PDSFileSync.exe.config** file.

PdsConnectionString

The **PdsConnectionString** parameter is a standard ADO.NET database connection string like the **PdsConnectionString** parameter in the administration configuration file.

Key: PdsConnectionString

Sample Value:

workstation id=PDSSERVER;packet size=4096;User id=sa; pwd=MyPdsPassword;data source=PDSSERVER;persist security info=False;initial catalog=Pds

DatabaseCommandTimeOut

The **DatabaseCommandTimeOut** parameter is used to set the maximum time (in seconds) that the FileSync application waits for a response from the database before timing out. The parameter is like the **DatabaseCommandTimeOut** parameter that is defined in the administration configuration file.

Key: DatabaseCommandTimeOut

Default Value: 60

Minimum Value: 60

FileWatcherBufferSize

The **FileWatcherBufferSize** parameter defines the amount of memory (in blocks of 4096 bytes) allocated for every accelerated buffer. Every accelerated folder is monitored for loan file changes. FileSync receives notifications from the operating system as Point makes changes to loan files in the accelerated folders. The notifications are queued up in a buffer the FileSync uses as it updates the information about the changed files in the PointCentral database.

Key: FileWatcherBufferSize

Default Value: 2

Minimum Value: 2

Maximum Value: 10

The default value is adequate. It corresponds to a buffer of 8Kb or 8,192 bytes for most installations.

The following files are monitored for every accelerated folder in the **BORROWER** directory:

- All *.BRW files (main borrower loan files)
- All *. CB files (co-borrower loan files)
- All *.TSK files (task files)

The following files are monitored for every accelerated folder in the **PROSPECT** directory:

- All *.PRS files (main prospect loan files)
- All *. CB files (co-borrower loan files)
- All *.TSK files (task files)

The following file is monitored in the root of the **Accelerated** folder:

- The FOLDER.INI file (for changes in the folder name)

Events are added to the **FileWatcherBuffer** when a file is created, changed (saved in Point), deleted, and renamed.

One **FileWatcherBuffer** is created for every file type defined. Seven **FileWatcherBuffers** are defined for every accelerated folder that corresponds to the seven file types. Be careful when increasing the value of the **FileWatcherBufferSize** parameter. Available RAM could be used and cause a significant degradation of system performance if many accelerated folders are defined.

The following table shows an example of the RAM used for different **FileWatcherBufferSize** parameter settings in environments that manage 50 or 500 accelerated folders.

Table 10: FileWatcherBufferSize RAM Usage

FileWatcherBufferSize	lRAM used by value (50 folders)	RAM used by value FileSync (500 folders)
2	18 MB	47 MB
5	22 MB	84 MB
10	28 MB	144 MB

TimeToWaitForDebug

The **TimeToWaitForDebug** parameter defines how long FileSync waits (in milliseconds) before attempting to connect to the SQL database and start monitoring data folders. The parameter is useful when the SQL Server is hosted on the same machine where FileSync is installed. FileSync waits a few seconds to provide enough time for SQL Server to start.

Key: TimeToWaitForDebug

Default Value: 40000

Minimum Value: 1

Maximum Value: 2147483647

MaxTemplateFileSizeKB

The **MaxTemplateFileSizeKB** parameter defines the maximum size (in KB) FileSync accepts for one template file. The default of 5 MB (5120 KB) is large enough, so most template files are included in a template set.

Key: MaxTemplateFileSizeKB

Default Value: 5120

Minimum Value: 1

Maximum Value: 2147483647

Stop and restart File Sync after making changes to any of the advanced parameters in the **PDSFileSync.exe.config** file.

Web Service Parameters

PdsConnectionString

The **PdsConnectionString** parameter is a standard ADO.NET database connection string like the **PdsConnectionString** parameter in the administration and FileSync configuration files.

Key: PdsConnectionString

Sample Value:

workstation id=PDSSERVER;packet size=4096;User id=sa; pwd=MyPdsPassword;data source=PDSSERVER;persist security info=False;initial catalog=Pds

DatabaseCommandTimeOut

The **DatabaseCommandTimeOut** parameter sets the maximum time (in seconds) the web service waits for a response from the database before timing out. This is like the **DatabaseCommandTimeOut** parameter defined in the administration and FileSync configuration files.

Key: DatabaseCommandTimeOut

Default Value: 60

Minimum Value: 60

MaxRecordsGetTasks

The **MaxRecordsGetTasks** parameter defines the maximum number of tasks PointCentral returns to Point on a single call. Point Users can search for all open tasks, or all overdue tasks in one or more folders.

Key: MaxRecordsGetTasks

Default Value: 5000

Minimum Value: 1

Maximum Value: 2147483647

The total number of tasks returned to the Point client could be quite large in a system with many accelerated folders, loans, and tasks.

The default setting for the **MaxRecordsGetTasks** parameter is 5000 to ensure all the bandwidth is not used by one Point client. **MaxRecordsGetTasks** parameter ensures large lists are not returned to Point clients. A warning message is sent to the Point User indicating the maximum number of tasks per list is reached (Warning code -3) when limit is reached.

The value is adequate for most installations, but it can be increased to a maximum of 2,147,483,647 tasks. the size of task lists sent from PointCentral to Point could increase for every request from Point clients and cause a degradation of overall system performance If the number is increased.

MaxRecordsGetLoanApps

The **MaxRecordsGetLoanApps** parameter defines the maximum number of loan records PointCentral returns to Point on a single call. Point Users can search for loans in the *Loans* and *Reports* screens. The parameter is like **MaxRecordsGetTasks** but limits the number of loans.

Key: MaxRecordsGetLoanApps

Default Value: 50000

Minimum Value: 1

Maximum Value: 2147483647

MaxRecordsGetCardexEntries

The **MaxRecordsGetCardexEntries** parameter defines the maximum number of Cardex entries PointCentral returns to Point on a single call. The parameter is like MaxRecordsGetTasks but limits the maximum number of tasks returned to Point. The Point client asks for a maximum of 500 Cardex entries by default.

The **MaxRecordsGetCardexEntries** parameter ensures PointCentral properly scales. Proper scaling occurs even if the Point client configuration changes to the limit of 500 Cardex entries retrieved per call.

Key: MaxRecordsGetCardexEntries

Default Value: 50000

Minimum Value: 1

Maximum Value: 2147483647

MaxTemplateFileSizeKB

The **MaxTemplateFileSizeKB** parameter defines the maximum size the web service accepts (in KB) for one template file. Point Users can save the most template files with the default value of 5 MB (5120 KB), but the maximum size can be further limited.

Key: MaxTemplateFileSizeKB

Default Value: 5120

Minimum Value: 1

Maximum Value: 2147483647

UpgradeMessage

Use the **UpgradeMessage** parameter to define a maintenance message that displays to Point Users. Save a message that describes the reason for maintenance and the expected completion time for example.

Setting a value in **UpgradeMessage** (not blank or empty) stops normal operation and displays the message to all Point Users when they access accelerated folders. Clearing the value from **UpgradeMessage** removes the maintenance message and returns to normal operation.

Key: UpgradeMessage

Default Value: None (blank or empty)

Stopping and Restarting IIS

IIS automatically reads changes made to the **Web.config** file during the next request made to any page in the *Administration* site in most cases. Stop and restart IIS when IIS takes a long time to respond after a change.

1. Open a **Command Prompt** window.
2. Enter **iisreset /restart** in the window.
3. Press **Enter**.

Messages display indicating the internet services were successfully started and stopped after a few seconds.

Chapter 5 - Resource Management

An integral part of PointCentral administration is creating and maintaining the following:

- Users
- User groups
- Access rights to data folders
- Access rights to template sets
- Access rights to Cardex databases

Creating User Groups and globally defined Users eliminates the inconvenience of having to create the same User in multiple locations.

Note: Conventional Point manages data folders, Users, and access rights in Point Administrator.

License Management

Making various license additions and access changes automatically updates the **MyCalyx** digital key in PointCentral. The update could trigger a condition called a grace period.

A grace period occurs when the total number of PointCentral Users is greater than the total license count embedded in the **MyCalyx** digital key.

Users are no longer able to connect to PointCentral until the **MyCalyx** digital key is refreshed when the grace period expires.

The following scenarios could cause the grace period to go into effect:

- Site that manually updates the **MyCalyx** digital key and forgets to update within the required 30 days.
- Users are added in PointCentral before the licenses are purchased and added in **MyCalyx.**
- The number of licensed Users is zero (typically occurs when a PointCentral site cancels an account).

The grace period for each of these scenarios is 24 days and begins on the day the message is issued.

The **User Summary** on the *Home* page provides a license count for Point and mobile licenses.

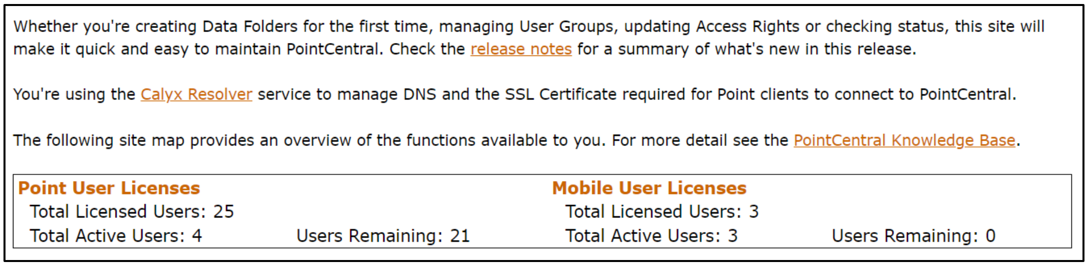


Figure 69: Point User Licenses

The message displays on the *Home* page below the license summary information when the license count exceeds the licenses. The grace period begins when the message displays.

The following options are available when the account enters the grace period:

- Delete or disable enough PointCentral Users to reduce the **Users Remaining** count to 0 (The grace period is terminated immediately.)
- Purchase additional licenses to accommodate the User increase.
- Allow the grace period to expire and service to lapse.
- Point and mobile Users cannot login to PointCentral until the issue is resolved if an action is not taken to reduce the increased User count.

Users

Assign Users a unique full name, a unique User ID, and a password.

Add Users

The following conventions apply when adding a new User:

- Full name and User ID must be unique.
- Full name, User ID, and password must be entered in the same format as created (such as PointCentral User is not the same as pointcentral User).
- Enter the full name exactly as it is in Point for each data folder to which the User is granted access, or the User will not be able to access the files if given **This Processor's Files Only** or **This Originator's Files Only** access rights.

Note: This data is set in the *Point Utilities* > *Dropdown Lists* function. (See the *Point User Guide* for details.)

1. Select **Add Users** from the **Users** menu on the PointCentral *Home* page**.**
2. Enter User **Full Name**.

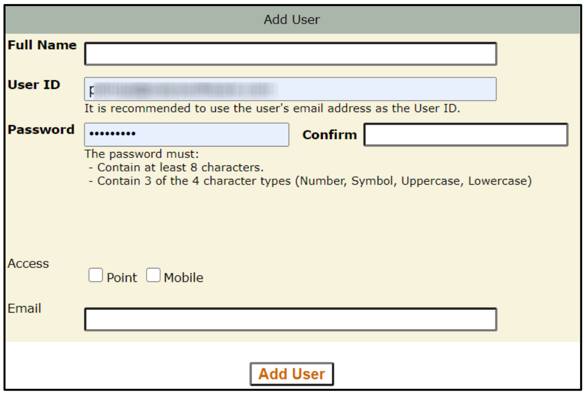


Figure 70: Add User Screen

3. Enter the **User ID**.
4. Enter the account **Password**.
5. Re-enter the password in the **Confirm** field.
6. Select the appropriate **Access** checkbox(es).
7. Enter the User's **Email**.
8. Click **Add User**.
9. Proceed to Edit User to add additional User information.

List Users

This screen displays the list of *Users* in for *PointCentral*. Use this screen to edit, delete, or view the user's *Effective Access Rights* and *Activity* log. This screen allows users to enable or remove access to Point *(Point Access)* or *Mobile Access.*

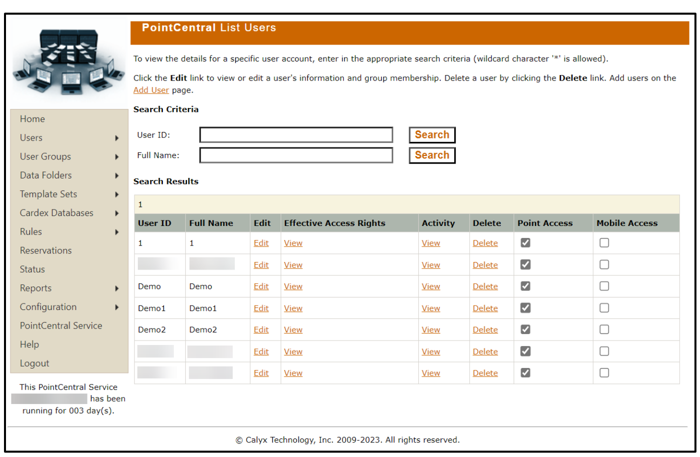


Figure 71: List Users

User Search

Use the following steps to perform a User search.

1. Select **List Users** from the *Users* menu on the PointCentral *Home* page**.**
2. Enter the **User ID** or **Full Name**.

Figure 72: User Search

3. Click **Search** to display the User in the list.

Edit User

Use the following steps to edit a User.

1. Perform a User search. (See User Search).
2. If needed, select the **Mobile Access** or the **Point** checkbox to enable for the User.
3. Click **Edit** for the appropriate User. (See Figure 71).
4. Update User information as required.

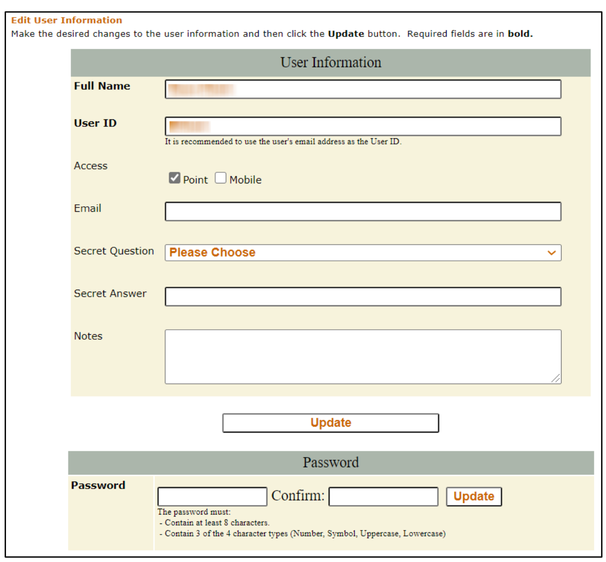


Figure 73: Edit User Information

5. Select a **Secret Question**.

6. Enter the **Secret Answer**.
7. Enter **Notes** if applicable.
8. Click **Update**.
9. Edit **Password** fields if applicable.
10. Click **Update**.

User Effective Access Rights

Click on the *View* link to display the specific user access right currently in effect. The *Search Criteria* fields allows the user to search for different *IDs* or *Names*.

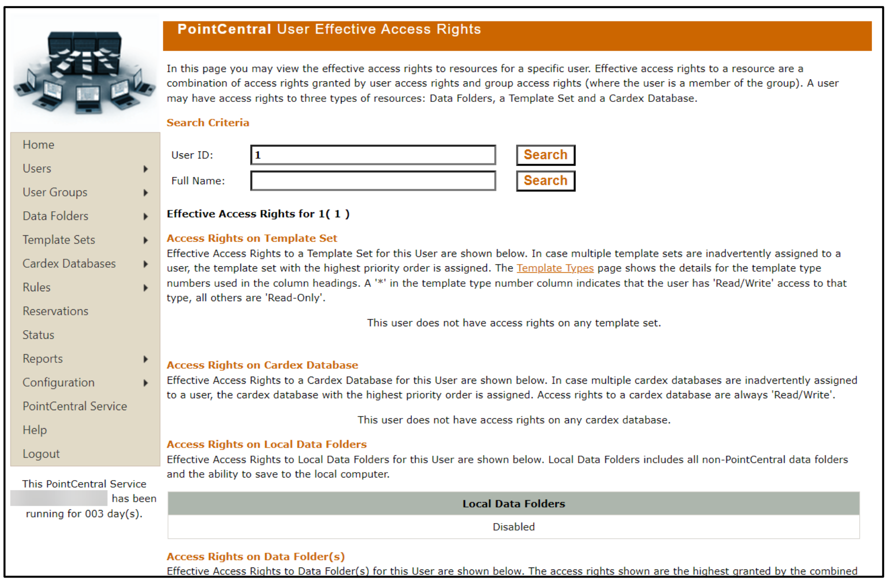


Figure 74: View Effective Access Rights

User Activity Log

The *Activity Log* allows access to view a user's activity for *Today* or view *All Activity.* To export the log, select the *ExportCSV*. The *Search Criteria* fields allows for search for different *IDs* or *Names*.

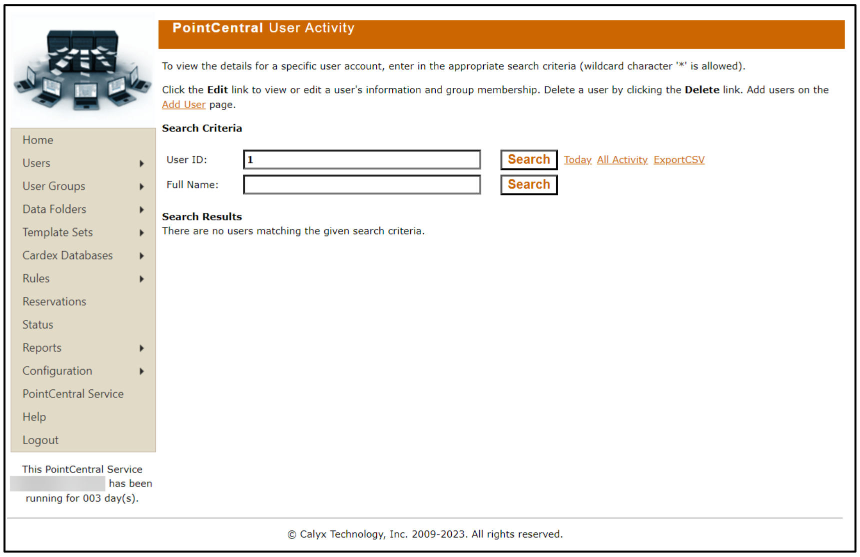


Figure 75: User Activity

Note: All activity is purged after 90 days.

Delete User

Use the following steps to edit a User.

1. Perform a user search. (See User Search.)
2. Click **Delete** for the appropriate User. (See Figure 71.)
3. Click **OK** on the *Delete Conformation* dialog.

Unlocking Users

Point has a login lock out security feature. Point Users are locked out from PointCentral after a maximum number of failed logs in attempts within a lock out period. The lockouts expire automatically after the lock out period.

1. Select **Locked Out Users** from the **Users** menu on the PointCentral *Home* page**.**
2. Click **Delete Lockout** for the User to cancel the lockout immediately.

User Groups

User groups are based on company structure. A User can be a member of multiple User Groups. User group management enables assigning data folder access rights to a set of designated Users. The access rights to a particular data folder are the highest access rights granted by any User Group to which the User belongs when a User is a member of multiple User Groups.

Add User Groups

Use the following steps to add User Groups.

1. Select **Add User Group** from the *User Groups* menu.
2. Enter the name of the group in the **Group Name** field.

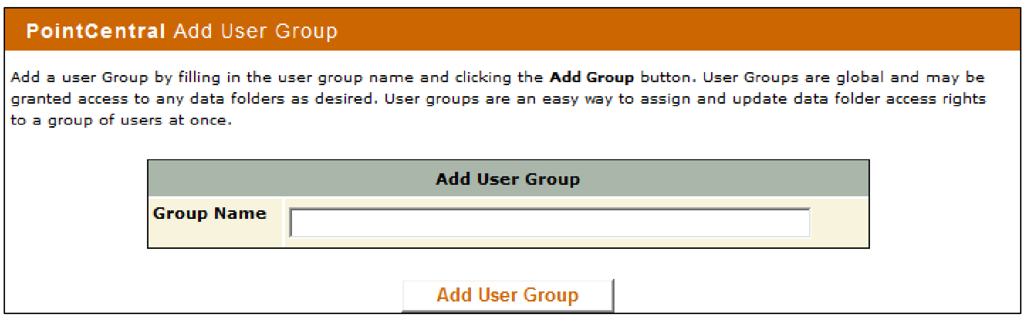


Figure 76: Add User Group

3. Click **Add User Group**.
4. Enter **Notes** if applicable.

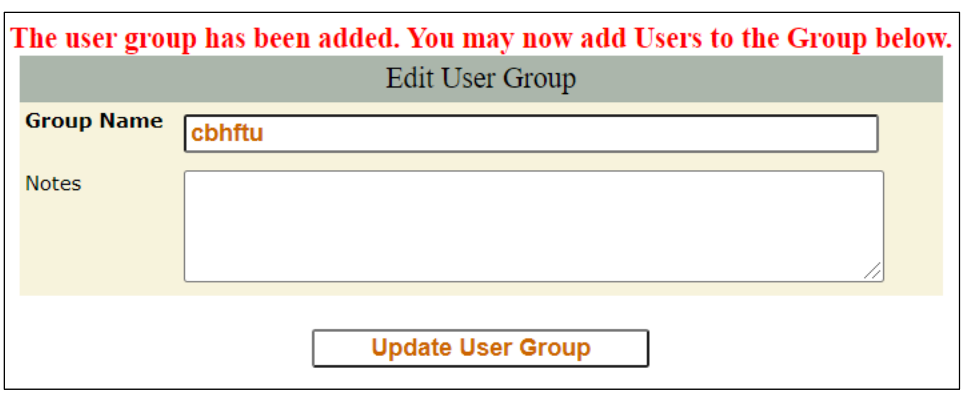


Figure 77: Update User Group

5. Click **Update User Group**.

Edit User Groups

Use the following steps to add *User Groups*.

1. Select **List User Groups** from the *User Groups* menu.

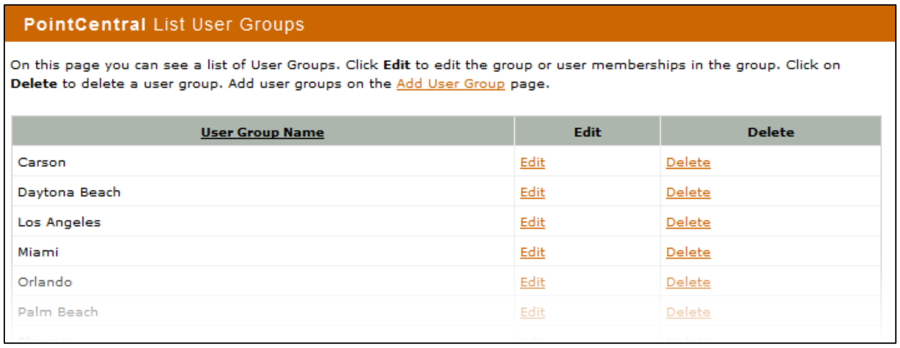


Figure 78: List User Groups

2. Click **Edit** for the *User Group* to edit.
3. Edit **Group Name** if applicable. (See Figure 74.)
4. Click **Update User Group**.

Add Users to Group

Use the following steps to add Users to groups.

1. Access the **User Groups List**.
2. Click **Add Other Users**.

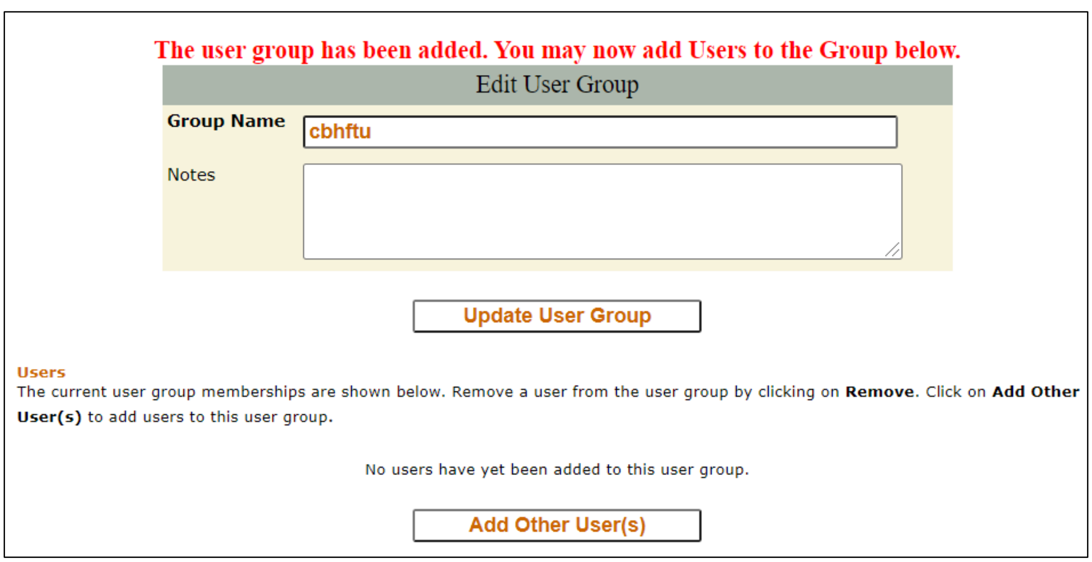


Figure 79: Add Other Users

3. Select the **Users** to add to the group.

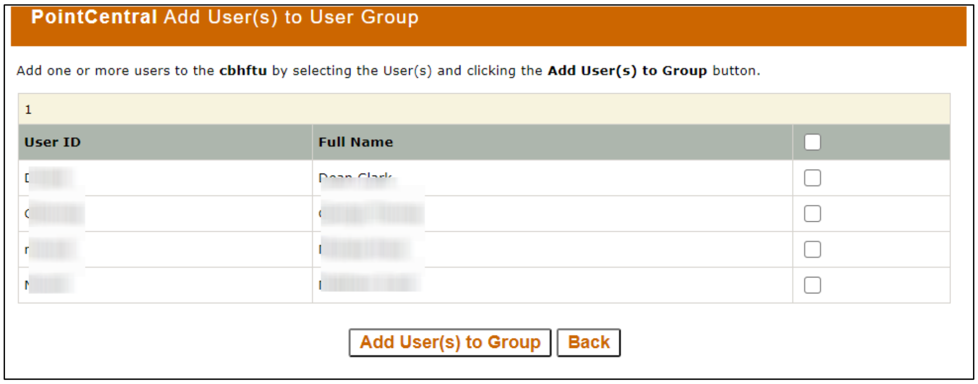


Figure 80: Add User(s) to Group

4. Click **Add User(s)** to group.
5. Click the **Back** button to return to the *Edit User Group* screen.

Remove Users from Group

Use the following steps to remove Users from groups.

1. Access the **User Groups List**.
2. Select the User to remove.

Figure 81: Remove Users

3. Click **Remove**.

Data Folders

Create data folders based on how loan files are processed by the company. Data folders are a resource to which Users or User Groups are granted access.

Data Folder Organization

Develop a standard folder deployment plan for the organization.

The following sections provide suggestions about the preferred method for deploying Point data folders. Methods for deploying PointCentral across one or multiple servers are covered.

Set up folders are based on how loan files are processed within the organization. The data folder organization reflects the following:

- Loan status
- Location
- Role

Loan Status

Point reflects several loan statuses. The loan originator or processor determines the loan status. Point updates the loan status according to the dates entered as the loan originator or processor works in the file.

The following table shows an example of a loan status data folder structure.

Table 11: Loan Status Data Folder Structure

Loan Status	Loan State	Data Folder
Open Submitted	In progress	In progress
Approved		
Clear to close Documents		
Funded		
Recorded		
Closed	Closed	Closed
Suspended	Canceled	Canceled
Denied		
Canceled		

Loans are not automatically transferred from folder to folder when their status changes. Define a procedure for loan originators and processors to move loans among the data folders manually as the status changes.

Location

Branches are defined as a physical location or a logical separation of units within your organization.

The following table shows an example of a location data folder structure when the organization has branches in different states.

Table 12: Location Data Folder Structure

Branch	City	Data folder
Florida	Daytona Beach Miami Orlando Palm Beach	Florida in progress Florida Closed Florida Canceled
California	Los Angeles Santa Fe San Francisco San Diego	California In progress California Closed California Canceled
Arizona	Phoenix Carson Tempe	Arizona in progress Arizona Closed Arizona Canceled

Role

Define data folders based on how the organization is structured. The following table shows an example of a data folder structure by organization roles.

Table 13: Organizational Data Folders

Users	User Groups	Data Folder
Orlando loan originator 1 Orlando loan originator 2	Orlando loan reps	Orlando potential
Orlando processor 1 Orlando processor 2	Orlando processors	Orlando in progress
Orlando manager 1 Orlando manager 2	Orlando managers	Orlando canceled Orlando closed

Add Data Folders

Use the following steps to add data folders.

1. Select **Add Data Folder** from the *Data Folders* menu.

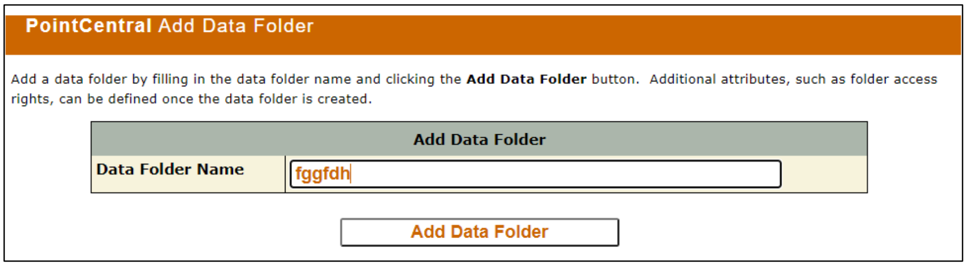


Figure 82: Add Data Folder

2. Enter the name of the folder in the **Data Folder Name** field.
3. Click **Add Data Folder**.

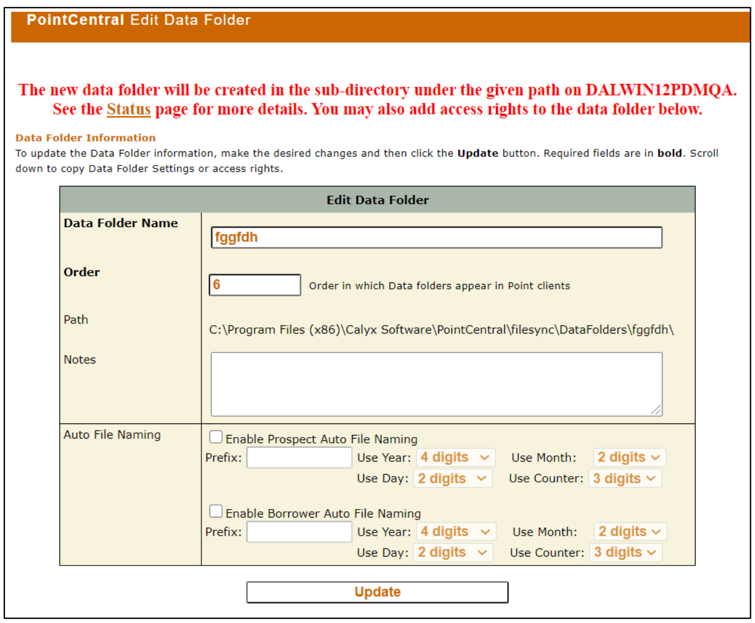


Figure 83: Edit Data Folder

Note: The confirmation message indicates where the data folder will be created.

4. Set the **Order**.
5. Enter **Notes** if applicable.
6. Select the appropriate **Auto File Naming** options.
7. Click **Update**.

Edit Data Folders

Use the following steps to edit data folders.

1. Select **Add Data Folder** from the *Data Folders* menu.

2. Make appropriate changes. (See Figure 80.)
3. Click **Update**.

Add User Group Access

Use the following steps to add User Group access rights.

Note: See Copy Access Rights for access rights details.

1. Select **Add Data Folder from the Data Folders** menu.
2. Click **Add User Group Access Rights**.

Figure 84: Add User Group Folder Access

3. Select the **User Group**.
4. If needed, choose an access level template (*Full Access*, *Read Only*, *Restricted Access*).

Note: Selecting an access level template will automatically choose the options related to the selected access.

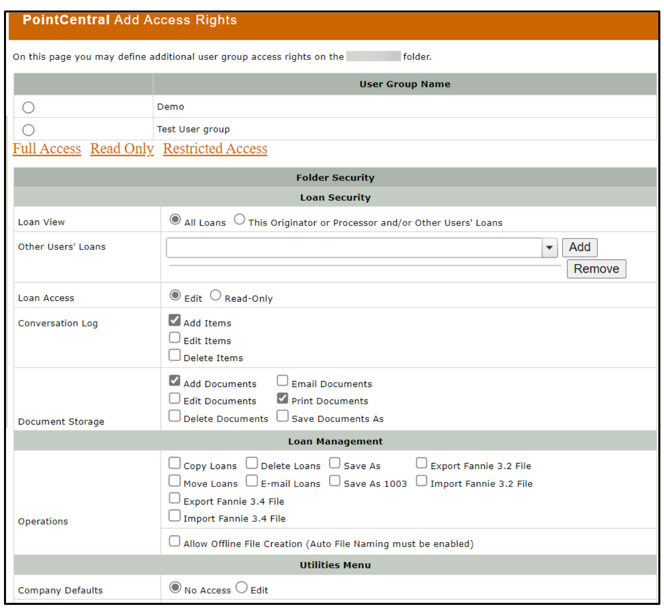


Figure 85: Complete Group Folder Access

5. Select the **Loan View** option.

6. Select **Other Users Loans** to which the **Group** has access from the dropdown.

Note: Use the *Add* button to add additional Users.

7. Select the **Loan Access** option.
8. Select the appropriate **Conversation Log** option(s).
9. Select **Document Storage** option.
10. Select **Operations** options.
11. Select the **Allow Offline File Creation** checkbox to allow offline file creation.
12. Select the **Utilities Menu** options.

Note: The *Utilities Menu* selections determine access to Point *Utilities* menu options.

13. Select the **Tracking** options.

Note: The *Tracking* selections determine access to Point *Track* menu options.

14. Select the **Banker** options.

Note: The *Banker* selections determine access to Point *Banker* menu options.

15. Click **Add Group Access Rights**.

Note: The document storage settings do not apply to the *Track* and *Banker* screens. The screen security settings for the *Track* and *Banker* screens take precedence over the document storage settings.

Add User Access

Use the following steps to add User access rights to folders.

Note: See Copy Access Rights for access rights details.

1. Select **Add Data Folder** from the *Data Folders* menu.
2. Click **Add User Access Rights**.
3. Use the steps for adding User Group access to add User access. (See Add User Groups.)
4. Click **Add User Access Rights** when complete.

Copy Folder Settings

Copy folder settings from an existing data folder to the selected data folder.

Note: Copied folder settings overwrite the selected folder settings.

1. Select **Add Data Folder** from the *Data Folders* menu.
2. Scroll down to the bottom of the screen.
3. In the *Copy Folder Settings*, select the dropdown menu.

4. Select the folder to be copied from the dropdown.
5. Click **Copy**.
6. Click **Yes** on the *Confirmation* prompt.

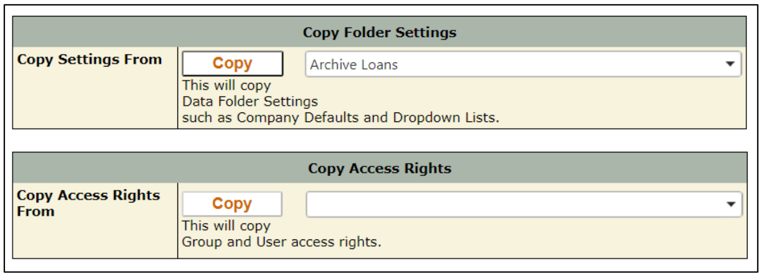


Figure 86: Copy Folder Settings

Copy Access Rights

Copy access rights from an existing data folder to the selected data folder.

Note: See Copy Access Rights for access rights details.

1. Select Add Data Folder from the Data Folders menu.
2. Select the User to be copied from the dropdown. (See Figure 83.)
3. Click Copy.
4. Click Yes on the *Confirmation* prompt.

Data Folder Access Rights

Setting access rights defines which Users are allowed access to which resources and the way access is achieved. Each access rights definition relates a single User Group or single User to a designated resource (such as a data folder) and defines the access granted.

The following figure shows an example of the relationship between Users, User Groups, and data folders.

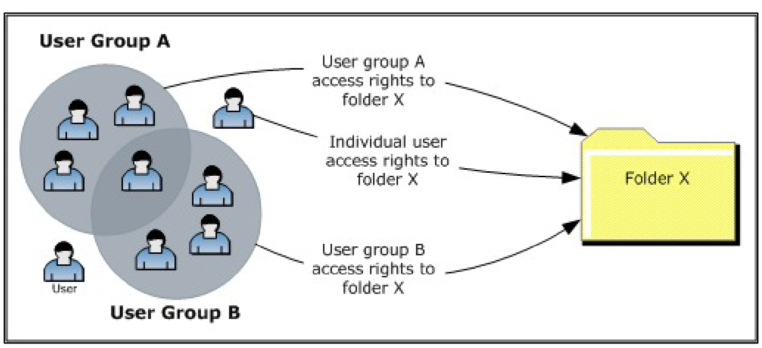


Figure 87: Data Folder Relationship

There are no default access rights. Establish the access rights definition between folders and Users/User Groups individually.

Creation of fewer access rights definitions is required when utilizing User Groups because definitions are set for the collective group rather than individuals.

A User and data folder can be involved in more than one access rights definition. A relationship can be defined directly between the folder and the User and additional relationships defined between the folder and a User Group that includes the same User. The access rights definitions are merged for the User that results in granting the User the highest access rights granted by any of the definitions to the data folder.

A User assigned **This Processor's Files Only** and **This Originator's Files Only** receives the **This Processor's Files Only** setting because the setting has higher precedence and access is granted accordingly. The following table shows the effective permissions for different access right combinations.

Table 14: Combined User Access Permissions

All Loans	This Processor's Files Only	This Originator's Files Only	Effective Permissions
Yes	Any	Any	All
No	Yes	No	Processor files
No	No	Yes	Originator files
No	Yes	Yes	Processor files

Refer to the P*oint User Guide* for information about creating processor and originator dropdown lists in Point.

Offline File Creation

Users can create files offline and store the files in a data folder that is enabled for offline file creation. The offline Loan files are automatically moved into PointCentral data folders when the User connects to PointCentral.

Offline file creation permission is specific to Users, User Groups, and data folders. The permission is assigned by selecting the **Allow Offline File Creation** checkbox in the *Edit User Group Access Rights* or *Edit User Access Rights* screens.

Auto File Naming must be enabled for both prospects and borrowers in the *Edit Data Folder* screen to allow offline file creation. An error occurs when adding User and User Group access rights to a data folder if **Auto File Naming** is not enabled. An error also occurs when attempting to save an offline file in a data folder that is not enabled for **Auto File Naming**.

Determine if a data folder is enabled for offline file creation when you view the data folder list in the **Loans** tab while working in Point offline. Data folders that are enabled for offline file creation are appended with (PDS-Offline), as shown in the following figure.

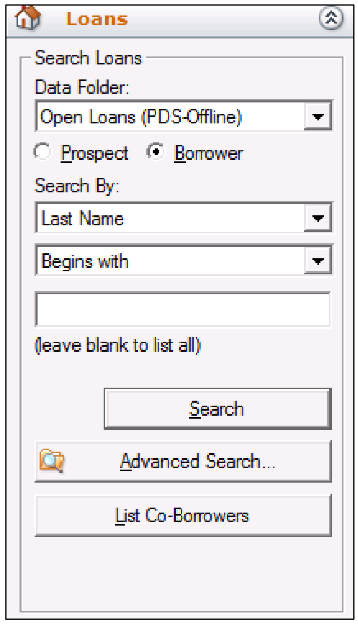


Figure 88: Offline Data Folder Example

The following functions are disabled when working with offline folders and files:

- Copy
- Move
- E-mail files
- Save As

The following dialog displays after the offline move to Point is complete:

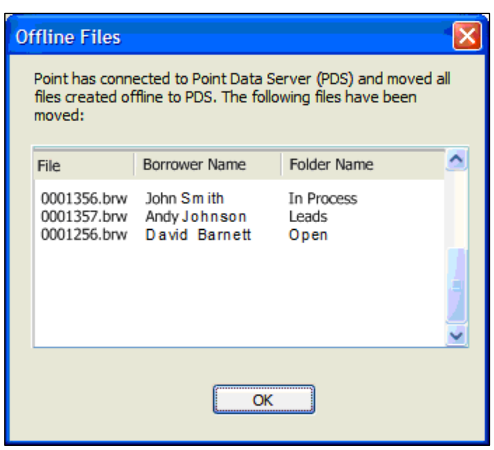


Figure 89: Offline Files Dialog

The following dialog box displays if an error occurs while moving the files from Point to PointCentral:

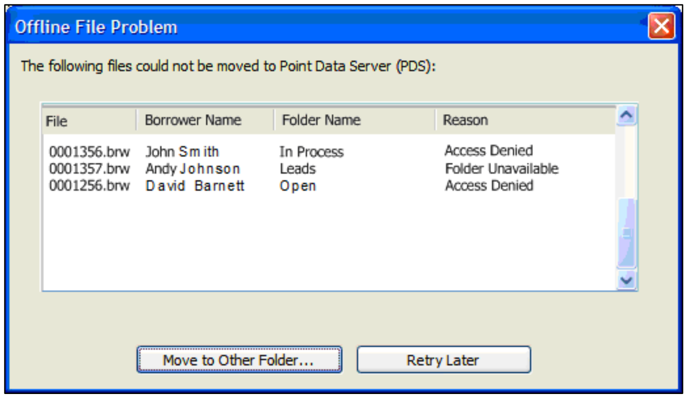


Figure 90: Offline File Problem Dialog

Errors can occur during synchronization for the following reasons.

Table 15: Offline File Creation Errors

Error	Description
Access Denied	The User does not have User or User Group read and write access rights for the data folder
Folder Unavailable	PointCentral is unable to access the data folder
Auto File Naming Not Enabled	The data folder does not have auto file naming enabled

Click the **Move to Another Folder** button on the *Offline File Problem* dialog to select a different folder.

Click the **Retry Later** button to attempt the move during the next PointCentral login.

Local Data Folder Access Overview

Point and PointCentral provide a centralized set of data folders and templates that can be accessed from any computer with an internet connection.

Local Point enables Administrators the ability to control Users ability connected to PointCentral, access data folders, and save files to unauthorized locations.

Set up local Point control in PointCentral Administration, under the *Data Folders* menu.

The feature assists Users using the system to process all loans in Point. Email and export activity is not impacted. All other behavior is the same.

The following limitations apply to Users who are not granted local data folder access rights:

- Local data folders are not visible.

- Saving files (Save As) to other locations is disabled.
- The option to copy borrower and prospect files from one location to another is not available.
- The option to move borrower and prospect files from one location to another is not available.

Point does not launch, and an error message is issued If Users do not have access to local data folders and are unable to connect to PointCentral. Individual User access privileges prevail over access rights granted to User Groups.

Point Administrator is available on the local computer, but restricted folders PointCentral are not available in Point and not included when performing the following actions:

- Search
- Advanced Search
- Reports
- Copy
- Move
- Rebuild List

Configure Local Data Folder Access

Use the following steps to configure local data folder access.

1. Select **Edit Local Data Folder Access** from the *Data Folders* menu.

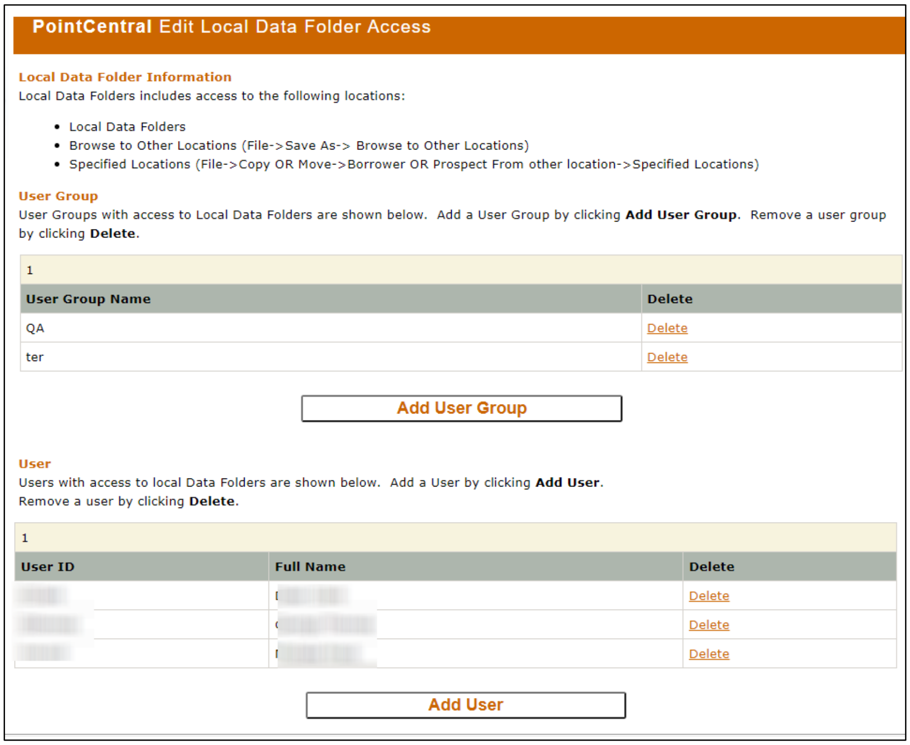


Figure 91: Edit Local Data Folder Access

2. Click **Add User Group**.
3. Select the radio button next to the User Group to add to the local data folders access list.
4. Click **Add Group Access Rights**.
5. Repeat Steps 3 – 4 for additional groups.
6. Click **Add User**.
7. Select the **User ID** radio button to add to the local data folders access list.
8. Click **Add User Access Rights**.
9. Repeat steps 8 – 9 for additional Users.
10. Click **Cancel** to return to the *Edit Local Data Folder Access* screen.

Folder Maintenance

Folder maintenance options are available under the *Configuration* menu.

Synchronize Data Folders

Use the following steps to synchronize data folders to the database.

1. Select **Folder Maintenance** from the *Configuration* menu.
2. Select **Synchronization**.
3. Select the folder(s) to synchronize.

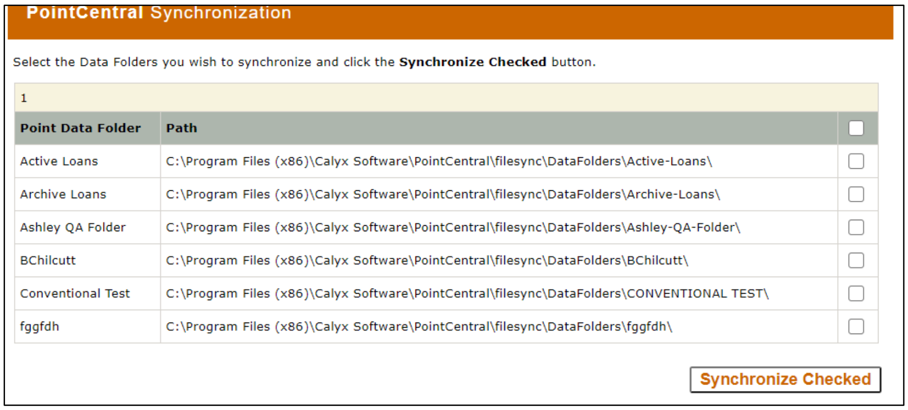


Figure 92: Synchronization

4. Click **Synchronize Checked**.

Convert PointCentral Data Folders

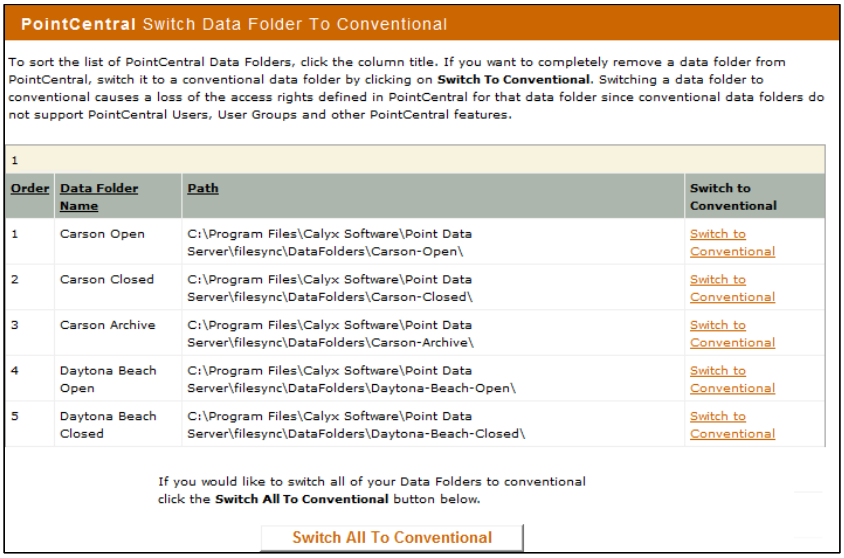
The root folder path cannot be changed until all the data folders are switched to conventional format and re-imported when PointCentral data folders exist.

Note: Folder access rights are not preserved when switching to conventional format.

Use the following steps to convert PointCentral folders to conventional folders.

1. Select **Folder Maintenance** from the *Configuration* menu.

2. Select **Switch To Conventional** to access the *Switch Data Folder To Conventional* screen.



PointCentral Switch Data Folder To Conventional

To sort the list of PointCentral Data Folders, click the column title. If you want to completely remove a data folder from PointCentral, switch it to a conventional data folder by clicking on **Switch To Conventional**. Switching a data folder to conventional causes a loss of the access rights defined in PointCentral for that data folder since conventional data folders do not support PointCentral Users, User Groups and other PointCentral features.

1

Order	Data Folder Name	Path	Switch to Conventional
1	Carson Open	C:\Program Files\Calyx Software\Point Data Server\filesync\DataFolders\Carson-Open\	Switch to Conventional
2	Carson Closed	C:\Program Files\Calyx Software\Point Data Server\filesync\DataFolders\Carson-Closed\	Switch to Conventional
3	Carson Archive	C:\Program Files\Calyx Software\Point Data Server\filesync\DataFolders\Carson-Archive\	Switch to Conventional
4	Daytona Beach Open	C:\Program Files\Calyx Software\Point Data Server\filesync\DataFolders\Daytona-Beach-Open\	Switch to Conventional
5	Daytona Beach Closed	C:\Program Files\Calyx Software\Point Data Server\filesync\DataFolders\Daytona-Beach-Closed\	Switch to Conventional

If you would like to switch all of your Data Folders to conventional click the **Switch All To Conventional** button below.

Switch All To Conventional

Figure 93: Change Data Folder

3. Click the **Link** for the folder to convert.

Note: Click the **Switch All to Conventional** button to convert all folders.

4. Click **Yes** on the *Confirmation* prompt.
5. Rebuild the indexes.

Note: Rebuild the index for each data folder switched to conventional mode.

Refer to the *Point User Guide* for instructions on rebuilding indexes.

Template Sets

Conventional Point manages templates. Templates populate loan files with common information, including:

- Loan programs
- Closing cost scenarios
- Prospect and borrower master files
- Data import and export
- Escrow
- Title tables

The template files that provide additional Point functionality, including:

- Reports

- Custom forms
- Shared print groups

First Log In Template Set Distribution

Conventional Point centralizes the location of a set of template files using a Windows network share.

Example: Set the folder location to \\MYFILESERVER\PNTTEMPL in Point Administrator.

The solution is inadequate in environments with low bandwidth or high latency. PointCentral enables centralizing template files and distributing the files to Point Users automatically without the need for a VPN. This allows defining multiple template sets and grants access rights to specific groups or Users accordingly.

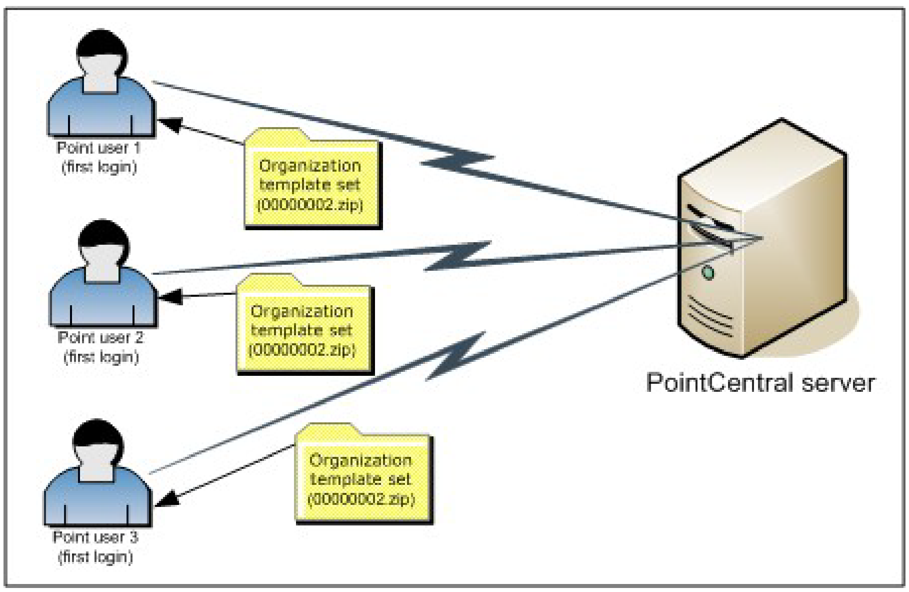


Figure 94: Initial Template Set Distribution

Template sets are stored under the root template set directory in PointCentral. The template sets are typically located at:

C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets.

Each template set is stored under its directory. All sub-directories and template files match the definitions for the conventional C:\PNTTEMPL directory.

Define the access rights for a template set. The access rights tell PointCentral to send a compressed archived file to the Point client containing the template files for the template set the first time a Point User logs in. Point then extracts the template files locally under the C:\Users\username\AppData\Roaming\Calyx Software\Point\AllUsers\Point user ID\PDSFolder.

Subsequent Log Ins

The full template set again does not download with subsequent log ins. Only files that changed since the last log in are sent from PointCentral to the Point client.

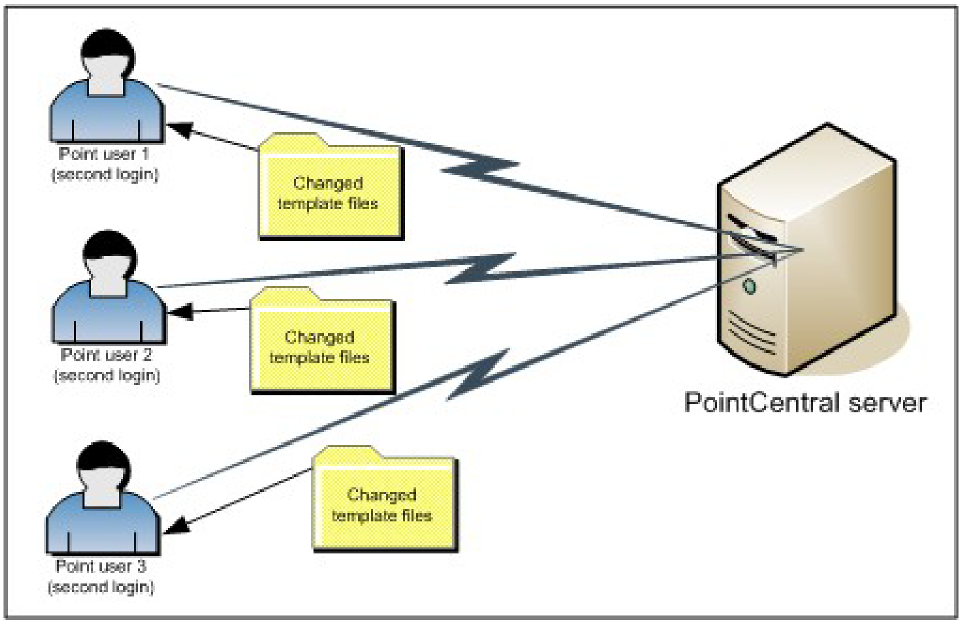


Figure 95: Template Set Distribution

Conventional Template Storage Location

The default directory for storing conventional Point templates is C:\PNTTEMPL on the client machine. The location makes the files unavailable to other Users on a network. Set a network directory as the default location to enable access to template files by authorized Users on the network.

1. Select **Point Administrator** from the *Start* menu.

2. Click **Change Template Directory**.

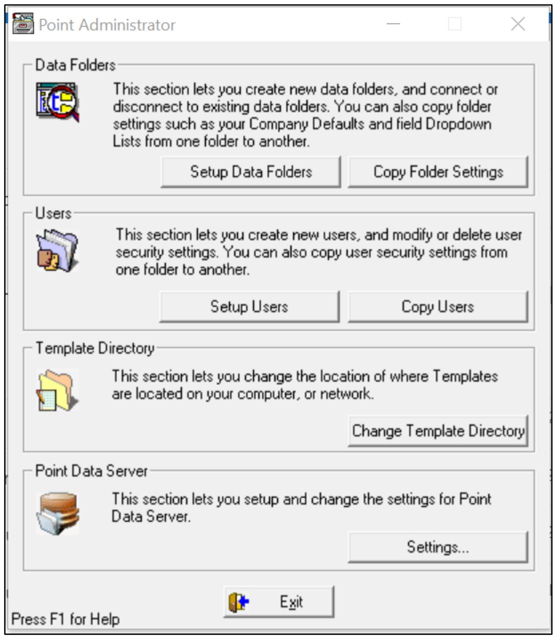


Figure 96: Change Template Directory

3. Click **Change Template Directory**.
4. Enter the new path to store templates.

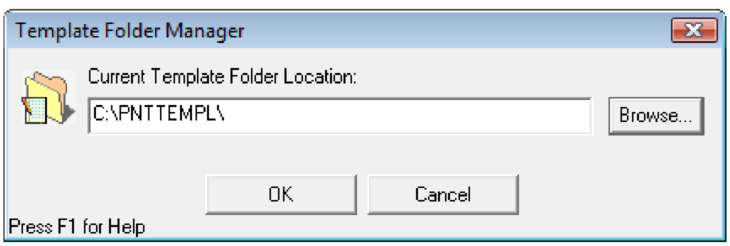


Figure 97: Point Template Folder Manager

Note: Click *Browse* to navigate to the new location.

5. Click **OK**.

See the *Point User Guide* for more details about changing the template file to default locations.

Add Template Sets

Create new template sets or import existing conventional template sets.

1. Select **Add Template Set** from the *Template Sets* menu.
2. Enter a **Template Set Name**.

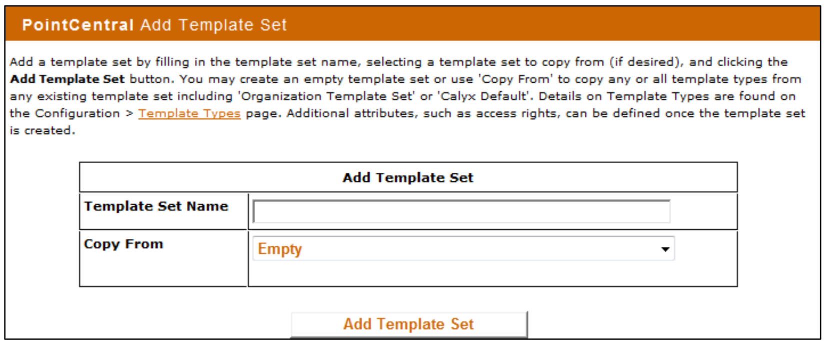


Figure 98: Add Template Set screen

3. Use the following table to determine the appropriate **Copy From option**.

Table 16: Template Set Copy From Options

Option	Description
Empty	Creates an empty template set that does not contain template files.
Calyx Default	Creates a template set from the Calyx default template set included with the PointCentral installation. The template set includes: • Reports • Escrow and title tables • Some custom forms **Note:** The Calyx Default template is read-only. Files cannot be edited.
Organization	The Organization template set is created when PointCentral is installed. The template contains the same files deployed in the Calyx Default template set. Organization templates are editable.

4. Proceed to Edit Template Sets to add template set properties.

Note: Template sets can be copied into an existing system. See Template Sets for details.

Edit Template Sets

Use the following steps to edit a template set.

1. Select **List Template Sets** from the *Template Sets* menu.
2. Click **Edit** to change the template set attributes and assign access rights.

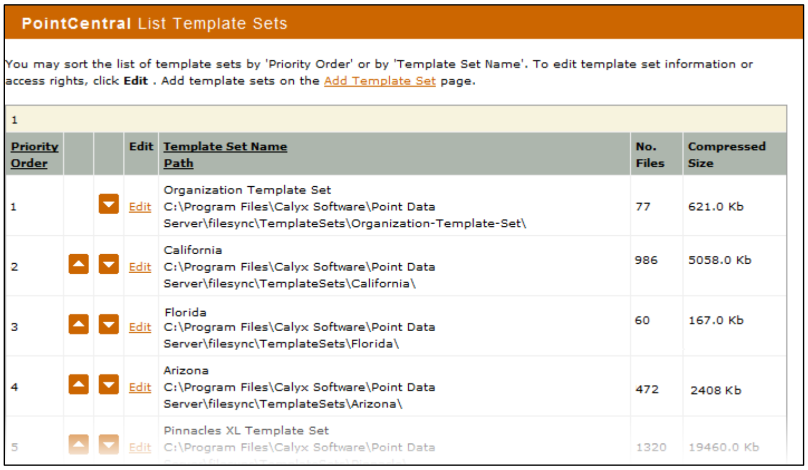


Figure 99: List Template Sets screen

3. Update the **Template Set Name** if applicable.

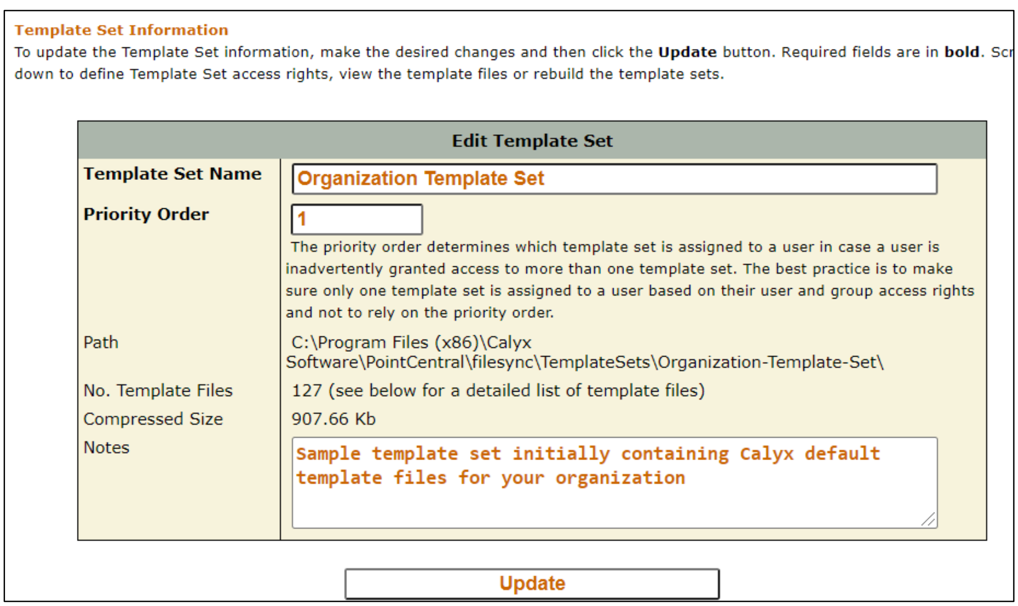


Figure 100: Edit Template Set

4. Set the Priority Order.
5. Enter template **Notes** if applicable.
6. Click **Update**.

Template Set Access Overview

Select a template type to grant read and write access rights. The following table defines access rights in Point when granted in PointCentral.

Table 17: Template Set Access Definitions

Point Option	User Capability
Loan Programs Closing Cost Scenarios Prospect Master Files Borrower Master Files Data Import Templates Data Export Templates Custom Forms Reports	Use and/or view function when selected
Escrow Tables Title Tables Escrow Account HMDA Register Info Docs Due In FHA Consumer Choice Disclosures	Option enabled in **Company Defaults** on **Utilities** menu
Print Groups (Shared)	**Edit Group** and **Delete Group** buttons enabled in the *Prospect*, *Borrower*, *Co-Prospect*, and *Co-Borrower* forms when User selects a shared print group.
Additional Utilities	The following options are available on the **Utilities** menu: • Custom Screen Settings • FHA Consumer Choice Disclosure • GFE/TIL Disclosure • Service Provider List Disclosure • Privacy Policy Disclosure • Condition Types • Fee Types • Impound Types • Document Categories/Types • Stacking Orders

Point Option	User Capability
	• Package Types • Automatic Document Storage • Warehouse Lenders • Investors • Trailing Documents • Docs Due in • Escrow Account
Auto Min Generation	Enables ability to automatically generate the MIN number for loans

Add User Group Access

Use the following steps to set template User Group access.

1. Select List Template Sets from the Template Sets menu.
2. Click the **Edit** for the template set to modify User Group access.
3. Click Add Group Access Rights.

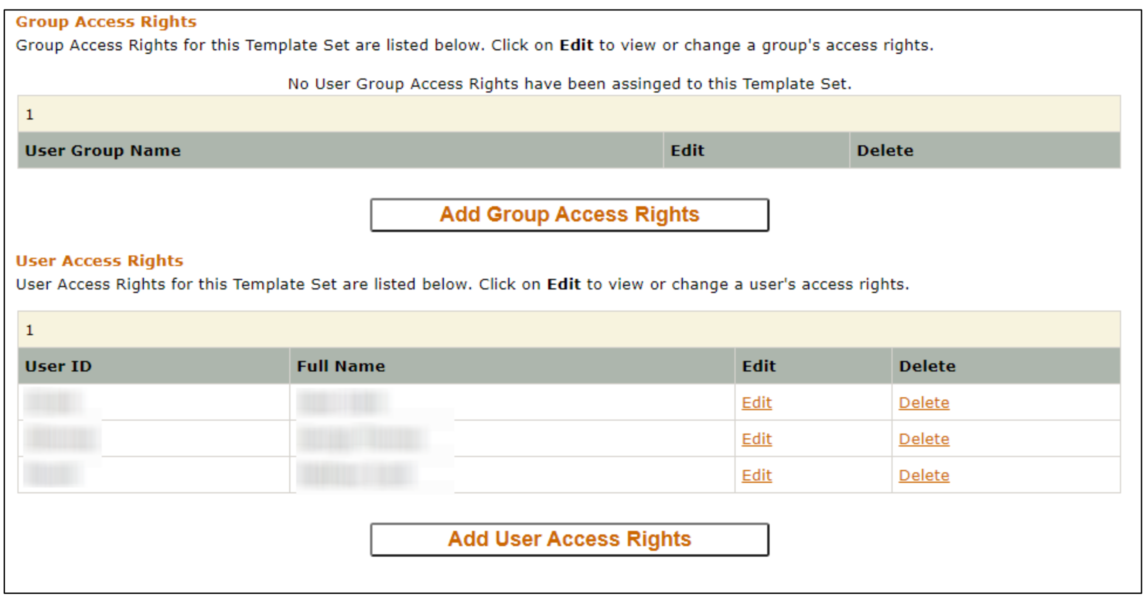


Figure 101: Add Template Group Access

4. Select the appropriate **User Group Name(s)**.

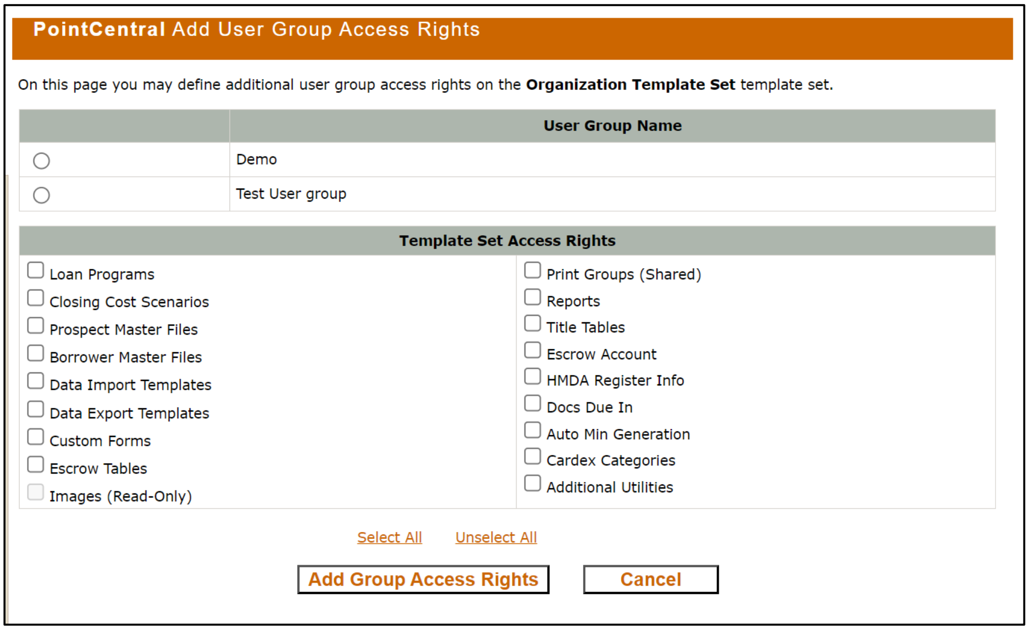


Figure 102: Select User Groups

5. Select the **Template Sets** to grant access.
6. Click Add Group Access Rights.

Note: Access to multiple templates sets can be assigned. The system will only use one template set labeled the effective template set. The effective template set is the set with the highest priority order assigned to the Point User. Assign only one template set to a User to simplify template management.

See Import Template Sets for information about importing a conventional template set.

Add User Access

Use the following steps to set template User access.

1. Select List Template Sets from the Template Sets menu.
2. Click the **Edit** for the template set to modify User group access.
3. Click Add User Access Rights.
4. Select the appropriate **User Group Name(s)**.
5. Select the **Template Sets** to grant access.
6. Click Add Group Access Rights.

Set User Template Set Access

Use the following steps to set User template set access.

1. Select **List Template Sets** from the *Template Sets* menu.
2. Click the **Edit** for the template set to modify User Group access.
3. Click **Add User Access Rights**. (See Figure 99.)
4. Select the User to grant access.
5. Select the **Template Sets** to grant access.
6. Click **Add User Access Rights**.

Rebuilding Template Sets

A list of available template files included in the selected template set are displayed at the bottom of the **Edit Template Set** page.

PointCentral is not aware of the newly copied files until the template set is rebuilt manually copying the files to the template set directory. Rebuilding the template set ensures the compressed archived file that is delivered to first time log in Point Users includes all template files. The rebuild also ensures other Point Users receive these files.

PointCentral also supports the automatic rebuild of template sets once a day. See Template Settings for additional information.

New template data is not available until the organization template set is rebuilt after upgrading to PointCentral. Rebuild the template set manually to access the templates immediately.

1. Select **List Template Sets** from the *Template Sets* menu.
2. Locate the organization template set located at **C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Organization-Template-Set**. (See Figure 96.)
3. Click the corresponding **Edit** link.

4. Click **Rebuild Template Set**.

For a list of template types, see Configuration > Template Set Maintenance > Template Types.

1 2 3 4 5 6 7

File Name	Size (Bytes)	Last Update	Template Type
00000000.ELP	207	4/23/2019 1:46:06 PM	Escrow Tables
00000000.TOP	208	4/23/2019 2:01:07 PM	Title Tables
1211212.RPT	6583	6/12/2019 1:41:41 PM	Reports
1509.RPT	4560	2/20/2019 8:03:05 PM	Reports
2729 Test.imp	66	10/8/2019 11:00:27 PM	Data Import
2729.RPT	3460	10/3/2019 9:04:17 PM	Reports
5760.RPT	3848	1/23/2019 9:59:20 PM	Reports
6029 test.RPT	3854	5/7/2019 7:19:29 PM	Reports
7336.RPT	3832	11/23/2019 12:12:45 AM	Reports
94 test.CCS	5467	4/29/2019 2:58:23 PM	Closing Cost Scenario
A Copy of test.ccs	2548	4/29/2019 2:58:23 PM	Closing Cost Scenario
American.elr	8564	7/23/2012 1:12:12 PM	Escrow Tables
American.tlr	19699	7/23/2012 1:12:08 PM	Title Tables
Calyx Business Analysis for Banker.xls	122368	4/1/2013 2:31:54 PM	Reports
Calyx Business Analysis Summary.xls	634368	4/1/2013 2:31:54 PM	Reports
Calyx Funded and Not Shipped.xls	36352	4/1/2013 2:31:54 PM	Reports
Calyx Loan Pipeline.xls	81920	4/1/2013 2:31:54 PM	Reports
Calyx Loan Profit Summary.xls	395264	4/1/2013 2:31:54 PM	Reports
Calyx Marketing - Address Labels (Property Address).RPT	9779	7/23/2012 1:12:10 PM	Reports
Calyx Marketing - Address Labels by Property Address.RPT	9799	8/28/2008 1:43:52 PM	Reports

Rebuild Template Set

Figure 103: Manual Template Sets Rebuild

5. Click **Yes** on the *Confirmation* prompt.
6. Select the **Status** menu option to view the **Rebuild** status.

Note: The new templates are available for use after the *Status* screen indicates the rebuild is complete.

Copy Template Sets

Use the following steps to copy files from an existing template set.

1. Select **Template Set Maintenance** from the *Configuration* menu.
2. Select **Copy Template Set**.
3. Select the source template set from the **Copy From dropdown list.**

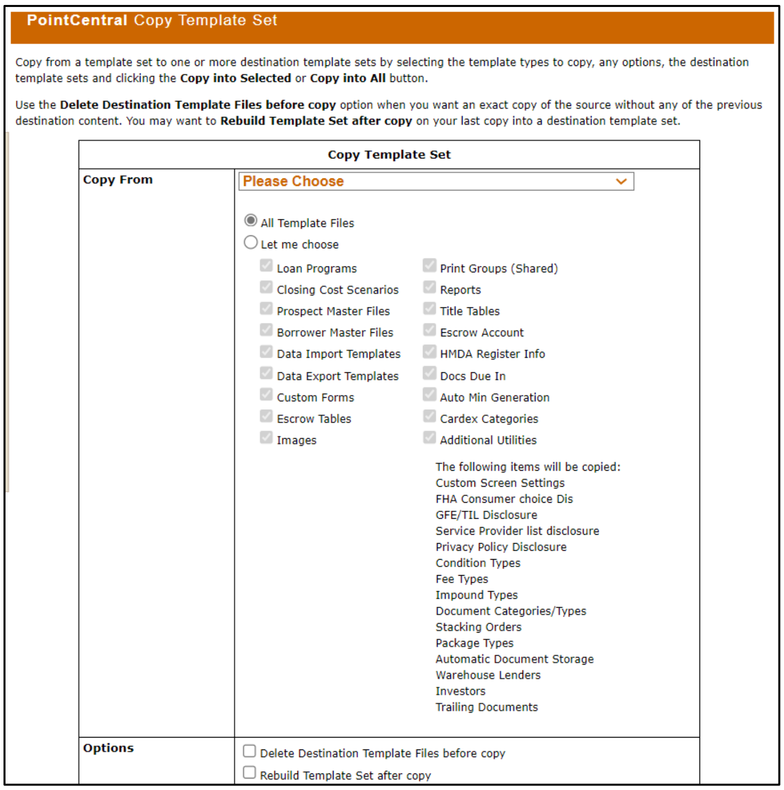


Figure 104: Copy Template Set

4. Select the **Copy From** option.
5. Select the **Template Files** to copy.
6. Select **Delete Destination Template Files** before copying to remove any existing files from the destination template set.

Note: Deleting the existing files synchronizes the two template sets.

7. Select **Rebuild Template Set** after copy to rebuild the template set after the template files are copied.
8. Select one or more destination template sets.
9. Click **Copy into Selected**.
10. Click the **Status** link to view the status of the copy process.

Convert Template Sets to Conventional

Use the following options to convert template sets to conventional templates.

1. Select **Template Set Maintenance** from the *Configuration* menu.
2. Select **Switch To Conventional**.
3. To convert individual template sets, click the link that corresponds to that template set. To convert all template sets, click the **Switch All to Conventional** button.

PointCentral Switch Template Set To Conventional

To sort the list of Template Sets, click the column title. If you want to completely remove a template set from PointCentral, switch it to a conventional template set by clicking on **Switch To Conventional**. Switching a template set to conventional causes a loss of the access rights defined in PointCentral for that template set since conventional template sets do not support PointCentral Users, User Groups and other PointCentral features.

1

Order	Name	Path	Switch to Conventional
1	Organization Template Set	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Organization-Template-Set\	Switch to Conventional

Figure 105: Convert Template Set

4. Click **Yes** on the *Confirmation* prompt.

Cardex Databases

The Cardex database for Point is an electronic database that contains information about companies Users interact with when processing loan files. Use Cardex entries to populate Point company name and address fields. Create a Cardex database from information already entered Point fields or by entering manually.

Centralizing Cardex Databases

Centralize the location of Cardex within the template directory by using Windows Network Share in conventional Point.

Example: It's possible to change the folder location to \\MYFILESERVER\PNTTEMPL in PointCentral. This option is unreliable in environments with low bandwidth or high latency.

Use PointCentral to centralize the Cardex database and make it available to Point Users automatically without VPN. Define the multiple Cardex databases and provide access rights to different groups or Users accordingly.

Cardex databases are stored in the PointCentral database to enable Point clients to access the database entries from a central location quickly (even from large Cardex databases). The User defined Cardex categories are stored with the templates.

The PDS suffix for Cardex files on the **Cardex Database** dialog title indicates access rights to Point Users. Users without access rights to a Cardex database default to the conventional Cardex in the Point **Template Directory**.

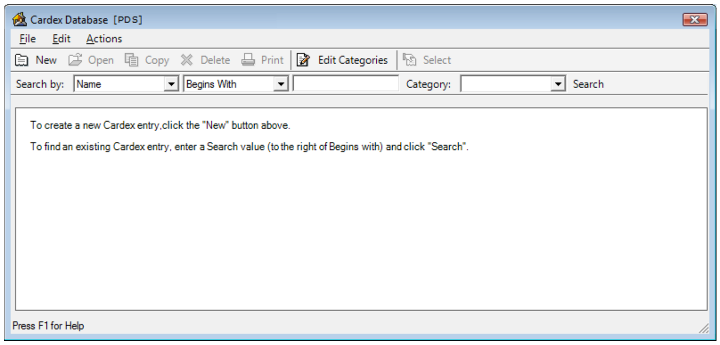


Figure 106: Point Cardex Database Dialog

Conventional Cardex Database Storage

Set a network directory as the default location for storing templates to enable authorized network access to the Cardex databases.

Note: See Template Settings for additional information.

Add Cardex Databases

Use the following steps to add Cardex databases.

1. Select **Add Cardex Database** from the *Cardex Databases* menu.
2. Enter Cardex database **Name**.

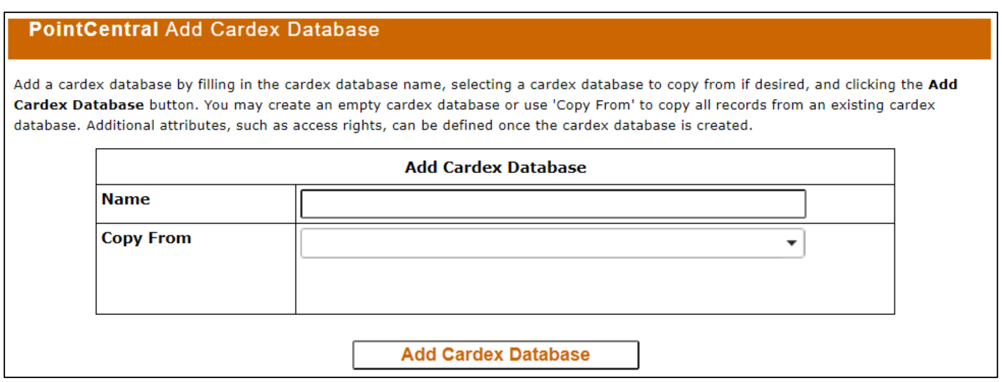


Figure 107: Add Cardex Database Screen

3. Select the database name from the **Copy From** dropdown to copy data from an existing database to the new database.
4. Click **Add Cardex Database**.
5. Proceed to Edit Cardex Database to enter database properties.

Edit Cardex Database

Use the following steps to edit an existing Cardex database.

1. Select **List Cardex Databases** from the *Cardex Databases* menu.

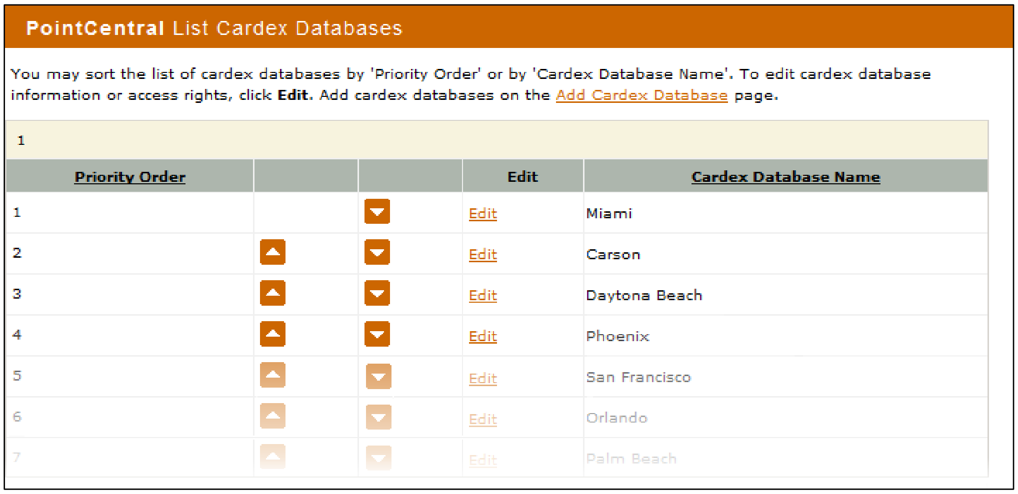


Figure 108: List Cardex Databases screen

2. Click **Edit** next to the database to edit.

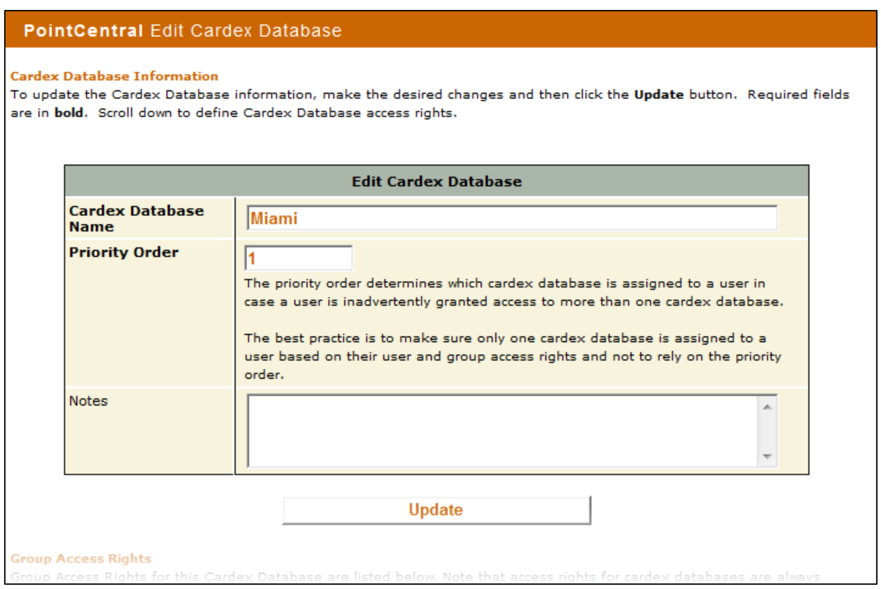


Figure 109: Edit Cardex Database

3. Update the **Cardex Database Name** if applicable.
4. Set the **Priority Order**.
5. Enter database **Notes** if applicable.

Add User Group Access

Use the following steps to set *User Group* access to a *Cardex Database*.

Note: Read/Write access is the only option for a Cardex database.

1. Select **List Cardex Databases** from the *Cardex Databases* menu.
2. Click **Edit** next to the database to edit. (See Figure 105.)
3. Click **Add Group Access Rights**.

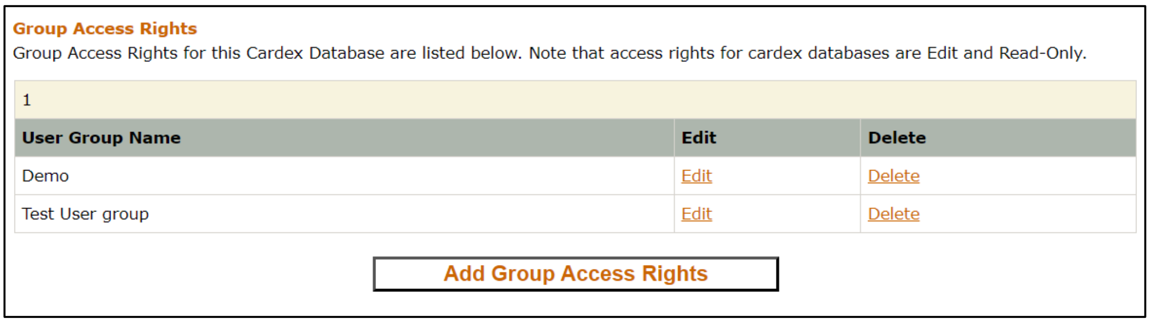


Figure 110: Edit Cardex Database Access

4. Select the groups to grant access to the Cardex database.

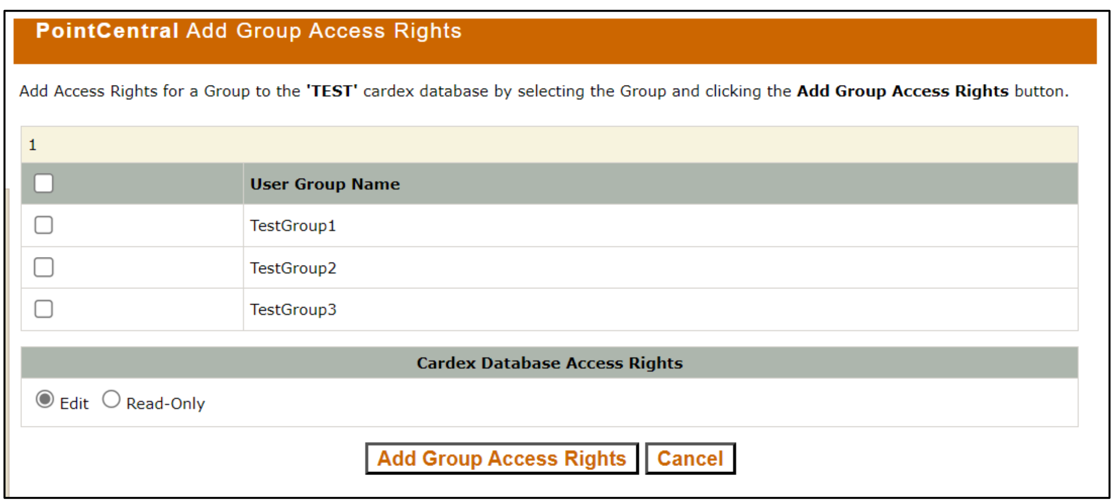


Figure 111: Add Cardex Database Access

5. Click **Add Group Access Rights**.

Edit User Group Access

Cardex Database allows users to edit group access rights. Use the steps below to edit the User Group Access for the Cardex Database.

To edit group access rights:

1. Select **Cardex Databases** > **List Cardex Databases**.
2. Select the **Edit** link for the desired *User Group*.
3. In the *Group Access Rights* section, select the **Edit** link.

Figure 112: Edit Link for Cardex Access Rights

4. Select either the **Edit** or the **Read-Only** option.

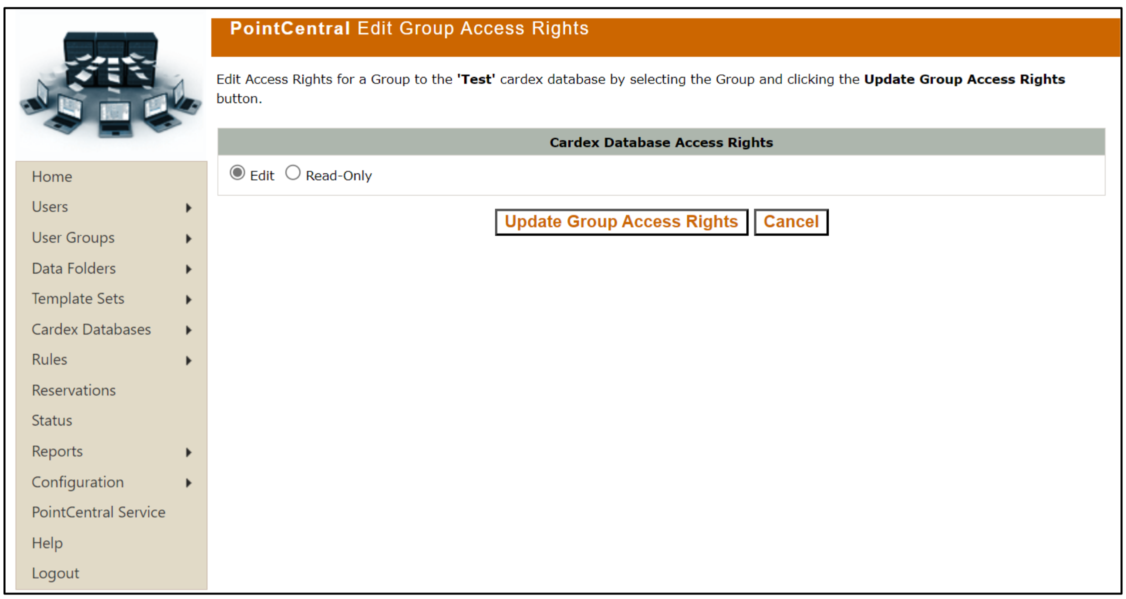


Figure 113: Edit Group Access Rights

5. Click on the **Update Group Access Rights** button.
6. Select **Cancel** to Return to the *List Cardex Database* screen.

Add User Access

Use the following steps to User access to the *Cardex* database.

Note: Read/Write access is the only option for a Cardex database.

1. Select **List Cardex Databases** from the *Cardex Databases* menu.
2. Click **Edit** next to the database to edit. (See Figure 105.)
3. Click **Add User Access Rights**.
4. Select the Users to grant access to the Cardex database.
5. Click **Add User Access Rights**.

Edit User Access Rights

Cardex Database allows users to edit group access rights. Use the steps below to edit the User Group Access for the *Cardex Database*.

To edit group access rights:

1. Select **Cardex Databases** > **List Cardex Databases**.
2. Select the **Edit** link for the desired *User Group*.
3. In the *Group Access Rights* section, select the **Edit** link.

Figure 114: Editing Cardex User Access Rights

4. Select the **Edit** or the **Read-Only** option.

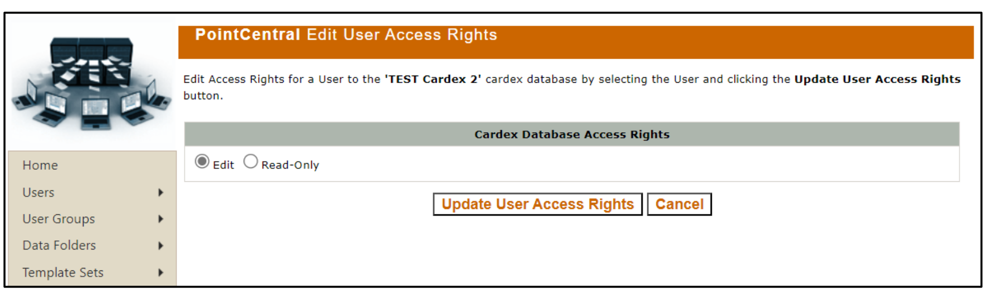


Figure 115: Edit User Access Rights

5. Click on the **Update User Access Rights** button.
6. Click on **Cancel** to return to the *List Cardex Database* screen.

Delete Cardex Databases

Use the following steps to delete a Cardex database.

1. Select **Delete Cardex Database** from the *Configuration* menu.
2. Click the **Delete** for Cardex database to delete.

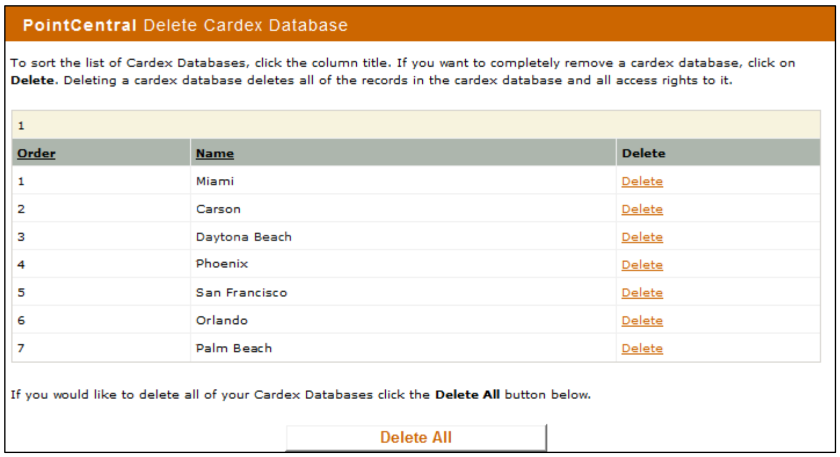


Figure 116: Delete Cardex Database Screen

3. Click **Yes** on the *Delete Confirmation*.

Convert Cardex Databases

PointCentral Cardex databases are exclusively stored in the PointCentral database. The process for exporting PointCentral Cardex databases and converting them to conventional Point databases involves exporting the PointCentral database from Point and importing it back into conventional Point.

Export from Point

Use the following steps to export the Cardex database from Point.

1. Log in to Point as a User with access rights to the Cardex database to export.
2. Select **Cardex Database** from the *Utilities* menu.
3. Select **Export** from the *Cardex Database File* menu.

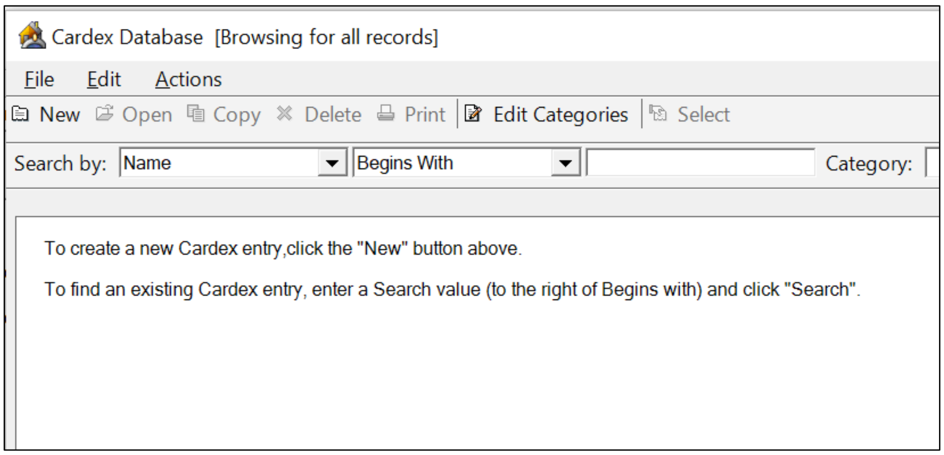


Figure 117: Point Cardex Database Dialog

4. Verify the information on the *Export Customer ASCII* dialog.

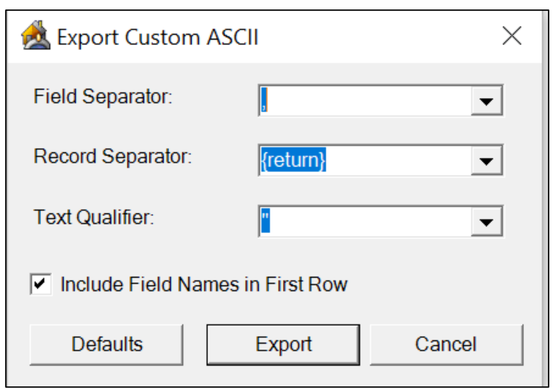


Figure 118: Export Customer ASCII Dialog

5. Click **Export**.
6. Use the *Export Cardex* dialog to browse to the location to save the file.
7. Enter a file name.
8. Click **Save**.
9. Close open Point dialogs.
10. Log out of Point Central.

Import Database to Point

Use the following steps to import the Cardex database to Point.

1. Log in to conventional Point.
2. Select **Cardex Database** from the *Utilities* menu.
3. Select **File > Import** on the Cardex Database dialog. (See Figure 110.)
4. Select the **Other Cardex** file on the *Import* dialog.

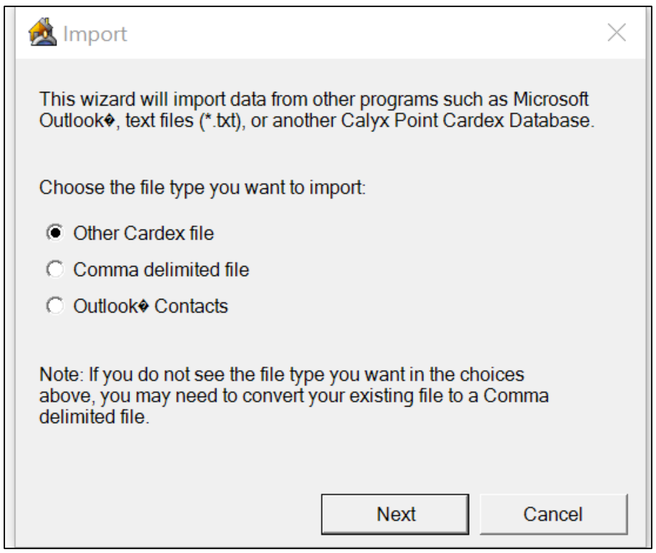


Figure 119: Import Dialog

5. Click **Next**.
6. Use the **Browse** button on the *Import Source* dialog to locate the file.

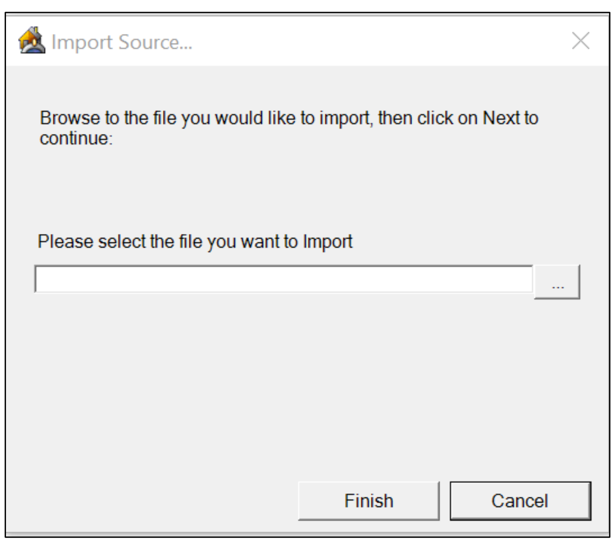


Figure 120: Import Source Dialog

7. Select the file.
8. Click **Finish**.

Note: Refer to the *Point User Guide* for more information about importing and exporting Cardex databases.

Rules

Rules are used to define parameters to control available fields, display messages, or require input into specific fields before the User can proceed with certain tasks. Rules are used to compare dates and other numeric values against expected values and the values in field IDs. Updated rules are downloaded from PointCentral to Users and User Groups when logging into Point or mobile devices. Rules are applied to Users and User Groups in PointCentral much like Users and User Groups are given access to data folders.

Note: PointCentral is supplied with a set of default rules.

Rule Types

The following table provides a description of the available *Rule Types*.

Table 18: Rule Types

Rule Type	Description
Disable Fields	Makes field unavailable for Users or User Groups **Note:** Disabled fields are read-only and cannot be edited by the User.
Required Fields	Defines fields that must contain data before the Point User can save or print the form. **Note:** A prompt displays input is required data is missing in a required field when the User attempts to save a loan file.
Custom Message	Define as rule that contains a custom message. **Note:** Indicate to the Point User to complete a task or stop and satisfy the rule conditions before they can proceed, etc.
State Licenses	Defines a rule based on the state where the Point User is licensed to originate loans. **Note:** The User cannot save, print, or e-mail a form or save a form with data to the document repository in a loan file with a property in a state that is not enabled in the rule. State license rules apply to the User regardless of the data folder where the loan resides.

Rule Activation

Rule Types activate when a Point User performs one of the following actions:

- Saves a loan file by clicking the **Save** icon or by selecting **Save** from the **File** menu.
- Initiates an action from the *Prospect Forms* or *Borrower Forms* to:
  - Print a form.
  - Save or e-mail a form in PDF format.
  - Store a form in the document repository when the Form with data option is selected from the **Print Option** dropdown.
- Clicks the following buttons:
  - Create **Registration Request** on the Registration & Rate Lock screen.
  - Create **Lock Request** on the *Registration & Rate Lock* screen.
  - Create **Lock Confirmation** on the *Secondary Marketing* screen.
  - Create **Suspense/Denial Notice** on the *Underwriting* screen.
  - Create **Loan Approval Notice** on the *Conditions* screen.
  - Create **Funding Conditions Notice** on the *Conditions* screen.
  - Create **a Funding Figures Worksheet** on the *Fees & Impounds* screen.

A notification dialog displays and the required fields with missing data are highlighted in red. The Point User attempts one of these actions in a screen with empty required fields and the **Rule Conditions** apply. The User is unable to complete the action until they enter data in the required fields.

The rule does not run when the following actions are performed:

- When a services interface request is submitted or transaction is completed.
- When a web-based interface is launched or transaction is completed.
- When a Fannie Mae DO/DU request is submitted or transaction is completed.
- When a Freddie Mac Loan Prospector request is submitted or transaction is completed.
- When the User is working in or switching to a co-borrower file.

Note: The above activation information does not apply to the *Disable Fields* rule. The *Disable Fields* rule requires not User interaction to be initiated.

Rule Conditions

Conditions dictate how a rule is applied. Many of the rules contain multiple conditions that must be met before the rule is triggered.

Example: Create a disable fields rule that contains a list of fields to be disabled and a condition that the rule applies when the **Lock Confirmed** field contains a date to prevent Users from changing certain field values in a loan file after the loan is locked.

The rule defines the fields the User cannot edit. The condition defines the field that requires data for the rule to apply. These constraints apply to all loan files that meet the rule criteria and the conditions defined.

The following table defines the condition examples.

Table 19: Condition Examples

Option	Definition
After	Triggers the rule when the value in the named field is after the specified value.
After or Equal	Triggers the rule when the value in the named field is after or the same as the specified value.
After Today	Triggers the rule when the date in the named field is the date after the current date.
Before	Triggers the rule when the value in the named field is before the specified value.
Before or Equal	Triggers the rule when the value in the named field is before or the same as the specified value.
Before Today	Triggers the rule when the date in the named field is the day before the current date.
Contains	Triggers the rule when the named field contains the specified value.
Decreased by % Decreased by Amount	Triggers the rule when the value in the named field decreases by the specified value.
Equal	Triggers the rule when the value in the named field is the same as the specified value.
Greater Than	Triggers the rule when the value in the named field is greater than the specified value.
Greater Than or Equal	Triggers the rule when the value in the named field is greater than or equal to the specified value.
Increased by % Increased by Amount	Triggers the rule when the value in the named field increases by the specified value.
Is Blank	Triggers the rule when the value in the named field is blank.
Is Not Blanks	Triggers the rule when data is entered in the named field.
Last Month	Triggers the rule when the date in the named field is in the previous month.

Option	Definition
Last Year	Triggers the rule when the date in the named field is in the previous year.
Less Than	Triggers the rule when the value in the named field is less than the specified value.
Less Than or Equal	Triggers the rule when the value in the named field is less than or equal to the specified value.
Not Equal	Triggers the rule when the value in the named field is not equal to the specified value.
This Month	Triggers the rule when the date in the named field is in the current month.
This Year	Triggers the rule when the date in the named field is in the current year.
Today	Triggers the rule when the date in the named field is the current day.

Add Rules

Use the following steps to add a new rule.

1. Select **Add Rule** from the *Rules* menu.
2. Enter a unique rule **Name**.

Figure 121: Add Rule Screen

3. Select a rule from the **Copy From** dropdown to copy the parameters from an existing rule.
4. Click **Add Rule**.

5. Select the **Disable Rule** checkbox to prevent rule application.

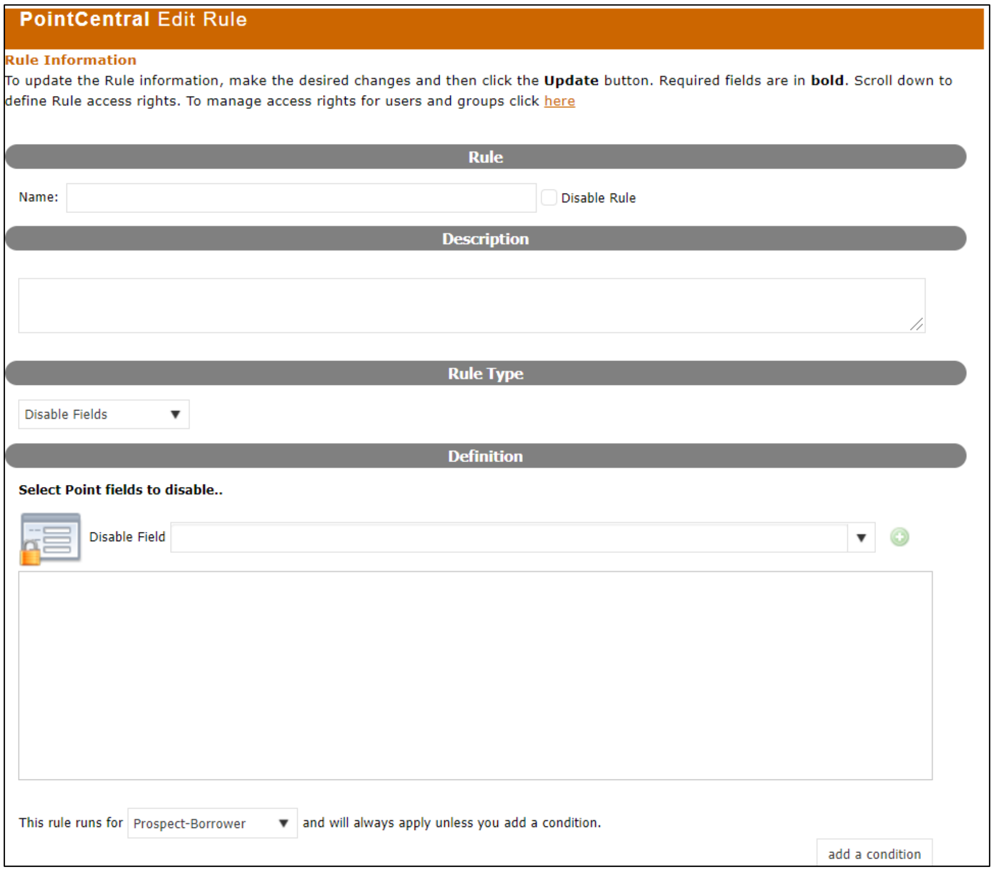


Figure 122: Edit Rule

6. Enter a Rule **Description**.
7. Use the appropriate link to select a **Rule Type**:
   - Disable Fields Rule
   - Required Fields Rule
   - Custom Message Rule
   - State Licenses Rule

Note: The information that is entered in the *Definition* section depends on the selected rule type.

Disable Fields Rule

The *Disable Fields* rule runs when a loan file is opened or saved and the Point User accesses a different screen in a loan file. Fields are disabled based on the conditions of the rule.

Note: Disabled fields in dialogs are exempt from the rule and are enabled to the User. Disabled fields are overwritten when data is imported into the loan file.

1. Select the **Disable Rule** from the *Rule Type* dropdown. (See Figure 115.)
2. Select the field name from the **Disable Field** dropdown.

Note: Manually start entering the name until it appears in the dropdown.

3. Click the **Plus Sign (+)** to add the field to the *Field List***.**

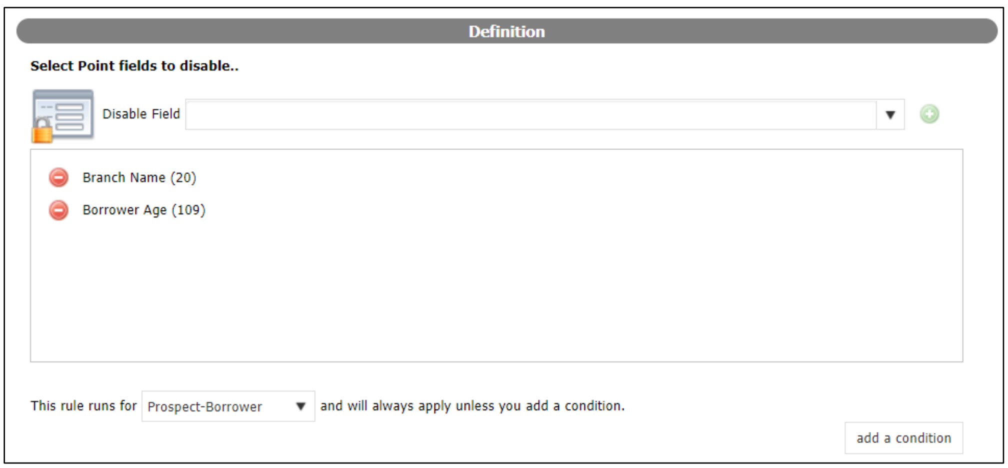


Figure 123: Disable Field List

4. Repeat Steps 2 – 3 to select additional fields.
5. Proceed to Add Rule Conditions to apply conditions to the selected fields.

Required Fields Rule

Use the following steps to create the **Required Fields** rule.

1. Select the **Required Fields Rule** from the *Rule Type* dropdown. (See Figure 115.)
2. Select the field name from the **Require Field** dropdown.

Note: Manually start entering the name until it appears in the dropdown.

3. Click the **Plus Sign (+)** to add the field to the *Field List*.

Figure 124: Definition Fields List

4. Repeat Steps 3 – 4 to select additional fields.
5. Proceed to [Add Rule Conditions] to apply conditions to the selected fields.

Custom Message Rule

Use the following steps to create the **Custom Message** rule.

1. Select **Custom Message** from the *Rule Type* dropdown.

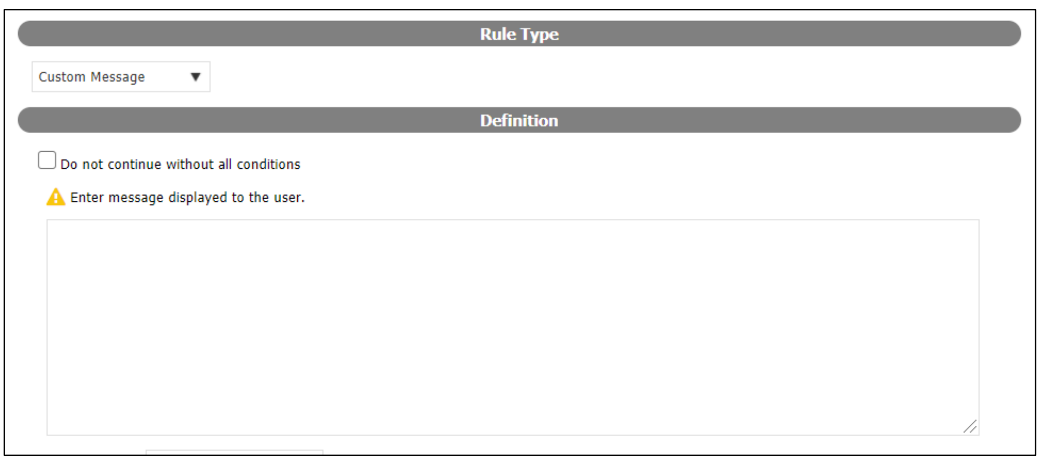


Figure 125: Customer Message Rule

2. Select the **Do not continue without satisfying all conditions** checkbox to prevent the Point User from continuing if all conditions are not met.
3. Enter the message to display to the User when the rule and conditions in the open field.
4. Proceed to [Add Rule Conditions] to apply conditions to the selected fields.

State Licenses Rule

Use the following steps to create the **State License** rule.

5. Select **State License** from the **Rule Type** dropdown list.

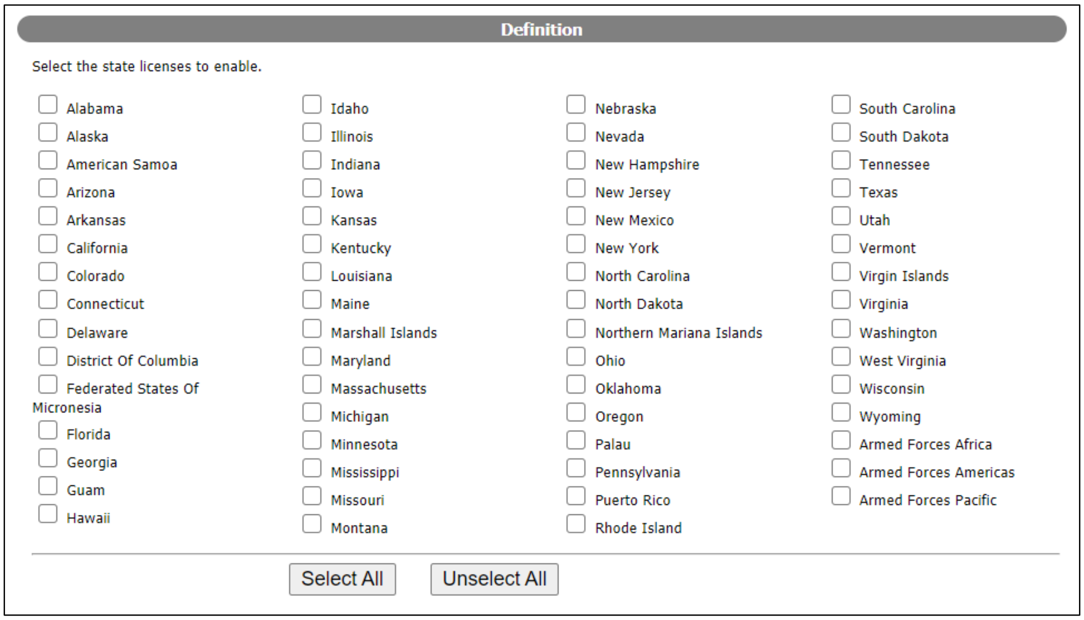


Figure 126: State License Definition List

6. Select the checkboxes that correspond to the states and territories where the User is licensed to process loans.
7. Click **Update Rule**.
8. Proceed to Rule Conditions.

Note: *Rule Conditions* are not available for *State License* rules.

Add Rule Conditions

Use the following steps to add conditions to the selected rules.

1. Select the **File Type** for which the rule runs from the dropdown.

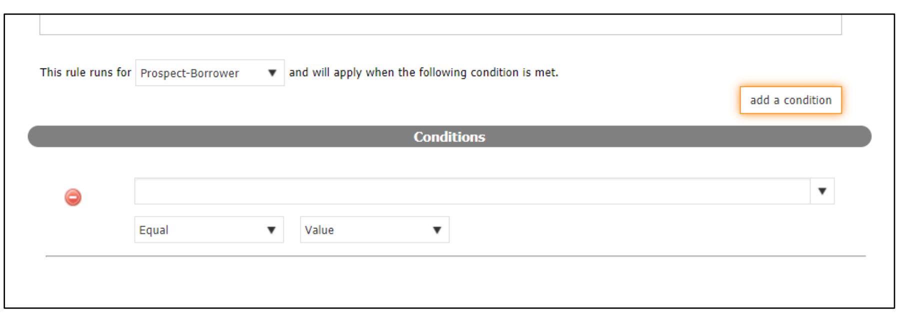


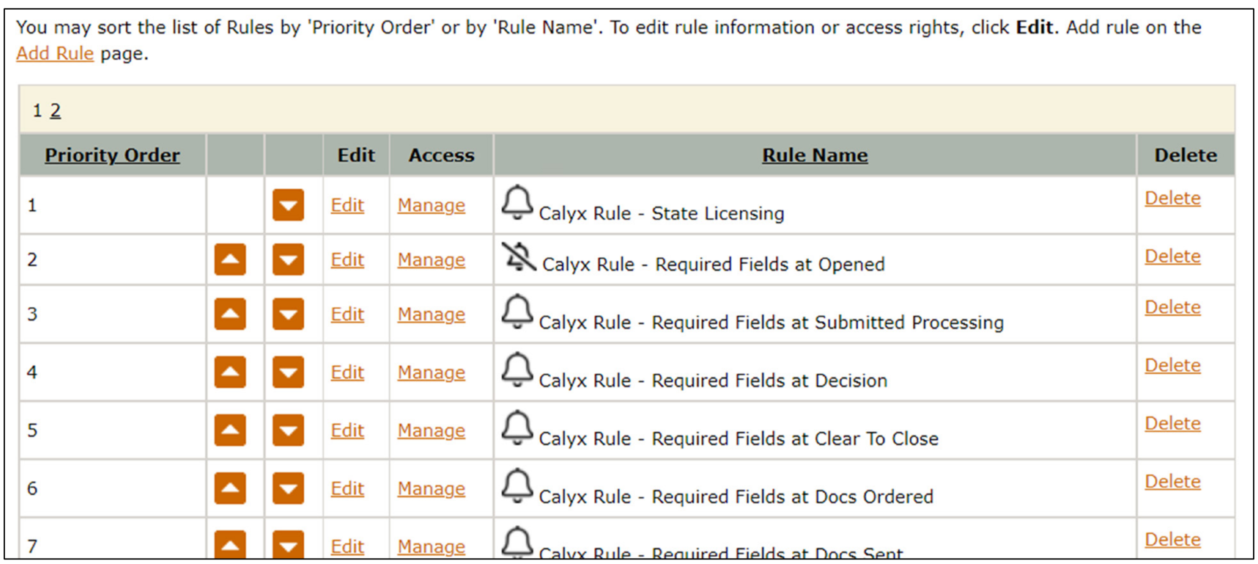
Figure 127: Add Condition

2. Click **Add Condition**.
3. Select the field to disable from the **Condition** dropdown.
4. Select the appropriate **Equal** option from the dropdown.
5. Select the **Value** option from the dropdown if applicable.
6. Click **Add a Condition** to add more conditions to the rule.
7. Repeat Steps 7 – 10 for additional conditions.
8. Repeat Steps 5 – 10 for other fields in the **Fields List**.
9. Click **Update Rule** at the bottom of the screen when complete.

Add User Groups Access

Use the following steps to set *User Group* access to a rule.

1. Select **List Rules** from the *Rules* menu.
2. Select the **Rule** to grant access.



You may sort the list of Rules by 'Priority Order' or by 'Rule Name'. To edit rule information or access rights, click **Edit**. Add rule on the Add Rule page.

1 2

Priority Order			Edit	Access	Rule Name	Delete
1			Edit	Manage	Calyx Rule - State Licensing	Delete
2			Edit	Manage	Calyx Rule - Required Fields at Opened	Delete
3			Edit	Manage	Calyx Rule - Required Fields at Submitted Processing	Delete
4			Edit	Manage	Calyx Rule - Required Fields at Decision	Delete
5			Edit	Manage	Calyx Rule - Required Fields at Clear To Close	Delete
6			Edit	Manage	Calyx Rule - Required Fields at Docs Ordered	Delete
7			Edit	Manage	Calyx Rule - Required Fields at Docs Sent	Delete

Figure 128: Rules List

3. Click **Edit User Access** at the bottom of the screen.

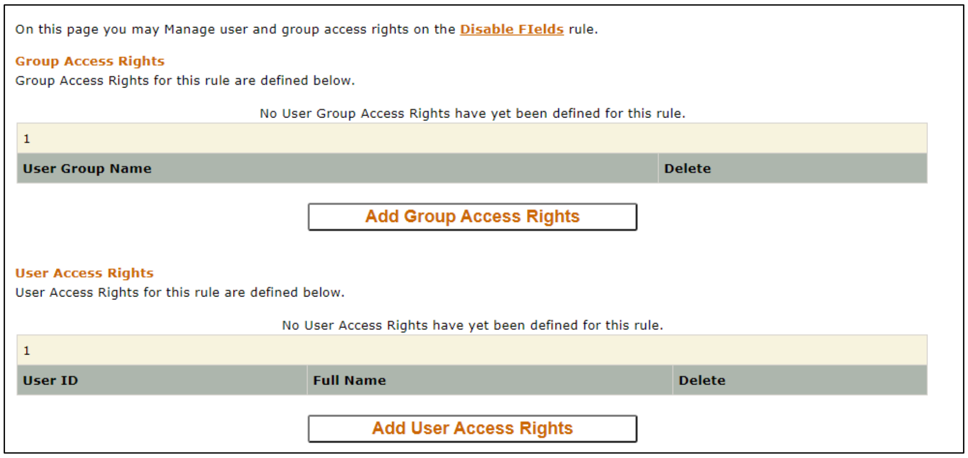


Figure 129: Edit Rules Access

4. Select the group(s) to grant access to the rule.

Figure 130: Edit Rules Add Group Access

5. Click **Add Group Access Rights**.

Add Users Access

Use the following steps to set User access to a rule.

1. Select **List Rules** from the *Rules* menu.
2. Select the **Rule** to grant access.
3. Click **Edit User Access** at the bottom of the screen.
4. Select the User to grant access to the rule.
5. Click **Add User Access Rights**.

Edit Rules

Use the following steps to edit the rules.

1. Select **List Rules** from the *Rules* menu.

2. Select the rule to edit from the **Rules List**. (See Figure 121.)

Note: Enabled rules will display the bell icon before the Rule Name. Disabled rules display the bell icon with a diagonal line. (See Figure 121.)

Reorder Rules

Click the *Up* or *Down Arrow* for the rule until positioned in the appropriate list location. (See Figure 121.)

Edit Rule Properties

Use the following steps to edit rule properties.

1. Click **Edit** for the rule to modify. (See Figure 121.)
2. Select the **Disable Rule** checkbox to disable the rule if applicable.

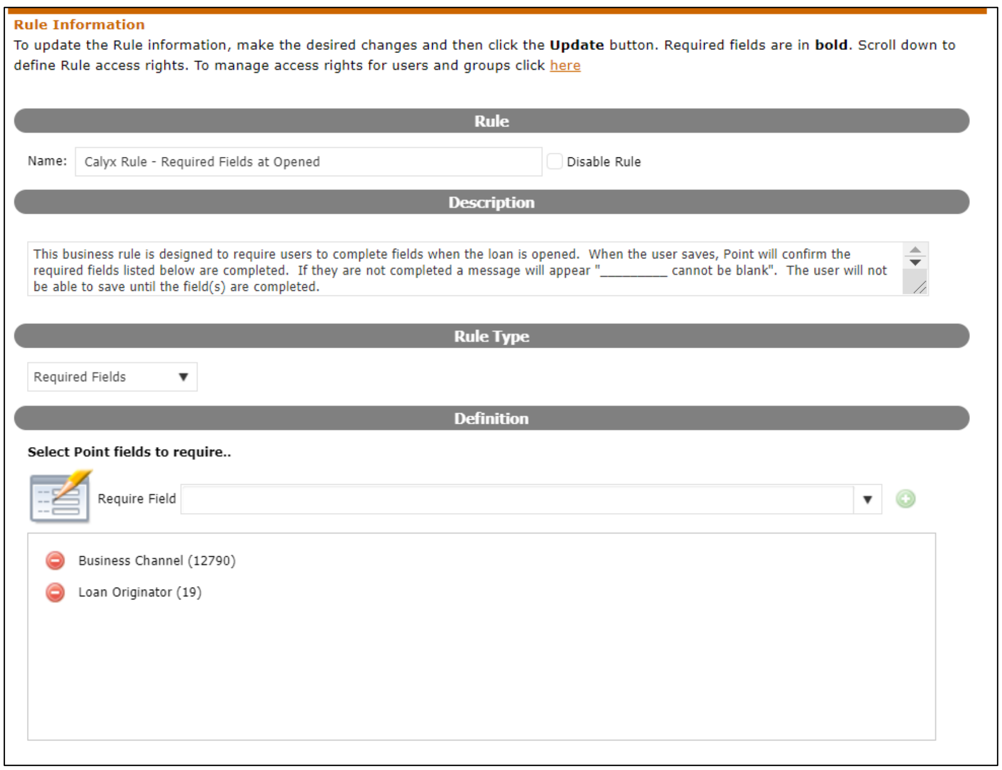


Figure 131: Edit Rule Properties

3. Select a **Role Type** if applicable.
4. Select a **Require Field** from the *Definitions* dropdown to add another field to the rule.
5. Select the **Minus (-)** sign for a rule in the **Rule List** to remove it from the rule.
6. Select a different **File Type** from the dropdown if applicable.

7. Click **Add Condition** and add another condition if applicable.
8. Click the **Minus(-)** sign for a listed condition to remove.
9. Click **Update Rule** at the bottom of the screen when complete.

Edit Rule User Groups and Users

Use the following steps to edit User Groups or Users.

1. Select **List Rules** from the **Rules** menu.
2. Click **Edit User Access** at the bottom of the screen.
3. Click Add **Group Access Rights** to add or remove User Groups from the rule.
4. Click **Add User Access Rights** to add or remove Users from the rule.

Delete Rules

Use the following steps to delete rules.

1. Select **List Rules** from the **Rules** menu.
2. Click **Delete** next to the rule to delete.
3. Click **Yes** on the *Delete Confirmation*.

Import Resources

PointCentral has a utility that imports existing data from conventional Point.

The following items can be imported to PointCentral:

- Cardex database (See Import Database to Point.)
- Data Folders
- Template Sets
- Users From File
- Users From Folder

Import From Cardex Database

Use the Cardex Database option to import Point Cardex into one or more PointCentral Cardex.

To Import from a Cardex Database:

1. Select **Configuration** > **Import** > **Cardex Database**.
2. Select the desired Cardex Database Names.

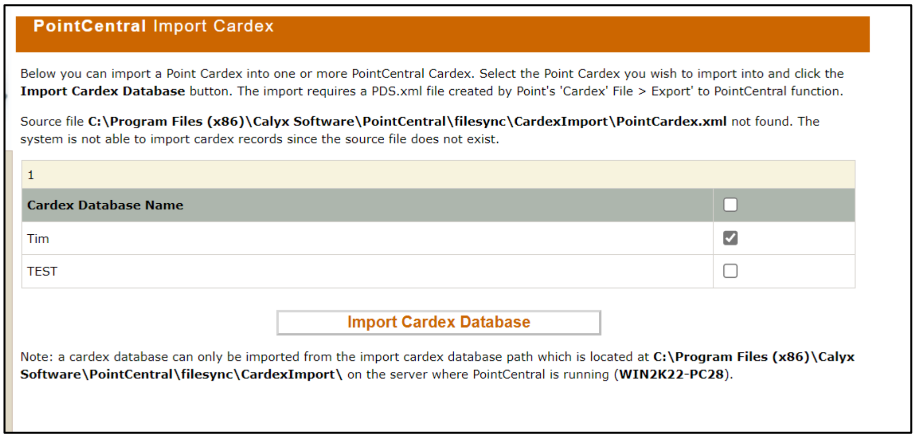


Figure 132: Import Cardex

3. Click **Import Cardex Database**.

Import Data Folders

PointCentral performs the following when importing a conventional data folder from Point:

- Create the data folder.
- Synchronize all the data folder loans to ensure that information about supported, custom, and additional fields is properly updated in the SQL database.
- Initiates data folder monitoring for any changes in the loan (*.BRW or *.PRS) files.

Use the following steps to import data folders.

1. Select **Parameters** from the *Configuration* menu.
2. Scroll to the **Root Folder Path** section.

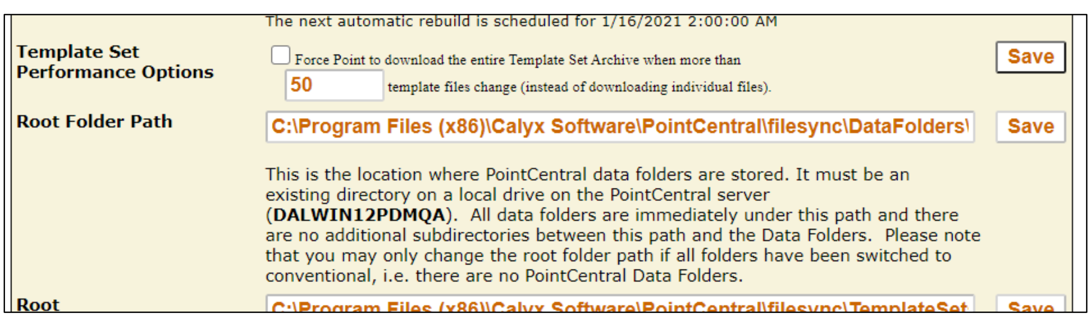


Figure 133: Root Folder Path

3. Make a note of the root folder path.

Note: This is the location where PointCentral data folders are stored. All data folders are stored in this location. There are no additional subdirectories between this path and the data folders.

4. Open **Windows Explorer** window.
5. Navigate to the current location of conventional Point data folders.
6. Copy the folders.
7. Paste them in the noted root folder.
8. Select **Import** from the *Configuration* menu.
9. Select **Data Folders** to display the list of folders in the *Root Folder Path* not yet imported into PointCentral.

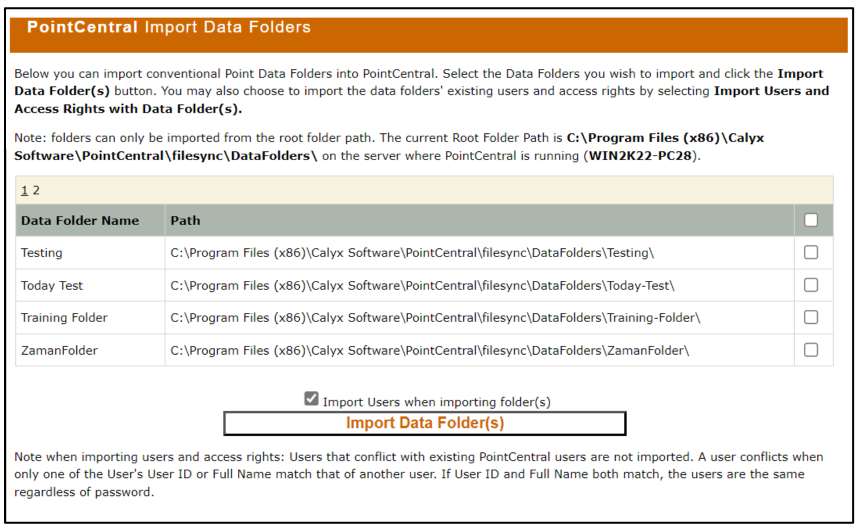


Figure 134: Import Data Folders

10. Select the checkboxes that correspond to the folders to import.
11. Click **Import Data Folder(s)**.
12. Click **Yes** on the *Confirmation Message* to initiate the import.

Note: The status changes to *Done* when the import is complete.

Import Template Sets

Template sets in conventional Point are a collection of folders that contain a different template type (such as: a folder named **CCS** contains closing cost scenarios, a folder named **Loan Prog** contains loan programs). The template sets are stored in the **PNTTEMPL** directory located on a client PC or local server.

PointCentral creates the template set in PointCentral and scans and synchronizes all template files during import. PointCentral builds the archived template set the first time a Point User logs in. The template types that are supported by PointCentral are added to a template set. An imported *Template Set* is named nnnn (where nnnn is a sequential number assigned by PointCentral). Change the template set name manually after the import is complete.

Use the following steps to import conventional template sets.

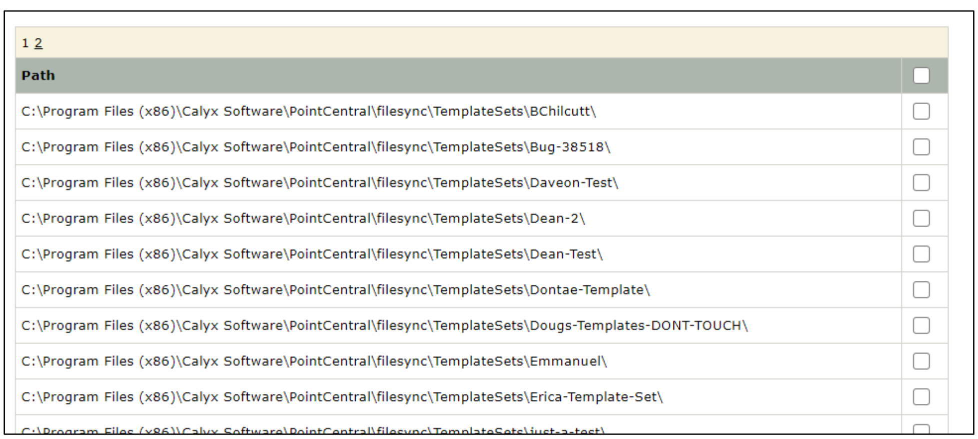
1. Select **Parameters** from the *Configuration* menu.
2. Scroll to the **Root Folder Path** section. (See Figure 125.)
3. Make a note of the root folder path.
4. Open a **Windows Explore** window.
5. Navigate to the current location of conventional Point data folders.

Note: Template sets are typically located in *C:\PNTTEMPL* on the Point client. Open Point Administrator and click *Change Template Directory* to view the current location to verify the location.

6. Rename the Template Sets after pasting into the **Root Directory**.

Note: Renaming template sets after copying prevents accidental data loss when copying another template set named *PNTTEMPL* from a different client.

7. Select **Import** from the *Configuration* menu.
8. Select **Template Sets**.



1 2

Path	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\BChilcutt\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Bug-38518\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Daveon-Test\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Dean-2\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Dean-Test\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Dontae-Template\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Dougs-Templates-DONT-TOUCH\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Emmanuel\	☐
C:\Program Files (x86)\Calyx Software\PointCentral\filesync\TemplateSets\Erica-Template-Set\	☐

Figure 135: Import Template Sets screen

9. Select the checkboxes that correspond to the template to import.
10. Click **Import Template Set(s)**.
11. Click **Yes** on the *Confirmation Message*.
12. Select **Status** from the menu to view import status.

See Template Sets for details on granting access to template sets.

Import Users from a Text File

PointCentral allows importing Users from text files. This method is useful for new Users and not assigned to folders in conventional Point.

The same data validation rules apply as those when a Point User is created:

- Full name cannot be blank and cannot exceed 255 characters.
- User ID cannot be blank and cannot exceed 255 characters.
- Password must:
    - Be at least 8 characters long.
    - Contain only lower- or upper-case letters (a-z, A-Z) or numbers (0-9).
    - Contain at least one letter (a-z, A-Z) and at least one number (0-9).

Use the following guidelines when creating the User file:

- One User per line.
- Separate each field with a tab.

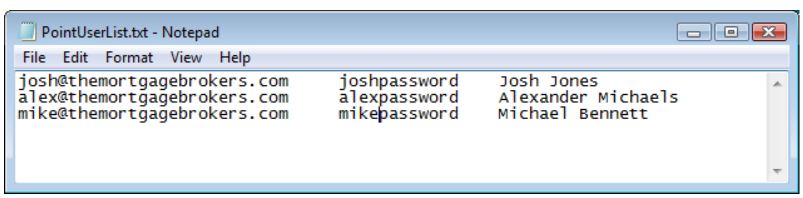
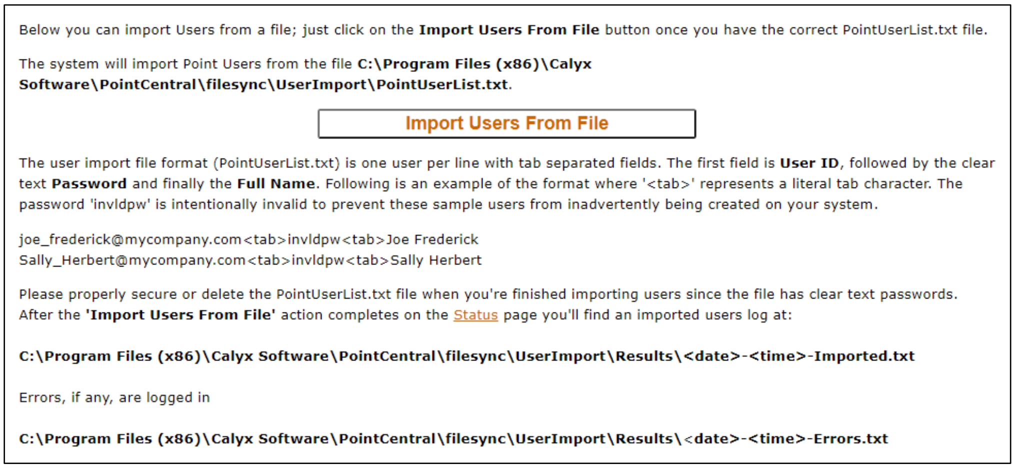


Figure 136: Import Users Text File Example

Use the following steps to import Users from a text file.

1. Copy the PointUserList.txt file into the **User Import** directory which is typically located at **C:\Program Files (x86)\Calyx Software\PointCentral\filesync** on PointCentral.
2. Select **Import** from the *Configuration* menu.
3. Select **Users**.

4. Click **Import Users From File**.



Below you can import Users from a file; just click on the **Import Users From File** button once you have the correct PointUserList.txt file.

The system will import Point Users from the file **C:\Program Files (x86)\Calyx Software\PointCentral\filesync\UserImport\PointUserList.txt**.

Import Users From File

The user import file format (PointUserList.txt) is one user per line with tab separated fields. The first field is **User ID**, followed by the clear text **Password** and finally the **Full Name**. Following is an example of the format where '<tab>' represents a literal tab character. The password 'invldpw' is intentionally invalid to prevent these sample users from inadvertently being created on your system.

joe_frederick@mycompany.com<tab>invldpw<tab>Joe Frederick
Sally_Herbert@mycompany.com<tab>invldpw<tab>Sally Herbert

Please properly secure or delete the PointUserList.txt file when you're finished importing users since the file has clear text passwords.
After the **'Import Users From File'** action completes on the Status page you'll find an imported users log at:

C:\Program Files (x86)\Calyx Software\PointCentral\filesync\UserImport\Results\<date>-<time>-Imported.txt

Errors, if any, are logged in

C:\Program Files (x86)\Calyx Software\PointCentral\filesync\UserImport\Results\<date>-<time>-Errors.txt

Figure 137: Import Users From File

5. Click **OK** on the *Confirmation* prompt.
6. Click the **Status** to view the import status.

Note: A log is created during import that records which Users were successfully imported. An error log is also created if any errors occur. The files are stored *in Results in the User Import* directory.

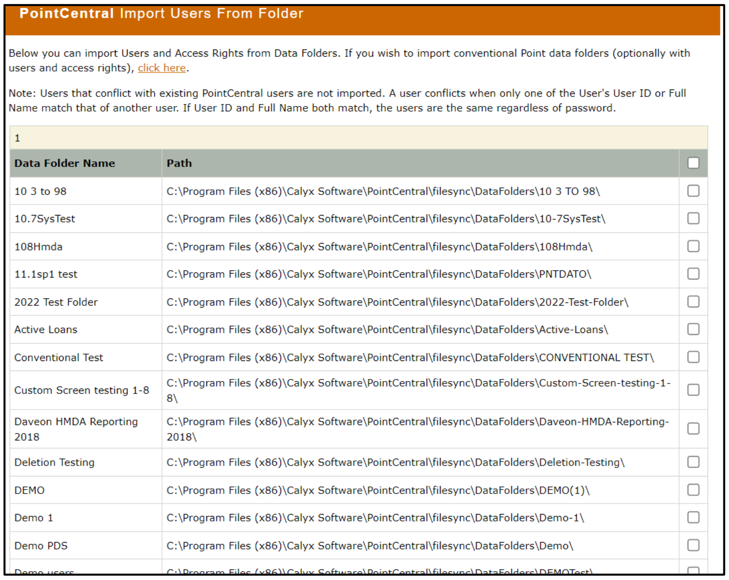
7. Delete or secure the **PointUserList.txt** file after importing the Users because the file has clear text passwords.

Import Users From Folder

Use the following steps to import Users from a folder manually.

1. Select **Configuration** > **Import** > **User From Folder**.

2. Select the checkboxes that correspond to the data folders(s) from which to import Users.



PointCentral Import Users From Folder

Below you can import Users and Access Rights from Data Folders. If you wish to import conventional Point data folders (optionally with users and access rights), click here.

Note: Users that conflict with existing PointCentral users are not imported. A user conflicts when only one of the User's User ID or Full Name match that of another user. If User ID and Full Name both match, the users are the same regardless of password.

1

Data Folder Name	Path	☐
10 3 to 98	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\10 3 TO 98\	☐
10.7SysTest	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\10-7SysTest\	☐
108Hmda	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\108Hmda\	☐
11.1sp1 test	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\PNTDATO\	☐
2022 Test Folder	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\2022-Test-Folder\	☐
Active Loans	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Active-Loans\	☐
Conventional Test	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\CONVENTIONAL TEST\	☐
Custom Screen testing 1-8	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Custom-Screen-testing-1-8\	☐
Daveon HMDA Reporting 2018	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Daveon-HMDA-Reporting-2018\	☐
Deletion Testing	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Deletion-Testing\	☐
DEMO	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\DEMO(1)\	☐
Demo 1	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Demo-1\	☐
Demo PDS	C:\Program Files (x86)\Calyx Software\PointCentral\filesync\DataFolders\Demo\	☐

Figure 138: Import Users

3. Click **Import Users**.
4. Select **Status** from the menu to view the import status.

Chapter 6 - Access Right Reports

Reports are available that illustrate the relationships between Users and User Groups, and their access rights to the following:

- Data folders
- Template sets
- Rules
- Cardex databases

The following reports are available:

- Rules Access Rights
- User Access Rights
- Users, Group Memberships
- Groups, User Members
- Data Folders Access Rights
- Template Sets Access Rights
- Cardex Databases Access Rights
- Rules Access Rights

User Access Rights

View the effective access rights to resources for a specific User. Effective access rights to a resource are a combination of:

- Access rights granted by User access rights.
- Group access rights (where the User is a member of the group).

Users can have access rights to three types of resources:

- Data folders
- Template sets
- Cardex databases
- Rules

Use the following steps to view User template set *Effective Access Rights* report.

1. Select **User Effective Access Rights** from the *Reports* menu.

2. Enter **User ID** or user **Full Name**.


In this page you may view the effective access rights to resources for a specific user. Effective access rights to a resource are a combination of access rights granted by user access rights and group access rights (where the user is a member of the group). A user may have access rights to three types of resources: Data Folders, a Template Set and a Cardex Database.

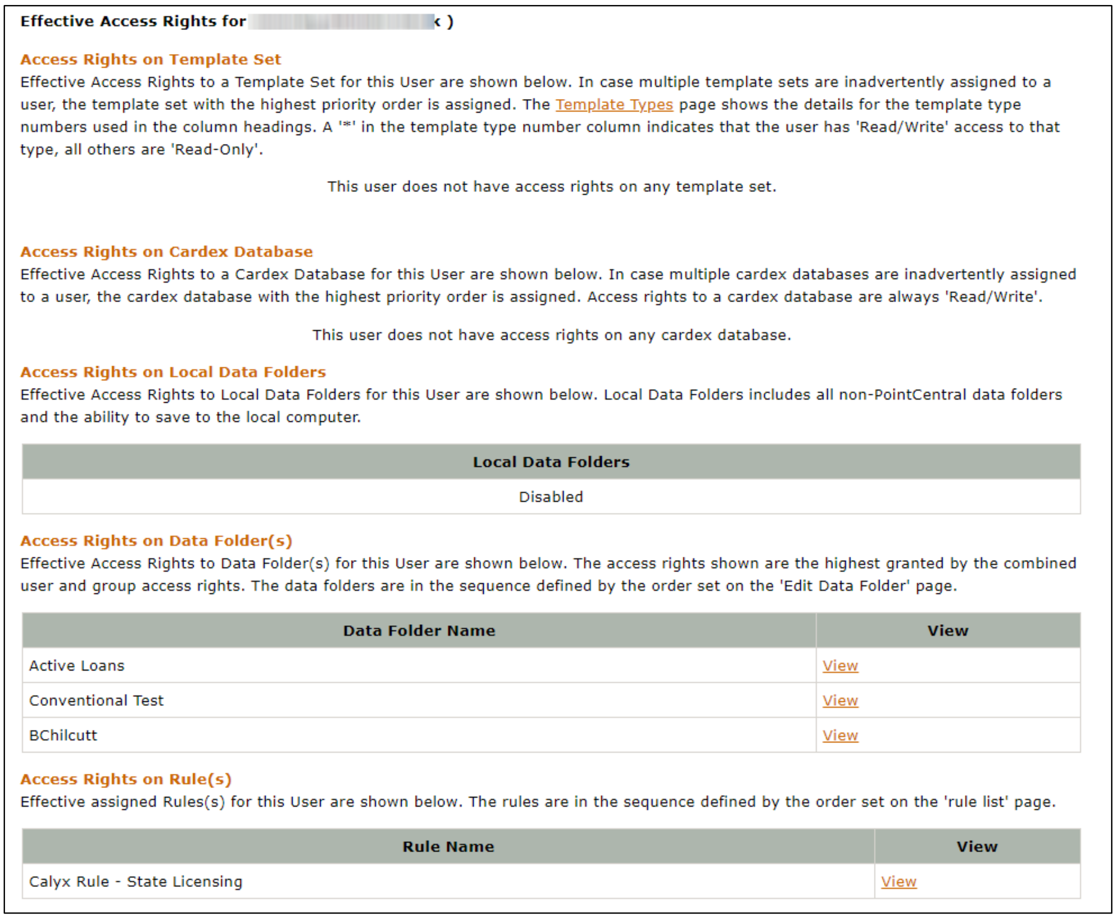
Search Criteria

User ID: [ ] Search

Full Name: [ ] Search

Figure 139: User Access Rights Search

3. Click **Search**.


Effective Access Rights for [redacted] **k)**

Access Rights on Template Set

Effective Access Rights to a Template Set for this User are shown below. In case multiple template sets are inadvertently assigned to a user, the template set with the highest priority order is assigned. The Template Types page shows the details for the template type numbers used in the column headings. A '*' in the template type number column indicates that the user has 'Read/Write' access to that type, all others are 'Read-Only'.

This user does not have access rights on any template set.

Access Rights on Cardex Database

Effective Access Rights to a Cardex Database for this User are shown below. In case multiple cardex databases are inadvertently assigned to a user, the cardex database with the highest priority order is assigned. Access rights to a cardex database are always 'Read/Write'.

This user does not have access rights on any cardex database.

Access Rights on Local Data Folders

Effective Access Rights to Local Data Folders for this User are shown below. Local Data Folders includes all non-PointCentral data folders and the ability to save to the local computer.

Local Data Folders
Disabled

Access Rights on Data Folder(s)

Effective Access Rights to Data Folder(s) for this User are shown below. The access rights shown are the highest granted by the combined user and group access rights. The data folders are in the sequence defined by the order set on the 'Edit Data Folder' page.

Data Folder Name	View
Active Loans	View
Conventional Test	View
BChilcutt	View

Access Rights on Rule(s)

Effective assigned Rules(s) for this User are shown below. The rules are in the sequence defined by the order set on the 'rule list' page.

Rule Name	View
Calyx Rule - State Licensing	View

Figure 140: User Access Rights Report

4. Click the **View** links to view access right specifics.

Note: The information on the *View* screens is non-editable.

5. Click **Back** to return to the *User Effective Access Rights* screen.

Users, Group Memberships

The *Users, Group Memberships* report shows the groups in which a User is a member. Only Users who are a member of at least one group are listed.

Select **Users, Groups Memberships** from the *Reports* menu.

This report shows for each user, all of the groups that the user is a member of. Only users that are a member of at least one group are shown.

User	Groups
DClark (Dean Clark)	QA
Gthomas (George Thomas)	QA
mmock (Michele Mock)	QA
Mscott (Matthew Scott)	QA

Figure 141: Users/Groups Members Report

Groups, User Members

The *Groups, User Members* report shows the groups and the members it contains. Only groups that have at least one member are listed.

Select **Groups, User Members** from the *Reports* menu.

PointCentral Groups, User Members

This report shows for each group, all of the user members. Only groups that have at least one member are shown.

Group	Users
Arizona	Alex M (Alexander Michaels), JJ (Josh Jones), Mike (Michael Bennett), Teddy (Theodore Rogers)
California	Jane (Jane Nguyen), Maggie (Margaret Bryant), Teddy (Theodore Rogers)
Florida	Brian (Brian Chen), Maria (Maria Espinosa), Teddy (Theodore Rogers)

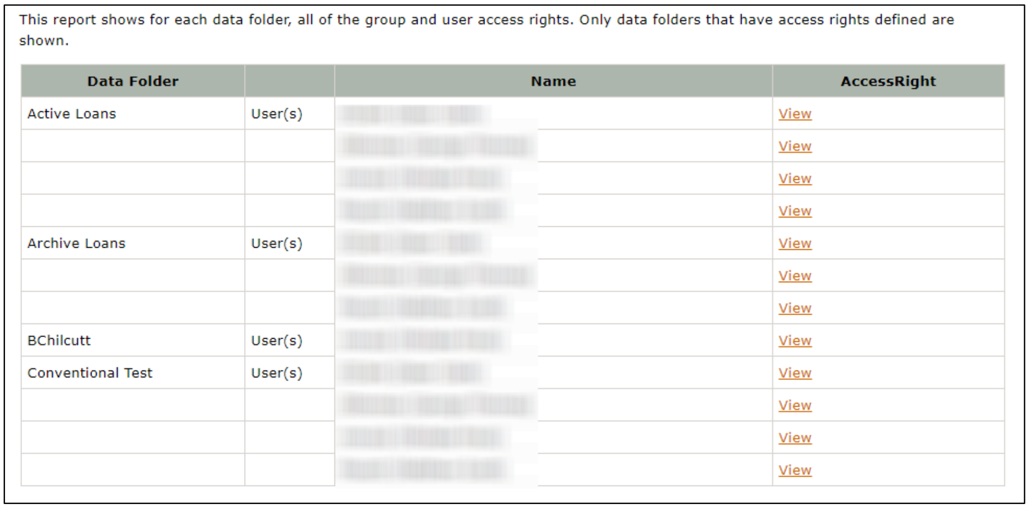
Figure 142: Groups/Users Members Report

Data Folders Access Rights

The *Data Folders, Groups and Users with Access Rights* report shows group and User access rights for each data folder. Older data folders with access rights defined are listed.

Use the following steps to view the *Data Folders, Groups, and Users Access Rights* report.

1. Select **Data Folders, Groups and Users** with *Access Rights* from the *Reports* menu.



This report shows for each data folder, all of the group and user access rights. Only data folders that have access rights defined are shown.

Data Folder		Name	AccessRight
Active Loans	User(s)	[illegible]	View
		[illegible]	View
		[illegible]	View
		[illegible]	View
Archive Loans	User(s)	[illegible]	View
		[illegible]	View
		[illegible]	View
BChilcutt	User(s)	[illegible]	View
Conventional Test	User(s)	[illegible]	View
		[illegible]	View
		[illegible]	View
		[illegible]	View

Figure 143: Data Folders Access Report

2. Click the **View** link next to the User or User Group name to view the access rights.

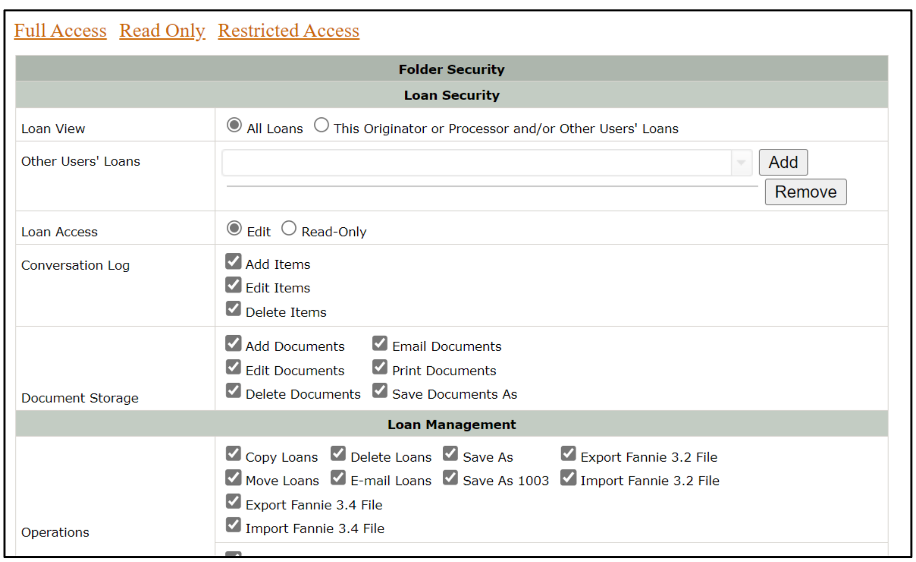


Figure 144: Edit Access Rights

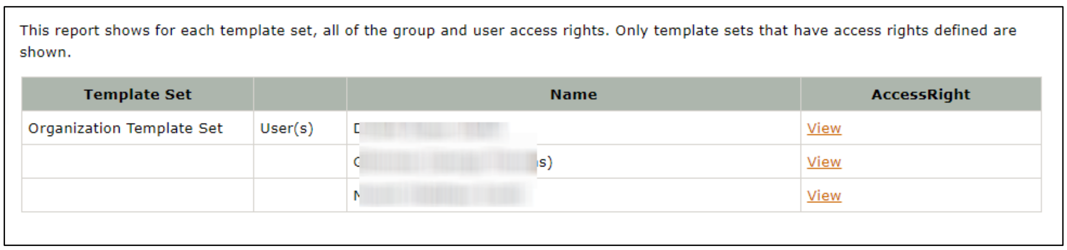
3. Edit the access rights if required.
4. Click **Update Group Access Rights** if changes are made.
5. Click **Cancel** to exit the screen.

Template Sets Access Rights

The *Template Sets, Groups and Users with Access Rights* report lists all the group and User access rights for each template set. Only template sets that have access rights defined are included in the list.

Use the following steps to view the *Template Sets, Groups and Users with Access Rights* report.

1. Select **Template Sets, Groups and Users with Access Rights** from the *Reports* menu.



This report shows for each template set, all of the group and user access rights. Only template sets that have access rights defined are shown.

Template Set		Name	AccessRight
Organization Template Set	User(s)	D[redacted]	View
		C[redacted]s)	View
		N[redacted]	View

Figure 145: Template Sets Access Report

2. Click the **View** link next to the User or group name to view the access rights.
3. Edit the access rights if required.

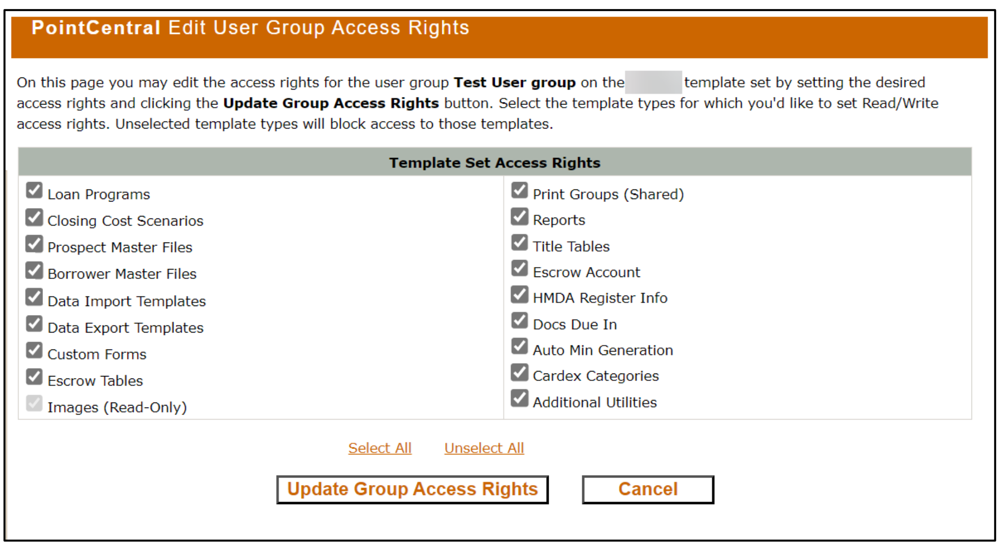


Figure 146: Edit User Access Rights

4. Click **Update Group Access Rights** if required.
5. Click **Cancel** to exit the screen.

Cardex Databases Access Rights

The *Cardex Databases, Groups and Users with Access Rights* Report lists the group and User access rights for the Cardex databases. Only Cardex databases that have access rights defined are listed.

Select **Cardex Databases, Groups and Users with Access Rights** from the *Reports* menu.

PointCentral Cardex Databases, Groups and Users with Access Rights

This report shows for each cardex database, all of the group and user access rights. Only cardex databases that have access rights defined are shown. Note that access rights for cardex databases are always Read/Write.

Cardex Database		Name
Carson	Group(s)	Carson
		Phoenix
		San Francisco
	User(s)	Alex M (Alexander Michaels)
		Mike (Michael Bennett)
Orlando	User(s)	Alex M (Alexander Michaels)
Phoenix	User(s)	Alex M (Alexander Michaels)

Figure 147: Cardex Access Report

Rules Access Rights

The *Rules, Groups and Users with Access Rights* Report lists the group and User access rights for Rules. Only rules that have access rights defined are listed.

Select **Rules, Groups and Users with Access Rights** from the *Reports* menu.

PointCentral Rules, Groups and Users with Access

This report shows for each rule, all of the group and user access rights. Only rules that have access rights defined are shown.

Rule		Name
Custom message rule	Group(s)	Carson
		Phoenix
	User(s)	Alex M (Alexander Michaels)
		JJ (Josh Jones)
Disable fields rule	Group(s)	Carson
		Los Angeles
	User(s)	Alex M (Alexander Michaels)
Required Fields	Group(s)	Daytona Beach
		Phoenix
	User(s)	Alex M (Alexander Michaels)
		Maria (Maria Espinosa)
State Licenses rule	Group(s)	Carson
		Los Angeles

Figure 148: Rules Access Report

Chapter 7 - Point Custom Report Support

PointCentral uses a database to accelerate Point operations. FileSync automatically scans the loan file for changes and updates the database when a loan file is updated in an accelerated folder. FileSync imports a selected number of fields instead of importing all possible field values from the loan file. The selected import enables quicker response times, support for more Point clients, and a reasonable database size. The imported fields are called PointCentral-supported fields.

Supported fields can refer to either the built-in supported fields in Point or the entire collection of supported fields, including:

- Built-in supported fields
- Custom fields
- Additional fields

Ensure the Point fields in the report definition are supported fields when creating custom reports. No data is returned from data folders if the report uses unsupported fields not added as additional fields. Add the fields by using the Additional fields procedure if data from the fields is required.

Note: Point reports can include a mix of PointCentral and conventional Point data folders.

Supported Fields

Supported fields significantly accelerate the following operations:

- Search
- Advanced Search
- List co-borrowers
- Tasks operations
- Commonly used fields in reports

PointCentral-supported fields include the following:

- Commonly used fields in reports.
- All fields used by the Point built-in reports.
- All report macros, such as NAME and HPURP.
- Custom screens and fields.
- Additional fields added by the administrator.

Use **Additional Fields** option to dynamically add up to 300 Point fields to the supported fields in PointCentral. Supported fields refer to built-in supported fields for reports and the entire collection of supported fields.

PointCentral supports all the fields required to perform Loan and Task operations, including:

- Search
- Advanced Search
- List Co-Borrowers
- Search
- Advanced Search

The operations always use PointCentral for accelerated data folders.

See Additional Fields for more information about using the **Additional Fields** option.

See **Point Knowledge Base article #0061**, Searching for *Field IDs* for more information about finding Point Field IDs and descriptions of the available Report Macros.

Reports Generated with PointCentral

Reports generated from data in PointCentral data folders are much faster than with conventional Point data folders. Reports can include a mix of PointCentral and conventional data folders. Running reports in PointCentral benefits from acceleration while conventional folders rely on the more time-consuming conventional file scanning.

The following figure shows an example of a User-created report. The report was not included in the standard Point reports. The PointCentral data folders are easily distinguished from conventional data folders by the text [PDS] appended to the folder name. The report is run on PointCentral and conventional data folders. Ordinarily, to get the fastest results, you would Keep the loan files in PointCentral data folders and run reports on the PointCentral folders only to avoid the slower conventional folders.

	Field Name	Field ID	Condition	Show	Total	Format	Width
1	Data Folder Name	FOLDER		☑		Auto	Auto
2	Filename	1		☑		Auto	Auto
3	Borrower First Name	100		☑		Auto	Auto
4	Loan Amount	11		☑		Auto	Auto
5	Note Rate	12		☑		Auto	Auto
6	School District	9900		☑		Auto	Auto
7	Other Reserve	1096		☑		Auto	Auto
8				☑		Auto	Auto
9				☑		Auto	Auto
10				☑		Auto	Auto
11				☑		Auto	Auto
12				☑		Auto	Auto
13				☑		Auto	Auto
14				☑		Auto	Auto
15				☑		Auto	Auto
16				☑		Auto	Auto

Figure 149: Point User-defined Report

The *Data Folder Name (Field ID: FOLDER) report* uses fields to demonstrate PointCentral report behavior. The report field shows the data folder where the loan is stored to illustrate the differences between PointCentral and conventional folders.

The following fields are all default supported fields:

- Data Folder Name (Field ID: FOLDER)
- Filename (1)
- Borrower First Name (100)
- Loan Amount (11)

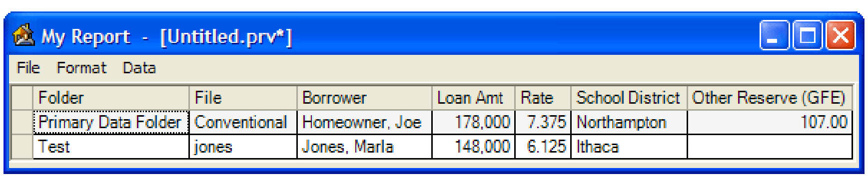
School District (9900) is a custom field. **Other Reserve (GFE) (1096)** is an unsupported field.

The **School District (9900)** custom field is defined with the **Custom Fields** table and supported. The Other **Reserve (GFE) (1096)** field was not added to PointCentral and is currently unsupported. An error occurs and the *Errors Detected* dialog displays when generating the report.

The *Errors Detected* dialog indicates errors or warnings were generated during the report that might impact the results. Click **Yes** to view the message details. The error message contains the following information:

- **Warning:** one or more requested Point fields are not currently supported by PointCentral
- Unsupported field: **f1096** (Error Code: **-1**)
- Column **f1096** does not belong to table **LoanApps**

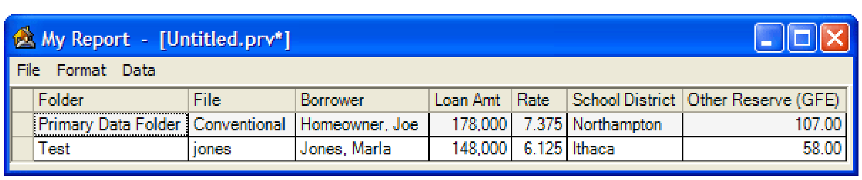
The message refers to field **f1096**. The **f** is prepended to the Point Field ID indicating the field has Point Field ID **f1096**: the unsupported **Other Reserve (GFE) (1096)** field in the report.



Folder	File	Borrower	Loan Amt	Rate	School District	Other Reserve (GFE)
Primary Data Folder	Conventional	Homeowner, Joe	178,000	7.375	Northampton	107.00
Test	jones	Jones, Marla	148,000	6.125	Ithaca	

Figure 150: Report Unsupported Fields

Checking the report results reveals the loan in the data folder is missing data for the **Other Reserve (GFE) (1096)** field that was mentioned in the unsupported fields warning.



Folder	File	Borrower	Loan Amt	Rate	School District	Other Reserve (GFE)
Primary Data Folder	Conventional	Homeowner, Joe	178,000	7.375	Northampton	107.00
Test	jones	Jones, Marla	148,000	6.125	Ithaca	58.00

Figure 151: Unsupported Fields Added

PointCentral returns the data for **Other Reserve (GFE) (1096)** when adding the unsupported field **Other Reserve (GFE) (1096)** to the supported fields collection and running the report again. Figure 143 shows the additional field.

Custom fields behave in a similar manner. **Custom** fields can be identified by their Field ID in the inclusive range of **9900** to **9999**.

An error occurs indicating PointCentral does not support any report fields in the event of having a report without at least one supported field.

The *Report Results* dialog does not display because no data is available if the report is run for only PointCentral data folders. Remedy this situation by adding a supported field to the report or including a **Custom** field and adding the unsupported field to PointCentral using additional fields.

PointCentral supports a select subset of Point fields. The Point fields fall into four groups:

- Normal point fields
- Custom fields
- Report macro fields
- Additional fields

Use the following steps to access the *Supported Fields* screen.

1. Select **Point Fields** from the *Configuration* menu.
2. Select **Supported Fields**.

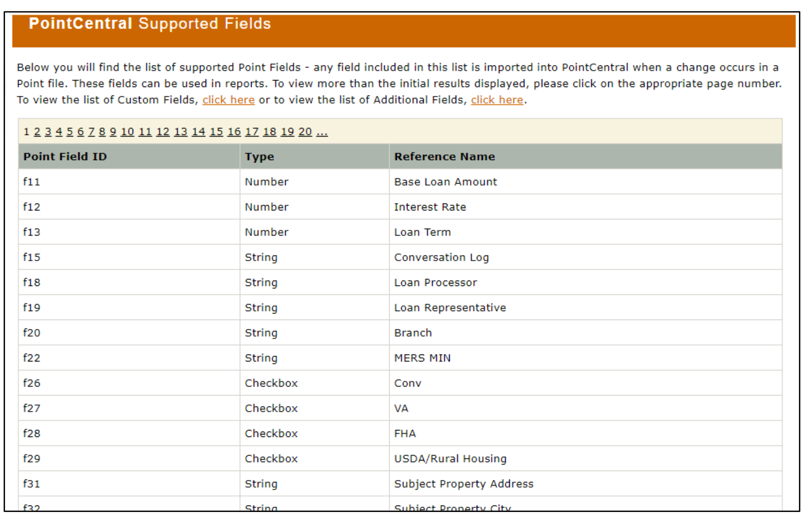


Figure 152: Supported Fields

The *Supported Fields* page lists the **Point** fields and the **Report Macro** fields.

The **Point Field ID** in the **Supported Fields** list is prepended with an **f**. The **Type** column contains the type of value that is used in the field. The **Reference Name** column is the descriptive common name for the field. The fields are listed in numeric order. Use the page numbers at the top of the list to move from page to page.

Report Macro fields begin with ID number **30000**. Select the page that contains field ID 30000 to access the fields.

Use the case-sensitive reference name to reference the **Report Macro** fields in Point reports. The reference is different from the normal **Point** fields and **Custom** fields referenced in Reports by numeric Point **Field ID** (without the f prefix).

The definitions that are used for **Custom** fields/screen are available on the *Custom Fields* screen. The fields that are added to PointCentral are available on the *Additional Fields* screen.

See Custom Screens and Fields for a list of **User- defined** custom screens and fields, information about custom fields, and how to update custom field definitions.

See Additional Fields for the list of User-specified fields, information about additional fields, and how to update additional fields definitions.

Using the Field Selection Dialog for Custom Reports

In the User-generated report example, an empty column is available. This empty column allows for the addition of an extra category.

To use this function:

1. Open **Templates** in Point.
2. Select **Reports & Marketing**.
3. Select the desired report.
4. Expand the empty column.

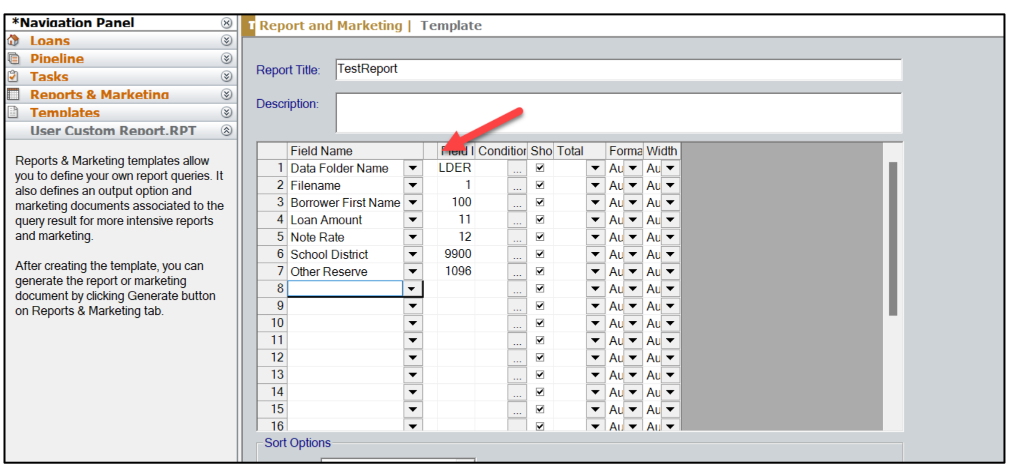
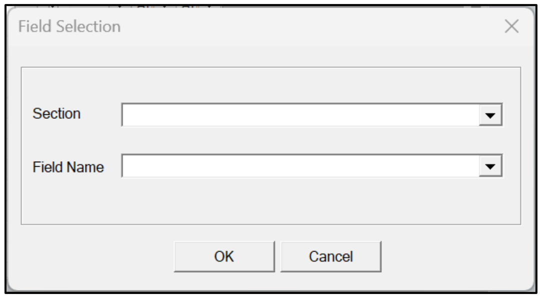
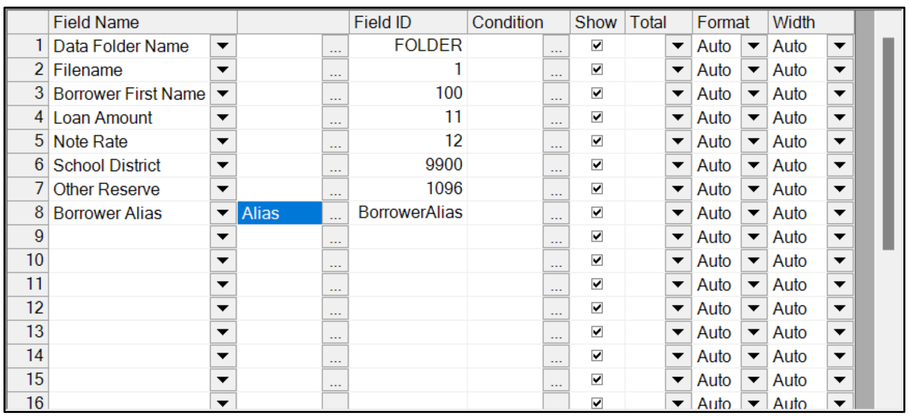


Figure 153: Reports Template

5. Select the ellipses (...) button.
6. Click on the **Section** dropdown to select an option.



7. Click on the **Field Name** dropdown menu and select an option.
8. Click **OK** to add the selection.



	Field Name		Field ID	Condition	Show	Total	Format	Width
1	Data Folder Name		FOLDER		☑		Auto	Auto
2	Filename		1		☑		Auto	Auto
3	Borrower First Name		100		☑		Auto	Auto
4	Loan Amount		11		☑		Auto	Auto
5	Note Rate		12		☑		Auto	Auto
6	School District		9900		☑		Auto	Auto
7	Other Reserve		1096		☑		Auto	Auto
8	Borrower Alias	Alias	BorrowerAlias		☑		Auto	Auto
9					☑		Auto	Auto
10					☑		Auto	Auto
11					☑		Auto	Auto
12					☑		Auto	Auto
13					☑		Auto	Auto
14					☑		Auto	Auto
15					☑		Auto	Auto
16					☑		Auto	Auto

Figure 154: Added Selection

Custom Screens and Fields

Use the *Custom Fields* screen to ensure PointCentral imports **Custom** fields into the database when required if the organization uses custom screens and fields in Point to support business processes.

Rebuild the **Custom Field** table to match the number of defined fields and data types changes to any of the custom screen definitions occur. Loan files synchronize to populate the newly defined custom fields in the database with the data from the loan files when the **Custom Field** table is rebuilt.

The Administrator is responsible for defining and maintaining the definitions creates the custom screen definitions. These definitions apply to all Point clients and loan files in the organization.

Point Users enter and view the Custom Field data by selecting **Custom Screens/(User defined Screen Name)** from the Point **Forms** menu.

Refer to the *Point User Guide* for more information about Point custom screens.

Point retrieves the custom screens definitions from the template folder definition in Point Administrator for conventional data folders. Point retrieves the custom screens definition from PointCentral over the secure HTTPS connection for PointCentral data folders.

Change Custom Screen Definitions

Use the following steps to change the custom screen definitions used by PointCentral.

1. Log in to the *Administration* web site after the custom screen fields are changed in Point.
2. Select **Point Fields** from the *Configuration* menu.
3. Select **Custom Fields**.

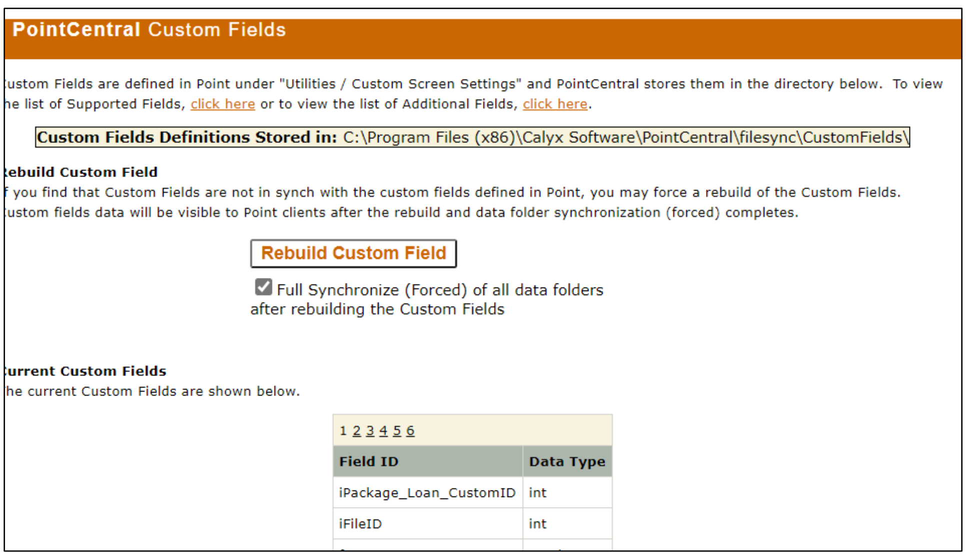


Figure 155: Custom Fields

4. Click **Rebuild Custom Field**.

Rebuilding the **Custom Field** table clears the custom field data from the database. Custom field data in the Point loan files is unaffected. Forcing a full synchronization synchronizes the Point loan files and custom field data into the database. Skip the forced full synchronization if the custom field data is not required at the time of the rebuild.

Rebuilding the table is an asynchronous operation that runs in the background to save resources and allow work to continue while the synchronization completes. Check the *Status screen* to see the synchronization status and verify completion.

The **Rebuild Custom Fields Table** process clears the previous custom field definitions from the database and creates a new **Custom Fields** table using the current definitions. Point clients see the new definitions the next time Point opens.

Running reports using the updated **Custom Field Definitions** returns empty custom fields for a loan file until the file synchronizes using the rebuilt **Custom Fields** table. The system synchronizes the loan files in the accelerated folders when using the **Full Synchronize (Forced) of all PDS Accelerated Folders after rebuilding Custom Field Table** option.

All Point Users must be logged off before performing a full synchronization. Refer to Forced Synchronization for information about performing a full, or forced, synchronization.

The Status screen shows the progress of the forced synchronization. There is a synchronize folder (forced) operation for every accelerated folder. The custom field data for loan files is available to reports when all the synchronized folder operations complete.

5. Monitor the progress of the custom fields rebuild on the administration *Status* screen for the **Done** status.
6. Check the **Windows Application Event Log** for any errors.
7. Review the **Current Custom Fields Definitions** on the administration *Custom Fields* screen to verify the new definitions.

The **current custom screen definitions** used by PointCentral are available on the *Custom Fields* screen after the rebuild is complete.

They ignore the **iCustomID** and **iFileID** fields used internally by PointCentral. The **Data Type** column displays the current definition of the data type used to validate and store the field in the database. The database types map to the **Custom Screen Settings Field Type** as shown in the following table.

Table 20: Custom Screen Mappings

Point Custom Screen Setting Field Type	Type	Sample Values
Text	Varchar	Our custom fields help us sell loans
Integer Number	float	934850
Currency (#. ##)	Float	908580.43
Percentage (#. ###)	Float	909.293
Date (MM/DD/YYYY)	datetime	12/31/1980
Phone (###-###-####)	Varchar	555-555-5525
SSN (###-##-####)	Varchar	435-89-5678
Dropdown List	Varchar	Wow! That's low

See Check PointCentral Status for more information about the *Status* screen.

See the *Point User Guide* for more information about custom screens and fields in Point.

Import Custom Screens

Import custom screens from Point to PointCentral. Create or import data folders to avoid having to synchronize data folders later.

The custom screen settings in Point are stored in the **CUSTOMn.CSF** files (where n is a number between 1 and 4 that corresponds to custom screens 1 through 4 in Point).

Note: Custom screen settings in Point are called custom screen definitions in PointCentral.

To import the custom screen settings:

1. Select **Administrative Tools** from the *Start* menu.
2. Select **Services**.
3. Double-click **CalyxPdsFileSync**.
4. Click **Stop** to stop the service.
5. Copy the custom screen and fields (*.CSF) files to C:\Program Files (x86)\Calyx Software\PointCentral\filesync\CustomFields.

Note: Substitute the appropriate installation path for *C:\Program Files (x86)\Calyx Software\PointCentral*. The default location for existing custom screen and field files in conventional Point is *C:\PNTTEMPL*.

6. Start the **CalyxPdsFileSync** service.
7. Open the Services Control Panel.
8. Click **Start** on the *CalyxPdsFileSync Properties* dialog.

Additional Fields

Use the following information to ensure custom reports are imported into the database. 300 additional field IDs can be identified that are not already included in supported or custom fields to use in custom reports.

A Point client sees the new definitions the next time the User opens Point and references the additional fields in Reports. The system returns empty fields for the additional fields in a loan file until the file is synchronized when the **Additional Fields** table is rebuilt. The synchronization occurs by default when selecting the **Full Synchronize (Forced) of all data folders after rebuilding the Additional Fields** table checkbox.

A forced full synchronization timeframe depends on the number of loan files and data folders in PointCentral. PointCentral synchronizes every Point loan file in the database, including the additional fields data. Skip some of the synchronization during rebuild if you do not need the additional field data.

Note: All Point Users must be logged off before performing a full synchronization. See Forced Synchronization for information about performing a forced or full synchronization.

Configuring Additional Field Definitions

The system deletes the previous **Additional Fields** table from the database and then re-creates it during. Use the following steps to configure additional field definitions.

1. Select **Load Field ID** from the Point *Utilities* menu.
2. Select **Prospect** or **Borrower** appropriately.
3. Notate the **Field ID** and **Description** for the fields to import.
4. Log in to the *Administration* website.
5. Select **Point Fields** from the **Configuration** menu.
6. Select **Additional Fields**.
7. Enter the **ID** in the *Field ID* field.

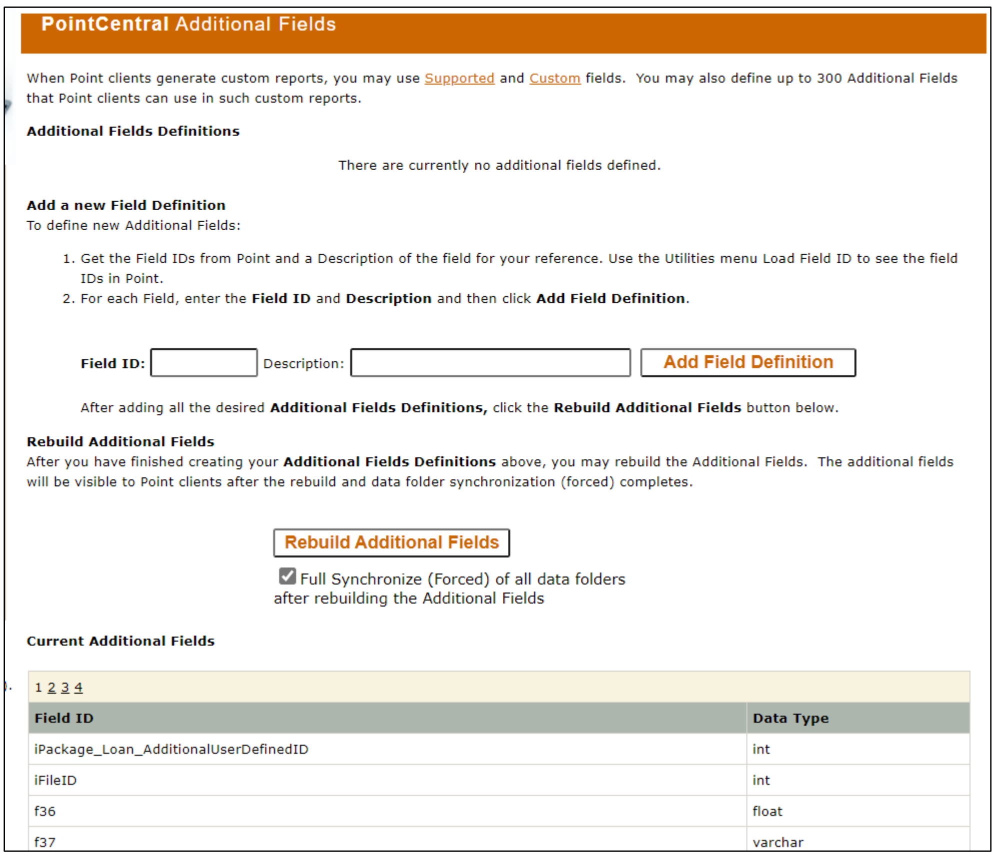


Figure 156: Additional Fields

8. Enter the field description in the **Description** field.
9. Click **Add Field Definition**.

Note: Descriptions can contain only letters, numbers, spaces, and the following characters: [] ( ) - . # $ + _ { } \ / @ ! * = : ; ? ,.

10. Repeat Steps 7 – 9 for each field to import.
11. Click **Rebuild Additional Fields**.

Rebuilding the table is an asynchronous operation that runs in the background to save resources and enable work to continue to work in PointCentral while the rebuilding completes. Check the *Status* screen view the table rebuild and verify completion.

There is a full synchronized operation for every accelerated folder. All **Additional Fields Definitions** data for all loan files is available when the full synchronization is complete.

View the *Status* screen to synchronize status. Review the **Windows Application Event Log** for error messages when errors occur.

The **Current Additional Fields** table shows the rebuilt table after rebuilding the **Additional Fields** table.

Ignore the **iAdditionalID** and **iFileID** fields that are used internally by PointCentral. The **Additional Fields Table Data Type** is used to validate and store the field in the database. The types used in reports for conditions map to **Additional Fields Table Data Types** are shown in the following table.

Table 21: Additional Fields Table Mappings

Report condition Type	Data Type	Sample Value
Date	datetime	12/31/2011
Decimal	float	908756.43
Integer	float	789567
Test	Varchar	Additional field accommodate your business processes
Time	Datetime	08:00 AM

Additional fields of **Data Type Varchar** (report condition type text) are stored within the Point file. Only the first 80 characters of these varchar fields are copied into the database to keep the database size reasonable. This means that custom reports only show the first 80 characters of these varchar fields. The actual fields on the Point screens (other than reports) show the entire field length that is stored in the Point file.

Note: See Point Knowledge Base article *#1131, Locating Field IDs* for more information about finding Point Fields IDs and descriptions of the available Report macros.

Forced Synchronization

The **Custom Fields** and **Additional Fields** table synchronization must be scheduled while Point is inactive. Forced synchronize both **Custom** and **Additional** tables is not required.

Use the following steps to perform a forced synchronization.

1. Verify that all Users have exited Point.
2. Access **PointCentral**.
3. Select **Parameters** from the *Configuration* menu.
4. Change the **Organization Security Key** to prevent User access to prevent interruption during the synchronization process.

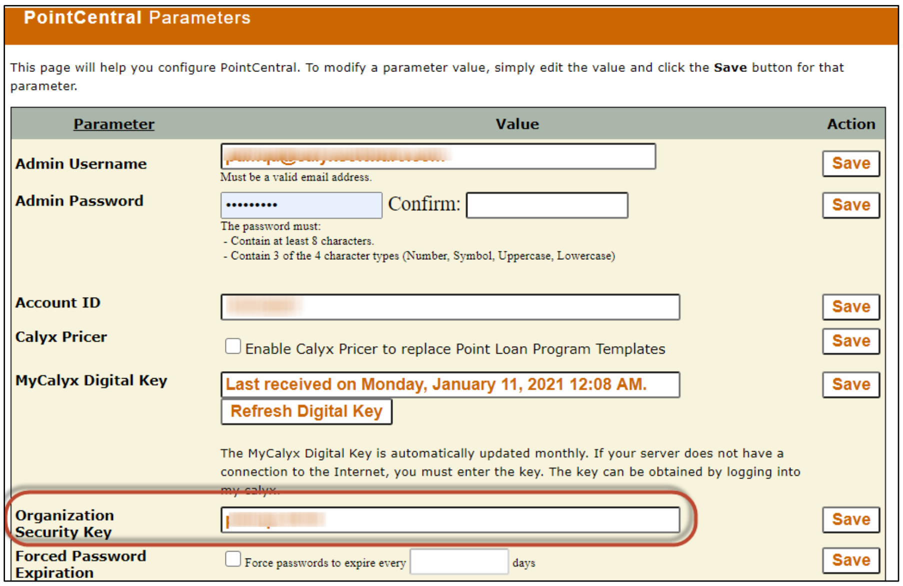


Figure 157: Organization Security Key

5. Restart the **CalyxPDSFilesync** service.
6. Review the **Application Event Log** for errors to ensure proper PointCentral operation prior to starting the synchronization.

Note: Errors may cause problems during the synchronization process.

7. Select **Point Fields** from the *Configuration* menu.
8. Select **Custom** Fields.

9. Select the **Full Synchronize (Forced) of all PDS Accelerated Folders after rebuilding Custom Field Table** checkbox.

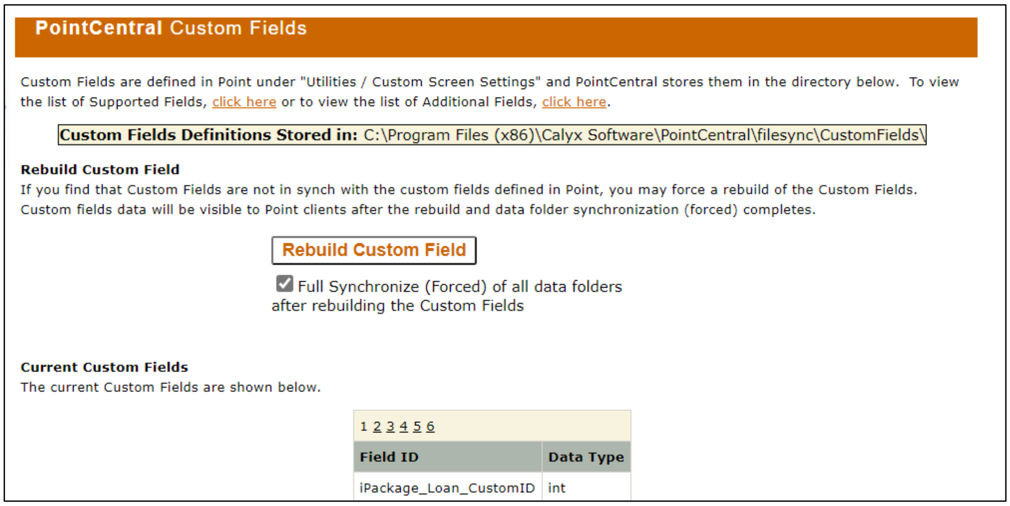


Figure 158: Full Synchronization

10. Click **Rebuild Custom Fields**.
11. Select **Point Fields** from the **Configuration** menu.
12. Select **Additional Fields**. (See Figure 146.)
13. Select the **Full Synchronize (Forced) of all data folders after rebuilding the Additional Fields Table** checkbox.
14. Click **Rebuild Additional Fields**.

Note: Monitor the Status screen for completion. It takes approximately one minute per one thousand files to sync.

15. Return the *Parameters* screen. (See Figure 147.)
16. Return the **Organization Security Key** back to the original setting.

Chapter 8 - Restoration Procedure

Perform regular server and data backups to an external hard drive storage location to prevent data loss if there is a hardware failure where your database and server are stored. Use any third-party software application that can interact with a SQL database.

Exclusive access to the SQL database is required to begin the backup.

Stop PointCentral Applications

Use the following steps to access the database.

1. Open a command prompt.
2. Enter **iisreset / stop**.
3. Press **Enter** to stop the *Administration* site and web service.
4. Type **net stop CalyxPdsFileSync**.
5. Press **Enter** to stop FileSync.

Start PointCentral Applications

Restart PointCentral applications after the backup is completed.

1. Open a command prompt.
2. Type **net start CalyxPdsFileSync**.
3. Press **Enter**.
4. Type **iisreset /start**.
5. Press **Enter**.

Restore the SQL Database

Restore the database using a saved backup file.

1. Stop PointCentral applications.
2. Start **SQL Server Management Studio Express**.
3. Log in appropriately.

4. Right-click the database name.

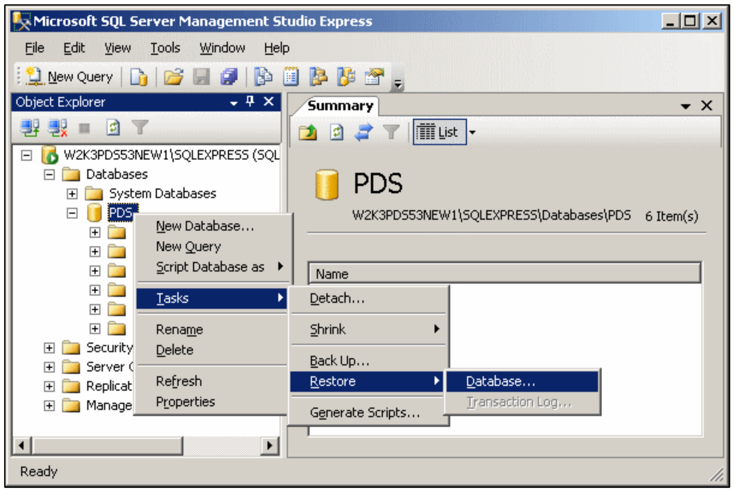


Figure 159: Restore SQL Database

5. Select **Tasks**.
6. Select **Restore**.
7. Select **Database**.
8. Select the database from the **To database** dropdown under *Destination for restore*.

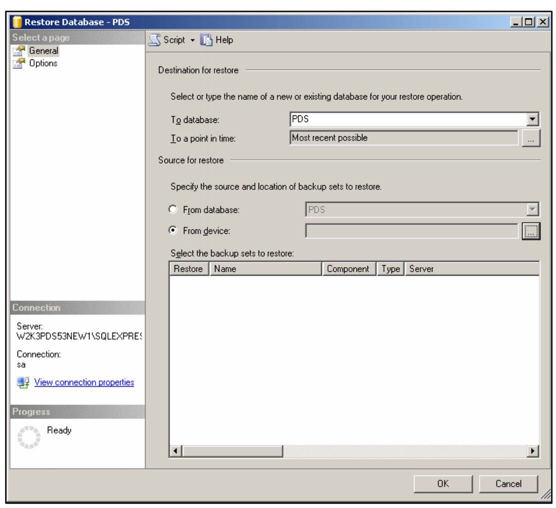


Figure 160: Restore Database Dialog

9. Select the **From device** radio button in the **Source for restore** section.
10. Click the **Display** button.

11. Select **File** from the **Backup media** dropdown.

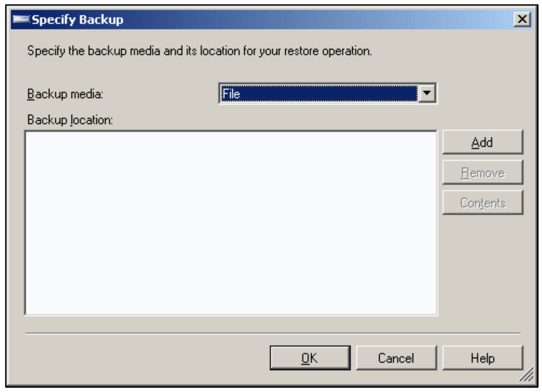


Figure 161: Specify Backup Dialog

12. Click **Add.**

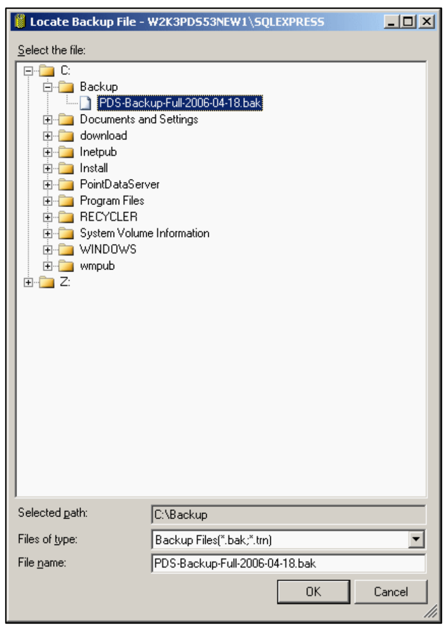


Figure 162: Locate Backup File

13. Navigate to the **C:\Backup directory.**
14. Select the most recent backup file.
15. Click **OK**.

16. Verify the path in the **Backup location** points to the backup file.

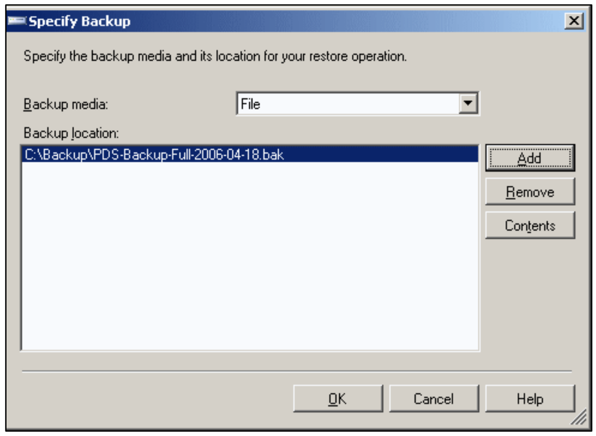


Figure 163: Specify Backup, with Location

17. Click **OK**.
18. Click the Restore checkbox in the Select the backup sets to restore section.

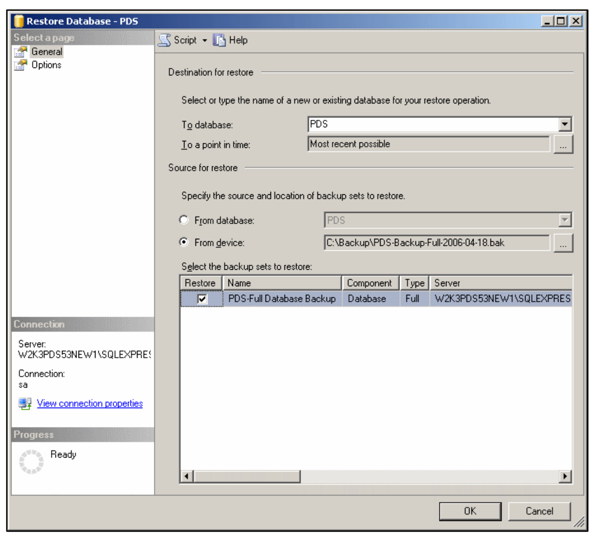


Figure 164: Restore Database

19. Click **Options** in the **Select a page** pane.

20. Select **Overwrite the existing database** in the **Restore Options** section.

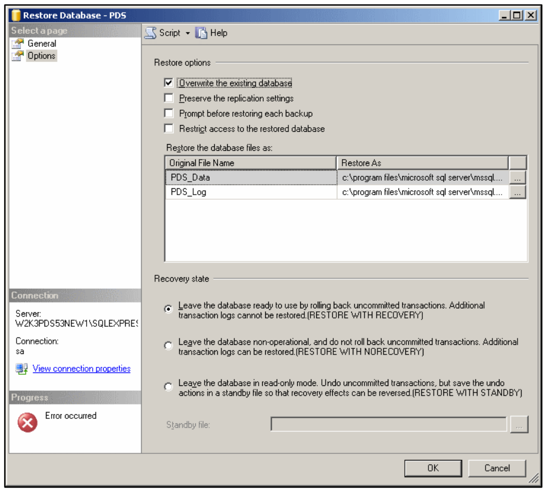


Figure 165: Restore Database Options

21. Click **OK**.

Note: Stop PointCentral applications if the restore fails.

A confirmation dialog displays after the database restoration is complete.

Chapter 9 – Verify DNS & Connectivity

Use the following information to verify PointCentral installation and configuration if problems are encountered during the installation and setup.

Name Resolution

Ensure the Point clients can properly resolve PointCentral before configuring PointCentral to allow incoming connections from Point clients.

The following four methods are available for Point clients to resolve the IP address:

- IP addresses
- Name resolution using NetBIOS/WINS
- Name resolution using DNS
- Calyx Resolver

The IIS web service accepts incoming connections from Point clients and processes them accordingly. Name resolution assists Users with server and computer identification without having to remember IP addresses.

Name Resolution with NetBIOS/WINS

NetBIOS names may be required in cases (such as setting up a test server in a lab with SSL certificates generated by SSL Certificate Authority). Ensure the Point clients can properly resolve the server connection by using the HTTPS protocol (port 443) when using NetBIOS/WINS names.

Use the NetBIOS name to identify computers. Use the following steps to obtain the computer name.

Locate Computer Name

Use the following steps to locate the computer name.

1. Access the Computer **Control Panel**.
2. Select the **System Settings**.

3. Locate the **NetBIOS name (PDS-SVR)** is in the **Computer name, domain, and workgroups settings** section.

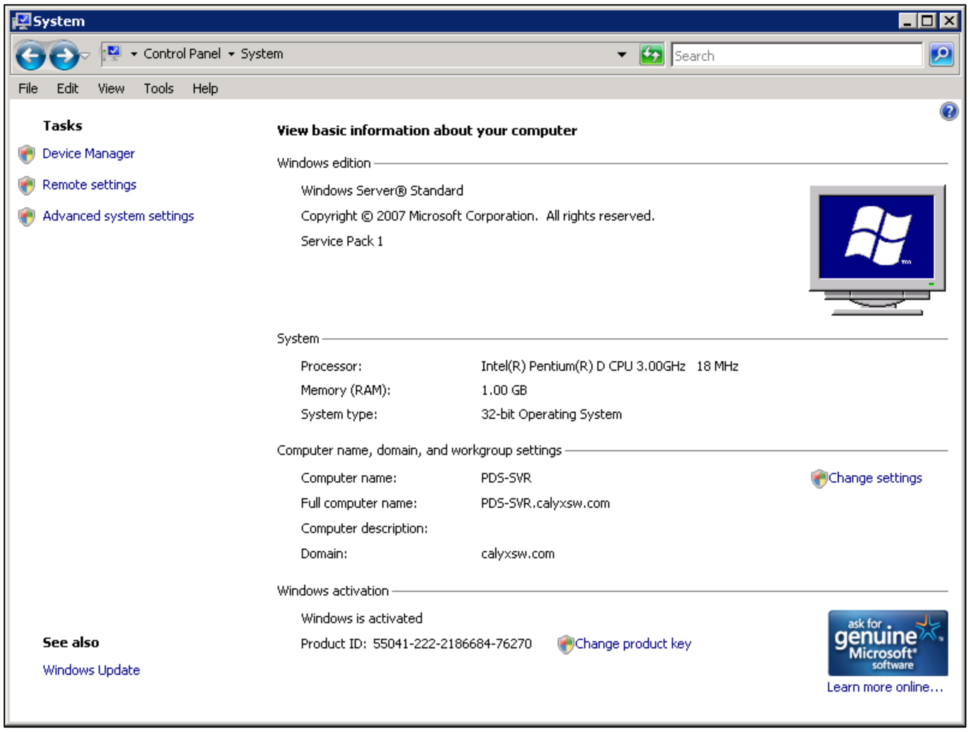


Figure 166: System Dialog

Determine Name Resolve Ability

Use the following to steps to verify NetBIOS name resolution capability.

1. Open a command prompt dialog.
2. Enter **ping** and the computer name (such as: **ping PDS-SVR**.)
3. Press **Enter**.

The IP address displays in the results such as the following example if the computer name can be resolved:

Pinging PDS-SVR [192.168.1.21] with 32 bytes of data:

Reply from 192.168.1.21: bytes=32 time<10ms TTL=128 Reply from 192.168.1.21: bytes=32 time<10ms TTL=128 Reply from 192.168.1.21: bytes=32 time<10ms TTL=128 Reply from 192.168.1.21: bytes=32 time<10ms TTL=128 Ping statistics for 192.168.1.21:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

The name is automatically translated to its IP address during the ping. The computer name is properly resolved if the IP address displays.

The message **Unknown host MYSERVER** displays if the computer name does not exist or is not properly set up on the network.

Note: The ping command does not work in some network configurations (such as: networks with certain firewalls).

PointCentral is still resolved and the response to the ping will look something like the following example if attempting to ping a computer in an environment that does not allow the ping command:

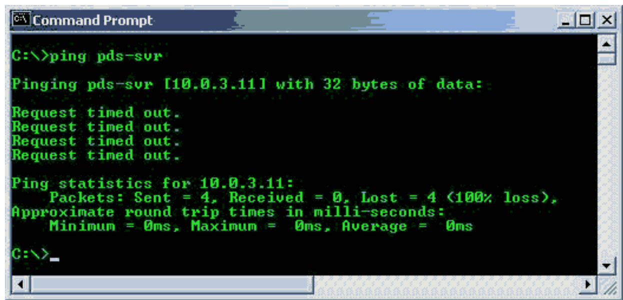


Figure 167: Request Error Example

Third-party tools are available to verify the client can resolve the IP address in environments where the ping command is not allowed.

Most installations should use DNS with valid domain names for Point clients to do the following:

- Resolve PointCentral to support connection over the public internet.
- Leverage existing DNS management and infrastructure.

Name Resolution with DNS

DNS is the recommended method to use to configure your network for clients to resolve to PointCentral.

The Domain Name system (DNS) is a distributed internet directory service used mostly for the following functions:

- Translating between domain names and IP addresses.
- Controlling Internet e-mail delivery.

Configure the DNS server to ensure the PointCentral server can be resolved using DNS. DNS services are provided if the Domain Name and SSL Certificate Store was used to register the domain.

Ensure Point clients can properly resolve the PointCentral server connect using the HTTPS protocol (port 443) when using DNS.

Firewall Setup

Configure the firewall to send incoming HTTPS traffic to PointCentral to enable internet access when the PointCentral server is behind a firewall or Network Address Translation (NAT) router.

The PointCentral server requires that only port 443 be open for inbound traffic. Test the PointCentral machine connection by visiting the web service URL in the web browser when not running a software firewall with the hardware firewall. Configure the firewall to allow PointCentral traffic when using a software firewall.

Web Service Errors and Warnings

The web service can return a warning or an error to the calling client. Contact the Point System Administrator when the error occurs.

- Messages contain the following:
- Warning or error Details
- Error code
- Instructions to contact System Administrator for assistance.

The results list is empty when an error occurs. The only returned values are the error code and description.

The information is logged in the **Event Log** in addition to the warnings/errors that are displayed to the Point User.

Web Service Warning Messages

Table 16: web service Warnings

Code	Warning Message	Resolution
-2	One or more requested Point fields are not currently supported by the Point Data Server (PDS). If these are valid fields, you can ask your Point System Administrator to support them using the PDS 'additional fields' feature.	Add the unsupported fields to the currently supported PointCentral fields. See Additional Fields for information about adding fields to the supported fields list fields.

Code	Warning Message	Resolution
-3	The maximum allowed number of tasks per list has been reached. Use more restrictive search criteria to select a smaller number of tasks. MaxRecordsGetTasks = 5000	The search result has exceeded the number of tasks per list limit. Use more restrictive search criteria to reduce the number of tasks returned in the search or change the **MaxRecordsGetTasks** default value to increase the maximum number of tasks allowed. See Web Service Parameters for more information about how to change the **MaxRecordsGetTasks** default value.
-4	The maximum allowed number of loans per list has been reached. Use more restrictive search criteria to select a smaller number of tasks. MaxRecordsGetLoanApps = 50000	The search result has exceeded the number of loans per list limit. Use more restrictive search criteria to reduce the number of loans returned in the search or change the **MaxRecordsGetLoanApps** default value to increase the maximum number of loans allowed. See Web Service Parameters for more information about how to change the **MaxRecordsGetLoanApps** default value.
-5	The maximum allowed number of Cardex records per list has been reached. Use more restrictive search criteria to select a smaller number of Cardex entries. MaxRecordsGetCardexEntries = 5000	The search result has exceeded the number of Cardex records per list limit. Use more restrictive search criteria to reduce the number of Cardex records returned in the search or change the **MaxRecordsGetCardexEntries** default value to increase the maximum number of Cardex records allowed. See Web Service Parameters for more information about how to change the **MaxRecordsGetCardexEntries** default value.

Web Service Error Messages

Table 22: web service Error Messages

Code	Error Message	Resolution
-11	Client internal error: Invalid condition in request.	Validate the condition type and value.
-12	An internal error has occurred on the Point Data Server.	Review the **Event Log** to determine error cause. Pay attention to Application events with the source **CalyxPdsService**. The Error is internal when unable to locate the cause in the **Event Log**. Record the exact details of the error and contact Calyx Support. See Event Log for more information about viewing the **Event Log**.
-13	Point Data Server cannot retrieve parameters from the database.	Verify the SQL Server is properly configured and running. Verify the components database connection strings are correct. Use the PointCentral Configuration Wizard to update the connection strings. See Configure PointCentral for information about the PointCentral Configuration Wizard.
-14	None of the requested fields are currently supported by Point Data Server (PDS). If these are valid fields, you can ask your Point System Administrator to support them using the PDS 'Additional Fields' feature.	Add the unsupported fields to the currently supported PointCentral fields. See Additional Fields for information about adding fields to the supported fields list fields.
-15	Client internal error: The requested search type is currently not supported by Point Data Server.	Record the exact details of the error and contact Calyx Support.
-16	Client internal error: The search date value is invalid. Please use a valid date.	Record the exact details of the error and contact Calyx Support.

Code	Error Message	Resolution
-17	Client internal error: Invalid Security Key. Client is not authorized to call this function. Please check the Point installation on the affected computer.	Verify the security key entered in the *Administration* site matches the key entered in Point Administrator. The error can also occur if the SQL database is offline on the PointCentral server.
-18	The Point Data Server is currently not available due to maintenance. See below for details.	Clear the **Upgrade Message** parameter in the web service configuration file. The error can also occur when not finished running the PointCentral Configuration Wizard. See PointCentral Components Configuration Files for more information about the Service configuration file.
-19	Client internal error: The array of folders passed to Point Data Server is invalid.	Record the exact details of the error and contact Calyx Support.
-20	Could not retrieve list from database.	Verify the database is properly configured and running. Verify the components database connection strings are correct. Use the PointCentral Configuration Wizard to update the connection string. Record the exact details of the error and contact Calyx Support if the database connection strings are properly configured. See Configure PointCentral for information about the PointCentral Configuration Wizard. See Administration Site Parameters for information about the database connection string parameters.
-21	Log in failed. Please check your User ID and Password and try again.	The Point User has entered an incorrect User ID or password. Reset the Point User password in the administration site.

Code	Error Message	Resolution
-22	Log in failed. This account has reached the maximum number of logs in attempts, and it is temporarily disabled.	Point Users are locked out of PointCentral after the maximum number of failed logs in attempts is reached within a lock out period. The lockouts expire automatically after the lock out period. See the Parameters page to configure the maximum number of failed login attempts and the lock out period. See Unlocking Users for information about unlocking Users. See Set Operational Parameters for information about accessing the parameters page and changing parameters.
-24	Could not update password, the new password did not pass the minimum-security requirements.	Set a different password that adheres to the following criteria: • Contains at least 8 characters. • Contain 3 of the 4 types (Number, symbol, Uppercase, Lowercase).
-25	The lender loan ID cannot be empty.	The error is internal. Record the exact details of the error and contact Calyx Support.
-26	Requests are only accepted through Secure Socket Layers (SSL).	The error is internal. Record the exact details of the error and contact Calyx Support.
-27	Could not access folder settings. User does not have the appropriate folder access rights.	Log out and log in again. The error can occur if a change is made to User access to a folder while the User is logged into Point.
-28	Client already has the latest version of requested settings file.	The caching mechanism of folder settings files is not working properly. The Point User should never see this message. Record the exact details of the error and contact Calyx Support.
-29	Invalid file setting name: it cannot be empty.	The error is internal. Record the exact details of the error and contact Calyx Support.

Code	Error Message	Resolution
-30	Invalid file setting ID: it could not be found.	The error is internal. Record the exact details of the error and contact Calyx Support.
-31	Invalid file setting ID and setting file name; when updating a file setting, they cannot be both empty.	The error is internal. Record the exact details of the error and contact Calyx Support.
-32	Invalid setting file name: it must end in .INI or. CSF.	The error is internal. Record the exact details of the error and contact Calyx Support.
-33	Could not find given file Setting ID for given Folder ID.	The error is internal. Record the exact details of the error and contact Calyx Support.
-34	Loan access rights not defined for given User ID.	Log out and log in again. Error can occur if a change is made to User access to a folder while the User is logged into Point.
-35	Loan can only be open in read-only mode for given User ID.	The Point User does not have the proper access rights to the folder to open the loan in read/write mode. See Add User Group Access for information about establishing and updating folder access rights.
-36	NetBios client name is blank.	The error is internal. Record the exact details of the error and contact Calyx Support.
-37	The file you have requested: is currently in use and reserved by ().	A Point User attempted to open a loan that is currently open by another Point User. Contact the Point User who has the file open or delete the reservation by force. See Delete Reservations for information about deleting loan reservations.

Code	Error Message	Resolution
-38	The loan you have requested is currently not accessible.	An internal error occurred when attempting to read a .BRW or .PRS file. Verify that the web service (the IIS anonymous User account) has the correct permissions to read loan files from the Point data folders. See Name Resolution for information about the IIS anonymous User.
-39	Could not save loan, the reservation does not exist.	See Reservations for information about loan reservations.
-40	Could not save loan, the reservation belongs to another User.	See Reservations for information about loan reservations.
-41	Could not save loan, the reservation was made from a different computer.	See Reservations for information about loan reservations.
-42	Could not save loan, the PDS internal queue that saves loans is unavailable.	The error is internal. Record the exact details of the error and contact Calyx Support.
-43	Could not save loan, at least one file to be saved or deleted must be supplied.	The error is internal. Record the exact details of the error and contact Calyx Support.
-44	Could not release loan reservation, only the original User may do so.	The error is internal. Record the exact details of the error and contact Calyx Support.
-45	Could not release loan reservation, it no longer exists.	The error is internal. Verify the date and time on both servers and ensure consistency. Record the exact details of the error and contact Calyx Support if not consistent.
-46	Folder access rights not defined for given User ID.	The Point User does not have the proper access rights to the folder. Change the folder access rights for the User. See Add User Group Access for information about establishing and updating User folder access rights.

Code	Error Message	Resolution
-47	Empty file name is not allowed, the data folder does not have borrower Auto File Naming enabled.	The Point User should log out and log in again. The auto file naming rules for a folder may have changes while a Point User was logged in.
-48	Empty file name is not allowed, the data folder does not have prospect Auto File Naming enabled.	The Point User should log out and log in again. The auto file naming rules for a folder may have changes while a Point User was logged in.
-49	Invalid file name when saving new borrower file; only. BRW, CB1, CB2, CB3, CB4 or. CB5 extensions are allowed.	The error is internal. Record the exact details of the error and contact Calyx Support.
-50	Invalid file name when saving new prospect file; only. PRS, CB1, CB2, CB3, .CB4, or .CB5 extensions are allowed.	The error is internal. Record the exact details of the error and contact Calyx Support.
-51	Invalid request when saving new file; only one new file may be saved.	The error is internal. Record the exact details of the error and contact Calyx Support.
-52	Invalid request when saving new file; file already exists.	The error is internal. Record the exact details of the error and contact Calyx Support.
-53	Invalid request when saving new file; could not create reservation.	The error is internal. Record the exact details of the error and contact Calyx Support.
-54	Could not find file.	The requested file no longer exists. Error may occur if a file is changed or deleted from PointCentral while a Point User had an obsolete list of files displayed on the screen.
-55	Only the main borrower loan file (with the 'BRW'extension) can be used in this operation.	The error is internal. Record the exact details of the error and contact Calyx Support.
-56	Only the main prospect loan file (with the 'PRS'extension) can be used in this operation.	The error is internal. Record the exact details of the error and contact Calyx Support.

Code	Error Message	Resolution
-57	When getting or saving a task file, file name must end with the '. TSK' extension.	Internal Error. Record the exact details of the error and contact Calyx Support.
-58	Requested TSK file not found.	The requested file no longer exists. Error may occur if a file is changed or deleted from PointCentral while a Point User had an obsolete list of files displayed on their screen.
-59	The file you have requested to delete is currently in use and reserved by (). This file has been reserved since on the computer ().	A Point User attempted to delete a loan that is currently open by another Point User. Contact the Point User that has the file open or delete the reservation by force. See Delete Reservations for information about deleting loan reservations.
-60	Loans in given folder can only be open in read-only mode for given User ID. New loans cannot be created in given folder.	The Point User does not have the proper access rights to the folder to write loans. The administrator can change the folder access rights for the User. See Add User Group Access for information about establishing and updating User folder access rights.
-61	Could not copy file to destination folder; could not generate auto file name since destination folder does not support auto file naming.	Point User should logout and log back in.
-62	Could not move file from source folder; User only has access mode of 'read-only' on source folder.	The Point User does not have the proper access rights to the folder to move loans. The PointCentral administrator can change the folder access rights for the User. See Add User Group Access for information about establishing and updating User folder access rights.
-63	Could not copy file to destination folder; access rights not defined on destination folder for given User ID.	The Point User does not have the proper access rights to the folder to copy loans. The PointCentral administrator can change the folder access rights for the User. See Add User Group Access for information about establishing and updating User folder access rights.

Code	Error Message	Resolution
-64	Could not copy file to destination folder; access rights are 'read-only' on destination folder for given User ID.	The Point User does not have the proper access rights to the folder to copy loans. The PointCentral administrator can change the folder access rights for the User. See Add User Group Access for information about establishing and updating User folder access rights.
-65	Could not copy file to destination folder; the destination file: is currently in use and reserved by (). This file has been reserved since on the computer ().	A Point User attempted to copy over a loan that is currently open by another Point User. Contact the Point User that has the file open or delete the reservation by force. See Delete Reservations for information about deleting loan reservations.
-66	Could not copy file to destination folder; the destination file already exists.	The error is internal. Record the exact details of the error and contact Calyx Support.
-67	Could not move file from source to destination folder; the source file is currently in use and reserved by (). This file has been reserved since on the computer ().	A Point User attempted to move a loan that is currently open by another Point User. Contact the Point User that has the file open or delete the reservation by force. See Delete Reservations for information about deleting loan reservations.
-68	Could not generate auto filename. Make sure the maximum number of unique filenames generated for the given period has not been reached.	Verify the auto file name rules in the *Administration* page. See Add User Group Access for information about auto file naming.
-69	Your computer's date and time are more than 24hours out of date relative to the Point Data Server (PDS). PDS security requires that your computer's date and time are accurate.	The difference between the date and time on the Point client and the date and time on PointCentral cannot exceed 24 hours. Verify that the correct date and time is set on all Point clients and PointCentral.
-70	The requested file is marked as read-only on the PDS Server.	Verify the files in the data folders in PointCentral are not marked as read-only (in the file system).
-71	The destination file is marked as read-only on the PDS Server.	Verify the files in the data folders in PointCentral are not marked as read-only (in the file system).

Code	Error Message	Resolution
-72	The source file is marked as read-only on the PDS Server; it cannot be moved.	Verify the files in the data folders in PointCentral are not marked as read-only (in the file system).
-73	The version of Point on this computer is not supported by this Point Data Server (PDS). Please contact your Point Administrator to upgrade Point on this computer.	Upgrade the Point client to the compatible version of PointCentral.
-74	The PDS database version does not match the expected database version.	Run the PointCentral Configuration Wizard to upgrade your database to the version required. See Configure PointCentral for information about the PointCentral Configuration Wizard.
-75	There is no template set access rights defined for this User.	Define access rights for the User for a template set as required. See Add User Group Access for information about defining template access rights.
-76	Your template set archive is currently not accessible.	Rebuild the relevant template set and run the PointCentral Configuration Wizard to reset NTFS Permissions as required. See Rebuilding Template Sets and Configure PointCentral for information about the PointCentral Configuration Wizard.
-77	The requested template file is not available for this User or does not exist.	Rebuild the relevant template set and run the PointCentral Configuration Wizard to reset NTFS Permissions as required. See Rebuilding Template Sets and Configure PointCentral for information about the PointCentral Configuration Wizard.
-78	The requested template file has not changed.	The error is internal. Record the exact details of the error and contact Calyx Support.
-79	You only have read-only access rights for the requested template file.	Give the User read and write access rights for the relevant template type as required.
-80	Invalid template file type or template file name; when updating a template file neither can be empty.	The error is internal. Record the exact details of the error and contact Calyx Support.

Code	Error Message	Resolution
-81	Invalid template file name: it can only be 255 characters or less.	Verify the Point User enters a template file name that is 255 characters or less.
-82	Invalid template file name: it must end with the correct file extension for this template type.	The error is internal. Record the exact details of the error and contact Calyx Support.
-83	Template file access rights not defined for given User ID -OR- this Template file no longer exists. It may have been deleted by another User since you logged in to Point. Please logout and then log in to Point to see the latest Template files.	Either the file has been deleted or the User does not have access rights for the given template type. Define access rights for the given template type as required. See Add User Group Access for information about defining template access rights.
-84	The template file you have requested: is currently in use and reserved by (). This file has been reserved since on the computer ().	A Point User attempted to open a loan that is currently open by another Point User. Contact the Point User that has the file open or delete the reservation by force. See Delete Reservations for information about deleting loan reservations.
-85	Wrong function called for given template type. The given template file type does not require a reservation.	The error is internal. Record the exact details of the error and contact Calyx Support.
-86	You do not have access rights on the requested template set.	Define access rights for the Point User for the given template set as required. See Add User Group Access for information about defining template access rights.
-87	Empty template file name is not allowed.	Define a proper name for the template file.
-88	Invalid file name when saving new template file; only the extensions are allowed for this template type.	The web service validates that the correct extension is sent from Point when a template file is being created or updated. **Note:** Error should not occur unless there is a problem with the Point client.
-89	Invalid request when saving new template file; file already exists.	Use a different name for the new template file.
-90	Could not save new template file, the PDS internal queue that saves template files is unavailable.	The error is internal. Record the exact details of the error and contact Calyx Support.

Code	Error Message	Resolution
-91	Invalid request when saving new template file; could not create reservation.	The error is internal. Record the exact details of the error and contact Calyx Support.
-92	Could not save template file, the reservation does not exist.	The reservation no longer exists for the template file that was being saved. Either a PointCentral administrator manually deleted the reservation or the reservation timed-out and another Point User has edited the template file. Close Point and open the template file (get a new reservation) before attempting to save the template file again.
-93	Could not save template file, the reservation belongs to another User.	The error is internal. Record the exact details of the error and contact Calyx Support.
-94	Could not save template file, the reservation was made from a different computer.	The error is internal. Record the exact details of the error and contact Calyx Support.
-95	Could not save template file, at least one file to be updated must be supplied.	The error is internal. Record the exact details of the error and contact Calyx Support.
-96	Could not save Cardex record: it is empty. At least one field value must be entered.	Enter at least one value in the Cardex record before saving it to PointCentral.
-97	You do not have access rights on the requested Cardex database.	Define access rights for the Point User for the given Cardex database as needed.
-98	The original Cardex record was not found.	The Cardex record might have been deleted by another Point User.
-99	Invalid Search of Cardex Entries. Error:	The error is internal. **Note:** Error should not occur unless there is a problem with the Point client.
-100	Invalid template file: file size (%FILESIZE% bytes) greater than maximum template file size (%MAXTEMPLATEFILESIZE% bytes).	A Point User attempted to save a template file that was larger than the maximum template file size allowed. See FileSync Parameters for information about the **MaxTemplateFileSizeKB** parameter.

Code	Error Message	Resolution
-101	Could not delete file from source folder.	User does not have delete access for source folder.
-102	Could not copy file from source folder.	User does not have copy access for source folder.
-103	Could not move file from source folder.	User does not have move access for source folder.
-104	Your password has expired. Please change your password.	Update password per the guidelines per company policy.
-105	You are only allowed to save your own files or other Users' files that you have access to.	Check the originator or processor name fields to verify that the names match.
-106	PointCentral server is not properly licensed and unable to log you in.	Contact the Point System Administrator.