PointCentral

User Guide

Version 9.8

February 2018

6475 Camden Avenue, Suite 207
San Jose, CA 95120

Corporate Office: **(408) 997-5525**
Product Support: **(800) 342-2599**
Sales: **(800) 362-2599**

Contents

Figures

Tables

Preface

This information describes how to use and administrate PointCentral and to provide an overview of PointCentral and its functions, as well as installation, configuration, and operation tasks.

This information includes:

- Installation and configuration steps
- System requirements and prerequisites
- Processes for using PointCentral

This information is designed to help PointCentral administrators perform the following tasks:

- Plan for installation
- Install and operate
- Configure operating environment
- Manage users, templates, data folders, rules, and Cardex databases

In this topic

Conventions

The following conventions are described in this information:

- Typographical conventions
- Terminology

Typographical conventions

The following table shows how typographical conventions are used in this information to identify different types of controls and screen characteristics:

Format	Example
Button	Click the **Rebuild Template Set** button to rebuild the template set.
Check box	Select the **Enable Auto File Naming** check box.
Dropdown list **Dropdown list option**	Select *SQL Server Authentication* from the ***Authentication*** dropdown list.
Field	Enter the user's first and last names in the *Full Name* field.
Links	For information about the configuration wizard, refer to ***Configuring PointCentral***, on page 28. For product support information, go to **www.calyxsupport.com**.
Menu name or path	Select ***Configuration > Point Fields > Supported Fields***.

Format	Example
Radio button	Select the **I accept the terms in the license agreement** radio button and click **Next** to proceed.
Screen	Select ***Users > Add User*** from the navigation bar to access the ***Add User*** screen.
Section	Scroll down to the *User Group Access Rights* section.
User input	Enter *iiserest /stop* and press <Enter>.

Terminology

The terminology shown in the following table is used throughout this information.

Example	Instruction
<Ctrl><F>	Press the <Ctrl> key on the keyboard while also pressing the <F> key.
Enter or complete	Refers to manual entry of information.
Configuration > Point Fields > Supported Fields	Select the ***Configuration*** menu, select ***Point Fields***, then select ***Supported Fields***.
Select	The selection of an item or option. For example, highlight an item by clicking the mouse and dragging it over the item, double-click the item to select it, or select the **Enable Auto File Naming** check box.

Related information

- *PointCentral User Guide*
- *Access* ***Knowledge Base articles***

Product assistance

The following product support is available:

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)	

Attention

When you contact Technical Support, have the following information available:

- *Your name*
- *Your company name*
- *The PointCentral version you are operating*
- *Your account ID*

Overview 1

PointCentral is a convenient, secure way to share Point files across your organization. Loan data is stored on a central server, making Point files accessible from any location—even if you must use public Internet access. With the PointCentral performance and speed, loan originators and processors can instantly search, open, edit, and save loan files on the central server—right from their Point desktops through an Internet connection. You can even generate management reports that include information from different offices.

In this topic

Time-consuming operations (such as searches and reports) that were not possible for large numbers of loans over the limited bandwidth connection to a network branch are now easy.

File access is centrally administered, which provides a high level of control over loan data. Each user's access rights to any data folder can be granted, modified, or revoked centrally. The User Group feature makes user management easy by grouping together those users who have similar access needs. Adding or removing access rights to a data folder for all users in a user group is now a single mouse click. Users are defined globally on PointCentral, which eliminates the repetitive creation of the same user in every data folder required by conventional Point. With PointCentral reports, you can quickly view user and group access rights to data folders, templates, rules, and Cardex at a glance.

PointCentral manages templates, including:

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

Now you can make changes to templates, confident that all Point users are running the latest versions. PointCentral also manages Cardex databases, so you can decide which users need to share the same database and know that all users can access Cardex quickly.

With Point users can change passwords at any time, without affecting their access rights. PointCentral combines the control that your organization needs with the speed and flexibility that loan originators and processors demand.

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, a log in, and an Internet connection. With PointCentral, you can copy or delete data files only from within Point, ensuring that loan data always remains secure.

Lightning-fast performance

With PointCentral you can search loan files, review task lists, and run reports hundreds of times faster than with Point alone. PointCentral compresses the Point files and other information exchanged between Point and PointCentral which speeds up all interactions, including file opens and saves.

Collaboration and visibility

Share loan files with everyone in your organization no matter where they work; in a branch office, remotely, or even from a client's location. With Point, headquarters and branch offices can monitor business by running reports based on loan files stored on PointCentral.

Transparent to Point users

With Point, loan originators and processors can work with files stored on the PointCentral server exactly as they work with their loan files today. There's nothing new to learn.

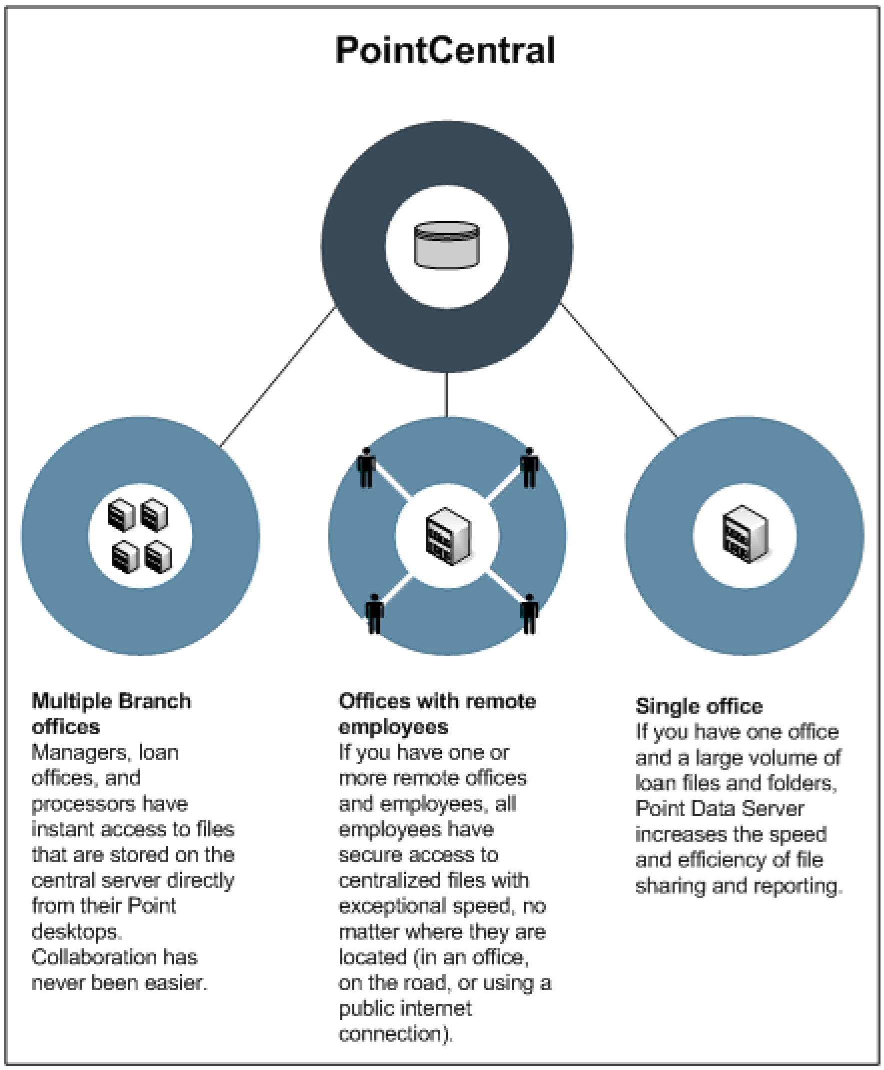


Figure 1. PointCentral configuration

Architecture

In a conventional Point environment, Point accesses all of the files and indexes by using the file system. Direct file access in conventional Point requires the following configuration:

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

For most local Point users, these solutions are fine. But in an organization with multiple branches, the data cannot be shared across the organization without a VPN. Some common operations in conventional Point are very time-consuming in an environment that contains multiple folders, a large number of loans, or a limited bandwidth VPN. This results in a system that can seem slow and unusable.

PointCentral eliminates the need for a VPN by transferring the Point files over a secure HTTPS connection to the PointCentral server at a central headquarters 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. Time-consuming Point operations such as find, tasks, and reports can access this common information from the database orders of magnitude faster than conventional Point.

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

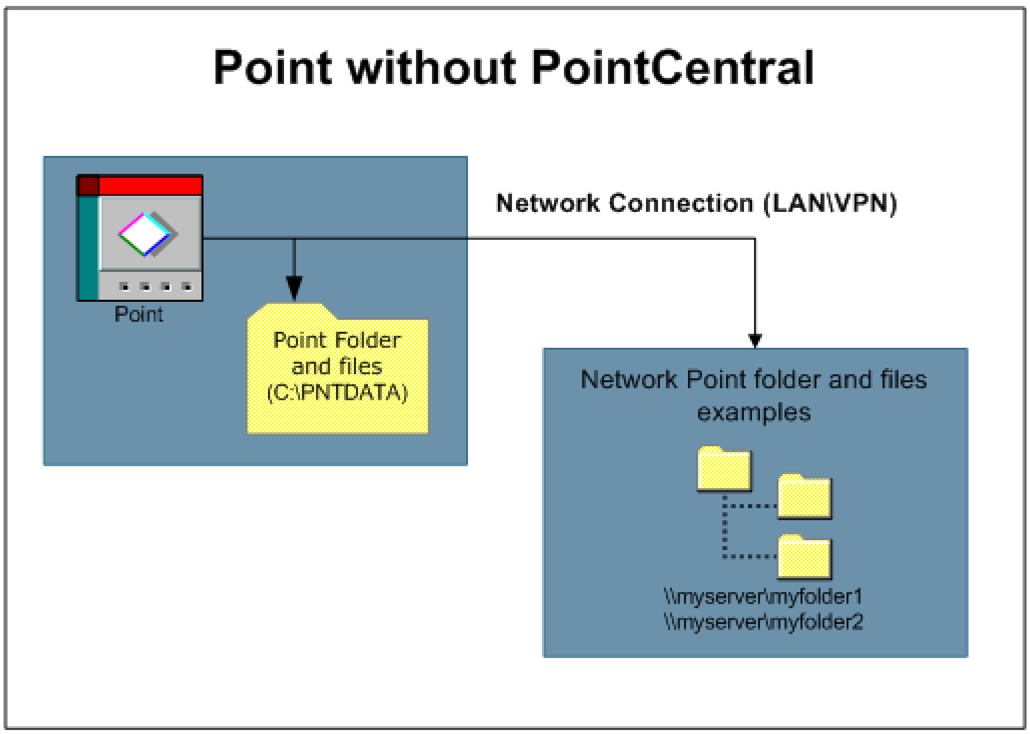


Figure 2. Conventional Point

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

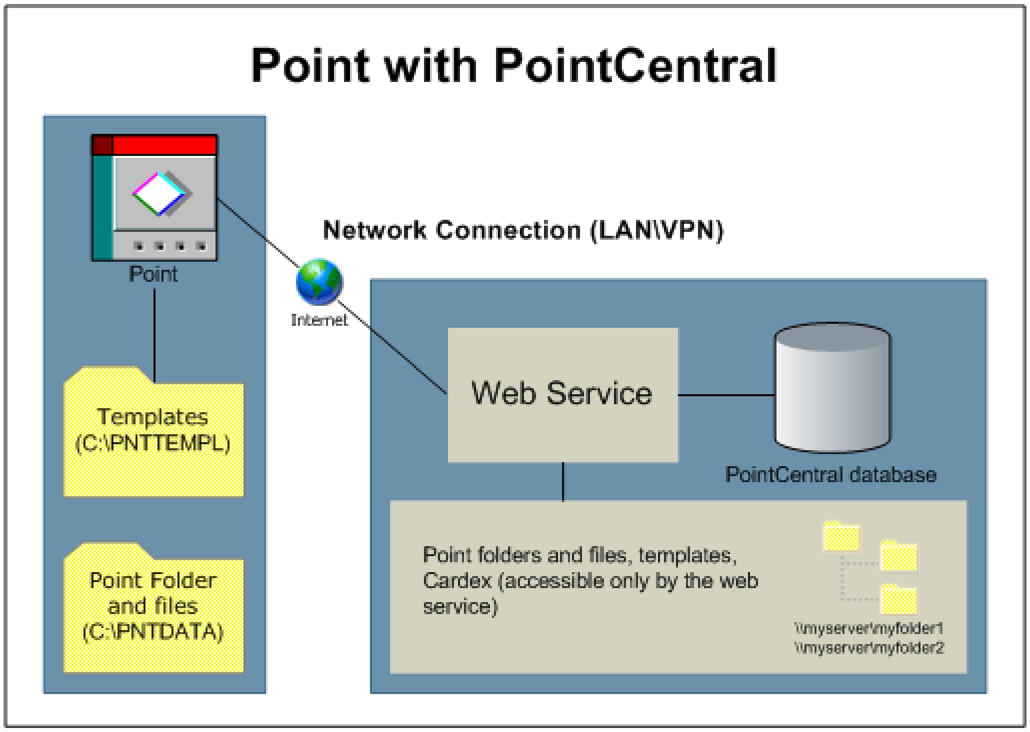


Figure 3. Point with PointCentral

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

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

The web service in turn accesses the SQL database. There is no file share. This eliminates the VPN and results in much faster execution times when accessing the Point Find, Advanced Find, List Co-Borrowers, Search Tasks or Reports screens.

The SQL database maintains read-only copies of select Point fields to accelerate certain operations, such as searches. 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 the 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

These components are shown in the following diagram.

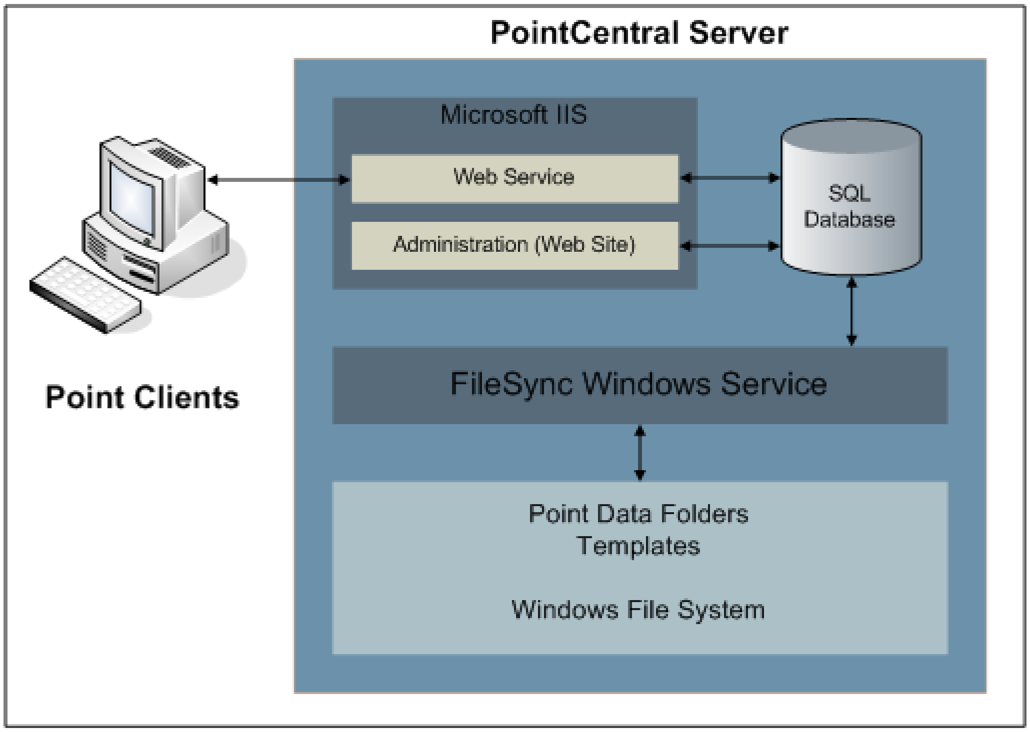


Figure 4. PointCentral components

Web service

Point sends requests to the web service (CalyxPdsService). This Microsoft Internet Information Services (IIS) Web Service queries the database and accesses loans or returns lists of results. Conventionally time-consuming operations such as searches, advanced searches, tasks, and reports are returned much faster than the file scanning method used by conventional Point.

Administration web site

The Administration Web Site is the administrative interface to PointCentral. The system administrator uses this interface to:

– Create Point data folders, users, and user groups
– Assign access rights to data folders
– Configure, monitor, and manage PointCentral

PointCentral administration has many other functions including importing of conventional Point data folders, users and access rights.

FileSync Windows Service

The FileSync (CalyxPdsFileSync) Windows Service monitors individual Point files for changes as they are saved by Point users through the HTTPS connection to the web service.

FileSync stores loan files internally on the server file system. The web service also reads the loan files from the server file system. This process is invisible to the Point client, which opens and saves Point files by transmitting them over the HTTPS connection to the PointCentral server. Any changes that are detected in the Point files are synchronized to the database almost instantaneously. This keeps the information in the database synchronized with the Point files and ready for a query at any time. The FileSync component is also responsible for switching conventional Point data folders to accelerated and vice-versa.

SQL database

The SQL database stores the common information that is required for Point searches, tasks, reports, and related operations which provides an instantaneous response to these common Point operations.

PointCentral Configuration Wizard

The PointCentral Configuration Wizard is used to easily create or upgrade a database. Through a series of Wizard screens, the administrator simply clicks *Next* to configure a new system or upgrade a previous version of the database. It updates the necessary connection strings in all components.

Point loan and data folder access

PointCentral can access all of the PointCentral loan files and data folders through the secure HTTPS connection to the web service. Point needs only the HTTPS connection to the PointCentral server. The Windows file share to data folders required by conventional Point is eliminated with PointCentral.

Templates and Cardex

PointCentral also manages templates and Cardex databases. All template files are stored on the centralized server and distributed to the Point clients as needed.

PointCentral processes requests from Point extremely quickly. When Point receives the results of an operation, most of that time is used for transmitting the results over the limited bandwidth available over the link between the net branch and headquarters.

Related information

- *Refer to* ***Operating requirements****, on page 17, for compatible SQL Server versions.*
- *See* ***Domain name setup****, on page 22, for more details.*

Performance tests

A test environment was created for you to check the performance of your server. 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 roughly a DSL connection shared by ten Point users.

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

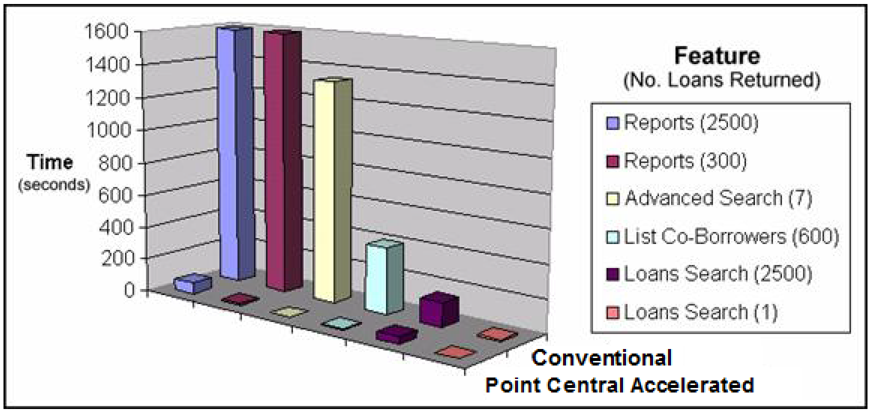


Figure 5. ***Performance advantage of PointCentral acceleration***

The following table shows the results when the bandwidth was limited to 100KB download (roughly a 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 tables shows the results in a 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
Loans search	2,500	9 seconds	2 seconds
Loans search	1	1 second	1 second

Web service

The web service is responsible for serving Point client requests when a Point user is searching for loans or tasks, opening and saving loans, generating reports, or other necessary operations.

Recommendation

Although none of the steps in this information are required, Calyx recommends that you read it to familiarize yourself with the concepts.

Web services enable programs on various computers to communicate with other programs on similar or disparate computers transparently over a network.

The web service, one of the major components of the PointCentral, is a Microsoft Internet Information Services (IIS) Web Service.

Access the web service from the Internet Information Services Manager (***Start > Administrative Tools > Internet Information Services (IIS) Manager***).

When PointCentral is installed, a virtual directory named **service** is created in the Microsoft IIS Default Web Site. When you access the URL, you are basically making a call to the web service.

When the client identifies a data folder as accelerated, rather than scanning the folder for files or accessing its file system-based index, it makes calls to the web service.

When there are a large number of folders or files, or limited bandwidth between the client and its data folders, such calls to the web service greatly improve the speed in receiving results.

A clear improvement in performance is noticeable in the following features:

Loans

- Search:
  - By Last Name
  - By File Name
  - By Loan Originator Name
  - By First Name
  - By Contact Date
- Advanced Search
  - By Subject Property Address
  - By Present Address
  - By Processor Name
  - By Borrower Home Phone
  - By Borrower Business Phone
  - By Co-Borrower First Name
  - By Co-Borrower Last Name
  - By Co-Borrower Home Phone
  - By Co-Borrower Business Phone
- List Co-Borrowers
- Open
- Save
- Copy
- Move

- Delete

Folders

- Retrieving list
- Retrieving access rights
- Retrieving and setting folder settings

Tasks

- All open tasks
- All overdue tasks
- Advanced search

Reports and Marketing documents

- Search in one or more accelerated data folders
- Support for all standard reports and marketing documents (included with Point)
- Support for custom screens and fields
- Support for additional fields

The back end database is implemented by using Microsoft SQL Server. The following figure illustrates that when the Point client makes a request to the web service, the request is made to the PointCentral middle tier. The middle tier then accesses the back-end SQL database to retrieve the results orders of magnitude faster than the conventional way. Not all loan information is stored in the PointCentral database; it contains only the information needed to improve performance when searching, opening or saving, loans and tasks.

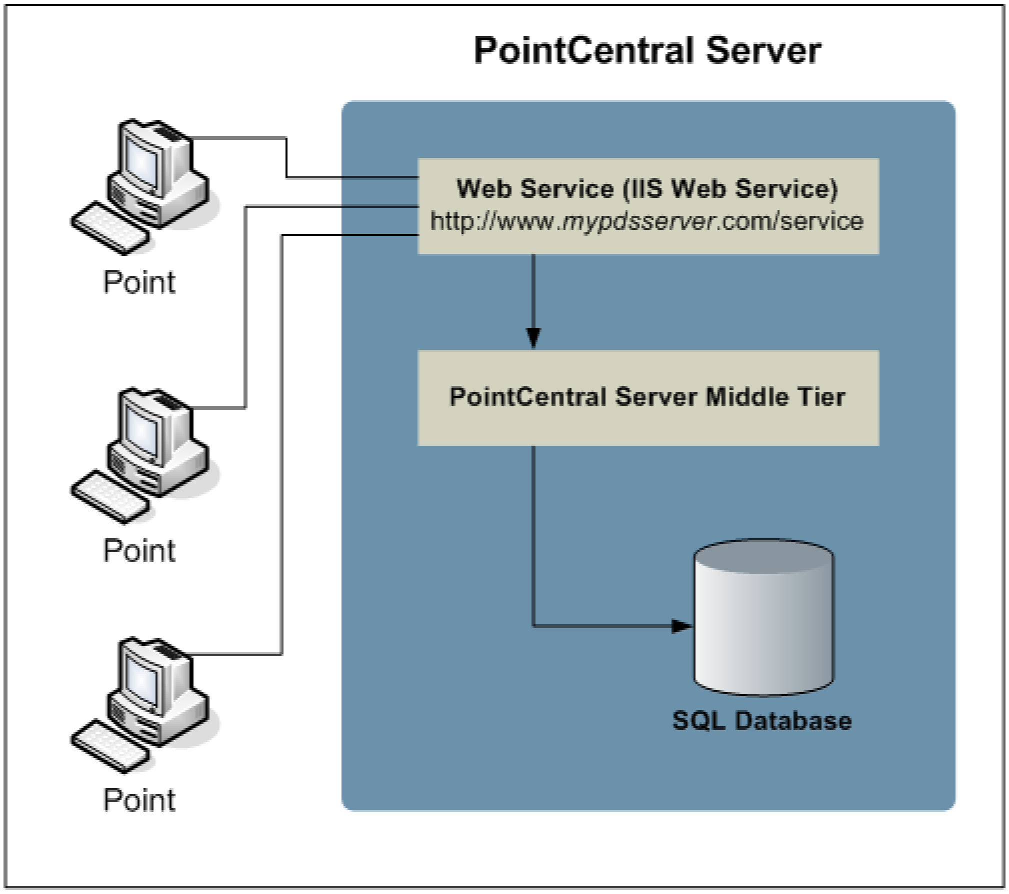


Figure 6. Loan retrieval from PointCentral server

Launching the web service

Unlike the administration site which is a standard web site, you cannot launch the web service because it is a web service that communicates with other applications. The Point client and web service exchange XML (Extensible Markup Language).

Although you cannot call the web service directly (you must use Point), you must verify whether the web service is properly configured and running. When you open the main web service page through a browser, it displays a standard HTML page with information about the web service status.

To open the main web service page:

1. Log on to the computer where PointCentral is installed.
2. Select ***Start > All Programs > Calyx Software > PointCentral > PointCentral Service***.

   This opens the local host web site.

   Note

   localhost *resolves to the IP address 127.0.0.1, which should resolve to your local server. You might receive a warning from Internet Explorer because you are not accessing your server URL, therefore the common name in the SSL Certificate does not match.*

3. From any server in your network, point your browser to your web service URL.

   Related information

   - *Refer to* ***Administration detail****, on page 44, for more information about the administration site.*
   - *See* ***SSL certificate****, on page 23, for more information about the local host service and the SSL certification.*

   The web service main page is displayed which indicates that the PointCentral and its back-end SQL database were installed properly, and that you can resolve PointCentral properly.

Event log

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

To start the Windows Event Viewer, select Administrative Tools from the Control Panel or the Start menu and select Event Viewer.

The Event Log displays a message from the web service (the event with a source of ***CalyxPdsService***). Double-click an event in the list from ***CalyxPdsService*** to view the event properties.

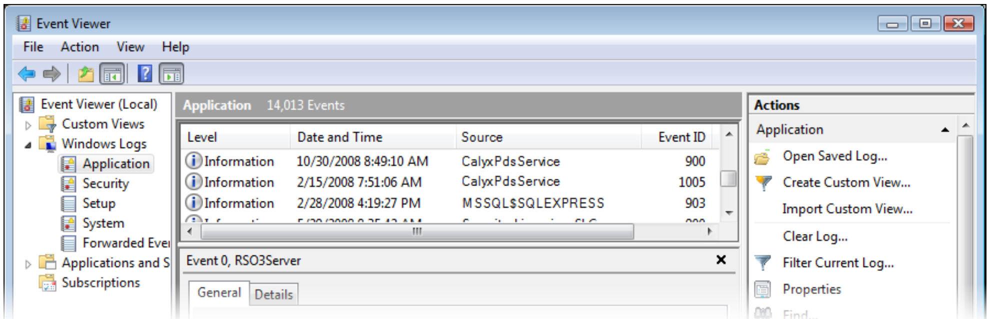


Figure 7. Event Viewer

In this example, the web service indicates that it has started. It also includes its exact major, minor, and build number. This event is created whenever the *first request* is made to the web service after it has previously stopped.

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

- PointCentral was rebooted
- Microsoft IIS was stopped and restarted
- The default web site in Microsoft IIS was stopped and restarted
- The maintenance message or any other value in the web service configuration file was changed
- The version was updated.

Attention

The first request to the web service might take a few moments to process because the web service is initializing. Subsequent requests are completed much faster.

Related information

*Refer to **Advanced configuration**, on page 59, for more information about changing values in the web service configuration file.*

Messages to Point users

In normal requests from clients to the web service, the results are returned to Point. However, sometimes a problem occurs which causes a warning or an error message to display. These messages are issued immediately after the results are returned to the Point client.

The following messages are some examples:

- The web service is in *Upgrade Mode* (while you are running the PointCentral Configuration Wizard to upgrade PointCentral or to update its connection strings).
- A Point user requested an unsupported field while you were running a report.

- The maximum number of loans or tasks requested exceeds the system maximum.

Related information

- *Refer to* ***Advanced configuration****, on page 59, for more information about the loan and task maximum capacity.*
- *For a full list of the possible error codes and messages returned to Point users and information about unsupported fields, refer to* ***Supported fields****, on page 151.*

Multiple server deployment

Most organizations that install and configure PointCentral need only one system to centralize all of their folders. However, PointCentral can also be deployed in other ways.

Regional deployment

For larger organizations, a regional deployment might accommodate bandwidth requirements better than a centralized deployment. In this scenario, the branches are divided into groups or regions. One server would be deployed for every region and support a feasible number of branches as shown in the following figure:

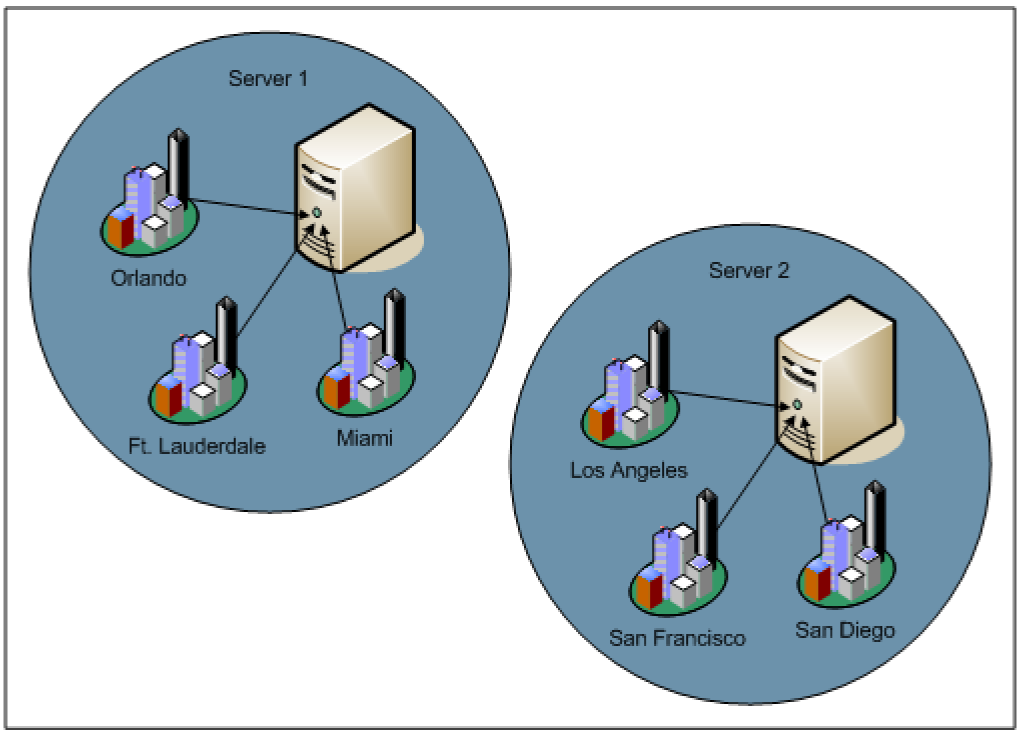


Figure 8. Regional deployment

Important

Currently, you cannot connect multiple PointCentral servers. The setup assumes you do not need to run reports across accelerated folders from different servers. However, you can create your own process to transfer data from all PointCentral databases into a centralized database (by using SQL Server replication, for example).

Calyx does not support any direct access to the PointCentral database, and it is beyond the scope of this information to define how this is done.

Branch deployment

In certain instances, your organization might want to set up one server per branch. This configuration provides lower bandwidth requirements, faster responses, and increased flexibility in reporting through the SQL server database.

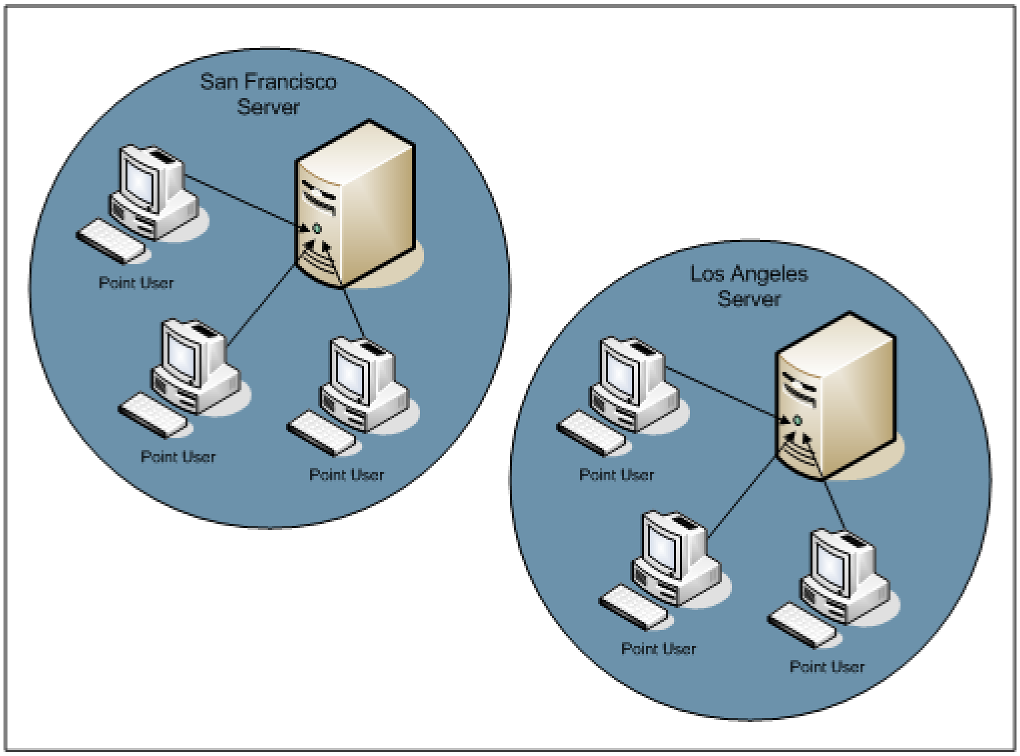


Figure 9. Branch deployment

Fault Tolerance

SQL Server backup

Make daily (or even hourly) backups of your data including your SQL Server data and transaction logs.

In addition, you could also have a warm backup SQL Server that implements SQL Server replication. If the primary SQL Server fails, you can easily switch to your hot backup, minimizing downtime.

Related information

See your Microsoft documentation for more details about SQL Server replication.

Data folder backup

Make daily (or even hourly) backups of your data folders.

In addition, you could create a process by which you are copying your data folders to another PointCentral server, its only purpose is a hot backup. Make sure you install PointCentral on this server, but do not run FileSync until needed. If the primary system fails, you can easily switch to the hot backup, minimizing downtime.

Important

Verify that only one FileSync Windows service is running at any given time.

If you implement a warm backup server with both SQL Server replication and the method for copying loan and template files that all directories in your warm backup server must match the directories used in the live production environment.

You can also increase reliability by using fault tolerant disk configurations such as RAID. RAID is the acronym for Redundant Array of Independent (or Inexpensive) Disks, a category of disk drives that employ two or more drives in combination for fault tolerance and performance.

The following table describes the RAID levels:

Table 1. 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) but no 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. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.
2	Error-Correcting Coding	Not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level.
3	Bit-Interleaved Parity	Provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used.

Table 1. RAID levels (Continued)

Level	Title	Description
4	Dedicated Parity Drive	A commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk. If a data disk fails, the parity data is used to create a replacement disk. A disadvantage to Level 4 is that the parity disk can create write bottlenecks.
5	Block Interleaved Distributed Parity	Provides data striping at the byte level and also stripe error correction information. This results in excellent performance and good fault tolerance. **Level 5 is one of the most popular RAID implementations**.
6	Independent Data Disks with Double Parity	Provides block-level striping with parity data distributed across all disks.
0+, 1	A Mirror of Stripes	Not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them. Used for both replicating and sharing data among disks.
10	A Stripe of Mirrors	Not one of the original RAID levels, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.
7	N/A	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, secure place. Without the Private Key, the SSL certificate cannot be restored into IIS.

Renew the SSL Certificate before it expires. If the SSL certificate expires or becomes invalid, Point clients cannot use PointCentral because the valid SSL certificate enables the secure connection between Point and PointCentral.

Installation 2

Before you can install PointCentral, your environment must meet the minimum system requirements. In addition, there are several prerequisites that must be met before installation can be successful.

In this topic

Operating requirements

System requirements

The following hardware is required to support PointCentral:

Table 2. System requirements

Component	Requirement
Processor	Intel Pentium 4 processor, 3.0+ GHz 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 3. Software requirements

Component	Version
Operating system	• Microsoft® Windows Server® 2016, with latest service pack, IIS 7.0 • Microsoft Windows Server 2012, Service Pack 1, with IIS 7.0 and Application Server Role* • Microsoft Windows Server 2008 (including R2), with IIS 7.0 and Application Server Role* *Calyx does not recommend or 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 4.6.2.
SQL Server*	
Large organizations (>50 users)	• Microsoft SQL Server® 2016 Standard or Enterprise Edition, with latest service pack • Microsoft® SQL Server® 2014 Standard or Enterprise Edition, with latest service pack • Microsoft SQL Server 2012 Standard or Enterprise Edition, with latest service pack • Microsoft SQL Server 2008 Workgroup, Standard, or Enterprise Edition, with latest service pack
Small organizations (<50 users)	• Microsoft SQL Server 2016 Express Edition, with latest service pack • Microsoft SQL Server 2014 Express Edition, with latest service pack • Microsoft SQL Server 2012 Express Edition, with latest service pack • Microsoft SQL Server 2008 Express or 2008 Express with Tools Edition, with latest service pack
Network environment	• Domain name • An SSL certificate that matches the domain name, installed on the IIS default web site *The Calyx Resolver System can provide, if needed, a Calyx-hosted domain name and *wildcard SSL certificate free of charge.* • Static IP address
Client	• Point, version 9.6, 9.7, or 9.8 • One of the following operating systems: – Microsoft Windows 10 – Microsoft Windows 8 – Microsoft Windows 7 • Internet Explorer version 11.0, or later

***Important**

Calyx Software does not directly support third-party products, including Microsoft .NET Framework, Internet Information Services (IIS), SQL Server, SQL Server Express, or any other third-party applications mentioned in this information.

Related information

- *Refer to **Calyx Resolver**, on page 23, for more information about Calyx Resolver.*
- *Refer to the **Point User Guide** for information about installing the Point client.*

Prerequisites

The following prerequisites are necessary before you can perform a new PointCentral installation:

Requirement

You must use the installation and configuration instructions that are provided in this information. If you do not install these components by using the PointCentral-specific instructions, the installation will fail.

- Set up a fixed IP address

Note

Contact your system administrator to properly set up the IP address. You must still set up your network so you have a fixed external (or public IP address available for your server.

- Purchase and register a domain name

Note

You can also use Calyx Resolver to provide a host name and DNS hosting.

- Configure the domain name server (DNS)
- Obtain and configure an SSL certificate
- Install and configure Microsoft .NET Framework,

Important

Calyx Software does not directly support third party products, including Microsoft .NET Framework, Internet Information Services (IIS), SQL Server, SQL Server Express, or any other third-party applications mentioned in this information.

- Install and configure Microsoft Internet Information Services (IIS)
- Install and configure Microsoft SQL Server or SQL Server Express

Recommendation

It is highly recommended that you review information about SQL log file sizing before you begin the installation.

Related information

- *Refer to **Calyx Resolver**, on page 23, for more information about Calyx Resolver.*
- *Refer to the Microsoft article, **Shrinking the Transaction Log**, for more information about log file sizing.*

Installation and configuration overview

To ensure proper installation and configuration, perform the installation and setup in the following sequence:

Table 4. Installation and configuration overview

Step	Description	
1	**Pre-Installation requirements**	
	• Add server roles: Application servers and Internet Information Services (IIS)	
	• Obtain a domain name and fixed IP address	
	• Configure the domain name server (if applicable)	
	• Request an SSL certificate (if applicable)	
	• Install SSL certificate (if applicable)	
	• Install Microsoft SQL server or SQL Server Express	
2	**Installation**	
	• Install PointCentral	Installing PointCentral
	• Run the PointCentral Configuration Wizard	Configuring PointCentral
3	**Resource administration and configuration**	
	• Set operational parameters	Setting the operational parameters
	• Set site parameters	Administration site parameters
	• Import existing Point resources	Importing resources
	• Add users and user groups	Users and user groups
	• Add data folders	Data folders
	• Add templates	Template sets
	• Add Cardex databases	Cardex databases
	• Add rules	Rules
	• Configure Point client	Client configuration

Pre-installation requirements

Adding server roles

Microsoft Internet Information Services (IIS) is a set of applications provided by Microsoft with their Windows Server operating systems (Windows Server 2008 and Windows Server 2012). These applications are the Microsoft implementation of Web, FTP, and SMTP servers.

Because three components (administration site, web service, and Calyx Resolver) are hosted by IIS, it is important that IIS is properly installed and configured before attempting to operate PointCentral.

Prerequisites

Before installing IIS:

- *Verify that IIS was not previously installed by selecting* ***Start > Administrative Tools****. If IIS is installed,* ***Internet Information Services (IIS) Manager*** *is an option under* ***Administrative Tools****.*

  If IIS is installed, you can skip these installation steps.
- *Verify that you have administrative privileges on the server where you are installing IIS.*
- *Have the Windows Server installation CD-ROM that was used to install Windows Server on this computer available. It might be needed during the installation.*

Note

Adding the Application server (IIS, ASP.NET) role with the Enable ASP.NET installs the required IIS components for PointCentral. If for some reason IIS was installed without the Application Server it is possible your installation of IIS only serves static content. Features such as ASP, ASP.Net, and server side do not work unless they are specifically enabled. You can go to Add or Remove Programs and install Application Server with its default components (ASP.NET, Enable network COM+ access and Internet Information Services (IIS)). Alternatively, you can configure these features, also called Web service extensions, through the Web Service Extensions node in IIS Manager.

In addition to creating a default web site during a default IIS installation, all or some of the following components are installed, depending on the installation method and Windows version. Many of these IIS components and applications are not needed, therefore, you can stop or uninstall them if you do not use them for other applications:

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

When you install PointCentral, the InstallShield Wizard creates the following three virtual directories at the IIS root default Web site:

Virtual Directory admin

This points to the administration site installation directory.

Virtual Directory service

This points to the web service installation directory.

Virtual directory resolver

This points to the Resolver service installation directory.

If you already have the virtual directories **admin**, **service**, or **filesync** in your default web site, you will need to either remove these virtual directories and re-install PointCentral or manually create IIS web sites and virtual directories that point to the administration site and web service.

Related information

- *Refer to* ***Installing PointCentral****, on page 25, for information about the virtual directories during installation.*
- *Refer to Microsoft documentation for information about how to install and configure IIS.*

Domain name setup

If you do not use Calyx Resolver to obtain your domain name and SSL certificate, preparing your domain to resolve the PointCentral to search, open, or save loans, entails the following actions:

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

You must still set up your network so you have a fixed external (or public) IP address available for your server.

Calyx Resolver

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

Hostname

Calyx provides up to five hostnames per account ID for your server. These hostnames are of the form *.calyxpds.com.

DNS Hosting

All DNS queries for your Calyx-provided hostname are resolved to your IP address.

SSL Certificate

Calyx issues an SSL certificate for your hostname.

Important

Calyx Resolver is a free service when your subscription is up to date.

Calyx Resolver is set up by using the PointCentral Configuration Wizard. The only additional requirement is that your machine have a static private or public IP address.

If you already have a domain name and SSL certificate, you can continue to use them rather than using Calyx Resolver to set them up. You can switch to Calyx Resolver at any time.

Configuring DNS

After you have purchased your domain name, you must configure it so that it connects to the correct IP address when a Point client attempts to access it.

If you have your own DNS servers, make sure you properly configure the new domain and point it to your DNS servers. If you don't have your own DNS servers, you can configure your account in the Domain Name and SSL Certificate Store,

SSL certificate

For security purposes, all data sent between the Point client and PointCentral is encrypted. To ensure that the data is properly encrypted, you must install a Secure Sockets Layer (SSL) certificate on the IIS server that hosts the administration and web service sites.

Use the following steps to properly install and configure the SSL certificate on your PointCentral web site:

- Create the SSL Certificate Request
- Purchase the SSL Certificate
- Configure the SSL Certificate
- Install the SSL Certificate

Advanced users can go through this process in a few minutes. However, if you don't feel comfortable managing networks and web sites, Calyx suggests that you contact a professional for assistance.

Microsoft SQL Server

PointCentral was designed and implemented to work with Microsoft SQL Server as its back end database.

As an alternative to purchasing the complete Microsoft SQL Server, PointCentral also supports Microsoft SQL Server Express Edition. Microsoft SQL Server Express Edition is a free and lightweight version of SQL Server for applications that serve up a small number of concurrent users.

Important

Although PointCentral supports both Microsoft SQL Server and Microsoft SQL Server Express as its back end database, Calyx recommends that you install Microsoft SQL Server. Microsoft SQL Server Express might not be able to support your requirements as your business grows and you have more users, loan files, and require more data folders.

Before you install SQL Server, ensure that you purchase the licensing model that is best for your organization. Before you make a decision, it is important that you understand the following concepts:

- SQL Server Processor licenses
- SQL Server plus device CALs
- SQL Server plus user CALs

- Differences between SQL Server Standard and Enterprise Editions (PointCentral supports both editions)

Related information

- *Refer to* ***Operating requirements****, on page 17, for compatible SQL Server versions.*
- *Consult your Microsoft documentation for more information about purchasing, installing, configuring, or managing SQL Server.*

.NET Framework

PointCentral requires Microsoft .NET Framework 4.6.1. Therefore, it does not directly require that an earlier version of Microsoft .NET Framework be installed. However, Microsoft SQL Server might have different Microsoft .NET Framework requirements.

Related information

For more information about the Microsoft .NET Framework, refer to your Microsoft documentation.

Installing PointCentral

When all the software and pre-installation requirements are complete, install PointCentral.

Prerequisites

- *If you are upgrading your database, make a backup of your data first. If a power outage or other unexpected event occurs during the upgrade, you could end up with a non-functional database. With a proper backup, you can restore the database and attempt the upgrade again.*
- *Verify that all of the prerequisites were properly installed and configured before you begin the installation process.*

Restriction

The installation process supports the installation of new systems and also upgrades of systems that run PDS version 5.3 and later. Upgrades from PDS version 5.1 and earlier are not supported.

Before you begin the installation, close all applications and any open dialog boxes.

Requirement

You must have administrative privileges on the computer where you are installing PointCentral to complete the installation.

Access to the installation executable is through MyCalyx. To install PointCentral:

1. After logging in to MyCalyx, click the **Download Server Software** button.
2. Select the PointCentral version that you are installing from the dropdown list and click **Download**.

Important

Installing PointCentral through Terminal Server is supported only in Remote Administration mode. If you have configured Terminal Server for Application Server mode, the installation and operation will not work.

3. In the *PointCentral Installation* section, click the **Install or upgrade PointCentral** link to run Calyx-Point-Data-Server.exe.
4. Double-click the Calyx-Point-Data-Server.exe file and the installer will begin.
5. Click **OK** to proceed.

   The **PointCentral InstallShield Wizard Welcome** dialog box is displayed:

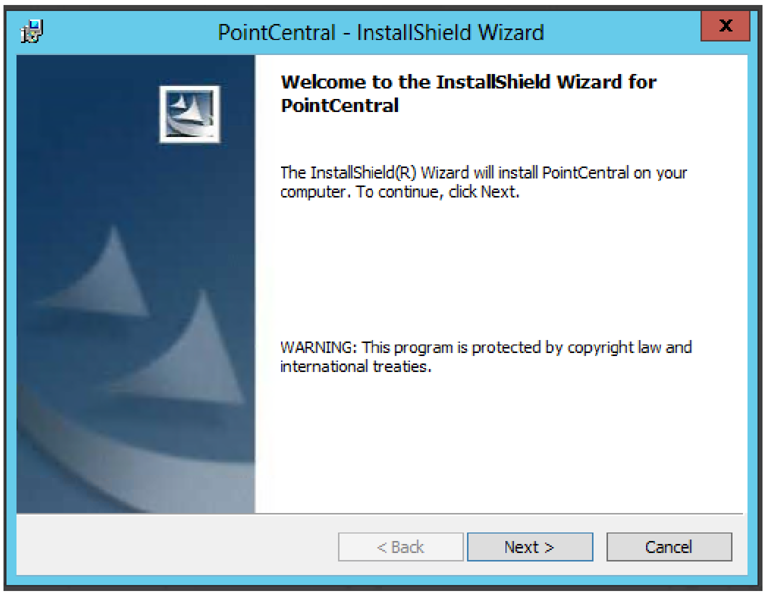


Figure 10. InstallShield Wizard Welcome

6. Click **Next** to proceed.

The **PointCentral License Agreement** dialog box is displayed:

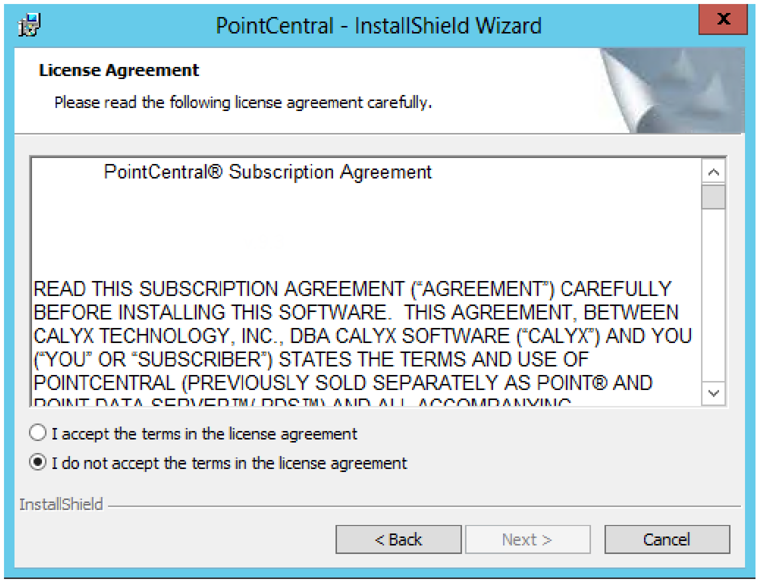


Figure 11. License Agreement

7 Read the Software License Agreement. If you accept the terms, select **I accept the terms in the license agreement** and click **Next** to proceed.

If you do not accept the terms of the agreement, the **Next** button is not available and you are unable to proceed with the installation process.

The **Destination Folder** dialog box is displayed.

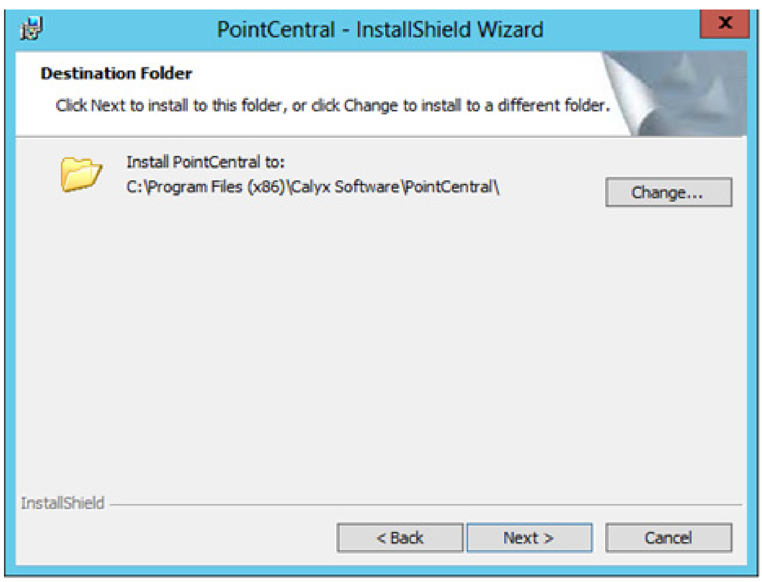


Figure 12. Destination Folder

By default, the InstallShield Wizard sets the destination folder to **C:\Program Files\Calyx Software\Point Data Server**, referred to as the root folder path.

8 Click **Change** to select another destination folder and click **Next**.

> **Important**
>
> *If you change the destination directory, select a path with sufficient disk space to accommodate future data folder growth.*

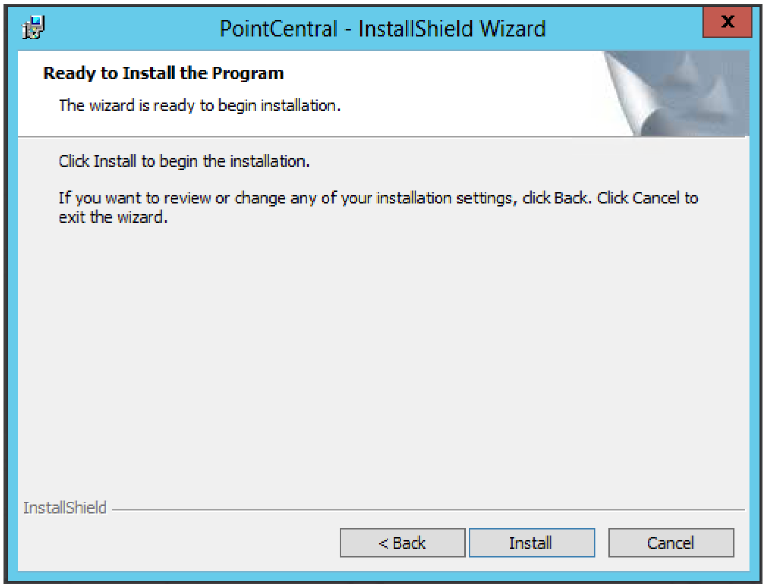


Figure 13. Ready to Install

9 Click **Install** to begin the installation.

When the installation is complete, a confirmation dialog box is displayed.

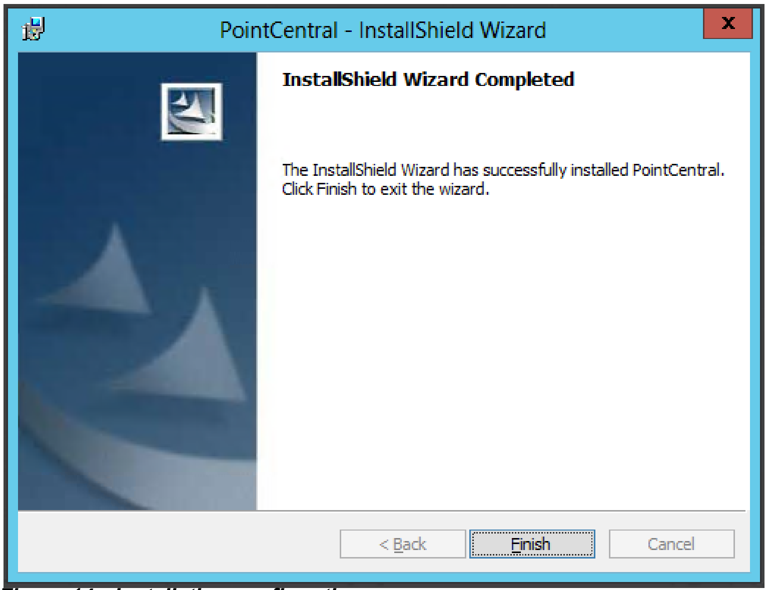


Figure 14. Installation confirmation

10 Click **Finish**.

Restart the server if you are prompted. If not, the Installshield Wizard automatically launches the PointCentral Configuration Wizard.

If a server restart was required, launch the PointCentral Configuration Wizard from **C:\Program Files (x86)\Calyx Software\PointCentral\PdsDbCreate.exe** (or the location where you installed PointCentral) as an administrator.

Tip

If the PointCentral Configuration Wizard isn't visible, it might be open behind other dialog boxes. Proceed to the configuration process to create or upgrade your SQL database and configure the SQL connections.

Related information

*See **Administration detail**, on page 44, for more information about the root folder path, the root template set path, and other important system folders.*

Configuring PointCentral

After you have finished installing PointCentral, you must configure your database. 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 the connections from the PointCentral components to the PointCentral database.

Prerequisite

If you do not plan to use Calyx Resolver and you do not have a domain name, DNS, and SSL certificate, you must obtain them before you proceed.

To configure PointCentral:

1 If the PointCentral Configuration Wizard does not launch automatically after the installation is finished, run it as an administrator from Windows File Explorer by going

to **C:\Program Files (x86)\Calyx Software\PointCentral** (or the location where you installed PointCentral) and double-clicking PdsDbCreate.exe.

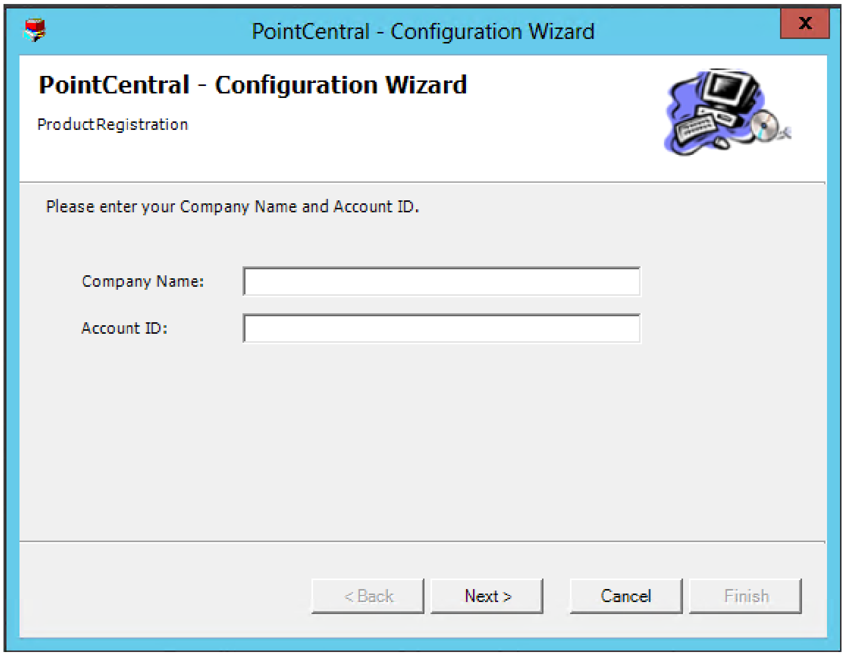


Figure 15. Product Registration

2 Enter your company name and your Calyx account ID and click **Next**.

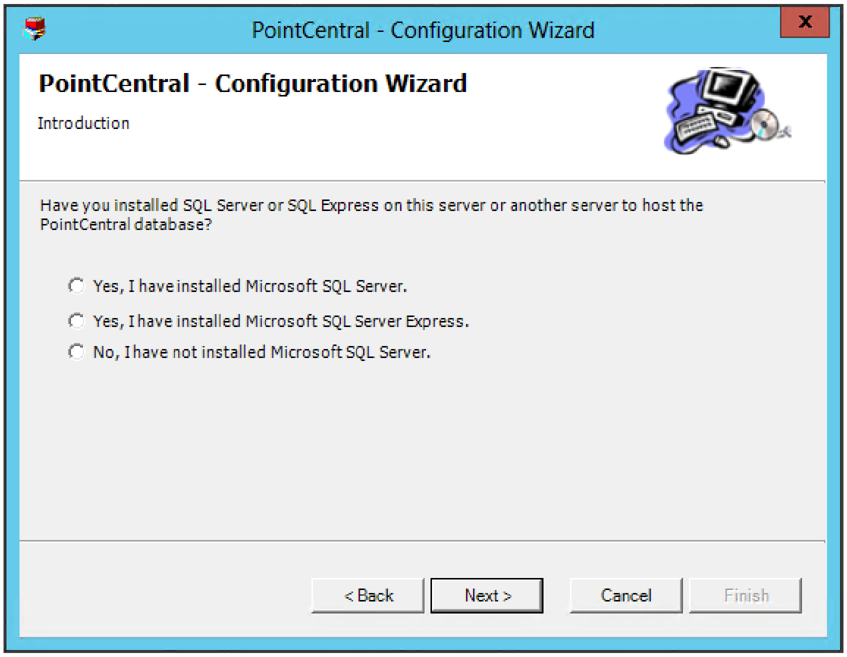


Figure 16. Specify SQL version

3 Specify the version of SQL Server you have installed and click **Next**.

The **Database Connection Information** dialog box is displayed.

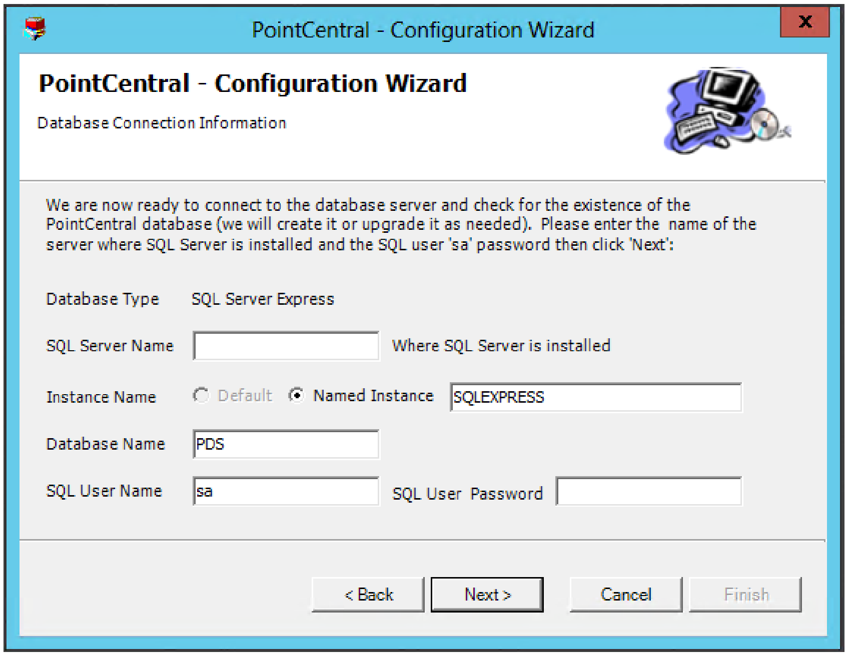


Figure 17. Database Connection Information

The *Database Type* is prepopulated with the selection made in the **Introduction** dialog box.

4 Complete the **Database Connection Information** dialog box and click **Next**.

a Enter the server name where Microsoft SQL Server is installed in the *SQL Server Name* field.

b Enter a name for your database in the *Database Name* field.

c Enter your Microsoft SQL Server user password in the *SQL User Password* field.

This password is defined when you install SQL Server.

The PointCentral Configuration Wizard attempts to connect to the Microsoft SQL Server, using the credentials you supplied.

After the connection is made, depending on your environment, one of the following dialog boxes is displayed:

- If you are creating a PointCentral database for the first time and SQL Server runs on the same server as the PointCentral server, the following screen is displayed for a local database:

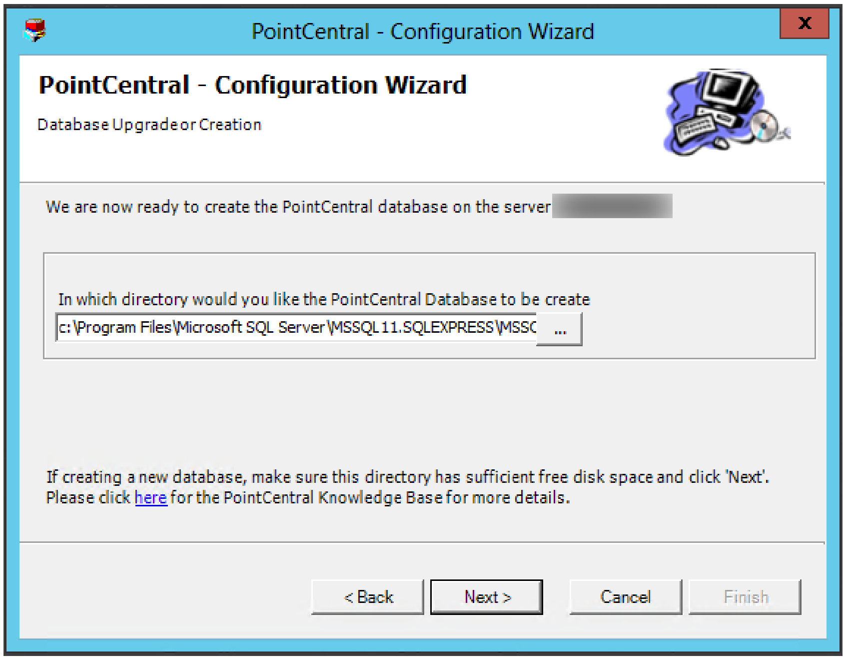


Figure 18. Database Upgrade or Creation (local database)

If you do not want to store the database files in the default directory, navigate to the directory where you want the database files to be created.

- If you are creating a database for the first time and SQL Server is on a different server from PointCentral (remote database), 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.) If you need the database in a different directory on the remote server, move that server from the default to the desired directory by using your database management tools.

- If you are upgrading, the following dialog box is displayed:

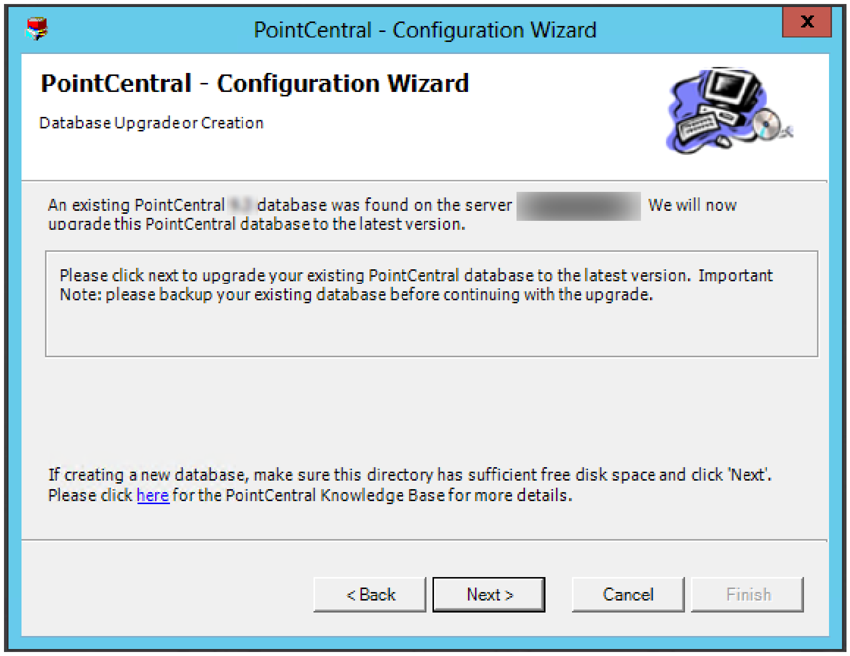


Figure 19. Database Upgrade or Creation, existing database found

During an upgrade, the PointCentral Configuration Wizard creates new tables and alters the schema of certain existing tables. It also retains any unchanged data such as the following information:

- Users
- User groups
- User group memberships
- Data folders
- Data folders access rights
- Loan file indexes

Before creating or upgrading your database, the PointCentral Configuration Wizard also:

- Stops the FileSync Windows Service. Because the database is unavailable while it's being created or upgraded, PointCentral applications cannot access it. Therefore, FileSync stops to prevent unwanted errors from being added to the Windows Event Log.
- Places the web service in Upgrade mode. While the database is being upgraded, Point users must be prevented from accessing it. By placing the web service in Upgrade mode, you ensure that the web service does not access the database until the upgrade is complete. When Point users attempt to access PointCentral during an upgrade, a message is displayed that their request has failed and they should contact their administrator.

5 Complete the **Database Upgrade or Creation** dialog box and click **Next**.

It takes only take a few seconds for the PointCentral Configuration Wizard to create a new database (whether the SQL Server is running locally or remotely). However, it can take longer to upgrade an existing database. It depends on the size of the database, but completing most upgrade installations should not take longer than two to five minutes.

Regardless of the environment in which you are operating (creating a new local SQL database, creating a new remote SQL database, or upgrading an existing database), a message that indicates the wizard is busy is displayed.

When the PointCentral Configuration Wizard is complete, the **Database Verification Complete** dialog box is displayed.

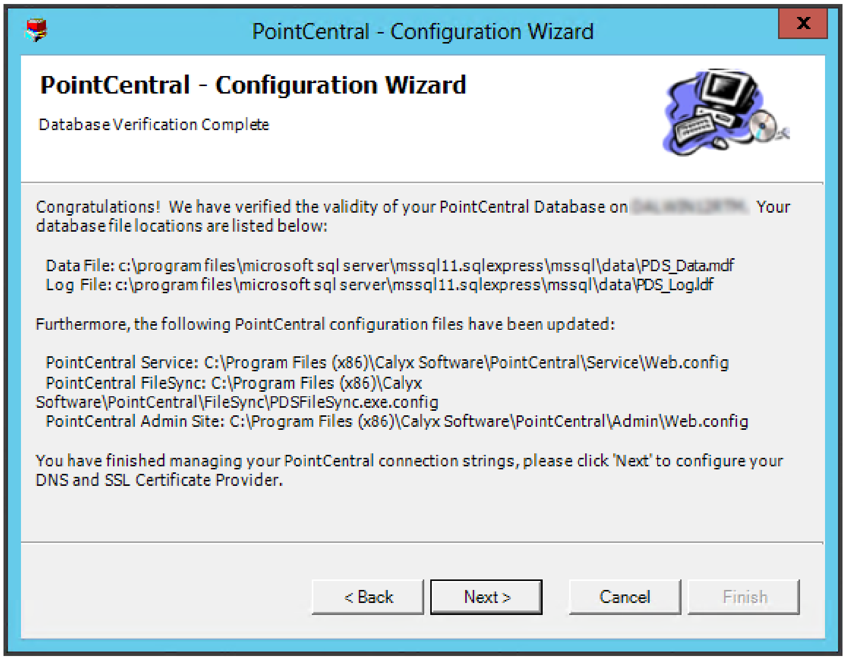


Figure 20. Database Verification Complete

The locations of the SQL Server database underlying files and the updated configuration files are displayed.

Note

Depending on your environment, the paths **C:\Program Files\Microsoft SQL Server\MSSQL\Data** *and* **C:\Program Files\Calyx Software\Point Data Server** *might vary.*

The PointCentral Configuration Wizard begins FileSync and takes the web service out of Upgrade mode.

Troubleshooting tips

If the PointCentral Configuration Wizard is not able to connect to the database, check the following:

- *Verify that one of the supported Microsoft SQL Servers is installed.*
- *Verify that Microsoft SQL Server is running.*
- *Verify that the correct sa password was entered and it matches the sa password that was defined when SQL Server was installed.*
- *Verify that the correct protocols enabled for your instance of SQL Server.*

6 Click **Next**.

The **DNS and SSL Certificate Provider** dialog box is displayed.

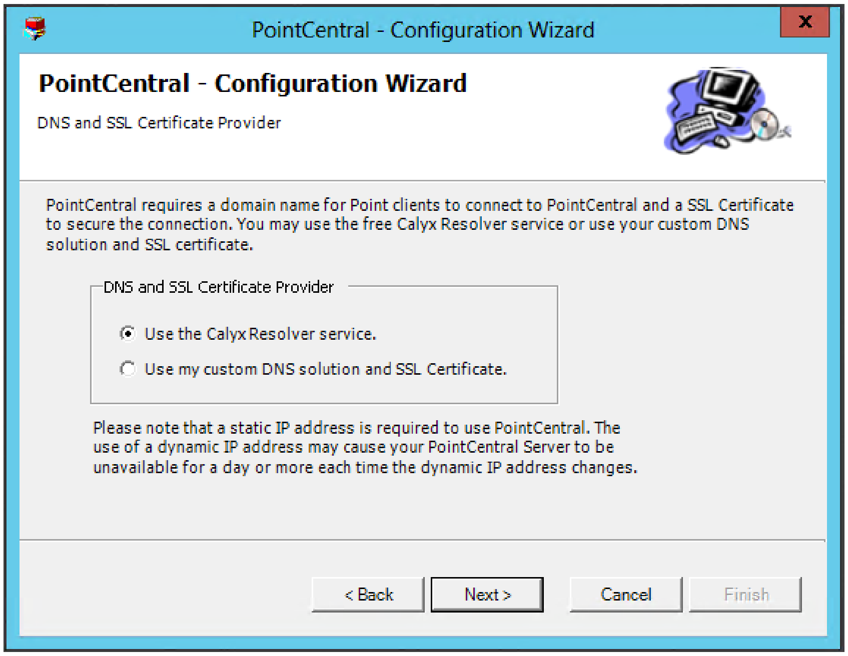


Figure 21. DNS and SSL Certificate Provider

7 Specify whether you will use Calyx Resolver to set up this data or whether you already have your own DNS solution and a pre-existing SSL certificate and click **Next**.

The **Calyx Resolver Domain Name and IP Address** dialog box is displayed.

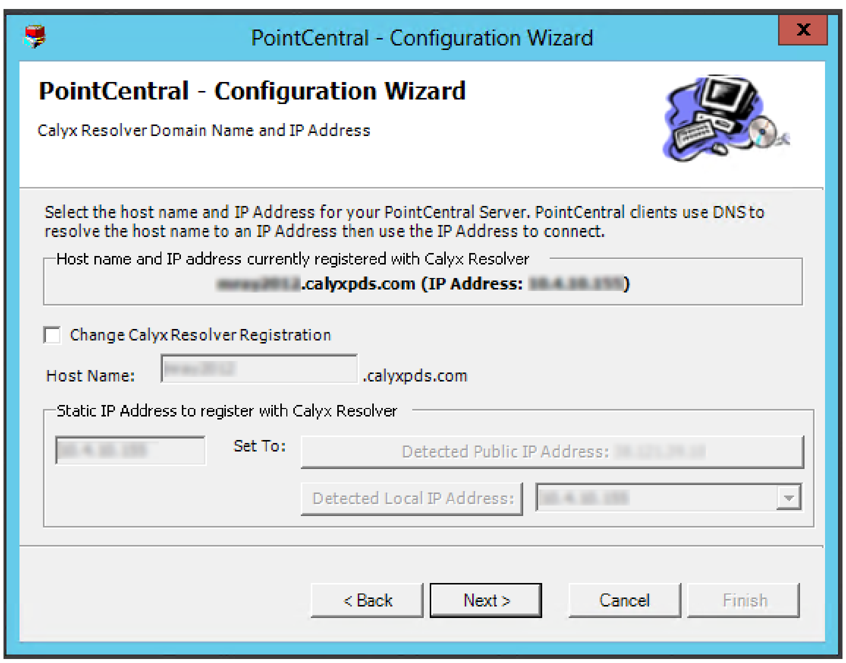


Figure 22. Calyx Resolver Domain Name and IP Address

8 Complete the **Calyx Resolver Domain Name and IP Address** dialog box.

a Enter a host name of your choosing.

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

b Enter the server IP address.

By default, the Configuration Wizard populates this field with your current public IP address.

- To make your server available over the Internet, enter its static IP address.
- To make your server available only within your local network, click the **Detected Local IP Address** button to automatically populate the field with your current local IP address, or enter the address manually.

9 Click **Next**.

The **Calyx Resolver Name and IP Address Confirmation** dialog box is displayed.

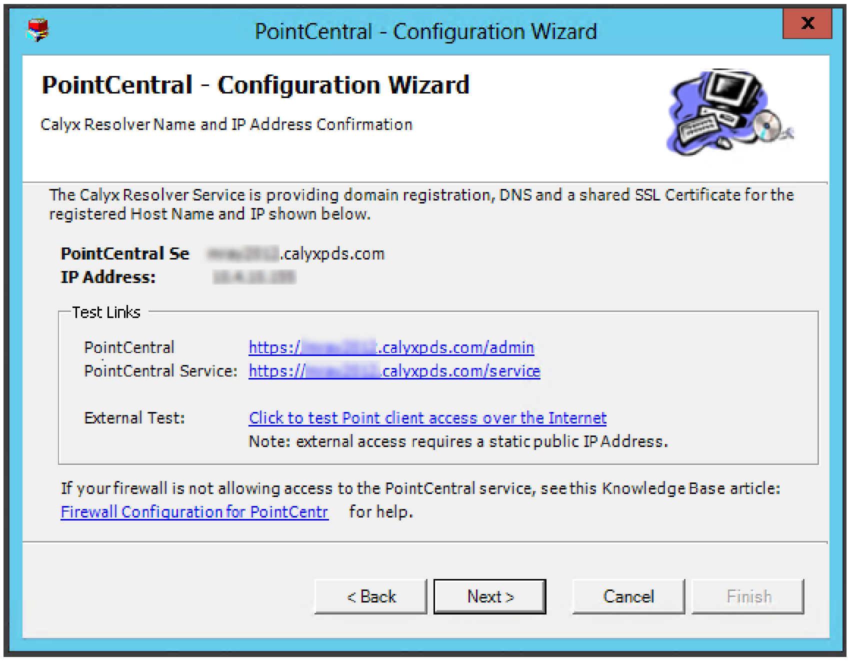


Figure 23. Calyx Resolver Name and IP Address Confirmation

10 Click **Next**.

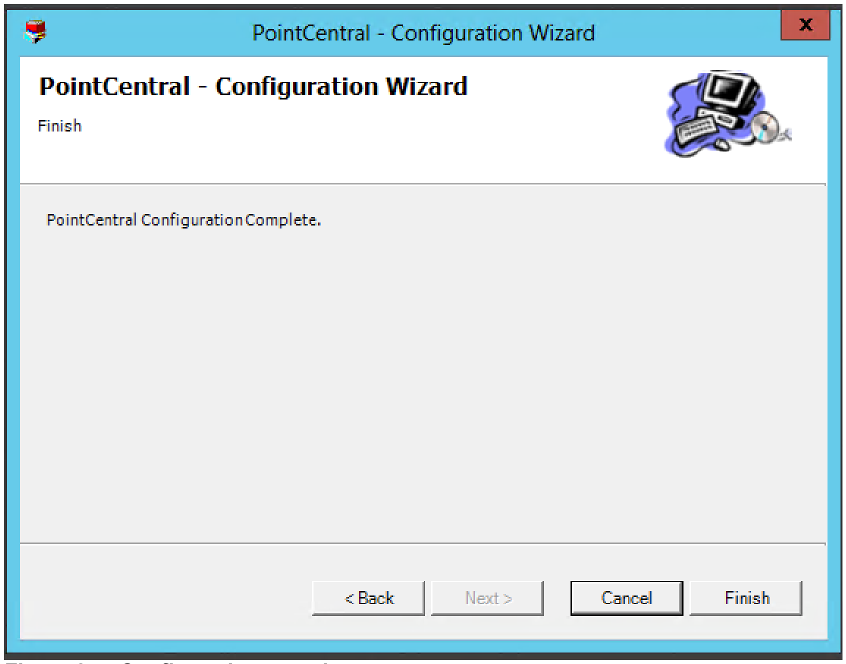


Figure 24. ***Configuration complete***

11 Click **Finish**.

Run the PointCentral Configuration Wizard again later to update the database connection information, reset NTFS permissions, or configure Calyx Resolver if your system changes in the future.

Related information

- *For more information about Microsoft SQL Server and SQL Server Express, refer to* ***Domain name setup****, on page 22.*
- *For more troubleshooting information, refer to the* ***PointCentral Knowledge Base*** *and locate the applicable article for your problem.*

Uninstalling PointCentral

In some cases users might revert from PointCentral back to conventional Point. To do this, you must reverse the configuration that was completed during installation.

The process to uninstall PointCentral includes the following actions:

- Back up your data
- Convert all data folders to conventional
- Convert all template sets to conventional
- Convert Cardex databases to conventional (export)
- Reset IIS, FileSync, and SQL Server
- Stop FileSync
- Uninstall PointCentral components

- Restart computer

Recommendation

To avoid loss of data, back up your database before you begin the uninstallation process.

Related information

- *Refer to* ***Converting PointCentral data folders to conventional****, on page 95,* ***Converting template sets to conventional****, on page 108, and* ***Converting Cardex databases to conventional Point****, on page 114, for information about how to convert data folders, template sets, and Cardex databases to conventional Point.*
- *Refer to Chapter 7,* ***Restoration procedure****, for information about backing up your system.*

Resetting IIS, FileSync, and SQL server

Before you delete the database, make sure that there are no open connections to the database, otherwise errors will occur.

The following actions must be performed before you begin the uninstallation process:

- Stop IIS
- Stop FileSync
- Stop and restart SQL Server

Important

You must have administrator privileges to perform these actions.

To stop IIS:

1 Open a command prompt dialog box in Microsoft Windows.

2 Enter *iisreset /stop* and press <Enter>.

After a few seconds a message is displayed that indicates that the Internet services were successfully stopped.

To stop FileSync:

1 Access Administrative Tools from the Start menu or the control panel.

2 Double-click Services and double-click CalyxPdsFileSync to open the **CalyxPdsFileSync Properties** dialog box.

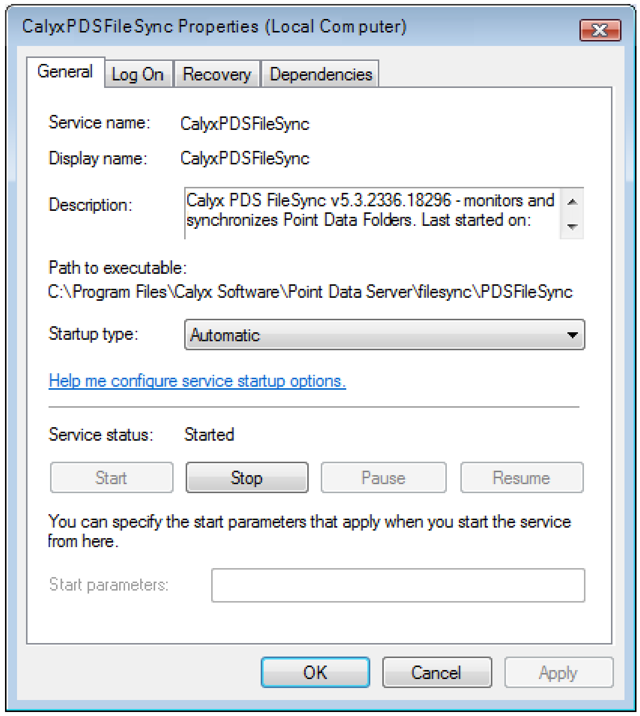


Figure 25. CalyxPDSFileSync Properties

3 Click **Stop**.

After a few seconds FileSync stops.

4 Click **OK** to close the dialog box.

Tip

Alternatively, you can type net stop CalyxPdsFileSync in the command prompt dialog box to stop FileSync.

To stop and restart the SQL database:

1 Open a command prompt dialog box in Microsoft Windows.

2 If you are running SQL Express, enter *net stop mssql$sqlexpress* and press <Enter>. If you are running SQL Server, enter *net stop mssqlserver*.

Messages are displayed that indicate the SQL server is stopping and that it was stopped successfully.

3 If you are prompted to stop the SQL SERVERAGENT service, click **Yes**.

4 If you are running SQL Express, enter *net start mssql$sqlexpress* in the command prompt dialog box and press <Enter>. If you are running SQL Server, enter *net start mssqlserver*.

Messages are displayed that indicate the SQL server is starting and that it was started successfully.

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

Deleting the PointCentral database

These instructions refer to Microsoft SQL Server 2005 Management Studio Express. The installation process for subsequent versions is similar.

Important

When you delete the PointCentral database, you also delete all users, user groups, Cardex databases, and access rights that exist in the database.

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 and select ***Delete***.

   The **Delete Object** dialog box is displayed.
5. Verify that the **Delete backup and restore history information for databases** check box is checked and click **OK**.

After the database is deleted, you can uninstall all the components.

Related information

- *For more information about SQL Server with PointCentral, refer to **Domain name setup**, on page 22.*
- *Refer to your Microsoft documentation for more information about Microsoft SQL server.*

Uninstalling PointCentral components

The InstallShield wizard contains an uninstall feature, which reverses the actions performed during installation.

To uninstall PointCentral:

1. Open the Add or Remove programs function from the Windows Control Panel.
2. Select **PointCentral** and click **Remove**.
3. Click **Yes** in response to the confirmation dialog box.
4. Restart your computer.

Related information

For more information about the Windows Add or Remove Program function, refer to your Microsoft documentation.

Configuration 3

Configuring PointCentral entails setting the operational parameters, configuring clients, and setting site parameters, FileSync parameters, and service parameters.

After you have installed PointCentral and created and configured its back end SQL database, you must configure it to accept incoming requests.

Important

Depending on your requirements, you can create a test environment to test your installation before creating actual users, groups, data folders, and template sets.

Create the test environment after you complete the configuration steps in this topic.

*Refer to the instructions in Chapter 4, **Resource management**, for information about how to create users, user groups, data folders, and templates.*

Tips

- *Add the administration site to your trusted sites zone. Internet Explorer prompts with a content blocking message where the site can be added to the trusted sites zone.*
- *If you receive an error when you attempt to access the administration site, verify that you have properly installed and configured IIS including the SSL certificate.*

In this topic

Accessing PointCentral for the first use

Before you can configure your users, user groups, and data folders, you must create an administrative user. Creating the administrative user is done the first time you access PointCentral.

Requirement

Internet Explorer is required to access the administration site.

To access PointCentral the first time:

1 Open PointCentral (select ***Start > All Programs > Calyx Software > PointCentral > PointCentral Administration***). This opens https://localhost/admin.

Because *localhost* does not match the name on your SSL certificate, a Security Alert message is displayed.

2 Click **Yes** to proceed.

Note

The localhost *resolves to the IP address 127.0.0.1, which should resolve to your local server.*

The **PointCentral Administration** log in dialog box is displayed.

3 For the first access, enter *admin* in the *Username* field. Leave the password field blank and click **Login**.

The release notes screen is displayed.

4 Review the release notes and click **Save and Continue** to proceed to the home page.

To prevent the release notes from displaying again at log in, select the **Do not show these Release Notes again at login** check box before you close them.

The ***Home Page*** is displayed.

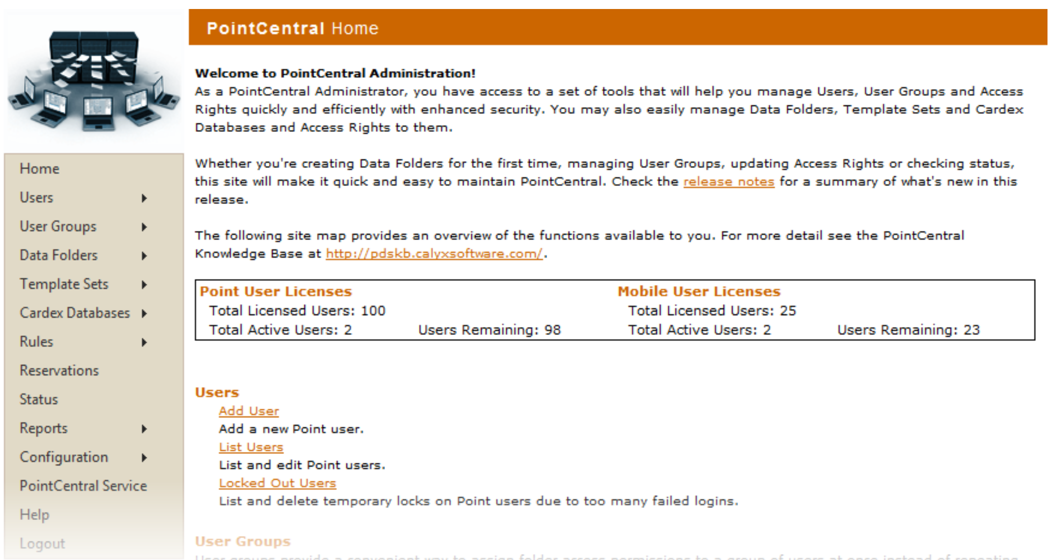


Figure 26. PointCentral home page

The ***Home*** page contains a summary of Point user licenses and mobile licenses in PointCentral. It also contains a description of the pages in the administration site and a menu bar which is used to perform the administrative functions.

5 Select ***Configuration > Parameters*** to continue with the configuration.

6 In the **First Time Login** dialog box, enter a new username and password.

Requirement
You must enter new login data to access the administration site.

A 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.)

Important
The password you use here is the only set of credentials you have to access the administration site.

The ***Parameters*** screen is displayed.

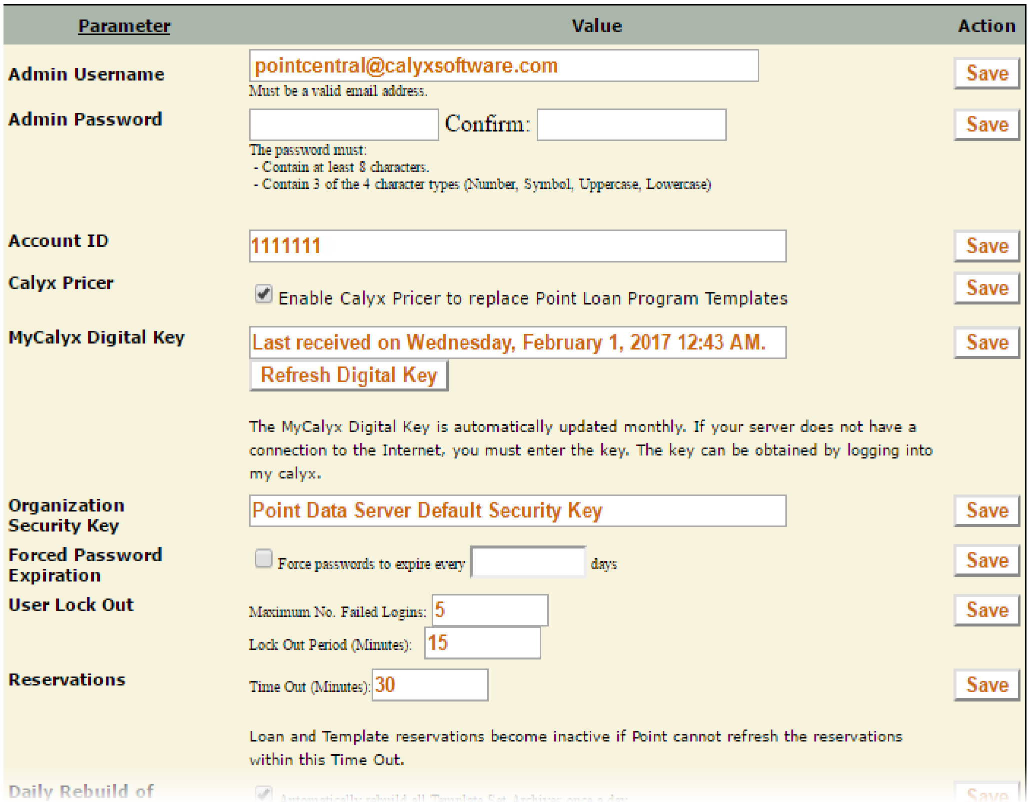


Figure 27. Parameters screen

Use this screen to set PointCentral operational parameters.

Related information

*For information about how to configure the parameters on this screen, refer to **Administration detail**, on page 44.*

Administration detail

The administration site contains the following administrative tools to help you manage PointCentral:

- Data folders
- Users
- Template sets
- Cardex databases
- Access rights to resources
- System parameters

After a successful log in, the administration site home page is displayed:

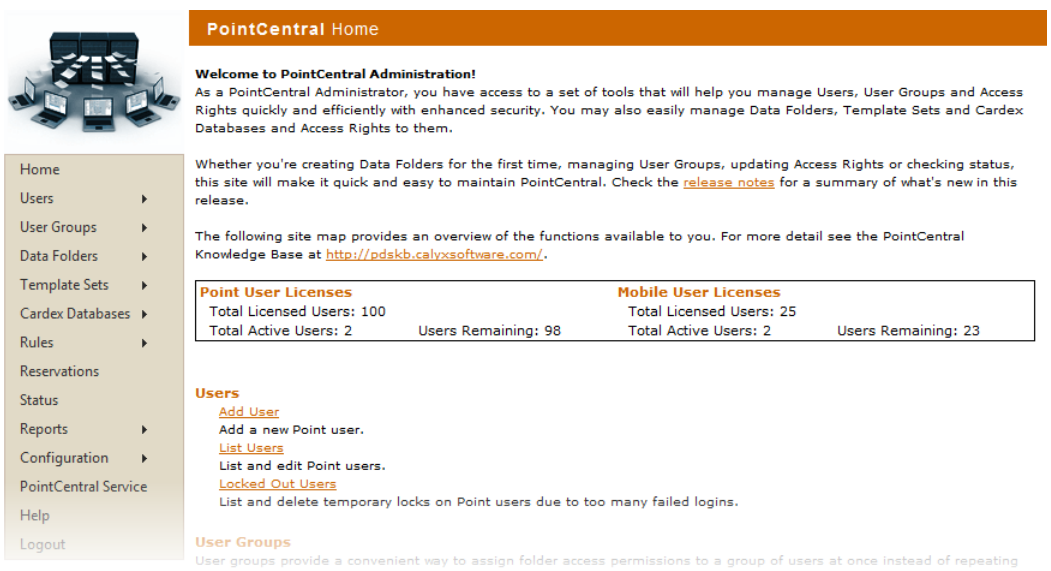


Figure 28. PointCentral Home page

To access a page in the administration site, select the option from the left navigation menu.

The following table describes the navigation menu options:

Table 5. Navigation menu options

Navigation menu option		Description
Home		Accesses the Home page which contains a description and links for the administrative pages.
Users	Add User List User Locked Out Users	• Add a new Point user • Edit an existing user • Delete a temporary lock out if a Point user attempts to unsuccessfully log in and exceeds the maximum number of failed log in attempts.
User Groups	Add User Group List User Groups	• Establish a new user group • Modify an existing group • Modify a specific user's membership in the group
Data Folders	Add Data Folder List Data Folders Edit Local Data Folder Access	• Create data folders • Edit data folders • Add user or user group access rights • Modify user or user group access rights • Copy folder settings or access rights from an existing data folder • Monitor and control local data and network
Template Sets	Add Template Set List Template Sets	• Create template sets • Edit template sets • Add user or user group access rights • Modify user or user group access rights • Copy folder settings or access rights from an existing data folder
Cardex Databases	Add Cardex Database List Cardex Databases	• Create a Cardex database • Edit a Cardex database • Add user or user group access rights • Modify user or user group access rights
Rules	Add Rule List Rules	• Create rules • Edit rules • Add user or user group access rights • Modify user or user group access rights
Reservations		List and delete loan or template reservations.
Status		View the status of a requested action, such as synchronization of a data folder.

Table 5. Navigation menu options (Continued)

Navigation menu option		Description
Reports	User Effective Access Rights Users, Group Membership Groups, User Members Data Folders, Groups and Users with Access Rights Template Sets, Groups and Users with Access Rights Cardex Databases, Groups and Users with Access Rights Rules, Groups and Users with Access Rights	Generate reports that show the access relationships for objects of a type (for example, the user group and user access rights for all users to all data folders).
Configuration	Parameters Delete Cardex Database Point Fields – Supported Fields – Custom Fields – Additional Fields Import – Data Folders – Users and Access rights – Template Sets – Cardex Database – Users From File Folder Maintenance – Synchronization – Switch to Conventional Template Set Maintenance – Template Types – Copy Template Set – Switch to Conventional	• Define PointCentral parameters • Delete a Cardex database • View and define supported fields • Import conventional Point users, data folders, Cardex databases, and template sets • Specify folder maintenance parameters • Manage template sets
PointCentral Service		The web service that verifies that the connection between PointCentral and Point is running smoothly.
Help		View resources available for help with using Point.
Logout		Logs the current user out of the system.

Setting the operational parameters

Use the configuration screen to set the following operational parameters for PointCentral.

- Admin username and password
- Organization security key
- Reservation time out period

- Number of failed log in attempts until lockout
- Root folder and template set paths

To set or change the configuration parameters:

1 Log in to the administration web site.

2 Select ***Configuration > Parameters***.

The ***Parameters*** screen is displayed.

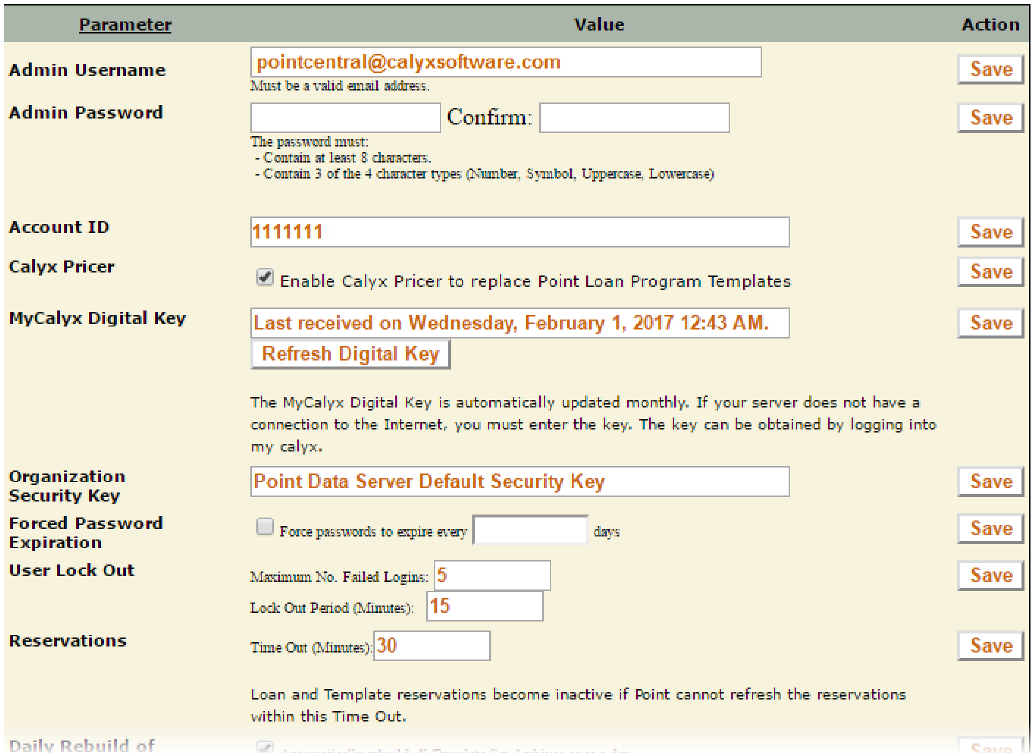


Figure 29. Parameters screen

3 Enter or change the administrative username and password and click **Save**.

The *Admin Username* and *Admin Password* fields establish the credentials that are used to log in to the administration server.

4 Enter your account ID in the *Account ID* field and click **Save**.

Your account ID is assigned by Calyx after you purchase PointCentral. If you do not know your account ID, contact your salesperson.

5 If your organization uses Calyx Pricer, select the **Enable Calyx Pricer to replace Point Loan Program Templates** check box and click **Save**.

When selected, Calyx Pricer is launched automatically when Point users click the **Loan Program** button.

Requirement

When Calyx Pricer is enabled, users must be assigned a template set in PointCentral to access Calyx Pricer from the **Loan Program** *button in Point. An error will occur for users who are not assigned a template set.*

6 If your server has an Internet connection, your MyCalyx digital key is entered automatically when PointCentral is downloaded from MyCalyx for the first time. If your site does not have an Internet connection, enter your MyCalyx digital key in the *MyCalyx Digital Key* field and click **Save**.

The MyCalyx digital key requires updating every 30 days. If your server has an Internet connection, your MyCalyx digital key is automatically updated about every two days. If your server has a firewall and does not allow outside access, you must update your key manually every 30 days. Updating the key manually entails retrieving the key from MyCalyx and entering it on the PointCentral ***Parameters*** page.

Note
Contact your MyCalyx Administrator for more information about accessing the MyCalyx digital key.

To view MyCalyx license and user updates immediately without having to wait until the license is automatically updated, click the **Refresh** button at any time. The information is imported into PointCentral.

7 Specify the default file type when new files are created in a mobile device, **Borrower** or **Prospect**.

8 If your organization has implemented a password expiration policy, select the check box and enter the number of days that a user's password is valid in the *Forced Password Expiration* field. The default value is *30* days.

When a user with an expired password attempts to log in to Point, a message is displayed that indicates their password has expired and they need to change it. The **Change Password** dialog box is then displayed for the user to proceed to change their password.

9 Enter the lock out parameters in the *User Lock Out* fields and click **Save**.

The lock out parameters defend against unauthorized users trying to gain access to your server by guessing passwords for a user ID until they find one that works.

Maximum No. Failed Logins

The maximum number of consecutive failed log in attempts before the user is locked out. The range is from 1 to 10 with a default of 5.

Lock Out Period (Minutes)

The number of minutes before the user can log in again after they have exceeded the *Maximum No. Failed Logins* parameter. The range is 5 to 60 minutes with a default of 15.

10 Specify how long a loan file remains reserved in the *Reservations* field and click **Save**.

The Reservations function is a mechanism to ensure that users cannot edit a loan or template while another user has the loan or template open for editing. In conventional Point data folders, loans are held open by keeping the file open in the file system. In PointCentral, Point transfers the loans and templates over the HTTPS connection when they are opened and closed and uses Reservations to guarantee exclusive access for editing.

Time Out (Minutes)

The time that a loan remains reserved if Point does not close properly, or if the network connection from Point to PointCentral becomes unavailable for an extended period. The range is 30 to 300 minutes with a default of 30.

Changes to this value do not take effect until the web service is restarted. The default value of 30 minutes is recommended.

11 Specify the parameters to automatically rebuild the template set archives and click **Save**.

Before it sends templates to a Point user, PointCentral compresses and archives all the template files within a template set into one template set Archive file. 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 (and only when a user accesses a certain template type).

PointCentral can automatically rebuild your template set archives once a day. This ensures that the first time a Point user logs in, PointCentral sends all the template files within the user's template set without additional calls to the server. The Rebuild Time is set in the time zone where PointCentral is located (in the example it was (GMT-07:00) Pacific Standard Time).

12 Specify the number of template files that are changed before downloading the archive from PointCentral and click **Save**.

When a large number of template files change on a daily basis and the size of your template sets is fairly small, you can force the Point client to always download the template set archive from PointCentral. This can improve performance because every Point client does not have to download every template file that changed since the last log in.

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

13 Specify the path for the location to store the data folders and click **Save**.

The location where data folders are stored must be an existing directory on a local drive on PointCentral. The root folder location must have sufficient disk space to contain all current and future data folders.

Attention

Changing the root folder path requires you to convert all data folders to conventional Point and re-import them. Access folders 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. If the **Root Folder Path** *field is empty, FileSync might not have started or an error has occurred.*

14 Specify the path for the location to store the PointCentral template sets and click **Save**.

The location where PointCentral template sets are stored must be an existing directory on a local drive on PointCentral. The template set location must have sufficient disk space to contain all current and future PointCentral template sets.

Attention

You can change the root template set path only if all template sets were converted to conventional Point and no PointCentral template sets exist.

Changing the root template set folder requires you to convert all template sets to conventional Point and re-import them. Access rights are not preserved when template sets are converted to conventional Point.

The default value is recommended.

15 Specify the temporary path and click **Save**.

The temporary path requires only enough space to buffer a few seconds of loan and template updates from Point clients.

Important

You must restart the web service for changes to this value to take effect.

The default value is recommended. If the default value is changed, it might be necessary to grant read and write access to the user account (IUSR_computername) that was configured for anonymous access in the IIS default web site.

16 To enable the audit trail to track changes and record actions for every loan file in Point, select the check box and click **Save**.

When this setting is enabled, users who are granted access rights to the audit trail log can see the ***Audit Trail*** option on the ***Utilities*** menu in Point. The option is not visible for any other users.

If the setting was turned on but later turned off, the audit trail log for loan files that were changed during the time the audit trail was enabled is retained with the loan file in Point.

The audit trail log remains with the loan file when it is moved or copied to another data folder unless the Point user selects the **Copy only 1003 data to start a new loan including co-borrowers** option in the **Copy Borrower** or **Copy Prospect** dialog boxes when they copy an existing loan file.

17 To participate in the Calyx Experience Improvement Program, select the corresponding check box and click **Save**.

The Calyx Experience Improvement Program anonymously collects data about your hardware configuration and how you use PointCentral. If you participate in the program, information to improve the quality, reliability, and performance of PointCentral is collected. The information is securely transmitted to Calyx by using Secure Sockets Layer (HTTPS/SSL). Calyx does not collect any individual loan data from within the loan files, or store your IP address or any other information with the anonymous data that could be used to identify your organization or your clients. You can elect to opt out of the program at any time.

Related information

- *Refer to* ***Configuring PointCentral****, on page 28, for more information about how to give the anonymous user access in IIS the proper NTFS access rights.*
- *Refer to* ***Reservations****, on page 54, for more information about reservations.*
- *Refer* ***Specifying user and user group data folder access rights****, on page 83, to for information about granting users access to the audit trail.*

Client configuration

Before users can access PointCentral, their computer must be configured to work with PointCentral.

Connecting the client to PointCentral

To connect a Point client to PointCentral:

1. Ensure that Point is closed on the Point client (not PointCentral).
2. Open Point Administrator by going to the desktop and selecting ***Start > All Programs > Calyx Software > Point Administrator***.

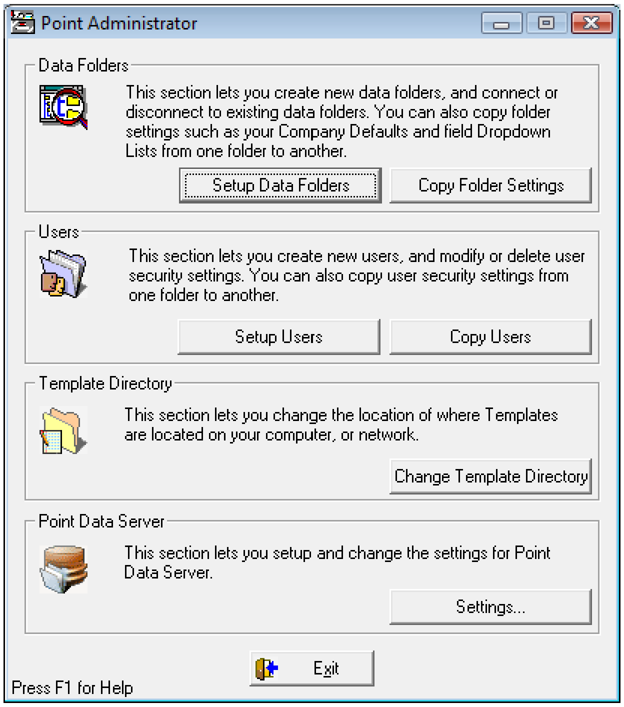


Figure 30. Point Administrator

3. Click **Settings** in the *Point Data Server* section.

The **Point Data Server Settings** dialog box is displayed.

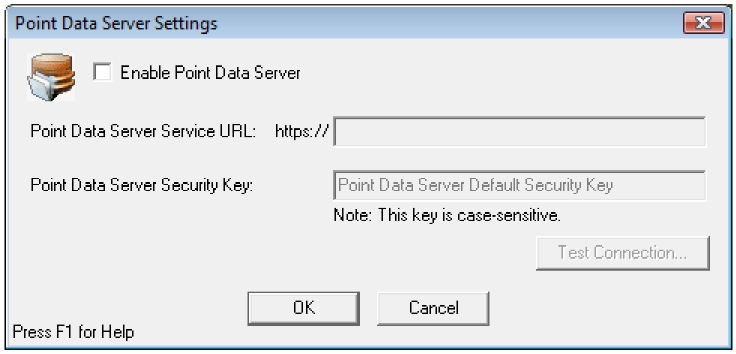


Figure 31. Point Data Server Settings

4 Select the **Enable Point Data Server** check box.

5 In the *Point Data Server Service URL* field, enter the domain name that is used in the SSL certificate and append it with */service*.

Service refers to the web service virtual directory in IIS.

6 In the *Point Data Server Security Key* field, enter the security key that you used when you set the security key parameter.

7 Click **Test Connection**.

The **Test Login to Point Data Server** dialog box is displayed.

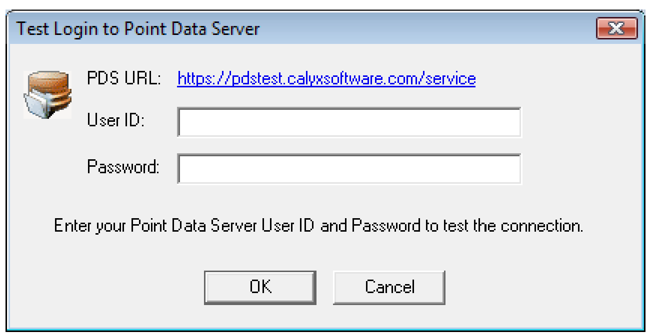


Figure 32. Test Login

This dialog box is to verify that the PointCentral settings were correctly entered and that the Point client has network connectivity to PointCentral.

8 Enter your user ID in the *User ID* field.

Any valid Point user defined in PointCentral can be used to test the connection.

9 Enter your password in the *Password* field.

10 Click **OK** to test the connection to PointCentral.

A dialog box is displayed that indicates a successful connection.

11 Click **OK** to dismiss the successful connection message.

12 Click **OK** to accept the settings.

13 Click **Exit**.

The Template Directory setting in Point Administrator is ignored when the user has effective access rights to a template set and Cardex database.

Many installations allow access to PointCentral and its data folders from the Internet. PointCentral has numerous security features to defend against unauthorized or malicious use from the Internet. One of the security features requires Point clients to log in with a valid user ID. With this feature you can centrally control access to Point by managing PointCentral users. When Point cannot contact PointCentral, users can access only Point conventional data folders.

Related information

In addition to using Point Administrator to set the PointCentral connection, you can connect Point clients to PointCentral by using MyCalyx to create an installation group. Refer to the Calyx Knowledge Base article #0688, ***Creating an Installation Group for MyCalyx Users****.*

Disabling search refresh settings

In conventional Point, by default, the navigation panel search results refreshes each time the user accesses the **Loans** and **Tasks** tabs. These search results are displayed in the Point workspace. The refresh occurs regardless of whether or not any of the data has changed.

This automatic refresh of the navigation panel search results for the **Loans** and **Tasks** tabs can generate significant network traffic which can consume bandwidth from the branch office to headquarters and resources. This will degrade the response time for all users.

To avoid the response time issues, disable the automatic refresh feature on all Point clients. Point users can refresh the Search Results at any time by clicking the **Search** button on the respective **Loans** or **Tasks** tab.

To disable the automatic refresh:

1. Open Point on the client.

   The **User Login** dialog box is displayed.

2. Enter your user ID in the *User ID* field.
3. Enter your password in the *Password* field and click **OK**.
4. Select ***Utilities > Search/Display Settings***.

The **Search/Display Settings** dialog box is displayed.

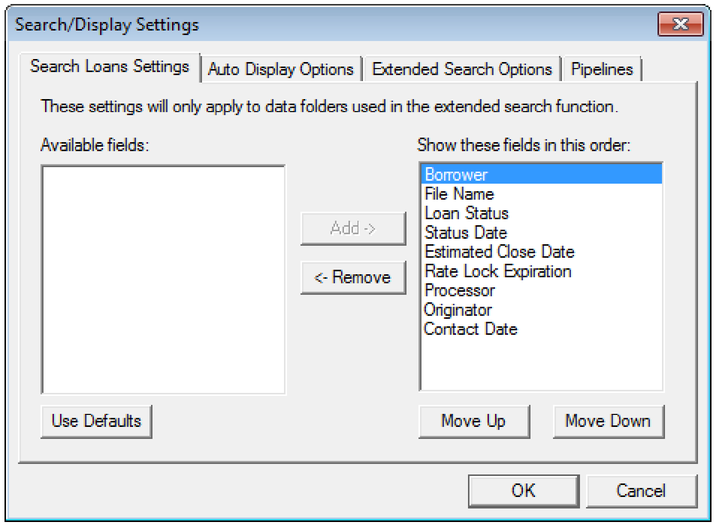


Figure 33. Point Search/Display Settings dialog box—Search Loan Settings tab

5 Click the **Auto Display Options** tab.

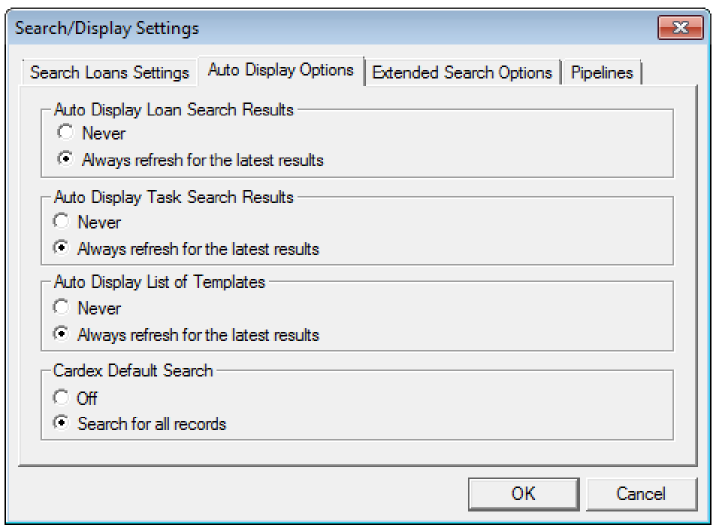


Figure 34. Point Search/Display Settings dialog box—Auto Display Options tab

6 In the *Auto Display Loan Search Results* section, click **Never**.

7 In the *Auto Display Task Search Results* section, click **Never**.

8 In the *Auto Display List of Templates* section, click **Never**.

9 In the *Cardex Default Search* section, click **Off**.

10 Click **OK** to save the settings.

Reservations

Reservations ensure that users cannot edit a loan or template file while another user has that file open for editing. In conventional Point data folders, loans are held open by keeping the file open in the file system. In PointCentral, Point transfers the loans and templates over the HTTPS connection when they are opened and closed and uses reservations to guarantee exclusive access for editing.

Creating reservations

When a Point user opens a prospect or borrower loan, the loan package (including the *.prs* or *.brw* file and all other files associated with the loan, such as the credit report) are transferred from PointCentral to the Point user's local machine.

Example

*Point user Alexander Michaels with user ID alex@themortgagebrokers.com logs in and searches for borrower loans in a data folder called **California Open**. He finds the loan he wants to edit (for example, a borrower named Johnathan Smith), and opens it for editing.*

A loan reservation is created on Johnathan Smith's loan. No other Point user is able to edit this loan until user Alexander Michaels finishes editing it and closes it.

Reservation warnings

If another Point user attempts to open a loan or template file that is reserved, an error message is displayed that indicates the file is reserved, who reserved the file, and when the file was reserved. The Point user has the option of opening the currently reserved file in read-only mode.

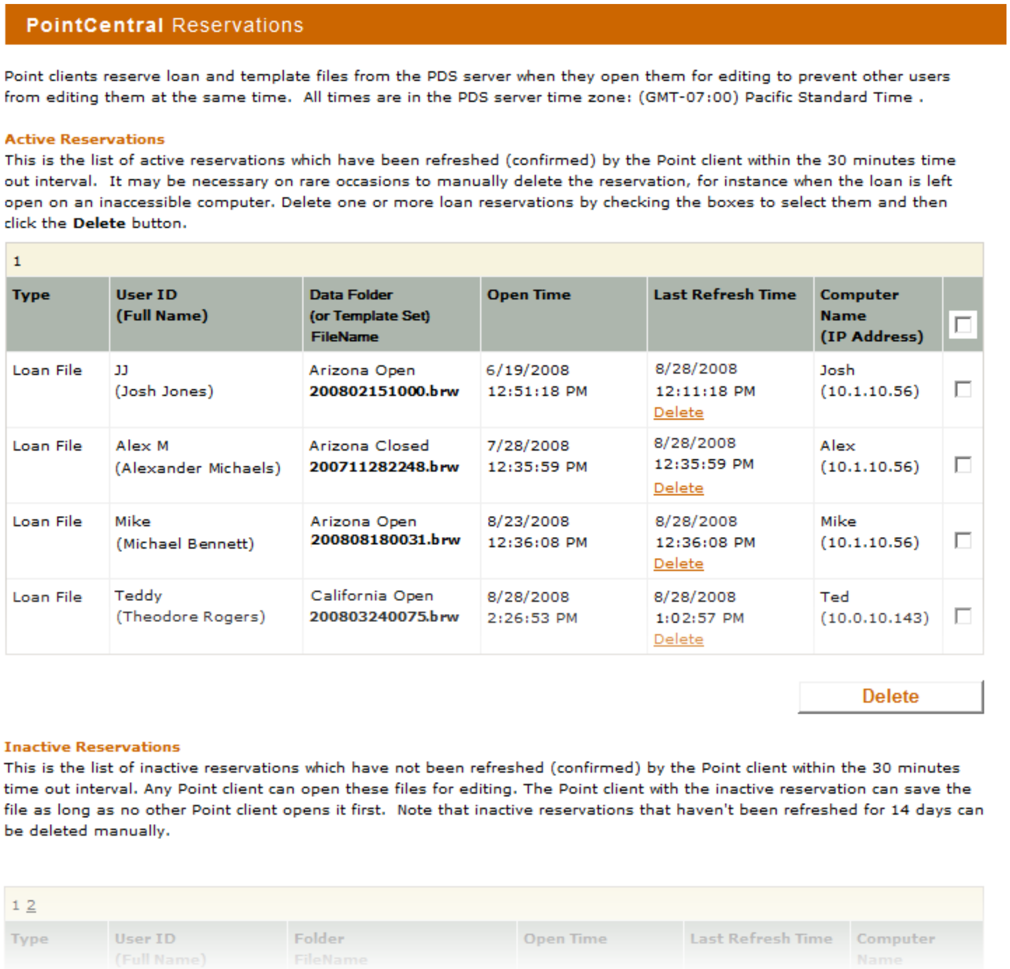
Active reservations

At any time, administrators can access the Administrator Reservations page to see relevant information about current reservations.

To access the Reservations page:

1 Select ***Reservations*** from the navigation menu.

The list of reserved files and the current user ID of the person who is working on the file is displayed.



PointCentral Reservations

Point clients reserve loan and template files from the PDS server when they open them for editing to prevent other users from editing them at the same time. All times are in the PDS server time zone: (GMT-07:00) Pacific Standard Time .

Active Reservations

This is the list of active reservations which have been refreshed (confirmed) by the Point client within the 30 minutes time out interval. It may be necessary on rare occasions to manually delete the reservation, for instance when the loan is left open on an inaccessible computer. Delete one or more loan reservations by checking the boxes to select them and then click the **Delete** button.

1

Type	User ID (Full Name)	Data Folder (or Template Set) FileName	Open Time	Last Refresh Time	Computer Name (IP Address)	
Loan File	JJ (Josh Jones)	Arizona Open **200802151000.brw**	6/19/2008 12:51:18 PM	8/28/2008 12:11:18 PM Delete	Josh (10.1.10.56)	
Loan File	Alex M (Alexander Michaels)	Arizona Closed **200711282248.brw**	7/28/2008 12:35:59 PM	8/28/2008 12:35:59 PM Delete	Alex (10.1.10.56)	
Loan File	Mike (Michael Bennett)	Arizona Open **200808180031.brw**	8/23/2008 12:36:08 PM	8/28/2008 12:36:08 PM Delete	Mike (10.1.10.56)	
Loan File	Teddy (Theodore Rogers)	California Open **200803240075.brw**	8/28/2008 2:26:53 PM	8/28/2008 1:02:57 PM Delete	Ted (10.0.10.143)	

Delete

Inactive Reservations

This is the list of inactive reservations which have not been refreshed (confirmed) by the Point client within the 30 minutes time out interval. Any Point client can open these files for editing. The Point client with the inactive reservation can save the file as long as no other Point client opens it first. Note that inactive reservations that haven't been refreshed for 14 days can be deleted manually.

1 2

Type	User ID (Full Name)	Folder FileName	Open Time	Last Refresh Time	Computer Name

Figure 35. Reservations screen

The following information is included for each reserved file:

Type

The type of file reserved, either a *Loan File* or a *Template File*.

User ID (Full Name)

The Point User ID and name that has reserved the file.

Data Folder (or Template Set) FileName

The data folder and filename of the reserved loan.

Open Time

The exact date and time the file was originally reserved.

Last Refresh Time

The last date and time the reservation was refreshed. As long as a network connection between Point and PointCentral is available, Point constantly updates PointCentral, letting it know that the reservation is still in effect. This is called refreshing the reservation.

Computer Name (IP Address)

The computer from which the loan was reserved, including the NetBIOS Name and IP address.

If a reservation is not refreshed after 30 minutes, it becomes inactive. A reservation can become inactive when the Point client loses its network connection or when a power outage occurs. The list of inactive reservations is available on the ***Reservations*** screen.

When a reservation becomes inactive, the following occurs:

- When a user who did not reserve the file attempts to open the file, the inactive reservation file is deleted and a new reservation is made for the current user.
- When the user who reserved an inactive file attempts to save the file, the file is saved and the reservation is reactivated. This feature is useful when a network connection is lost temporarily but the Point user continues to work in the file.

Tip

The default inactivity period for a reservation to become inactive is 30 minutes. You can change the default value by selecting ***Configuration > Parameters*** *and changing the Reservations* ***Time Out*** *value.*

Under normal working conditions, an inactive reservation rarely occurs.

Related information

For more information about changing the default parameters, refer to ***Setting the operational parameters****, on page 46.*

Deleted reservations

Reservations are deleted for various reasons:

- A Point user closes the reserved loan.
- An administrator deletes a reservation manually in the ***Reservations*** page.
- Point is restarted after it terminates in an abnormal way (for example, the operating system crashes or a power outage occurs and Point does not have a chance to close the loan and release the reservation).

After a reservation is deleted, any user with the appropriate access rights can open the loan or template that had previously been closed to editing.

Checking system status

Because PointCentral does not complete all requests in the sequence they are received (requests are completed asynchronously), the ***Status*** screen is helpful to view the status of requested operations.

Actions such as synchronizing data folders that host a large number of loans are typically time-consuming actions. Rather than waiting for a time-consuming action to complete, the administration site queues the requests for FileSync to complete.

The following table contains a list of possible actions:

Table 6. 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

These actions are created as the administrator submits administrative requests. When you request an action, you can access the ***Status*** screen to view feedback about the action.

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 status of **Pending**.
- FileSync begins the requested action; its status becomes **In Progress**.
- Requested action is complete; its status becomes **Done**.

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

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

Requested Actions:Pending/In Progress

The upper portion of the status page contains all requested actions that have a status of Pending or In Progress.

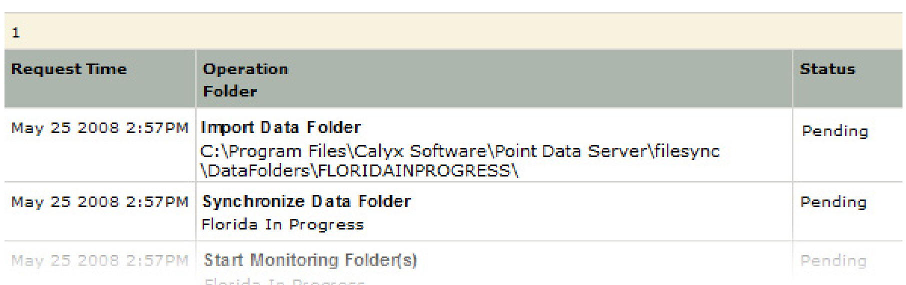


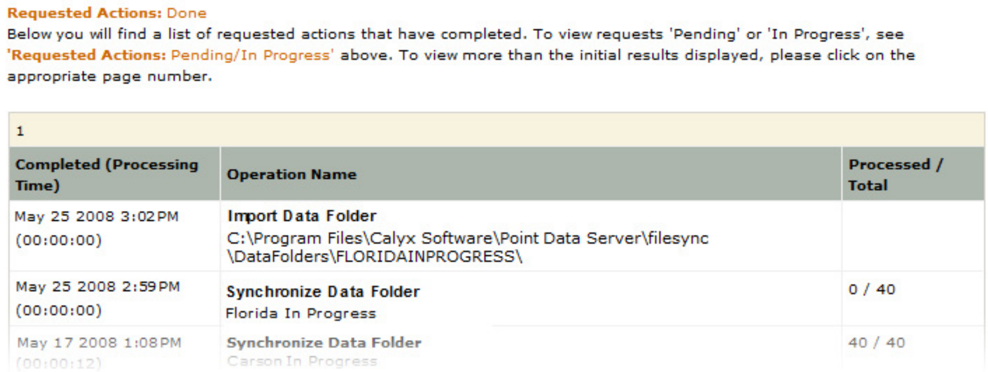
Figure 36. Status screen—Requested actions—Pending/In Progress

In this case, the request to import the conventional data folder resulted in three requested actions:

– FileSync creates the data folder in PointCentral.
– It synchronizes the data folder, scanning all loan files and saving selected values from every loan file in the SQL database.
– It monitors the new folder for any changes in the loans.

Done

When the requested actions are completed, they move from the Pending/In Progress list to the list of actions that are Done.



Requested Actions: Done
Below you will find a list of requested actions that have completed. To view requests 'Pending' or 'In Progress', see '**Requested Actions:** Pending/In Progress' above. To view more than the initial results displayed, please click on the appropriate page number.

1

Completed (Processing Time)	Operation Name	Processed / Total
May 25 2008 3:02PM (00:00:00)	**Import Data Folder** C:\Program Files\Calyx Software\Point Data Server\filesync \DataFolders\FLORIDAINPROGRESS\	
May 25 2008 2:59PM (00:00:00)	**Synchronize Data Folder** Florida In Progress	0 / 40
May 17 2008 1:08PM (00:00:12)	**Synchronize Data Folder** Carson In Progress	40 / 40

Figure 37. Status screen—Requested actions—Done

Requested actions that have been completed (with a status of Done) are listed in reverse chronological order from the time FileSync completes them. As shown in the previous figure, the three actions that had a status of Pending/In Progress are now complete, and have been moved to the list of actions with a status of Done. In this example, a fourth action is completed, because users and folder access rights were imported with the conventional data folder.

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. However, in some cases you might want to access more advanced parameters that are used to better control the system component behavior. All components include a private configuration file that contains these advanced parameters.

Use this information to define where these parameters are located and to define their possible values.

PointCentral components configuration files

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

Admin*

...\Calyx Software\Point Data Server\admin\Web.config

FileSync*

...\Calyx Software\Point Data Server\filesync\PDSFileSync.exe.config

Web service

...\Calyx Software\Point Data Server\service\Web.config

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

Admin

...\Calyx Software\Point Data Server\admin\dataconfiguration.config

PDS FileSync

...\Calyx Software\Point Data Server\filesync\dataconfiguration.config

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

Caution

The default values for the component configuration parameters should be adequate for most installations. However, you can make changes to these parameters if necessary. Carefully consider the consequences of any changes before you make them.

Administration site parameters

The administration site configuration file, web.config, is a standard ASP.NET configuration file for web sites. The administration advanced parameters are located in the <appSettings> entry inside the <configuration> entry, 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 that is used to connect the administration site to the PointCentral database.

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

Important

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

NumFoldersPerPage

The *NumFoldersPerPage* parameter is used to set the number of folders that are displayed per page on any of the relevant administration site pages.

Key

NumFoldersPerPage

Default value

20

Minimum value

1

If the number of folders to be displayed is greater than the value set in the *NumFoldersPerPage* parameter, the administration site breaks down the list into multiple pages and so the administrator can access the pages individually. This way, the system can scale and support hundreds of data folders without any visible degradation of performance.

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 is used to set the maximum time (in seconds) that the administration application waits for a response from the database before it times out. The default is 60 seconds which should be enough for most installations. If your system contains a very large number of folders, loan files, or tasks and you start experiencing time outs, you might want to increase the value.

Key

DatabaseCommandTimeOut

Default value

60

Minimum value

60

DbVersionNeeded

The *DbVersionNeeded* parameter defines which database works with the deployed component. This parameter is available in all three components. You should not change it.

Key

DbVersionNeeded

Default value

Version specific (*n.n.n*)

Related information

For more details about ASP.NET configuration, refer to your Microsoft documentation.

FileSync parameters

The FileSync configuration file, PDSFileSync.exe.config, 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 similar to 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 it times out. It is similar to 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) that is allocated for every accelerated buffer. Every accelerated folder is monitored for loan file changes. As changes to loan files are made by Point in the accelerated folders, FileSync receives notifications from the operating system. These notifications are queued up in a buffer (or a queue), which 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

For most installations, the default value should be adequate. It corresponds to a buffer of 8Kb or 8,192 bytes.

For every accelerated folder, the following files are monitored:

In the ***BORROWER*** directory:

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

In the ***PROSPECT*** directory:

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

In the root of the accelerated folder:

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

In addition, events are added to the File Watcher Buffer when a file is created, changed (saved in Point), deleted, and renamed.

One File Watcher Buffer is created for every file type defined. Seven FileWatcher Buffers are defined for every accelerated folder that correspond to the seven file types. Be careful when you increase the value of the *FileWatcherBufferSize* parameter. If you have defined a large number of accelerated folders, you could use your available RAM and cause a significant degradation of system performance.

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

Table 7. RAM usage for FileWatcherBufferSize parameter settings

FileWatcherBufferSize value	RAM used by FileSync (50 folders)	RAM used by 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 will wait (in milliseconds) before it attempts to connect to the SQL database and start monitoring data folders. This parameter is useful when the SQL Server is hosted on the same machine where FileSync is installed. By waiting a few seconds, FileSync gives enough time to 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) that FileSync will accept 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

After you make a change to any of the advanced parameters in the PDSFileSync.exe.config file, you must stop and restart File Sync for the changes to be picked up.

Web service parameters

PdsConnectionString

The *PdsConnectionString* parameter is a standard ADO.NET database connection string similar to 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) that the web service waits for a response from the database before it times out. This is similar to 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 that 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

In a system with a large number of accelerated folders, loans, and tasks, the total number of tasks returned to the Point client could be quite large. To ensure that all the bandwidth is not used by one Point client and that very large lists are not returned to Point clients, the default setting for the *MaxRecordsGetTasks* parameter is *5000*. If this limit is reached, a warning message is sent to the Point user, that indicates that the maximum number of tasks per list has been reached (Warning code -3).

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

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. This parameter is similar to *MaxRecordsGetTasks*, but instead of limiting the maximum number of tasks returned to Point, it 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 that PointCentral returns to Point on a single call. This parameter is similar to *MaxRecordsGetTasks*, but instead of limiting the maximum number of tasks returned to Point, it limits the number of Cardex entries. By default, the Point client asks for a maximum of 500 Cardex entries. The *MaxRecordsGetCardexEntries* parameter ensures that PointCentral properly scales. This occurs even if the Point client configuration changes so the limit of 500 Cardex entries retrieved per call is removed.

Key

MaxRecordsGetCardexEntries

Default value

50000

Minimum value

1

Maximum value

2147483647

MaxTemplateFileSizeKB

The *MaxTemplateFileSizeKB* parameter defines the maximum size that 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 you can further limit the maximum size.

Key

MaxTemplateFileSizeKB

Default value

5120

Minimum value

1

Maximum value

2147483647

UpgradeMessage

Use the *UpgradeMessage* parameter to define a maintenance message that will display to Point users. For example, the administrator can save a message that describes the reason for maintenance and the expected completion time.

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

In most cases, IIS automatically reads any changes you make to the Web.config file during the next request you make to any page in the administration site. But in some cases, (for example, IIS takes a long time to respond after a change) you might need to stop and restart IIS.

Requirement
You must have administrative privileges to stop and restart IIS.

To stop and restart IIS:

1. Open a command prompt window.
2. In the command prompt window, enter *iisreset /restart* and press the <Enter> key.

   After a few seconds, messages that indicate the Internet services was successfully started and stopped are displayed.

Resource management 4

An integral part of PointCentral administration is creating and maintaining users, user groups and access rights to data folders, template sets and Cardex databases. Creating user groups and globally-defined users eliminates the inconvenience of having to create the same user in multiple locations. Conventional Point manages data folders, users, and access rights in Point Administrator. The administration site manages users, user groups, data folders and access rights in the PointCentral environment.

The steps to create users, user groups, data folders, and folder access rights are typically done in the following sequence:

- Create new users
- Create new user groups
- Add users to user groups
- Create new data folders, template sets, rules, and Cardex databases
- Grant access rights to the appropriate user groups in each relevant data folder, template set, rules, and Cardex database
- Grant individual user access rights to specific resources (data folders, template sets, rules, or Cardex databases) when a user has an access need that is not addressed in their group membership

In this topic

Related information

If you are not familiar with the administration site, see ***Administration detail****, on page 44.*

Users and user groups

Users

Each user is a Point login for an individual user. Users are assigned a unique full name, a unique user ID, and a password.

License management

With license control, making various license additions and access changes automatically updates the MyCalyx digital key in PointCentral, which could potentially 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. When the grace period expires, users are no longer able to connect to PointCentral until the MyCalyx digital key is refreshed.

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

- Sites that update their MyCalyx digital key manually forgot to do the 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. This scenario typically occurs when a PointCentral site cancels their account.

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

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

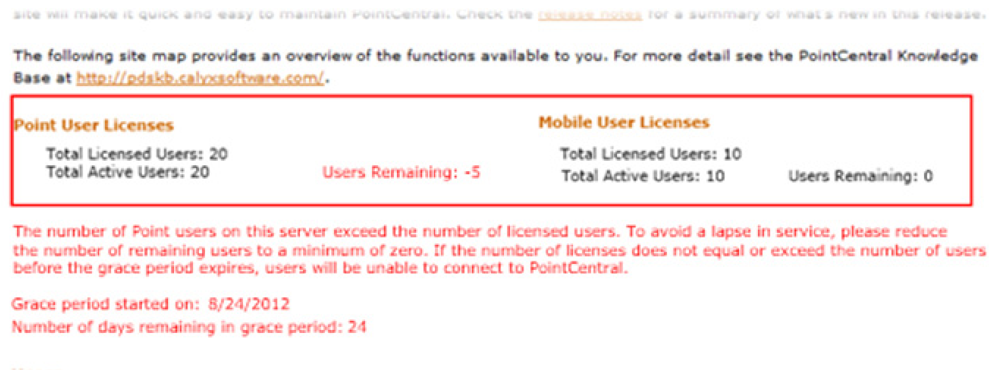


Figure 38. Point User Licenses, Mobile User Licenses

When the license count exceeds the licenses, the message is issued on the ***Home*** page below the license summary information. The grace period begins at this time.

The following options are available when your 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, allowing your service to lapse.

If an action is not taken to reduce the increased user count, Point and mobile users cannot log in to PointCentral until the issue is resolved.

Adding users

The following conventions apply when adding a new user:

- The full name and user ID must be unique.
- The full name, user ID, and password must be entered in the same format as created. For example, *PointCentral User* is not the same as *pointcentral User*.
- If the new user is given *This Processor's Files Only or This Originator's Files Only* access rights, 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. This data is set in the Point ***Utilities > Dropdown Lists*** function.

To add a PointCentral user:

1 Select ***Users > Add User*** from the navigation bar to access the ***Add User*** screen.

Figure 39. Add User screen

2 Enter the name of the user in the *Full Name* field.

Important

- *Full Names are case-sensitive and must be unique.*
- *User IDs are case-sensitive and must be unique.*
- *Passwords are case-sensitive and must be unique.*

3 Enter the user ID in the *User ID* field.

4 Enter the password for the account and repeat it in the *Confirm* field**.**

5 Specify whether the user will have **Point** access, **Mobile** access, or both.

Important

If the option is not selected for a user to have Point access, they will receive an error when they attempt to log in to Point.

6 Optionally, enter the user's e-mail address in the *Email* field.

7 Click **Add User**.

> **Related information**
>
> *For information about **Utilities > Dropdown Lists** in Point, refer to the **Point User Guide**.*

Editing users

Use the ***List Users*** option to access all user accounts, search for a user, edit a user, and delete a user.

To list the users:

1 Select ***Users > List Users*** from the navigation bar to access the ***List Users*** screen.

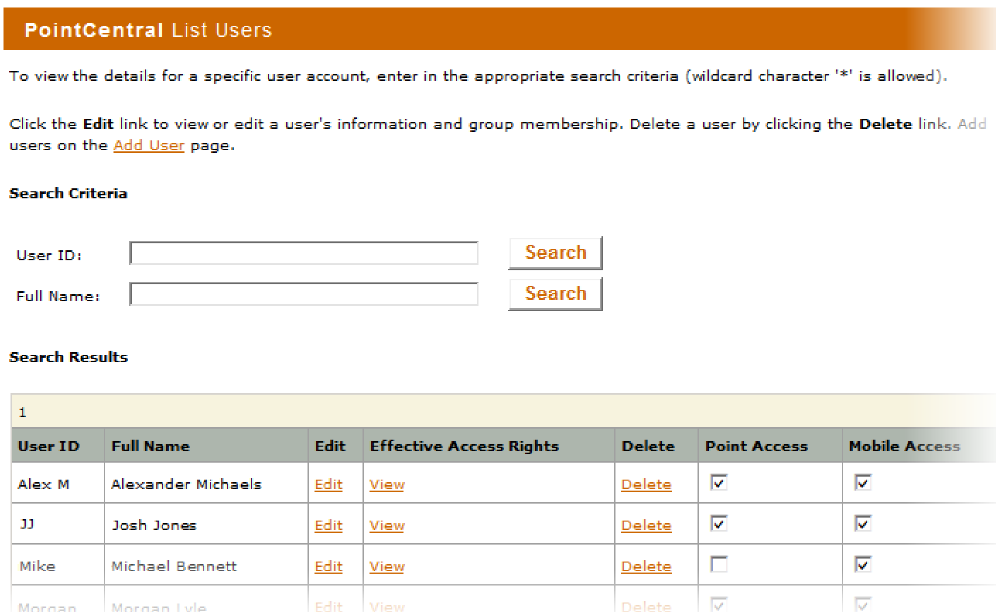


Figure 40. List Users screen

2 To search for a user, enter their user ID or full name and click **Search**.

The username that matches the search criteria is displayed in the list.

3 To delete a user, click **Delete** and confirm the deletion.

4 To change a user’s Point or mobile access, remove or select the check boxes in the *Point Access* and *Mobile Access* columns.

5 To edit the user information, click **Edit**.

The ***Edit User*** screen is displayed.

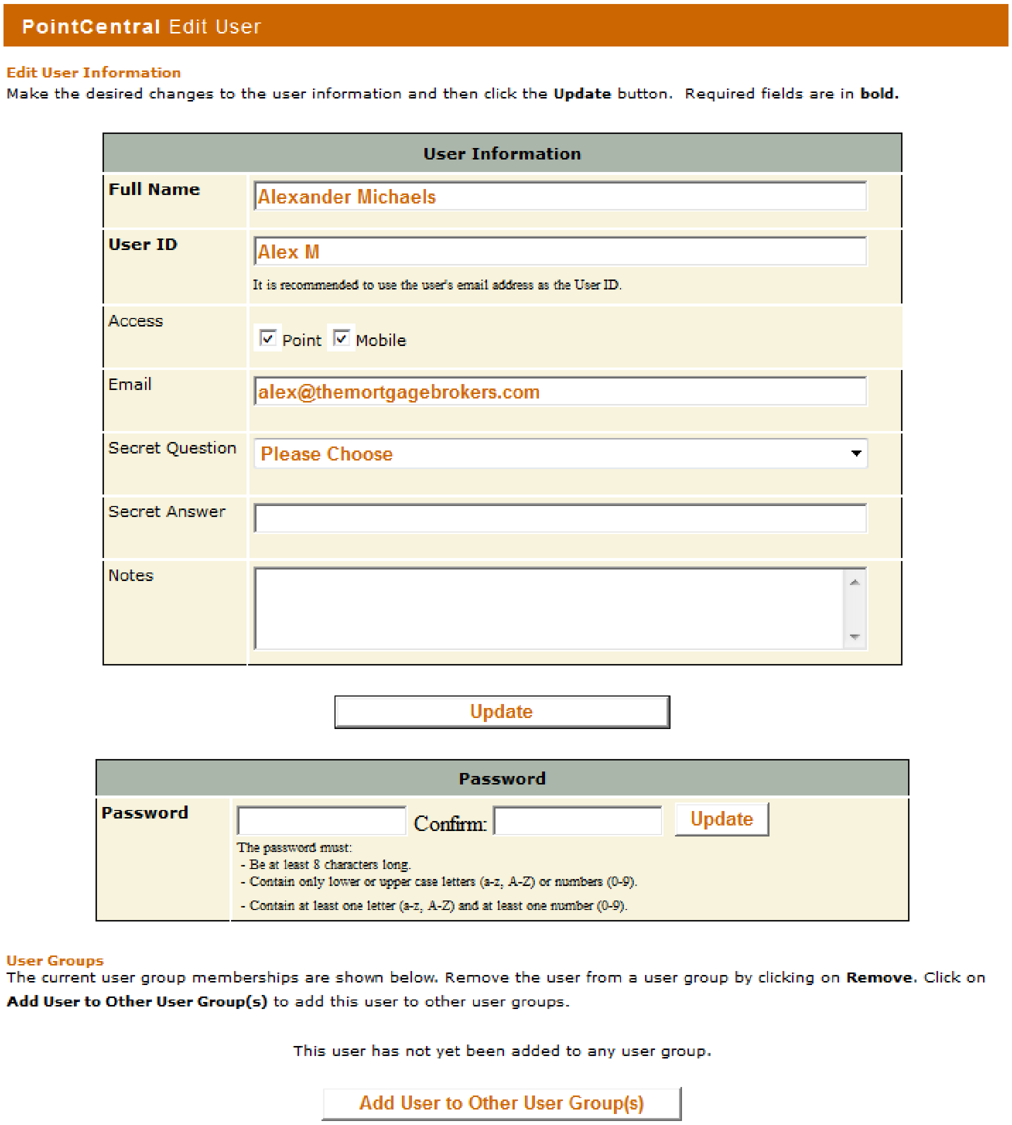


Figure 41. Edit User screen

The ***Edit User*** screen contains detailed information about the user account.

6 Edit the user information as needed, select a secret question and provide the answer, and enter any notes about the user.

7 Click **Update**.

8 To change the user password, enter a new password in the *Password* field, and repeat it in the *Confirm* field.

9 Click **Update**.

10 Click **Add User to Other User Group(s)** to add the user to an existing user group.

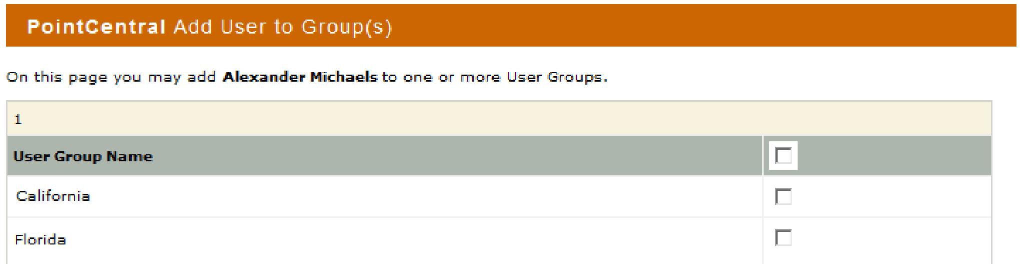


Figure 42. Add User to Group(s) screen

11 Select the check boxes next to the groups to which you want to add the user and click **Add User to Group(s)**.

A message is displayed that indicates the user was added to the selected groups.

12 Click **Back** to return to the ***Edit User*** screen.

Unlocking users

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

To unlock a locked user:

1 Select ***Users > Locked Out Users*** from the navigation bar to access the ***Locked Out Users*** screen.

2 To cancel a lockout immediately, click *Delete Lockout* for the user.

Related information

*Refer to **Setting the operational parameters**, on page 46, for more information about how to configure the lock out period.*

User groups

User groups are typically based on how the company is structured. This could be by department, location, or function (for example, Orlando processors). A user can be a member of any number of user groups. For example, the Director of Underwriting can belong to the Orlando Processors user group as well as the Orlando Management user group.

User groups are a convenient way to grant and manage the same access rights to a set of data folders to a group of users at once. User groups make it very easy to add or change access rights to a data folder for all the users in the group in a single operation. Say you have a new hire in the Orlando Processors group. Granting that processor access rights to all the necessary data folders is a simple process of adding them to the Orlando Processors group.

When a user is a member of multiple user groups, the access rights to a particular data folder are the highest access rights granted by any of the user groups to which the user belongs. If one user group grants the user read-only access to the data folder called ***Orlando In Progress***, and another user group grants the user read/write access to the same data folder, then the user has read/write access to the data folder.

Adding user groups

To create a new user group:

1 Select ***User Groups > Add User Group*** to access the ***Add User Group*** screen.

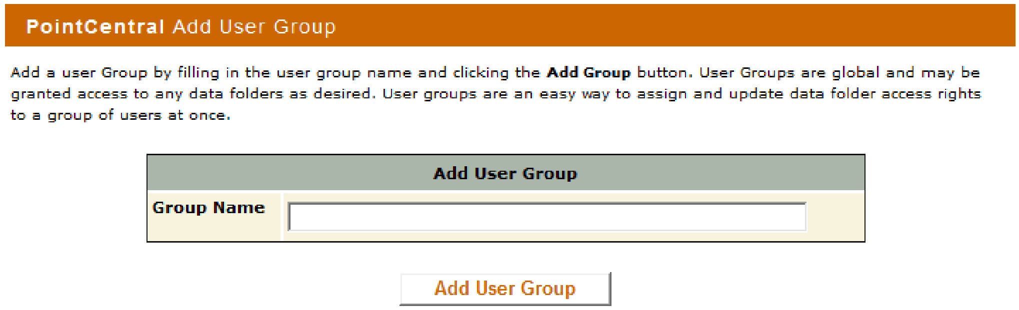


Figure 43. Add User Group screen

2 Enter the name of the group in the *Group Name* field.

3 Click **Add User Group**.

The user group is created and the ***Edit User Group*** screen is displayed.

Editing user groups

Edit the user group or a user's membership, or delete the user group entirely.

1 Select ***User Groups > List User Groups*** to access the list of user groups.

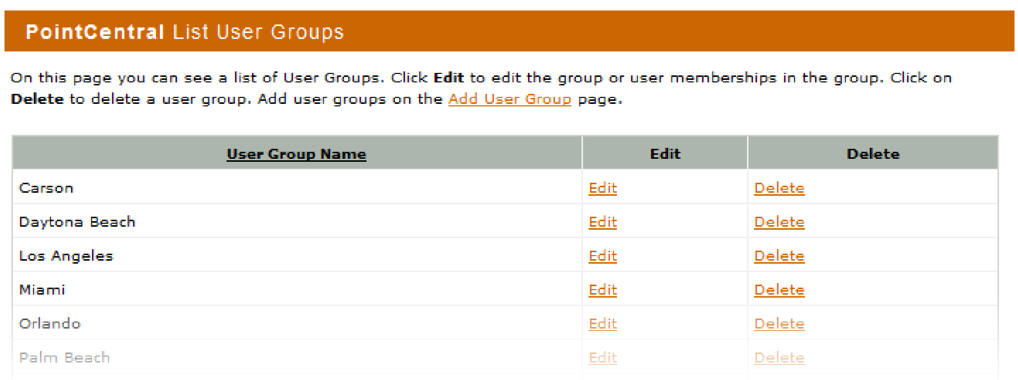


Figure 44. List User Groups screen

2 To delete a user group, click **Delete** and confirm the deletion.

3 To edit the user group information, click **Edit**.

The ***Edit User Group*** screen is displayed.

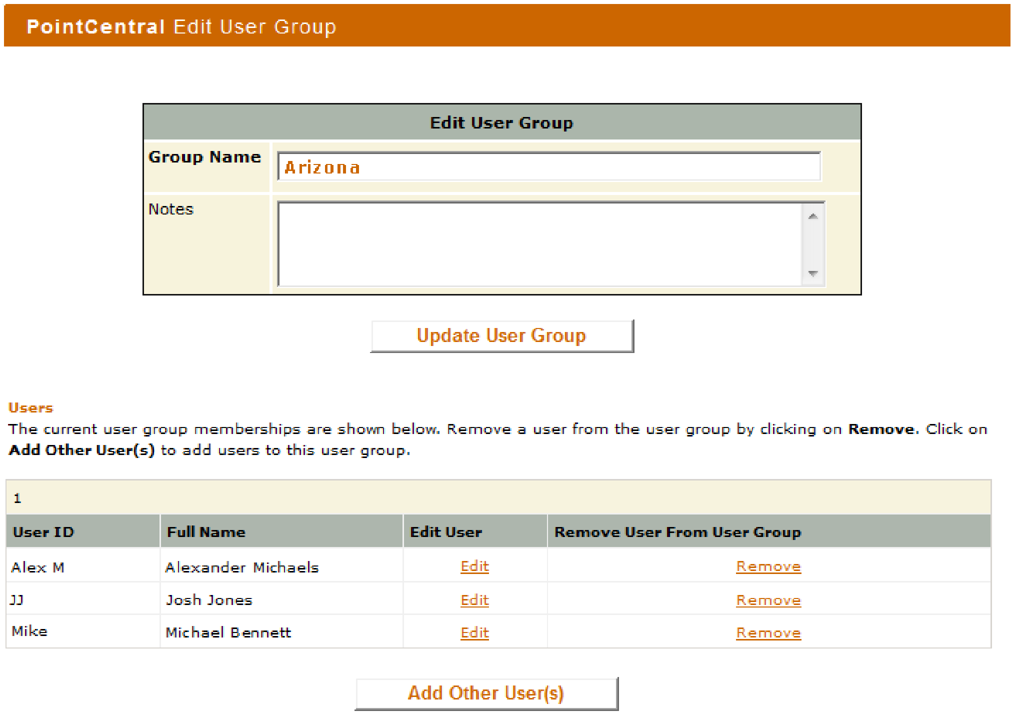


Figure 45. Edit User Group screen

The ***Edit User Group*** screen shows the selected user group and the list of the group members.

4 Click **Add Other Users(s)**.

The ***Add User(s) to User Group*** screen is displayed.

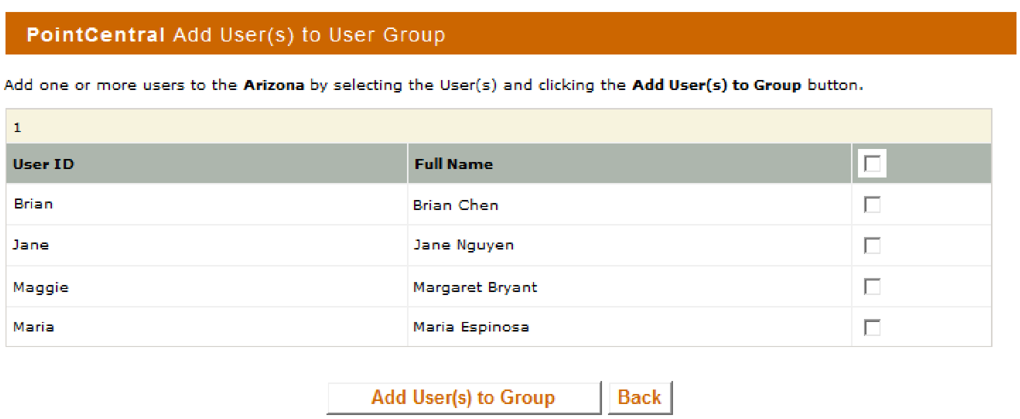


Figure 46. Add User(s) to User Group screen

5 Select the users to add to the group and click **Add User(s) to Group**.

6 Click the **Back** button to return to the ***Edit User Group*** screen.

The new user is in the user list.

Data folders

Data folders are typically created based on how loan files are processed by the company. This could be by status, location, or team (for example, *Orlando In Progress*). Each data folder of Point files is a resource to which users or user groups can be granted access.

Data folder organization

While PointCentral can access any data folder you have set up on PointCentral, you must develop a standard folder deployment plan for your organization. This topic provides suggestions about the preferred method for deploying Point data folders, and discusses methods for deploying PointCentral across one or multiple servers.

Folders are typically set up based on how loan files are processed within the organization. The data folder organization often reflects the loan status, location, and role (Loan Processor, Loan Originator, etc.).

Loan status

Point reflects a number of loan statuses (such as Open, Submitted, Approved). The Loan Status is determined in Point by the loan originator or processor who performs certain actions on a loan and enters the dates they were completed. As the loan originator or processor continues working in the file, Point displays the Loan Status according to the dates entered. For example, if an Open date is entered, the status reflects Open but when the loan originator enters a Submitted date, the status moves from Open to Subm.

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

Table 8. Loan status data folder structure

Loan status	Loan state	Data folder
Open Submitted Approved Clear to close Documents Funded Recorded	In progress	In progress
Closed	Closed	Closed
Suspended Denied Canceled	Canceled	Canceled

Attention

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

Location

Branches are defined as a physical location or a logical separation of units within your organization. You might have branches in different cities or have multiple branches in the same city.

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

Table 9. Location data folder structure with branches in different states

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

The following table shows an example of a location data folder structure when your organization has multiple branches in the same state:

Table 10. Location data folder structure with multiple branches in one state

Branch	City	Data folder
Florida	Daytona Beach	Daytona Beach In progress Daytona Beach Closed Daytona Beach Canceled
	Miami	Miami In progress Miami Closed Miami Canceled
	Orlando	Orlando In progress Orlando Closed Orlando Canceled
	Palm Beach	Palm Beach In progress Palm Beach Closed Palm Beach Canceled

Role

You can also define data folders based on how your organization is structured (including user groups). The following table shows an example of a data folder structure by organization:

Table 11. Organizational data folder structure

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

Adding data folders

To create a new data folder:

1 Select ***Data Folders > Add Data Folder*** to access the ***Add Data Folder*** screen.

The ***Add Data Folder*** screen is displayed.

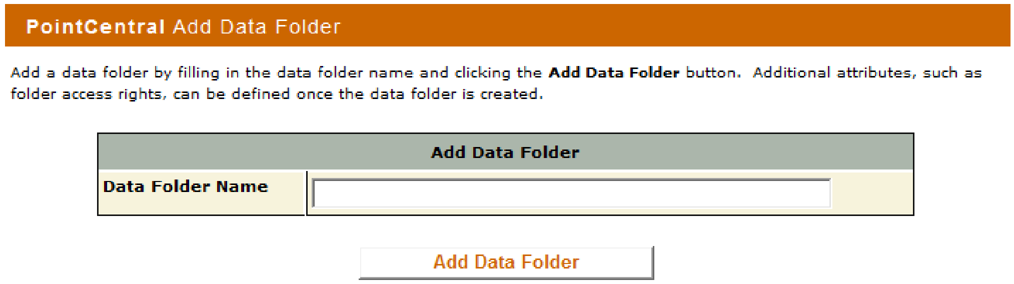


Figure 47. Add Data Folder screen

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

3 Click **Add Data Folder**.

The ***Edit Data Folder*** screen is displayed.

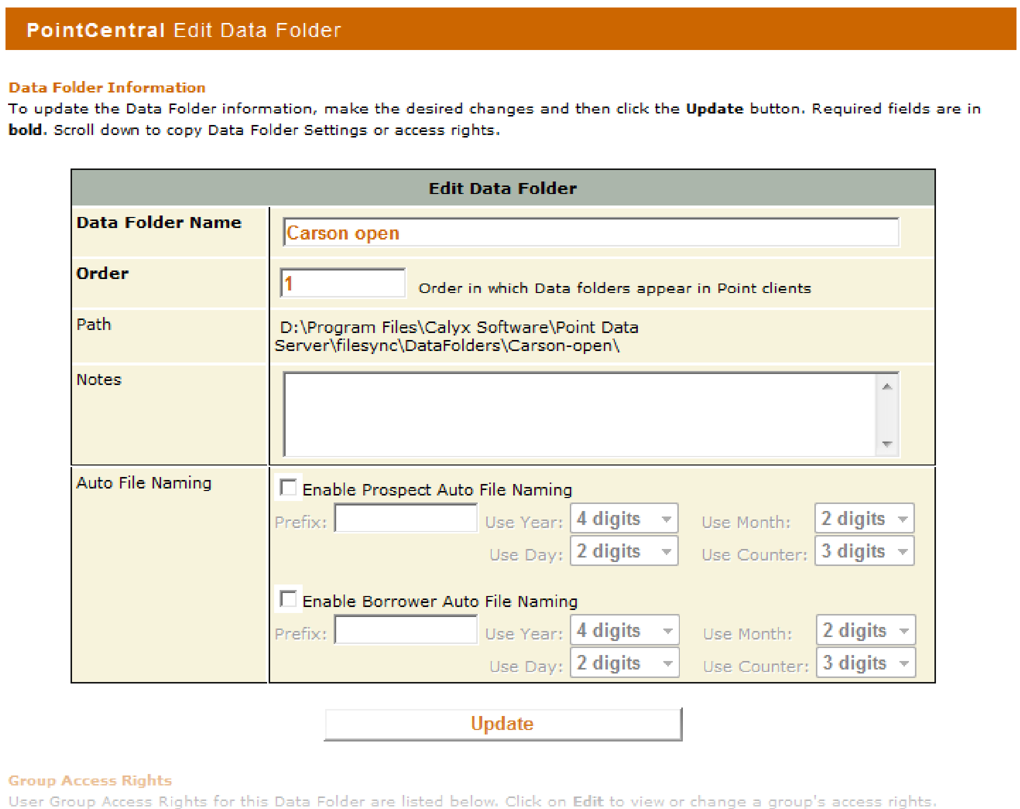


Figure 48. Edit Data Folder screen

Note

The confirmation message at the top of the screen states that the data folder will be created. Some operations, such as creating data folders, are queued for execution asynchronously by the FileSync component. If there are no operations in the queue, the request can complete within seconds. With asynchronous execution you can continue to work while time-consuming operations are completed in the background.

*To view the status, click the **Status** link.*

You can perform the following actions on this screen:

- Edit the folder name
- Specify the sequence to list in the client data folder list
- Enter notes
- Specify auto file naming options
- Add user group access rights
- Add user access rights
- Copy folder settings from another folder
- Copy user and group access rights from another folder

4 Change the data folder properties and enter notes about the folder, as needed.

5 Specify Auto File Naming options.

With Auto File Naming, Point names files according to the parameters that you set. This feature reduces the accidental overwriting of file names and is required to use offline file creation.

a Click the **Enable Auto File Naming** check box for prospect or borrower files to enable auto file naming.

Important

To allow Point mobile users to create new loan files from their mobile devices, you must enable auto file naming for borrowers. If auto file naming is not enabled, users cannot save new loan files.

b Enter a prefix for the file names in the *Prefix* field.

c Select the number of digits to use from the ***Use Year***, ***Use Day***, ***Use Month***, ***Use Counter*** dropdown lists.

d Click **Update**.

Related information

For information about offline file creation, refer to ***Offline file creation**, on page 80.*

Data folder access rights

Setting access rights defines which users are allowed access to which resources and the manner in which they can achieve access. Each access rights definition relates a single user group or user to a single resource, such as a data folder, and defines the nature of the access granted. The following figure shows an example of the relationship between users, user groups, and data folders:

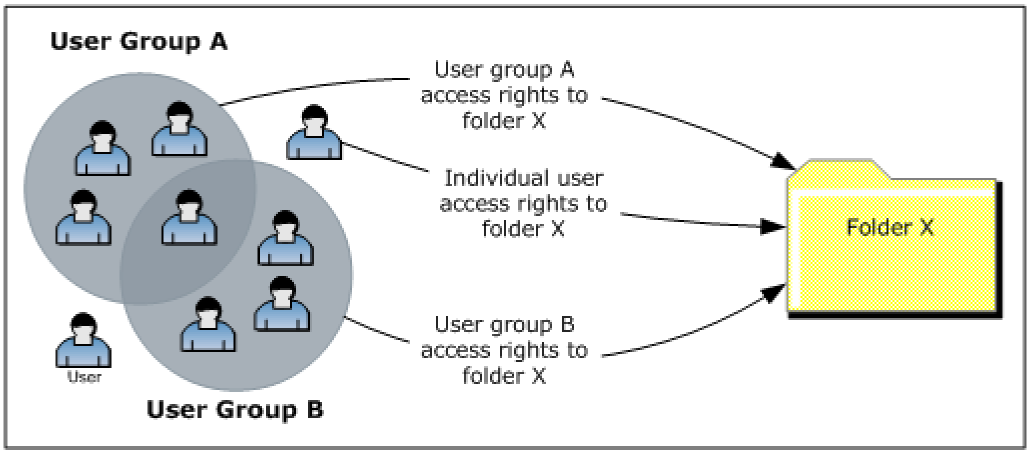


Figure 49. User, user group, and data folder relationship

There are no default access rights. For a user to access a data folder, you must establish an access rights definition between the two of them.

When you utilize user groups, you create fewer access rights definitions because these are defined for the collective user group rather than for every individual user and data folder they access.

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 can be defined between the folder and a user group that includes the same user. The access rights definitions are merged for the particular user that results in granting the user the highest access rights granted by any of the definitions to the data folder.

If a user is assigned, **This Processor's Files Only** and **This Originator's Files Only**, the **This Processor's Files Only** setting takes precedence and access is granted accordingly. The following table shows the effective permissions for different access right combinations:

Table 12. Effective permissions for user access right combinations

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

Important

*If a user's access rights are set to **This Processor's Files Only** or **This Originator's Files Only**, the full name must be entered exactly as it was created in the originator or processor dropdown list in Point.*

Related information

- *Refer to* ***Template sets****, on page 96, for information about adding a template set and granting access rights.*
- *Refer to* ***Importing resources****, on page 134, for information about adding a Cardex database and granting access rights.*
- *Refer to Chapter 5,* ***Access right reports****, for information about reports that show the relationship between users, groups, access rights, and for resources that make the relationships easy to understand. The User Effective Access Rights report is particularly useful for showing all the resources that a specific user can access.*
- *For information about creating processor and originator dropdown lists in Point, refer to the* ***Point User Guide****.*

Offline file creation

If a user creates a loan file while disconnected from PointCentral and stores it in a data folder that is enabled for offline file creation, the file is automatically moved into the corresponding data folder on PointCentral the next time the user is connected.

Offline file creation permission is specified at the user, user group, and data folder levels by selecting the **Allow Offline File Creation** check box in the ***Edit User Group Access Rights*** or ***Edit User Access Rights*** screens. You can store a loan file that is created offline in an offline-enabled data folder by a user or user within a group with offline privileges for that data folder.

Requirement

Auto file naming must be enabled for both prospects and borrowers in the ***Edit Data Folder*** *screen. If Auto File Naming is not enabled, an error will occur when adding user and user group access rights to a data folder. An error will also occur if you attempt to save an offline file in a data folder that is not enabled for Auto File Naming. You must either enable Auto File Naming for the selected data folder or select a data folder with Auto File Naming enabled.*

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

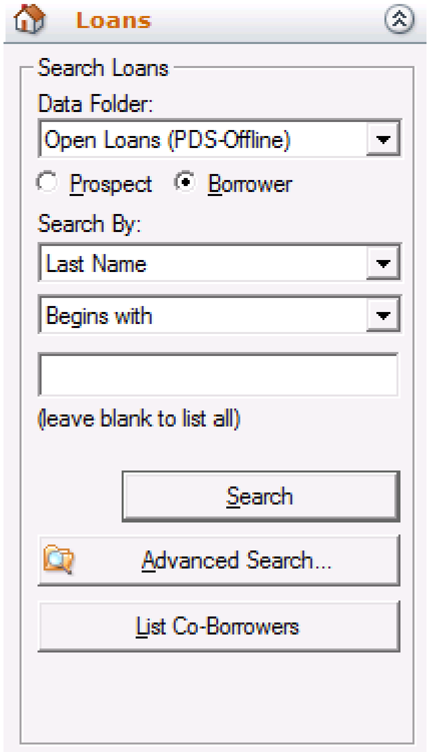


Figure 50. Offline data folder example

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

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

Loan files that were saved locally in offline-enabled data folders are automatically moved the next time the you are connected to PointCentral. The moved files are no longer accessible on the local machine.

After the move is complete, the following dialog box is displayed:

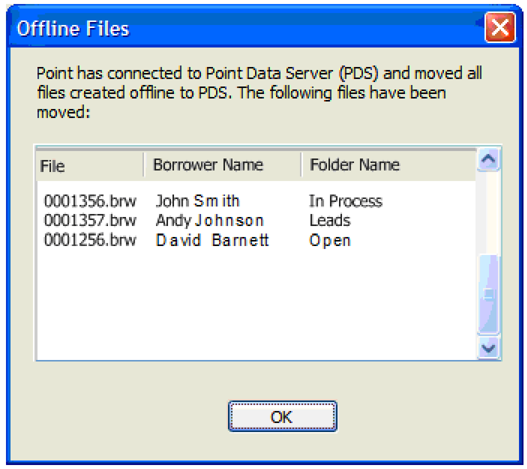


Figure 51. Offline Files dialog box

If an error occurs when moving the files from Point to PointCentral, the following dialog box is displayed:

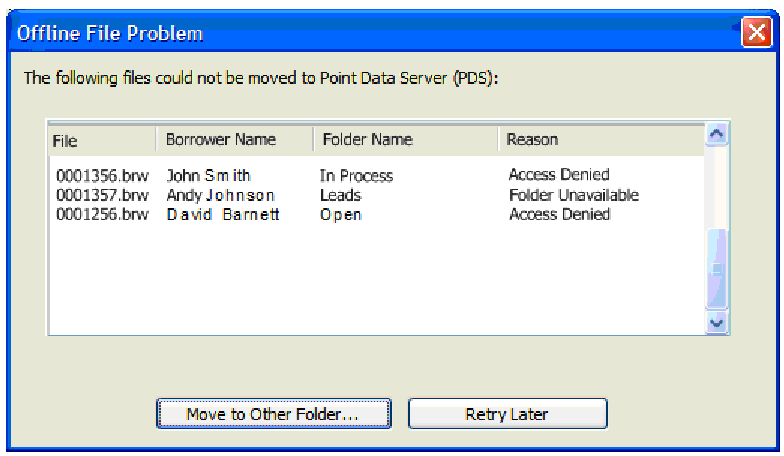


Figure 52. Offline File Problem dialog box

Errors can occur during synchronization for the following reasons:

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.

To select a different folder to move the file to, click the **Move to Other Folder** button.

To make another attempt to move the offline file the next time you log in to PointCentral, click the **Retry Later** button.

> **Related reading**
>
> *Refer to **Users and user groups**, on page 67, for more information about specifying users and group access rights and Auto File Naming options.*

Specifying user and user group data folder access rights

When access rights are modified for a user or group, changes are effective immediately. The user can log out and log in again (without closing and re-opening Point) to activate the changes.

The process to set access rights to data folders for user groups and users is the same. The steps to specify user group access rights to data folders are used in this example.

To add access rights for a user group to a data folder:

1 Select ***Data Folders > List Data Folder*** to access the ***List Data Folders*** screen.

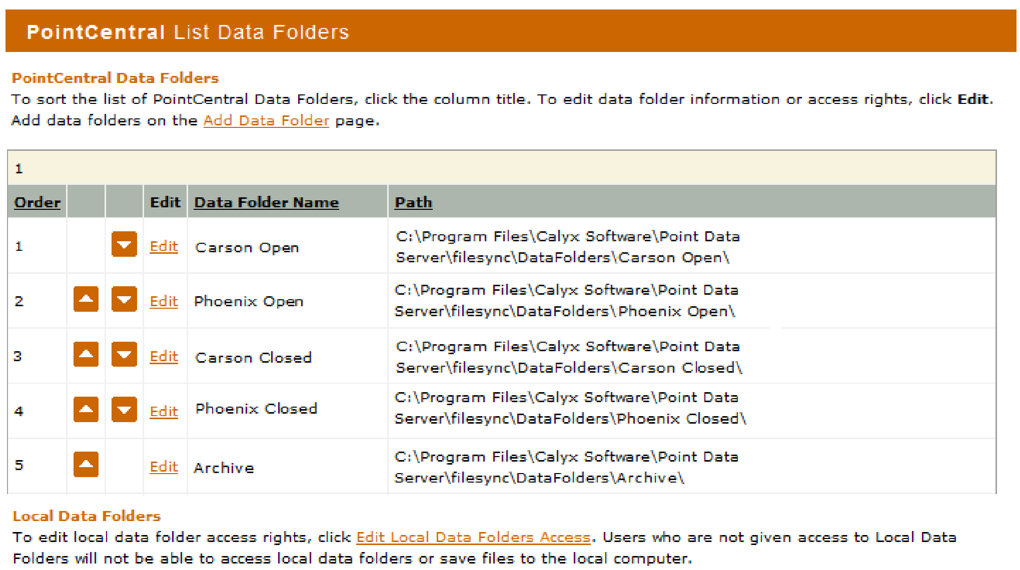


Figure 53. List Data Folders screen

You can do the following actions from the ***List Data Folder*** screen:

- Edit data folder information
- Configure Auto File Naming as needed.
- Edit the user and user group access rights.
- Enable offline file creation.

2 Click the **Edit** link that corresponds to the folder you want to edit.

The ***Edit Data Folder*** screen is displayed.

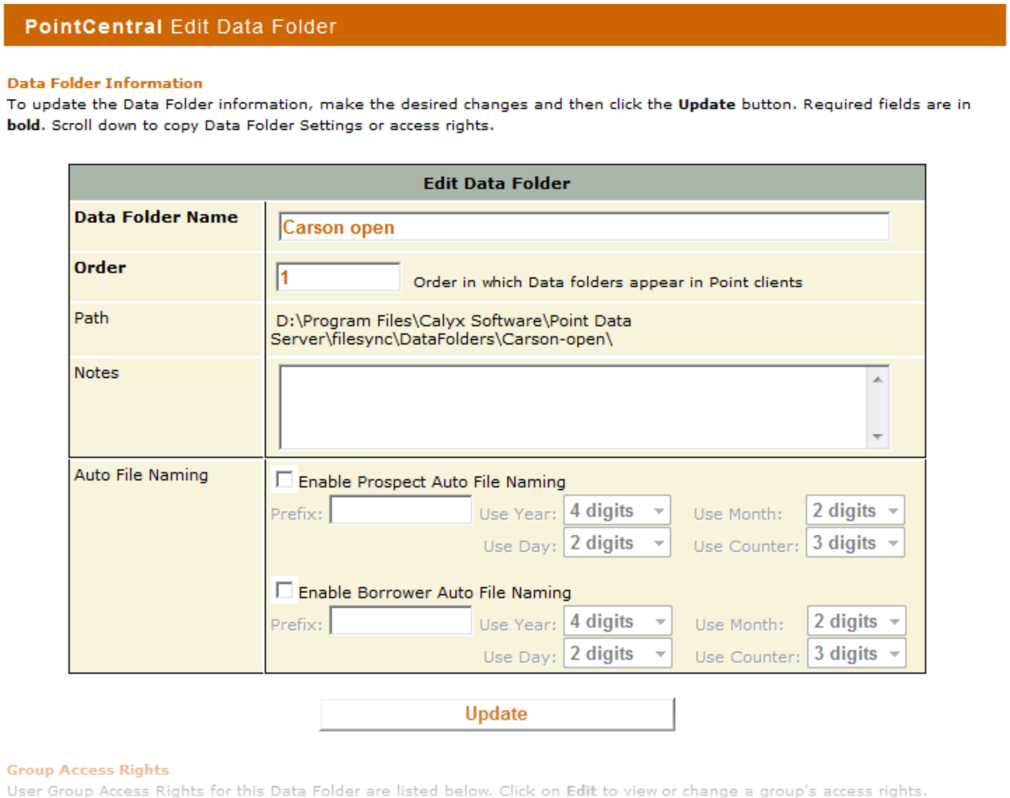


Figure 54. Edit Data Folder screen

In addition to adding and updating user and user group access rights, you can edit the data folder name, priority order, enter notes about the data folder, and specify auto file naming options in this screen.

3 To change the data folder name, priority order, enter notes, and specify auto file naming options, enter new values and click ***Update***.

4 Scroll down to the *Group Access Rights* section.

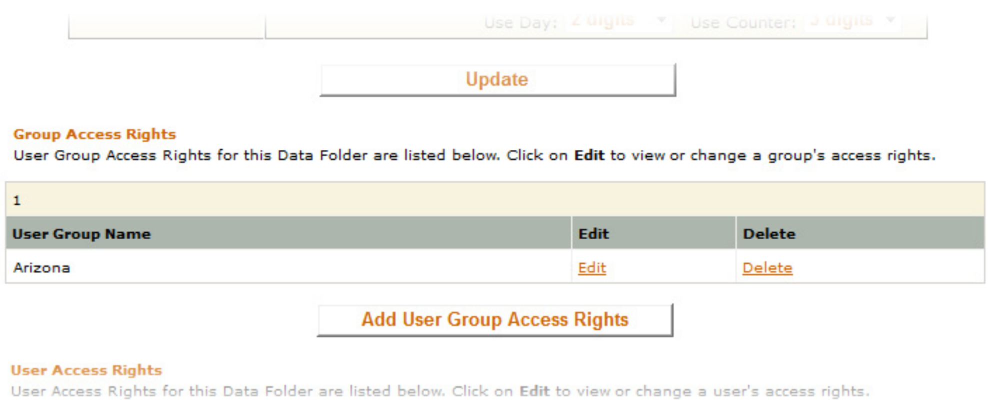


Figure 55. Edit Data Folder screen—Add User Group Access Rights

User groups with access rights to the data folder are displayed.

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

Tip

To specify user access rights to data folders, scroll to the User Access Rights section and click **Add User Access Rights**.

The ***Add Access Rights*** screen is displayed.

Figure 56. Add Access Rights screen

Use this screen to establish group security and access rights, specify operations that group members can perform on loans in the data folder, such as copying and moving, and specify whether the group members can access certain functions on the ***Utilities*** menu in Point.

6 Select a user group.

7 Complete the *Loan Security* section.

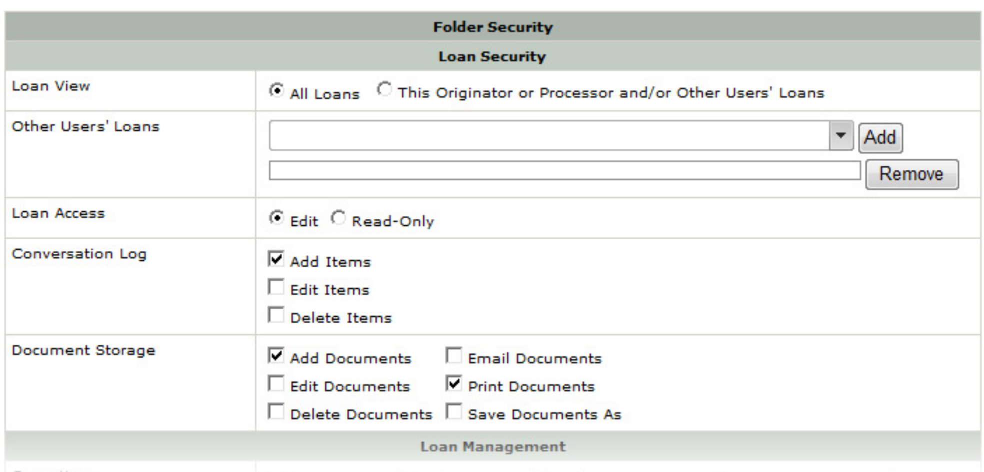


Figure 57. Add Access Rights—Loan Security

a Select **All Loans** to specify whether the users (loan processors or loan originators) in the group have access to all the files in the folder or select **This Originator or Processor and/or Other Users' Loans** to indicate that the users can access only specific user's loans.

To specify which user's loans, type the user's name in the dropdown list to filter the list and click **Add** when you select a name to add it to the text box.

Click **Remove** to delete a selected user from the text box.

All Loans is the default selection.

> **Important**
>
> *The access rights of the current user apply to the data folders and loans of other loan originators and processors. The user does not have any additional privileges if the owner of the data folder has a higher level of access.*

b Specify if the users in the group can edit loans in the folder or if they have read-only privileges.

Edit is the default selection.

c Specify the level of control the users in the group have with items in the conversation log (add, edit, or delete). You can select more than one option.

Add Items is the default selection.

d Select the document repository operations that group members can perform on the loans in this data folder (add, edit, delete, e-mail, print, or save as). You can select more than one option.

Add Documents and **Print Documents** are the default selections.

> **Important**
>
> *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.*

8 Complete the *Loan Management* section.

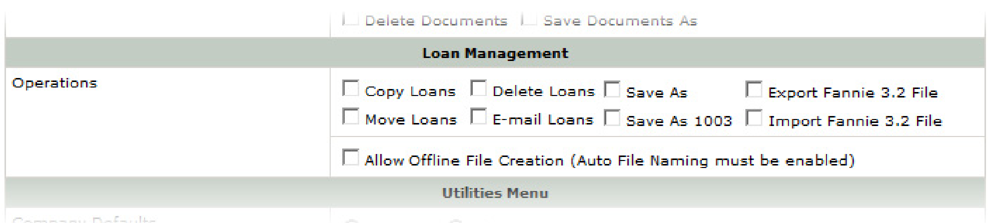


Figure 58. Add Access Rights—Loan Management

a Specify the actions that users in the group can take with the loans in this data folder (copy, move, delete, e-mail, save as, save as 1003, or import or export Fannie 3.2 file). You can select more than one option. When these actions are disabled here, the actions are not available for the files in that data folder.

b Select the **Allow Offline File Creation** check box to allow users in the group to create files in this data folder when they are not connected to PointCentral.

9 Specify whether users in this group have the ability to edit the company defaults and the dropdown lists that are created in the ***Utilities*** menu in Point, or access the audit trail log in Point.

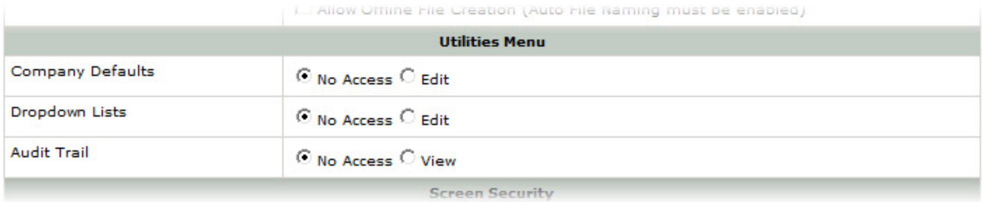


Figure 59. Add Access Rights—Utilities Menu

Definitions

No Access (default)

*The following **Company Defaults** options are disabled on the **Utilities** menu when* **No Access** *is selected:*

- *Company Info*
- *Processing Center*
- *Days Per Year*
- *ECOA Address*
- *CA Fair Lending Address*
- *Denial Letter Address*
- *Servicing Disclosure Info*

*All **Dropdown List** menu options on the **Utilities** menu in Point are disabled and grayed out for loans in the selected data folder.*

Edit

*The following **Company Defaults** options are enabled on the **Utilities** menu when* **Edit** *is selected:*

- *Company Info*
- *Processing Center*
- *Days Per Year*
- *ECOA Address*
- *CA Fair Lending Address*
- *Denial Letter Address*
- *Servicing Disclosure Info*

*All **Dropdown List** menu options on the **Utilities** menu in Point are enabled for loans in the selected data folder.*

To allow specified users access to the audit trail log in Point, select **View**. Authorized Point users can view and access the ***Audit Trail*** option from the ***Utilities*** menu. The ***Audit Trail*** option is not visible on the ***Utilities*** menu for unauthorized users.

Requirement

*You must enable the Audit Trail option on the PointCentral **Parameters** page to activate the audit trail in Point. If this setting is not enabled, the **Audit Trail** does not track any changes and the menu option is not available in Point, even if the user is granted access to the audit trail log.*

10 Specify the screen security settings that the users in the group have to the ***Registration & Lock***, ***Trust Account***, and ***Loan Profit/Loss*** tracking screens and the Banker screens in the loan.

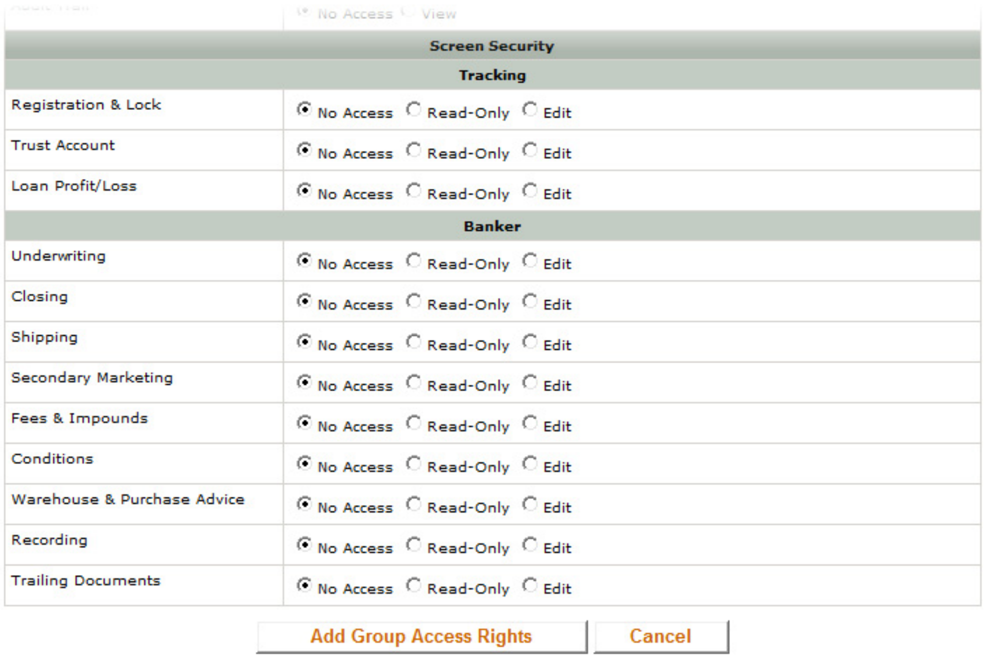


Figure 60. Add Access Rights—Screen Security

Definitions

The following definitions apply for tracking and banker screen access options:

No Access (default)

The screen name is grayed out in the Point menu and is not accessible, screen-specific fields are not viewable in reports, and the **Banker** *tab in the* **Borrower Forms** *dialog box not visible.*

Read-Only

The screen and the contents are visible in Point. However, the fields are disabled and the user is unable to change or enter any values.

The following buttons, which are used to create documents, are disabled:

- *Create Registration Request (**Registration & Rate Lock** screen)*
- *Create Lock Request (**Registration & Rate Lock** screen)*
- *Create Lock Confirmation (**Secondary Marketing** screen)*
- *Create Suspense/Denial Notice (**Underwriting** screen)*
- *Create Loan Approval Notice (**Conditions** screen)*
- *Create Funding Conditions Notice (**Conditions** screen)*

The following buttons are enabled and the user can access the associated function. However, the **OK** *button is disabled in the dialog box which prevents the user from saving any changes to the fields.*

- *Appraisal*
- *Insurance*
- *Escrow & Title*
- *Program/Lock Details (**Closing, Conditions**, **Fees & Impounds**, and **Underwriting** screens)*
- *Loan Program Details (**Secondary Marketing** screen)*

Edit

The screen is available in Point and all fields are editable.

Important

*The settings specified for **Track** and **Banker** screens take precedence over the specified document storage settings.*

11 Click **Add Group Access Rights**.

12 Set up security for additional user groups as needed.

13 When finished specifying user group access rights, click **Cancel** to return to the ***Edit Data Folder*** screen.

Related information

- *For information about enabling the audit trail option, refer to* ***Setting the operational parameters****, on page 46.*
- *Refer to* ***Adding data folders****, on page 76, for more information about specifying auto file naming options.*
- *Refer to* ***Offline file creation****, on page 80, for more information about offline file creation.*

Copying folder settings and access rights

To copy folder settings and access rights from another folder:

1 Select ***Data Folders > List Data Folder*** to access the ***List Data Folders*** screen.

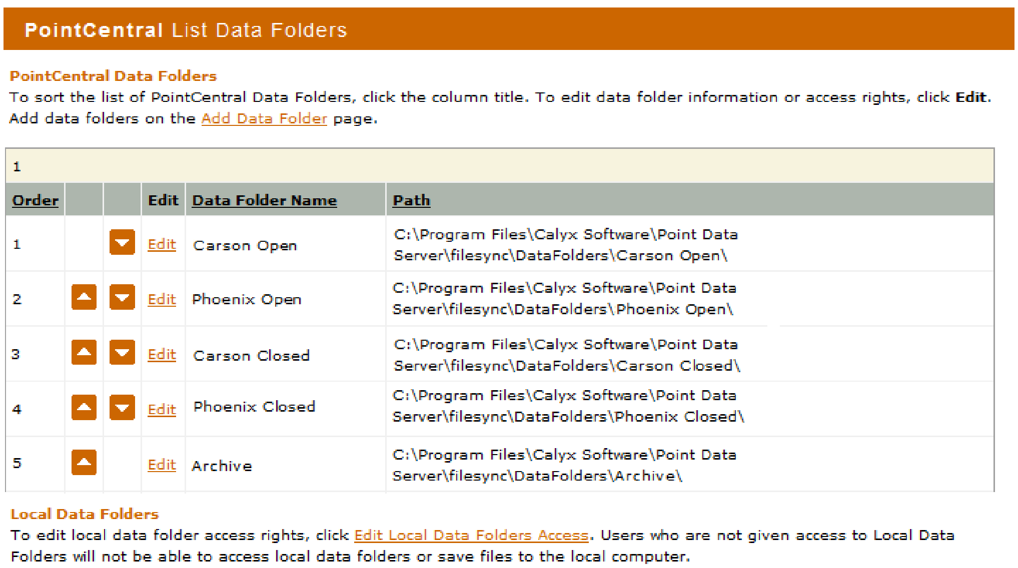


Figure 61. List Data Folders screen

2 Click the **Edit** link that corresponds to the folder you want to edit.

The ***Edit Data Folder*** screen is displayed.

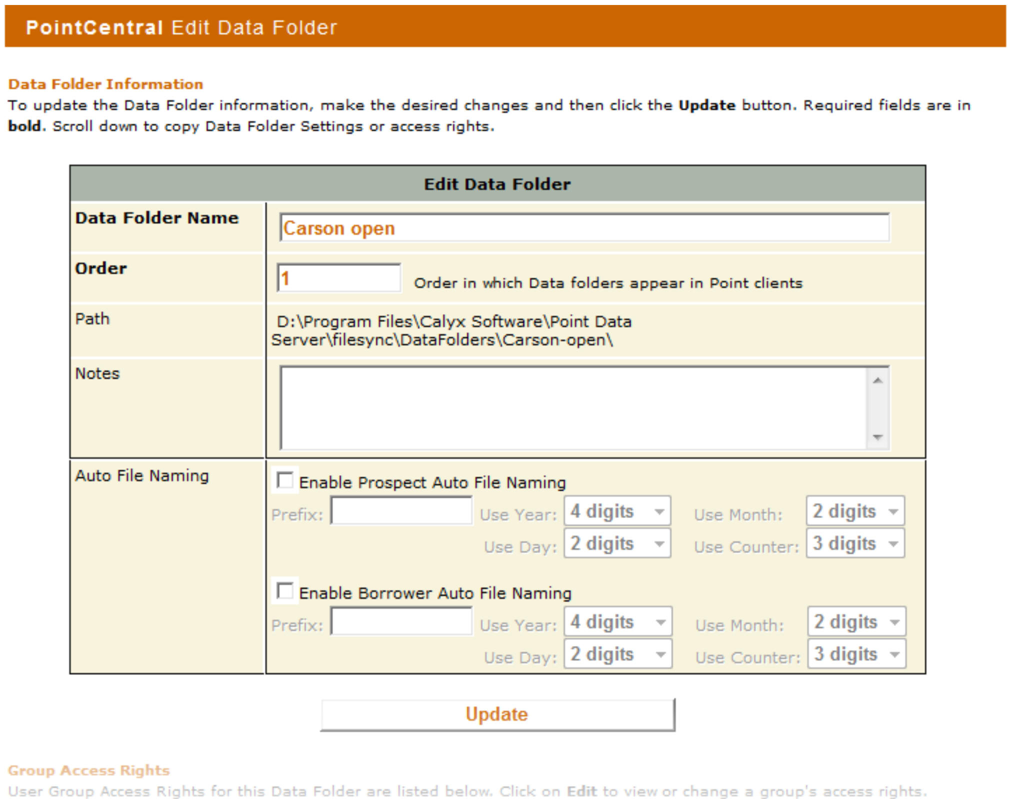


Figure 62. Edit Data Folder screen

3 Scroll down to the *Copy Folder Settings* section.

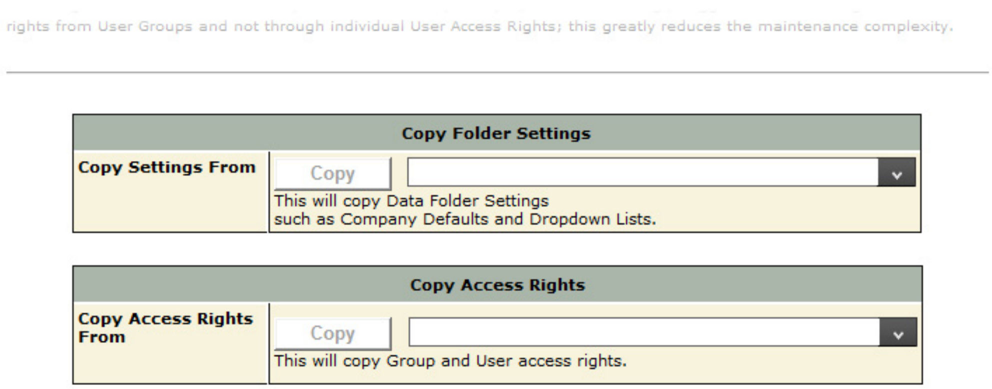


Figure 63. Edit Data Folder screen—Copy Folder Settings and Access Rights

4 To copy folder settings from an existing data folder, select the folder name from the dropdown list and click **Copy**.

5 To copy access rights from an existing data folder, select the folder name from the dropdown list and click **Copy**.

Local data folder access

Point and PointCentral provide a centralized set of data folders and templates that you can access from any computer with an Internet connection.

Local Point control provides administrators with the ability to control Point users connected to PointCentral and to control local Point data folders and save files to unauthorized locations. You can set up local Point control in PointCentral Administration, under the Data Folders menu.This feature helps all users using the system to process all loans in Point. E-mail and export activity is not affected. 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

If users do not have access to local data folders and are unable to connect to PointCentral, Point does not launch and an error message is issued.

Similar to regular access rights, individual user access privileges prevail over access rights granted to user groups.

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

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

Configuring local data folder access

To configure local data folder access:

1 Select ***Data Folders > Edit Local Data Folder Access***.

> **Tip**
>
> *You can also access the* ***Edit Local Data Folder Access*** *screen by clicking the* **Local Data Folder Access** *link which is on the PointCentral home page and the* ***List Data Folders*** *screen.*

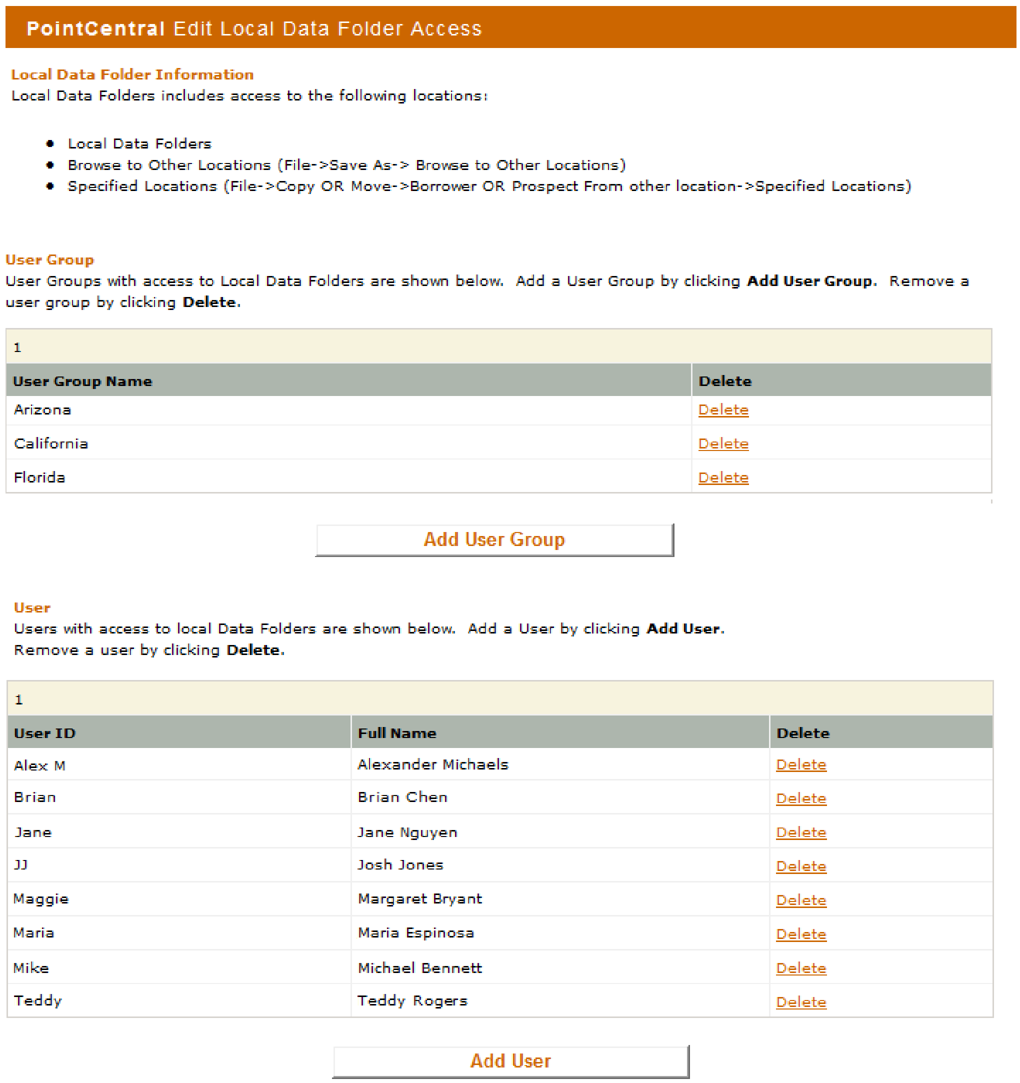


Figure 64. Edit Local Data Folder Access screen

The ***Edit Local Data Folder Access*** screen shows the user groups and users that currently have local data folder access.

2 Specify the user groups to grant local data folder access:

a Click **Add User Group**.

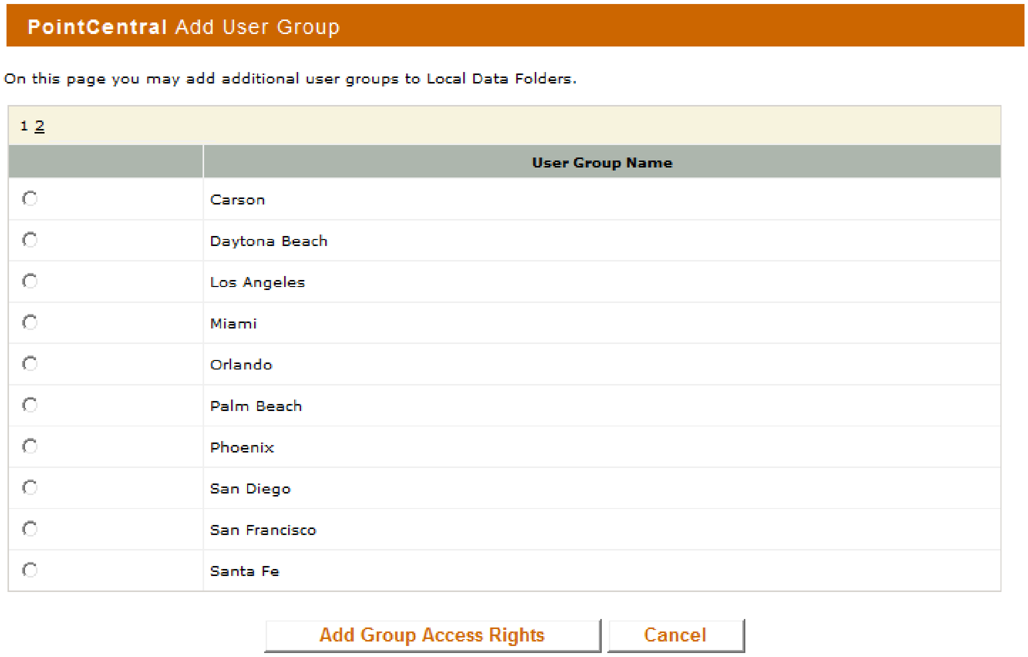


Figure 65. Add User Group screen

b Select the radio button next to the user group to add to the local data folders access list.

c Click **Add Group Access Rights**.

d Repeat the process to add multiple groups.

e Click **Cancel** to return to the ***Edit Local Data Folder Access*** screen.

3 Specify individual users to have local data folder access:

a Click **Add User**.

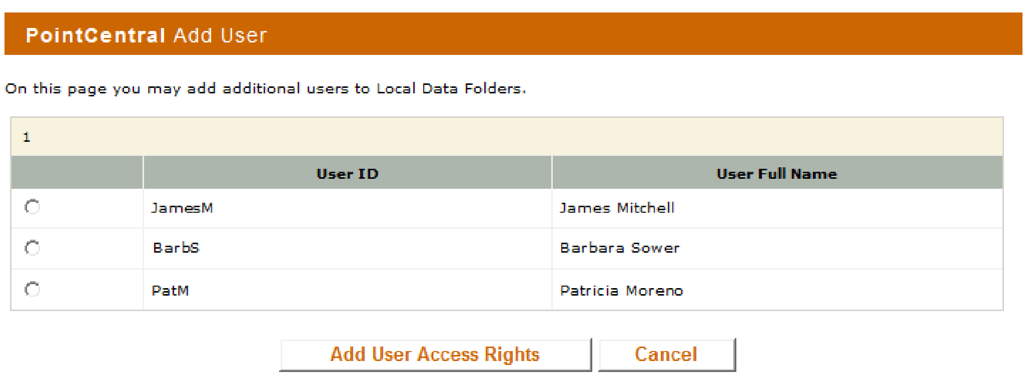


Figure 66. Add User to Local Data Folders screen

b Select the radio button next to the user to add to the local data folders access list.

c Click **Add User Access Rights**.

d Repeat the process to add multiple users.

e Click **Cancel** to return to the ***Edit Local Data Folder Access*** screen.

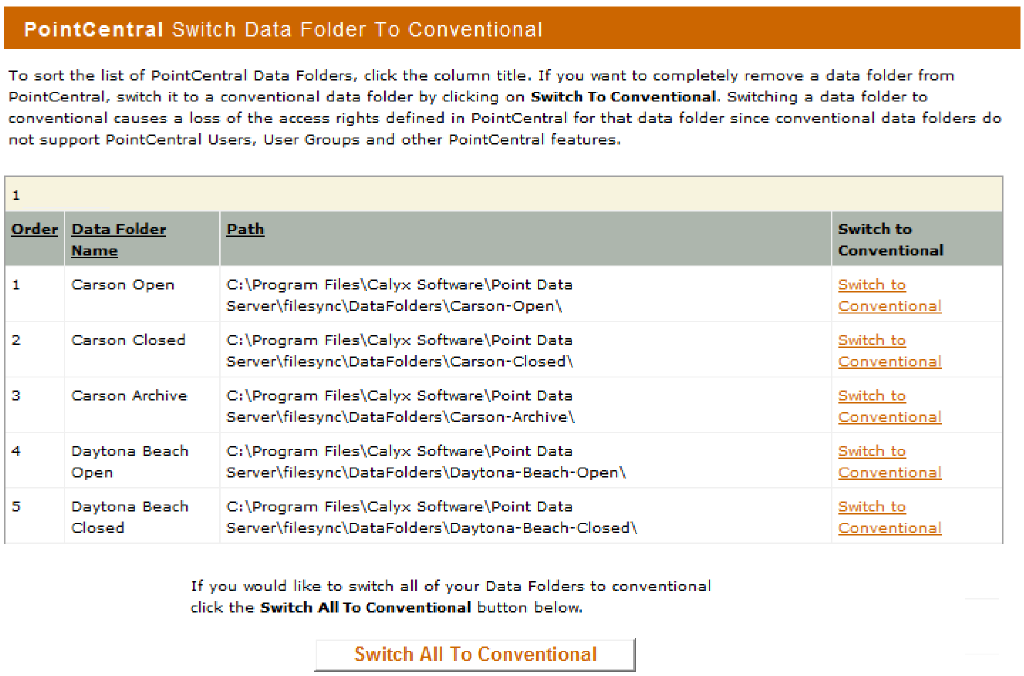
Related information

*For information about the configuration wizard, refer to **Configuring PointCentral**, on page 28.*

Converting PointCentral data folders to conventional

To convert PointCentral folders to conventional:

1 Select ***Configuration > Folder Maintenance > 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 67. Switch Data Folder to Conventional screen

Each folder has a corresponding **Switch to Conventional** link.

Important

When PointCentral data folders exist, you cannot change the root folder path until all the data folders are switched to conventional format and re-imported.

Folder access rights are not preserved when you switch them to conventional format.

2 To convert individual folders, click the link that corresponds to that folder. To convert all folders, click the **Switch All to Conventional** button.

3 Click **Yes** in response to the confirmation prompt.

4 Rebuild the indexes.

Important

You must rebuild the indexes one time for each data folder you switch to conventional mode.

Related information

*For instructions about how to rebuild indexes, refer to the **Point User Guide**.*

Template sets

Conventional Point manages a set of files called templates. They are not loan files. They include not only template files that populate your loan file with often-used information (such as loan programs, closing cost scenarios, prospect and borrower master files, data import and export, escrow and title tables), but also template files that provide additional Point functionality such as reports, custom forms and shared print groups.

Template set distribution (first log in)

In conventional Point you can centralize the location of a set of template files by using a Windows network share. For example, in Point Administrator you can set the folder location to \\\\MYFILESERVER\PNTTEMPL.

Unfortunately, in environments with low bandwidth or high latency, this solution is inadequate. With PointCentral you can centralize your template files and distribute them to Point users automatically, without the need for a VPN. In addition, you can define multiple template sets and grant access rights to specific groups or users accordingly.

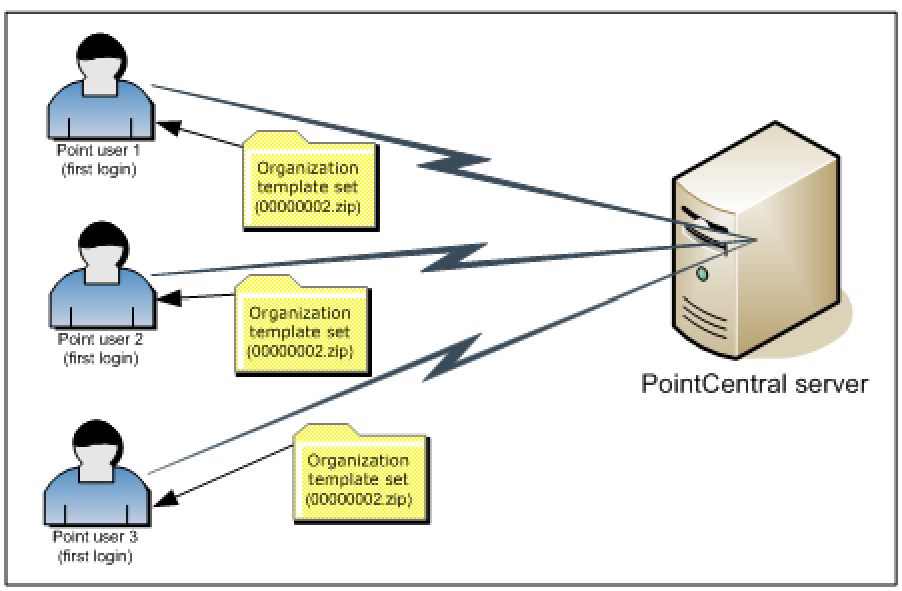


Figure 68. Template set distribution (first log in)

When you use PointCentral, all the template sets are stored under the root template set directory, which is generally located at **C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets**.

Each template set is stored under its own 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 first time a Point user logs in, PointCentral sends a compressed archived file to the Point client containing all the template files in a given template set. Point then extracts the template files locally under the **C:\WINPOINT\User** directory.

The directory in the **C:\WINPOINT\User** folder is named according to the NetBios name and a unique number that identifies the specific template set. All files and folders in this directory match the corresponding files and folders in the template set directory.

Related information

For more information about the root template set directory see ***Administration detail****, on page 44.*

Template file distribution (since last log in)

The next time you log in you do not need to download the full template set again. In most cases, most of the template files have not changed, therefore only files that changed since the Point user last logged in are sent from PointCentral to the Point client.

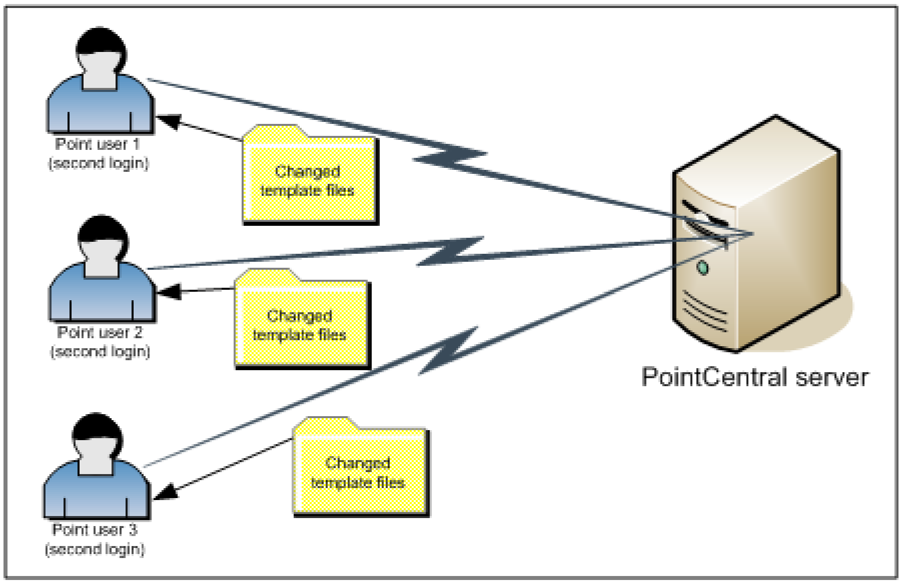


Figure 69. Template set distribution (since last log in)

In addition, Point downloads only files that have changed when those files are needed. A few reports might have been changed by other Point users, but those template files are only downloaded from PointCentral when the Point user accesses the **Reports** tab.

Now that you have a general understanding of how template sets are distributed to Point users, see how you can create and manage such template sets.

Specifying conventional template storage location

The default directory for storing conventional Point templates is **C:\PNTTEMPL** on the client machine, rendering them unavailable to other users on a network. To enable access to template files by authorized users on your network, you can specify a network directory as the default location.

To specify the template storage location:

1. From the Windows desktop, select ***Start > All Programs > Calyx Software > Point Administrator***.
2. Click **Change Template Directory**.

   The **Template Folder Manager** dialog box is displayed.

Figure 70. Point Administrator—Template Folder Manager

3. Enter the new path to store templates, or click **Browse** to navigate to the new location.
4. Click **OK**.

Tip

To view a list of all template types, including their sub-directories, select ***Configuration > Template Set Maintenance > Template Types****.*

Related information

For more details about changing the template file default location, refer to the ***Point User Guide****.*

Adding template sets

To add a template set, you can create a new template set or you can import an existing conventional template set.

To create a new template set:

1 Select ***Template Sets > Add Template Set***:

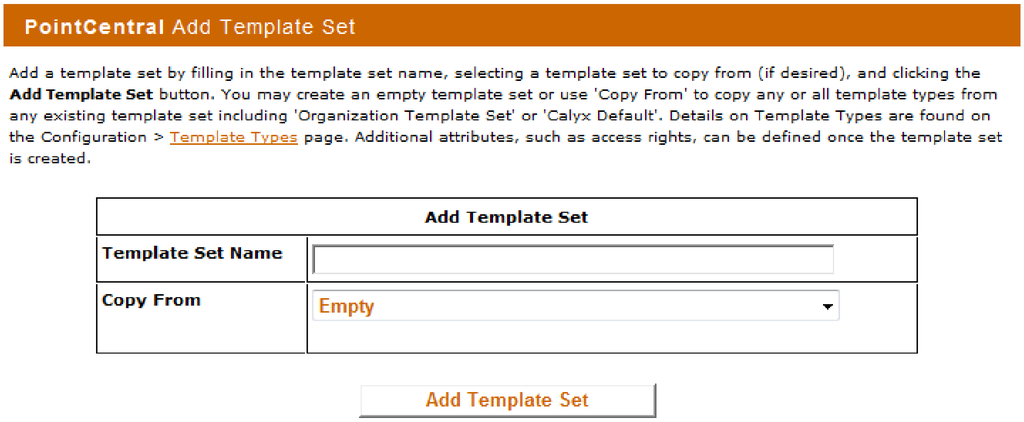


Figure 71. Add Template Set screen

2 Enter a template set name in the *Template Set Name* field.

3 Select an option from the ***Copy From*** dropdown list.

The following options are available for the source template set on a new system:

Empty

Creates an empty template set that does not contain any template files.

Calyx Default

Creates a template set from the Calyx default template set, which is included with the PointCentral installation. The template set includes reports, escrow and title tables, and some custom forms.

> ***Note***
>
> *The Calyx Default template is read-only, you cannot edit and change these template files.*

Organization

The Organization template set is created when PointCentral is installed. It contains the same files that are deployed in the Calyx Default template set, but you can edit the Organization template set. If you do not want to define multiple template sets for your organization, you do not need to create a new template set. You can start using the Organization template set right away.

> ***Attention***
>
> *On an existing system you can copy template files from an existing template set when you create a new template set.*
>
> *To copy files from an existing template set, select the template set name from the **Copy From** dropdown list.*

4 Click **Add Template Set**.

A message is displayed that indicates the template set will be created and to check the status page for more details.

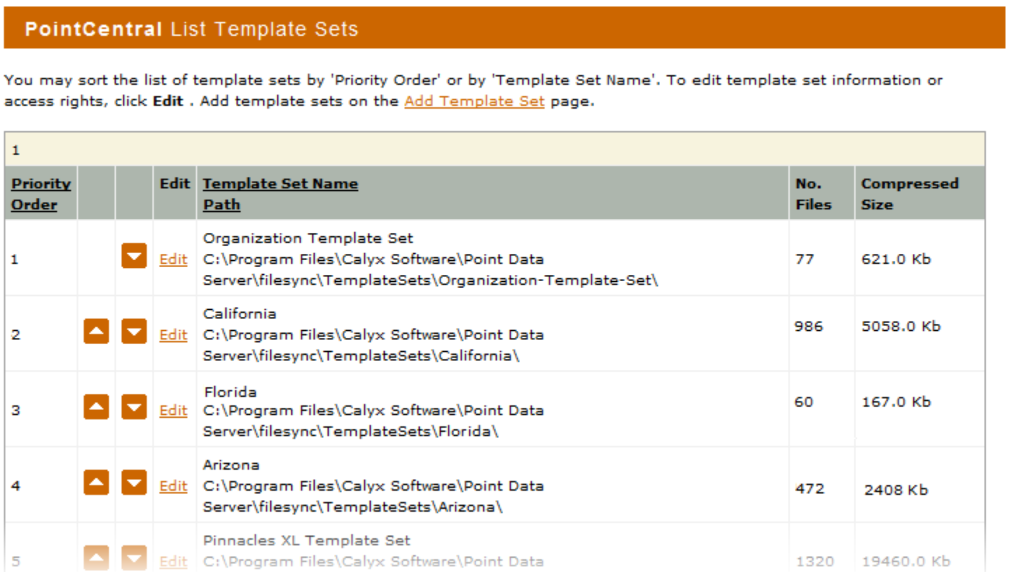
Specifying user and user group template set access rights

The process to set access rights to templates for user groups and users is the same. The steps to specify user group access rights to templates are used in this example.

To specify the template set access rights:

1 Click ***Template Sets > List Template Sets***.

The ***List Template Sets*** screen is displayed.



PointCentral List Template Sets

You may sort the list of template sets by 'Priority Order' or by 'Template Set Name'. To edit template set information or access rights, click **Edit** . Add template sets on the Add Template Set page.

1

Priority Order			Edit	Template Set Name Path	No. Files	Compressed Size
1			Edit	Organization Template Set C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Organization-Template-Set\	77	621.0 Kb
2			Edit	California C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\California\	986	5058.0 Kb
3			Edit	Florida C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Florida\	60	167.0 Kb
4			Edit	Arizona C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Arizona\	472	2408 Kb
5			Edit	Pinnacles XL Template Set C:\Program Files\Calyx Software\Point Data	1320	19460.0 Kb

Figure 72. List Template Sets screen

2 Click the **Edit** link to change the template set attributes and assign access rights.

The ***Edit Template Set*** screen is displayed.

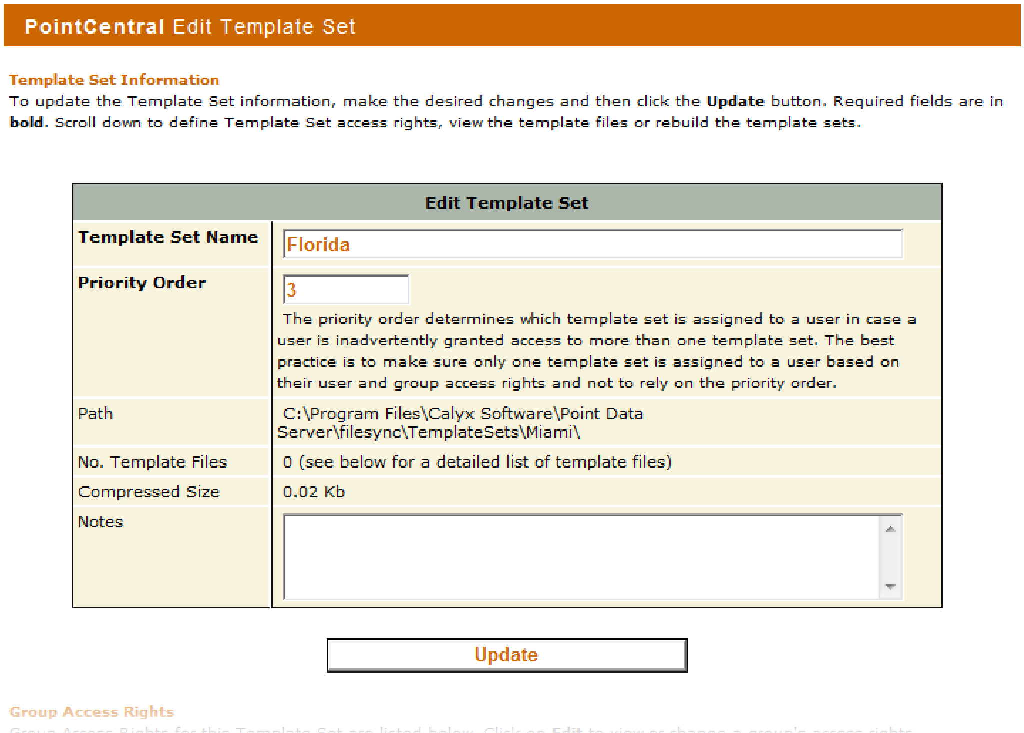


Figure 73. Edit Template Set screen

In addition to adding and updating user and user group access rights, you can edit the template set name, priority order, and enter notes about the template set in this screen.

3 To change the template set name, priority order, and notes, enter new values and click ***Update***.

> **Note**
>
> *Although you can assign multiple template sets to one Point user (through group and user access rights), the system will only use one template set, called the effective template set. In such a case, the template set with the highest priority order will be the effective template set assigned to the Point user.*
>
> *To simplify the management of template set access rights, you should assign only one template set to a user and not rely on the priority order to determine which template set is used.*

4 Scroll down to the *Group Access Rights* section.

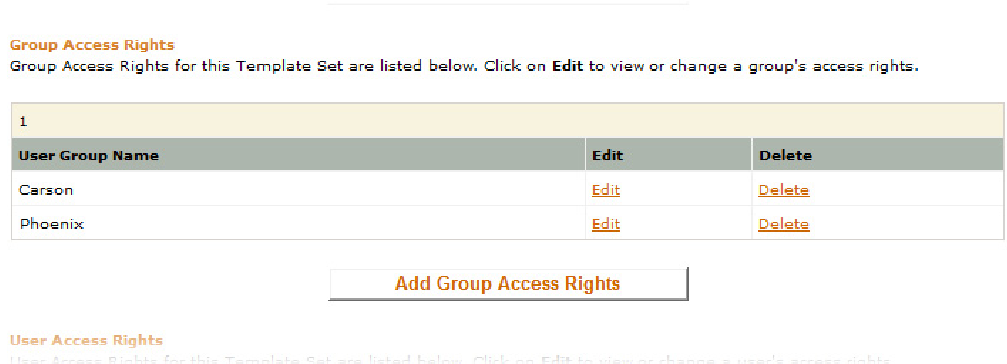


Figure 74. Edit Template Set screen—Add Group Access Rights

User groups with current access rights to the template set are displayed, if any. Use the **Edit** or **Delete** link to edit or delete an existing group.

5 Click **Add Group Access Rights**.

> **Tip**
>
> *To specify user access rights, scroll to the* User Access Rights *section and click* **Add User Access Rights***, however, managing access rights through groups is more efficient.*

The ***Add User Group Access Rights*** screen is displayed.

Figure 75. Add User Group Access Rights screen

Use this screen to establish access rights for the selected template set.

6 Select a user group.

7 Scroll to the *Template Set Access Rights* section and select the template sets that the selected user group can access.

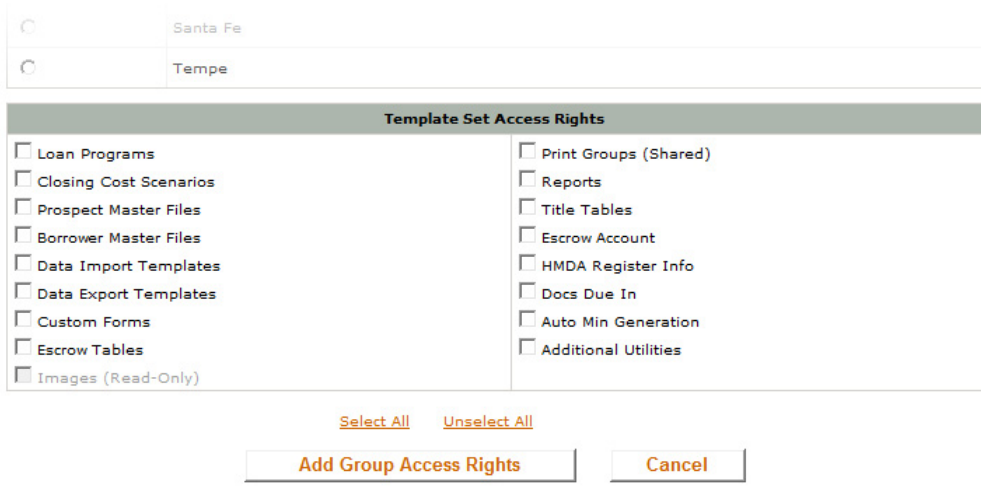


Figure 76. Add User Group Access Rights—Template Set Access Rights

8 Select the template sets that the selected group is allowed to access.

When you select a specific template type, you are granting read and write access rights for that template type. The group (or user) does not have access rights for any template sets that are unchecked.

Important

- *When* **Loan Programs**, **Closing Cost Scenarios**, **Prospect Master Files**, **Borrower Master Files**, **Data Import Templates**, **Data Export Templates**, **Custom Forms**, *or* **Reports** *are selected, the buttons that enable the user to use or view these functions is enabled. Unselected options are disabled in Point.*
- *When* **Escrow Tables**, **Title Tables**, **Escrow Account**, **HMDA Register Info**, **Docs Due In**, *or* **FHA Consumer Choice Disclosures** *are selected, the option is enabled in the* ***Utilities Company Defaults*** *menu. Unselected options are disabled in Point.*
- *When* **Print Groups (Shared)** *is selected, the* **Edit Group** *and* **Delete Group** *buttons are enabled in the* **Prospect**, **Borrower**, **Co-Prospect**, *and* **Co-Borrower Forms** *dialog boxes when the user selects a shared print group.*

  If this option is not selected, the user can create a new print group, however, the **Edit Group** *and* **Delete Group** *buttons and the* **Share this print group** *check box are disabled.*
- *When* **Additional Utilities** *is selected, the following options in the Point* ***Utilities*** *menu are enabled. If it is not selected, these functions are disabled.*
  - *Custom Screen Settings*
  - *FHA Consumer Choice Disclosure*
  - *Condition Types*
  - *Fee Types*
  - *Impound Types*
  - *Trailing Documents*
  - *Warehouse Lenders*
  - *Investors*

Use **Select All** and **Unselect All** to select or clear all options.

9 Click **Add User Group Access Rights**.

10 Specify template set access rights for additional groups as needed.

11 When you are finished specifying template set access rights, click **Cancel** to return to the ***Edit Template Set*** screen.

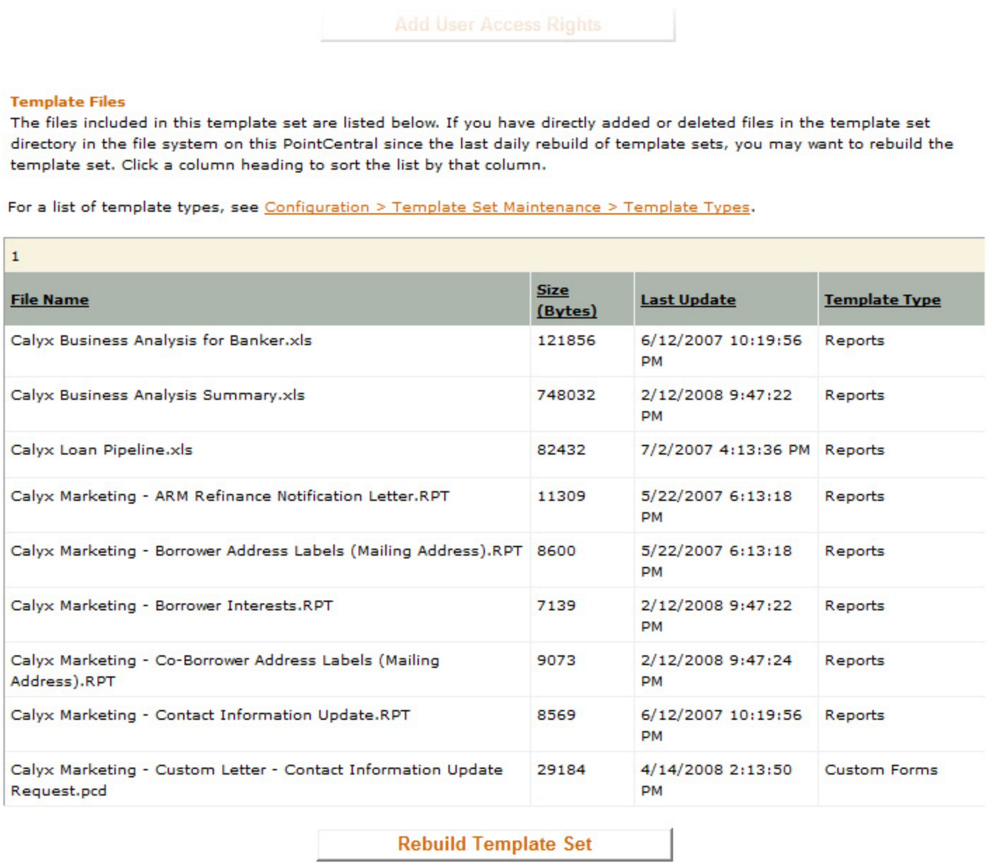
Related information

For information about importing a conventional template set, refer to ***Importing template sets****, on page 137.*

Rebuilding template sets

The ***Edit Template Set*** page contains a list of template types that are contained in the selected template set.

A list of all the template files that are in included in the given template set are displayed at the bottom of the ***Edit Template Set*** page.



Add User Access Rights

Template Files

The files included in this template set are listed below. If you have directly added or deleted files in the template set directory in the file system on this PointCentral since the last daily rebuild of template sets, you may want to rebuild the template set. Click a column heading to sort the list by that column.

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

1

File Name	Size (Bytes)	Last Update	Template Type
Calyx Business Analysis for Banker.xls	121856	6/12/2007 10:19:56 PM	Reports
Calyx Business Analysis Summary.xls	748032	2/12/2008 9:47:22 PM	Reports
Calyx Loan Pipeline.xls	82432	7/2/2007 4:13:36 PM	Reports
Calyx Marketing - ARM Refinance Notification Letter.RPT	11309	5/22/2007 6:13:18 PM	Reports
Calyx Marketing - Borrower Address Labels (Mailing Address).RPT	8600	5/22/2007 6:13:18 PM	Reports
Calyx Marketing - Borrower Interests.RPT	7139	2/12/2008 9:47:22 PM	Reports
Calyx Marketing - Co-Borrower Address Labels (Mailing Address).RPT	9073	2/12/2008 9:47:24 PM	Reports
Calyx Marketing - Contact Information Update.RPT	8569	6/12/2007 10:19:56 PM	Reports
Calyx Marketing - Custom Letter - Contact Information Update Request.pcd	29184	4/14/2008 2:13:50 PM	Custom Forms

Rebuild Template Set

Figure 77. Edit Template Set screen—Rebuild Template Set list

You can sort the list by:

- File name
- Size (in bytes)
- Last update date and time
- Template type

Sorting by size is useful when a specific template set is too big and is causing performance issues for Point users. If you manually copy template files to the template set directory, PointCentral is not aware of the newly copied files until you rebuild the template set. Rebuilding the template set ensures that the compressed archived file that is delivered to first-time-log in Point users includes all template files and that other Point users receive these files.

PointCentral also supports the automatic rebuild of template sets once a day.

After upgrading to PointCentral, the new template data is not available until the organization template set is rebuilt. To access the templates immediately, you can rebuild the template set manually.

To rebuild the organization template set manually:

1 Click ***Template Sets > List Template Sets***.

The organization template set is usually the first one on the list.

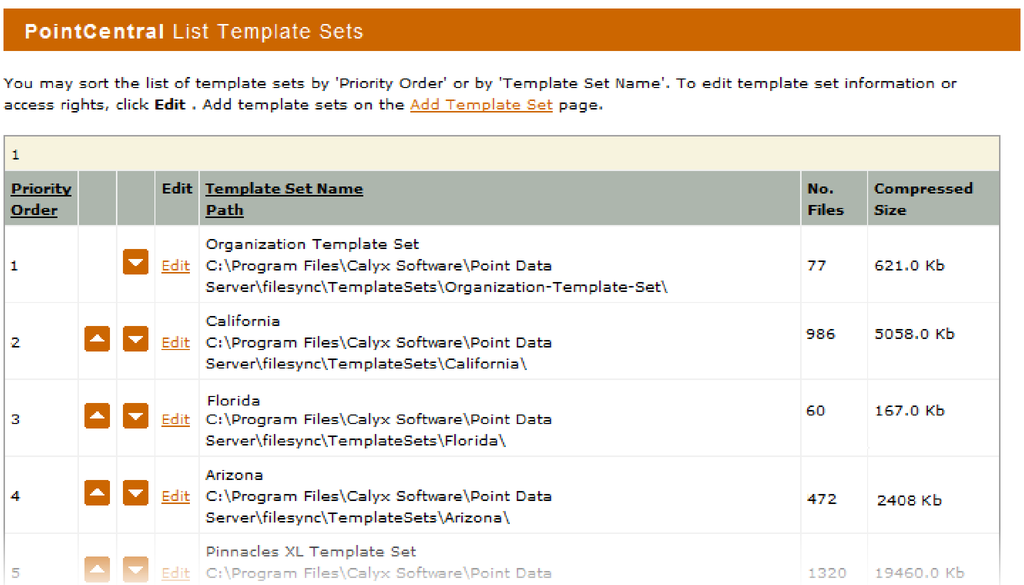


Figure 78. List Template Sets screen

2 Locate the organization template set (which is located at **C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Organization-Template-Set**), and click the corresponding **Edit** link.

3 Scroll to the bottom of the screen to view the template files.

Add User Access Rights

Template Files

The files included in this template set are listed below. If you have directly added or deleted files in the template set directory in the file system on this PointCentral since the last daily rebuild of template sets, you may want to rebuild the template set. Click a column heading to sort the list by that column.

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

1

File Name	Size (Bytes)	Last Update	Template Type
Calyx Business Analysis for Banker.xls	121856	6/12/2007 10:19:56 PM	Reports
Calyx Business Analysis Summary.xls	748032	2/12/2008 9:47:22 PM	Reports
Calyx Loan Pipeline.xls	82432	7/2/2007 4:13:36 PM	Reports
Calyx Marketing - ARM Refinance Notification Letter.RPT	11309	5/22/2007 6:13:18 PM	Reports
Calyx Marketing - Borrower Address Labels (Mailing Address).RPT	8600	5/22/2007 6:13:18 PM	Reports
Calyx Marketing - Borrower Interests.RPT	7139	2/12/2008 9:47:22 PM	Reports
Calyx Marketing - Co-Borrower Address Labels (Mailing Address).RPT	9073	2/12/2008 9:47:24 PM	Reports
Calyx Marketing - Contact Information Update.RPT	8569	6/12/2007 10:19:56 PM	Reports
Calyx Marketing - Custom Letter - Contact Information Update Request.pcd	29184	4/14/2008 2:13:50 PM	Custom Forms

Rebuild Template Set

Figure 79. Rebuild Template Sets (manually) screen

4 Click the **Rebuild Template Set** button.

5 Click **Yes** in response to the confirmation prompt.

6 To view the rebuild status, select the Status option from the menu.

After the status page indicates that the rebuild is complete, the new templates are available for use.

Related information

*See **Administration detail**, on page 44, for more information about the daily rebuild of template set archives.*

Copying template sets

To copy template sets:

1 Select ***Configuration > Template Set Maintenance > Copy Template Set***.

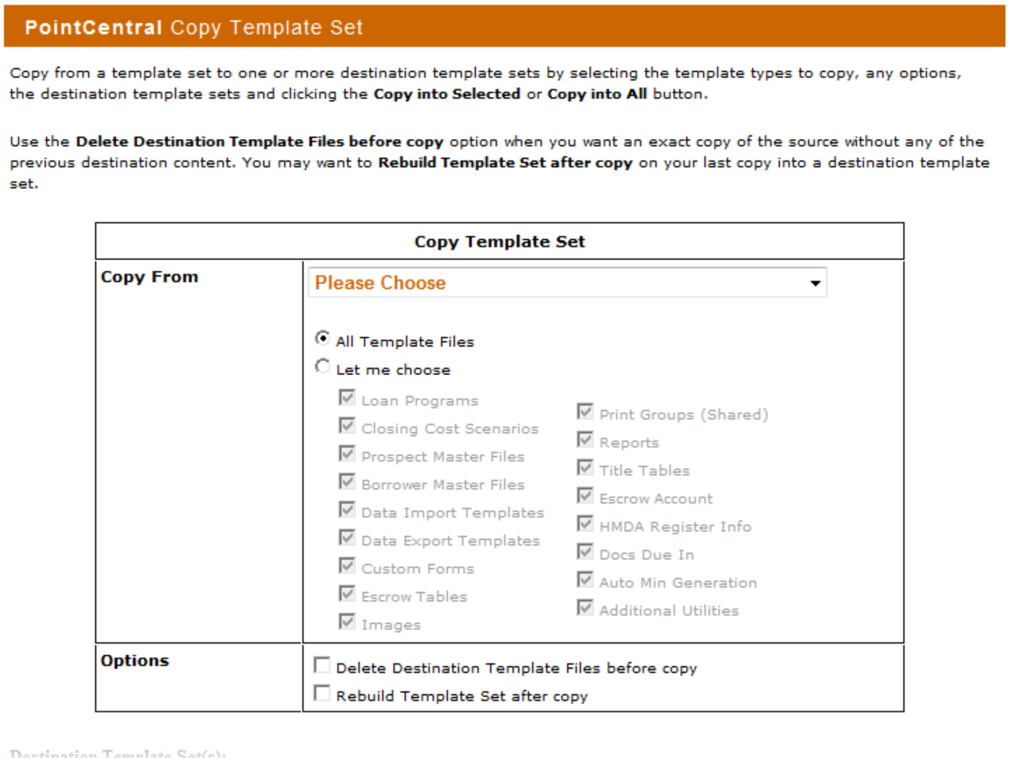


Figure 80. Copy Template Set screen

2 Select the source template set from the ***Copy From*** dropdown list

3 To copy all template files from the specified template set, select **All Template Files**, otherwise select **Let me choose**.

If you select **Let Me choose**, the check boxes next to the template names become enabled.

Individually select the template files to include in the copy process.

4 Select **Delete Destination Template Files before copy** to remove any existing files from the destination template set.

Deleting the existing files synchronizes the two template sets.

5 Select **Rebuild Template Set after copy** to rebuild the template set after the template files are copied.

6 Scroll down to view the template sets.

1		
Template Set Name	**Path**	☐
Arizona	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Arizona\	☐
California	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\California\	☐
Florida	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Miami\	☐
Organization Template Set	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Organization-Template-Set\	☐

Copy into Selected

Copy into All

Figure 81. Copy Template Set screen—Copy into Selected

7 Select one or more destination template sets and click **Copy into Selected**.

Click the **Status** link to view the status of the copy process.

Converting template sets to conventional

To convert template sets to conventional:

1 Select ***Configuration > Template Set Maintenance > Switch To Conventional*** to access the ***Switch Template Set To Conventional*** screen.

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\Calyx Software\Point Data Server\filesync\TemplateSets\Organization-Template-Set\	Switch to Conventional
2	Arizona	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Arizona\	Switch to Conventional
3	California	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\California\	Switch to Conventional
4	Florida	C:\Program Files\Calyx Software\Point Data Server\filesync\TemplateSets\Miami\	Switch to Conventional

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

Switch All To Conventional

Figure 82. Switch Template Set to Conventional screen

Each template set has a corresponding **Switch to Conventional** link.

2 To convert individual template sets, click the link that corresponds to that template set. To convert all template set, click the **Switch All to Conventional** button.

3 Click **Yes** in response to the confirmation prompt.

Cardex databases

The Cardex database for Point is an electronic database that contains information about companies you 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 into Point fields, or by entering the information manually.

Centralizing Cardex databases

In conventional Point you can centralize the location of Cardex within the template directory by using a Windows Network Share.

For example, in Point Administrator it is possible to change the folder location to **\\MYFILESERVER\PNTTEMPL**. Unfortunately, in environments with low bandwidth or high latency, this option is unreliable. With PointCentral you can centralize your Cardex database and make it available to Point users automatically, without a need for a VPN. In addition, you can define multiple Cardex databases and give access rights to different groups or users accordingly.

Cardex databases are stored in the PointCentral database which allows all Point clients to access Cardex entries from a central location quickly, even from large Cardex databases. The user-defined Cardex categories are stored with the templates.

Point users will notice they have access rights to a Cardex database by the [PDS] suffix in the Cardex database dialog box title. Point users that do not have access rights to a Cardex database default to the conventional Cardex in the Point Template Directory.

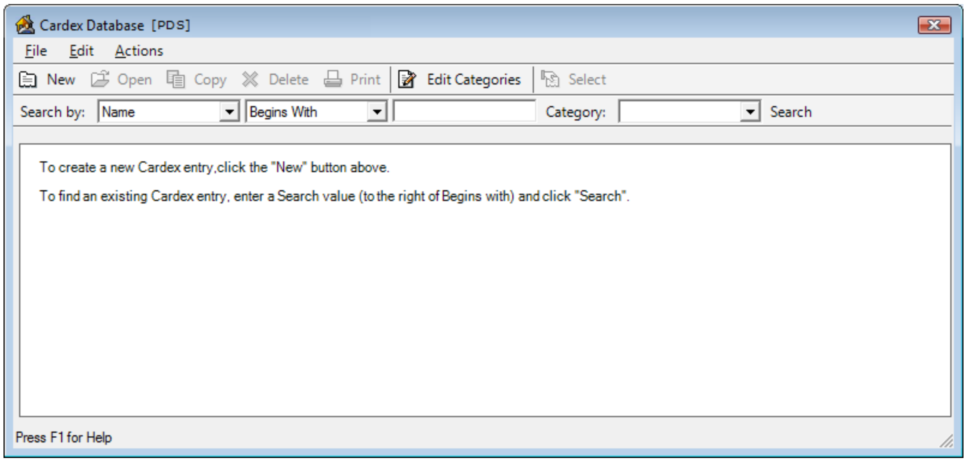


Figure 83. Point Cardex Database (PDS) dialog box

Conventional Cardex database storage

The default directory for storing the Cardex database in conventional Point is in the template directory on the client machine, **C:\PNTTEMPL**, rendering it unavailable to other users on a network. To enable authorized users on your network to access the Cardex databases, you can specify a network directory as the default location for storing templates.

Related information

*Refer to **Specifying conventional template storage location**, on page 98, for instructions about how to change the directory location.*

Adding Cardex databases

To add a Cardex database, you can create a new Cardex database or you can import an existing conventional Cardex database.

To create a new Cardex database in the administration site:

1. Select ***Cardex Databases > Add Cardex Database***.

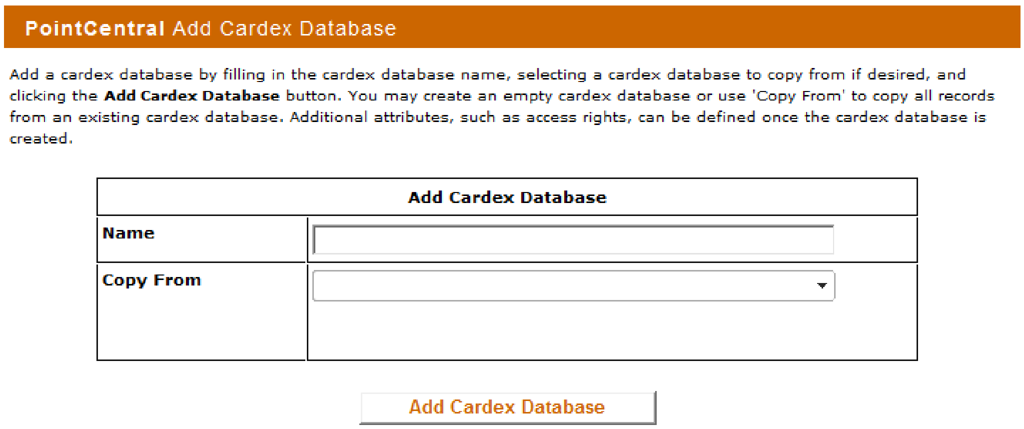


Figure 84. Add Cardex Database screen

2. Enter a name for the new Cardex database in the *Name* field.
3. To copy data from an existing database into the new database, select the database name from the ***Copy From*** dropdown list.
4. Click **Add Cardex Database**.

Related information

For information about importing a conventional Cardex database, see ***Importing resources****, on page 134.*

Specifying user group and user access rights

The process to set access rights to Cardex databases for user groups and users is the same. The steps to specify user group access rights to Cardex databases are used in this example.

To edit a Cardex database:

1 Select ***Cardex Databases > List Cardex Databases***.

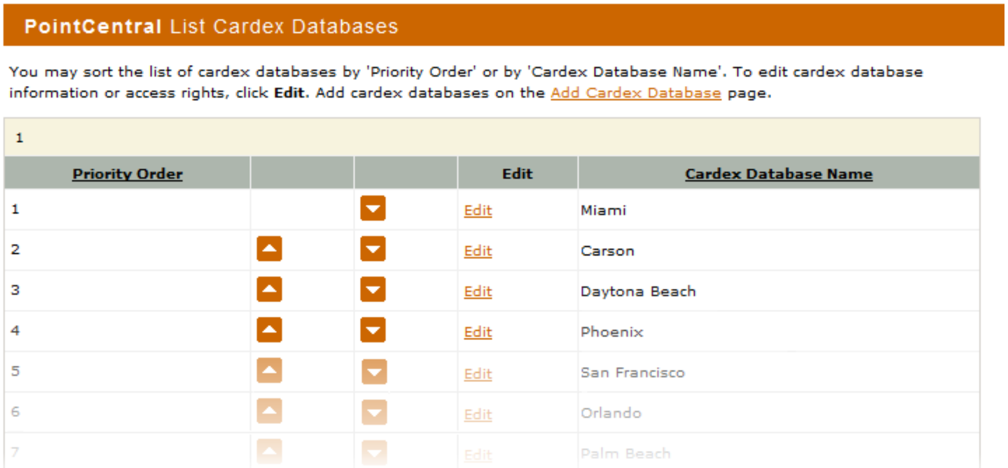


Figure 85. List Cardex Databases screen

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

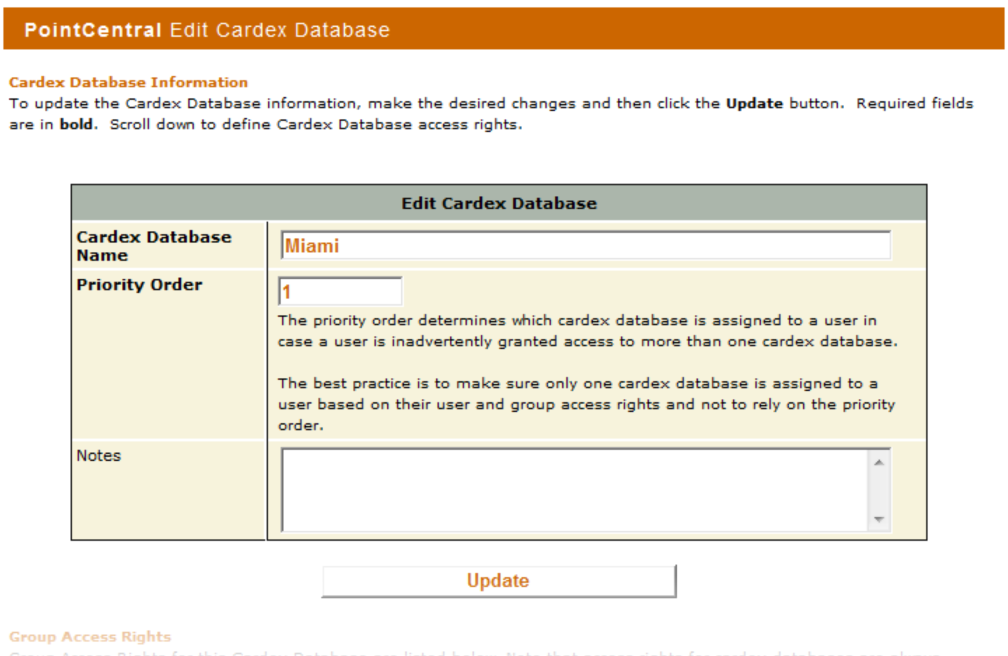


Figure 86. Edit Cardex Database screen

3 To change the Cardex database name, priority order, and notes, enter new values and click ***Update***.

Recommendation

Although you can assign multiple Cardex databases to one Point user (through group and user access rights), the system will use only one, called the effective Cardex database. In such a case, the Cardex database with the highest priority order is the effective Cardex database assigned to the Point user.

To simplify the management of Cardex database access rights, you should assign only one Cardex database to a user and not rely on the priority order to determine which one is used.

4 Scroll down to the *Group Access Rights* section.

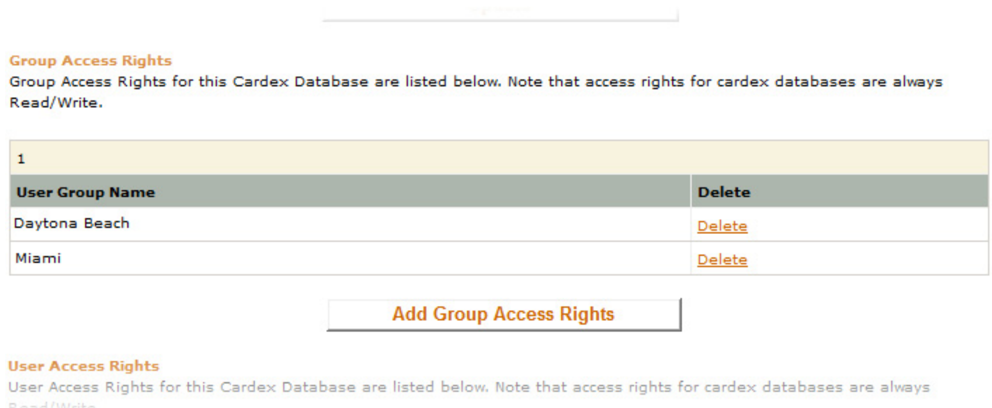


Figure 87. Edit Cardex Database screen—Add Group Access Rights

User groups with access rights to the database are displayed, if any.

Tip

To specify user access rights, scroll to the User Access Rights *section and click* **Add User Access Rights***, however, managing access rights through groups is more efficient.*

5 Click **Add Group Access Rights**.

The ***Add Group Access Rights*** screen is displayed.

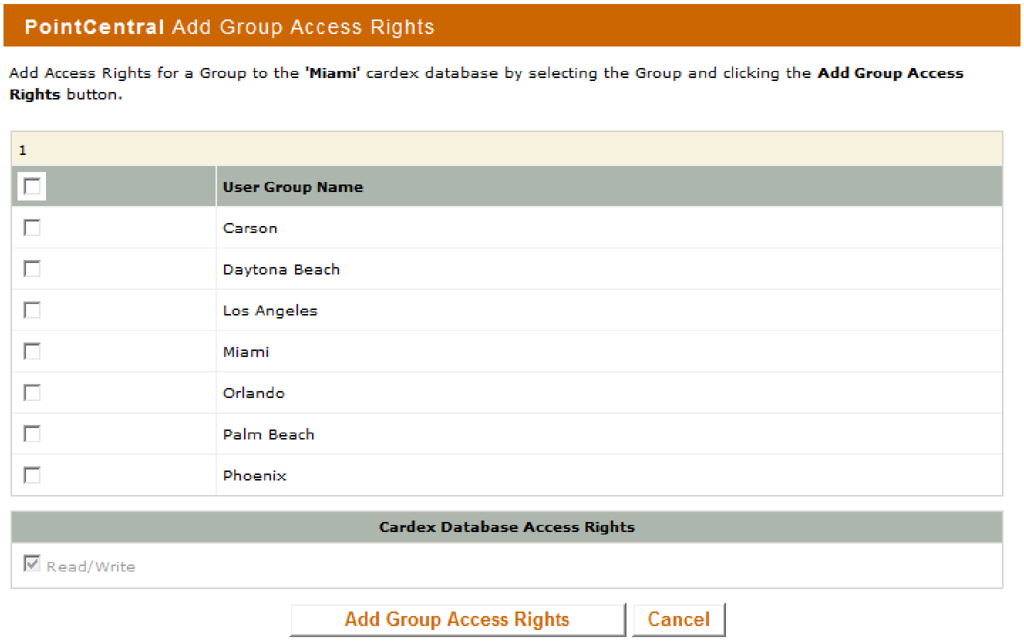


Figure 88. Add Group Access Rights—Cardex Database screen

6 Select the groups that are allowed to access the Cardex database and click **Add Group Access Rights**.

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

Deleting Cardex databases

To delete a Cardex database:

1 Select ***Configuration > Delete Cardex Database***.

The ***Delete Cardex Database*** screen is displayed.

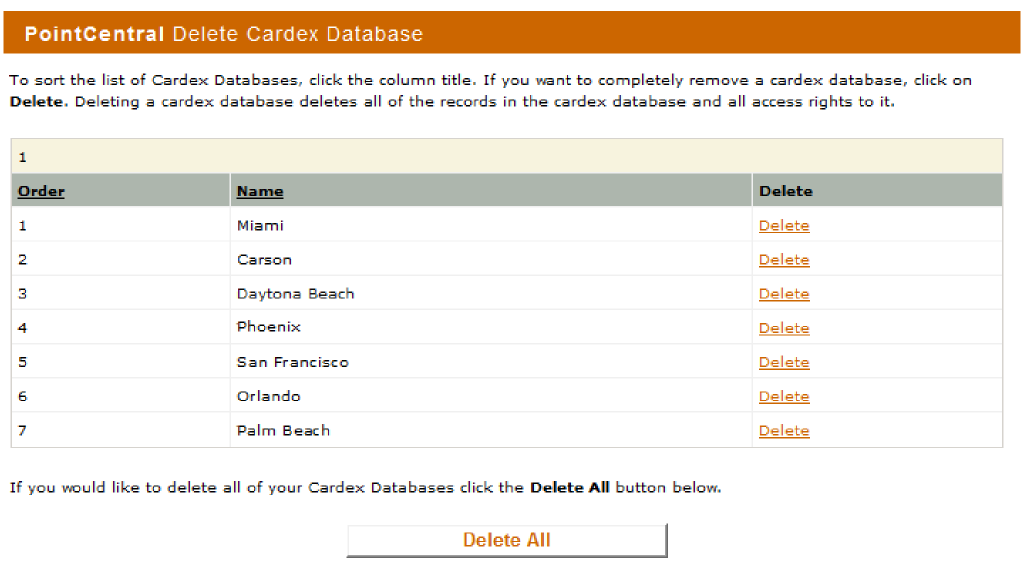


Figure 89. Delete Cardex Database screen

2 Click the **Delete** link that corresponds to the Cardex database you want to delete.

To delete all of the databases, click **Delete All**.

3 Click **Yes** to confirm the deletion.

A confirmation message is displayed.

Converting Cardex databases to conventional Point

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, then importing it back into conventional Point.

To convert the Cardex databases to conventional Point:

1 Log in to Point as a user with access rights to the Cardex database you want to export.

2 Export the PointCentral databases that you want to convert to conventional Point.

Attention

To export multiple databases with different access rights, you must export them individually. Log out of Point and log back in with user credentials that can access each database.

If additional databases exist with different access rights, log out of Point and log back in with user credentials that have access to those databases.

a Select ***Utilities > Cardex Database***.

The **Cardex Database** dialog box is displayed.

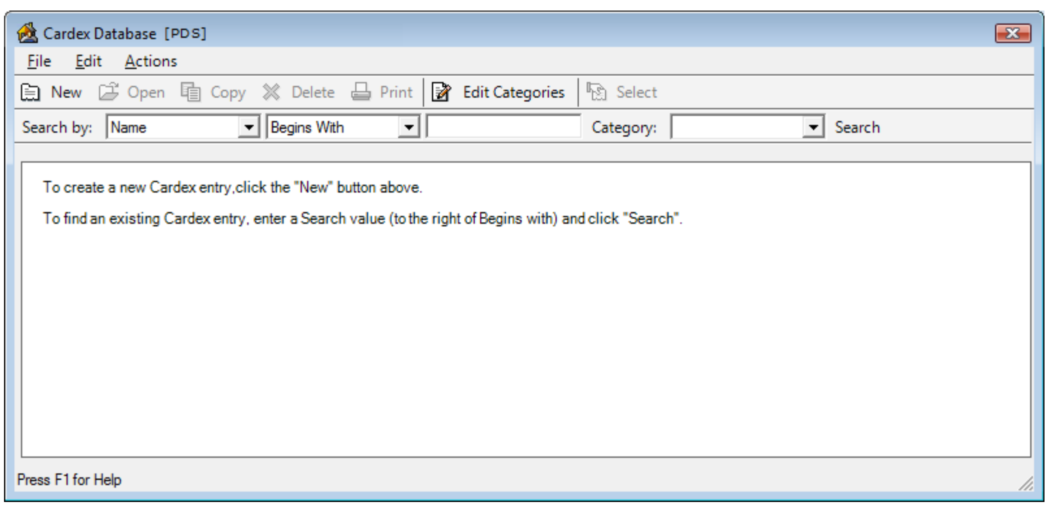


Figure 90. Cardex database dialog box, in Point

b Select ***File > Export***.

The **Export Custom ASCII** dialog box is displayed.

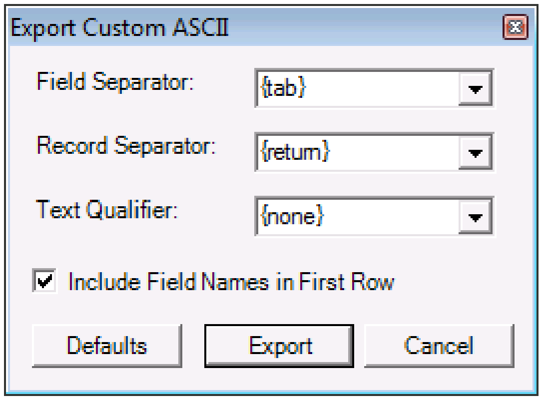


Figure 91. Cardex database Export Custom ASCII dialog box, in Point

c Click **Export**.

The **Export Cardex** dialog box is displayed.

d Select a location to save the file and enter a file name.

3 Log out of PointCentral.

4 Log in to conventional Point.

a Select ***Utilities > Cardex Database***.

The **Cardex Database** dialog box is displayed.

b Select ***File > Import***.

Attention

*The **File > Import** function is not available when Point is configured to use PointCentral.*

Related information

*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. In addition, 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 they log in to Point or their mobile device. Rules are applied to users and user groups in PointCentral much like users and user groups are given access to data folders.

Conditions are used to further define the rule and the circumstances under which it is applied by specifying fields and the values that must be present.

For example, to prevent users from changing certain field values in a loan file after the loan is locked, you would 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.

The rule would define the fields that the user cannot edit and the condition would define 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 that are defined.

PointCentral is supplied with a set of default rules.

Prerequisite

Microsoft Silverlight is required to edit rules in Point Version 9.4 and earlier. If Silverlight is not currently installed, a link to download the application is provided on the Rules page. If a link is not present, Silverlight was detected.

Adding rules

This topic provides basic instructions for creating rules. Subsequent topics provide additional information about how to create each rule type.

To add a new rule:

1 Select ***Rules > Add Rule***.

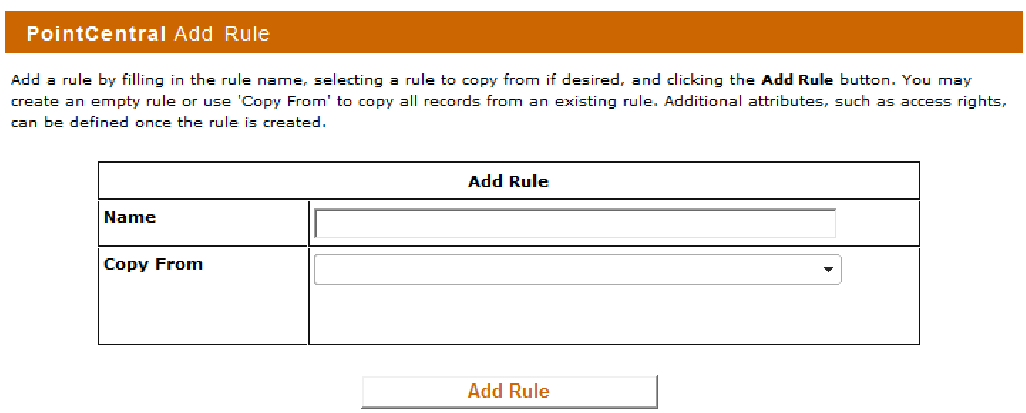


Figure 92. Add Rule screen

2 Enter a unique rule name.

3 To copy the parameters from an existing rule, select a rule from the ***Copy From*** dropdown list.

4 Click **Add Rule**.

The new rule is added and the ***Edit Rule*** screen is displayed.

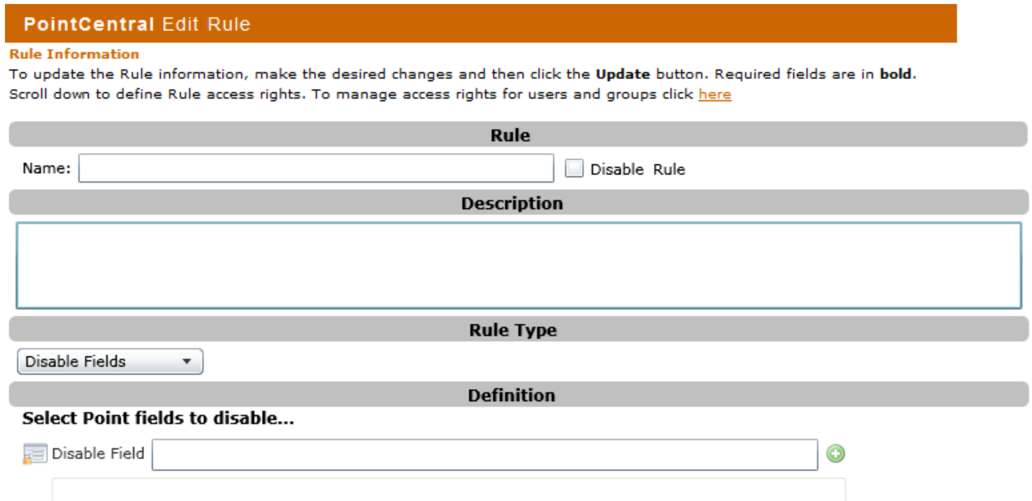


Figure 93. Edit Rule screen

5 To prevent the rule from being applied, select the **Disable Rule** check box.

6 Select the ***Rule Type*** from the dropdown list.

The following rule types are available:

Disable Fields

Use this option to make specific fields unavailable for users or user groups. 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. If data is missing in a required field when the user attempts to save a loan file, a dialog box is displayed that informs them of the fields that require input.

Custom Message

Used to define a rule that contains a custom message. Depending on the rule configuration, you can specify if the Point user can complete the task or if they must stop and satisfy the rule conditions before they can proceed.

State Licenses

Used to define a rule that is based on the state where the Point user is licensed to originate loans. 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.

7 Complete the *Definition* section.

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

Disable Fields

Select the fields that are to be disabled (read-only) when certain conditions are met for a Disable Fields rule.

Required Fields

Select the fields that must contain data for a Required Fields rules. When the conditions that are specified for the rule are met and any of the specified fields are empty, the rule is triggered.

Custom Message

Enter a message specific to your business rules for a Custom Message rule.

State Licenses

Select the states where your organization holds licenses to prevent loan origination in unlicensed states for the State Licenses rule.

8 Select an option from the dropdown list to specify whether the rule runs only for borrower files or for both borrower and prospect files.

When multiple conditions are added, a dropdown list is included that is used to specify whether all conditions must be present to apply the rule or to apply the rule when at least one condition is present.

9 Complete the *Conditions* section.

a Click **Add a Condition**.

The *Conditions* section is expanded.

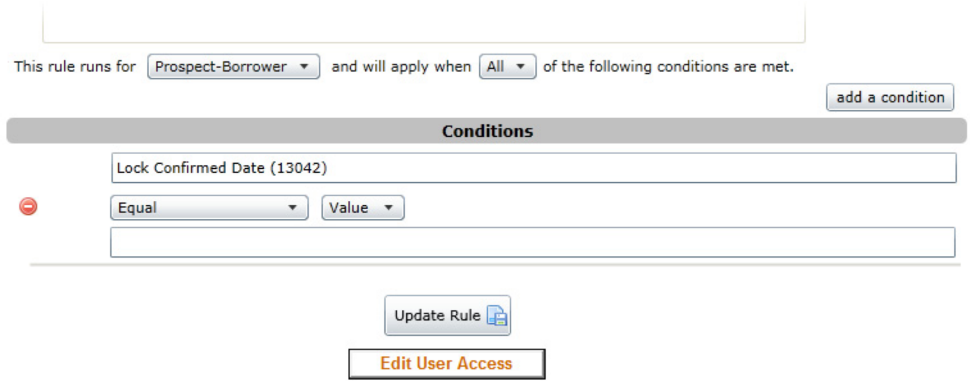


Figure 94. Edit Rule screen—Add Condition example

b Begin to enter the field name or ID in the first field or select a field from the dropdown list. A list of fields pops up on the screen and is filtered as you type. When the field you want is visible, select it to populate the field.

c Select a condition from the second dropdown list.

The values that are available on this list depend on the type of field that you select. The rule is triggered when the event in this field occurs and meets the criteria specified in the condition.

Note

Many of the rules contain multiple conditions that must be met before the rule is triggered.

Note

If you selected Pending Request, the values in this dropdown list change to types of requests. Select the condition that must be met for a pending request from the dropdown list.

The following table defines the options:

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.
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.
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.
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.

d Select either *Field* or *Value* to indicate whether a field or value will trigger the rule.

e Enter the value or field that the condition requires to be applied in the next field.

f Click **Add a Condition** to add another condition.

If you enter more than one condition, a dropdown list is displayed that is used to specify if the rule applies when all conditions are met or when at least one condition is met.

g Select the option (*All* or *One*) that applies to your rule.

10 When you are finished adding conditions, click **Update Rule**.

Creating a Disable Fields rule

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

> **Restriction**
>
> *Due to technical limitations, disabled fields that are located in dialog boxes are exempt from the rule and are enabled to the user. In addition, disabled fields are overwritten when data is imported into the loan file.*

To create a new Disable Fields rule:

1. Create a new rule.

   After the new rule is created, the ***Edit Rule*** screen is displayed.

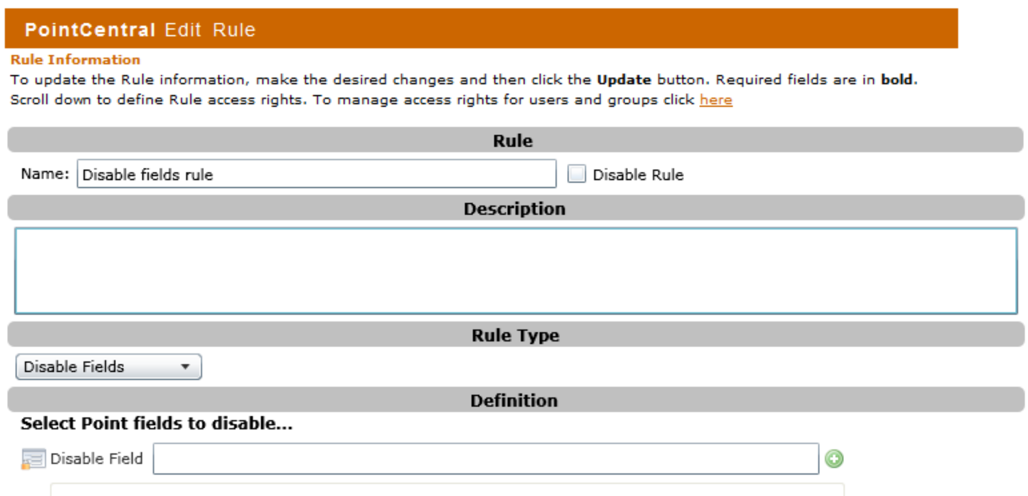


Figure 95. Edit Rule screen—Disable Fields

   Disable Fields is the default rule type selection.

2. To prevent the rule from being applied, select the **Disable Rule** check box.
3. Enter a description of the rule in the *Description* field.
4. Begin to enter the field name or ID in the *Disable Field* field. A list of fields pops up on the screen and is filtered as you type. When the field you want to disable is visible, select it and click the plus sign (+) button.

   The field name is moved to the *Disable Fields* section.

5. Repeat the process to disable multiple fields.
6. Scroll to the Add condition section of the screen.
7. Select *Prospect-Borrower* or *Borrower* from the dropdown list to specify that the rule will run in both borrower and prospect files, or only in borrower files.
8. Specify the rule conditions:

   a. Click **Add a Condition**.

The *Conditions* section is expanded to specify a rule.

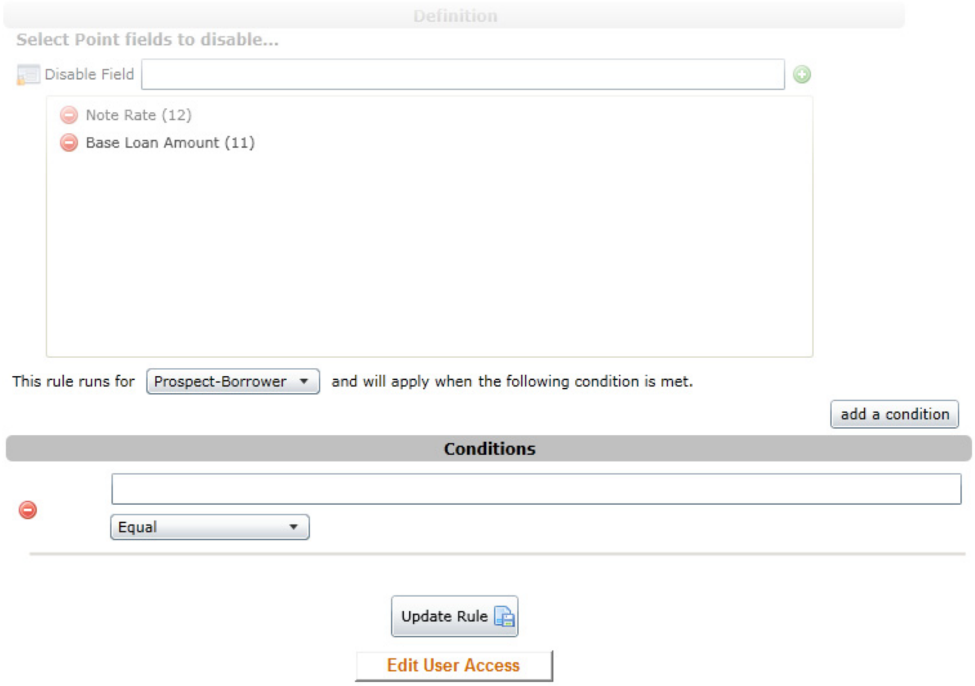


Figure 96. Edit Rule screen—Disable Fields Condition

b Begin to enter the field name or ID in the first field or select a field from the dropdown list. A list of fields pops up on the screen and is filtered as you type. When the field you want is visible, select it to populate the field.

> **Attention**
>
> *Although it is not a field name, Pending Request is also an option on this list. Select this option to create a condition that applies when a type of request, for example, credit report, flood certification, or print is pending in Point.*

c Select a condition from the second dropdown list.

d Enter the value that the condition must meet to be applied in the third field.

If you selected *Pending Request*, the values in this dropdown list change to types of requests. Select the condition that must be met for a pending request from the dropdown list.

e Click **Add a Condition** to add another condition.

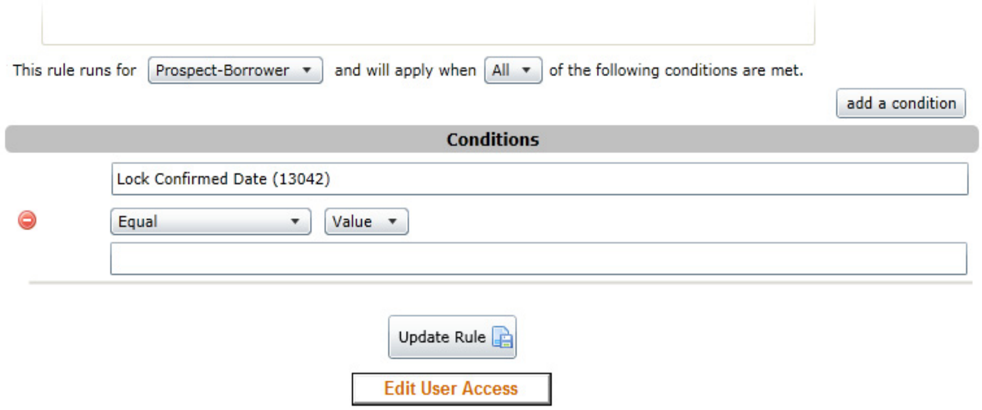


Figure 97. Edit Rule screen—Disable Fields, adding multiple conditions

If you enter more than one condition, a dropdown list is displayed that is used to specify if the rule applies when all conditions are met or when only one condition is met.

f Select the option (*All* or *One*) that applies to your rule.

g When you are finished adding conditions, click **Update Rule**.

Use the **Edit User Access** button or click the link at the top of the screen to specify user access rights.

Example

To create a rule that prevents users from changing the **Note Rate** *and* **Base Loan Amt** *fields after the loan is locked:*

1 *Select Disable Fields from the* ***Rule Type*** *dropdown list.*
2 *Select Base Loan Amt (11) from the* ***Disable Field*** *dropdown list and click the plus sign (+) button.*
3 *Select Note Rate (12) from the* ***Disable Field*** *dropdown list and click the plus sign (+) button.*
4 *Click* **Add a Condition**.
The *Conditions* section is now visible.
5 *Enter Lock Confirmed Date (13042) in the first field.*
6 *Select Is Not Blank from the second dropdown menu.*
7 *Leave the last field empty.*
8 *Click* **Update Rule**.

Users are unable to edit the specified fields after the loan is locked.

Related information

For information about editing user access rights, refer to ***Defining rule access rights****, on page 133.*

Creating a Required Fields rule

Required Fields rules run when the Point user performs one of the following actions:

- Saves a loan file by clicking the Save icon or by selecting ***File > Save***

- Initiates an action from the **Prospect Forms** or **Borrower Forms** dialog box to print a form, save or e-mail a form in PDF format, or store a form in the document repository when the *Form with data option* is selected from the ***Print Option*** dropdown list
- Clicks the following buttons:
  - **Create Registration Request** (***Registration & Rate Lock*** screen)
  - **Create Lock Request** (***Registration & Rate Lock*** screen)
  - **Create Lock Confirmation** (***Secondary Marketing*** screen)
  - **Create Suspense/Denial Notice** (***Underwriting*** screen)
  - **Create Loan Approval Notice** (***Conditions*** screen)
  - **Create Funding Conditions Notice** (***Conditions*** screen)
  - **Create Funding Figures Worksheet** (***Fees & Impounds*** screen)

When the Point user attempts one of these actions in a screen with empty required fields and the rule conditions apply, a notification dialog box is displayed and the required fields with missing data are highlighted in red. The user is unable to complete the action until they enter data in the required fields.

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

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

To create a new Required Fields rule:

1 Create a new rule.

After the new rule is created, the ***Edit Rule*** screen is displayed.

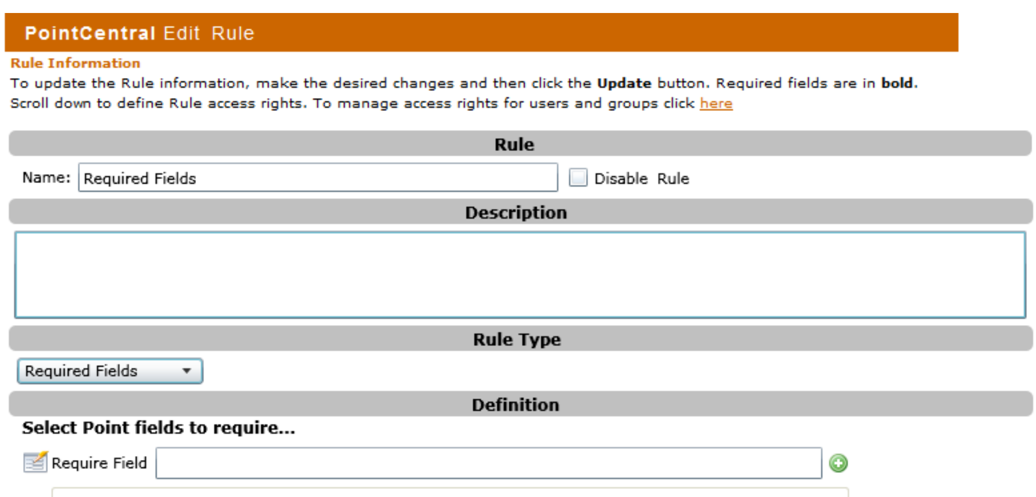


Figure 98. Edit Rule screen—Required Fields

2 To prevent the rule from being applied, select the **Disable Rule** check box.

3 Enter a description of the rule in the *Description* field.

4 Select *Required Fields* from the ***Rule Type*** dropdown list.

5 Begin to enter the field name or ID in the *Require Field* field. A list of fields pops up on the screen and is filtered as you type. When the field you want is visible, select it and click the plus sign (+) button.

The field name is moved to the *Required Fields* section.

6 Repeat the process to define multiple required fields.

7 Scroll to the Add condition section of the screen.

8 Select *Prospect-Borrower* or *Borrower* from the dropdown list to specify that the rule will run in both borrower and prospect files, or only in borrower files.

9 Specify the rule conditions.

a Click **Add a Condition**.

The *Conditions* section is expanded to specify a condition.

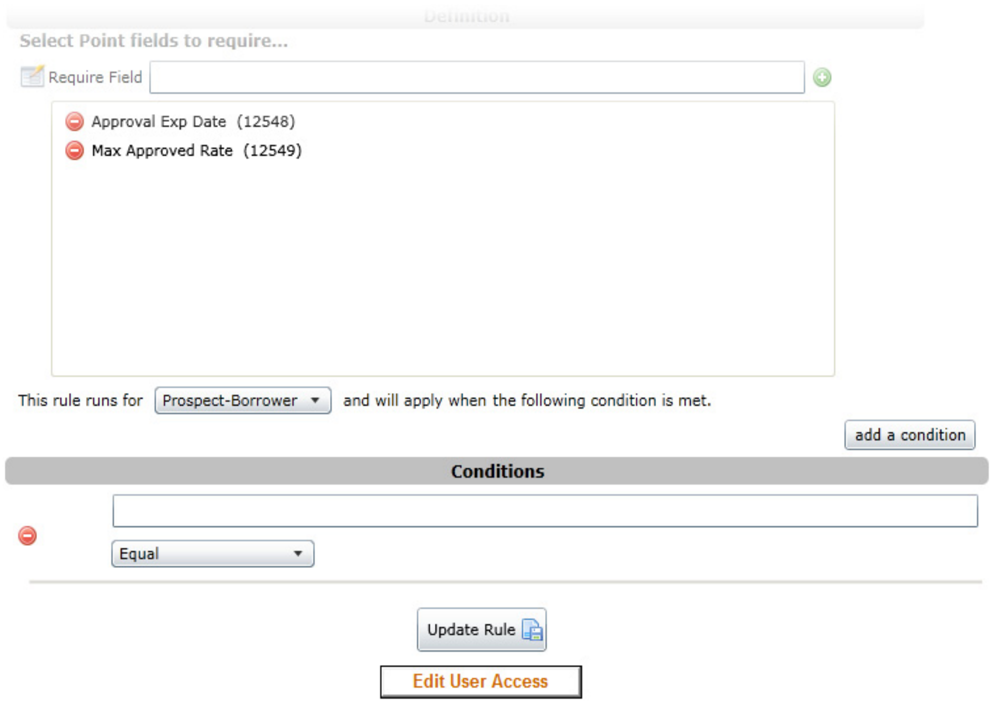


Figure 99. Edit Rule screen—Required Fields Condition

b Begin to enter the field name or ID in the first field. A list of fields pops up on the screen and is filtered as you type. When the field you want is visible, select it to populate the field.

Attention

Although it is not a field name, Pending Request is also an option on this list. Select this option to create a condition that applies when a type of request, for example, credit report, flood certification, or print, is pending in Point.

c Select the condition from the second dropdown list.

d Enter the value that the condition must meet to be applied in the third field.

If you selected *Pending Request*, the values in this dropdown list change to types of requests. Select the condition that must be met for a pending request from the dropdown list.

e Click **Add a Condition** to add another condition.

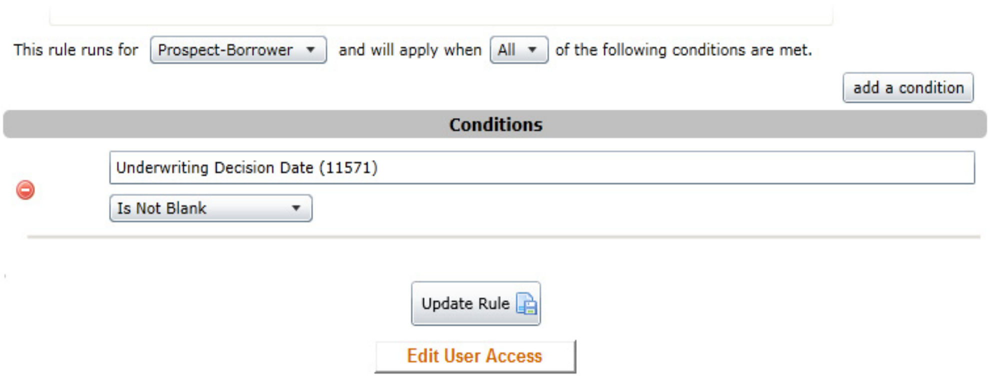


Figure 100. Edit Rule screen—Required Fields, adding multiple conditions

If you enter more than one condition, a dropdown list is displayed that is used to specify if the rule applies when all conditions are met or when only one condition is met.

f Select the option (*All* or *One*) that applies to your rule.

g When you are finished adding conditions, click **Update Rule**.

Use the **Edit User Access** button or click the link at the top of the screen to specify user access rights.

Example

*To create a rule that requires that the **Approval Exp Date** and **Max Approved Rate** fields be completed when a date is entered in the **Decision Date** field:*

1. *Select Required Fields from the **Rule Type** dropdown list.*
2. *Select Approval Exp Date (12458) from the **Require Field** dropdown list and click the plus sign (+) button.*
3. *Select Max Approved Rate (12549) from the **Require Field** dropdown list and click the plus sign (+) button.*
4. *Click* **Add a Condition**.
   The *Conditions* section is now visible.
5. *Select Underwriting Decision Date (11571) from the first dropdown menu.*
6. *Select Is Not Blank from the second dropdown menu.*
7. *Click* **Update Rule**.

The user must complete the required fields before they can continue with the task.

Related information

*For information about editing user access rights, refer to **Defining rule access rights**, on page 133.*

Creating a Custom Message rule

Custom Message rules run when the Point user performs one of the following actions:

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

When the Point user attempts one of these actions and the rule conditions apply, the custom message is displayed. Whether or not the user can proceed with the task depends on the rule conditions and parameters.

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

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

To create a new Custom Message rule:

1 Create a new rule.

After the new rule is created, the ***Edit Rule*** screen is displayed.

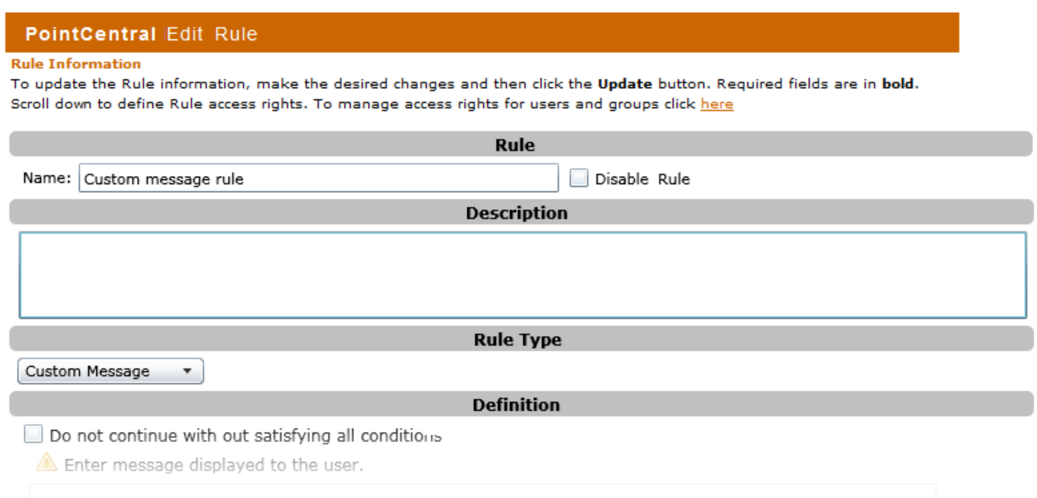


Figure 101. Edit Rule screen—Custom Message

2 To prevent the rule from being applied, select the **Disable Rule** check box.

3 Enter a description of the rule in the *Description* field.

4 Select *Custom Message* from the ***Rule Type*** dropdown list.

5 To prevent the Point user from continuing if all conditions are not met, select the **Do not continue without satisfying all conditions** check box. Otherwise, the user can continue with their task after the message is issued.

6 Enter the message to display to the user when the rule and conditions are not met.

7 Scroll to the Add condition section of the screen.

8 Select *Prospect-Borrower* or *Borrower* from the dropdown list to specify that the rule will run in both borrower and prospect files, or only in borrower files.

9 Specify any conditions of the rule:

a Click **Add a Condition**.

The *Conditions* section is expanded to specify a rule.

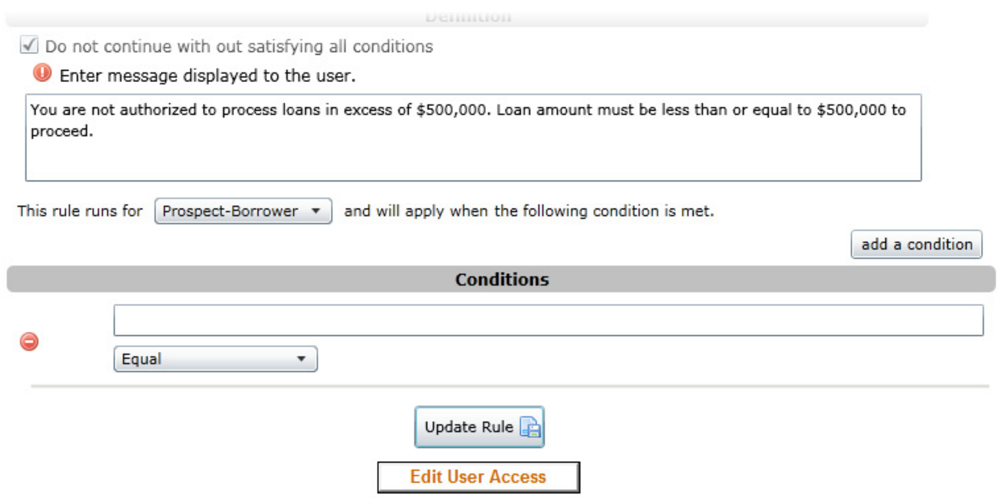


Figure 102. Edit Rule screen—Custom Message condition

b Begin to enter the field name or ID in the first field. A list of fields pops up on the screen and is filtered as you type. When the field you want is visible, select it to populate the field.

Attention

Although it is not a field name, Pending Request is also an option on this list. Select this option to create a condition that applies when a type of request, for example, credit report, flood certification, or print, is pending in Point.

c Select the condition from the second dropdown list.

d Enter the value that the condition must meet to be applied in the third field.

If you selected *Pending Request*, the values in this dropdown list change to types of requests. Select the condition that must be met for a pending request from the dropdown list.

e Click **Add a Condition** to add another condition.

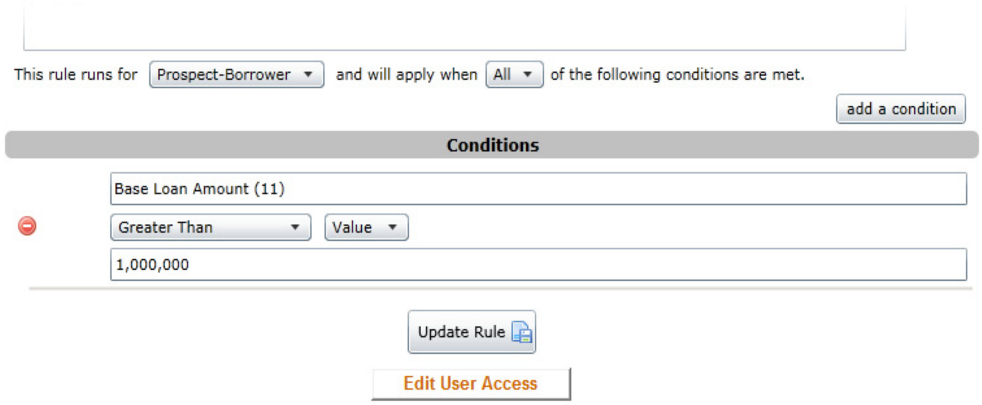


Figure 103. Edit Rule screen—Custom Message, adding multiple conditions

If you enter more than one condition, a dropdown list is displayed that is used to specify if the rule applies when all conditions are met or when only one condition is met.

f Select the option (*All* or *One*) that applies to your rule.

g When you are finished adding conditions, click **Update Rule**.

Use the **Edit User Access** button or click the link at the top of the screen to specify user access rights.

Example

To prevent a user from updating loan files when the loan amount is in excess of $1,000,000:

1. *Select Custom Message from the **Rule Type** dropdown list.*
2. *Select the* **Do not continue without satisfying all conditions** *check box.*
   Selecting this check box prevents the user from continuing to work in the loan file until all the conditions are met. If this check box is not selected, the user can continue working in the loan.
3. *Enter the message that is to display to the user when they perform one of the actions that runs the rule.*
4. *Click* **Add a Condition**.
   The *Conditions* section is now visible.
5. *Select the Base Loan Amount (11) from the first dropdown menu.*
6. *Select Greater Than from the second dropdown menu.*
7. *Enter 1,000,000 in the empty field.*
8. *Click* **Update Rule**.

The user will be unable to continue working in the loan file.

Related information

For information about editing user access rights, refer to ***Defining rule access rights****, on page 133.*

Creating a State Licenses rule

State Licenses rules run when the Point user performs one of the following actions:

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

When the Point user attempts one of these actions, the rule runs. If the subject property state does not match the selected states for the user, a notification dialog box is displayed and the user cannot proceed with the task.

The State Licenses rule does not run under the following conditions:

- When a web-based interface is launched or a transaction is completed
- When the user is switching to a co-borrower file

To create a new State Licenses rule:

1 Create a new rule.

After the new rule is created, the ***Edit Rule*** screen is displayed.

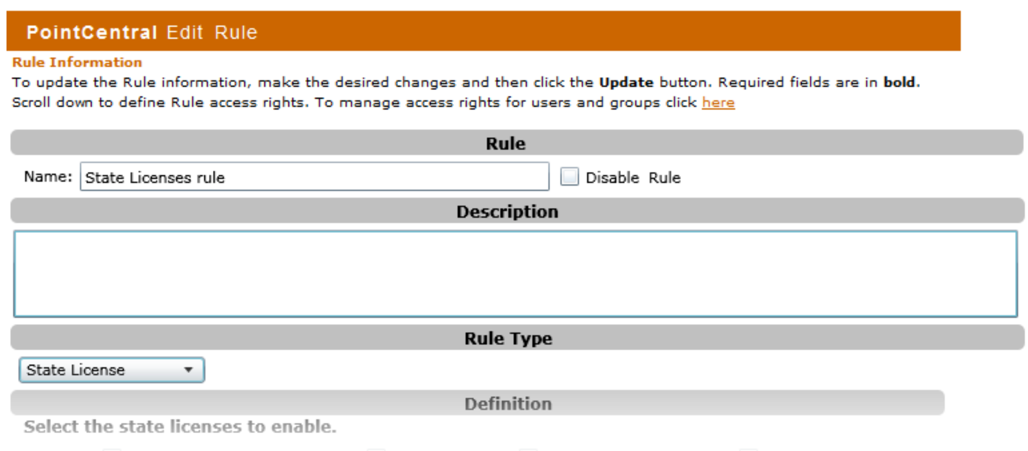


Figure 104. Edit Rule screen—State License

2 To prevent the rule from being applied, select the **Disable Rule** check box.

3 Enter a description of the rule in the *Description* field.

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

A list of states and U.S. territories is displayed.

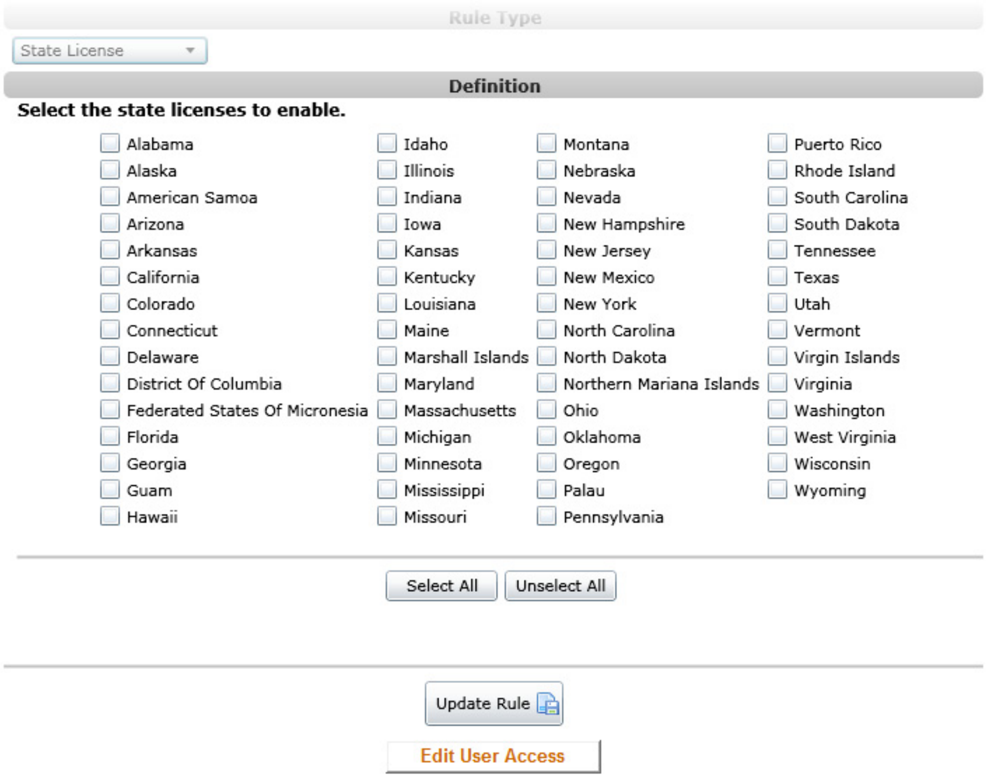


Figure 105. Edit Rule screen—State and territory list

5 Select the check boxes that correspond to the states and territories where the user is licensed to process loans.

If a property resides in a state or territory that is not selected for the current user, they are unable to save, print, and e-mail forms for that loan.

6 Click **Update Rule**.

Use the **Edit User Access** button or click the link at the top of the screen to specify user access rights.

Related information

For information about editing user access rights, refer to ***Defining rule access rights**, on page 133.*

Editing rules

To edit a rule:

1 Select ***Rules > List Rules***.

The ***List Rules*** screen is displayed.

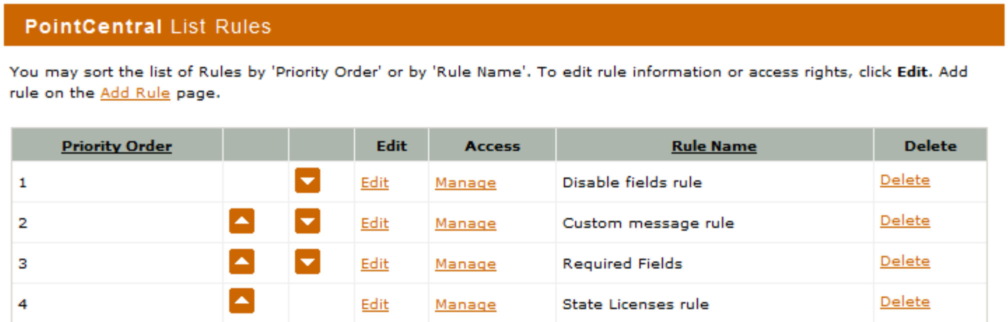


Figure 106. List Rules screen

You can perform the following actions from this screen:

- Change the order in which rules are applied by clicking the arrow buttons to move the rule up or down in the list
- Edit a rule
- Add group and user access rights
- Delete a rule

2 Click the **Edit** link next to the rule you want to edit.

The ***Edit Rule*** screen is displayed.

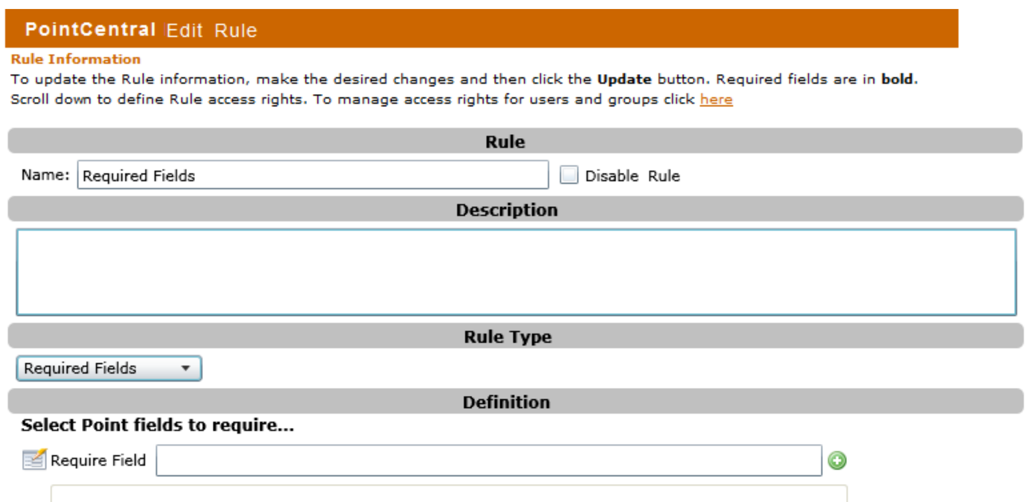


Figure 107. Edit Rule screen

3 The rule name is displayed in the *Name* field. Edit the name as needed.

4 Edit the rule as needed.

Related information

Refer to the following topics for specific information about the different rule types:

- ***Creating a Disable Fields rule***, *on page 120*
- ***Creating a Required Fields rule***, *on page 122*
- ***Creating a Custom Message rule***, *on page 126*
- ***Creating a State Licenses rule***, *on page 129*

Disabling rules

To prevent a rule from being applied, rather than permanently deleting the rule, you can disable it.

To disable any type of rule:

1 Select ***Rules > List Rules***.

The ***List Rules*** screen is displayed.

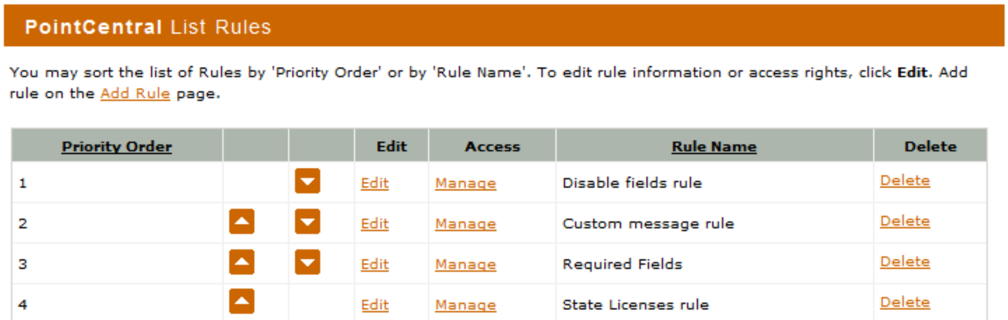


Figure 108. List Rules screen

2 Click the **Edit** link next to the rule you want to disable.

The ***Edit Rule*** screen is displayed.

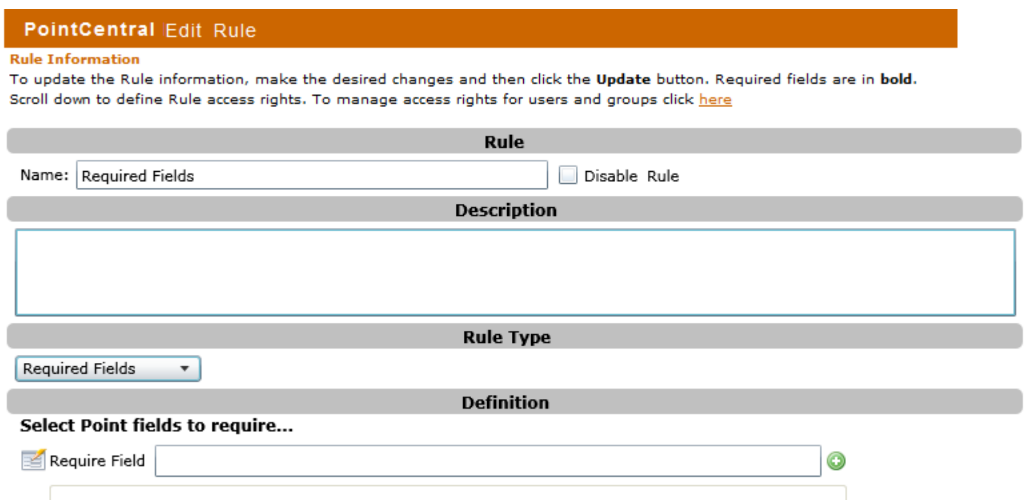


Figure 109. Edit Rule screen—Disable rule

3 Select the ***Disable Rule*** check box next to the *Name* field to deactivate the rule so it is not applied when the conditions are met.

4 Click **Update Rule**.

A confirmation message is displayed at the top of the screen.

> ***Tip***
>
> *You can enable the rule again by unselecting the* **Disable Rule** *check box.*

Defining rule access rights

The process to apply rules to user groups and users is the same. The steps to apply rules to user groups is used in this example.

To apply user group rule definitions:

1 Select ***Rules > List Rules***.

The ***List Rules*** screen is displayed.

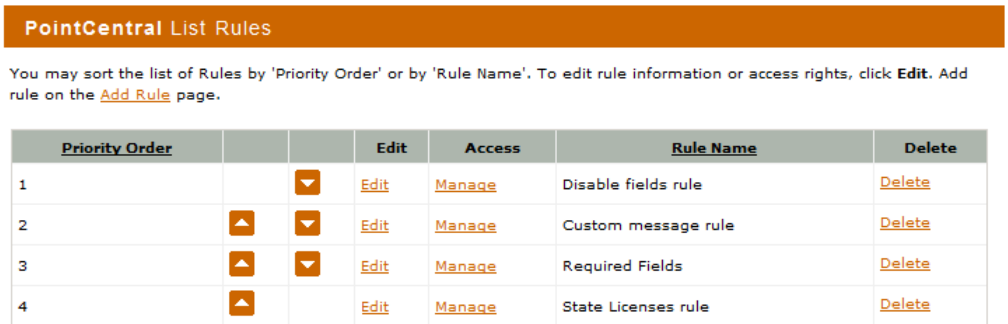


Figure 110. List Rules screen—Manage rules

You can perform the following actions from this screen:

- Change the order in which rules are applied by clicking the arrow buttons to move the rule up or down in the list
- Edit a rule
- Add group and user access rights
- Delete a rule

2 Click the **Manage** link for the rule you want to define access.

The ***Edit Rule Access*** screen is displayed.

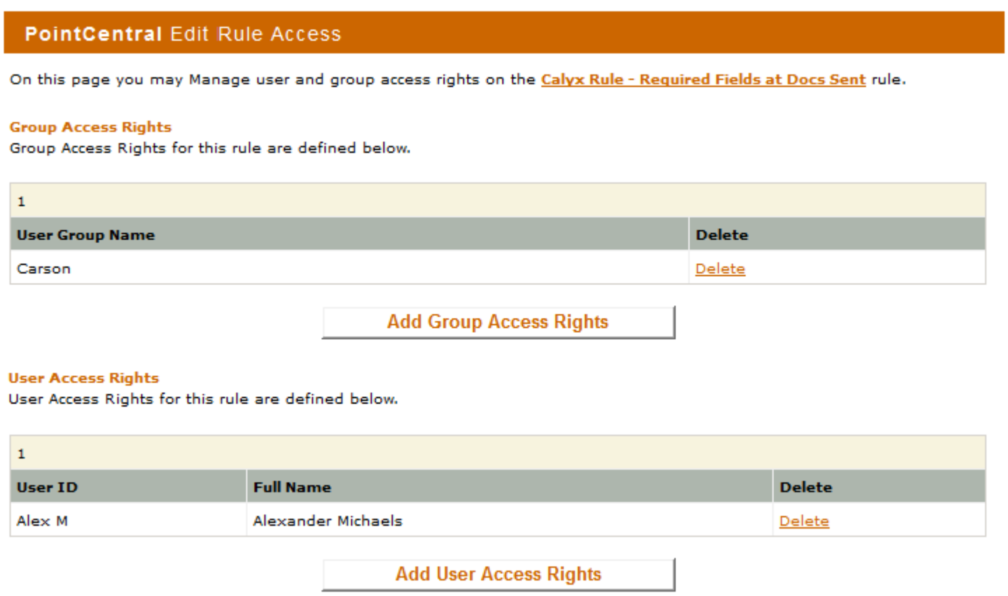


Figure 111. Edit Rule Access screen—Add Group Access Rights

The user groups with this rule applied are displayed.

3 Click **Add Group Access Rights**.

> ***Tip***
>
> *To apply rules to users, scroll to the* **User Access Rights** *section and click* **Add User Access Rights**.

The ***Add User Group*** screen is displayed.

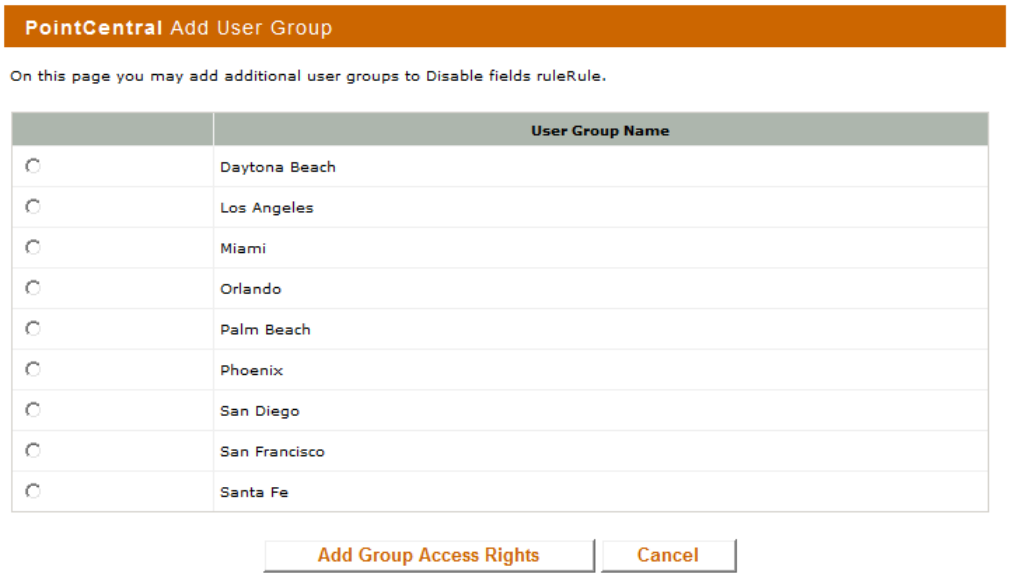


Figure 112. Add User Group

Use this screen to define the groups to which the rule applies.

4 Select a user group.

5 Click **Add Group Access Rights**.

6 Add additional groups to the rule as needed.

7 Click **Cancel** to return to the ***Edit Rule Access*** screen.

Importing resources

Although you can create components of your database individually, PointCentral has a utility that will import your existing data from conventional Point.

You can import the following information into PointCentral:

- Data folders
- Users and access rights
- Template sets
- Cardex database
- Users

The import function is available from the ***Configuration*** menu.

Importing conventional Point data folders

When you import a conventional data folder, the system will:

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

To import one or more conventional Point data folders:

1 Select ***Configuration > Parameters***.

2 Scroll to the *Root Folder Path* section. Make a note of the value of the root folder path.

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

3 Open a Windows Explore window and navigate to the current location of your conventional Point data folders. Copy the folders and paste them in the root folder.

4 In the administration site, select ***Configuration > Import > Data Folders***.

A list of the folders in the root folder path that have not been imported into PointCentral is displayed.

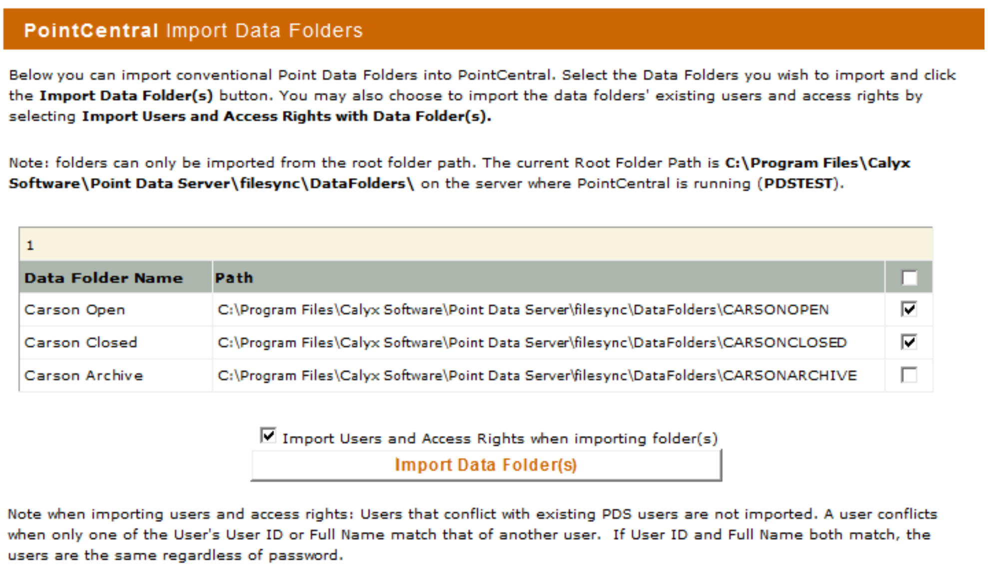


Figure 113. Import Data Folders screen

5 Select the check boxes that correspond to the folders you want to import.

6 To import the users and access rights with the folders, select the **Import Users and Access Rights when importing folder(s)** check box.

The following guidelines apply when importing users and access rights with data folders:

- If a user does not exist, the user is created during the import. Their password is the same one that was previously defined for the data folder.
- If a user ID or full name already exists, a user is not created.

- If a user already exists, and the user ID or full name for the conventional data folder matches the user ID or full name in PointCentral, the system grants access rights to the existing user for the given folder.
- The access rights that you give to the user for the given folder match the defined access rights that were created through Point Administrator.

Users and access rights are imported after the data folder import is complete.

> ***Tip***
>
> *After the import is finished you can view the list of imported users by selecting* ***Users > List Users*** *from the PointCentral menu.*

7 Click **Import Data Folder(s)**.

A confirmation message is displayed that indicates the folders to be imported. The folders are imported asynchronously.

8 To view the status of the import, click the **Status page** link in the confirmation message or select ***Status*** from the menu.

When the import is complete, the status changes to Done.

Importing users and access rights

If you do not elect to import users and access rights when you import the data folders, you can perform the import manually.

To import users and access rights manually:

1 Select ***Configuration > Import > Users and Access Rights*** to open the ***Import Users and Access Rights*** screen.

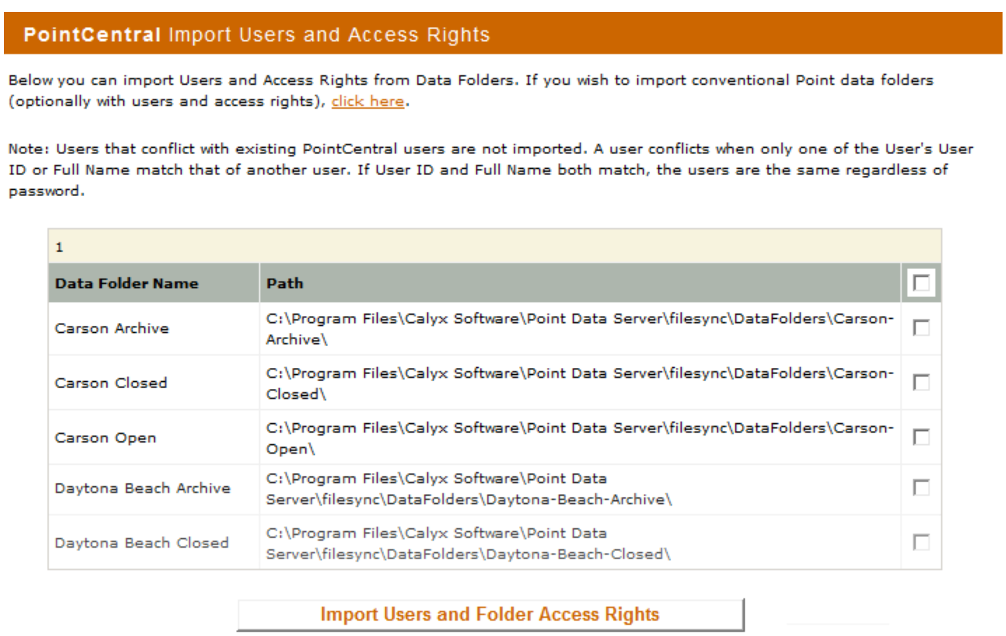


Figure 114. Import Users and Access Rights screen

2 Select the check boxes that correspond to the data folders from which you want to import users and access rights.

3 Click **Import Users and Folder Access Rights**.

A confirmation message is displayed that indicates from which folder the user and access rights are being imported.

4 To view the status of the import, click the **Status page** link in the confirmation message or select ***Status*** from the menu.

Importing template sets

Template sets in conventional Point are a collection of folders that each contain a different template type (for example, 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 which is located on a client PC or local server.

To import one or more conventional template sets:

1 Click ***Configuration > Parameters***.

2 Scroll to the *Root Template Set Path* section. Make a note of the value of the root template set path.

This is the location where template sets are stored. All template sets are stored in this location and there are no additional subdirectories between this path and the template sets.

3 Open a Windows Explore window and navigate to the current location of your conventional Point template sets. Copy one or more template sets and paste them in the root template set directory. Be sure to copy all of the subdirectories.

Tip

Template sets are typically located in C:\PNTTEMPL on the Point client.

To verify the location, open Point Administrator and click **Change Template Directory** *to view the current location.*

4 After you paste the template set into the root directory, rename it.

Important

Renaming template sets as you copy them will prevent accidental loss of data if you copy another template set named PNTTEMPL from a different client.

5 In the administration site, select ***Configuration > Import > Template Sets***.

The ***Import Template Sets*** screen is displayed.

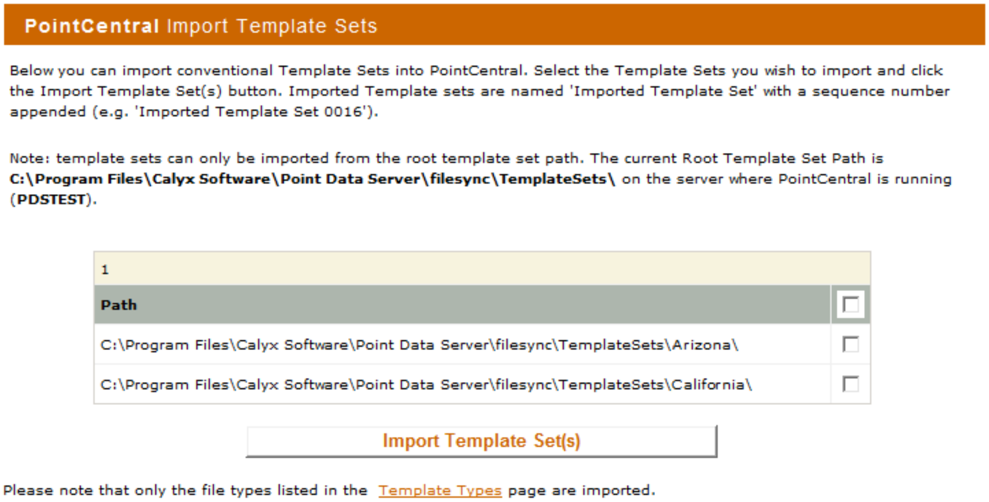


Figure 115. Import Template Sets screen

The templates sets that were copied from the client are listed.

6 Select the check boxes that correspond to the template sets you want to import and click **Import Template Set(s)**.

A confirmation message is displayed.

When a template set is imported, it is named **Imported Template Set *nnnn***, where ***nnnn*** is a sequential number assigned by PointCentral. You can change the template set name manually after the import is complete.

The template sets are imported asynchronously.

7 To view the status of the import, click the **Status page** link in the confirmation message or select ***Status*** from the menu.

When the import is complete, the status changes to Done.

Note

When you import a conventional template set, the system creates the template set in PointCentral and scans and synchronizes all template files. It also 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.

Tip

To view a list of all template types, including their sub-directories, select ***Configuration > Template Set Maintenance > Template Types****.*

After the template sets are imported, you can grant the access rights to these template sets to the appropriate user groups or users.

> **Related information**
>
> *For information about setting and changing access rights to templates, refer to* ***Template sets****, on page 96.*

Importing a Cardex database

You can import an existing conventional Cardex database from Point into PointCentral. You can also import one Cardex database into another Cardex database.

> **Prerequisite**
>
> *As a security measure and to maintain administrative control over the Cardex records being imported, it is not possible for a Point user to export Cardex records directly from a Point client into PointCentral.*
>
> *Therefore, the Cardex database must first be exported from Point before the import can occur.*

To import one Cardex database into another:

1 Export data from the Cardex database from Point.

   a Open Point.

   b Select ***Utilities > Cardex Database***.

   c From the toolbar in the **Cardex Database [Browsing for all records]** dialog box, select ***File > Export to Calyx PDS***.

   d In the **Export Cardex** dialog box, navigate to where you want to save the file and accept the default file name.

   e Click **Save**.

   The file is exported to the specified location.

2 Copy the Cardex file into the **Cardex Import** directory which is typically located at **C:\Program Files\Calyx Software\Point Data Server\filesync** on PointCentral.

3 If the Cardex database that you want to import the files into does not already exist on PointCentral, create a new one to receive the imported database.

4 Select ***Configuration > Import > Cardex Database*** to access the ***Import Cardex Database*** screen.

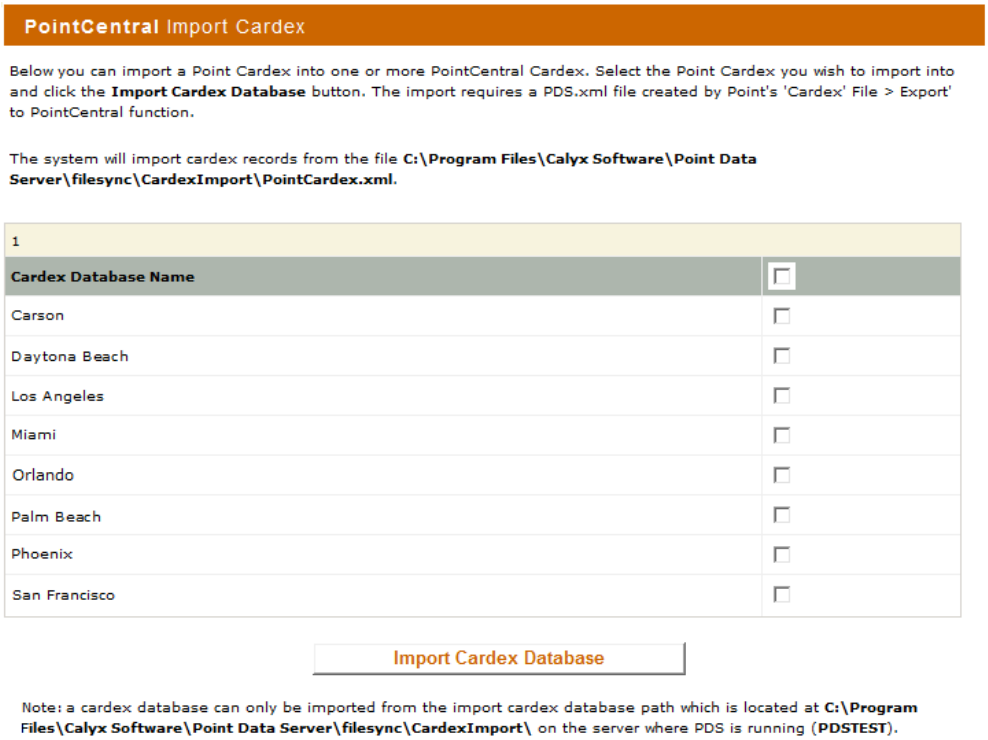


Figure 116. Import Cardex Database screen

5 Select the database into which you want to import and click **Import Cardex Database**.

A confirmation message is displayed. The Cardex records are imported asynchronously.

6 To view the status of the import, click the **Status page** link in the confirmation message or select ***Status*** from the menu.

When the import is complete, the status changes to Done.

Related information

- *For information about creating a Cardex database, refer to* ***Adding Cardex databases****, on page 110.*

Importing users from a text file

It is also possible to import users from a text file. This method is useful if you are a new user and have not yet created data folders and users in conventional Point.

When you import a Point user, the same data validation rules apply as those when a Point user is created:

- The full name cannot be blank and cannot exceed 255 characters.
- The user ID cannot be blank and cannot exceed 255 characters.
- The 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)

To import Point users from a file:

1 Create a text file.

   a Open a new file from a text editor of your choice.

   b Enter the user ID, clear text password, and full name for each user.

   Use the following guidelines when creating the user file:

   - One user per line
   - Separate each field with a tab

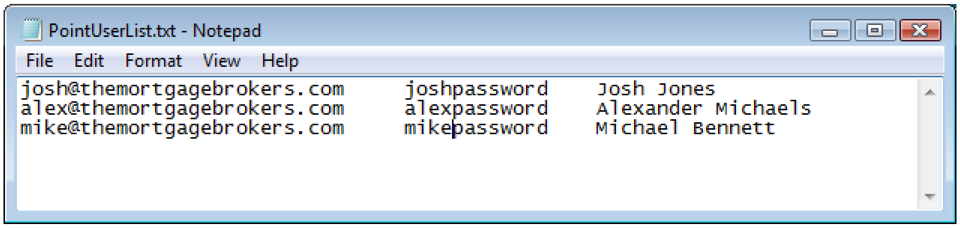


Figure 117. Import users from text file example

2 Copy the PointUserList.txt file into the **User Import** directory which is typically located at **C:\Program Files\Calyx Software\Point Data Server\filesync** on PointCentral.

3 Select ***Configuration > Import > Users From File*** to access the ***Import Users From File*** screen.

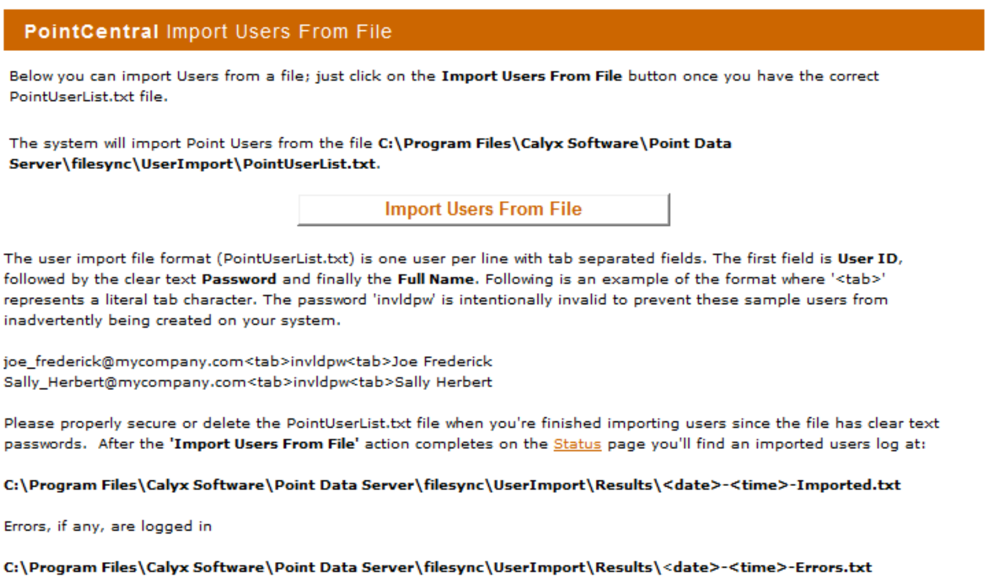


Figure 118. Import Users From File screen

4 Click **Import Users From File** and click **OK** in response to the confirmation prompt.

   A confirmation message is displayed. The users are imported asynchronously.

5 To view the status of the import, click the **Status page** link in the confirmation message or select ***Status*** from the menu.

   When the import is complete, the status changes to Done.

   During the import, a log is created that records which users were successfully imported. If any errors occur, an error log is also created. These files are stored in **Results** in the **UserImport** directory.

6 Delete or secure the PointUserList.txt file after importing the users because the file has clear text passwords.

Access right reports 5

To help with large directory structures and a large number of users, reports are available that illustrate the relationships between users and user groups, and their access rights to data folders, template sets, rules, and Cardex databases. These reports make it easy to check that users have access to the resources they need.

The following reports are available:

- User Effective Access Rights
- Users, Group Memberships
- Groups, User Members
- Data Folders, Groups And Users with Access Rights
- Template Sets, Groups And User with Access Rights
- Cardex Databases, Groups And Users with Access Rights
- Data Folder Status Chart

To access reports, select ***Reports*** in the navigation menu on the administration site.

In this topic

User effective access rights

You can 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

Viewing user effective access rights

To view user template set effective access rights:

1 Select ***Reports > User Effective Access Rights***.

Figure 119. User Effective Access Rights screen

2 Enter the user ID or full name of the user and click **Search**.

The effective access rights for the specified user are displayed for the template set, Cardex database, data folders, and rules.

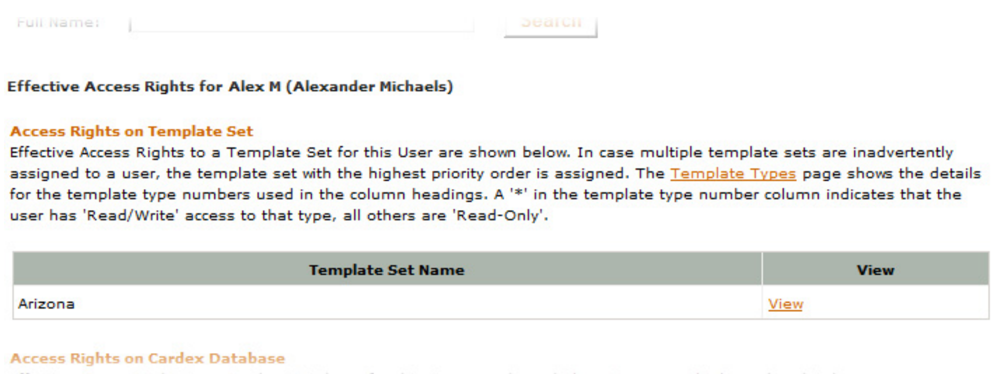


Figure 120. User Effective Access Rights

3 Scroll down the screen to view additional access rights.

4 To view the access rights for template sets, data folders, and rules, click **View**.

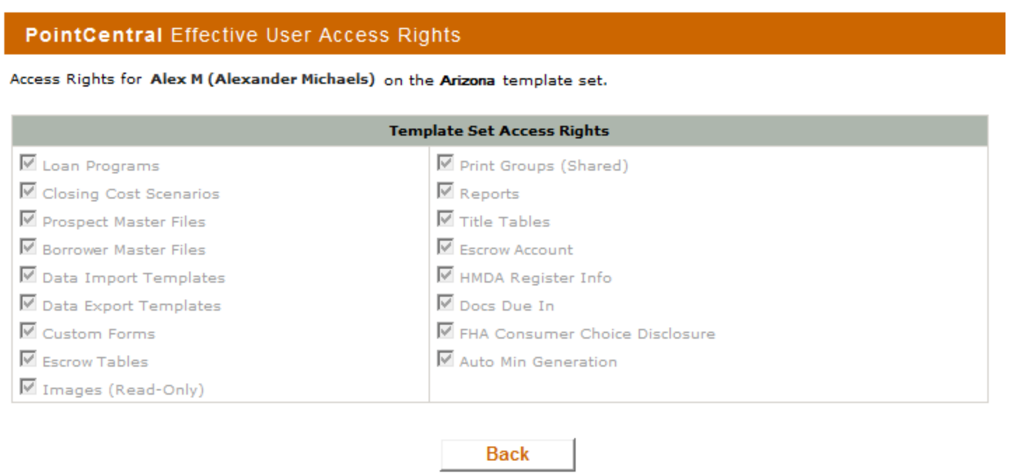


Figure 121. Effective User Access Rights—Template Set Access Rights

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.

To view the Users, Group Memberships report, select ***Reports > Users, Groups Memberships***.

PointCentral Users, Group Memberships

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
Alex M (Alexander Michaels)	Arizona
Brian (Brian Chen)	Florida
Jane (Jane Nguyen)	California
JJ (Josh Jones)	Arizona
Maggie (Margaret Bryant)	California
Maria (Maria Espinosa)	Florida

Figure 122. Users, Groups Memberships screen

Groups, User Members

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

To access the Groups, User Members report, select ***Reports > Groups, User Members***.

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 123. Users, Groups Memberships screen

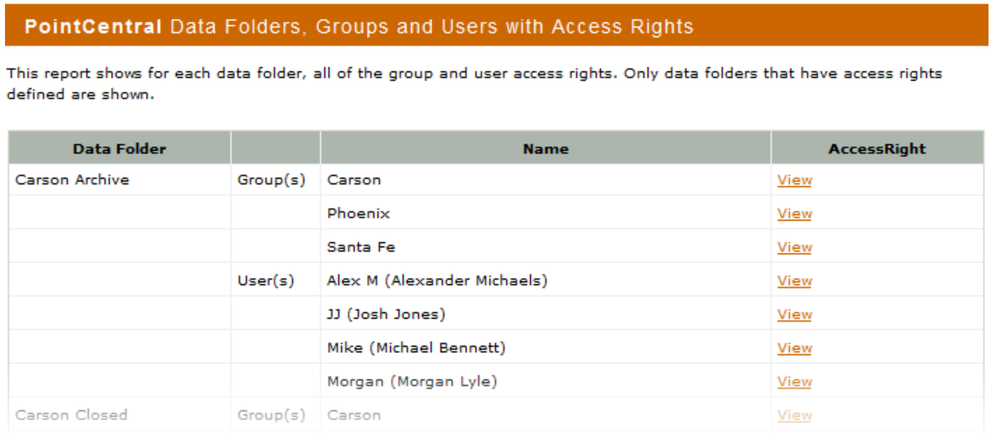
Data Folders, Groups and Users with Access Rights

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.

Viewing the Data Folders, Groups and Users with Access Rights report

To view the Data Folders, Groups, and Users Access Rights report:

1 Select ***Reports > Data Folders, Groups and Users with Access Rights***.



PointCentral Data Folders, Groups and Users with Access Rights

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
Carson Archive	Group(s)	Carson	View
		Phoenix	View
		Santa Fe	View
	User(s)	Alex M (Alexander Michaels)	View
		JJ (Josh Jones)	View
		Mike (Michael Bennett)	View
		Morgan (Morgan Lyle)	View
Carson Closed	Group(s)	Carson	View

Figure 124. Data Folders, Groups and Users with Access Rights report

2 Click the **View** link next to the user or group name to view the access rights for that user or group.

3 The ***Edit User Group Access Rights*** (or ***Edit User Access Rights***) screen is displayed.

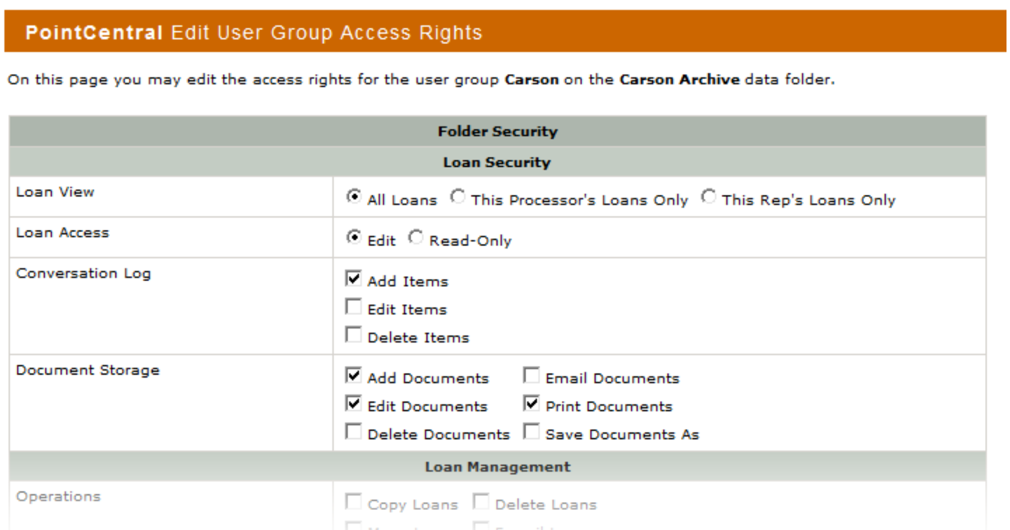


Figure 125. Edit User Group Access Rights

4 Edit the access rights if needed.

5 Scroll to the bottom of the screen and click **Update Group Access Rights** or click **Cancel** to exit the screen.

Template Sets, Groups and Users with Access Rights

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

Viewing the Template Sets, Groups and Users with Access rights report

To view the Template Sets, Groups and Users with Access rights report:

1 Select ***Reports > Template Sets, Groups and Users with Access Rights***.

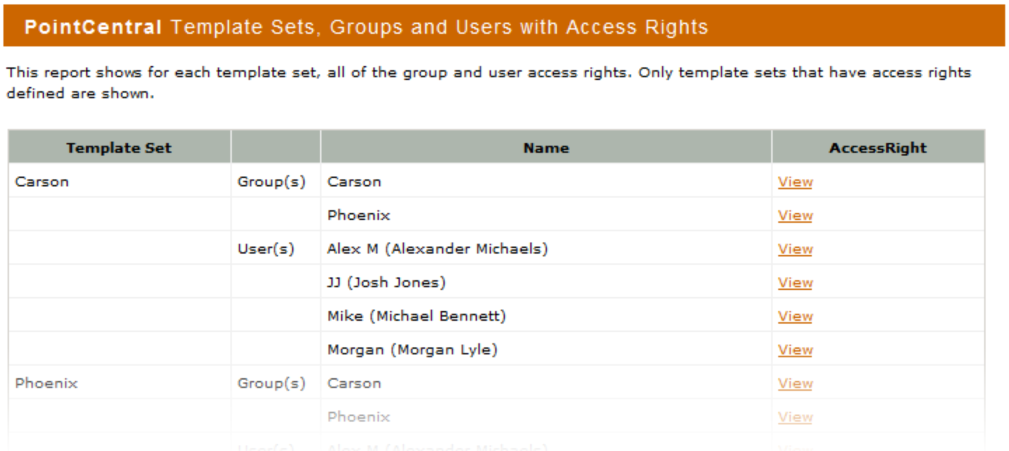


Figure 126. Template Sets, Groups and Users with Access Rights report

2 Click the **View** link next to the user or group name to view the access rights for that user or group.

3 The ***Edit User Group Access Rights*** (or ***Edit User Access Rights***) screen is displayed.

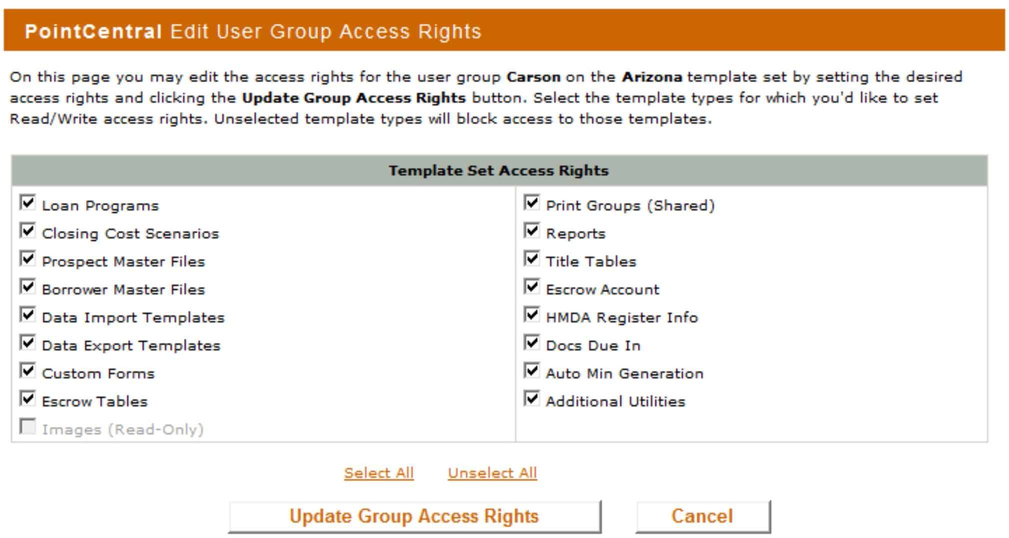


Figure 127. Edit User Group Access Rights—template sets

4 Edit the access rights if needed.

5 Scroll to the bottom of the screen and click **Update Group Access Rights** or click **Cancel** to exit the screen.

> **Tip**
>
> *To view a list of all template types, including their sub-directories, select* ***Configuration > Template Set Maintenance > Template Types****.*

Cardex Databases, Groups and Users with 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.

To view the Cardex Databases, Groups and Users with Access rights report, select ***Reports > Cardex Databases, Groups and Users with Access Rights***.

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 128. Cardex Databases, Groups and Users with Access Rights report

Rules, Groups and Users with 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.

To view the Rules, Groups and Users with Access rights report, select ***Reports > Rules, Groups and Users with Access Rights***.

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
		San Francisco

Figure 129. Rules, Groups and Users with Access Rights report

Point custom report support 6

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

In this information, supported fields can refer to either the built-in supported fields in Point or the entire collection of supported fields, which includes built-in supported fields, custom fields, and additional fields.

If you create custom reports, you must ensure that the Point fields in the report definition are supported fields.

If the report uses unsupported fields that were not added as additional fields, then no data is returned from data folders. If you need the data from these fields, add the fields by using the Additional fields procedure. Point reports can include a mix of PointCentral and conventional Point data folders.

In this topic

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

With the Additional fields feature, you can dynamically add up to 300 Point fields to the supported fields in PointCentral.

Definition

In this information, Support fields refers to built-in supported fields for reports and the entire collection of supported fields which also include

PointCentral supports all the fields that are required to perform Loan and Task operations (Search, Advanced Search, List Co-Borrowers, Search and Advanced Search). These operations always use PointCentral for accelerated data folders.

Related information

- *For more information about using the Additional fields function, refer to* ***Additional fields****, on page 158.*
- *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 that are generated from data in PointCentral data folders is much faster than with conventional Point data folders. Reports can include a mix of PointCentral and conventional data folders. However, 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. This 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. For illustration purposes, this report is being run on PointCentral and conventional data folders. Ordinarily, to get the fastest results, you would keep your loan files in PointCentral data folders and run reports on the PointCentral folders only, completely avoiding the slower conventional folders.

	Field Name	Field ID	Condition	Show	Total	Format
1	Folder	FOLDER		☑		Auto
2	File	1		☑		Auto
3	Borrower	NAME		☑		Auto
4	Loan Amt	11		☑		Auto
5	Rate	12		☑		Auto
6	School District	9900		☑		Auto
7	Other Reserve (GFE)	1096		☑		Auto
8				☑		Auto

Figure 130. Point user-defined report example

This report uses carefully selected fields to demonstrate PointCentral report behavior. The *Folder* (Field ID: FOLDER) 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:

- File (Field ID: 1)
- Borrower (NAME)
- Loan Amt (11)
- Rate (12)

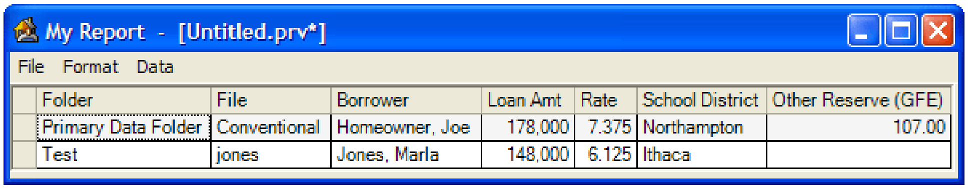
School District (9900) is a custom field. Other Reserve (GFE) (1096) is an unsupported field.

In this example, the School District (9900) custom field is defined with the Custom Fields table (which was rebuilt and is now supported). However, the Other Reserve (GFE) (1096) field was not added to PointCentral and is currently unsupported. When you generate this report (by clicking the ***Generate*** button on the reports screen in Point), an error occurs and the ***Errors Detected*** dialog box is displayed.

The ***Errors Detected*** dialog box indicates that errors or warnings were generated during the report that might affect 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

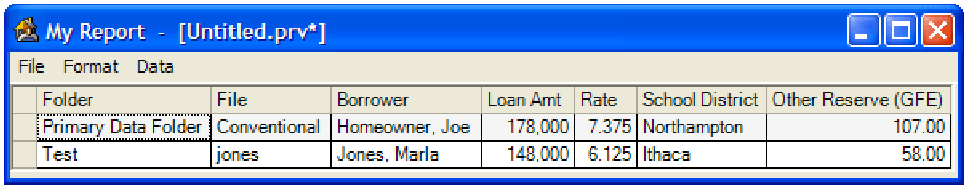
The message refers to field ***f1096***. An ***f*** is prepended to the Point Field ID, so this is Point Field ID f1096. This is the unsupported Other Reserve (GFE) (1096) field in the report.



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 131. Report results with unsupported fields not

Checking the report results reveals that 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 132. Report results after adding unsupported fields to Additional Fields

If you add the unsupported field *Other Reserve (GFE) (1096)* to the supported fields collection by using additional fields and run the report again, the system returns the data for *Other Reserve (GFE) (1096)*. This example shows an additional field.

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

In the unlikely event that you have a report without at least one supported field, an error occurs that indicates that PointCentral does not support any of the fields in the report.

If the report is run for only PointCentral data folders, then the report results dialog box does not display because no data is available to display. You can remedy this situation by adding a supported field to the report such as borrower name or file name, or by including a custom field and adding the unsupported field to PointCentral by using additional fields.

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

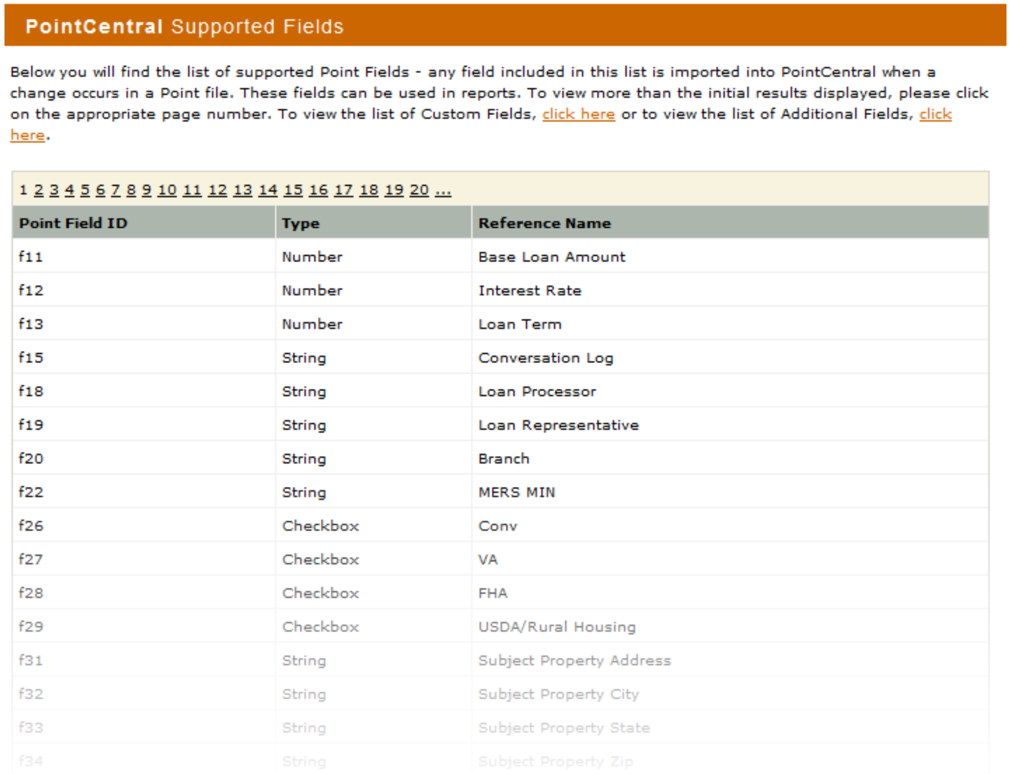
- Normal point fields
- Custom fields
- Report macro fields
- Additional fields

To access the ***Supported Fields*** page:

1 Log in to the administration web site.

2 Select ***Configuration > Point Fields > Supported Fields***.

The ***Supported Fields*** screen is displayed:



PointCentral Supported Fields

Below you will find the list of supported Point Fields - any field included in this list is imported into PointCentral when a change occurs in a Point file. These fields can be used in reports. To view more than the initial results displayed, please click on the appropriate page number. To view the list of Custom Fields, click here or to view the list of Additional Fields, click here.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 ...

Point Field ID	Type	Reference Name
f11	Number	Base Loan Amount
f12	Number	Interest Rate
f13	Number	Loan Term
f15	String	Conversation Log
f18	String	Loan Processor
f19	String	Loan Representative
f20	String	Branch
f22	String	MERS MIN
f26	Checkbox	Conv
f27	Checkbox	VA
f28	Checkbox	FHA
f29	Checkbox	USDA/Rural Housing
f31	String	Subject Property Address
f32	String	Subject Property City
f33	String	Subject Property State
f34	String	Subject Property Zip

Figure 133. Supported Fields screen

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, for example, a number or date. 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. To access the report macro fields, select the page that contains field ID 30000.

To reference the Report macro fields in Point reports, use the case-sensitive reference name. This reference is different from the normal Point fields and custom fields that are 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 were added to PointCentral are available on the ***Additional Fields*** screen.

Related information

- *Refer to **Custom screens and fields**, on page 155, for a list of user-defined custom screens and fields, information about custom fields, and how to update custom field definitions.*
- *Refer to **Additional fields**, on page 158, for the list of user-specified fields, information about additional fields, and how to update additional fields definitions.*

Custom screens and fields

If your organization uses custom screens and fields in Point to support your business processes, you can use the custom fields page to ensure that PointCentral imports them into the database when needed.

If you change any of the custom screen definitions, you must rebuild the Custom Field Table to match the number of defined fields and their data types. When you rebuild the Custom Field Table, all the loan files are synchronized to populate the newly defined custom fields in the database with the data from the loan files.

The person in your organization who is responsible for defining and maintaining the definitions creates the custom screen definitions. These definitions apply to all Point clients and loan files in your organization. Point users enter and view the custom field data by selecting ***Forms > Custom Screens/(User defined Screen Name)***. For more information about Point custom screens, refer to your Point documentation.

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

Changing custom screen definitions

To change the custom screen definitions used by PointCentral:

1 After the custom screen fields are changed in Point, log in to the administration web site.

2 Select ***Configuration > Point Fields > Custom Fields***.

The ***Custom Fields*** screen is displayed.

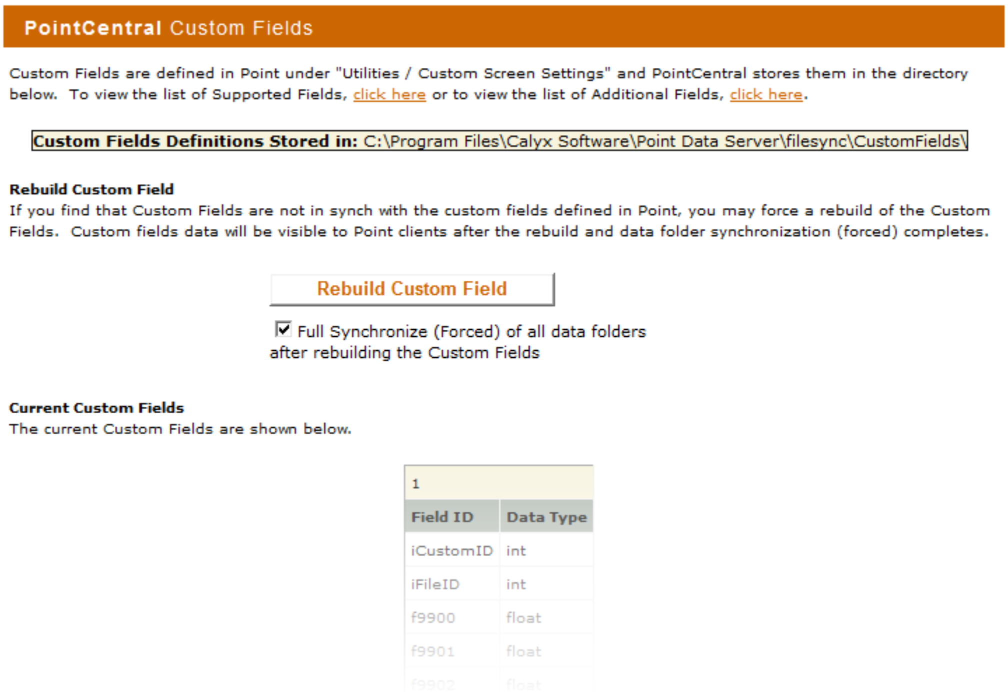


Figure 134. Custom Fields screen

3 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 all the Point loan files into the database, including the custom field data.

If you force a full synchronization on all the folders (highly suggested), it could take a while. You can skip the forced full synchronization if you do not need the custom field data in the Point loan files at the time of the rebuild.

Rebuilding the table is an asynchronous operation that runs in the background to save resources and allow you to continue to work in PointCentral while it completes. Check the ***Status*** page to see the current status of the operation and to verify its completion.

The Rebuild Custom Fields Table process clears the previous custom field definitions from the database, then creates a new Custom Fields Table by using the current definitions. Point clients see the new definitions the next time they open Point. They can reference the custom fields in reports.

Running reports by using the updated Custom Field Definitions returns empty custom fields for a loan file until that file is synchronized by using the rebuilt Custom Fields Table. If you selected the **Full Synchronize (Forced) of all PDS Accelerated Folders after rebuilding Custom Field Table** option, the system synchronizes the loan files in all accelerated folders.

Important

All Point users must be logged off before you can perform a full synchronization. Refer to ***Forced synchronization****, on page 161, for information about performing a full, or forced, synchronization.*

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

4. Monitor the progress of the custom fields rebuild on the administration ***Status*** page. (Rebuild Custom Fields Table and optionally, Synchronize folder (forced) operations.) Check for a status of Done.
5. Check the Windows Application Event Log for any errors.
6. Review the Current Custom Fields Definitions on the administration ***Custom Fields*** page to verify the new definitions.
7. When you have rebuilt your custom fields table, the current custom screen definitions used by PointCentral are available on the custom fields page.

The *iCustomID* and *iFileID* fields are used internally by PointCentral. You can ignore them. The *Data Type* column shows the current definition of the data type that is used to validate and store the field in the database. These database types map to the Custom Screen Settings Field Type as shown in the following table:

Table 13. 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.

Related information

- *Refer to* ***Checking system status****, on page 57, for more information about the* ***Status*** *screen.*
- *Refer to the* ***Point User Guide*** *for more information about custom screens and fields in Point.*

Importing custom screens

If your organization creates custom screens and fields in Point, you must import them into PointCentral. If your organization does not use custom screens and fields, you can skip this information.

Note

In some cases it is more efficient to re-create your screen settings and rebuild the custom fields table rather than by using the import function. However, to avoid having to synchronize your data folders later, create or import your data folders at this stage in the configuration.

The custom screen settings in Point are stored in the files CUSTOM*n*.CSF where *n* is a number between 1 and 4 that corresponds to custom screens 1 through 4 in Point. Custom screen settings are called custom screen definitions in PointCentral.

To import the custom screen settings:

1 From the desktop, select ***Start > Administrative Tools > Services***.

2 Double-click CalyxPdsFileSync, then click **Stop** to stop the service.

3 Copy the custom screen and fields (**.CSF*) files to **C:\Program Files\Calyx Software\Point Data Server\filesync\CustomFields**, substituting your installation path for **C:\Program Files\Calyx Software\Point Data Server**.

The default location for existing custom screen and field files in conventional Point is **C:\PNTTEMPL**.

4 Start the CalyxPdsFileSync service. Use the Services Control Panel and click **Start** in the **CalyxPdsFileSync Properties** dialog box.

Related information

For information about creating custom screens and rebuilding the custom fields table, refer to ***Custom screens and fields****, on page 155.*

Additional fields

If your organization uses custom reports that require additional fields, use this information to ensure that imports them into the database when needed. You can identify up to 300 additional field ID that are not already included in supported or custom fields to use in custom reports.

Configuring additional field definitions

To configure additional field definitions:

1. In Point, select ***Utilities > Load Field ID > Prospect*** or ***Utilities > Load Field ID > Borrower***.
2. Write down the field ID and a brief description for every field that you want to import.
3. Log in to the administration web site and select ***Configuration > Point Fields > Additional Fields***.

The ***Additional Fields*** screen is displayed.

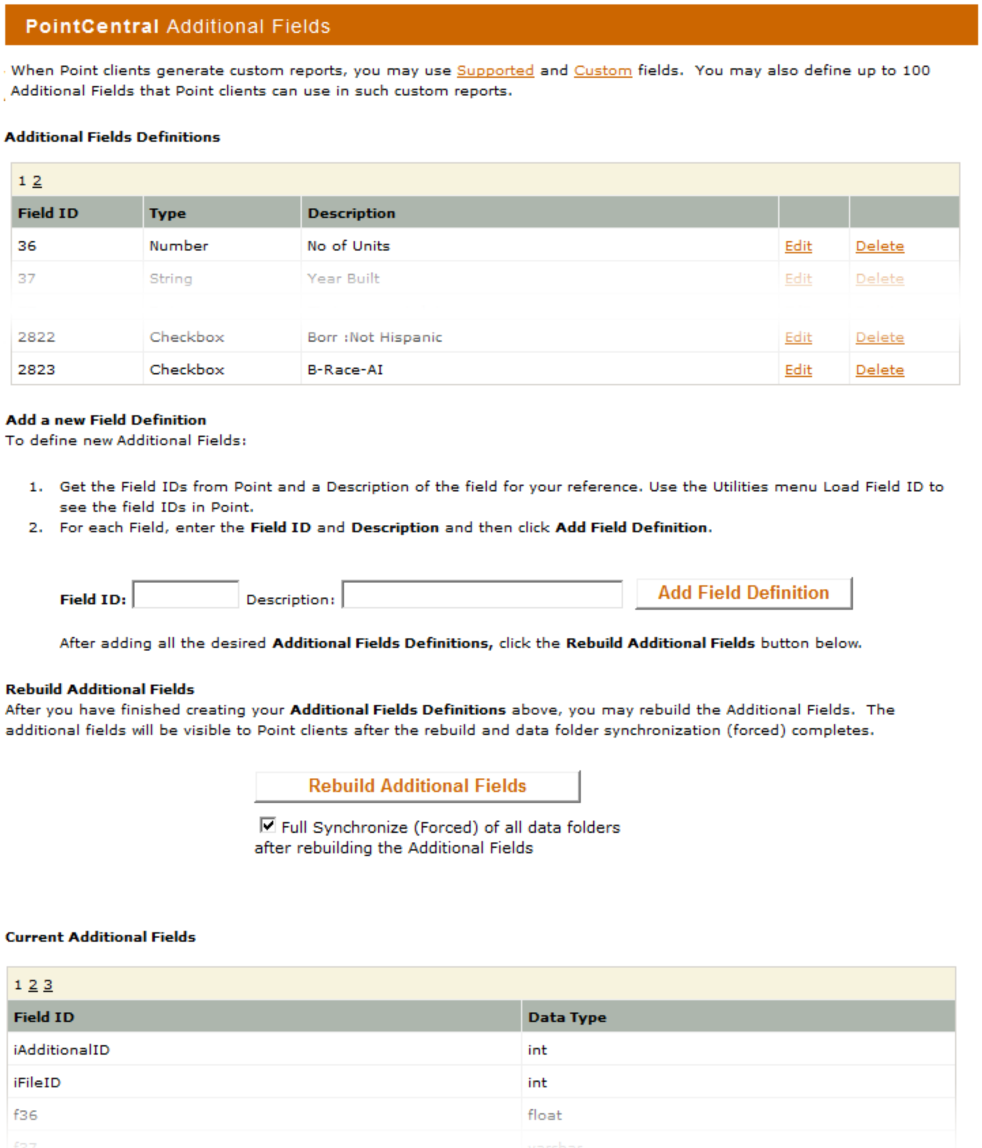


Figure 135. Additional Fields screen

4 Scroll to the *Add new field Definition* section and enter the ID and a description in the *Field ID* and *Description* fields and click **Add Field Definition**.

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

Enter the field ID and description for each field that you want to import.

5 After you add all the field definitions, click **Rebuild Additional Fields**.

Rebuilding the table is an asynchronous operation that runs in the background to save resources and allow you to continue to work in PointCentral while it completes. Check the ***Status*** page to see the current status of the operation and to verify its completion.

When you rebuild the table, the system deletes the previous Additional Fields Table from the database and then re-creates it. It is recreated by using the current Additional Fields Table with the current Additional Fields Definitions.

A Point client sees the new definitions the next time that user opens Point and references the additional fields in Reports. When you run reports by using the updated Additional Fields Definitions, the system returns empty fields for the additional fields in a loan file until that particular file is synchronized when you rebuild the Additional Fields Table. The synchronization occurs by default if you leave the **Full Synchronize (Forced) of all data folders after rebuilding the Additional Fields Table** check box checked. The forced full synchronization occurs in the background. Check the current status on the ***Status*** page.

Important

All Point users must be logged off before you can perform a full synchronization. Refer to ***Forced synchronization****, on page 161, for information about performing a forced, or full, synchronization.*

A forced full synchronization can take a while, depending on the number of loan files and data folders within PointCentral. PointCentral synchronizes every Point loan file in the database, including the additional fields data. You can skip some of the synchronization if you do not need the additional field data when you rebuild.

For example, if your organization wants to begin tracking income and monthly payments in the next quarter, you do not need to recreate these fields in all previous loan files. Therefore, you can rebuild the Additional Fields Table without full synchronization. If your organization wants to track income and monthly payments from loan data prior to rebuilding the table, rebuild the table with a forced full synchronization.

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

6 To monitor the progress of the rebuild, review the ***Status*** page. If you find any errors, check the Windows Application Event Log. The ***Status*** page in the following figure shows the progress of rebuilding a table with forced synchronization selected.

After you have rebuilt your Additional Fields Table, the Current Additional Fields Table shows the rebuilt table.

Ignore the *iAdditionalID* and *iFileID* fields, which 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 14. Additional Fields Table Data Type 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 in their entirety 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 will only show the first 80 characters of these varchar fields. The actual fields within Point screens, other than reports, always show the entire field length that is stored in the Point file.

Related information

See *Point Knowledge Base article #0061,* ***Searching for 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 when no users are using Point so it is necessary to perform forced synchronization operations after hours. It is not necessary to force synchronize both Custom and Additional tables. Only one is needed.

Use the following steps to perform a forced synchronization:

1. Verify that all users have exited Point.
2. Access PointCentral and change the security key (***Configuration > Parameters***) to prevent user access so no users can interrupt the synchronization process.
3. Restart the CalyxPDSFilesync service and check the Application Event Log for errors to ensure proper PointCentral operation before starting the synchronization and reduce problems during the synchronization process.
4. In PointCentral, go to ***Configuration > Point Fields > Custom Fields***.
5. Select the **Full Synchronize (Forced) of all PDS Accelerated Folders after rebuilding Custom Field Table** check box and click the **Rebuild Custom Fields** button.
6. Go to ***Configuration > Point Fields > Additional Fields***.
7. Leave the **Full Synchronize (Forced) of all data folders after rebuilding the Additional Fields Table** check box checked and click the **Rebuild Additional Fields** button.

   It takes approximately one minute to sync 1000 loan files, you can monitor the ***Status*** page for completion.
8. Return the security key back to the original setting.

   Users are allowed to use to Point.

Restoration procedure 7

To prevent loss of data in the event that there is a hardware failure where your database and server are stored, you should perform regular server and data back ups to an external hard drive storage location. You can use any third-party software application that is capable of interacting with SQL database.

Prerequisite

Before you can begin the back up, exclusive access to the SQL database is required.

In this topic

Stopping PointCentral applications

To access the database:

1. Open a command prompt dialog box in Microsoft Windows.
2. Type *iisreset /stop*, then press the <Enter> key.

   This command stops the administration site and the web service.
3. Type *net stop CalyxPdsFileSync* and press the <Enter> key.

   This command stops FileSync.

Recommendation

It would be a good idea to perform backups during non-business hours because Point users will not have access to PointCentral after the PointCentral applications are stopped.

Starting PointCentral applications

After the back up is finished, you must restart the PointCentral applications.

To restart the database:

1. Open a command prompt dialog box in Microsoft Windows.
2. Type *net start CalyxPdsFileSync* and press the <Enter> key.

   This command starts FileSync.
3. Type *iisreset /start* and press the <Enter> key.

   This starts administration site and the web service.

PointCentral is now ready to accept incoming connections from Point users again.

Restoring the SQL database

If something happens to your SQL database and you lose your data, you can easily restore it by using one of your backup files.

1 Stop PointCentral applications.

2 Start SQL Server Management Studio Express and log in.

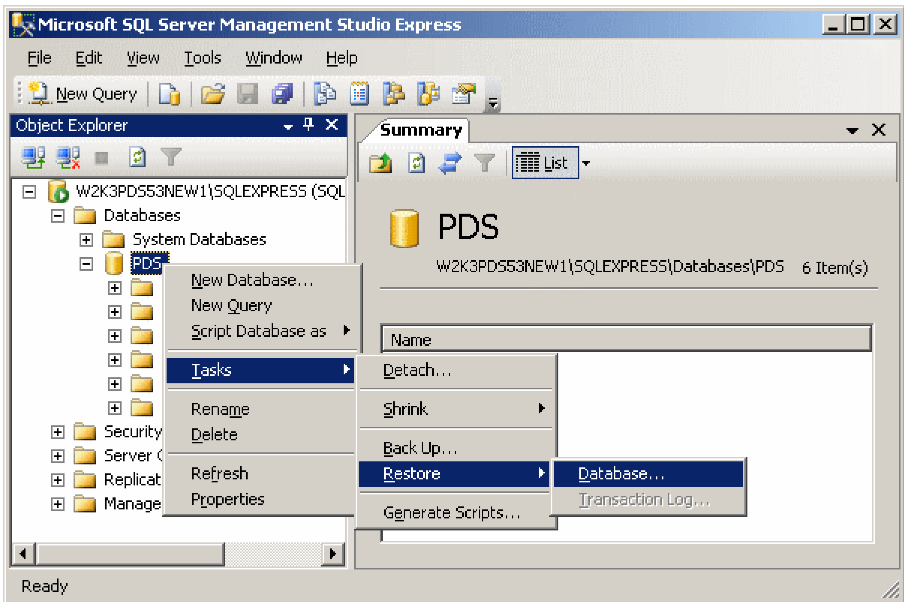


Figure 136. SQL Server Management Studio Express

3 Right-click the database name and select ***Tasks* > *Restore* > *Database***.

The **Restore Database** dialog box is displayed.

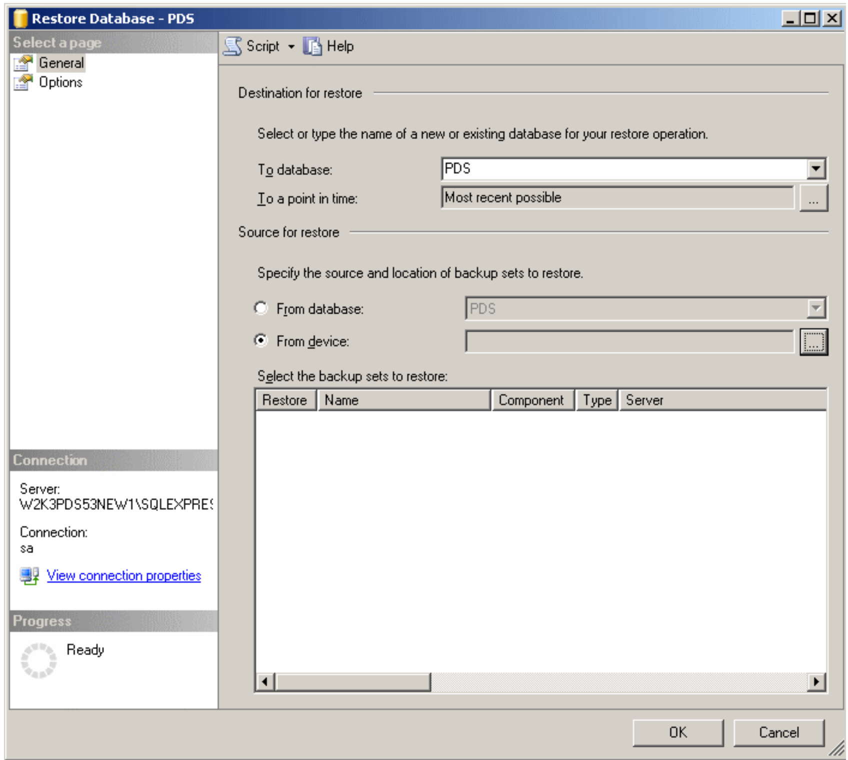


Figure 137. Restore Database

4 Under Destination for restore, select your database from the ***To database*** dropdown menu.

5 In the *Source for restore* section, click the **...** button next to the *From device* field.

The **Specify Backup** dialog box is displayed.

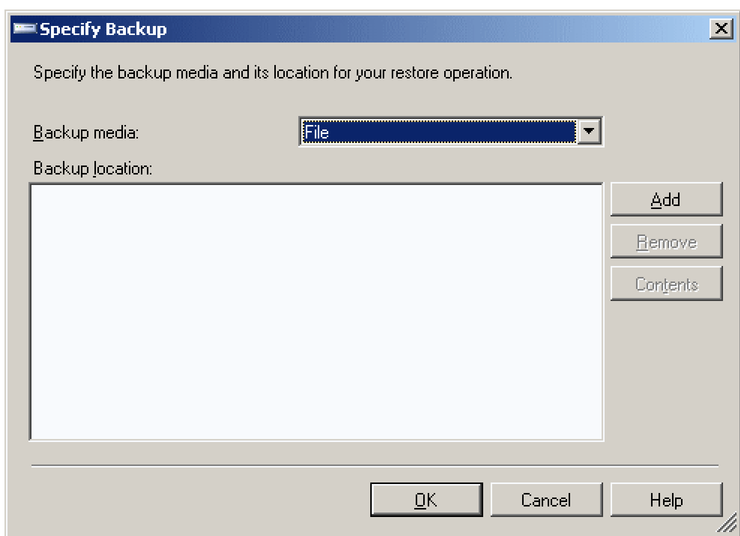


Figure 138. Specify Backup

6 Select *File* from the ***Backup media*** dropdown menu and click **Add**.

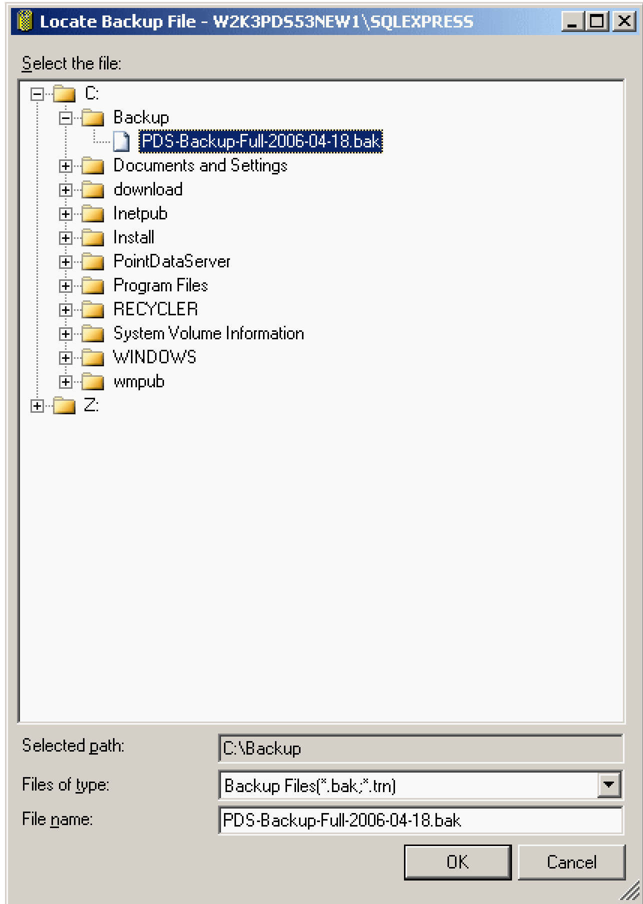


Figure 139. Locate Backup File

7 Navigate to the ***C:\Backup*** directory, select the most recent backup file, and click **OK**.

The backup location is added to the *Backup Location* field.

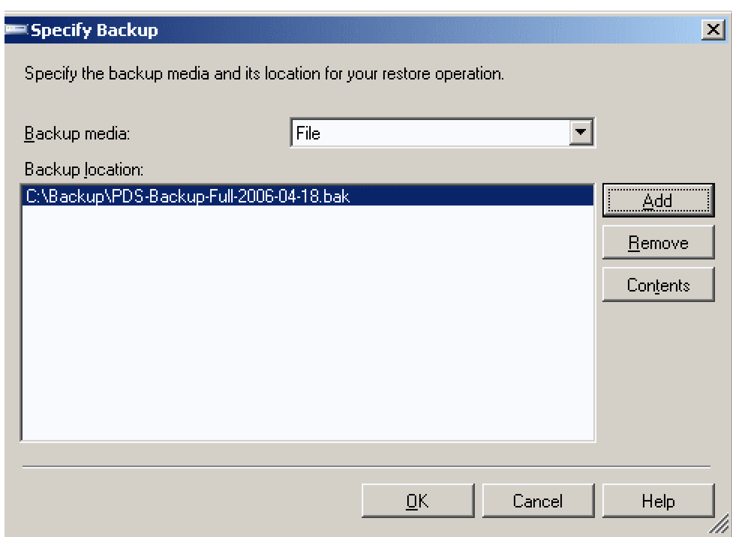


Figure 140. Specify Backup, with location

8 Verify that the path in the *Backup location* section is to your backup file and click ***OK***.

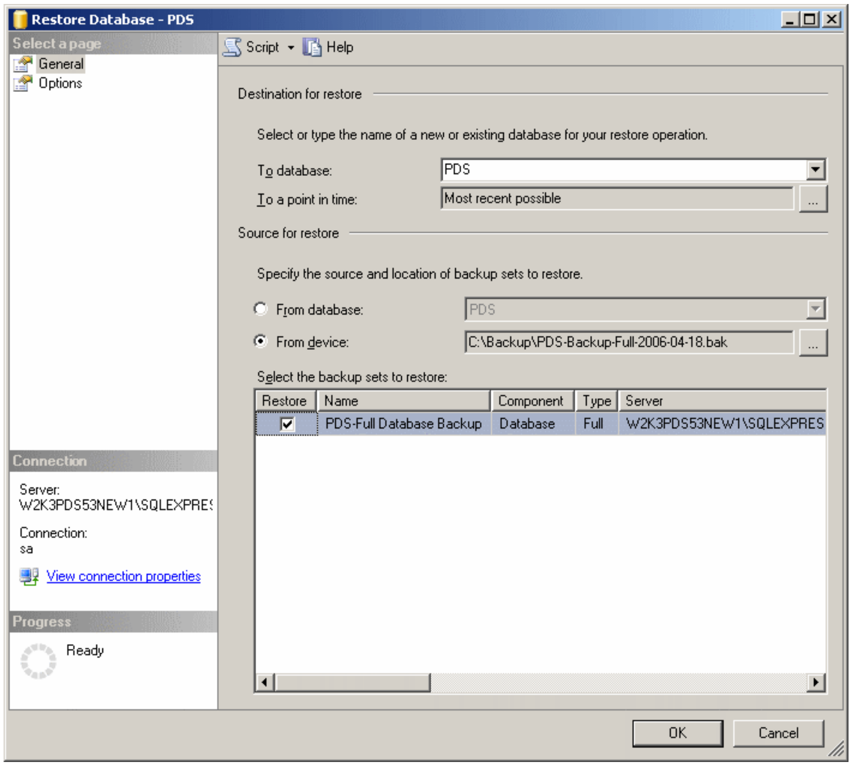


Figure 141. Restore Database

9 In the *Select the backup sets to restore* section, click the **Restore** check box. In the Select a page pane on the top left, click ***Options***.

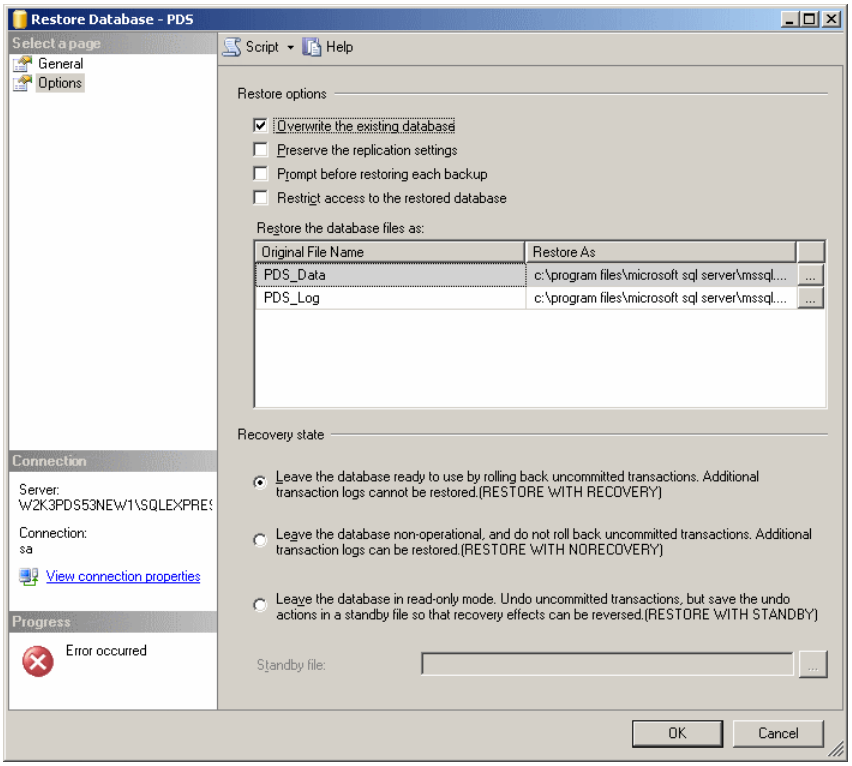


Figure 142. Restore Database, restore options

10 In the *Restore Options* section, select **Overwrite the existing database**, and click **OK**.

Important

The current database is overwritten with the database backup file. If your backup file is old and outdated, it is possible that some information will be lost.

If the restore fails, stop PointCentral applications.

After the database is restored, a confirmation dialog box is displayed.

Requirement

You must back up your database often. Frequent backups ensure that you can restore your system to a working state in the event of a failure. In addition, ensure that your backup files are copied to separate servers.

DNS and connectivity verification

A

If you encounter any problems with the installation and setup, refer to the information in this topic to verify that you have correctly installed and configured PointCentral and the required components.

Name resolution

Before you can configure PointCentral to allow incoming connections from Point clients, you must make sure that the Point clients are able to properly resolve PointCentral. If you are an experienced network administrator and you are sure all the computers that run Point can properly resolve PointCentral, you can skip this information.

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

One of the PointCentral components is the web service. This IIS web service accepts incoming connections from Point clients and processes them accordingly.

Name resolution helps users to identify servers and computers without having to remember IP addresses.

Name resolution with NetBIOS/WINS

One way to identify computers by name is by using the NetBIOS name.

To obtain your computer name:

1 Select ***Start > Control Panel***.

2 Double click the System icon.

The **System** dialog box is displayed.

The NetBIOS name (***PDS-SVR***) is located in the *Computer name, domain, and workgroups settings* section.

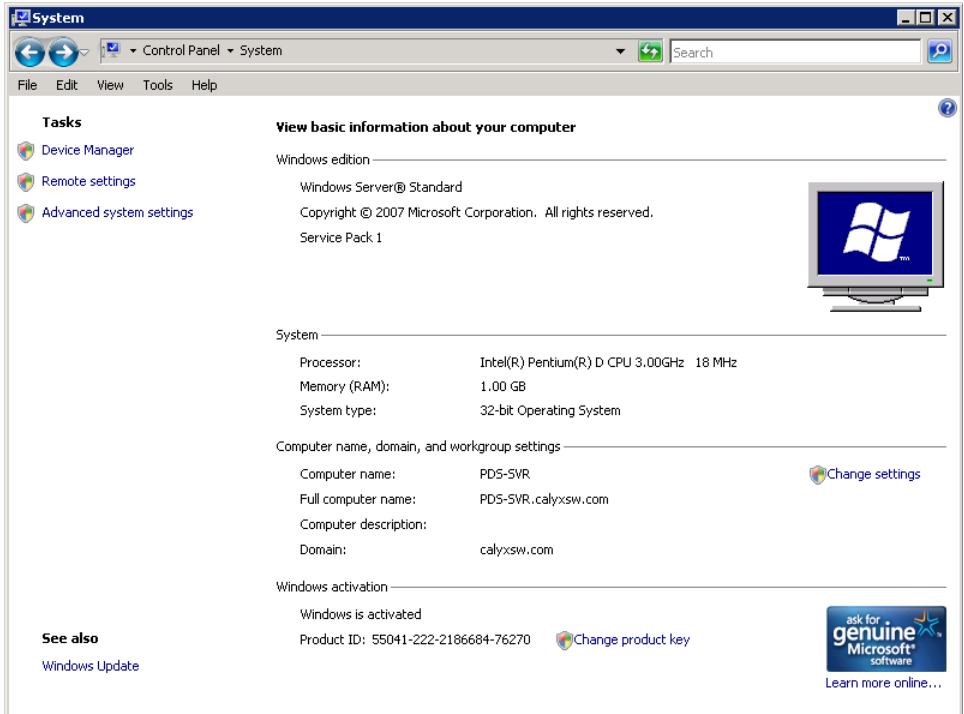


Figure 143. System dialog box

To verify if you can resolve your NetBIOS name:

1 Open a command prompt dialog box in Microsoft Windows.

2 Type *ping* and your computer name. For example, *ping PDS-SVR*.

If your computer is able to resolve the IP address of the name you tried to ping, the IP address will show in the result which will look similar to the following example:

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

When you ping your server, the name is automatically translated to its IP address. If the IP address is displayed, the computer name is properly resolved.

However, if you try to ping a computer name that does not exist or that is not properly set up on your network, the message *Unknown host MYSERVER* is dispalyed.

Important

The ping command will not work in some network configurations (for example, networks with certain firewalls).

If you try to ping a computer in an environment that does not allow the ping command, PointCentral is still resolved, however, the response to the ping will look something like the following example:

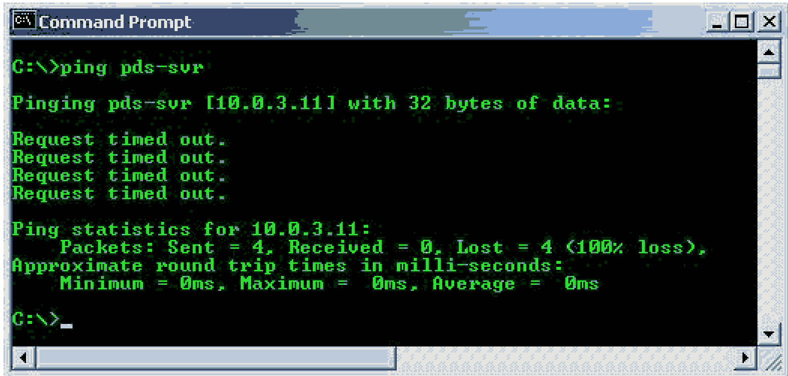


Figure 144. Ping request error example

Third-party tools are available to use to verify that 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

In some limited cases, such as setting up a test server in a lab with SSL certificates generated by your own SSL Certificate Authority, you might want to use NetBIOS names. But even in these cases, DNS is often preferred. Many certificate authorities only issue certificates for valid Internet DNS names. The bottom line when you use NetBIOS/WINS names is that you must make sure that the Point clients can properly resolve the server connection by using the HTTPS protocol (port 443). Contact your network administrator if these conditions are not met.

Name resolution with DNS

Another way to properly resolve computer names into IP address is DNS (Domain Name System). The Domain Name system (DNS) is a distributed Internet directory service that is used mostly for the following functions:

- Translating between domain names and IP addresses
- Controlling Internet e-mail delivery

Recommendation

DNS is the recommended method to use to configure your network for clients to resolve to PointCentral.

To make sure the PointCentral server can be resolved by using DNS, you must configure your DNS server. If you used the Domain Name and SSL Certificate Store to register your domain, DNS services are provided for you.

When you use DNS, you must ensure that the Point clients can properly resolve the PointCentral server connect by using the HTTPS protocol (port 443).

Regardless of how you set up your network or which method is used for your Point clients to resolve PointCentral (IP Address, NetBIOS/WINS name resolution, or DNS), Calyx makes certain assumptions. Throughout this information, when DNS name is used, it refers to the URL of the web service.

Firewall setup B

If your PointCentral server is behind a firewall or NAT router, and you want your users to be able to access it from the Internet, you will need to configure it so that it sends all incoming HTTPS traffic to PointCentral.

The PointCentral server requires that only port 443 be open for inbound traffic. This traffic must be forwarded to your PointCentral machine.

Create a rule that permits inbound connections on port 443 and forwards them to your PointCentral machine.

If you are not running a software firewall in addition to your hardware firewall, you should test that you can connect to your PointCentral machine by visiting your web service URL in your web browser.

If you have a software firewall, you might need to configure it to allow PointCentral traffic.

Web service errors and warnings

C

In some cases, the web service can return a warning or an error to the calling client. When you see the error, contact the Point System Administrator.

This topic contains the possible warnings and errors that can occur and potential solutions to help repair the problem. These errors should rarely occur, but if you report such a message, check the error code and follow the steps to address it.

Each message contains details about the warning or error, the error code, and instructions to the Point user to contact their system administrator for assistance.

When a warning occurs, the original request is completed.

When an error occurs, the list of results is empty. The only returned values are the error code and description.

In addition to the warnings and errors that are displayed to the Point user, the information is logged in the Event Log.

The following tables contain the possible warnings and errors and their possible resolution.

Code	Warning message	Resolution
-2	Warning: 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***, on page 158, for information about adding fields to the supported list of fields.
-3	Warning: 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. Refer to ***Web service parameters***, on page 64, for more information about how to change the MaxRecordsGetTasks default value.

Code	Warning message	Resolution
-4	Warning: 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. Refer to ***Web service parameters***, on page 64, for more information about how to change the MaxRecordsGetLoanApps default value.
-5	Warning: 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. Refer to ***Web service parameters***, on page 64, for more information about how to change the MaxRecordsGetCardexEntries default value.

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 the cause of the error. Pay particular attention to Application events with the source CalyxPdsService. If you cannot locate the cause in the Event Log, this is an Internal Error. In this case, record the exact details of the error and contact Calyx Support. Refer to ***Event log***, on page 10, for more information about viewing the Event Log.
-13	Point Data Server cannot retrieve parameters from the database.	Check that your SQL Server is properly configured and running and that your components database connection strings are correct. Use the PointCentral Configuration Wizard to update the connection strings. Refer to ***Configuring PointCentral***, on page 28, 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***, on page 158 for information about adding fields to the supported list of fields.
-15	Client internal error: The requested search type is currently not supported by Point Data Server	If this occurs, 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	If this occurs, 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.	If this occurs, verify the security key that was entered in the administration site matches the key entered in Point Administrator. This 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. This error can also occur if you are not finished running the PointCentral Configuration Wizard. Refer to ***PointCentral components configuration files***, on page 59, for more information about the Service configuration file.
-19	Client internal error: The array of folders passed to Point Data Server is invalid.	If this occurs record the exact details of the error and contact Calyx Support.
-20	Could not retrieve list from database.	Check that your database is properly configured and running and that your components database connection strings are correct. Use the PointCentral Configuration Wizard to update your connection string. If the database connection strings are properly configured, record the exact details of the error and contact Calyx Support. Refer to ***Configuring PointCentral***, on page 28, for information about the PointCentral Configuration Wizard. Refer to ***Administration site parameters***, on page 60, 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's password in the administration site.
-22	Log in failed. This account has reached the maximum number of log in attempts and it is temporarily disabled.	As a security measure, Point users are locked out of PointCentral after the maximum number of failed log 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 log in attempts and the lock out period. Refer to ***Unlocking users***, on page 72, for information about unlocking users. Refer to ***Setting the operational parameters***, on page 46, for information about accessing the parameters page and changing parameters.
-23	This version of Point Data Server only works with Point version 5.3 and above.	Message displayed to a Point 5.0 client that attempts to connect to Point Data Server v5.3. Upgrade the client to Point 5.3.
-24	Could not update password, the new password did not pass the minimum security requirements.	Specify a different password that adheres to the following criteria: • 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).

Code	Error message	Resolution
-25	The lender loan ID cannot be empty.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-26	Requests are only accepted through Secure Socket Layers (SSL).	Internal Error. If this occurs, 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. This can occur if a change is made to a user's access rights 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 properly working. The Point user should never see this message. If this occurs, record the exact details of the error and contact Calyx Support.
-29	Invalid file setting name; it cannot be empty.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-30	Invalid file setting ID; it could not be found.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-32	Invalid setting file name; it must end in .INI or .CSF.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-33	Could not find given file Setting ID for given Folder ID.	Internal Error. If this occurs, 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. This can occur if a change is made to a user's access rights 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. Refer to ***Data folder access rights***, on page 78, for information about establishing and updating user folder access rights.
-36	NetBios client name is blank.	Internal Error. If this occurs, 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. Refer to for ***Deleted reservations***, on page 57, for information about deleting loan reservations.
-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. Refer to ***Name resolution***, on page 169, for information about the IIS anonymous user.
-39	Could not save loan, the reservation does not exist.	Refer to for ***Reservations***, on page 54, for information about loan reservations.
-40	Could not save loan, the reservation belongs to another user.	Refer to for ***Reservations***, on page 54, for information about loan reservations.
-41	Could not save loan, the reservation was made from a different computer.	Refer to for ***Reservations***, on page 54, for information about loan reservations.
-42	Could not save loan, the PDS internal queue that saves loans is unavailable.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.

Code	Error message	Resolution
-43	Could not save loan, at least one file to be saved or deleted must be supplied.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-44	Could not release loan reservation, only the original User may do so.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-45	Could not release loan reservation, it no longer exists.	Internal Error. If you are running SQL on a different server than PointCentral, check the date and time on both servers and ensure that they are congruent. If this does not resolve the problem, record the exact details of the error and contact Calyx Support.
-46	Folder access rights not defined for given User ID.	The Point user does not have the proper access rights to the folder. You can change the folder access rights for the user. Refer to ***Data folder access rights***, on page 78, for information about establishing and updating user folder access rights.
-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. Someone might have changed the auto file naming rules for a folder 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. Someone might have changed the auto file naming rules for a folder 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.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-52	Invalid request when saving new file; file already exists.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-53	Invalid request when saving new file; could not create reservation.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-54	Could not find file.	The requested file no longer exists. This could occur if a file is changed or deleted from PointCentral while a Point user had an obsolete list of files displayed on their screen.
-55	Only the main borrower loan file (with the 'BRW' extension) can be used in this operation.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-57	When getting or saving a task file, file name must end with the '.TSK' extension.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-58	Requested TSK file not found.	The requested file no longer exists. This could occur if a file is changed or deleted from PointCentral while a Point user had an obsolete list of files displayed on their screen.

Code	Error message	Resolution
-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. Refer to for ***Deleted reservations***, on page 57, 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. Refer to ***Data folder access rights***, on page 78, 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. If a change makes a change to the auto file naming rules of a data folder while a Point user is logged in, this error could occur.
-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. Refer to ***Data folder access rights***, on page 78, 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. Refer to ***Data folder access rights***, on page 78, for information about establishing and updating user folder access rights.
-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. Refer to ***Data folder access rights***, on page 78, 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. Refer to for ***Deleted reservations***, on page 57, for information about deleting loan reservations.
-66	Could not copy file to destination folder; the destination file already exists.	Internal Error. If this occurs, 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. Refer to for ***Deleted reservations***, on page 57, for information about deleting loan reservations.

Code	Error message	Resolution
-68	Could not generate auto filename. Make sure the maximum number of unique filenames generated for the given period has not been reached.	Verify your auto file name rules in the administration page. Refer to ***Users and user groups***, on page 67, for information about auto file naming.
-69	Your computer's date and time are more than 24 hours out of date relative to the Point Data Server (PDS). PDS security requires that your computer's date and time are accurate.	For security reasons, 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 that 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 that the files in the data folders in PointCentral are not marked as read-only (in the file system).
-72	The source file is marked as read-only on the PDS Server; it cannot be moved.	Verify that 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. Refer to ***Configuring PointCentral***, on page 28, for information about the PointCentral Configuration Wizard.
-75	There are no template set access rights defined for this user.	Define access rights for the user for a template set as needed. Refer to ***Specifying user and user group template set access rights***, on page 100, 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 needed. Refer to ***Rebuilding template sets***, on page 104, for information about rebuilding template sets and ***Configuring PointCentral***, on page 28, 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 needed. Refer to ***Rebuilding template sets***, on page 104, for information about rebuilding template sets and ***Configuring PointCentral***, on page 28, for information about the PointCentral Configuration Wizard.
-78	The requested template file has not changed.	Internal Error. If this occurs, 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 needed.
-80	Invalid template file type or template file name; when updating a template file neither can be empty.	Internal Error. If this occurs, 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 that 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.	Internal Error. If this occurs, 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 needed. Refer to ***Specifying user and user group template set access rights***, on page 100, 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. Refer to for ***Deleted reservations***, on page 57, for information about deleting loan reservations.
-85	Wrong function called for given template type. The given template file type does not require a reservation.	Internal Error. If this occurs, 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 needed. Refer to ***Specifying user and user group template set access rights***, on page 100, 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. Unless there's a problem with the Point client this should never happen.
-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.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-91	Invalid request when saving new template file; could not create reservation.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, 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.	Internal Error. If this occurs, record the exact details of the error and contact Calyx Support.
-96	Could not save cardex record: it's empty. At least one field value must be entered.	Enter at least one value in the Cardex record before saving it to PointCentral.

Code	Error message	Resolution
-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: .	Internal error, should never happen.
-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 which was larger than the maximum template file size allowed. Refer to ***FileSync parameters***, on page 62, for information about the MaxTemplateFileSizeKB parameter.
-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 your password per the guidelines established in your 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 your Point System Administrator.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z @ #

E

F

G

H

I

L

M

S

T

U

V

W

Symbols