Planview ChangePoint

Installation Guide

Planview ChangePoint 2022

Version 1.9

Document version history

Version	Updates	Date
1.0	Initial version	2022-01-31
1.1	• Updated procedure for installing and upgrading Intelligent Forms. • Updated procedure for identifying test and training environments	2022-02-15
1.2	• Added MaxIncomingWebSocketMessageSize setting in the `WebSockets\Web.config` file.	2022-03-31
1.3	• Added settings for SMTP authentication in the ChangePoint Mail service configuration file. • Updated ChangePoint product name and logo.	2022-09-30
1.4	Added installation and configuration information for the ChangePoint OData service.	2022-12-16
1.5	Added cross-reference to ChangePoint Administration for managing authentication tokens for the OData service.	2022-12-20
1.6	• Removed installation information for the ChangePoint OData service, which is automatically installed. • Updated upgrade notes for Cognos Analytics 11.2.3.	2023-01-31
1.7	Added instructions for upgrading Infiniti to SmartIQ (Intelligent Forms).	2023-05-05
1.8	• Added new Web.config file parameters for increasing the number of daily and fiscal time periods displayed in Resource Planner. • Added configuration parameter for enabling SSL to the ChangePoint Mail Service.	2023-07-31
1.9	Added new AlwaysUseFromAddress setting to the `CPMail.exe.config` for the ChangePoint Mail Service.	2023-10-31

Contents

1. Installation Requirements and Preparation

Introduction

The document provides instructions for installing and upgrading to the 2022 release of ChangePoint.

Some of the information in this document is for the ongoing maintenance of a ChangePoint installation.

ChangePoint components

A minimal ChangePoint installation consists of the following required components:

- database (ChangePoint database, CPTempDB, CPExtended, InfinitiDB)

- website

- scheduled jobs

- Redis (third-party caching component)

Optional applications, features, and services include ChangePoint software and third-party software.

About the secondary databases

CPTempDB and CPExtended are secondary databases that are on the same server as the main ChangePoint database, and are installed automatically when you install the ChangePoint database using the installer.

CPTempDB provides dedicated temporary storage and processes transient, session-based data and code. By design, the CPTempDB database is created using Simple Recovery Mode to minimize log space requirements. The session-based architecture virtually eliminates the need for dynamic SQL and schema level locks, thereby drastically minimizing time consuming recompilation within the SQL Server.

CPExtended provides storage for logging error messages and performance data as well as background job scheduling and management.

InfinitiDB is the storage location for Intelligent Forms. The database stores the forms as well as the administration and configuration data.

File path conventions

Throughout this document, the following conventions are used for common paths:

Convention	Meaning
<cp_root>	The root path of the ChangePoint installation. The default is: C:\Program Files (x86)\Changepoint\Changepoint\
<cp_common>	The root location for common ChangePoint utilities, such as the Login Settings utility. The default is: C:\Program Files (x86)\Common Files\Changepoint\Changepoint\

Note: The Login Settings utility is installed in

`C:\Program Files\Common Files\Changepoint\Changepoint\LoginSettings\`

regardless of the root folder for ChangePoint installation.

ChangePoint documentation

This guide contains references to the following documentation, which is available from the Customer Success Center (https://success.planview.com/Planview_Changepoint), team folders in Client Portal, or from your client manager:

- *ChangePoint Software Compatibility Matrix*

- *ChangePoint Hardware Recommendations Guide*

- *User Basics User Guide*

- *ChangePoint API Installation Guide*

Unless stated otherwise, use the version of the documentation that corresponds to your ChangePoint installation.

Hardware and software requirements

ChangePoint server software can be deployed on a single server or on multiple servers.

Ensure that each server meets the following requirements:

- hardware requirements in the *ChangePoint Hardware Recommendations Guide.*

- software requirements in the *ChangePoint Software Compatibility Matrix*

   Warning: If the servers do not meet the hardware and software requirements, the installation might fail silently.

Temporary license for Intelligent Forms

You require a new Intelledox Infiniti Manage license key for Intelligent Forms due to changes to the license management component,.

You must first contact your customer support manager to obtain a temporary license file for Intelledox Infiniti Manage, which is to be applied on a test environment. From there, you can initiate the process to obtain a valid license file. For more information, see "Configuring Intelligent Forms" on page 130.

Required skills

To install ChangePoint, you must be familiar with administering the following software:

- Microsoft SQL Server

- Microsoft Windows Server

- Microsoft Internet Information Services (IIS)

- .NET

If you do not have these skills, or require assistance with implementing ChangePoint, contact your ChangePoint client services representative or client manager.

Latest patches and service packs

Check the **ChangePoint 2022 Releases** section in the Customer Success Center (https://success.planview.com/Planview_Changepoint) or team folders in Client Portal, for service packs and for general patches that have been posted for this release.

You install service packs and general patches according to the instructions in the service pack or patch release notes.

Required accounts and permissions

You require the following credentials on each host:

- All servers – local or domain administrator account

- The user account running the SQL server service must have write permission to the ChangePoint data and log folders.

- Database server:

- SQL administrator (sa) account, which is required to install and configure the ChangePoint database

- SQL account, which is required for the ChangePoint applications to access the database. If the SQL account does not already exist on the SQL Server, an account is created with the same password as the user ID during installation. Be sure to configure this account with an appropriate password.

Notes about the SQL account:

- Create the SQL account with default settings and permissions.

- *Do not* use "Changepoint" as the user ID for the account.

- *Do not* give the sysadmin role to the account. During the ChangePoint installation, the SQL account will be configured with "DBO" as the default schema against ChangePoint databases, and later during the ChangePoint Analytics installation, with the "Changepoint" schema against the content store database.

Installation considerations

Installation using Remote Desktop Protocol (RDP)

In the RDP dialog, set the connection to Highest Quality:

Remote Desktop Connection > Display > Colors

Otherwise installation fails with the message:

```
"Error Number: 0x80004005 Description: Unspecified error Setup will now
terminate"
```

Enabling enhanced session management

Keep the following points in mind if you plan to enable enhanced session management, which restricts authenticated users to one active session per browser container.

- Web server name

- Client Portal website

- Mobile access to ChangePoint

- Naming constraints for the web server name – ensure that the web server name does not contain an underscore, otherwise client workstations need to connect to the server using the IP address instead of server name to log into ChangePoint.

Perform a backup

To prevent data loss, back up each host before installation.

Install on a test environment first

It is strongly recommended that you install the ChangePoint database and applications in a test environment before installing in a production environment.

Required components on the web server

The following are required on the web server:

- You must enable the following roles/features on IIS:

  - NET Framework 3.5 Features

  - WebSocket Protocol

SQL Server services required

Before installing ChangePoint, ensure that the following SQL Server services are running on the database server:

- SQL Server (MSSQLSERVER)

- SQL Server Agent (MSSQLSERVER)

- SQL FullText Filter Daemon Launcher (MSSQLSERVER)

Installation parameters

Before you start installation, determine the values in the following table. You are prompted for this information during installation.

Information needed	Notes	Your installation value
Setup Language	• Dutch • English • French • German • Spanish	
New Instance, or Maintain or update an existing instance		
Setup type	**Complete** – installs the entire ChangePoint application including the database files, website files, and tools on a single server. This is the recommended option for a new installation when all features will be installed on a single server. **Database Only** – Installs the required database files and scheduled jobs. The Login Settings utility is also installed. **Website Only** – Installs and configures only the web application files. Use this option to install the web application files on a separate server from the SQL database. **Custom** – Installs the features that you select. **Note:** For an upgrade, the features are preselected based on the previous installation. Clearing the check box of a feature uninstalls the feature from the machine.	
Destination folders for application files		

Information needed	Notes	Your installation value
Destination Location (root folder for installation)	Default: `C:\Program Files (x86) \Changepoint\Changepoint\` Referred to throughout this document as `<cp_ root>`.	
Destination Location (ChangePoint web application files)	Default: `<cp_root>\Enterprise\`	
Destination Location (Intelligent Forms web files)	Default: `<cp_root>\Intelligent Forms\Websites\`	
Destination Location (Web Services API files)	Default: `<cp_root>\API\CP Web Services\`	
Destination Location (Redis cache service)	`<cp_root>\Redis\` `Note:` The Redis cache service will use "redisservice" as the service name and 6379 as the port number. If either is already in use, the Redis service install and startup will fail. Refer to the RedisCacheService.log file under the ChangePoint InstallLog folder for details. You will need to perform manual steps to install and start the Redis service with a unique service name and port number. For more information, see "Installing and Configuring Redis" on page 33.	
Website names and ports		
Name and port for the ChangePoint website	Default: Enterprise, 8080 **Note:** The name and port must be dedicated to the ChangePoint website.	

Information needed	Notes	Your installation value
Name of the Intelligent Forms application pool	Default: CPInfiniti	
ChangePoint URL	URL, including the protocol (http or https) for end users to access ChangePoint.	
Destination locations for database files		
Destination Location (Changepoint.mdf database file)	Default: `<cp_root>`\Database\Data\	
Destination Location (Changepoint2.ndf database file)	For best performance, select a dedicated I/O channel (LUN, RAID set or physical disk) for each of the file types (.mdf, .ndf, and .ldf) If only three channels are available, you can put the log and tempdb on the same channel.	
Destination Location (Changepoint3.ndf database file)		
Destination Location (Changepoint4.ndf database file)		
Destination Location (database log file)	Default: `<cp_root>`\Database\Log\	
Destination Location (Intelligent Forms database file - InfinitiDB.mdf)	Default: The same location as the Changepoint.mdf database file.	
Destination Location (Intelligent Forms database log file - InfinitiDB.ldf)	Default: The same location as the ChangePoint database log file.	
Database login information		

Information needed	Notes	Your installation value
Database server	Select the SQL Server name where the ChangePoint database will be installed.	
Login ID (SQL Server)	sa	
Password (SQL Server)	password for the sa account	
Database Name	Recommended default: Changepoint	
User ID for the SQL account that will be used for the database connection	Used in the Login Settings (Connection settings) setup.	
Intelligent Forms database name	Recommended default: InfinitiDB	
Mode		
Mode	• PSO – ChangePoint SA (Services Automation) • ITD – ChangePoint PPM (Project Portfolio Management)	

2. Installing Required ChangePoint Components

Installing ChangePoint using the installer

The installer sets the Anonymous Authentication Credential to use Application Pool Identity. The ChangePoint website is assigned to its own application pool (*sitename_*AppPool).

1. Copy the contents of the ChangePoint product media to a location on the server.

2. Run the `setup.exe` file from the copied location.

   The Changepoint 2022 window opens.

3. On the **Changepoint** tab, click the **Install Changepoint 2022** link.

4. At each prompt, select or type the appropriate parameter from the table in "Installation parameters" on page 19, and click **OK** or **Next** to move to the next prompt.

5. After you select the **Changepoint Application Mode**, click **Next**.

   The **Start Copying Files** screen appears.

6. Review the current settings to ensure all information is correct.

7. If correct, click **Next** to continue with the installation.

   When installation is complete, the **InstallShield Wizard Complete** screen displays.

8. To review the installation log for any errors or warnings, select **I would like to open the Installation Log file**. The installation log file provides details about the issues that were encountered and possible remedies that you can apply manually after the installation.

9. To run the Login Settings utility after the installation, select **I would like to launch Login Settings (Connection Settings)**. This utility is used to configure and encrypt the connection settings for security purposes. At this time, you can configure the connection settings for:

   • ChangePoint

   • Enterprise\global.asa

   • Enterprise Report Server\global.asa

   • Enterprise\WebAPI\web.config

   • Enterprise\WebSocket\web.config

- Intelligent Forms\Websites\IntelledoxSchedulerIntelledoxScheduler.exe.config

- Intelligent Forms\Websites\ChangepointDataService\web.config

- Intelligent Forms\Websites\Manage\web.config

- Intelligent Forms\Websites\Product\web.config

Note: For new ChangePoint installations, the Intelligent Forms web.config files are preconfigured

- API\CP Web Services\web.config

- the executables associated with ChangePoint scheduled jobs

See "About configuring database connection settings" on page 65 for instructions.

10. To install additional instances of ChangePoint on this server, see "Installing multiple ChangePoint instances" on page 26.

11. Configure Redis. For more information, see "About Redis" on page 33

12. Complete the post-installation instructions.

    For more information, see "Configuring ChangePoint" on page 49.

Installing multiple ChangePoint instances

You can run the installer multiple times on the same servers to install multiple ChangePoint websites and databases.

A common scenario for creating multiple databases on a server is setting up training and test environments. For more information, see "Creating a Test and Training Environment" on page 187.

Note the following:

- The ChangePoint website names and database names must be unique for each instance on the server.

- The port number for each ChangePoint website on the server must be unique.

- Scheduled jobs are created for each database with the database name prepended to the job names.

- You must configure the database access settings for the appropriate database and the applicable .exe jobs

- Because you can install only one instance of each Changepoint Windows service on a server, you must set up each Windows service instance for each database on a separate server.

- Windows service instances for each database after the first must be set up on separate servers.

1. Install the first website instance using the procedure described in "Installing ChangePoint using the installer" on page 25.

2. Run the `setup.exe` file again.

   The **Changepoint 2022** window opens.

3. On the **Changepoint** tab, click the **Install 2022** link.

   The **Existing Installed Instances Detected** screen displays.

4. Select the **Install a new instance** option, and then click **Next**.

5. The remaining steps are the same as the standard procedure for installing using the wizard.

   Note: Be sure to change the service name and port number for the additional Redis service from the default values or the install and startup will fail. Refer to the RedisCacheService.log file under the Changepoint InstallLog folder for details. You will need to perform manual steps to install and start the Redis service with a unique service name and port number. For more information, see "Installing and Configuring Redis" on page 33.

Modifying a ChangePoint instance

To add or remove features, use the Windows Control Panel, or run the InstallShield Wizard again on an installed ChangePoint instance.

Note: You must use SQL Server Management Studio to remove a database.

Modifying ChangePoint using the InstallShield Wizard

1. Run the `setup.exe` file again.

   The **Changepoint 2022** window opens.

2. On the **ChangePoint** tab, click the **Install Changepoint 2022** link.

The **Existing Installed Instances Detected** screen displays.

3. Do the following:

    a. Select the **Maintain or update the instance of this application selected below** option.

    b. Select the instance that you want to modify from the list of instances.

    c. Click **Next**.

    The **Welcome** screen appears.

4. Select the **Modify** option and click **Next**.

    The **Select Features** screen displays.

5. Do the following:

    • To install a feature, select the check box.

    • To remove a feature, clear the check box.

6. The remaining steps are the same as the standard procedure for using the wizard.

Uninstalling a ChangePoint instance

You can uninstall ChangePoint using the Windows Control Panel, or the InstallShield Wizard.

Note: All features are removed except the database. To remove the database you must use SQL Server.
If you uninstall ChangePoint after an upgrade, the previous installation of ChangePoint is not restored.

To uninstall a ChangePoint instance using the InstallShield Wizard

1. Run the setup.exe file.

    The **Changepoint** window appears.

2. On the **Changepoint** tab, click the **Install Changepoint** link.

    The **Existing Installed Instances Detected** screen appears.

3. Do the following:

      a.   Select the **Maintain or update the instance of this application selected below** option.

      b.   Select the instance that you want to uninstall.

      c.   Click **Next**.

      The **Preparing Setup** screen appears, followed by the **Welcome** screen.

4.   Select the **Remove** option, and then click **Next**.

5.   Click **OK** to confirm.

6.   Click **Finish**.

Installing the ChangePoint database manually

When you install the database manually, you must also install the scheduled jobs, CPTempDB, and CPExtendedDB.

The default name of the CPTempDB database is: <Changepoint database name>_CPTempDb, and the default location is the location of the ChangePoint database files (mdf, ldf). However, you can specify a different name and location, if necessary.

1.   Review "Destination locations for database files" on page 22.

2.   Copy the following database files for the appropriate language from the ChangePoint product media to the target locations on the database server:

```
\Changepoint\Manual Install\New Database\<language>\Changepoint.mdf
\Changepoint\Manual Install\New Database\<language>\Changepoint2.ndf
\Changepoint\Manual Install\New Database\<language>\Changepoint3.ndf
\Changepoint\Manual Install\New Database\<language>\Changepoint4.ndf
\Changepoint\Manual Install\New Database\<language>\Changepoint_log.ldf
```

Ensure that the newly copied files are read-write.

3.   From the ChangePoint product media, copy the files from the following folder:

```
\Changepoint\Manual Install\New Database\
```

to:

```
<cp_root>
```

Note: For the remaining steps in this procedure, use the files in the destination folder. After installation is complete you can delete the files in the destination folder.

4.   Connect to the database server using the SQL server `sa` account or equivalent:

      a.   Manually attach the Changepoint database to the server..

      b.   If the database name is not "Changepoint", replace "Changepoint" with the database name.

5.   Execute the following:

- `Exec DBM_EnableSQLDependency 'webconfiguser'`

- `Exec DBM_SetupCPTempDB`

- `Exec DBM_SetupCPExtended`

- `Exec DBM_SetupFullText`

Installing the scheduled jobs manually

1.   Execute the following against the Changepoint database to set up scheduled jobs:

```
Exec DBM_SetupScheduledJob
```

2.   Do the following:

      a.   Copy the Login Settings utility (`Login Settings.exe`) from:

`<cp_root>\Manual Install\Components\LoginSettings\`

to:

`<cp_common>\LoginSettings\`

      b.   Run the Login Settings utility on the configuration files to configure the database connection settings:

- Enterprise\global.asa
- Enterprise Report Server\global.asa
- Enterprise\WebAPI\web.config
- Enterprise\WebSocket\web.config
- API\CP Web Services\web.config\web.config

      c.   Run the Login Settings utility on `CPEffectiveDates.exe.config` to configure the database connection settings.

      d.   Run the Login Settings utility on `CPGuestLicenses.exe.config` to configure the database connection settings.

For more information on the Login Settings utility, see "About configuring database connection settings" on page 65.

Installing the Infiniti database manually

When you install the Changepoint database manually, you must also install the Infiniti database manually.

The default name is InfinitiDB, and the default location is the location of the Changepoint database files (mdf, ldf). You can specify a different name and location, if necessary.

1. Review the destination locations for database files in "Installation parameters" on page 19.

2. From the ChangePoint product media:

    a. Copy the following files to the target locations on the database server:

        ```
        \Changepoint\Intelligent Forms\Database\InfinitiDB.MDF
        \Changepoint\Intelligent Forms\Database\InfinitiDB.LDF
        ```

    b. Ensure the files are read-write.

    c. Copy the files from the `\Changepoint\Manual Install\New Database\Setup_ InfinitiDB.sql` folder to `<cp_root>`.

    d. Ensure that the .sql files are read-write.

    Note: For the remaining steps in this procedure, use the files in the destination folder.

    After installation is complete you can delete the files in the destination folder.

3. Connect to the database server using the SQL server `sa` account or equivalent.

4. Edit `Setup_InfinitiDB.sql` by replacing the following placeholder text with actual values from the Changepoint instance:

    *   @CP_DB_SERVER@ = SQL Server instance where Changepoint database resides

    *   @MDFPATH@ = Physical path to the InfinitiDB.mdf database file (for example, D:\SQL\Database\InfinitiDB.mdf)

    *   @LDFPATH@ = Physical path to the InfinitiDB.ldf database log file (for example, L:\SQL\Log\InfinitiDB.ldf)

    *   @CP_DATABASE@ = Changepoint database name (for example, Changepoint)

    *   @INF_DATABASE@ = Infiniti database name (for example, InfinitiDB)

- @CP_USERID@ = SQL account used for Changepoint connection set via the Login Settings utility

- @CP_PASSWORD@ = Password for the Changepoint SQL userid

- @WSAPI_URL@ = URL for the Changepoint Web Services API (for example, https://{changepoint_website}/CPWebService)

- @INF_URL@ = URL for the Intelligent Forms web application (for example, https://{changepoint_website}/Infiniti)

5. Execute `Setup_InfinitiDB.sql`.

6. Configure Intelligent Forms. For more information, see "Configuring Intelligent Forms" on page 130.

3. Installing and Configuring Redis

About Redis

Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker. Redis also supports master-slave asynchronous replication and optionally provides high availability with Redis Sentinel.

Redis is designed to be accessed by trusted clients inside trusted environments. Therefore, the Redis instance must not be exposed directly to the Internet or to an environment where untrusted clients can directly access the Redis TCP port. Redis should be directly accessible only by authorized operators, and the computers that implement the application that uses Redis.

While Redis does not implement Access Control, it does provide a simple layer of authentication that you can enable by editing the `redis.windows.conf` file. When the authentication layer is enabled, Redis will refuse any query by clients that are not authenticated. A client can authenticate itself by sending the AUTH command followed by the password.

The goal of the authentication layer is to optionally provide a layer of redundancy. If firewalls or any other system that was implemented to protect Redis from external attackers fail, an external client will still not be able to access the Redis instance without providing the authentication password.

About installing the Redis server

The ChangePoint installer automatically creates a new Redis Server instance that is preconfigured for a single web server deployment. The installer also creates a new Redis service instance that has a temporary authentication password and is linked one-to-one with the ChangePoint website instance that is being installed or upgraded on the web server.

The startup configuration for the Redis Server is in the `redis.windows.conf` file in the Redis Server folder, and the corresponding Redis cache settings are in the `web.config` file for the website.

The following are the default settings for the Redis service:

- name – RedisService

- port – 6379

- authentication password is required (temporary password is provided)

Warning: It is highly recommended that you use a strong password that is unique to your organization. For more information about the importance of using a strong password, see the `redis.windows.conf` file.

Note: This guide includes the basic information that is required to install and configure Redis for use with ChangePoint. For more information, see the Redis website at https://redis.io/.

Multiple web servers

If you are setting up multiple ChangePoint website instances that are load balanced across multiple web servers, then the Redis Server installed and preconfigured with the default service name, port, and authentication password on each instance. You must designate a master server and configure the remaining server instances as slave servers.

Common Redis commands

Use these commands for Redis service installations.

Installing the Redis service manually

```
redis-server --service-install redis.windows.conf --service-name RedisService --port
6379
```

The service is configured as Autostart and will be launched as "NT AUTHORITY\NetworkService". Upon successful installation, a success message is displayed and Redis exits. Redis will listen on the specified port number.

This command does not start the service.

Uninstalling the Redis service

```
redis-server --service-uninstall --service-name RedisService
```

This command removes the Redis service configuration information from the registry. Upon successful uninstallation, a success message is displayed and Redis exits.

This command does not stop the service. To remove the service completely, stop the service first.

Starting the Redis service

```
redis-server --service-start --service-name RedisService
```

This command starts the Redis service. Upon successful startup, a success message is displayed. You can also start the service by using the Services dialog or the net start command.

Stopping the Redis service

```
redis-server --service-stop --service-name RedisService
```

This command stops the Redis service. Upon successful termination, a success message is displayed and Redis exits. You can also stop the service by using the Services dialog or the net stop command.

Naming the Redis service

```
--service-name name
```

This parameter can be used with any of the preceding commands to set the name of the installed service. This command is required if you plan on deploying multiple instances (for example, development, test, production) of ChangePoint on the same server because each ChangePoint instance requires a separate Redis instance. If there are only one instance of the ChangePoint website on the machine, the service name change is not required.

Specifying the Redis server port

```
--port 6379
```

You can use this parameter to configure the port that Redis listens on. If you do not configure a port, Redis uses the port that is specified in the `redis.windows.conf` file (default port is 6379). If you are accessing Redis from an external machine you must ensure that a firewall exception exists.

Single web server deployment

This configuration is set up by default when you use the ChangePoint installer to install or upgrade. A single web server deployment requires a single Redis master server, which is responsible for all requests (read/write).

You must do the following:

- Configure a single Changepoint web server: Web01

- Implement a single master Redis server with authentication enabled:

    - Redis service name: RedisService

    - Redis port: 6379

Note: To edit the Redis configuration file (`redis.windows.conf`), you require a text editor, such as Notepad++, that recognizes Unix-style line breaks. You cannot use Windows Notepad for this purpose.

1. Configure Redis authentication:

   a. Open the `redis.windows.config` and locate the following lines:

      ```
      requirepass 6ed18d5c7df443940...
      masterauth 6ed18d5c7df443940...
      ```

   b. Replace the temporary authentication password with a strong password that is unique to your organization. For more information see the note about `requirepass` in the configuration file.

   Warning: It is strongly recommended that you use a strong password that is unique to your organization. For more information about the importance of using a strong password, see the redis.windows.conf file.

2. Install the Redis Server as a service:

```
redis-server --service-install redis.windows.conf --service-name RedisService --port
6379
```

   After installation, the RedisService is available in the Windows Service Management Console.

3. Start the Redis Server service:

```
redis-server --service-start --service-name RedisService
```

   The Redis master server configuration is complete and ready to accept connections.

4. Configure the ChangePoint web site:

   a. In the ChangePoint `web.config` file, locate the following lines:

      ```
      <add key="cache.Password" value="6ed18d5c7df443940..." />
      <add key="cache.Servers" value="servername:6379" />
      ```

   b. Replace the values of the authentication password, server and port number as specified in the Redis configuration file.

   c. Repeat for the WebAPI web.config file.

   d. Repeat for the WebSockets web.config file.

5. Configure the global.asa file:

a. Locate the following lines:

```
Application("cache.Password") = "6ed18d5c7df443940..."
Application("cache.Servers") = "servername:6379"
```

b. Replace the values of the authentication password, server, and port number as specified in the Redis configuration file.

Multiple web server deployment, without high availability

A multiple web server deployment requires a Redis server to be designated as the Redis master, and all additional servers to be configured as Redis slave servers. In this type of environment, all read/write requests are directed to the master, and read-only requests preferably target a Redis slave server.

Note: With this configuration, if the master server goes down, then an operator must intervene manually to promote a slave server to the master role.

The process for configuring this sample deployment includes the following:

*   Two ChangePoint web servers:

    *   Web01 (Redis Master)

    *   Web02 (Redis Slave)

*   A single master Redis server with authentication enabled:

    *   Redis service name: RedisService*

    *   Redis port: 6379*

*   A single slave server Redis server with authentication enabled:

    *   Redis service name: RedisService

    *   Redis port: 6379

1. Configure Web01 as the Redis master server by following the procedure in "Single web server deployment" on page 35, but do not configure the ChangePoint web site.

2. Configure Web02 as the Redis slave server:

    a. Follow the procedure in "Single web server deployment" on page 35, but do not configure the ChangePoint web site.

    b. Navigate to the Redis installation path (default installation path is `<cp_root>\Redis`).

    c.   Configure Redis Replication. Open the `redis.windows.config` and locate the following lines:

```
# slaveof <masterip> <masterport>
# masterauth <master-password>
```

    d.   Uncomment the lines, and configure the replication parameters:

```
slaveof Web01 6379
masterauth 6ed18d5c7df443940...
```

Note: The passwords used for `masterauth` and `requirepass` must all be the same within a master-slave configuration.

3.   Install the Redis Service:

```
redis-server --service-install redis.windows.conf --service-name RedisService --port
6379
```

4.   Start the Redis Server service:

```
redis-server --service-start --service-name RedisService
```

The Redis slave server configuration is complete, and ready to accept connections.

5.   Configure the Changepoint web sites. Make the following edits to the web.config files on all web servers:

    a.   In the ChangePoint web.config file, locate the following line:

```
<add key="cache.Password" value="6ed18d5c7df443940..." />
```

    a.   Replace the value of the authentication password.

    b.   In the following line:

```
<add key="cache.Servers" value="Web01:6379;Web02:6379" />
```

    c.   Add the values for all of the Redis servers and their port numbers as specified in the Redis configuration file.

    d.   Make the same changes in the WebAPI `web.config` file.

    e.   Make the same changes in the WebSockets `web.config` file.

6.   Make the following edits to the `global.asa` files on all web servers:

    a.   Locate the following lines:

```
Application("cache.Password") = "6ed18d5c7df443940..."
```

```
Application("cache.Servers") = "servername:6379"
```

b. Replace the values of the authentication password

c. Add the values for all of the Redis servers and their port number as specified in the Redis configuration file.

Note: The cache.Servers value must contain all Redis servers and their defined listening ports, separated by semicolons. For example:

```
Application("cache.Servers") =
"Web01:6780;Web02:6781;Web03:6379;Web04:6379"
```

Multiple web server deployment with high availability

Using Redis Sentinel, you can create a Redis deployment that handles service outages without manual intervention. Redis Sentinel provides monitoring of the Redis deployments, and automatic failover when failures occur.

The high availability configuration is based on a multiple server deployment to which Redis Sentinel is added. Therefore the starting point is to create a multiple server deployment as described in "Multiple web server deployment, without high availability" on page 37. The following diagram outlines the deployment.
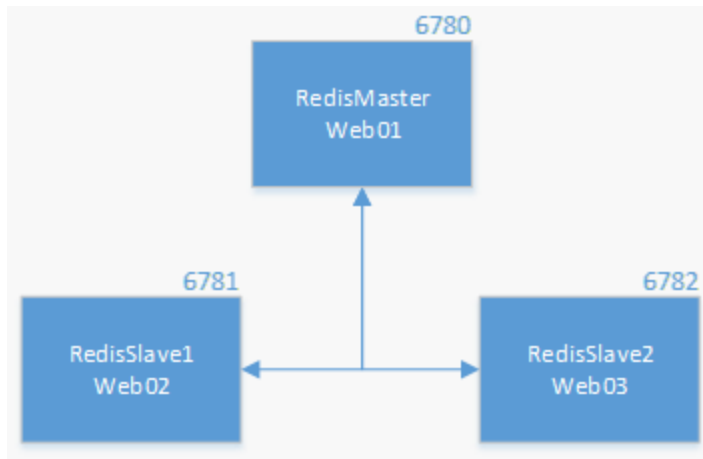
The process for configuring this sample deployment includes the following:

• Configure three Changepoint web servers:

 • Web01 (RedisMaster)

 • Web02 (RedisSlave1)

 • Web03 (RedisSlave2)

- Implement single master Redis server with authentication enabled

    - Redis service name: RedisMaster

    - Redis port: 6780

- Implement slave instance of Redis server with authentication enabled

    - Redis service name: RedisSlave1

    - Redis port: 6781

- Implement slave instance of Redis server with authentication enabled

    - Redis service name: RedisSlave2

    - Redis port: 6782

- Implement Redis Sentinel

Configure a multiple server deployment

Configure a multiple server deployment by following the procedures in "Multiple web server deployment, without high availability" on page 37

Installing Redis Sentinel

1. On each of the web servers, copy the existing Redis folder to a folder named Sentinel.

   Note: Each web server can have only one Sentinel instance, regardless of the number of websites that are installed on the server.

2. From the Sentinel folder, edit the following lines in the `sentinel.conf` file by replacing the port number and password with the appropriate values:

```
port <sentinel-port>
sentinel monitor <master-name> <ip> <redis-port> <quorum>
sentinel auth-pass <master-name> <password>
sentinel down-after-milliseconds <master-name> <milliseconds>
sentinel failover-timeout <master-name> <milliseconds>
sentinel parallel-syncs <master-name> <numslaves>
logfile "sentinel.log"
```

   Based on the example in this guide, the values would be:

```
port 26380
sentinel monitor RedisMaster Web01 6780 2
sentinel auth-pass RedisMaster rx6RB2CHt1lYkQnm$2jc3#CgL
```

```
sentinel down-after-milliseconds RedisMaster 30000
sentinel failover-timeout RedisMaster 180000
sentinel parallel-syncs RedisMaster 1
logfile "sentinel.log"
```

port <sentinel-port>

The port that the Sentinel instance will run on.

sentinel monitor <master-name> <ip> <redis-port> <quorum>

Specifies the master server to be monitored, and to consider it in ODOWN (Objectively Down) state only if at least the number of Redis Sentinel servers specified in <quorum> agree.

> **Warning:** The master name cannot include special characters or spaces. The valid characters are: A-z, 0-9, and the characters ".-_" (period, dash, and underscore).

> **Note:** Regardless of the number that is defined as the ODOWN quorum, the majority of Redis Sentinel servers must be online to start the failover process. In this example, if the quorum of two (2) Sentinel instances detect that the master Web01 is not available, the failover process begins the process of promoting one of the slave servers as the new master.

Slave servers are autodiscovered by Sentinel, therefore you do not have to specify slave servers in any way. Sentinel rewrites the configuration file by adding the slave servers using additional configuration options. The configuration file is also rewritten when a slave server is promoted to master.

sentinel auth-pass <master-name> <password>

Set the password to use to authenticate with the master and slave servers. Useful if there is a password set in the Redis instances to monitor.

sentinel down-after-milliseconds <master-name> <milliseconds>

Number of milliseconds that the master (or any attached slave server or Sentinel server) must be unavailable (as in, not accepting reply to PING, continuously) to be considered in S_DOWN state (Subjectively Down).

sentinel failover-timeout <master-name> <milliseconds>

Specifies the failover timeout in milliseconds.

sentinel parallel-syncs <master-name> <numslaves>

The number of slave servers that can be reconfigured simultaneously to point to the new slave server during a failover. Use a low number to avoid all slave servers being unreachable while performing a synchronization with the master.

Starting Redis Sentinel (Console mode)

From a command line prompt on each of the servers, go to the `Sentinel` folder, and issue the following command:

```
redis-server sentinel.conf --sentinel
```

As each Sentinel server comes online, you should receive output similar to the following:

```
[5372] 16 Jan 11:54:18.485 # Sentinel runid is 5b50429514954dab8f24a099aaf3e1442fe2f2ac
[5372] 16 Jan 11:54:18.486 # +monitor master RedisMaster 127.0.0.1 6780 quorum 2
[5372] 16 Jan 11:54:56.816 * -dup-sentinel master RedisMaster 127.0.0.1 6780 #duplicate
of 127.0.0.1:26381 or 3b1854570beabaaac8551db88bb5dd51625424c2
[5372] 16 Jan 11:54:56.817 * +sentinel sentinel 127.0.0.1:26381 127.0.0.1 26381 @
RedisMaster 127.0.0.1 6780
[5372] 16 Jan 11:55:02.787 * -dup-sentinel master RedisMaster 127.0.0.1 6780 #duplicate
of 127.0.0.1:26383 or 53525d1ebcbb8627ed3dcfbc84b858e31626c2db
[5372] 16 Jan 11:55:02.788 * +sentinel sentinel 127.0.0.1:26383 127.0.0.1 26383 @
RedisMaster 127.0.0.1 6780
```

The output shows that each Sentinel server found the master server and autodiscovered the slaves. This particular configuration is hosted on the same machine, which is why there are multiple references to 127.0.0.1.

If the master were to go offline, you will receive output similar to the following:

```
[5372] 16 Jan 12:00:42.415 # +sdown master RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:42.475 # +odown master RedisMaster 127.0.0.1 6780 #quorum 2/2
[5372] 16 Jan 12:00:42.475 # +new-epoch 4
[5372] 16 Jan 12:00:42.475 # +try-failover master RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:42.476 # +vote-for-leader 5b50429514954dab8f24a099aaf3e1442fe2f2ac 4
[5372] 16 Jan 12:00:42.478 # 127.0.0.1:26383 voted for
5b50429514954dab8f24a099aaf3e1442fe2f2ac 4
[5372] 16 Jan 12:00:42.478 # 127.0.0.1:26381 voted for
5b50429514954dab8f24a099aaf3e1442fe2f2ac 4
[5372] 16 Jan 12:00:42.567 # +elected-leader master RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:42.571 # +failover-state-select-slave master RedisMaster 127.0.0.1
6780
[5372] 16 Jan 12:00:42.662 # +selected-slave slave 127.0.0.1:6781 127.0.0.1 6781 @
RedisMaster 127.0.0.1 6780
```

```
[5372] 16 Jan 12:00:42.662 * +failover-state-send-slaveof-noone slave 127.0.0.1:6781
127.0.0.1 6781 @ RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:42.726 * +failover-state-wait-promotion slave 127.0.0.1:6781
127.0.0.1 6781 @ RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:43.534 # +promoted-slave slave 127.0.0.1:6781 127.0.0.1 6781 @
RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:43.536 # +failover-state-reconf-slaves master RedisMaster 127.0.0.1
6780
[5372] 16 Jan 12:00:43.599 * +slave-reconf-sent slave 127.0.0.1:6782 127.0.0.1 6782 @
RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:44.562 * +slave-reconf-inprog slave 127.0.0.1:6782 127.0.0.1 6782 @
RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:44.562 * +slave-reconf-done slave 127.0.0.1:6782 127.0.0.1 6782 @
RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:44.628 # -odown master RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:44.628 # +failover-end master RedisMaster 127.0.0.1 6780
[5372] 16 Jan 12:00:44.628 # +switch-master RedisMaster 127.0.0.1 6780 127.0.0.1 6781
[5372] 16 Jan 12:00:44.629 * +slave slave 127.0.0.1:6782 127.0.0.1 6782 @ RedisMaster
127.0.0.1 6781
[5372] 16 Jan 12:00:44.629 * +slave slave 127.0.0.1:6780 127.0.0.1 6780 @ RedisMaster
127.0.0.1 6781
```

In this scenario, 2 Sentinel servers agreed that the master is not responding. Because the majority of Sentinel servers are online, a leader is agreed upon and a new master (6781) is elected and all remaining slaves are reconfigured accordingly. The Sentinels continue to monitor for the missing server.

If the old master comes back online you will see similar output to the following:

```
[5596] 16 Jan 12:05:55.564 * +convert-to-slave slave 127.0.0.1:6780 127.0.0.1 6780 @
RedisMaster 127.0.0.1 6781
```

Note: Sentinel does not promote the old master, but reconfigures it as a slave of the new master.

Installing Redis Sentinel Service

From a command line prompt on each of the servers, go to the Sentinel folder and issue the following command:

```
redis-server --service-install sentinel.conf --service-name Sentinel --sentinel
```

The service is configured as Autostart and will be launched as "NT AUTHORITY\Net-workService". Upon successful installation, a success message is displayed and Redis exits. Sentinel will listen on the port number that is specified in the sentinel.conf file.

This command does not start the service.

Uninstalling Redis Sentinel Service

From a command line prompt on each of the servers, go to the `Sentinel` folder and issue the following command:

```
redis-server --service-uninstall sentinel.conf --service-name Sentinel --
sentinel
```

This command removes the Sentinel service configuration information from the registry. Upon successful uninstallation, a success message is displayed and Redis exits.

This command does not stop the service.

Starting the Redis Sentinel Service

```
redis-server --service-start --service-name Sentinel
```

This command starts the Redis Sentinel service. Upon successful startup, a success message is displayed and Redis service is started. You can also start the service by using the Services dialog or the net start command.

Stopping the Redis Sentinel Service

```
redis-server --service-stop --service-name Sentinel
```

This command stops the Redis Sentinel service. Upon successful termination, a success message is displayed and Redis exits. You can also stop the service by using the Windows Services Management Console or the net stop command.

Common Redis Sentinel commands

Querying the status of Redis Sentinel

Redis is installed with client application called `redis-cli.exe` that enables command line console to interact with and manage Redis and Redis Sentinel services.

```
redis-cli -p 26380
127.0.0.1:26380> ping
PONG
127.0.0.1:26380>
```

Show the state and information of a master

```
SENTINEL master <master name>
```

Example:

```
sentinel master MyRedisInstance
127.0.0.1:26380> SENTINEL master MyRedisInstance
1) "name"
2) "MyRedisInstance"
3) "ip"
4) "127.0.0.1"
5) "port"
6) "6781"
7) "runid"
8) "5a9d14a5a72c87e203a92650c4cd17dfe1f66394"
9) "flags"
10) "master"
11) "pending-commands"
12) "0"
13) "last-ping-sent"
14) "0"
15) "last-ok-ping-reply"
16) "117"
17) "last-ping-reply"
18) "117"
19) "down-after-milliseconds"
20) "60000"
21) "info-refresh"
22) "2113"
23) "role-reported"
24) "master"
25) "role-reported-time"
26) "815163"
27) "config-epoch"
28) "4"
29) "num-slaves"
30) "2"
31) "num-other-sentinels"
32) "2"
33) "quorum"
34) "2"
35) "failover-timeout"
36) "180000"
37) "parallel-syncs"
38) "1"
```

Return the IP address and port number of a master

```
SENTINEL get-master-addr-by-name <master name>
```

Example:

```
127.0.0.1:26380> sentinel get-master-addr-by-name MyRedisInstance
1) "127.0.0.1"
```

```
2) "6781"
127.0.0.1:26380>
```

Show a list of slave servers and their states for a master

```
SENTINEL slaves <master name>
```

Example:

```
127.0.0.1:26380> sentinel slaves MyRedisInstance
1) 1) "name"
2)    "127.0.0.1:6782"
3)    "ip"
4)    "127.0.0.1"
5)    "port"
6)    "6782"
7)    "runid"
8)    "9925a92da3a3770684532dd77cdf687b72137b0d"
9)    "flags"
10)   "slave"
11)   "pending-commands"
12)   "0"
13)   "last-ping-sent"
14)   "0"
15)   "last-ok-ping-reply"
16)   "582"
17)   "last-ping-reply"
18)   "582"
19)   "down-after-milliseconds"
20)   "60000"
21)   "info-refresh"
22)   "3686"
23)   "role-reported"
24)   "slave"
25)   "role-reported-time"
26)   "1228352"
27)   "master-link-down-time"
28)   "0"
29)   "master-link-status"
30)   "ok"
31)   "master-host"
32)   "127.0.0.1"
33)   "master-port"
34)   "6781"
35)   "slave-priority"
36)   "100"
37)   "slave-repl-offset"
38)   "1939136"
2) 1) "name"
```

```
 2) "127.0.0.1:6780"
 3) "ip"
 4) "127.0.0.1"
 5) "port"
 6) "6780"
 7) "runid"
 8) "33c8446fd8218705843aac4f057aaf7812eb9699"
 9) "flags"
10) "slave"
11) "pending-commands"
12) "0"
13) "last-ping-sent"
14) "0"
15) "last-ok-ping-reply"
16) "582"
17) "last-ping-reply"
18) "582"
19) "down-after-milliseconds"
20) "60000"
21) "info-refresh"
22) "3686"
23) "role-reported"
24) "slave"
25) "role-reported-time"
26) "1228352"
27) "master-link-down-time"
28) "0"
29) "master-link-status"
30) "err"
31) "master-host"
32) "127.0.0.1"
33) "master-port"
34) "6781"
35) "slave-priority"
36) "100"
37) "slave-repl-offset"
38) "1"
```

Common Redis Sentinel scenarios

To view the complete set of Redis commands, go to: https://redis.io/commands.

Scenario: Master server goes off line, need to promote a slave server to master.

```
localhost:6781> SLAVEOF NO ONE
```

Scenario: New master has been designated, need to attach existing slave servers to new master (localhost 6781).

```
localhost:6782> SLAVEOF localhost 6781
localhost:6783> SLAVEOF localhost 6781
```

Scenario: Query current replication settings

```
localhost:6780> INFO Replication
# Replication
role:master
connected_slaves:1
slave0:ip=::f0f3:a200:0:0,port=6781,state=online,offset=3025,lag=0
master_repl_offset:3025
repl_backlog_active:1
repl_backlog_size:1048576
repl_backlog_first_byte_offset:2
repl_backlog_histlen:3024
```

Scenario: Query information related to memory consumption

```
localhost:6780> INFO Memory
# Memory used_memory:2011808
used_memory_human:1.92M
used_memory_rss:1938032
used_memory_peak:2048576
used_memory_peak_human:1.95M
used_memory_lua:36864
mem_fragmentation_ratio:0.96
mem_allocator:jemalloc-3.6.0
```

Using arguments to send a command to redis-cli

```
C:\Redis>redis-cli -h localhost -p 6780 -a "rx6RB2CHt1lYkQnm$2jc3#CgL" PING
PONG
```

4. Configuring ChangePoint

Overview of configuration

After you have completed the installation, perform the following configuration steps:

1. Configure the settings for token authentication as follows:

   a. Open the `Enterprise\Web.config` file, and then replace the default value of the `WebApiSecret` setting with a unique string of UTF-8 characters with a recommended size of 64 bytes. For example, you can use any combination of 64 single byte characters.

   b. Open the `Enterprise\WebAPI\Web.config` file and then replace the value of `WebApiSecret` with the same unique string used above.

   c. Open the `Enterprise\WebSockets\Web.config` file, and then replace the value of `WebApiSecret` with the same unique string used above.

   d. In a load balanced environment, ensure that you use the same `WebAPISecret` value within the environment.

   Note: For security reasons, it is strongly recommended that you use a different `WebAPISecret` value for each ChangePoint instance that you deploy.

2. Set the permissions on the ChangePoint folders.

   For more information, see "Setting permissions on the ChangePoint folders" on page 50.

3. Review the default settings for the ChangePoint scheduled jobs, and change them as required.

   For more information, see "Configuring ChangePoint Scheduled Jobs" on page 79.

4. Install and set up the optional components as required. For more information, see:

   • "Installing ChangePoint Windows Services" on page 55.

   • "About creating and configuring an archive database" on page 222

   • "Installing and Configuring Single Sign-on (SSO)" on page 135

   • "Setting up mobile access to Changepoint" on page 142.

   • "Installing the ChangePoint online help" on page 141.

   • "Setting up a Client Portal website" on page 143

- "Setting up a survey response website" on page 144.

- "About Microsoft Exchange/Outlook synchronization" on page 144

- "Configuring batch printing" on page 146.

- "About installing ChangePoint APIs" on page 147.

5. Run the script to update the Infiniti database:

   a. Copy the `UpdateTimeIdToNotMandatoryInTimeAction.sql` file from the following folder on the media:

   ```
   \\Enterprise\Changepoint\Manual Install\Upgrade\Intelligent Forms
   ```

   b. Execute the script against InfinitiDB database.

6. If you have not already done so, configure the database connection settings for the ChangePoint websites, installed Windows services, and scheduled job executables.

   For more information, see "Configuring database connection settings" on page 65.

7. To verify connectivity, sign into all websites.

8. Review "Optimizing Performance" on page 179 for performance optimization recommendations.

9. Run the chained scheduled jobs by starting Update Time Rate, and ensure that Resource Demand Calculation completes successfully.

10. As required, enable or disable financial analysis record types. For more information, see "Enabling financial analysis record types" on page 219.

11. As required, add fiscal periods to group data. For more information, see "Adding fiscal periods to group financial analysis data" on page 219.

Setting permissions on the ChangePoint folders

On the web server:

1. Set NTFS security for the Changepoint\tempimages folder to allow Full Control for all users and groups.

2. To allow users to export survey results, grant authenticated users **Modify** access to the `<cp_root>\Temp` folder.

About setting up ChangePoint websites for SSL

If ChangePoint websites are set up for SSL in ChangePoint Administration, then changes are needed in the Web.config files for ChangePoint.

If you plan to install SSO, these changes are made when you run the PowerShell script for your chosen SSO endpoint type.

To use SSL with application authentication, follow the instructions in "About application authentication" on page 137.

Enabling HTTP Compression

It is recommended that you enable both static and dynamic compression.

> **Note:** You must be a member of the `Administrators` group on the local computer to run scripts and executables. As a security best practice, log onto your computer using an account that is not in the Administrators group, and then use the `runas` command to run your script or executable as an administrator. The script assumes that `inetpub\Adminscripts` is located on the system drive. The script performs an IIS reset when the configuration is complete.

1. In IIS Manager, on the **Compression** page, select:

    *   **Enable dynamic content compression**

    *   **Enable static content compression**

2. Restart IIS.

3. At a command prompt, run:

```
Changepoint\Utilities\HTTP Compression Utility\HTTPCompressionConfigIIS.bat
```

If you receive the following error message when you run the .bat file, you can safely ignore it:

```
ERROR ( message:New scheme object missing required attributes. Cannot add
duplicate collection entry of type 'scheme' with unique key attribute
'name' set to 'deflate'. )
```

Tech Notes and Knowledge Base Articles

Search the Microsoft TechNet articles for more information on enabling HTTP compression.

Setting Global IIS Parameters

Use IIS Manager to do the following for each ChangePoint website:

1. On the **Connections** panel, select the website.

2. Double-click the ASP feature.

3. Expand **Limit Properties**.

   a. Set the value of the **Maximum Requesting Entity Body Limit** to **10000000**

   b. Set the value of the **Response Buffering Limit** to **10000000**

4. In the **Actions** panel, click **Apply**.

5. Restart IIS.

Configuring IIS to allow plug-in downloads

To allow users to download .exe plug-ins from **My settings**, you must configure the appropriate permissions in IIS.

If you have added .exe files to the **deny** list on your IIS server, then in the **URL** tab of the Request Filter Module add the following URLs:

```
/ChangepointMSP.exe
/ChangepointOutlookSetup.exe
```

Importing licences for a new installation

Use ChangePoint Administration to import the licenses for granting users access to ChangePoint. You need a user license file for each database instance.

Note: You must configure the database connection settings for ChangePoint before you can import licenses.

1. Open ChangePoint Administration.

2. To sign into ChangePoint Administration for the first time, use `cpadmin` for both the user ID and password.

   If ChangePoint is not registered, the **Import Licenses** dialog appears.

3. Click **Choose File** to locate and open the ChangePoint license file (*.lic).

4. Click **Import**.

The **License Management** view displays the license file information.

5. Click **Close**.

For more information about licensing, see the *ChangePoint Administration Guide*.

Install the latest monthly releases

Check the **ChangePoint2022 Releases** section in the Customer Success Center (https://success.planview.com/Planview_Changepoint) or team folders in Client Portal, for releases that have been posted after this cumulative release

We encourage you to keep ChangePoint up to date with the monthly releases, which allows users to take advantage of the latest feature enhancements and fixed issues.

To install the monthly releases, follow the instructions in the corresponding release notes.

5. Installing ChangePoint Windows Services

Installing a ChangePoint Windows service

The ChangePoint Windows services require access to the database server, but do not have to be installed on the same server as the database or websites.

For information about installing and configuring a specific ChangePoint Windows service, see the topic for the service.

1. Do one of the following:

   - From the ChangePoint installer, click the **Services** tab and click the **<servicename> Service** link.

   - Run the service installation program from the ChangePoint product media:

     `\Changepoint\Services\<installation program name>`

2. Follow the prompts until the installation completes. The service is installed under the following folder:

   `C:\Program Files (x86)\Planview`

3. Configure the database connection settings for the service.

   For more information, see "About configuring database connection settings" on page 65.

4. If necessary, edit the service configuration file to configure the service. The service configuration file, by default, is located in the installation directory.

   Note: This is the same file that you edit to configure the SQL connection settings for the service in step 3.

5. Start the service.

Uninstalling a ChangePointWindows Service

Use the Windows Control Panel to uninstall the service.

ChangePoint Email Notification service

The ChangePoint Email Notification service queues messages for the ChangePoint Mail service.

If you enable any email notifications in ChangePoint Administration, you must install the ChangePoint Email Notification service and the ChangePoint Mail service, and make sure that these services run at suitable intervals. If these services do not run often enough, the EmailAuditStaging, EmailAuditNotification, and EmailQueue tables in the ChangePoint database can grow very large.

If you do not enable email notifications, then it is sufficient to install and run only the ChangePoint Mail Service. If in doubt, install and run both services.

Installation information

Use the following information with the generic procedure for installing and configuring a ChangePoint Windows service:

Information needed	Notes
Installation Program name	`ChangePoint Email Notification Service Installer.exe`
Installation path	Default: `C:\Program Files (x86)\Planview\Changepoint Email Notification Service\`
Configuration file	`CPEmailNotification.exe.config`
Configuration settings	
SendInterval	How often (in minutes) the service sends notifications. Default value: 5 Recommended value: 5 or greater

ChangePoint Exchange Synchronization Service

The ChangePoint Exchange Online Synchronization service synchronizes Microsoft Office 365 calendar entries with ChangePoint calendars. For installation instructions, see the "Installing the online ChangePoint Exchange Synchronization service " section on page 56.

> **Note:** Only the primary email account associated with each Exchange or Office 365 account can be synchronized with ChangePoint.

Installing the online ChangePoint Exchange Synchronization service

Installing the online ChangePoint Exchange Synchronization service includes the following:

- "Registering the online ChangePoint Exchange Synchronization Service with Azure" below

- "Information required to install the online ChangePoint Exchange Synchronization Service" on the next page

- "Installing the online ChangePoint Exchange Synchronization Service" on page 60

- "Configuring the online ChangePoint Exchange Synchronization Service" on page 60

Registering the online ChangePoint Exchange Synchronization Service with Azure

Register the service with Azure and obtain the following IDs that are required for the configuration:

- ApplicationId

- TenantId

- ClientSecret

1. Sign into the Azure portal (https://portal.azure.com).

2. Select **Azure Active Directory**.

3. Select **App registrations**.

4. Click **New registration**.

5. Set **name** to **ChangePoint Exchange Online Synchronization Service**.

6. For **Redirect URI**:

   a. Select **Public client/native (mobile & desktop)**.

   b. Set the value to **urn:ietf:wg:oauth:2.0:oob**.

7. Click **Register**. The overview page appears.

8. Take note of the **Application (client) ID** value and **Directory (tenant) ID** value, which are required for the service configuration (ApplicationId and TenantId).

9. Create the ClientSecret:

   a. Click **Add a certificates and secret**.

   b. Under **Client Secrets**, click **New client secret**.

   c. Set **description** to **ChangePoint Exchange Online Synchronization Service Secret**.

      d.   Set an expiration for the secret.

      Note: A new secret must be generated prior to the expiration.

      e.   Click **Add**.

      f.   Take note of the value of the secret, which is required for the service configuration (ClientSecret).

10. Grant permission to the service to connect through the API:

      a.   Click **API permissions**.

      b.   Click **Add a permission**.

      c.   Click **APIs my organization uses** tab.

      d.   Find and select **Office 365 Exchange Online**.

      e.   Click **Application permissions**.

      f.   Select full_access_as_app permission.

      g.   Click **Add permissions**.

11. Verify that the permission was granted. If the status of **full_access_as_app** is **API Permission is not granted** and the **Grant admin consent for Your Active Directory Name** button at the top of the list is disabled, then do the following:

      a.   Sign out of the Azure portal and then sign back in.

      b.   Go to API Permissions page and click the **Grant admin consent for Your Active Directory Name** link.

Information required to install the online ChangePoint Exchange Synchronization Service

Information needed	Notes
Installation Program name	`Exchange Synchronization Service.exe`
Installation path	Default: `<cp_root>\Changepoint Exchange Synchronization Service\`
Configuration file	`CPSynchronizationService.exe.config`

Information needed	Notes
User account and password for the service	User account and password for the ChangePoint Exchange Synchronization Service.
Configuration settings	
SynchSchedule	Interval in minutes for synchronizing between ChangePoint and Office 365. Default: 15
NewUserHistory	Number of days from the current date to go back when synchronizing new users. Includes all calendar entries that have been created or modified within the specified number of days. Default: 5
SynchronizationDirection	0 – synchronization is bidirectional 1 – synchronization is unidirectional from ChangePoint to Exchange 2 – synchronization is unidirectional from Exchange to ChangePoint. Default: 0
ConflictResolutionMethod	For bidirectional synchronization, defines which modification is accepted when a calendar entry has been edited in both ChangePoint and Exchange. E – the ChangePoint modification is ignored and the Exchange modification is applied C – the Exchange modification is ignored and the ChangePoint modification is applied N – the earlier modification is ignored and the later modification is applied. Default: N **Note:** The setting does not apply to unidirectional synchronization. If a conflict occurs between a deletion and an update, the deletion is applied regardless of the setting.

Information needed	Notes
LogInformativeEvents	0 – informative messages are not logged to the event log 1 – informative messages are logged to the event log Default: 1
ForcePersistenceInTarget	0 – the target system in a unidirectional synchronization is overwritten by the source when changes occur in the target 1 – the target system in a unidirectional synchronization is not overwritten by the source when changes occur in the target Default: 0
MaxOccurencesToSyncWhenNo EndDateSpecified	Maximum number of recurring appointments going to ChangePoint from Outlook on the Exchange synchronization. Default: 50
ApplicationId	Application (client) ID of the Azure app registration.
TenantId	Directory (tenant) ID associated to the Azure app registration.
ClientSecret	Client secret associated with the Azure app registration.

Installing the online ChangePoint Exchange Synchronization Service

1. Copy the ChangePoint Exchange Synchronization Service to a machine that has access to Microsoft Office 365 and the ChangePoint installer.

2. Install the service.

3. Follow the prompts to complete the installation.

4. Run LoginSettings.exe to configure CPSynchronizationService.exe.config file for the service.

Configuring the online ChangePoint Exchange Synchronization Service

1. Open the CPSynchronizationService.exe.config file, and then add the values (obtained above) for the following keys:

```
<add key="ApplicationId" value="" />
<!-- The Application (client) ID of the Azure app registration -->
<add key="TenantId" value="" />
<!-- The Directory (tenant) ID associated to the app registration -->
<add key="ClientSecret" value="" />
<!-- The client secret associated with the app registration -->
```

2. Start the service.

ChangePoint Mail Service

The ChangePoint Mail service sends automated emails from ChangePoint. You can install the service on any machine that has access to the SQL Server where the ChangePoint database is hosted. The service also requires access to an SMTP server, either locally or through the network in order to relay mail.

If you are upgrading the ChangePoint Mail Service, you must uninstall the old service first, and then install the new service.

> **Note:** If you enable email notifications in ChangePoint Administration, you must install the ChangePoint Mail service and the ChangePoint Email Notification service, and make sure that these services run at suitable intervals. If these services do not run often enough, the EmailAuditStaging, EmailAuditNotification, and EmailQueue tables in the ChangePoint database can grow very large.
>
> If you do not enable email notifications, then it is sufficient to install and run only the ChangePoint Mail Service.

Error messages

The ChangePoint Mail service removes badly formed email addresses from the To, Cc, and Bcc lines of the emails, and logs them in the ChangePoint Mail service server as:

```
Unable to send email to malformed email address: address
```

See the Event Viewer, **Applications and Services Logs > ChangePoint**.

Installation information

Use the following information with the generic procedure for installing and configuring a ChangePoint Windows service.

Information needed	Notes
Installation Program name	`ChangePoint Mail Service Installer.exe`
Installation path	**Default:** `C:\Program Files (x86)\Planview\Changepoint Mail Service\`

Information needed	Notes
Configuration file	`CPMail.exe.config`
Configuration settings	
SmtpServer	IP address or fully qualified domain name of the SMTP server that the ChangePoint Mail service uses. Default: 127.0.0.1 Ensure that the SMTP server allows mail to be relayed from the machine on which the ChangePoint Mail service is hosted. **Note:** If virus protection is enabled on the server that hosts the ChangePoint Mail service, consider adding a scanning exception for the ChangePoint Mail service to prevent it from being falsely detected as a mass mailing worm.
SmtpPort	The port used to contact the SMTP server. Default: 25
SmtpUserName	Authenticated SMTP user name. Leave value blank if not using authentication.
SmtpPassword	Password for the authenticated SMTP user name. **Note:** Password must be encrypted using the ChangePoint Encryption Utility.
EnableSSL	When SMTP port is set to 587, 2525, or 465, must be set to `true` to support encrypted connections. Default: `false`
AlwaysUseFromAddress	When set to `true`, the address specified in the `FromAddress` setting in this config file is always used and not the from address specified by the caller. Default: `false`
FromAddress	Default *from* address to use when `AlwaysUseFromAddress` is enabled or when a *from* address is not supplied by the caller when the mail is queued. Default: `username@domain.com`

Information needed	Notes
FromAddressDisplayName	Default name to display in the email's *from* address when a *from* address is not supplied when the mail is queued. Default: `username`
SendInterval	How often (in minutes) the service sends new notifications. Default value: 5 Recommended value: 5 or greater

Managing Changepoint Windows Services

You manage the Changepoint Windows Services the same way as other Windows services.

To start, stop, and set the startup type for services, use the **Administrative Tools > Component Services** in the Windows Control Panel.

6. Configuring Database Connection Settings

About configuring database connection settings

To access the database, each ChangePoint application requires an encrypted connection string, which is stored in a configuration file. To encrypt the database connection settings, you use the Login Settings utility.

The default path to the utility is:

```
<cp_common>\LoginSettings\Login Settings.exe
```

Default user ID and password

The configuration files that contain the connection strings are password protected. By default, the user ID is USERID and the password is PASSWORD (case-sensitive) in all of the configuration files.

The first time that you access a configuration file using the Login Settings utility, you must use the default user ID and password. You then specify the user ID and password that are used for database access, as described in "Required accounts and permissions" on page 17. The login settings utility encrypts these values and updates the configuration file with the encrypted values.

Configuring database connection settings

These are the general instructions for using the Login Settings utility. For more information, see the database connection settings topic for the application.

1. Run:

```
<cp_common>\LoginSettings\Login Settings.exe
```

    The **Changepoint Connection Settings** dialog box appears.

2. From the **Connection Settings** list, select the application.

3. In the **File Location** field, browse to the configuration file for the application.

4. Enter the user ID and password of the account for database access, then click **OK**.

    Note: The first time you run the Login settings utility on a configuration file, use "USERID" and "PASSWORD" (case sensitive) for the User ID and Password.

5. In the **Connection Settings** section, specify the server name, database name, and time-out information to be used in the connection string.

   Time-out is optional and can be left blank, or can be used to specify the ADO connection.timeout value (in seconds) used in the connection string.

   The .asp implementations use the time-out values specified in the **Connection Settings** dialog. The .NET implementations (.aspx) use the CommandTimeOut setting value specified in the application Web.config file instead.

6. In the **User ID** and **Password** fields, enter the user ID and password for the SQL account for accessing the ChangePoint database.

7. To verify the connection string, click **Test**.

8. Click **Save**.

Database connection settings for Batch Print

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilities
File location	Default: `<cp_root>\BatchPrint\PrintInvoices.exe.config`
User ID (for file)	Initial Default: USERID
Password (for file)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for ChangePoint

The ChangePoint option updates the DSN, DataDSN, and DSN2 information in the Global.asa and Web.config files in the ChangePoint folder. You only have to select the Global.asa file because the Web.config file inherits the same values that you input.

Note: To render reports in ChangePoint, you must also configure the ChangePoint Report Server. If your organization has a separate reporting database, then specify its server name and database name for the **ChangePoint Report Server** settings; otherwise, use the same server name and database that you entered for ChangePoint.

Field	Notes
Connection Settings	Enterprise
File location	Default: `<cp_root>\Enterprise\Global.asa`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Field	Notes
Connection Settings	Enterprise Report Server
File location	Default: `<cp_root>\Enterprise\Global.asa`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	Server for the separate reporting database, if used. Otherwise, the name of the main ChangePoint database server.

Field	Notes
Database	Name of the separate reporting database, if used. Otherwise, the name of the main ChangePoint database.
Time Out	Time Out for the separate reporting database, if used.
User ID (for database access)	User ID for the separate reporting database, if used.
Password (for database access)	Password for the separate reporting database, if used.

Database connection settings for ChangePoint Email Notification Service

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilities

File location	Default:
	`<cp_root>\Changepoint Email Notification Service`
	`\CPEmailNotification.exe.config`

User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for ChangePoint Exchange Synchronization Service

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilities

File location	Default:
	`<cp_`
	`root>\Changepoint Exchange Synchronization Service`
	`\CPSynchronizationService.exe.config`

User ID (for file)	Initial Default: USERID
Password (for file)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for ChangePoint Export Publishing Service

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilities
File location	Default: `<cp_root>\Changepoint Export Publishing Service` `\CPExportPublishingService.exe.config`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	

Field	Notes
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for ChangePoint Mail Windows Service

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilities
File location	Default: `<cp_root>\Changepoint Mail Windows Service \CPMail.exe.config`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Cognos Client Tools

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Jobs and Utilitiesr
File location	Default: `C:\Program Files (x86)\Changepoint\Cognos Client Tools`
User ID (for File)	Initial Default: USERID

Field	Notes
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Data Archiving Source SQL server

Field	Notes
Connection Settings	Data Archiving (Source SQL Server)
File location	Default: C:\Program Files\Changepoint\Changepoint\Data Archiving\Data Archiving.ini
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Data Archiving Target SQL server

Field	Notes
Connection Settings	Data Archiving (Target SQL Server)
File location	Default: C:\Program Files\Changepoint\Changepoint\Data Archiving\Data Archiving.ini
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Infiniti Scheduler

Field	Notes
Connection Settings	Inifiniti Scheduler
File location	`<cp_root>Intelligent Forms\Websites\ IntelledoxScheduler\ IntelledoxScheduler.dll.config`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	Infiniti Server value
Database	InfinitiDB value

Field	Notes
Time Out	
User ID (for database access)	User ID that has dbo access to the InfinitiDB
Password (for database access)	Password of User ID that has dbo access to the InfinitDB

Database connection settings for Intelligent Forms

You use the Login settings utility to update the settings for an Intelligent Forms instance or to configure an additional Intelligent Forms instance for example, a test instance.

1. Run: `<cp_common>\LoginSettings\Login Settings.exe`.

2. In the **Connection Strings** field, select **Intelligent Forms Database Setup**.

Intelligent Forms Setup dialog box options

Field	Notes
New Database Server	Server that hosts the new ChangePoint database and Infiniti database.
New ChangePoint Database	Name of the new ChangePoint database.
New ChangePoint User ID	User ID for the new ChangePoint database.
New ChangePoint Password	Password for the new ChangePoint database.
Infiniti Database	Name of the Infiniti database.
Infiniti User ID	User ID for the new Infiniti database.
Infiniti Password	Password for the new Infiniti database.
Old ChangePoint API URL	URL for the previous ChangePoint API.
New ChangePoint API URL	URL for the new ChangePoint API.

Field	Notes
Old Database Server	Server that hosted the previous ChangePoint database.
Old ChangePoint Database	Name of the previous ChangePoint database.
Old ChangePoint User ID	SQL account for accessing the ChangePoint database.
Old ChangePoint Password	Password for the SQL account.
Old Infiniti URL	URL for the previous Infiniti instance.
New Infiniti URL	URL for the new Infiniti instance.

Database connection settings for Intelligent Forms (Manage and Produce)

Note: You must configure the database connection settings for each of the appsettings.json files for Manage and Produce.

Field	Notes
Connection Settings	Intelligent Forms (Manage and Produce)
File location	<cp_root>\Intelligent Forms\Websites\Manage\appsettings.json <cp_root>\Intelligent Forms\WebsitesProduce\appsettings.json
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	Infiniti Server value
Database	InfinitiDB value
Time Out	
User ID (for database access)	User ID that has dbo access to the InfinitiDB
Password (for database access)	Password of User ID that has dbo access to the InfinitDB

Database connection settings for RESTful API

Field	Notes
Connection Settings	RESTful API
File location	<cp_root>\Enterprise\WebAPI\Web.config
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for CPEffectiveDates scheduled job

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Job, and Utilities
File location	Default: `<cp_root>\ScheduledJobs\` `CPEffectiveDates.exe.config`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Release Guest Licenses scheduled job

Field	Notes
Connection Settings	ChangePoint Windows Services, Scheduled Job, and Utilities
File location	Default: `<cp_root>\ScheduledJobs\CPGuestLicenses.exe.config`
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Transport Tool

Field	Notes
Connection Settings	Transport Tool
File location	Default: `<cp_root>\Enterprise\web.config`
User ID (for file)	Initial Default: USERID
Password (for file)	Initial Default: PASSWORD
Server	Server that CPTransport database it installed on.
Database	CPTransport
Time Out	

Field	Notes
User ID (for database access)	User ID that has dbo access to CPTransport Database
Password (for database access)	Password of User ID that has dbo access to CPTransport Database

Database connection settings for Web Services API

Field	Notes
Connection Settings	Web Services
File location	Default: `<cp_root>\API\CP Web Services\web.config`
User ID (for file)	Initial Default: USERID
Password (for file)	Initial Default: PASSWORD
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

Database connection settings for Web Sockets

Field	Notes
Connection Settings	WebSockets
File location	<cp_root>\Enterprise\WebSockets\Web.config
User ID (for File)	Initial Default: USERID
Password (for File)	Initial Default: PASSWORD

Field	Notes
Server	
Database	
Time Out	
User ID (for database access)	
Password (for database access)	

7. Configuring ChangePoint Scheduled Jobs

About ChangePoint scheduled jobs

ChangePoint scheduled jobs run at various intervals to ensure that data is refreshed and up-to-date. Some of the scheduled jobs run individually and independently. Others have dependencies and are run as part of a sequence of scheduled jobs.

Chained scheduled jobs

Some scheduled jobs have dependencies on other scheduled jobs, and for this reason, a scheduling chain has been set up for these jobs.

The steps in the chain are:

1. Update Time Rate job

    *   By default, the Update Time Rate job starts at 12.01 AM.

    *   When it completes, whether it failed or succeeded, the Update Time Rate job starts the Resource Demand Calculation job.

2. Resource Demand Calculation job

    *   If the Resource Demand Calculation job fails, none of the remaining jobs in the chain is started.

    *   If the Resource Demand Calculation job succeeds, it starts the Financial Analysis Summary job.

3. Financial Analysis Summary job

    *   Whether the Financial Analysis Summary job succeeds or fails, it starts the Calculate Project Costs and Portfolio Calculation Engine jobs (these jobs run in parallel).

4. Calculate Project Costs job

5. Portfolio Calculation Engine job

6. Populate Demand and Capacity job

Reasons for the Dependencies

All the jobs in step 2–step 5 of the chain have dependencies on step 1, which is the Update Time Rate job. The Resource Demand Calculation job runs upon completion of the Update Time Rate job regardless of the pass/fail status of the Update Time Rate job.

Do not alter the sequence of jobs in the chain, because:

• The Update Time Rate jobs needs to run and finish successfully before the Financial Analysis Summary job starts to ensure that the most recent data from the Time table is retrieved and costs are updated in FinAnnSummary table.

• The Update Time Rate job needs to run and finish successfully before the Resource Demand Calculation job starts to ensure that a portfolio can retrieve the most recent data from the Time tables.

• Until the Update Time Rate job has finished running, no data is available for display in the portfolio for cost metrics.

• Bad data can cause some of the steps in the Portfolio Calculation Engine job to fail; however, it may not be necessary to fail the entire job. Go through the job history and Windows EventLog for more details.

Running the Update Time Rate job more frequently

To run the Update Time Rate job more frequently than once a day without initiating the chained scheduled jobs, create another scheduled job (for example, Update Time Rate Hourly) that does not launch the Resource Demand Calculation job. Schedule the new job to run at the chosen interval, but leave a gap when the chain of scheduled jobs is running.

For example, to run Update Time Rate Schedule every hour throughout the day, if:

• Update Time Rate is scheduled for 12:01AM, its default start time, and

• your job history tells you that the average time taken by the chained jobs is 4 hours, and that Update Time Rate takes, on average, 30 minutes

set the schedule for Update Time Rate Hourly to hourly, starting at 5:00 AM and ending at 11:00 PM.
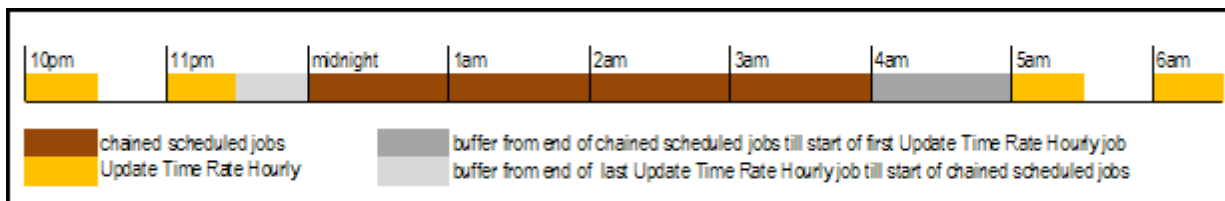
This leaves is a gap of 5 hours (4 hours for the chained jobs, plus an hour of a buffer) from the time that the chained jobs start until the first run of Update Time Rate Hourly job.

It also allows a buffer of 30 minutes from the end of the last run of Update Time Rate Hourly until the chained jobs start.

Scheduled Jobs reference list

The following table lists the scheduled jobs that are included with ChangePoint. The times and frequencies listed are the default settings. The statuses (enabled or disabled) are the recommended settings. For a new installation, all scheduled jobs are disabled. For an upgrade, the existing status of each job is maintained.

Review and reschedule the jobs as required according to the needs of your organization.

The names of the scheduled jobs that appear in SQL Server Manager are prepended by the database name and an underscore, for example "ChangePoint_Adjust Daylight Savings".

Adjust Daylight Saving scheduled job

Sets a flag in the time zone table to indicate which time zones are currently observing daylight savings time.

File or Stored Procedure	AdjustDaylightSaving
Schedule	Daily at 3:01 AM
Status	Enabled

Archive Aged Entities scheduled job

Validates all relevant entities (including those previously validated by the Archive Validation job), archives them into the archive database, then removes them from the ChangePoint database.

Before running the job for the first time, create an empty archive database on the target server. The .dtsx file must exist on the source server; it is not required on the target archive server.

File or Stored Procedure	ARC_ValidateProjectRequests
	ARC_ValidateProjects
	ARC_ValidateEngagement
	ARC_ValidateFinalization
	C:\Program Files\Changepoint\Changepoint\Data Archiving\Data Archiving.dtsx
Schedule	Not scheduled
Status	Enabled

Archive Validation scheduled job

Validates entities to be archived and generates archive validation logs.

File or Stored Procedure	ARC_ValidateProjectRequests
	ARC_ValidateProjects
	ARC_ValidateEngagement
	ARC_ValidateFinalization
Schedule	Not scheduled
Status	Enabled

Auto Dispatch Request to Queues scheduled job

For request types for which queues have been configured, sends qualifying requests to queues.

File or Stored Procedure	AutoDispatch
Schedule	Every 5 minutes
Status	Enabled

Auto Escalate Requests scheduled job

Escalates requests based on a Service Level Agreement.

File or Stored Procedure	AutoEscalate
Schedule	Every 30 minutes
Status	Enabled

BatchCommitInvoices scheduled job

Commits batch invoices, which populates the necessary data for the Batch Invoice Process Report.

The batch invoice commit can also be done through the UI. Your organization's policies determine which method you use.

If you set up a schedule for this job, it is recommended that you set the job to run during off-peak hours and ensure that the job does not overlap other jobs.

File or Stored Procedure	BatchCommitInvoice
Schedule	Not scheduled
Status	Enabled

BatchInvoicingGetInvoiceDefaultList scheduled job

Starts the batch invoice/cross charge generation process, using selections previously saved from the Batch Invoice/Cross Charge report.

File or Stored Procedure	BI_BatchGetInvoiceDefaultList
Schedule	Daily at 3:30 AM
Status	Enabled

Calculate Project Costs scheduled job

Calculates budget, planned costs and actual costs at the project, task and task assignment levels. This job populates the ProjectCostInfo table that is used to generate the earned value data providers

Note: Do not set an independent schedule for this job. The Calculate Project Costs job is called by the Financial Analysis Summary job, and both are included in the chained scheduled jobs. For more information, see "Chained scheduled jobs" on page 79.

File or Stored Procedure	dbo.EVR_Calculate ProjectCosts
Schedule	Not scheduled
Status	Enabled

CheckTimeToApprove scheduled job

Generates the **You have time to approve** email notification.

File or Stored Procedure	CheckTimeToApprove
Schedule	Daily at 5:00 AM
Status	Enabled

CleanResourceAvailability scheduled job

Removes availability calendar entries that are more than (default) 30 days old. This job is optional, but recommended if your organization has a large number of availability entries. Removing the old entries helps to minimize table size.

To change the default number of days, edit the job step to pass the `@ndays` parameter to the stored procedure.

To change the value to *n* days, add the parameter as follows:

```
CleanResourceAvailability @ndays = n
```

The larger the number of days, the larger the database size.

For more information, see "Editing parameters for scheduled jobs " on page 98.

File or Stored Procedure	CleanResourceAvailability
Schedule	Daily at 12:00AM
Status	Disabled

CPEffectivedates scheduled job

Activates effective dates for work history information about a resource.

You must encrypt the database connections settings for `CPeffectiveDates.exe`. For more information, see "About configuring database connection settings" on page 65.

`CPEffectiveDates.exe` uses both sets of server name and database name parameters (from the Login Settings utility and from the command line).

File or Stored Procedure	`<cp_root>\ScheduledJobs\ CPeffectiveDates.exe` `[DATABASETYPE], [DATABASESERVER], [DATABASE]` Where: `[DATABASETYPE]` – SQL `[DATABASESERVER]` – name of ChangePoint database server `[DATABASE]` – name of ChangePoint database
Schedule	Daily at 12:00:01 AM.
Status	Enabled

CPExtended_Compile stats and purge data scheduled job

Compiles statistics from Traces table in the CPExtended database, and purges old trace data. Default threshold is one month.

File or Stored Procedure	CompileStatsAndPurgeData
Schedule	Every Sunday at 2:00 AM
Status	Disabled

CPFullText scheduled job

Populates the full text catalogs for both knowledge management and request items. Items that have been created since the previous job run cannot be located until after the subsequent job run.

Note: Enable either CPFullText *or* CPFullText using background updates, but not both.

File or Stored Procedure	sp_fulltext_catalog
Schedule	Daily at 12:15 AM.
Status	Enabled

CPFullText using background updates scheduled job

Updates the catalog immediately using incremental updates. A full-text rebuild is performed weekly in case any of the incremental updates fails.

Note: Enable either CPFullText *or* CPFullText using background updates, but not both.

File or Stored Procedure	sp_fulltext_catalog
Schedule	Weekly on Sunday at 4:00 AM.
Status	Disabled

CPTempDB_Clean up idle-orphaned schemas scheduled job

Removes schema for low use schemas. By default, schemas that have not been accessed for 14 days will be removed. Schemas will not be removed when the schema owner is currently logged into ChangePoint.

File or Stored Procedure	exec CPTempDBCleanupOrphanedSchemas 14
Schedule	Weekly on Sunday at 2:00 AM.
Status	Enabled

Financial Analysis Summary scheduled job

Populates the tables used by the financial analysis data provider, for use in reporting and analysis.

Do not set a schedule for this job. The Financial Analysis Summary job is called by the Resource Demand Calculation job, and both are included in the chained scheduled jobs. For more information, see "Chained scheduled jobs" on page 79.

A step in the Financial Analysis Summary job detects if the Portfolio CalculationEngine job exists and is enabled. If not, it clears the portfolio recalculation table, which is normally processed and cleared by the portfolio job.

If you have re-named the portfolio calculation engine job, do one of the following:

- Re-enable it under the exact name "Portfolio Calculation Engine"

- Remove the step from the Financial Analysis Summary job to ensure the data is not truncated when portfolio information is being calculated.

  Note: If you have multiple instances of the Financial Analysis Summary job and have renamed the jobs with unique names, remove the step.

File or Stored Procedure	FinAnnSummary_ToDate FinAnnSummary_ToDateTwo FinAnnSummary_Forecast FinAnnSummary_Unbillable RD_GetRDMonetaryData msdb..sp_start_job @job_name = 'Calculate Project Costs' msdb..sp_start_job @job_name = 'Portfolio Calculation Engine'
Schedule	Not scheduled
Status	Enabled

IPM Calculation Engine scheduled job

The Copy Assignments step copies the metric assignments (if the carry forward option is selected) from the previous IPM period to the current period. This step runs only on the first day of the period.

The Calculate Raw Data step gathers data from the ChangePoint database, generates raw data and inserts it into the MetricRawData table. This calculation gathers only data that is required since the last time the calculation ran. If the raw data is from a previous period (refdate), the system inserts a record into the IPIReCalcuLastPeriod table. From this table, the calculation engine can re-calculate the data from the end of the day for a previous period.

In the Calculate Metric Data step, the IPM Calculation engine calculates raw data that is associated with a resource who is assigned to a metric. It inserts the results into the MetricData table. This calculation calculates only the raw data based on the current IPM period. The criteria are as follows:

- The resource is assigned to a metric and the assignment is not deleted

- The metric is not deleted

- The standard metric is not deleted

- The engine includes an IPM re-calculation step that re-calculates the last day of the previous period if metric data for the last period is detected.

The Clean up step clears the raw data tables of information that is no longer required.

File or Stored Procedure	IPI_periodcopy IPICalculationEngine IPI_ReCalcuLastPeriod IPI_deleteRawData
Schedule	Daily at 10:30 PM.
Status	Enabled

Nonworking Days Task Assignments Email scheduled job

Generates and sends email notifications to the project manager and assigned resources when effort from task assignments is assigned to resources on nonworking days.

File or Stored Procedure	GenerateNonworkingDaysEmail.sql
Schedule	Every 15 minutes
Status	Enabled

PercentOfContractIncurred scheduled job

Notifies the contract/initiative manager if:

- the invoiced/cross-charged amount is near the threshold (80% of the contract approved amount), or

- the contract approved amount has been exceeded.

Generates the email notifications for "ContractApproved amount near threshold" and "ContractApproved amount has been exceeded".

File or Stored Procedure	PercentOfContractIncurred
Schedule	Weekly on Sunday at 7:00 PM
Status	Disabled

PerformanceCPGrowth scheduled job

Monitors the growth of ChangePoint database files and tables.

For more information, see "Monitoring database growth" on page 99.

File or Stored Procedure	PerformanceCollectAndCalculateDbGrowth
Schedule	Daily at 11:50 PM
Status	Enabled

Populate Demand and Capacity scheduled job

Populates table tblDemandAndCapacity used by table Demand and Capacity data provider, for use in reporting and analysis.

File or Stored Procedure	PopulateDemandAndCapacity
Schedule	Daily at 2:00AM
Status	Enabled

Portfolio Calculate Report Cards

Calculates customer/client report card information used by the customer/client report card and customer/client radar reports.

All data is stored in a table on the ChangePoint database server, and is displayed when the report card is generated for a specific customer/client profile, or when the Customer/Client Radar report is run.

> **Note:** Financial information is displayed in the user's home currency.

Because the job normalizes all of its financial calculations to the most common currency specified in the global workgroups, at least one global workgroup must have a currency selected.

If you use Survey Management, enable this job.

File or Stored Procedure	PF_CalculateReportCards
Schedule	Daily at 10:00 PM
Status	Disabled

Portfolio Calculation Engine scheduled job

This job performs all the calculations required by portfolio management. The parameter in the second step determines whether the step runs: set to 0 or greater to run, less than 0 to skip.

Do not set a schedule for this job. The Portfolio Calculation Engine job is called by the Financial Analysis Summary job, and both are included in the chained scheduled jobs. For more information, see "Chained scheduled jobs" on page 79.

File or Stored Procedure	ProjectToSubProjects
	PF_AutomaticUpdate 1
	PF_FiscalPeriodEndReCalc
	PF_ReCalcuLastPeriod
	PFRollupProjectNoBillingOffice
	PopulateProjectCost
	PF_BudgetvsActual
	PFRequestCost
	PFRequestEffort
	PFPlanningHoursEffort
	PFRemainingHoursCost
	PFPlanningHoursCost
	PFUninvoicedBillingAmount
	PFPlanningHoursBillingAmt
	PFRevRecAmount
	PFRequestBillingAmount
	PFRemaingBillingAmt
	PF_RecalcuLastPeriod_UsrEntr
	PF_CalculationEngine
	PFPortfolioSummary
	PF_Recalc_RollupPortfolios
	PFRollup_CalcEngine
Schedule	Not scheduled
Status	Enabled

Process Expense Approval scheduled job

Processes expense approver records and updates the records with the approver and status in a table accessed by the standard ChangePoint **You have expense reports to approve** notification.

If no contract approver is defined, the expense record is updated with the line approver.

If no line approver is defined, this job automatically approves the record.

File or Stored Procedure	ProcessExpenseApproval
Schedule	Every 30 minutes
Status	Enabled

Process Time Entries for Approval scheduled job

Processes time records pending approval, and stores the records in a table accessed by the standard ChangePoint **You have time to approve** notification.

File or Stored Procedure	ProcessTimeApproverRecords
Schedule	Every 30 minutes
Status	Enabled

Reindex and Update Statistics daily scheduled job

Calculate statistics for the indexes it updates in the ChangePoint database for SQL Query Optimizer purposes.

File or Stored Procedure	(scripts) Daily Reindex Defrag Indexes Daily Update Statistics
Schedule	Daily at 6:00AM.
Status	Enabled

Reindex and Update Statistics weekly scheduled job

Updates statistics for all rows in all tables in the ChangePoint database for SQL Query Optimizer purposes.

File or Stored Procedure	(scripts) Weekly Reindex Weekly Update Statistics
Schedule	Weekly on Sunday at 3:00 AM
Status	Enabled

Release Guest Licenses scheduled job

Releases licenses of Client Portal users whose access has expired.

You must encrypt the database connections settings for `CPGuestLicenses.exe`. For more information, see "About configuring database connection settings" on page 65.

`CPGuestLicenses.exe` uses both sets of server name and database name parameters (from the Login Settings utility and from the command line).

File or Stored Procedure	`<cp_root>\ScheduledJobs\CPGuestLicenses.exe`
	`[DATABASETYPE], [DATABASESERVER], [DATABASE]`
	Where:
	`[DATABASETYPE]` – SQL
	`[DATABASESERVER]` – name of the ChangePoint database server
	`[DATABASE]` – name of the ChangePoint database

Schedule	Daily at 12:00 AM
Status	Enabled

Release Held Locks scheduled job

Releases system locks from the RecordLock table after there has been no activity for the designated time by deleting locks that belong to a Login session that has expired. Does not apply to PRJ or MSP. Default is 330 seconds.

The designated time can be set in the step.

For more information, see "Editing parameters for scheduled jobs " on page 98.

File or Stored Procedure	ReleaseLocks 330
Schedule	Every 6 minutes.
Status	Disabled

Resource Demand Calculation scheduled job

Performs the updates to budgets for which the option to replace values in past periods with actual values has been enabled.

Updates the daily effort in the budgets based on changes made to fiscal period amounts.

Updates the working days table which is used by various parts of the application (such as resource demand analysis).

> **Warning:** Do not set a schedule for this job. This Resource Demand Calculation job is called by the Update Time Rate job, and both are included in the chained scheduled jobs. For more information, see "Chained scheduled jobs" on page 79.

File or Stored Procedure	SetWorkingDays UpdateRD_NonWorkingDaysTable RollupProjectsByFiscalPeriods BU_ReplacePastWithActuals BU_SaveDailyEffort msdb..sp_start_job @job_name = 'Financial Analysis Summary'
Schedule	Not scheduled
Status	Enabled

Resource Utilization scheduled job

Notifies the manager of a resource whose forecast hours related for the following week are less than 80% or more than 100% of a full week.

Generates the "Resource on Bench" and the "Resource Overloaded" email notifications.

File or Stored Procedure	ResourceLoad
Schedule	Once a week on Sunday at 7:20 PM.
Status	Disabled

Revenue Recognition Tentative scheduled job

Runs the revenue recognition tentative process with saved values as of the last time "start on schedule" was chosen in the process.

File or Stored Procedure	RevRec_Tent_Schedule
Schedule	Once a day at 5:30 AM
Status	Disabled

Rollup Project Planned Data scheduled job

Rolls up the planned date and effort changes for all projects that have time entry restrictions based on project planned data.

File or Stored Procedure	RollupProjectPlannedData
Schedule	Every 5 minutes
Status	Not Enabled

Session Clean Up scheduled job

Disconnects user sessions under the following circumstances:

- The user did not sign out of ChangePoint properly and the session has been inactive for more than 5.5 minutes (330 seconds). This can occur when the user closes the browser without signing out, or when the user's computer shuts down unexpectedly.

- The user has been logged on for more than 1 day.

- The user is accessing ChangePoint using a mobile device and has not interacted with ChangePoint for more than 5.5 minutes (330 seconds).

> **Note:** When the user signs into ChangePoint using a desktop or laptop computer, a keep-alive is triggered every 5 minutes provided that the main window remains open. With mobile access, the behavior is different.

The default value for the allowed period of inactivity is 5.5 minutes (330 seconds). To modify this time, change the optional seconds parameter that is passed to the SessionCleanup stored procedure called by the Session Clean Up scheduled job.

For more information, see "Editing parameters for scheduled jobs " on page 98.

File or Stored Procedure	SessionCleanup
Schedule	Every 5 minutes
Status	Enabled

Survey Set Expired Survey scheduled job

Changes the status of expired "Automated" surveys to "Inactive".

Deletes all pending approval survey records from the SurveySanTrigger table when the associated project or opportunity is deleted.

File or Stored Procedure	SV_SetExpiredSurveyInactive DeleteSurveySanTrigger
Schedule	Once a day at 1:00 AM
Status	Disabled

Task Slippage scheduled job

Sends the notification to the project manager and contract/initiative manager when either of the following occurs:

- the resource forecasts a later date than the original plan on the task

- the resource forecasts a larger number of hours than the original planned hours

Used by the "Task slippage" email notification.

File or Stored Procedure	TaskSlippage
Schedule	Once a week on Sunday at 8:00 AM.
Status	Disabled

Time Conformance scheduled job

Sends email notices to resources whose total hours for the previous week were not in conformance with the required hours.

Generates the "Time sheet compliance report" email notification.

File or Stored Procedure	CheckTimeConformance
Schedule	Once a week on Sunday at 8:00 PM.
Status	Disabled

Update Time Rate scheduled job

Updates the billing/cross charge rates, cost rates, fixed fee IDs and the billable/chargeable flag in the time tables based on resource/billing role/staffing level combinations and effective dates. Also updates the task actual cost into the task assignment table that is used by the Microsoft Project interface.

The Update Time Rate job is the first job in a chain of dependent scheduled jobs. For more information, see "Chained scheduled jobs" on page 79.

File or Stored Procedure	TI_UpdateTimeBillingRate UpdateAssignmentCost msdb..sp_start_job @job_name = 'Resource Demand Calculation'
Schedule	Once a day at 12:01 AM.
Status	Enabled

Validate UDFs scheduled job scheduled job

Calculates and populates calculated field values for all entities for which a calculated configurable field has been configured. Before the calculation occurs, the job checks that the calculation formula is valid. If the formula is invalid, the job bypasses the field and writes a message to the Windows event log.

File or Stored Procedure	ValidateFormulas UpdateUDFCalculationField
Schedule	Once a day at 2:00 AM.
Status	Enabled

Workflow Management scheduled job

Starts the workflow process, populates default configurable fields for system-generated resource requests, and processes workflow escalations for all records.

> **Note:** WorkflowEscalation.exe requires a trusted connection.

File or Stored Procedure	<cp_root>\ScheduledJobs\ WorkflowEscalation.exe [DATABASESERVER], [DATABASE] Where: `[DATABASESERVER]` – name of ChangePoint database server `[DATABASE]` – name of ChangePoint database
Schedule	Every 30 minutes
Status	Enabled

Editing parameters for scheduled jobs

Some of the scheduled jobs call stored procedures or run .exe files using parameters.

1. Access SQL Server Management Studio.

1. In the **Object Explorer** tree view, expand the following nodes:

   ServerName > **SQL Server Agent** > **Jobs**

2. Right-click the job, and then select **Properties**.

   The **Job Properties** dialog appears.

3. Select the **Steps** page, and then double-click the step that contains the parameter.

   The **Job Step Properties** dialog appears.

4. In the **Command** field on the **General** page, edit the parameter value as required.

5. Click **OK**.

6. Click **OK** again.

Monitoring database growth

The PerformanceCPGrowth scheduled job monitors the growth of database files and tables. The job gathers information on table growth, file growth, and I/O statistics. By default, the job collects counter data once a day. The data is stored in the following database tables:

- perfCPFileGrowth – Stores daily details about file growth. Data is saved for 70 days.

- perfCPFileGrowthSum – Stores monthly aggregate data on file growth. Data is saved for 10 years.

- perfTableGrowth – Stores daily details about table growth. Data is saved for 70 days.

- perfTableGrowthSum – Stores monthly aggregate data on table growth. Data is saved for 10 years.

- CPstartuptimes – Stores the startup times. Some counters are cumulative from the last SQL Server start. At startup they are reset.

You can use the data in these tables to monitor database growth over time. Under normal use, the database will grow. The database tables and files may shrink if auto-shrink is enabled or if you use the archiving functionality to move old data from the database to an archive database.

Abnormal database file shrinkage or growth could result in the following issues:

- server resources consumption

- performance problems

- physical file fragmentation

- a need for more maintenance

Therefore it is recommended that you monitor the database growth to diagnose potential issues.

You can use the following sample queries in SQL Server Management Studio to access the data gathered by the PerformanceCPGrowth scheduled job.

File Growth Details Query

The following query retrieves file growth details over the past 50 days based on the current server date and time.

```
declare @StartDate datetime, @EndDate datetime

set @StartDate = GetDate()-50
set @EndDate = GetDate()- 1

exec performanceCPfilesGrowthDetails @StartDate,@EndDate
GO
```

File Growth Summary Query (for a range of months)

The following query retrieves file growth summary data for October 2012 – November 2012.

```
/**********************
Parameters:
Start year
Start month
End year
End month
**********************/

exec performanceCPfilesGrowthSum 2012,10,2012,11

GO
```

File I/O Details Query

```
THE FOLLOWING QUERY RETRIEVES FILE I/O DETAILS (READS, WRITES, READS+WRITES)
OVER THE PAST 50 DAYS BASED ON THE CURRENT SERVER DATE AND TIME.

declare @StartDate datetime, @EndDate datetime

set @StartDate = GetDate()-50
set @EndDate = GetDate()- 1

exec performanceCPFilesWritesDetail @StartDate,@EndDate
exec performanceCPFilesReadsDetail @StartDate,@EndDate
exec performanceCPFilesIODetail @StartDate,@EndDate

GO
```

File I/O Summary Query

The following query retrieves file I/O summary data (reads, writes, reads+writes) for November 2012.

```
exec performanceCPfilesWriteSum 2012,11
exec performanceCPfilesReadSum 2012,11
exec performanceCPfilesIOSum 2012,11

GO
```

Table Growth Details Query

The following query retrieves table growth details over the past 50 days based on the current server date and time.

This query contains two optional parameters for the column to order by (default: table name) and for the number of rows in the output list.

```
declare @StartDate datetime, @EndDate datetime

set @StartDate = GetDate()-50
set @EndDate = GetDate()- 1

/*******************
parameters:
Start date
End date
Column to order by (optional)
Number of rows in the output list (optional)
*******************/
exec performanceTableGrowthDetail  @StartDate,@EndDate
exec performanceTableGrowthDetail  @StartDate,@EndDate, 'RowsGrowth'
exec performanceTableGrowthDetail  @StartDate,@EndDate, 'RowsGrowth', 30
exec performanceTableGrowthDetail  @StartDate,@EndDate, NULL, 20

GO
```

Table Growth Summary Query

The following query retrieves table growth summary data for the specified range of months. For a single month, set the start month and year parameters equal to the end month and year.

This query contains two optional parameters for the column to order by (default: table name) and for the number of rows in the output list.

```
/*******************
```

```
              parameters:
              Start year
              Start month
              End year
              End month
              Column to order by (optional)
              Number of rows in the output list (optional)
              ******************/

              exec performanceTableGrowthSum 2011,10,2012,10
              exec performanceTableGrowthSum 2011,10,2012,10,'InitialSize_kb'
              exec performanceTableGrowthSum 2011,10,2012,10,'InitialSize_kb',10
              exec performanceTableGrowthSum 2011,10,2012,10,NULL,10

              GO
```

Retaining daily demand distributions in past fiscal periods

By default, the daily distributions for demand are removed from past fiscal periods by the `Resource Demand Calculation` job. However, you can retain the daily distribution data by specifying a lag period in days after the fiscal period before the data is to be removed.

> **Warning:** If you specify a lag period, then you must monitor the database to manage the database size and avoid performance degradation in certain areas.

The database administrator must run the following query to set the number of days for the lag period. The following query adds a 60 day lag after the end date of the fiscal period.

```
DECLARE @DailyAllocationCleanUpLag INT = 60--- Number of lag days
UPDATE ServerSettings SET DailyAllocationCleanUpLag = @DailyAllocationCleanUpLag
```

8. Installing and Configuring Cognos Analytics

Overview of Cognos Analytics installation and configuration

Installation and configuration of Cognos Analytics takes place in several stages, which are described in the following sections:

- "Stage 1. Creating the Cognos Content Store database" on page 106

- "Stage 2. Installing the Cognos Application Tier" on page 106

- "Stage 3. Configuring the Cognos Application Tier" on page 107

- "Stage 4. Installing the Cognos web components" on page 110

- "Stage 5. Configuring ChangePoint server integration for Cognos Analytics " on page 111

- "Stage 6. Assigning ChangePoint security features for access to Cognos functionality" on page 112

- "Stage 7. Importing the ChangePoint metadata package" on page 112

- "Stage 8. Setting up the data source for IBM Cognos Analytics" on page 113

- "Stage 9. Setting the security settings in Cognos" on page 115

For information about installing the ChangePoint-Cognos Sync Utility, see "About the ChangePoint-Cognos Sync Utility " on page 116.

About installing multiple instances of Cognos Analytics

For information about installing multiple Application Tier and web component instances, see "Installing additional instances of Cognos Application Tier and web components" on page 121.

You can configure Cognos Analytics to use multiple databases, for example to implement a Test and Training setup. For more information, see "Installing additional instances of Cognos Application Tier and web components" on page 121.

To configure Cognos for reports from more than one database, you must create and configure a separate connection to the data source for each database. For more information, see the IBM Cognos Analytics *Business Intelligence Administration and Security Guide*.

Note: For more information about the IBM Cognos Analytics software, see the IBM Cognos Analytics product documentation.

Preparing to install Cognos Analytics

In addition to the standard ChangePoint requirements, you require an overall understanding of the following:

- architecture of a Cognos Analytics solution

- TCP/IP port assignments within the deployment environment (for multiple Application Tier and web component instances)

About roles and feature mapping between Cognos and ChangePoint

Access to Cognos functionality is based on resource roles and features in ChangePoint. During installation, ChangePoint roles are mapped to Cognos groups, and ChangePoint features are mapped to Cognos roles. The Cognos groups and roles control resources' access permissions to objects, such as directories, folders, and content in the Cognos software.

Each Cognos role has a specific set of access permissions. For a description of these roles, see the IBM Cognos Analytics *Business Intelligence Administration and Security Guide*.

The following table shows how the predefined Cognos roles are mapped to ChangePoint features.

Cognos role	ChangePoint feature
ChangePoint Analysis Users	Cognos Professional Author
ChangePoint Authors	Cognos Professional Author
ChangePoint Consumers	Base User License
ChangePoint Directory Administrators	Cognos Administrator
ChangePoint Portal Administrators	Cognos Administrator
ChangePoint Query Users	Cognos Professional Author
ChangePoint Report Administrators	Cognos Professional Author
ChangePoint Server Administrators	Cognos Administrator
ChangePoint Systems Administrator	Cognos Administrator

Installation parameters for Cognos Analytics

Before you start the installation, use the following table to determine the parameter values for your installation. You are prompted for this information during installation and configuration.

Note: For server names, always use the *fully-qualified domain name*.

Field	Description
Destination for Cognos Analytics	The installation path for Cognos Analytics. Default is: C:\Program Files\ibm\cognos\analytics
ChangePoint database server name, and port or instance name	
ChangePoint database name	Default is Changepoint.
ChangePoint database connections account ID and password	SQL account and password used to give the ChangePoint applications access to the database.
Cognos content store database name	ContentStore
SQL server administrator ID and password	"sa" or equivalent account
Cognos dispatcher port (optional)	If required, port to use in place of "9300".
SMTP mail server name and port	Used to send notifications from Cognos
Email account and password	Used to send notifications from Cognos
Email address of default sender	Used as the "From" address on notifications from Cognos
ChangePoint website URL and port	
ChangePoint website name	
Whether ChangePoint website uses SSL	
Cognos Application Tier server name	

Stage 1. Creating the Cognos Content Store database

Note: If you are upgrading Cognos Analytics, do not perform this stage.

1. On the ChangePoint database server, log in as a system administrator.

2. From the root of the Cognos Analytics media, run `setup.exe` as an administrator.

3. Click **Step 1: Create Content Store Database**.

    The **Select Database** appears.

4. In the **Select the SQL Server that ChangePoint is installed on** field, enter the name of the ChangePoint database server.

5. In the **ChangePoint Database Name** field, enter the name of the ChangePoint database. The default name is Changepoint.

6. In the **ContentStore Database Name** field, enter the name of the Cognos ContentStore database.

7. In the **ChangePoint ID** field, enter the login ID of the SQL account used to give the ChangePoint applications access to the database.

8. In the **Login ID** and **Password** fields, enter the SQL server administrator (sa) user ID and password.

9. Click **Start**.

Stage 2. Installing the Cognos Application Tier

1. Log into the Cognos Application Tier server as system administrator.

2. Disable the server's antivirus software, or exclude %ProgramFiles%\IBM.

    Note: If you choose to keep your antivirus software running, the installation will take much longer because the antivirus software scans each file that is installed.

3. From the root of the Cognos Analytics media, run `setup.exe` an an administrator.

4. Click **Step 2: Install and Configure Cognos Application Tier**, and then follow the prompts.

5. At each prompt, select or type the appropriate parameter from the table in "Installation parameters for Cognos Analytics" on page 105.

6. On the **Installation Completed** screen, click **Finish**.

7. Review the installation log (`C:\Program Files (x86)\Changepoint\Changepoint\InstallLog`) to ensure that no warnings were generated during the installation. Follow the instructions to manually resolve the issues,if any.

8. Right-click **Computer**, and select **Properties > Advanced system settings > Performance > Settings > Data execution prevention**.

9. In the **Data Execution Prevention** tab, do one of the following:

    •   Select **Turn on DEP for essential Windows programs and services only**

    •   Select **Turn on DEP for all programs and services except those I select**, then add as exceptions all Cognos executables in the Cognos directories, for example, java.exe, cogbootstrapservice.exe, etc.

        The default Cognos root directory is: `%programfiles%\ibm\cognos\analytics\`

10. If you changed the selected option in step 9, restart the server.

Stage 3. Configuring the Cognos Application Tier

The Cognos Application Tier components are configured using the IBM Cognos Analytics Configuration application.

1. On the Cognos Application Tier server, log in as administrator.

2. From the **Start** menu, launch **IBM Cognos Configuration**.

3. Click **OK** to acknowledge that the configuration files have been updated.

To configure environment properties

1. In the **Explorer** pane, select **Environment**.

2. In the **Environment - Group Properties** pane, for each URI field that includes localhost:9300 (for example, External dispatcher URI), verify that localhost has been changed to the name of the Cognos Application Tier server.

    Some URI fields, for example, Content Manager URIs, have an **Edit** 🖉 button that opens a dialog box to edit multiple URIs

    Note: By default, Cognos Analytics uses port 9300 for the dispatcher. To change the dispatcher port, replace 9300 with the new port number in all dispatcher and Content

Manager URIs. You must provide the URIs of the Internal and External dispatchers in Stages 4 and 5 respectively.

To configure authentication properties

1. In the **Explorer** pane, select **Security > Authentication**.

2. In the **Authentication - Component Properties** pane, **Inactivity timeout in seconds** field, enter 43200.

3. In the **Explorer** pane, select **Security > Authentication > Cognos**.

4. In the **Cognos - Namespace - Resource Properties** pane, **Allow anonymous access?** list, select **False**.

    Note: Set this parameter to **False** regardless of whether you use Single Sign-on (SSO) for ChangePoint.

5. In the **Explorer** pane, right click **Security > Authentication**, and select **New resource > Namespace**.

    The **New Resource - Namespace** dialog box appears.

6. In the **Name** field, enter **Changepoint**.

7. In the **Type (Group)** list, select **Custom Java Provider**.

8. Click **OK**.

9. In the **Explorer** pane, select **Security > Authentication > Changepoint**.

10. Complete the following fields in the **Changepoint - Namespace - Resource Properties** pane:

    a. In the **Namespace ID** field, enter **Changepoint**.

    b. In the **Java class name** field, enter **com.changepoint.cap.CapControl**. The Java class name is case-sensitive.

    c. In the **Selectable for authentication** list, select **True**.

To configure Content Manager properties

1. In the **Explorer** pane, right click **Data Access > Content Manager > Content Store**, and select **Delete**.

2. In the **Explorer** pane, right click **Data Access > Content Manager**, and select **New resource > Database**.

    The **New resource - Database** dialog box appears.

3. In the **Name** field, enter **Content Store**.

4. In the **Type Group** list, select **Microsoft SQL Server database**.

5. Click **OK**.

6. In the **Explorer** pane, select **Data Access > Content Manager > Content Store**.

7. Complete the following fields in the **Content Store - Database - Resource Properties** pane:

    a. In the **Database server with port number or instance name** field, enter the name and port or instance name of the ChangePoint database server.

    b. In the **Database name** field, enter **ContentStore**.

    Note: This is the default name of the content store database that was created in "Creating the Cognos Content Store database" on page 106.

8. Click in the **User ID and password** field, then click the **Edit** button.

9. In the **User ID** field and **Password** and **Confirm Password** fields, enter the SQL account and password used to give the ChangePoint applications access to the database.

10. To test the Content Manager database connection, right click **Data Access > Content Manager > Content Store**, and select **Test**.

To send Cognos workflow notifications by email

1. In the **Explorer** pane, select **Data Access > Notification**.

2. Complete the following fields in the **Notification - Component Properties** pane:

    a. In the **SMTP mail server** field, enter the name and port of the mail server to use to send notifications.

    b. In the **Default sender** field, enter the email address to use as the "From" address on email notifications.

    Note: This does not have to be the same account that is in the **Account and password** field

3. Click in the **Account and password** field, then click the **Edit** 🖉 button, and complete

   the **Value - User ID and password** dialog box:

   a. In the **User ID** field, enter the user ID for any valid account on the mail server. This is the account that notifications are sent from.

   b. In the **Password** and **Confirm Password** fields, enter the password of the user ID account.

   Note: If you do not configure a mail server, when you start the IBM Cognos Analytics service, a warning message appears when the mail server connection is tested. You can ignore the warning.

To increase the timeout value for the Cognos service to start up

You can add an entry to the `cogconfig.prefs` file to increase the timeout value if the Cognos service fails during start up.

1. Exit from the IBM Configuration panel.

2. Open the `cogconfig.prefs` file using Notepad++. The default location of the file is:

   `C:\Program Files\ibm\cognos\analytics\configuration\cogconfig.prefs`

3. Add the following entry to the file:

   `ServiceMaxTries=1200`

   The `ServiceMaxTries` property represents the number of times that IBM Cognos Configuration checks the progress of the start request. The default is 360.

To save the Cognos Application Tier configuration

1. Click **Save**.

2. When the **Close** button is enabled, click it.

3. To start the IBM Cognos Analytics service, open the IBM Cognos Configuration panel, and then click the **Start** button.

Stage 4. Installing the Cognos web components

1. On each ChangePoint web server, sign in as administrator.

2. Disable the server's antivirus software, or exclude %ProgramFiles%\IBM.

Note: If you choose to keep your antivirus software running, the installation will take much longer because the antivirus software scans each file that is installed.

3. From the root of the Cognos Analytics media, run `setup.exe` as an administrator.

4. Click **Step 3: Install the web components on the ChangePoint website** and then follow the prompts.

5. Complete the **ChangePoint Cognos Web Components** dialog box:

   a. In the **Cognos Dispatcher server name** field, enter the server name from the Internal dispatcher URI of the Cognos Application Tier server. For example:

   `cognos.domain.com`

   Note: Do not include the port, or the path `/bi/v1/disp`, or the path `p2pd/servlet/dispatch`

   b. In the **Dispatcher Port** field, enter the port assigned to the internal dispatcher: default 9300, or the value you set in Stage 3.

   c. If the Cognos Application Tier uses SSL, select the **Use SSL for Dispatcher URI** check box.

6. Click **Next**.

7. In the **Choose the ChangePoint Enterprise website** list, select the name of the ChangePoint website

8. In the **Application Pool Name** field, enter the Application Pool name used by Cognos. Default name is **IBM Cognos 11**.

9. Click **Next**, then click **Install**.

Stage 5. Configuring ChangePoint server integration for Cognos Analytics

1. Sign in to ChangePoint Administration.

2. Select **General > Server Integration**.

3. Select the **Enable Cognos integration** check box.

4. In the **Cognos application tier URL** field, enter the external dispatcher URI of the Cognos Application Tier server. For example:

`http://cognos.domain.com:9300/p2pd/servlet/dispatch`

5. Click **Save**.

Stage 6. Assigning ChangePoint security features for access to Cognos functionality

By default, all ChangePoint resources can access **Analytics Portal** and **Create Dashboard** and do the following:

- run reports

- set up report schedules

The **Base User** security feature controls the general access granted to all resources. To allow resources to access other ChangePoint Analytics reporting functionality, you must assign the following Cognos-related features to resources or roles:

- **View Reports** feature – View ChangePoint Analytics reports and other Cognos content in the **Reports** tree view in ChangePoint.

- **Cognos Professional Author** feature – Create or edit a report using the reporting interface, and manage report scheduling. These features provide the same access rights, but you can make them different by granting different access rights or restricting access for one of them in Cognos Analytics.

- **Cognos Administrator** feature – Administer IBM Cognos Analytics software configuration, server settings, and all security aspects; install and run the ChangePoint-Cognos Sync Utility.

For more information about assigning the security features to resources and roles, see the *ChangePoint Administration Guide*.

Stage 7. Importing the ChangePoint metadata package

If you have more than one ChangePoint website, apply this procedure on only one.

1. Sign in to ChangePoint as ChangePoint administrator.

2. Click ⚏ > **Analytics > Portal**. **IBM Cognos Analytics with Watson** appears.

3. Click the **Open menu** icon at top left corner, and then click **Manage > Administration console** . The **IBM Cognos Administration** console appears.

4. Click the **Configuration** tab.

5. In the left pane, click **Content Administration**. **Administration** details appear in the **Configuration** tab.

6. Click the new import icon .

7. In the **Deployment archive** section, select **ContentStore**, then click **Next**.

8. In the **Password** field, enter **Changepoint**, then click **OK**.

9. In the **Specify a name and description** - **New Import Wizard** pane, in the **Name** field, change the default from ContentStore to Import ContentStore.

10. Click **Next**, **Next**, then **Next** again.

11. In the **Select an action** - **New Import Wizard** pane, select the **Save and run once** option, and click **Finish**.

12. Complete the **Run with options** - **Import ContentStore** pane:

    a. In the **Time** option section, select **Now**. All the **Content** check boxes are selected by default.

    b. In the **Report specification upgrade** option section, select **Keep the existing report specification versions**.

    c. In the **Store IDs** option section, select **Do not assign new IDs during import**. Ignore the warning message.

13. Click **Run**, then click **OK**.

14. To view run history and confirm that the package was imported successfully, click **More**, and then click **View run history**.

15. Click **Close**.

    The **Administration** details includes two packages: Import ContentStore and ContentStore. These packages are not required.

16. Select the check boxes for both packages, and click the delete icon .

17. Click **Log off**.

Stage 8. Setting up the data source for IBM Cognos Analytics

Note: If you have more than one ChangePoint web site, apply this procedure on only one.

1. Sign in to ChangePoint as ChangePoint administrator.

2. Click ▦ > **Analytics > Portal**. **IBM Cognos Analytics with Watson** appears.

3. Click the **Open menu** icon at top left corner, and then click **Manage > Administration console** . The **IBM Cognos Administration** console appears.

4. Click the **Configuration** tab.

5. In the left pane, click **Data Source Connections**. **Directory > Cognos** details appear in the **Configuration** tab.

6. Click the new data source icon ▯.

7. In the **Name field**, enter **Changepoint**, and then click **Next**.

8. Complete the **Specify the connection - New Data Source wizard**:

   a. In the **Type** list, select **Microsoft SQL Server (Native Client)**.

   b. In the **Isolation level** field, select **Specify a value** and then select **Read Uncommitted**.

   c. Select the **Configure JDBC connection** check box.

   d. Click **Next**.

9. Complete the **Specify the Microsoft SQL Server (Native Client) connection string - New Data Source wizard**:

   a. In the **Server name** field, enter the name of the database server.

   b. In the **Database name** field, enter the name of the ChangePoint database.

   c. Select the **Signons** option.

   d. Select the **Password** check box.

   e. Select the **Create signon that the Everyone group can use** check box.

   f. In the **User ID** field, and **Password** and **Confirm Password** fields, enter the SQL account and password used to give the ChangePoint applications access to the database.

10. Click the **Test the connection** link:

    a. Click **Test**, then click **Close**.

    b. Click **Close** again.

    c.   Click **Next**.

11. Complete the following fields in the **Specify the Microsoft SQL Server (JDBC) connection string** - **New Data Source wizard**:

    a.   In the **Server name** field, enter the name of the ChangePoint database server.

    b.   In the **Database name** field, enter the name of the ChangePoint database.

12. Click the **Test the connection** link:

    a.   Click **Test**, then click **Close**.

    b.   Click **Close** again.

    c.   Click **Next**.

13. Click **Finish**.

    The ChangePointdata source now appears under **Directory > Cognos** in the **Configuration** tab.

14. Click the **ChangePoint** data source link to display the data source connection, which is also named ChangePoint.

15. Restart Cognos Services on the Cognos Application Tier.

Stage 9. Setting the security settings in Cognos

When Cognos imports user information from ChangePoint, every user is given the Cognos administrator role. This procedure removes that role from all users, except for those users that have specifically been assigned the Cognos Administrator feature.

To remove the administrator role from all ChangePoint users

1. Sign into ChangePoint as ChangePoint administrator.

2. Click **Analytics > Portal**. **IBM Cognos Analytics with Watson** appears.

3. Click the **Open menu** icon at top left corner, and then click **Manage > People**.

4. Click **Accounts > Cognos**

5. Scroll to the **System Administrator** role, and then click **More (…)**.

6. Click **View Members**.

7. Remove **Everyone** by selecting the minus sign (-).

8. Click **OK** to confirm.

About the ChangePoint-Cognos Sync Utility

The ChangePoint-Cognos Sync Utility synchronizes the ChangePoint Analytics of the database with ChangePoint. You must synchronize the data model when:

- you import a base data model that you received from Planview, Inc.. The base data model contains the default field labels for the standard fields in the supported languages.

- you make one or more of the following changes in ChangePoint Administration:

    - create a configurable field

    - modify a configurable field label

    - modify the field label of a standard field that is included in the model

Hardware and software requirements

For details of the hardware and software requirements of the workstation that is used to run the ChangePoint-Cognos Sync Utility, see the *ChangePoint Software Compatibility Matrix* and the *ChangePoint Hardware Recommendations Guide.*

Synchronization process overview

After you upgrade ChangePoint and install and configure Cognos Analytics, you must import the base data model from the new release, and then synchronize the model. This initial synchronization creates a new revision with your configurable fields, and labels that you modified before you upgraded.

New revisions are incremental, which means that only configurable fields that have been added and field label changes that have been made since the previous revision are synchronized.

The length of time for the synchronization depends on the number of configurable fields that you have, and the number of field labels that have been changed in ChangePoint Administration since the last time that a revision was created. Only fields for which values have been entered and saved in ChangePoint are synchronized. That is, if you create a new configurable field for which there are no values, the field and the label for that configurable field are not synchronized.

Tip: Record the length of time that it takes to import the base data model and create the initial revision during testing. This information will help you to plan the production implementation.

Note: Use the fully-qualified domain name for server names.

About the ChangePoint-Cognos Sync Utility log file

The log file `CognosUILog.txt` is located in:

`C:\Program Files (x86)\Changepoint\Changepoint\InstallLog`

Warning: The Sync Utility does not monitor the size of the log file. You must manually delete or truncate the log file.

Ad hoc changes to field labels in reports

To make a one-time field label change in a report without changing the ChangePoint Analytics, either set the Text Source **Source type** to text for the field label and manually override the value in a single language, or set a text source variable for the field label, then use the Cognos Condition Explorer to set the value. For more information, see the IBM Cognos Analytics online help.

About using the Sync Utility with multiple Cognos Analytics instances

When you install the ChangePoint-Cognos Sync Utility, it is configured for a specific database on a specific database server.

Therefore, if you have multiple databases (for example, separate databases for production, test, and training), then you require a separate administrator workstation with the Sync Utility installed on it for each database, even if all of the databases use the same SQL Server version.

Upgrading the Sync Utility

You must always use the version of the Sync Utility that corresponds to the ChangePoint version.

To upgrade the Sync Utility

1. Using Windows Control Panel, uninstall the previous release sync prerequisite and Sync Utility.

2. Delete the sync prerequisite install folder.

3. Install the current release version.

Installing the Sync Utility

By default, the Changepoint-Cognos Sync Utility is installed and configured for the SA version of ChangePoint. To configure the Sync Utility for Changepoint PPM, see step 8.

To install the prerequisites for the sync utility

1. Disable User Access Control.

2. From the root of the Cognos Analytics media, run `setup.exe`.

3. Click the **Cognos Sync Utility** Tab and select **Step 1: Install Changepoint Sync Tool Prerequisites**. The Sync Tool prerequisites must be reinstalled on each client.

4. Click **Next**, then click **Install**.

To install the sync utility

1. As administrator, from the root of the Cognos Analytics media, run `setup.exe` as an administrator.

2. Click on the Cognos Sync Utility Tab and select **Step 2: Install Changepoint Sync Utility**.

3. In the **Cognos Dispatcher Server Name** field, enter the name of the Cognos Application Tier server.

4. In the **Dispatcher Port** field, enter the port used for the Cognos dispatcher.

5. If the Cognos Application Tier uses SSL, select the **SSL Enabled** check box.

6. Click **Next**, then click **Install**, then click **Finish**.

7. In the **Changepoint Connection Settings** dialog box:

   a. In the **Connection Settings** list, select **Changepoint Window Service, Scheduled jobs and Utilities**.

   b. In the **File location** field, browse to:

```
C:\Program Files (x86)\Changepoint\Cognos Client Tools\Cognos Client Tools\
CognosClientTools.exe.config
```

   For more information, see "Configuring database connection settings" on page 65

   A shortcut named **Changepoint Cognos Sync Utility** is added to the **Start** menu.

8. To configure the Sync Utility for Changepoint PPM:

a. Open the `CognosClientTools.exe.config` file in a text editor.

b. Search for the `CompanyProfile` key, and change the value from `PSO` to `ITD`.

c. Save and close the file.

9. Import the initial base data model from the Cognos Analytics media Setup/Model folder.

Uninstalling the Sync Utility

You uninstall the Sync Utility from the **Windows Control Panel**.

Importing the base data model

When you import a base data model, the previously imported base data model and later revisions are replaced by the newly imported base data model.

> **Note:** To add configurable fields and field label changes to the model, you must create a new revision after importing a base data model.

1. Launch the Changepoint-Cognos Sync Utility, and sign in with your user ID and password.

2. In the **Changepoint-Cognos Sync Utility** dialog box, click **Import Revision**.

3. Select the zip file that corresponds to the ChangePoint version:

   • Model.zip (Changepoint SA)

   • Model-ITD.zip (Changepoint PPM)

4. Click **OK**.

Adding customized field labels and configurable fields to the data model

To add configurable fields and field label changes to the data model, you must create a new revision after importing the base data model.

1. Launch the Changepoint-Cognos Sync Utility, and sign in with your user ID and password.

2. In the **Changepoint-Cognos Sync Utility** dialog box, click **New Revision**.

   The **New Revision** dialog box appears.

3. In the **Comments** field, enter a comment.

4. Do the following:

   • To import configurable fields, select the **Include configurable field delta** check box.

- To import new or changed field labels or page content strings, select the **Include language string delta** check box.

5. Click **Publish Model**.

6. Advise report creators to open each of their reports in the Analytics Portal and follow the prompts to accept the changed package.

Reverting to a previous version of the base data model

You can revert to the imported base data model, or to a previous revision. All revisions that were published after the one you revert to are deleted.

1. Launch the Changepoint-Cognos Sync Utility, and sign in with your user ID and password.

2. In the **Changepoint-Cognos Sync Utility** dialog box, double-click the version you want to revert to.

3. In the **Model Detail** dialog box, click **Revert model**.

4. Advise report creators to open each of their reports in the Analytics Portal and follow the prompts to accept the changed package.

9. Installing additional instances of Cognos Application Tier and web components

About installing additional instances of Cognos Application Tier and web components

You can install additional instances of the Cognos Application Tier on a server and the web components on a web server. For example, you could create a combined Test and Training environment using a single physical server for the Cognos Application Tier instances, and a single physical web server for the ChangePoint websites.

> **Note:** The initial instances of the Cognos Application Tier, content store database, and web components must be installed using the installer supplied by Planview, Inc..

All procedures must be executed as an administrator.

Installation parameters for additional instances of Cognos Application Tier and web components

The following table lists the parameter values that you will require during installation and configuration.

> **Note:** Use the fully-qualified domain name for server names.

Field	Description
ChangePoint database server name, and port or instance name	
ChangePoint database name	
Cognos ContentStore database name	
ChangePoint database connections account ID and password	SQL account and password used to give the ChangePoint applications access to the database.
ChangePoint website URL and port	
ChangePoint website name	

Field	Description
Cognos Application Tier server name	
Port to use for new Cognos instances	Default port for the initial instance is 9300
Local log server port	Default port for the initial instance is 9362
Local shutdown port	Default port for the initial instance is 9399
SMTP mail server name and port	Used to send notifications from Cognos
Email account and password	Used to send notifications from Cognos
Email address of default sender	Used as the "From" address on notifications from Cognos

Installing an additional Cognos Application Tier instance

The content store database is installed on the ChangePoint database server. Each Application Tier instance requires a separate content store database.

> **Warning:** Be sure to specify a different ContentStore database name and ChangePoint database than the names used on the existing installation. If you use the names from the existing installation, you will damage it.

Installing an additional content store database

You can use the installer from the Cognos Analytics media to install an additional Cognos ContentStore database.

1. On the ChangePoint database server, log in as a system administrator.

2. From the root of the Cognos Analytics media, run `setup.exe` as an adminstrator.

3. Click **Step 1: Create Content Store Database**.

    The **Select Database** appears.

4. In the **Select the SQL Server that Changepoint is installed on** field, enter the name of the ChangePoint database server.

5. In the **Changepoint Database Name** field, enter the name of the additional ChangePoint database.

6. In the **ContentStore Database Name** field, enter the name of the additional Cognos ContentStore database.

7. In the **Changepoint Id** field, enter the login ID of the SQL account used to give the ChangePoint applications access to the database.

8. In the **Login ID** and **Password** fields, enter the SQL server administrator (`sa`) user ID and password.

9. Click **Start**.

Installing an additional Cognos Application Tier component

1. Log into the Cognos Application Tier server as system administrator.

2. Close the IBM Cognos Configuration panel, if open.

3. From the root of the Cognos Analytics media, run `setup.exe` as an administrator.

4. Click **Step 2: Install and Configure Cognos Application Tier**, and then follow the prompts. Dispatcher port number 9400 is assigned to the second instance if 9300 was assigned to the first instance.

5. To avoid damaging the existing installation, you must ensure that the installation directory is unique (for example, `C:\Program Files\ibm\cognos\analytics_at2`).

6. On the **Installation Completed** screen, click **Finish**.

7. Review the installation log (`C:\Program Files (x86)\Changepoint\Changepoint\InstallLog`) to check for warnings. Follow the instructions to manually resolve any warnings.

Configuring an additional Cognos Application Tier component

The Cognos Application Tier components are configured using the IBM Cognos Configuration application.

Launch the newly installed instance, for example:

```
All Programs > IBM Cognos - AppTier2 > IBM Cognos Configuration
```

where IBM Cognos - AppTier2 is the unique shortcut folder name you entered in "Installing an additional Cognos Application Tier component" on page 123.

Note: A shortcut is created for each instance. You can also launch the IBM Cognos Configuration from the following folder:

```
C:\Program Files\ibm\cognos\analytics\bin64\cogconfigw.exe
```

To configure environment properties

1. In the **Explorer** pane, select **Environment**.

2. Complete the following fields in the **Environment - Group Properties** pane:

3. For each URI field that includes `localhost:9300`, replace:

   • `localhost` with the name of the Cognos Application Tier server

   • `9300` with the port for the new application instance

To configure notification properties

1. In the **Explorer** pane, select **Notification**.

2. In the **Notification** - **Component Properties** pane, in the **SMTP mail server** field, enter the name and port of the mail server to use to send notifications.

To configure Content Manager properties

1. In the **Explorer** pane, right-click **Content Store** and select **Delete**.

2. In the **Explorer** pane, right click **Data Access > Content Manager**, and select **New resource > Database**.

3. Complete the **New resource - Database** dialog box:

   a. In the **Name** field, enter the name of the content store database you created earlier, for example, ContentStore_CS2.

   b. In the **Type** list, select **Microsoft SQL Server database**.

   c. Click **OK**.

4. In the **Explorer** pane, select **Data Access > Content Manager > Content Store**.

5. Complete the following fields in the **Content Store - Database - Resource Properties** pane:

    a.   In the **Database server with port number or instance name** field, enter the name and port or instance name of the ChangePoint database server.

    b.   In the **Database name** field, enter the name of the content store database you created earlier, for example, ContentStore_CS2.

6. Click in the **User ID and password** field, then click the **Edit** 🖉 button, and complete the **Value** - **User ID and password** dialog box:

    a.   In the **User ID** field, enter the SQL account used to give the ChangePoint applications access to the database.

    b.   In the **Password** and **Confirm Password** fields, enter the password of the SQL account.

7. Click **OK**.

To configure authentication properties

1. In the **Explorer** pane, select **Security > Authentication**.

2. In the **Authentication** - **Component Properties** pane, in the **Inactivity timeout in seconds** field, enter 43200.

3. In the **Explorer** pane, select **Security > Authentication > Cognos**.

4. In the **Cognos** - **Namespace** - **Resource Properties** pane, in the **Allow anonymous access?** list, select **False**.

    Note: Set this parameter to **False** regardless of whether you use Single Sign-on (SSO) for ChangePoint.

5. In the **Explorer** pane, right click **Security > Authentication**, and select **New resource > Namespace**.

6. Complete the **New Resource** - **Namespace** dialog box:

    a.   In the **Name** field, enter Changepoint.

    b.   In the **Type** list, select Custom Java Provider.

    c.   Click **OK**.

7. In the **Explorer** pane, select **Security > Authentication > Changepoint**.

8. Complete the following fields in the **Changepoint - Namespace - Resource Properties** pane:

   a. In the **Namespace ID** field, enter `Changepoint`.

   b. In **Java class name** field, enter `com.changepoint.cap.CapControl`. The Java class name is case sensitive.

   c. In the **Selectable for authentication** list, select **True**.

9. Click **Test**.

10. Save the configuration file.

11. Click **Start**.

Installing additional Cognos web component instances on a single server

> **Warning:** Be sure to specify different Application Pool name and ChangePoint website names than the names used on the existing installation. If you use the names from the existing installation, you will damage it.

Installing an additional Cognos web component

1. On the ChangePoint web server, sign in as administrator.

2. From the root of the Cognos Analytics media, run `setup.exe` as an administrator.

3. Click **Step 3: Install the web components to enable Cognos Analytics on the Changepoint website**.

4. Follow the prompts.

5. In the **CP_CognosWebComponents** dialog box:

   a. In the **Cognos Dispatcher server name** field, enter the server name from the Internal dispatcher URI of the Cognos Application Tier server. For example:

   `cognos.domain.com`

   Note: Do not include the port, or the path `/bi/v1/disp`, or the path `p2pd/servlet/dispatch`.

   b. In the **Dispatcher Port** field, enter the port assigned to the internal dispatcher that will be used for the additional installation.

    c.   If the Cognos Application Tier uses SSL, select the **Use SSL for Dispatcher URI** check box.

6.   Click **Next**.

7.   In the **Choose the Changepoint Enterprise website** list, select the name of the additional Changepoint website that you will install the Cognos web components on.

8.   In the **Application Pool Name** field, enter a unique Application Pool name (for example, `IBM Cognos 11_2`) that will be used by Cognos.

    Warning: Do not use an existing application pool name.

9.   Click **Next**, then click **Install**.

10. Complete the configuration by doing the following:

- "Stage 5. Configuring ChangePoint server integration for Cognos Analytics " on page 111

- "Stage 6. Assigning ChangePoint security features for access to Cognos functionality" on page 112

- "Stage 7. Importing the ChangePoint metadata package" on page 112

- "Stage 8. Setting up the data source for IBM Cognos Analytics" on page 113

- "Stage 9. Setting the security settings in Cognos" on page 115.

11. Import the base data model.

Pointing the Cognos web component to a different server

1.   On the ChangePoint web server, launch IIS Manager.

2.   Under the Changepoint Enterprise website, locate the ibmcognos application.

3.   On the /ibmcognos Home page in the IIS section, double-click **URL Rewrite**.

4.   on URL rewrite page detail, double-click ARR All folder.

5.   On the **Edit Inbound Rule** page, in the **Action** section, **Rewrite URL** field, change the Cognos instance name and port number. For example:

```
http://cognosB.com:9500/{R:0}
```

Configuring the Custom Authentication Provider (CAP) manually

The following procedure configures the ChangePoint database that is used by Cognos for login authentication.

1. You must use the instance of `java.exe` that is installed with Cognos to configure the CAP. It is strongly recommended that you include the path to the `java.exe` instance in the **path** system environment variable:

    ```
    C:\Program Files\ibm\cognos\analytics\ibm-jre\jre\bin
    ```

2. Run the following statements from a command line in the `<new cognos instance>\webapps\p2pd\WEB-INF\lib` directory. For example:

    ```
    %programfiles%\ibm\cognos\analytics_at2\webapps\p2pd\WEB-INF\lib
    ```

    where `analytics_at2` is the unique installation directory name that you entered in "Installing an additional Cognos Application Tier component" on page 123.

3. Encrypt the database connection parameters:

    ```
    java -jar changepointCAP.jar file ..\..\..\..\configuration\CAP.properties
    <sqlserver> <userid> <password> <ChangepointDB>
    ```

    where:

    - sqlserver – name of the ChangePoint database server. If required, include the instance name.

    - userid – SQL account used to give the ChangePoint applications access to the database.

    - password – password for the SQL account.

    - ChangepointDB – name of the database.

4. Test the Encrypted Database Connection Parameters:

    ```
    java -jar changepointCAP.jar ..\..\..\..\configuration\CAP.properties
    ```

10. Configuring Intelligent Forms

About Intelligent Forms

Intelligent Forms is a wizard-driven solution for entering data and generating documents. You use Intelligent Forms to simplify work for resources by streamlining complex tasks and automating data entry processes.

The ChangePoint Intelligent Forms connector integrates Intelledox Infiniti with ChangePoint. After the connector is installed and the standard form templates are configured, resources can access the standard forms from the ChangePoint interface. The forms guide resources through the process of creating or updating an entity record or creating a document. Resources with Infiniti administrator access can access Infiniti Manage from the **Intelligent Forms** menu in ChangePoint Administration.

This document includes instructions that are specific to using Infiniti Manage with ChangePoint. For general information about using Infiniti Manage, please refer to the Intelledox Knowledge Base, which is available at:

https://knowledgehub.intelledox.com/

Standard form templates

ChangePoint includes seven standard form templates, which can be used as-is, or which can be used as templates and enhanced to meet business requirements. The standard form templates that create entity records include all of the standard fields that are mandatory by default.

> **Note:** The Create Project Request form is preconfigured to support three request types in ChangePoint: Issue, Risk, and Change Request. If you use different request types then you must update the form with the appropriate request types. If you require any assistance in applying this change, please contact Changepoint services.

> **Note:** Before you can use the standard form templates in your ChangePoint installation, you must add all of the mandatory fields that are specific to your organization. This includes both standard ChangePoint fields and configurable fields that have been set as mandatory in metadata.

Form Purpose	How to access the form
Create Contract Create a customer and contacts, contract, project, tasks, and knowledge management items.	> Create Contract
Create Opportunity Create an opportunity from a customer profile.	Customer profile > Actions menu > View > Intelligent Forms > Create Opportunity
Create Project Create a project from a contract profile.	Contract profile > Actions menu > View > Intelligent Forms > Create Project
Create Project Request Create a request from a project profile.	Project profile > Actions menu > View > Intelligent Forms > Create Project Request
Project Status Report Create a status report from a project profile.	Project profile >Actions menu > Project Status Report
Statement of Work (SOW) Create a statement of work from a contract profile.	Contract profile > Actions menu > View > Intelligent Forms > Statement of Work (SOW)
Generate Invoice Document Generate an invoice document in PDF format.	Invoice profile > Actions menu > View > Intelligent Forms > Invoice Document

Configuring Intelligent Forms

After installing Intelligent Forms, you must do the following.

1. Ensure that the database connection settings have been configured for Intelligent Forms, Infiniti Scheduler, and Intelligent Forms (Manage and Produce). For more information, see "Configuring Database Connection Settings" on page 65.

2. Configure the settings for token authentication:

   a. In the \CP Web Services\Web.config file, replace the default value of the APISharedSecret setting with a unique string of UTF-8 characters with a recommended size of 64 bytes. For example, you can use any combination of 64 single byte characters.

   b. In the `Intelligent Forms\Websites\Produce\appsettings.json` file, replace the value of APISharedSecret with the same unique string used above.

3. Sign into ChangePoint Administration.

4. Import the ChangePoint license file (.lic) for Intelligent Forms (**Tools > License Management**).

5. In user setup (**Resources > User Setup**), assign either the security feature **Access Forms Administration** or **Access Document Administration** to your user. These security features allow you to access Infiniti Manage from ChangePoint Administration.

6. Sign out of ChangePoint and then sign back in to trigger the security feature changes.

7. In ChangePoint Administration, click **Intelligent Forms > Infiniti Manage**.

8. Sign in to Infiniti Manage using "admin" for both the user name and password. "License invalid" appears in the Licensing view.

9. Import the temporary license file that you obtained when preparing to install or upgrade:

    a. In the **License Holder** field, enter the name of your organization.

    b. Beside **Upload New License File**, click **Choose File** and then select the temporary license file.

    c. Click **Save**.

    Note: While a temporary license file is being used, "Test Form Only – Powered by Intellefox Infiniti" appears on standard forms.

10. To obtain a license file:

    a. Beside the **Tenancy Key** field, click **Copy To Clipboard**.

    b. In the **Tenancy Key** field, select (highlight) the value.

    c. Click **Copy To Clipboard** again, and then paste and save the value in a text document.

    d. Send the text document to your customer support manager to request a license file.

11. Click **Data Sources** and then update the connection strings for each of the data sources as follows:

    a. Click the data source name link.

    b. On the **Edit Data Source** panel complete the fields as follows:

    c. **Connection Type** field, select SQL Server

    d. In the **Connection Attributes** field, enter the following:

```
Initial Catalog={{ChangepointDBName}};Data Source={{ChangepointDB Server}}
```

  e. In the **Credentials** section, enter the User Name and Password that is used for Changepoint database connection.

  f. Click **Test Connection**. The **Connection successful** message appears.

  g. Click **Save**.

12. Access each form project, click **Design** and then add the user-defined mandatory fields for the entities:

   • Create Engagement (customer, contact, engagement, project, task, task assignment)

   • Create Opportunity (customer, opportunity)

   • Create Project (project, task, task assignment)

   • Create Project Request (request)

   Note: For more information about using **Design**, see the Intelledox knowledge base or contact ChangePoint support to engage professional services

13. In ChangePoint Administration, assign the security features for Intelligent Forms to resources as required. For more information about the security features, see the *Security Access Reference Guide* or the online help.

14. If you are upgrading from a version prior to ChangePoint 2022, note that the terms "engagement" and "company" remain in existing Intelligent Forms forms. To update the terms to "contract" and "customer", you can import the new forms, and add the applicable fields. The new forms are available in the following folder on the ChangePoint product media:

```
\Enterprise\Changepoint\Intelligent Forms\Forms
```

Configuring Intelligent Forms on an SSO environment

To enable Intelligent Forms to work on a ChangePoint SSO environment, you must enter the email address (**Email**) and password (**Web password**) for each resource into their user account in ChangePoint. The email and password is required by the API for forms authentication.

Note: The WebServicesAPI site under Enterprise must be set as Application Authentication.

Configuring Intelligent Forms in a load-balanced environment

If you are installing Intelligent Forms in a load-balanced environment, you must ensure that all of the URLs are configured to point to the same instance of a website and not to the Load Balancer URL because the underlying security token must always be generated from the same website.

1. Sign in to Infiniti Manage.

2. Click **Settings > Connector Settings**.

3. Select **Changepoint**.

4. Ensure that all of the URLs are configured to point to the same instance of a website and not to the Load Balancer URL.

11. Installing and Configuring Single Sign-on (SSO)

About ChangePoint and SSO

You can implement Single Sign-On (SSO) capabilities for ChangePoint users.

The following implementation options are available using Secure Token Service (STS):

- Installing SSO using ISAPI (HTTPS optional)

- Installing SSO using WS-Federation for ADFS implementations (HTTPS required)

- Installing SSO using SAML for ADFS implementations (HTTPS required)

- Installing SSO using SAML for PingFederate implementations (HTTP required)

- Install SSO using SAML for Azure Active Directory implementations (HTTPS required)

The installation instructions for the implementations are available on the Customer Success Center (https://success.planview.com/Planview_Changepoint).

The configuration scripts for ISAPI and application authentication can optionally enable SSL.

> **Note:** Information on additional unsupported SSO providers are available as tech notes from your customer support representative or client manager.

SSL

If you are using SSL with SSO, the SSO scripts enable SSL in the configuration files.

If you are using SSL with application authentication, the application authentication script has an option to enable SSL.

Configuration of scripts and certificates

In each of the procedures that follow, you run one or more PowerShell scripts. These scripts are used to install required certificates and to modify ChangePoint configuration files.

Copy the contents of the `\Changepoint\Utilities\Configuration\` folder on the ChangePoint product media to `\<cp_common>\Configuration\`.

ChangePoint MSP add-in and SSO

For Internet Explorer, users must use their domain user account and password when required to sign in to access ChangePoint for example at first sign and subsequent sign ins if they have not selected the option to stay signed in.

Using Internet Explorer on a SAML ADFS environment

Users must configure Internet Explorer by adding the ADFS server URL to the local intranet zone and enabling the option for automatic logon only in the intranet zone.

> **Note:** On ADFS on-premise environments, users must sign in using their domain email account and password each time they click **Link ChangePoint Project**.

1. In Internet Explorer, launch **Internet Options**.

2. To add the ADFS server URL to the local intranet zone:

   a. In the **Security** tab, click **Local intranet**, and then click **Sites**.

   b. In the **Local intranet** dialog box, click **Advanced**.

   c. In the **Add this website to the zone**, enter the URL for the ADFS server and then click **Add**.

   d. Click **Close**, then click **OK**.

3. To enable automatic logon only in the intranet zone:

   a. In the **Security** tab, click **Custom level**.

   b. In the **Settings** dialog box, for the **User Authentication** option (at the bottom), select **Automatic logon only in Intranet zone**.

   c. Click **OK**, and then **OK**.

Other ChangePoint add-ins and SSO

The type of authentication used on the ChangePoint website determines whether end users are required to sign in when they use an add-in for the first time in a ChangePoint session.

ChangePoint authentication type	End-users required to sign in
Application authentication	Yes
ISAPI	No
ADFS 2.0	Yes
SAML 2.0 / ADFS 2.0	Yes

About application authentication

By default, ChangePoint websites are installed with application authentication for end-user sign in. Some websites and features require application authentication, and some require integrated Windows authentication. The following websites and features require application authentication:

blah blah blah

- Client Portal website

- Survey Response website

  For more information, see "Setting up a survey response website" on page 144.

Using both application authentication and SSO

You can configure a ChangePoint website for either application authentication or SSO, but not both. However, to use both application authentication and SSO, you can do the following:

1. Create two website instances that point to the same ChangePoint database.

2. Configure one website instance for SSO and the other for application authentication.

3. Distribute the URLs for the website instances to users according to the type of access you want to give them.

Implementing application authentication

You can use these procedures to do either of the following:

- revert a website to application authentication after having implemented one of the SSO implementations

- configure ChangePoint to use application authentication with SSL

Configure PowerShell

1. Open a Windows PowerShell prompt.

2. Modify the execution policy:

```
Set-ExecutionPolicy Unrestricted
```

Stage 1 – Collect configuration parameters

Determine the actual values for the following items. They are used as replacement parameters during configuration.

Parameter	Description
Enterprise_URI	The domain identifier that you use for ChangePoint, for example: `https://changepoint.abc.corp`
Enterprise_Path	The location of the ChangePoint web application files. Default: `<cp_root>\Enterprise\`
RequireHTTPS	Require HTTPS (True/False) Default: `False`.

Stage 2 – Execute configuration scripts

Use the information collected in stage 1 to modify the configuration of the websites.

1. Open a PowerShell prompt.

   Note: If the server has User Account Control enabled, you must open the PowerShell prompt using elevated administrator permissions.

2. Navigate to the Web Service configuration directory, default:

`<cp_common>\Configuration\Enterprise`

3. Execute:

`./Configuration_AppAuth.ps1`

4. Follow the prompts.

Authentication configuration scenarios

Scenario 1

IF a user is authenticated on the domain (for example, a user who is physically in the office and logged on to the domain/network with AD credentials)

AND the IdP site (somename.yourdomain.com) is part of the user's trusted sites in IE

AND the user's AD account is valid/active

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is specified in ChangePoint

THEN the user will automatically be signed into ChangePoint.

Scenario 2

IF a user is authenticated on the domain (for example, a user who is physically in the office and logged on to the domain/network with AD credentials)

AND the IdP site (somename.yourdomain.com) is part of the user's trusted sites in IE

AND the user's AD account is valid/active

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is NOT specified in ChangePoint

THEN the user will be presented with the native ChangePoint sign-in AFTER they have been authenticated against the IdP.

Scenario 3

IF a user is authenticated on the domain (for example, a user who is physically in the office and logged on to the domain/network with AD credentials)

AND the IdP site (somename.yourdomain.com) is NOT part of the user's trusted sites in IE

AND the user's AD account is valid/active

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is specified in ChangePoint

THEN the user will be prompted with an AD login dialog box when accessing ChangePoint

The user MUST authenticate via the IdP BEFORE they are signed into ChangePoint.

Scenario 4

IF a user is authenticated on the domain (for example, a user who is physically in the office and logged on to the domain/network with AD credentials)

AND the IdP site (somename.yourdomain.com) is NOT part of the user's trusted sites in IE

AND the user's AD account is valid/active

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is NOT specified in ChangePoint

THEN the user will be prompted with an AD login dialog box when accessing ChangePoint

The user MUST authenticate via the IdP BEFORE they are presented with the native ChangePoint sign-in dialog box.

Scenario 5

IF a user is NOT authenticated on the domain (for example, a user who is on the public internet, such as a subcontractor, an employee using a home computer, and so on)

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is specified in ChangePoint

THEN the user will be prompted with an AD login dialog box when accessing ChangePoint

The user MUST authenticate via the IdP BEFORE they are signed into ChangePoint.

Scenario 6

IF a user is NOT authenticated on the domain (for example, a user who is on the public internet, such as a subcontractor, an employee using a home computer, and so on)

AND SSO has been configured on both the ChangePoint site and the IdP site

AND the user's UPN is NOT specified in ChangePoint

THEN the user will be prompted with an AD login dialog box when accessing ChangePoint

The user MUST authenticate via the IdP BEFORE they are presented with the native ChangePoint sign-in dialog box.

12. Installing and Configuring Other Optional Applications, Features, and Services

Installing the ChangePoint online help

You install the English online help from the ChangePoint product media.

The version of help (ChangePoint SA or PPM) that appears when launched from the interface is determined by the mode that was selected when the websites were installed. You must install the online help on each ChangePoint instance.

1. On the ChangePoint product media, run:

    ```
    \Changepoint\Online Help\setup.exe
    ```

2. Click **Next**, accept the license terms, then click **Next** again.

    The **Select Features** screen displays.

3. Select the check boxes for the type of online help to install.

4. Click **Next**.

5. Select the folders for the ChangePoint applications (not the Help subfolder) that you are installing. Client Portal help is installed with the ChangePoint help.

6. Click **Next**.

    When the installation is complete, the **InstallShield Wizard Complete** screen displays.

7. Click **Finish**.

8. If you have multiple ChangePoint websites, install the help on the remaining websites.

9. Confirm that the online help launches by signing in to each of the websites and selecting the **Help** menu option.

Once the online help is installed, it becomes part of the ChangePoint website and is removed only if the website is uninstalled.

Setting up the Changepoint Mobile app

The topic covers the setup required to enable users to use the Changepoint Mobile app.

1. Obtain the license for the Access Mobile Application (AMA) security feature, which includes the values for the keys:

- • NotificationProvider.Key1

- • NotificationProvider.Key2

2. Uncomment the keys and add the values for them into the following configuration files:

- • `Enterprise\WebApi\web.config`

- • `Changepoint\Changepoint Mail Service\CPMail.exe.config`

3. Ensure the server where Changepoint and the Changepoint Mail Service are installed can communicate through the firewall with Amazon Web Services at:

   `https://sns.us-west-2.amazonaws.com`

4. Advise users of the following information:

- • Changepoint Mobile app is available at the online app stores.

- • ChangePoint URL or domain, and the user ID and password that are required to sign in to the app.

- • ChangePoint functionality that is available in the app.

   Note: The Changepoint Mobile app is designed to be intuitive and easy to use, and it supports a subset of the functionality of the desktop ChangePoint application. Therefore there is no end user documentation for the app.

Setting up mobile access to Changepoint

Note: This topic refers to setting up the use of mobile devices to access the ChangePoint website. For information about setting up the ChangePoint mobile app, see "Setting up the Changepoint Mobile app" on the previous page.

The ChangePoint start page automatically detects mobile browsers and redirects them to the mobile login page.

For information on supported mobile devices, see the *ChangePoint Software Compatibility Matrix*.

Review the default period of inactivity for the Session Clean Up scheduled job, and change if necessary. For information on the Session Clean Up scheduled job, see "Session Clean Up scheduled job" on page 95.

For information on configuration settings for mobile access, see "Mobile access settings" on page 194.

Configuring the OData Service

The OData Service is automatically installed with ChangePoint. The OData Service is required to access ChangePoint data through Cognos datasets using tools such as Power BI and Excel.

> **Note:** The OData Service is dependent on ChangePoint 2022-R10 22.00.052.000.

For information about setting up access to the OData service, see "Setting up OData access to ChangePoint data for reporting" on page 221.

1. In the OData Service\Web.config file, configure the ChangePointFetchDataUrl key with the ChangePoint website URL:

    a. Open the `<cp_root>\Enterprise\ODataService\Web.config` file.

    b. In the "ChangePointFetchDataUrl" key, replace "http://mylocalweb" with the ChangePoint website URL.

Setting up a Client Portal website

If enhanced session management has been enabled in ChangePoint Administration, you must create a separate Client Portal website.

1. Use the InstallShield Wizard to create a new ChangePoint website on the target server.

    •   For information on using the wizard, see "Installing ChangePoint using the installer" on page 25.

    •   If you already have a ChangePoint website on this server, see "Installing multiple ChangePoint instances" on page 26.

2. Do not install SSO, but allow the website to default to application authentication.

3. Use the Login Settings utility to configure the database connection settings. For more information, see "About configuring database connection settings" on page 65.

4. Remove the following login file from the root level of the website:

    `fclogin.aspx`

5. In IIS, change the default document to the following login file, which is located at the root level of the website:

    `fcelogin.asp`

6. In ChangePoint Administration, do the following:

    a. Define the Client Portal login URL that will be included in the email notifications (**General > Email Integration**).

    b. Enable the standard Client Portal email templates (**General > Email Templates**.)

    c. Set up Client Portal (**Client Portal Management**).

7. To set up the Client Portal website for SSL, see "About setting up ChangePoint websites for SSL" on page 51.

Setting up a survey response website

A survey response website is required to allow clients, customers and internal resources to access the Survey system and respond to surveys.

1. Use the InstallShield Wizard to create a new ChangePoint website on the target server.

   - For information on using the wizard, see "Installing ChangePoint using the installer" on page 25.

   - If you already have a ChangePoint website on this server, see "Installing multiple ChangePoint instances" on page 26.

2. Do not install SSO: allow the website to default to application authentication.

3. Use the Login Settings utility to configure the database connection settings. For more information, see "About configuring database connection settings" on page 65

4. Remove the following login files from the root level of the new ChangePoint website:

   ```
   fclogin.aspx
   fcelogin.asp
   ```

5. In IIS, change the default document for the new ChangePoint website to the following file, which is located at the root level of the new ChangePoint website:

   ```
   sredir.asp
   ```

6. In ChangePoint Administration, define the URL that will be included in the Changepoint email notifications to survey recipients (**General > Email Integration**).

7. To set up the Survey Response website for SSL, see "About setting up ChangePoint websites for SSL" on page 51.

About Microsoft Exchange/Outlook synchronization

The following calendar synchronization options are available:

- Server-side (Exchange) – Server-side synchronization is handled through the ChangePoint Exchange Synchronization Service, and supports the synchronization of calendar entries only. Each user must select one synchronization method in the **Preferences** view of ChangePoint. No client-side installation is required.

- Client-side (Outlook) – The ChangePoint Outlook Tools must be installed on the users' desktops. For more information, see the *User Basics User Guide* or the ChangePoint online help. No server-side installation is required.

ChangePoint supports running a server-side synchronization and client-side synchronization deployment in one environment. Each user must select one synchronization method in their ChangePoint preferences.

Users are discouraged from switching back and forth between the syncronization methods, which can result in duplicate entries. During a switch, the ability to completely restore data is dependent on the synchronization direction selected in the ChangePoint Exchange Synchronization service configuration file. The synchronization direction is controlled at the server level and cannot be directly controlled by the end user.

If a user changes from Outlook to Exchange synchronization, the resynchronization repopulates the cleared ChangePoint calendar entries based on the Exchange data. If the user changes from Exchange to Outlook synchronization, the cleared ChangePoint calendar entries are repopulated based on the Outlook data that is in the date range specified when the batch synchronization is run from Outlook.

Synchronization direction

Calendar synchronization is either one-way or two-way depending on whether the process is real-time or batch. Calendar synchronization requires that the calendar items in Outlook match the General Calendar Synchronization Options settings (Daily Start Time, Daily End Time and Time Zone) in the **Preferences** view in ChangePoint.

About Microsoft Project Desktop integration

No server-side configuration is required. Users must install the ChangePoint Microsoft Project (MSP) COM Add-in on their desktops in order to link a ChangePoint project to MSP through the MSP interface. For more information, see the *ChangePoint User Basics User Guide* or online help.

Configuring batch printing

You can create different print directories and use different printers for different workgroups by using the htmlprint utility. All invoices, cross charges, and credit notes generated by the batch printing report will be saved to the appropriate directory according to the workgroup of the resource who runs the report.

Note: The BatchPrint directory is automatically installed if you selected the **Complete** option when installing ChangePoint.

1. If you upgraded ChangePoint, delete the BatchPrint directory.

2. Install the BatchPrint directory on the web server by doing one of the following:

    • Use the ChangePoint installer to install BatchPrint (**Custom** > **Select Features** page > **Batch Print** check box).

    • Copy the BatchPrint directory and its contents from the ChangePoint product media:

    ```
    \Changepoint\Manual Install\Components\BatchPrint
    ```

3. On the web server, run:

    ```
    <cp_root>\BatchPrint\htmlprint.exe
    ```

4. Review the license, and then close the Bersoft HTMLPrint window.

    The htmlprint.ini file is added to the BatchPrint directory.

5. Open the htmlprint.ini file:

    a. Record the information in the [Printers] section, for example:

    ```
    [Printers]
    0=\\printserver\printerA
    1=\\printserver\printerB
    2=local printer
    ```

    b. Close the file.

6. Configure the database connection settings for the Batch Print configuration file (PrintInvoices.exe.config) using the Login Settings utility (Login Settings.exe).

    For more information, see "Configuring database connection settings" on page 65.

7. Open the PrintInvoices.exe.config file in the BatchPrint directory, and locate the following entry.

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

In the `value` attribute, insert the printer name (from the `[Printers]` section) for the printer that you want to use as the default printer for batch printing. For example:

```
<add key="PrintServername" value="\\printerserver\printerA"/>
```

8. To set up different print directories and use different printers for different workgroups:

   a. Under the BatchPrint directory, create subdirectories for the workgroups. Do not use spaces in the subdirectory names. For example:

```
<cp_root>\BatchPrint\Finance
<cp_root>\BatchPrint\Sales
<cp_root>\BatchPrint\Marketing
```

   b. For each workgroup subdirectory, create a `utility` subdirectory for the batch print files for the workgroup. For example:

```
<cp_root>\BatchPrint\Finance\utility
<cp_root>\BatchPrint\Sales\utility
<cp_root>\BatchPrint\Marketing\utility
```

   c. Set the permissions on the workgroup subdirectories to allow new files to be added and existing files to be deleted.

   d. Copy the files from the BatchPrint directory into each of the `utility` subdirectories.

   e. Open the `PrintInvoices.exe.config` file in each `utility` subdirectory. Set the PrintServername key to the name of the printer (from the `htmlprint.ini` file) for the workgroup. For example:

```
<add key="PrintServername" value="\\printerserver\printerB"/>
```

   f. Save the file.

9. In ChangePoint Administration, set up batch printing:

   a. Assign the BatchPrint directory to workgroups.

   b. Set up access to the Batch Printing Report.

About installing ChangePoint APIs

For information about installing the COM API and Web Services API, see the *ChangePoint API Installation Guide*.

Installing the connection string decryption utility

1. Uninstall any previous versions of the utility using Windows Control Panel.

2. Run the following file from the ChangePoint product media:

```
\Changepoint\Utilities\Connection String Decryption\setup.exe
```

3. Follow the prompts.

4. In the **Setup Status** screen, click **Finish**.

   The installation location now contains:

   ```
   Changepoint.CommonServices.Crypto.dll
   CPPubUtility.dll
   ```

Uninstalling the Connection String Decryption Utility

To uninstall the connection string decryption utility, use Windows Control Panel.

Browser settings for end users

Ensure that users configure their web browers as follows:

- Browser popup settings – Browsers must be set to allow pop-ups from the ChangePoint website URLs.

- Internet Explorer Compatibility mode – compatability mode in Internet Explorer must be disabled by clearing the **Display intranet sites in Compatibility View** check box.

- Browser cache – users must clear their browser cache before logging into an upgraded version of ChangePoint. If the browser has the option to preserve data from websites that have been added to favorites, ensure that the **Favorites website data** is cleared.

13. Upgrading to ChangePoint 2022

About the upgrade

Supported upgrade paths

You can upgrade to ChangePoint 2022 from the following general availability versions at any monthly release level:

• Changepoint 2021

• Changepoint 2020

The upgrade to ChangePoint 2022 replaces *all website files*, but the ChangePoint websites and configuration files remain as is.

Upgrade overview

The upgrade process includes:

1. Ensuring that you meet all of the requirements as detailed in "Installation Requirements and Preparation" on page 15.

2. Preparing for the upgrade.

3. Upgrading the ChangePoint web and database servers.

4. Upgrading the optional ChangePoint components.

Preparing for the upgrade

Unless otherwise stated, information in this chapter concerning ChangePoint websites applies to websites that were set up for ChangePoint, Client Portal, and Survey Response.

Assess the impact on customizations and product extensions

Review your customizations prior to upgrading, and save and/or modify them as necessary.

Upgrading to ChangePoint 2022 replaces all website files. Therefore it is strongly recommended that you review the list of files in the applicable *Differences* documents to assess whether your customizations and product extensions are affected by the upgrade. All customizations to existing website pages must be reapplied after the upgrade.

All customizations made to SQL objects (tables, stored procedures) will be affected.

Warning: If it appears that any of the code associated with a product extension is at risk, contact your ChangePoint customer representative before upgrading. Failure to do so may result in the files being overwritten or deleted, and the extended functionality failing.

Perform backups

Back up the database and web servers before proceeding with the upgrade.

Upgrade in a test environment first

It is strongly recommended that you upgrade your production ChangePoint database and websites in a test environment before upgrading the production environment. If any errors occur, report them to ChangePoint customer care immediately. Do not create test environments on your production servers.

If the test environment and production environment use the same version and the same edition of SQL Server, back up your database and full text catalogs on the production environment and restore them on the test environment. You can then run the upgrade in the test environment.

If the testing environment and production environment use different versions or different editions of SQL Server, then follow the database porting instructions in the "Porting the ChangePoint database" on page 175. After porting the database to the test environment, run the upgrade in the test environment.

Upgrading multiple ChangePoint instances on the same server

If you have more than one ChangePoint instance on a server, you must upgrade all instances.

Warning: ChangePoint will not function correctly if different versions are installed on the same server.

Reinstalling ChangePoint components

If you use the following components, you must reinstall them from the ChangePoint product media:

• Windows services, including the Integration Framework services

• ChangePoint online help

• ChangePoint COM and Web Service API (API media)

• ChangePoint Transport Tool (Transport Tool media)

Intelligent Forms installation parameters

Before you start installation, determine the values in the following table. You are prompted for this information during installation.

Information needed	Notes	Your installation value
Destination folders for application files		
Destination Location (Intelligent Forms web files)	Default: `<cp_root>\Intelligent Forms\Websites\`	
Destination Location (Web Services API files)	Default: ` <cp_root>\API\CP Web Services\`	
Destination Location (Redis cache service)	`<cp_root>\Redis\`	
Website names and ports		
Name of the Intelligent Forms application pool	Default: CPInfiniti	
ChangePoint URL	URL, including the protocol (http or https) for end users to access ChangePoint.	
Destination locations for database files		
Destination Location (Intelligent Forms database file - InfinitiDB.mdf)	Default: The same location as the Changepoint.mdf database file.	
Destination Location (Intelligent Forms database log file - InfinitiDB.ldf)	Default: The same location as the Changepoint database log file.	
Database login information		

Information needed	Notes	Your installation value
Login ID (SQL Server)	sa	
Password (SQL Server)	password for the sa account	
Database Name	Recommended default: Changepoint	
User ID and password for the SQL account that will be used for the database connection	Used in the Login Settings (Connection settings) setup.	
Intelligent Forms database name	Recommended default: InfinitiDB	

Identifying nonstandard database objects

You can create a database inventory report that identifies all nonstandard database objects that exist in your current ChangePoint database. Nonstandard database objects include all database objects (table, view, stored procedure, functions, trigger, index, primary and foreign key constraints) that were created by customizations, accelerators, and third-party integrations.

The database inventory report allows you to catalog existing customizations in the current database, identify the affected customizations, and plan the migration work for the upgrade.

Note: The database inventory report does not replace any change tracking procedures or processes that you may already have in place to track customizations, accelerators, or third-party integrations.

Creating the database inventory report

To create the database inventory report, execute the following query against the ChangePoint database:

```
SELECT * FROM CPObjectsModified
```

The result of the query includes the following:

- custom database objects show as **Added**.

- standard objects that no longer exist show as **Deleted**.

- if a customization has been made directly to a standard database object, the object is not identified as a customized object in the report.

- the report does not report on all CHECK_CONSTRAINTS.

Pre-upgrade steps

One to two weeks before upgrading

Send an email message to users

Send an email to users to notify them about the upcoming upgrade.

Review and standardize existing Location field values

ChangePoint 2022 includes an update that changed the **Location** field from a text field to a drop-down value field.

If you are upgrading to from a release prior to 19.00.136.000, it is recommended that you review and standardize the values for the **Location** field for resources that exist prior to upgrading to ensure that only valid values are converted into location values. Otherwise, a separate location value will be created during the upgrade for each existing value that is unique, which might result in duplicate values that have only minor differences in spelling, capitalization, and spacing.

1. In SQL Server Management Studio, execute the following SQL statement, which collects the existing location values that have been assigned to resources. The resulting CSV file includes the resource ID, resource name, and resource location for all resources that have an assigned location:

```
SELECT r.ResourceId Resource_Id,
r.Name Resource_Name,
ra.[Location] Resource_Location
FROM ResourceAddress ra WITH(NOLOCK)
INNER JOIN Resources r WITH(NOLOCK) ON ra.resourceId = r.ResourceId
AND r.Deleted = 0x0
AND ISNULL(ra.[Location], '') <> ''
ORDER BY ra.[Location];
```

   Note: Locations that are not assigned to resources will be deleted.

2. In the **Results** tab, right-click and save the results as a CSV file with file name: `CP_Resource_Location.csv`.

3. Open the `CP_Resource_Location.csv` file:

a. Review the location values and replace duplicate values with the appropriate value. Ensure that there is only one value per location, and remove locations that are not required.

b. Save the file, which will be imported just before upgrading.

Determine parameter values for Intelligent Forms

If are installing Intelligent Forms for the first time, determine the values for the installation parameters. For more information, see "Intelligent Forms installation parameters" on page 151.

Immediately before upgrading

1. Import the `CP_Resource_Location.csv` file that contains the standardized location values into the Changepoint database:

   a. In SQL Server Management Studio, right-click on the Changepoint database and select **Tasks > Import Flat File**.

   b. Select `CP_Resource_Location.csv` as the file to be imported.

   c. In the **New table name** field, specify CP_Resource_Location.

   d. Click **Next**, then **Next** again.

   e. In **Modify Columns**, change the column names to:

      • Resource_ID
      • Resource_Name
      • Resource_Location

   Note: If any resource names are longer than 50 characters, then you must change the Data Type for the Resource_Name column manually to ensure it has the sufficient number of characters.

   f. Click **Next**, then **Finish**.

2. In ChangePoint Administration, lock ChangePoint.

3. (Web server) Do the following:

   a. Back up the ChangePoint files.

   b. If you have implemented single sign-on for ChangePoint, and you have also implemented Intelligent Forms or the Integration Framework (Salesforce.com), back

up the `<cp_root>\API\CP Web Services\Web.config` file so that you have a copy for reference purposes after upgrading.

    c.   Disable IIS caching of static files.

4. (Database server) Do the following:

    a.   Stop all scheduled jobs from running while you are performing the upgrade.

    b.   Back up the ChangePoint database.

    c.   If required, port the ChangePoint database.

    d.   Back up the Cognos content store database.

    e.   Back up the Infiniti database.

5. If you use the Integration Framework, create backup copies of the following files:

- `adapter.xml` file in the `Changepoint Communication Dispatcher Service\configuration` folder

- `Changepoint.IntegrationServices.WindowsServices.CommunicationDispatcher.exe.config` file from the `Changepoint Communication Dispatcher Service` folder

- `Changepoint.IntegrationServices.WindowsServices.DataMapper.exe.config` file under Changepoint DataMapper Service

- transformation files in the `Changepoint Data Mapper Sevice\Configuration` folder

- `CPExportPublishingService.exe.config` file from the `Changepoint Export Publishing Service` folder.

Upgrading the ChangePoint servers using the installer

Note: If you are upgrading the web server and database server separately, it is best to upgrade the database server first because it is easier to restore the database than it is to roll back the website files.

1. Follow the instructions in the "Pre-upgrade steps" section on page 153.

2. Copy the contents of the ChangePoint product media to the server.

3. From the `\Changepoint\Setup\` directory on the server, run:

```
setup.exe
```

4. Follow the prompts. A confirmation message appears after a successful upgrade.

   • If you are installing Intelligent Forms for the first time, refer to the installation parameters in "Intelligent Forms installation parameters" on page 151.

   • If you are upgrading Intelligent Forms:

     • Both the website and database are updated.
     • do not change the Changepoint URL or Web.config user

   • Run the LoginSettings.exe only if you need to configure database connections

5. Check the log file in the following folder for errors and warnings:

   ```
   C:\Program Files (x86)\Changepoint\Changepoint\InstallLog
   ```

   Note: The log file is always placed in the above location regardless of the root path of the ChangePoint installation.

6. If you have multiple web server or database server installations, repeat the upgrade procedure on each server.

7. Complete the post-upgrade instructions. For more information, see the "Completing the upgrade" section on page 160.

Upgrading the ChangePoint database server manually

1. Copy the contents of the following folder on the ChangePoint product media to a location on the SQL server that contains the database:

   ```
   \Changepoint\Manual Install\Upgrade\
   ```

2. Remove the read-only attribute on the copied files, if set.

3. Run the SQL import utility from the server location:

   ```
   SQLImport.exe
   ```

   The **Changepoint SQL Update Utility** dialog box appears.

4. If you are upgrading from Changepoint 2020, do the following (if you are upgrading from Changepoint 2021, go to the next step):

   a. In the **MigrationDll** folder, select **Changepoint.DatabaseServices.DBMigrations_ CP2021_GA.dll**, and then click **Open**.

   b. In the **SQL Server** field, enter the name of the SQL server.

   c. In the **Database** field, enter the name of the ChangePoint database.

      d. In the **Login ID** field, enter the SQL server account for the ChangePoint database.

      e. In the **Password** field, enter the password.

5. Complete the following fields:

      a. In the **MigrationDll** folder, select **Changepoint.DatabaseServices.DBMigrations.dll**, and then click **Open**.

      b. In the **SQL Server** field, enter the name of the SQL server.

      c. In the **Database** field, enter the name of the ChangePoint database.

      d. In the **Login ID** field, enter the SQL server account for the ChangePoint database.

      e. In the **Password** field, enter the password.

6. Confirm that the upgrade was successful by checking that the `VersionHistory` table on the database server contains the following entry:

```
Upgrading Changepoint database with migration package 22.00.042.000 completed
Configuration of CPTempDB database (Changepoint_CPTempDB) completed successfully
```

Upgrading the Infiniti database manually

1. From the `Changepoint\Manual Install\Upgrade\Intelligent Forms` folder on the ChangePoint product media, copy the SQL files to a local folder on the database server.

2. Edit SetInfinitiDBCompatibilityTo140.sql by replacing "@INF_DATABASE@" with the InfinitiDB name, and then execute the file against the Infiniti database.

3. Edit InsertResourceActionIntoInfinitiDB.sql by replacing "@INF_DATABASE@" with the InfinitiDB name, and then execute the file against the Infiniti database.

4. Edit UpdateMandatoryFields_InfinitiDBScript.sql. by replacing "@INF_DATABASE@" with the InfinitiDB name, and then execute the file against the Infiniti database.

5. Edit AddErrorOutputtoInfinitiDb.sql by replacing "@INF_DATABASE@" with the InfinitiDB name, and then execute the file against the Infiniti database.

6. Execute the following scripts against the Infiniti database:

      a. UpdateOpportunitySubobjectFields.sql

      b. UpdateTimeIdToNotMandatoryInTimeAction.sql

7. Update Redirect URL for Intelligent Forms, if this has not been done prior to the upgrade:

a. Sign into Infiniti Manage, and then open the existing form.

b. Open the form in Design.

c. In the **Finish** section, click **Redirect**. The Redirect Action Properties appear.

d. In the **Text Value** field, replace existing value with the new value:

`[Enterprise URL]/Core/ContentRedirector.aspx?id=[EntityId]&type=EntityType`

For Create Project:

[q196]/Core/ContentRedirector.aspx?id=[Create Project.Project ID]&type=PRJ

For Create Contract:

[q95]/Core/ContentRedirector.aspx?id=[New Engagement.EngagementId]&type=ENG

8. Configure Intelligent Forms. For more information see, "Configuring Intelligent Forms" on page 130.

Updating a customized Create Project Request form:

If you have changed or customized the forms and want to keep those changes, you must do the following:

1. In Infiniti Manage, save the **Create Project Request** form as a separate project.

2. Publish the project.

3. Copy the project ID.

4. In ChangePoint Administration (**User Interface >Actions Menu Integration**), create a new submenu header and submenu item.

5. Import the **Create Project Request** form:

a. Copy the files from the Intelligent Forms folder to a folder where client can access.

b. Sign into ChangePoint.

c. In Infiniti Manage, import the `Create Project Request.ixpkg` form from the `Manual upgrade\Intelligent Form` folder. Be sure to select the "Overwrite project if it already exists" check box.

Note: Before you can use the standard form template in your ChangePoint installation, you must add all of the mandatory fields that are specific to your organization. This

includes both standard ChangePoint fields and configurable fields that have been set as mandatory in metadata.

Upgrading Infiniti 11.1.13 to SmartIQ 17.5.0

This upgrade applies to ChangePoint 2022 R12 (22.00.054.000) and later.

1. If not already installed, install Infiniti from the Changepoint 2022 GA release package.

2. Upgrade to ChangePoint 2022 R12 (22.00.054.000).

3. Copy the `ChangePoint Intelligent Forms Upgrade.exe` from the ChangePoint 2022 R12 (22.00.054.000) package to the server where Infiniti is installed.

4. Run the executable as administrator and then follow the prompts.

5. On the **Select a Web Site** screen, select the ChangePoint website that Infiniti was installed on.

6. Review the settings, and then click **Next**. The ASP.Net Core Runtime Bundle 6.0.13 and Intelligent Forms websites files are installed, and the websites are configured.

7. Because SmartIQ only supports HTTPS, you must update the URLs accordingly in the following places:

   a. ChangePoint Web Services\web.config file

   b. ChangePoint API in Infiniti Manage – Update the database connection settings using LoginSettings.exe. For more information, see "Database connection settings for Intelligent Forms" on page 73

Upgrading the Infiniti database to version 17.5.0

You upgrade the Infiniti database by signing into SmartIQ Manage as ChangePoint administrator.

1. Sign into ChangePoint as ChangePoint administrator.

2. Access SmartIQ Manage (ChangePoint Administration > **Intelligent Forms > Infiniti Manage**).

The Infiniti database is upgraded.

Upgrading Infiniti to SmartIQ on multiple instances

1. Copy the ChangePoint Intelligent Forms Upgrade.exe from the ChangePoint 2022 R12 (22.00.054.000) package to the server where Infiniti is installed.

2. Run the executable as administrator and then follow the prompts.

3. On the **Existing Installed Instances Detected** screen, select the **Maintain or update the instance of this application selected below** option, and then click **Next**.

4. Follow the prompts as documented above.

Completing the upgrade

After you have upgraded the database and web servers, you must complete the upgrade restoring customizations, running scheduled jobs, and so on. For more information see:

1. "Completing the upgrade on the database server" on page 161.

2. "Completing the upgrade on the web servers" on page 163.

3. "Completing the installation of Intelligent Forms" on page 162.

4. "Upgrading ChangePoint Windows services" on page 164.

5. Upgrade the following optional components as required:

   - "Upgrading the online help" on page 165

   - "Setting up the Changepoint Mobile app" on page 165

   - "Upgrading the ChangePoint API" on page 166

   - "Upgrading Integration Framework" on page 168

   - "Upgrading Cognos Analytics" on page 169

   - "Upgrading the Transport Tool" on page 168

   - "Upgrading the archive database and websites" on page 168

6. Assess and grant new security features to the applicable resources and roles:

   - Edit Service Scheduler

   - View Service Scheduler

   - Access Workforce Planning Notifications

7. Advise users that they must delete their browser history before signing into ChangePoint for the first time after the upgrade.

Completing the upgrade on the database server

1. Restore and test customizations (custom SQL code, accelerators, and extensions).

2. Configure the CPEffectiveDates scheduled job for access to the Redis cache. For more information see "Configuring the CPEffectiveDates scheduled job for access to the Redis cache" on page 161.

3. To prevent time entry on summary tasks, see "Preventing time entry on summary tasks" on the next page.

4. To optimize performance, follow the performance optimization recommendations in "Optimizing Performance" on page 179.

5. Adjust the ChangePoint and tempdb databases to the limits and settings according to your internal administration policies. The size of the databases may have increased due to the processing done during the upgrade.

6. Run the following scheduled jobs:

   a. Reindex and Update Statistics daily

   b. Chained scheduled jobs by starting the Update Time Rate job.

   Note: It is recommended that you run the scheduled jobs immediately after upgrading, and before end users sign in.

   Tip: The chained scheduled jobs may take a long time to run. Record the duration of the job in the test environment so that you can plan for the initial scheduled job run on the production database.

7. If you dropped custom full-text catalogs before the upgrade, recreate the catalogs.

8. Restart the database server.

Configuring the CPEffectiveDates scheduled job for access to the Redis cache

The CPEffectiveDates scheduled job requires access to the Redis cache that is used by ChangePoint because the scheduled job performs work that triggers certain cache region data evictions. Because the CPEffectiveDates scheduled job can be installed independently from

Changepoint (possibly on a different location than the web server), you must configure the Redis cache manually.

In the `CPEffectiveDates.exe.config` file, edit the following entries in the <configuration> <appSettings> section to match the values that are in the `Enterprise\Web.config` file:

```
<add key="cache.Enabled" value="true" />
<add key="cache.Password"
value="6ed18d5c7df4439409d65eba624de2aeb7aea1e3b745987b9cd81d6e052a01f8" />
<add key="cache.Servers" value="cacheServer:Redis Cache port number" />
```

Note: The server that hosts the CPEffectiveDates scheduled job must allow outbound firewall access to the Redis cache port number.

Completing the installation of Intelligent Forms

1. Configure the database connection settings for Intelligent Forms. For more information, see:

    • "Database connection settings for Intelligent Forms" on page 73

    • "Database connection settings for Intelligent Forms (Manage and Produce)" on page 74

2. Configure Intelligent Forms according to the instructions in "Configuring Intelligent Forms" on page 129.

3. If forms fail to launch or submit properly after installing or upgrading, check if a **Display Message** action has been added to the form.

    a. Open the form in **Infiniti Manage > Design**.

    b. Expand the **Finish** section at the bottom of the left pane.

    c. Locate and delete the **Display Message** action.

    d. Save the form and then test it again.

Preventing time entry on summary tasks

The default behavior for ChangePoint 2022 is to allow time entry for summary tasks and their subtasks.

If you want to prevent time entry for summary tasks, you can run a script to lock task assignments for all summary tasks or for specific entities.

To lock all task assignments for all summary tasks

```
EXEC LockAssignmentFromSummaryTask @Lock=0x1
```

To lock all task assignments for a specific entity

You can lock the task assignments for one or more summary tasks in a project, engagement/initiative or customer) by specifying only the parameter for the entity. If more than one parameter is specified, the parameter for the lowest level entity is used, and the others are ignored.

```
@Lock BIT = 0x1,
@SummaryTaskId UNIQUEIDENTIFIER = NULL,
@ProjectId UNIQUEIDENTIFIER = NULL,
@EngagementId UNIQUEIDENTIFIER = NULL,
@CustomerId UNIQUEIDENTIFIER = NULL
```

For example, if you run the script as follows, only the task assignments under the specified summary task will be locked.:

```
EXEC LockAssignmentFromSummaryTask @Lock=0x1
, @SummaryTaskID = 'EE8CFFBA-05DA-4C8A-9BA5-8DB5F929A361'
, @ProjectID = 'C8999EF9-06FB-4279-A7C9-25CF7C46B84A'
```

If you want to lock all assignments for all summary tasks on that project, specify only the project ID as follows:

```
EXEC LockAssignmentFromSummaryTask @Lock=0x1
, @ProjectID = 'C8999EF9-06FB-4279-A7C9-25CF7C46B84A'
```

Completing the upgrade on the web servers

1. Restore and test customizations (asp pages and extensions).

2. For optimum performance, Resource Planner has default values set for the following keys. To increase the limit, change the value in the `Enterprise\WebAPI\Web.config` file for the following settings:

```
<add key="ResourceSchedulingWorksheet.DemandItemLimit" value="300" />
<add key="ResourceSchedulingWorksheet.ViewColumnsLimit" value="50" />
<add key="ResourceSchedulingWorksheet.PastWorkingDaysLimit" value="90" />
```

Note: For the DemandItemLimit, the maximum value is 1000. Keep in mind that it is best to use as low a value as possible that provides good performance in Resource Planner.

3. During the upgrade, the SQL connection strings are copied from the `Enterprise\Web.config` file to the CP Web Services\Web.config file, which replaces the `<cp_root>\API\CP Web Services\Web.config` file.

   You must review the settings in the `CP Web Services\Web.config` file and execute the applicable scripts if you have previously implemented single sign-on for ChangePoint, Intelligent Forms, or the Integration Framework (Salesforce.com), or have enabled WSE, and so on. For the previous settings, refer to the copy of the file that you backed up before upgrading.

4. To optimize performance, follow the performance optimization recommendations in "Optimizing Performance" on page 179.

5. If you have enabled Request Filtering on the ChangePoint website or use tools to restrict HTTP verbs in HTTP traffic, you must ensure that the following HTTP verbs *are not set* to "Block" or "Deny":

   - PUT

   - PATCH

   - DELETE

   For more information, see "Troubleshooting the upgrade" on page 172.

6. Restart the ChangePoint website.

7. Sign into ChangePoint Administration, and do the following:

   a. If you purchased additional licenses, import the licenses (**Tools > License Management**).

   b. Check the server integration settings (**General > Server Integration**).

8. Restart all websites and check that you can sign in to each website.

9. Enable IIS caching of static files.

10. Restart IIS.

11. Restart the Redis cache service.

Upgrading ChangePoint Windows services

The following standard ChangePoint Windows services have been updated:

- Changepoint Email Notification Service

- Changepoint Exchange Synchronization Service

- Changepoint Mail Service

For more information about installing and configuring the ChangePoint Windows services, see "Installing ChangePoint Windows Services" on page 55.

1. For each of the Windows services that you use, you must do the following:

    a. Create a backup copy of the configuration file for the service.

    b. Uninstall the service using Windows Control Panel.

    c. Reinstall the service from the ChangePoint product media.

2. For each of the standard ChangePoint Windows services:

    a. Configure the database connection settings.

    b. For the Changepoint Mail Service only: If you are not planning to enable the Changepoint Mobile app, then you must comment out the following keys in the configuration file for the service(CPMail.exe.config):

```
< add key="NotificationProvider.Key1" value="" />
< add key="NotificationProvider.Key2" value="" />
```

Upgrading the online help

Install the online help files from the ChangePoint product media. For more information, see "Installing the ChangePoint online help" on page 141. It is not necessary to uninstall the previous help files.

Setting up the Changepoint Mobile app

The topic covers the setup required to enable users to use the Changepoint Mobile app.

Note: The Mobile app requires that Changepoint be configured with SSL using one of the following authentication modes:

- SSO using ADFS

- SSO using SAML

- Changepoint Application Authentication

For information about the supported platforms, see the *ChangePoint Software Compatibility Matrix*.

1. Obtain the license from Planview, Inc. for the Access Mobile Application (AMA) security feature, which includes the values for the keys NotificationProvider.Key1 and NotificationProvider.Key2.

2. Add both keys to the following configuration files according to the instructions provided with the keys:

   - `Enterprise\WebApi\web.config`

   - `Changepoint\Changepoint Mail Service\CPMail.exe.config`

3. Set up Changepoint and the Changepoint Mail Service to communicate with Amazon Web Services over https (port 443). The SNS access point for Amazon is: `https://sns.us-west-2.amazonaws.com`.

   Note: This might require changes to firewall settings.

4. Advise users of the following:

   - Changepoint Mobile app is available at the online app stores.

   - ChangePoint URL or domain, and the user ID and password that are required to sign in to the app.

   - ChangePoint functionality that is available in the app.

   Note: The Changepoint Mobile app is designed to be intuitive and easy to use, and it supports a subset of the functionality of the desktop ChangePoint application. Therefore there is no end user documentation for the app.

Upgrading the ChangePoint API

1. Uninstall the previous version of the ChangePoint API.

2. Create an application pool as follows:

Name	<API application pool name>
.NET Framework version	v4.0.30319

Managed pipeline mode	Integrated
Enable 32-Bit Applications	True
Identity	ApplicationPoolIdentity

3. Create an empty website as follows:

Site Name	<API website name>
Application Pool	<API application pool name>
Physical Path	C:\Program Files\Changepoint\<API website name>
Authentication	Only Anonymous Authentication

4. If you are installing the WCF API, configure the website to *not* use SSL.

5. Install the ChangePoint 2022 version of the API using the website that you created.

    Note: The virtual directory name is hard coded as CPWebService.

    For more information, see the *Changepoint 2022 API Installation Guide*.

6. If you installed the WCF API on a server that does not have WSE installed, you must do the following:

    a. Open web.config.

    b. Find the three instances of the following comment line:

```
<!-- Remove the following element if you are using WCF services and are not installing
Web Service Enhancements (WSE) -->
```

    c. Remove or comment out the element that follows each instance of the comment line:

```
<section name="microsoft.web.services2" ... >
<webServices>
<microsoft.web.services2>
```

    Note: The `<webServices>` element is a child of `<system.web>`.

Upgrading Integration Framework

For information about upgrading the Integration Framework, see the *Integration Framework Reference*.

Upgrading Salesforce.com integration toolkit

For information about upgrading the Salesforce.com integration toolkit, see the the *Integration Framework Reference*.

Upgrading the Transport Tool

To upgrade the Transport Tool, you must uninstall the previous version and then reinstall from the Transport Tool product media.

For more information, see the *ChangePoint Transport Tool User Guide*.

Upgrading the archive database and websites

If you have an archive database and websites, follow the same procedure as for upgrading the ChangePoint database and websites. When prompted, substitute the details for the archive database and websites in place of the ChangePoint database and websites.

Note: The archive environment must always be at the same patch level as the production environment, otherwise the Archive scheduled jobs might fail.

1. Upgrade the archive database and websites.

2. Copy the `Data Archiving.dtsx` and `GenerateEmptyArcDestDB.dtsx` packages from the Changepoint product media at:

   ```
   \Changepoint\Manual Install\Data Archiving
   ```

3. Paste the files into the `Data Archiving` folder on the archive environment.

Configuring the archive database

If you have a website set up to access the archive database, execute the following commands against the archiving database:

```
exec DBM_SetupCPTempDB
exec DBM_SetupCPExtended
exec DBM_EnableSqlDependency (with the user used in the Web.config files)
```

Verifying component versions

After you upgrade to ChangePoint 2022, the version for all components is: 22.00.042.000.

Upgrading Cognos

Upgrading Cognos Analytics

You can upgrade Cognos Analytics on the following ChangePoint versions:

- Changepoint 2021 (Cognos Analytics 11)

- Changepoint 2020 (Cognos Analytics 11)

    Note: In this upgrade, Cognos Analytics can be upgraded only to the tip version.

Upgrade notes for installing Cognos Analytics:

- The Cognos gateway is no longer required. Only the Cognos application tier is required. The Changepoint installer removes the Cognos gateway during the upgrade.

Upgrade notes for using Cognos Analytics 11.2:

- The Cognos Analytics 11.2 user interface is different from the Cognos 11.1.x user interface. Users will need to familiarize themselves with the new interface. The same functionality and options are available, but many of them are in a different location in the new interface.

Upgrade notes for upgrading to Cognos Analytics 11.2.3

- To support the use of entity links in dashboard tables, you must install a custom ChangePoint HTML visualization file. For more information, see the "Adding ChangePoint entity profile links to an Analytics dashboard table" article on the ChangePoint Customer Success Center (https://success.planview.com/Planview_Changepoint).

Upgrading Cognos includes the following steps:

1. Upgrading ChangePoint.

2. Backing up the content store database by creating a SQL Server backup and a Cognos deployment archive using IBM Cognos Administration. For more information, see the "Creating a deployment archive" knowledge center article on the IBM website.

3. Backing up the Cognos startup configuration file:

```
C:\Program Files\ibm\cognos\analytics\configuration\cogstartup.xml
```

    Note: You might want to back up this file and other configuration files and use the configuration data with the new version.

4. If there are any customizations, create a `preserve.txt` file to preserve the custom files during the upgrade. For more information, see the "Preserved files and folders when upgrading Cognos Analytics" knowledge center article on the IBM website.

5. Run the script to update the ContentStore database:

   a. Copy the CognosUpdateResourceId.sql file from the Setup\Utility\ folder on the ChangePoint Analytics media to the server where ContentStore is installed.

   b. Open SQL Management Studio with sufficient rights and execute CognosUpdateResourceId.sql against the ContentStore database.

6. Installing Cognos Analytics (be sure to use the same installation folder as the previous installation):

   a. Close the IBM Cognos Configuration panel.

   b. Stop the Cognos service.

   c. Do the following:

      - "Stage 2. Installing the Cognos Application Tier" on page 106
      - "Stage 4. Installing the Cognos web components" on page 110
      - "Stage 6. Assigning ChangePoint security features for access to Cognos functionality" on page 112(where applicable)

   d. Open the IBM Cognos Configuration panel. The message "Older versions of configuration files were found. The configuration files have been upgraded to the latest version" appears.

   e. Click **OK**, and wait for configuration data to be loaded

   f. In the IBM Cognos Configuration panel, ensure that either the FQDN or the IP address is used consistently throughout the configuration.

   g. Click the **Start** button to start the Cognos Service.

   h. Confirm that you want to save the changes by clicking **Yes** in the confirmation message that appears.

7. If required, in IBM Cognos Administration, reimport the deployment archive created above. For more information, see the "Creating a deployment archive" knowledge center article on the IBM website.

8. Remove the **Everyone** role from the following capabilities:

- Data sets

- Upload files

- Web based modeling

9. Ensure that the **Everyone** role has been removed from the Cognos System Administrators role.

10. If Business Author licenses are to be granted full reporting capabilities, add the **Changepoint Query Users** role to the Cognos **Authors** role.

11. By default, Cognos portlets and portals open in a new browser window. However, you can configure Cognos portlets and portals to open inline. In the `Enterprise\Web.config` file, set `Cognos.IE.LaunchPortletsInNewWindow` to "false."

12. Upgrade the Changepoint-Cognos Sync Utility and import the new base data model. For more information, see "About the ChangePoint-Cognos Sync Utility " on page 116.

13. Restart the Cognos service on the Cognos Application Tier server.

14. Upgrade the report specifications in bulk according to the instructions in the "Upgrade your report specifications" knowledge center article on the IBM website.

Manually uninstalling Cognos

The installer will uninstall the previous Cognos instance, but you can uninstall Cognos Analytics manually from each of the locations where it has been installed:

- Application Tier server

- Cognos Gateway on each ChangePoint web server

- Sync Utility client workstation

1. On each of the servers, go to the following folder:

`C:\Program Files\ibm\cognos\analytics\uninstall`

2. Uninstall Cognos Analytics by double-clicking:

`Uninstall IBM Cognos.exe`

3. After you have verified that you do not require any files, delete the Cognos IBM directory:

`C:\Program Files\ibm\cognos\analytics`

Troubleshooting the upgrade

"Member coordination host in Configuration Group is not configured properly" error

Ensure that the FQDN is used consistently throughout the configuration.

Encryption certificate error or cryptographic service error when starting the Cognos Service

If there is an error related to the encryption certificate or cryptographic service when starting the Cognos Service, ensure that the Supported ciphersuits value is set to the default value and then regenerate the cryptographic key.

For more information, see the How to regenerate cryptographic keys in Cognos Analytics 11.knowledge base article on the IBM website.

Execution timeout error in Resource Planner.

If you are getting timeout errors in Resource Planner, add and configure the CommandTimeOut setting in the Enterprise\WebApi\Web.config file.

Add the following key to the `appSettings` section of the `Enterprise\WebApi\Web.config` file. Ensure that the value is greater than 30 (seconds).

```
< add key="CommandTimeOut" value="300" />
```

Changepoint Mail Service error in event log

If you enabled the Changepoint Mail Service but did not enable the Changepoint Mobile app, then you must comment out the following keys in the service configuration file (`CPMail.exe.config`):

```
< add key="NotificationProvider.Key1" value="" />
< add key="NotificationProvider.Key2" value="" />
```

Access to the path '…\RP-STS_ADFS\Web.config' is denied" error when signing into Changepoint

If your environment is configured for single sign-on (SSO) using WS-Federation (ADFS), you must grant the **IIS_IUSRS** group **Modify** access to the `Enterprise\RP-STS_ ADFS\Web.config` file.

ChangePoint Analytics report in a dashboard will not load

The report version may be out of date. Regenerating the report in ChangePoint Analytics will update the report version.

HTTP 403 error/
Project Worksheet fails to save/
Preferred resources cannot be edited

If you have enabled Request Filtering on the ChangePoint website or use tools to restrict HTTP verbs in HTTP traffic, you must do the following:

1. Add the following verbs to the [AllowVerbs] section:

    • PUT

    • PATCH

    • DELETE

2. Remove the same verbs from the [DenyVerbs] section.

Blocking these verbs can result in unexpected HTTP errors and functional issues in ChangePoint. ChangePoint deploys the ChangePoint REST API internally (and externally as an option) to enable mobile app support and some internal product functionality. The REST API uses the HTTP verbs in its transactions.

Errors in the Changepoint Installer.log

* WARNING: add app pool (IIS APPPool\\<website>_AppPool) in [Performance Monitor Users] group failed. Please add the user manually.

* WARNING: add app pool (IIS APPPool\\<website>_AppPool) in [Performance Log Users] group failed. Please add the user manually.

or

Server error in browser

Server Error in '/' Application.
Access to the registry key 'Global' is denied.

The application pools of the Enterprise website and the Enterprise REST web application must be included as members of both the **Performance Monitor Users** and the **Performance Log Users** groups.

You can manually add the <website>_AppPool to the Performance Monitor Users group and Performance Log Users group using the Computer Management console on the corresponding web server.

1. On the web server or web application, open **Computer Management** console as **Administrator**.

2. In the console tree, select **Computer Management > System Tools > Local Users and Groups> Groups**.

3. Double-click the Performance users group listed in the warning.

4. In the Properties dialog for the Performance users group, click **Add**.

5. In the **Select Users** dialog box, type the name of the application pool from the warning, and then click **OK**.

   The application pool appears in the **Members** section of the Properties dialog box.

6. Restart the web server or web application.

Project Worksheet does not load/
Error when accessing Manage Preferred Resources/
"Access to registry key 'Global' is denied" in Changepoint event log

Restart the web server. These errors can occur when registry permissions have been changed.

Install the latest monthly releases

Check the **ChangePoint2022 Releases** section in the Customer Success Center (https://success.planview.com/Planview_Changepoint) or team folders in Client Portal, for releases that have been posted after this cumulative release

We encourage you to keep ChangePoint up to date with the monthly releases, which allows users to take advantage of the latest feature enhancements and fixed issues.

To install the monthly releases, follow the instructions in the corresponding release notes.

14. Porting the ChangePoint database

Overview

This section describes how to port the ChangePoint database between different versions or editions of SQL Server.

> **Note:** If the version of SQL server you are currently using is not supported in the new version of ChangePoint, then you must port the database first before upgrading it. Otherwise, the order is not important.

Porting the ChangePoint database

> **Note:** ChangePoint does not support SQL Server partitions.

On the source database server

1. Log in as `sa` to SQL Server Management Studio.

2. Disconnect all users from the database and set it to "Restricted Access to db_owner, dbcreator or sysadmins" only.

3. Issue a CHECKPOINT.

4. Detach the database.

5. Copy only the .mdf and .ndf database files to the target SQL server.

6. Repeat this procedure for the CPExtended database.

On the target database server

1. Copy the following folder from the ChangePoint product media to any location on the target SQL server:

    `\Changepoint\Utilities\Porting SQL Databases\`

2. Remove the read-only attributes from the copied files.

3. Log in as `sa` to SQL Server Management Studio.

4. Open the following script in an editor:

    `<TargetServerPath>\Porting Changepoint.sql`

5. If you did not use the default database name, replace "ChangePoint" with the database name.

6. Update the full path and file names of all the .mdf and .ndf files in the script.

7. Scroll to the bottom of the script, and then edit the input value for the stored procedure `DBM_EnableSqlDependency`. For more information, see the comments in the script for details.

8. Replace the CPSQLUser string in the script with the SQL account on the target server that will be used for the ChangePoint database connection.

9. (Optional) Edit the value of the input parameter for the stored procedure `DBM_SetupCPTempDB`. For details, see the comments in the script.

10. Edit the value of the input parameter for the stored procedure `DBM_SetupFullText`. Do one of the following:

    • To populate the full text indexes immediately: set `@Populate = 0x1`

    • For a large sized database, it is recommended to set `@Populate = 0x0`, and run the CPFullText scheduled job later.

11. Edit the value of the input parameter for the stored procedure `DBM_SetupScheduledJob`. For details, see the comments in the script.

    a. If you are not using the default ScheduledJobs path, replace the value of the following variable with the path used:

    ```
    @SCHEDULE_JOB_PATH = '<cp_root>\ScheduledJobs\'
    ```

    b. If you are not using the default Data Archiving path, replace the value of the following variable with the path used:

    ```
    @DATAARCHIVING_JOB_PATH = ' C:\Program Files\Changepoint\Changepoint\Data Archiving\'
    ```

12. Update the full path and file names of all the .mdf and .ndf files in the script for the CPExtended database.

13. Run the script against the ChangePoint database.

After porting the ChangePoint database

After you port the ChangePoint database to the target SQL server, perform the following steps.

1. Copy the contents of the Scheduled Jobs directory from the source SQL server, for example:

    ```
    <SourceServerPath>:\<cp_root>\ScheduledJobs\*.*
    ```

to the Scheduled Jobs location on the target SQL server:

```
<TargetServerPath>:\<cp_root>\ScheduledJobs\
```

2. After porting the database, the size of the ChangePoint and tempdb databases may have increased due to the processing done during the porting. Adjust them back to the limits and settings as per your internal policies.

3. Run the Login Settings utility on all the applicable applications and services to change the **Server** field to the correct value for the target SQL server.

   For more information about using the Login Settings utility, see the *ChangePoint Installation Guide*.

4. If you have an archive database and you are porting the source database, do the following:

   a. Copy the contents of the Data Archiving directory from the source SQL server:

```
<SourceServerPath> C:\Program Files\Changepoint\Changepoint\Data
Archiving\*.*
```

   to the Data Archiving location on the target SQL server:

```
<TargetServerPath> C:\Program Files\Changepoint\Changepoint\Data Archiving
```

   b. Edit the following file:

```
<TargetServerPath> C:\Program Files\Changepoint\Changepoint\Data
Archiving\Data Archiving.ini
```

   c. Change the server name in the following section and save the file:

```
[CPSQLServer]
Name=TargetServerName
```

Porting an archive database

The procedure for porting an archive database is similar to the procedure for porting a ChangePoint database, except for the following:

• Do not set up scheduled jobs on the archive database

• If the source database remains on the same server, and only the archive database is ported to a new server, change the [ARCSQLServer] section instead of the [CPSQLServer] section of the `<TargetServerPath> C:\Program Files\Changepoint\` `Changepoint\Data Archiving\Data Archiving.ini` file.

   Change the server name in the following section and save the file:

```
[ARCSQLServer]
Name=ArcSQLName
```

15. Optimizing Performance

ChangePoint performance guidelines

You can improve the overall performance of the ChangePoint application by making the following adjustments to the default configuration of the ChangePoint website.

Configuring the antivirus exclusion list

To prevent performance issues caused by virus scans, you must configure the exclusion list in the antivirus software.

Exclusion list for the database server

To determine the exclusion list for the SQL server, refer to the following information on the Microsoft website:

```
https://support.microsoft.com/en-ca/help/309422/how-to-choose-antivirus-software-to-
run-on-computers-that-are-running-sql-server
```

Exclusion list for the web server

Include the subdirectories as well for all the excluded directories.

1. Changepoint installation directory: <cp_root>

2. .NET Framework files:

    *   `C:\Windows\Microsoft.NET\assembly`

    *   `C:\Windows\Microsoft.NET\Framework\v4.0.30319`

    *   `C:\Windows\Microsoft.NET\Framework64\v4.0.30319`

3. IIS config folder:

    `%SystemDrive%\Windows\System32\inetsrv\config\`

4. IIS Temporary Compressed Files

    `%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files`

5. Pagefile.sys

6. IIS Logs files, if IIS logging is enabled. The default is:

    `C:\inetpub\logs\LogFiles`

Performance guidelines for the ChangePoint database server

The performance of the database server is particularly important when you are preparing an environment for high user loads. High performance is achieved by splitting as many I/O calls as possible across multiple I/O channels, disks, and spindles in order to keep I/O queuing to a minimum while using the entire available memory in the most efficient way.

Adjust maximum SQL server memory

By default, SQL Server configured with maximum server memory set to 2147483647 MB, which in effect is all of the server memory that is available. The default setting can result in insufficient memory for the operating system and other applications, which can cause instability and performance issues.

Therefore, you must adjust the value for the default setting to allow some of the server memory for the operating system and other applications. Use the following formula:

Maximum SQL Server Memory = Maximum Physical Memory – Memory for OS

Memory for the OS is between 1 GB and 4 GB, depending on the total physical memory of the server.

Virtualized SQL server using VMware

If you have virtualized the SQL server using VMware, review the guidelines in the *Architecting Microsoft SQL Server on VMware vSphere,* best practices guide, which is available on the Vmware website:

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf

Dedicated I/O channels for database file types

Each database file type should have its own dedicated I/O channel (LUN, RAID set or physical disk):

- Database log file on a RAID 10 array

- Database ndf files on a RAID 10 array

- Database mdf file on a RAID 10 array

- tempdb database on RAID 0

If only three channels are available, the log file and tempdb can be on one channel. Use multiple data files for tempdb (one per CPU-Core), set the initial size to 1 GB, and set the auto-grow to 1 GB.

16. ChangePoint Connection String Decryption Utility

About decrypting connection strings

This document provides code samples for using the ChangePoint Public Utility (CPPubUtility) to decrypt the reportsdsn connection string in the Global.asa for use in customizations. For additional information, contact your client services representative or client manager.

CPPubUtility runs under the .NET Framework. This utility provides a single method interface, which can be used to decrypt the connection string information that is stored in an encrypted format in the Global.asa and Web.config files.

Typically, the CPPubUtility is installed on the web server, but it can also be installed on the database server if needed.

ChangePoint Public Utility object interfaces

Object: `CPPubUtility.Decrypt`

Method: `DecryptString`

```
Public Function DecryptString(ByVal sConnectionString As String) As String
```

Time-out limits for decrypted connection strings

Time-out periods are enforced for the decrypted connection strings. If a time-out is set, the decrypted connection string includes the time-out value in seconds. For example:

```
provider=SQLOLEDB; Server=SERVER; database=Changepoint; uid=xxj;
password=xxj; Trusted_Connection=No; Timeout=900
```

If there is no time-out limit, the decrypted connection string does not include a time-out value. For example:

```
provider=SQLOLEDB; Server=SERVER; database=Changepoint; uid=xxj;
password=xxj; Trusted_Connection=No
```

Code examples for decrypting connection strings

VB

```
Dim cmdSQL As ADODB.Command
Dim oCPDecrypt as CPPubUtility.Decrypt
Dim sConnectionString as String
Set cmdSQL = New ADODB.Command
Set oCPDecrypt = New CPPubUtility.Decrypt
```

```
sConnectionString = GetObjectContext("Session").Contents("DSN")
With cmdSQL
.ActiveConnection = oCPDecrypt.DecryptString(sConnectionString)
```

    …

VBScript

```
Dim cmdSQL
Dim oCPDecrypt
Dim sConnectionString
set cmdSQL = server.CreateObject("Adodb.Command")
set oCPDecrypt = server.CreateObject("CPPubUtility.Decrypt")
sConnectionString = Session("dsn")
With cmdSQL
.ActiveConnection = oCPDecrypt.DecryptString(sConnectionString)
```

.NET

```
Dim cmdSQL As SqlCommand
Dim oCPDecrypt As New CPPubUtility.Decrypt()
Dim sConnectionString As String
' Get connection string from configure file
sConnectionString = ConfigurationSettings.AppSettings("SQLSettings")
' Decrypt the connection string
sConnectionString = oCPDecrypt.DecryptString(sConnectionString)
If sConnectionString <> "" Then
cmdSQL = New SqlCommand()
cmdSQL.Connection = New SqlConnection(sConnectionString)
....
```

Report example for using CP Decrypt Interface

This report uses the CPDecrypt Interface to display a list of resource names and email addresses on any ChangePoint customer database.

```
<!--#include virtual="/IncludeFiles/inSession.asp"-->

<html>
<head>
<meta HTTP-EQUIV="PRAGMA" CONTENT="NO-CACHE"
<link rel="stylesheet" type="text/css" href="/css/<%=strLCID%>_documents.css
media="screen">
<link rel="stylesheet" type="text/css" href="/css/<%=strLCID%>_docPRINT.css
media="print">
</head>
<body>
<table cellspacing=0 cellpadding=2 width='98%' border=0>
<tr>
```

```
<td class=head style="width:80%;" valign=top>Sample Report</td>
</tr>
<tr>
<td colspan=2 class=fadeline> </td>
</tr>
<td>v0.1<td>
</tr>
</table>
<p><span class="SummaryHead">Date & Time run:</span>  
<%=FormatDateTime(date(),1)%></p>
<%
dim sSQL, rst
Dim cmdSQL
Dim oCPDecrypt
Dim sConnectionString
set cmdSQL = server.CreateObject("Adodb.Command")
set oCPDecrypt = server.CreateObject("CPPubUtility.Decrypt")
sConnectionString = Session("reportsdsn")
With cmdSQL
.ActiveConnection = oCPDecrypt.DecryptString(sConnectionString)
.CommandType = AdCmdText
End With

sSQL="SELECT Resources.Name AS ResourceName,
ResourceAddress.EmailAddress AS ResourceEmailAddress" &_
"FROM Resources, ResourceAddress" &_
"WHERE Resources.ResourceID = ResourceAddress.Resourceid"
cmdSQL.CommandText = sSQL
set rst = cmdSQL.Execute
if not rst.EOF then
Response.Write("<table cellpadding='0' cellspacing='0' border='0'
width='100%'>")
Response.Write("<tr><td class='TableHead'>Resource Name</td>")
Response.Write("<td class='TableHead'>Resource Email Address</td>")
while not rst.EOF
Response.Write("<tr><td class='rowUnderline'>" &
rst("ResourceName").Value & "</td>")
Response.Write(<tr><td class='rowUnderline'>" &
rst("ResourceEmailAddress").Value & "</td>")
rst.MoveNext
wend
rst.Close
Response.Write("</table>")
else
Response.Write("<p><span class='SummaryHead'>No data to display</p>")
end if
set rst = nothing
%>
```

```
        </body>
        </html>
```

17. Creating a Test and Training Environment

You can install both a test and training environment on the same server. For illustration purposes, the test and training environments in these topics are called TEST and TRAIN.

For each environment, the database and full text catalogs are backed up on the production environment and restored on the test/train server.

> **Warning:** Do not install the TEST and TRAIN instances on the ChangePoint production server. It is recommended that the production server have only one instance of the ChangePoint database.

Backing up and restoring your production database to a different server still requires backing up the full text catalogs and running the SQL Dependencies script for each server, as outlined in step 3 to step 4 below.

Creating a test and training environment on the same server

1. For the first database instance, run the installer on the test/train database server. When prompted, do the following:

    •   Select the **Database only** setup type.

    •   For the database name, enter a name for the test database, for example, TEST.

2. For the second database instance, run the installer again on the test/train database server. When prompted, do the following:

    •   Select the **Database only** setup type.

    •   Select a different <cp_root> location than the first instance.

    •   For the database name, enter a name for the training database, for example, TRAIN.

3. Back up the database and full text catalogs on the production environment and restore them on the TEST and TRAIN database instances.

4. In the EnableSQLDependency.sql script (located on the ChangePoint product media in the \Changepoint\Manual Install\Upgrade folder), replace all occurrences of the CPSQLUser string with the SQL user ID you used when running the installer to create the test and train database instances for each database that you restored.

5. Run EnableSQLDependency.sql.

6. Run the following scripts:

      a.   Setup_Full_Text.sql

      b.   Setup_Scheduled_jobs.sql

      c.   Setup-CPExtended.sql

      d.   Setup-CPTempDB.sql (Ensure that the value for @CPTemp_DB is different from the name of the original CPTempDB.)

7.   Run the installer on the web server for each instance you want to create (TEST and TRAIN, for example). Each website must have a unique name and port number. Configure the Global.asa and Web.config files using the SQL accounts you created for each database.

8.   As required, run the installer on the same server or another server to install the required ChangePoint Windows services. For more information on installing and configuring the services, see "Installing a ChangePoint Windows service" on page 55.

9.   To clearly identify the TEST and TRAIN environments, do one of the following:

- Create a Corporate News Knowledge Item with an expiry several years from now indicating that this is a test/training environment.

- In the Registration table, add "**TRAIN**" OR "**TEST**" to the company name. Then change the following settings in the Enterprise\Web.config file:

  - To display the company name in the interface:

  < add key="ShowRegistration" value="true" />

  - To display the name of the currently signed-in user and the company name:

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

  - To change the color of the bar, set the hexadecimal code for the color as the value for the following key:

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

  - To change the color of the text, set the hexadecimal code for the color as the value for the following key:

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

10. Install and configure Redis.

11. Sign in to ChangePoint Administration and update the server integration and email integration settings with the appropriate URLs for each instance.

12. If you use IBM Cognos Analytics, you must port the Cognos content store database. For more information, see "Porting the Cognos content store database" on page 189.

Porting the Cognos content store database

Porting the Cognos content store database includes the following steps:

1. Export the Cognos content store database.

2. Import the Cognos metadata package.

3. Set up the Cognos data source for the testing site.

Export the Cognos content store database

1. Sign in to ChangePoint as ChangePoint administrator.

2. Click ▦ > **Analytics > Portal**. **IBM Cognos Analytics with Watson** appears.

3. Click the **Open menu** icon at top left corner, and then click **Manage > Administration console** . The **IBM Cognos Administration** console appears.

4. Click **Content Administration**, and then select the export icon.

5. Enter a name for the deployment specification (for example ChangePoint, and then click **Next**.

6. In the **Deployment method** section, click **Select the entire Content Store** and then click **Next**.

7. In the **New archive** option, enter a name for the deployment archive (for example, Changepoint_Export) and then click **Next**.

8. Enter an encryption password for the archive and then click **OK**.

9. Review the summary and then click **Next**.

10. Click **Save and run once**, and then click **Finish**.

11. Select **Now**, and then click **Run**.

12. Click **OK**.

Import the Cognos metadata package

Import the Cognos metadata package for the testing site by following the instructions in "Importing the ChangePoint metadata package" on page 112.

Set up the Cognos data source for the testing site

1. Delete the production ChangePoint data source.

2. Recreate the data source following the instructions in "Setting up the data source for IBM Cognos Analytics" on page 113.

Setting up Client Portal in a training environment

For users to access Client Portal in a training environment, you can either set up a separate Client Portal website, or users can specify a different login page in the URL of an existing ChangePoint website, for example:

```
http://servername:port/fcelogin.asp
```

Note: If enhanced session management is enabled in ChangePoint Administration, you must create a separate Client Portal website. For more information, see "Setting up a Client Portal website" on page 143.

A. Configuration file settings

About ChangePoint configuration files

There are two types of files that contain configuration settings for ChangePoint.

Web.config files

Web.config files are application configuration files that contain settings that apply to the areas of ChangePoint that were developed using ASP .NET web application technology (.aspx).

There is a configuration file for each application. The default locations are:

```
<cp_root>\Enterprise\Web.config
<cp_root>\CP Web Services\Web.config
<cp_root>\API\CP Web Services\Web.config
<cp_root>\Enterprise\WebAPI\Web.config
<cp_root>\Enterprise\WebSockets\Web.config
```

Global.asa file

The Global.asa file is a centralized file that contains settings that apply to areas of ChangePoint that were developed using the ASP web application technology.

The default location is:

```
<cp_root>\Enterprise\Global.asa
```

Web.config configuration file settings

Authentication settings

By default, all ChangePoint website folders and files are set to application authentication. If you set up your websites for SSL, you must change settings in the corresponding Web.config files. To use SSL with application authentication, see "About application authentication" on page 137.

Caching settings

- EnableSQLDependency

  If set to 1, the ChangePoint SQL dependency cache is enabled. Resource feature information will be cached as resources sign into the application. The default value is 1.

- SQLDependencyCacheDuration

The elapsed time required in minutes before the ChangePoint SQL dependency cache is cleared. The default is 240.

Cognos Analytics settings

Launch Cognos portlets and portals in new browser window

By default, Cognos portlets and portals are launched within the ChangePoint container. However, you can configure Cognos portlets and portals to open in a new browser window.

- Cognos.IE.LaunchPortletsInNewWindow

  When set to "true", Cognos portlets and portals are launched in a new browser window.

Cookie settings

By default, cookies are enabled. To disable cookies, edit the sessionState element and set cookieless="true".

Export Publishing settings

These settings in the ChangePoint Web.config file apply only to the export publishing resend option in ChangePoint Administration.

- MessageBroker.HostName

  FQDN of the machine running the RabbitMQ Service.

- EnableEmail

  If set to 1, email notifications are enabled for export publishing errors. The ChangePoint Mail Service must be installed in order to send notifications. The default is 0.

- EmailAddress

  A semicolon-separated list of email addresses to which notifications of export publishing errors are sent. The EnableEmail setting must be enabled and the ChangePoint Mail Service must be installed in order to send notifications to the specified addresses.

Field settings

The Fields.MaxSearchResult setting defines the maximum number of records that can be returned for certain type-ahead fields. When the maximum is exceeded, the user is prompted to narrow the search criteria. The default is 500.

The Fields.MaxSearchResult setting applies to the following type-ahead fields:

- new type-ahead fields (excluding the tree view type-ahead fields), which are identified by the yellow background when the user starts entering data in the field

- new type-ahead fields for configurable fields

- scenarios comparisons

There are no configuration settings for the old type-ahead fields with the clear fields icons. The maximum search results for these fields are hard coded and vary depending on the field.

Type-ahead configurable fields on projects and requests have an internal limit of 1000 for the maximum number of records that can be returned. The imposed limit is the lesser of 1000 or the value of the Fields.MaxSearchResult setting.

There is a separate setting for mobile access. For more information, see "Mobile access settings" on page 194.

File type filter settings

The upload.FileExtensionNameExcludeFilter setting defines the file types that are blocked from being uploaded through File Upload dialogs. The default list is "exe,bat,com."

HTTP runtime settings

If required, you can modify the values of these attributes of the httpRuntime setting:

```
<httpRuntime executionTimeout="900" maxRequestLength="40960" ... />
```

The descriptions of the attributes are as follows:

- executionTimeout

  The maximum number of seconds that a request is allowed to execute before being timed out. The default is 900.

- maxRequestLength

  The input buffering threshold in KB when uploading files. The default is 40960.

Logging settings

- Logging.UseInProcessLogging

Enables/disables in-process logging. If set to false, then nothing is logged unless the out-of-process logging process is running.

- Logging.LogToDB

Enables/disables database logging. When database logging is enabled, the data is stored in the Trace table in the Changepoint_Extended database, which is located on the same server as the ChangePoint database.

- Logging.LoggingFilePath

Creates a new logging file under the specified path every day, unless the path is empty, in which case nothing is logged to the file.

- Logging.RollingFileSize

Threshold size of the file in KB after which a new file is created. Default size is 10000 KB.

- Logging.LoggingLevel

Default logging level is set to `Informational`, which logs minimal information that is required to diagnose issues. `Verbose` level logs more incoming WebAPI request payload information for in-depth diagnostics.

- Logging.LoggingKeywords

  - `WebAPI` keyword logs all WebAPI Errors/Critical Errors

  - `Performance` keyword logs response time information for WebAPI requests.

Mobile access settings

The following settings are related to mobile access:

- MobileFields.MaxSearchResult

The maximum number of records that can be returned for type-ahead fields when ChangePoint is accessed using a mobile device. The default value is 25.

- SupportedMobileDevice

A semicolon-separated list of supported mobile devices as referenced in the browser's user-agent string. You can add unsupported mobile devices to allow them access, if required.

Page Content IDs (PCIDs)

Each string on the user interface is associated with a page content ID (PCID). There is a setting that you can use to to display the PCIDs instead of the strings, which can be helpful if you want to identify certain strings.

> **Warning:** It is strongly recommended that you enable this setting only in a test environment.

- GlobalDebug

When set to 1, the PCIDs are displayed on the user interface instead of the strings.

Page Size

The default page size used in some areas of ChangePoint (for example, project portfolio and advanced search) is controlled by the following setting:

- PageSize

The number of records to display before paging. The default is 100.

Projects tree view settings – Web.config

The **Projects** tree view display is controlled by several parameters, some of which are set in Web.config. Other parameters are set in Global.asa.

Number of projects in the Projects tree view

- tvProject.Project.RecordAmount

Determines the number of projects (default 500) that are displayed initially in the **Projects** tree view.

- tvProject.Project.PackAmount

Determines the number of projects (default 50) by which the **Projects** tree view is incremented on demand.

Refresh of the Projects tree view

- tvProject.Project.AutoRefresh

When enabled (tvProject.Project.AutoRefresh=1, default), the **Projects** tree view is refreshed automatically when a project is created or deleted, or when the project name is modified.

When disabled (tvProject.Project.AutoRefresh=0), the **Projects** tree view is not refreshed when a project is created or deleted, or when the project name is modified, until the **Filter** button is clicked.

- tvProject.Task.AutoRefresh

When enabled (tvProject.Task.AutoRefresh=1, default), the **Projects** tree view is refreshed automatically when a task is created or deleted, or when the task name is modified using the **Edit Task** dialog.

When disabled (tvProject.Task.AutoRefresh=0), the **Projects** tree view is not refreshed when a task is created or deleted, or when the task name is modified using the **Edit Task** dialog, until the **Filter** button is clicked.

Initial loading when a project is selected in the tree

See "Projects tree view settings – Global.asa" on page 200.

Copy project

See "Projects tree view settings – Global.asa" on page 200.

Resource Planner settings

Maximum number of fiscal or daily periods displayed

By default, the maximum number of fiscal periods that can be displayed in a worksheet view is one year's worth, which is specified as 364 (days).

The maximum number of daily periods is 31 (days).

You can increase the number periods using the following settings:

- ResourcePlanner.MaxFiscalPeriodDays = 364

- ResourcePlanner.MaxDailyPeriodDays = 31

  Warning: Keep in mind that increasing the values of these settings too high can negatively affect system performance due to the amount of data that is processed and displayed. Be sure to test the settings using actual data to ensure there are no adverse affects.

Scenario comparisons worksheet (SCW) settings

The following settings apply to scenario comparisons:

- ScenarioComparison.MaxViewColumnCount

   The maximum number of columns that can be selected in a view. The default is 100.

- ScenarioComparison.MaxFilterColumnCount

   The maximum number of columns that can be displayed in the filter column of the **Manage Filter** dialog. The default is 5000.

- ScenarioComparison.MaxFilterScenarioCount

   The maximum number of items that can be selected in the **Selected items** list on the **Other Criteria** tab of the **Manage Filter** dialog. The default is 50.

Session expiration settings

These settings control the number of minutes in a ChangePoint session during which there is no user activity before an alert message is displayed to warn the user they will be signed out. The alert message provides the user with the option to remain signed in or sign out. If the user takes no action within the alert timeout value, they are automatically signed out of the session.

Note: The expiration settings do not apply to the following components: ChangePoint Analytics, Intelligent Forms pages, ASP reports such as revenue recognition, scenario comparisons and surveys. However, the session expiration countdown will begin when the user closes the component.

- <add key="sessionExpiration.idleTime" value="20" />

   The value is the number of minutes that the ChangePoint session is idle before the alert message is displayed. Default value is "0" (no limit).

- <add key="sessionExpiration.AlertTimeout" value="5" />

   The value is the number of minutes that the alert message is displayed before the user is automatically signed out of the ChangePoint session if the user does not intervene. Default value is "0".

Time-out settings

The ASP .NET implementations (.aspx) in ChangePoint use the following setting:

- CommandTimeOut

   The default value is 600 seconds.

Terminology mode settings

The mode is selected when ChangePoint is installed or upgraded. The only reason for changing this setting after installation is to switch terminology.

For ChangePoint PPM (Project Portfolio Management):

```
Application("CompanyProfile") = "ITD"
```

For ChangePoint SA (Services Automation):

```
Application("CompanyProfile") = "PSO"
```

Note: Other changes are required to switch terminology. For more information, see "Switching between ChangePoint PSA and PPM (PSO mode and ITD mode)" on page 231.

Tree view settings

The naming pattern for the tree view settings in the Web.config file is:

```
<add key="treeview.node.property" value="n"/>
```

For example, the following is a typical pair of tree view settings:

```
<add key="tvMyContact.Contact.RecordAmount" value="500"/>
<add key="tvMyContact.Contact.PackAmount" value="50"/>
```

This example sets the RecordAmount and PackAmount properties for the Contact node of the MyContact tree view. The RecordAmount property defines the maximum the number of records to load when the node is first expanded. The PackAmount property defines the size of the next lot of records to load for this node. Using the above example, if there are more than 500 contacts in the database, the first expansion shows the first 500 contacts, with a "next" link at the bottom of the list. Clicking the "next" link retrieves the next 50.

Note: You cannot use tvOpportunity.Engagement as a treeview.node pair for this purpose.

Websocket message size

The following setting is in the WebSockets\Web.config file.

• MaxIncomingWebSocketMessageSize

The default value of 65536 fixes the concurrent task locking issue in Project Worksheet for projects that have approximately 200 tasks. The general guideline is to increase the key value by 65536 per 100 tasks above 200.

Workflow settings

The following settings control when a filter appears in the workflow view:

*   WorkFlow.Layout.StateShapeThreshold

    The maximum number of states that can be displayed in the workflow view before a filter appears.

*   WorkFlow.Layout.StateTransitionThreshold

    The maximum number of transitions that can be displayed in the workflow view before a filter appears.

The filter will also appear if the total number of states and transitions in the workflow is greater than the sum of these two settings.

Global.asa configuration file settings

Caching settings

*   Application("EnableSQLDependency") = 1

    If set to 1, the ChangePoint SQL dependency cache is enabled. Resource feature information will be cached as users log onto the application.

*   Application("SQLDependencyCacheDuration") = 240

    The ChangePoint SQL dependency cache is cleared after 240 minutes.

Cookie settings

By default, the AgentlessCookie setting is enabled:

```
Application("AgentlessCookie") = 1
```

When enabled (set to 1), a cookie will be returned to the client machine with the user's logon ID. The cookie can be used by monitoring software to identify a user for reporting purposes. You can disable the setting by changing the value to 0.

Page Content ID (PCID) settings

```
Application("GlobalDebug")=0
```

When enabled, the page content IDs (PCIDs) are displayed in the user interface instead of the PCID strings (field labels). This can be helpful to debug changes to the labels, but should only be done in a test environment. The setting is disabled by default.

Page size

The default page size used in some areas of ChangePoint (for example, project portfolio and advanced search) is controlled by the following setting:

```
Application("PageSize") = 100
```

The value is the number of records to be displayed before paging.

Projects tree view settings – Global.asa

The **Projects** tree view display is controlled by several parameters, some of which are set in Global.asa. Other parameters are set in Web.config.

Initial loading when a project is selected in the tree view

- tvProject.SkipAutoLoad

When enabled (tvProject.SkipAutoLoad=1), the **Projects** tree view is displayed only after a resource clicks the **Filter** button.

When disabled (tvProject.SkipAutoLoad=0, default), the **Projects** tree view is displayed when the resource selects the project in the tree.

Refresh project tree after copying a project

- tvProject.CopyProject.AutoRefresh

When enabled (tvProject.CopyProject.AutoRefresh=1, default), the project tree view is refreshed automatically when copy project is used to create a new project.

When disabled (tvProject.CopyProject.AutoRefresh=0), the project tree view is not refreshed after a project is copied, until the **Filter** button is clicked.

Number of projects in the project tree view

See "Web.config configuration file settings " on page 191.

Refresh of the project tree view

See "Web.config configuration file settings " on page 191.

Reporting

The following configuration settings relate to reporting:

- Application("VacationTrackStartDate") = "YYYY-MM-DD"

  The start date for reports that track vacation.

- Application("rsNotificationInterval") = 5

  The interval, in minutes, that the ChangePoint UI checks to see if the user has any report schedules that have completed. If reports have completed, then a small, informational window is displayed in the ChangePoint interface.

- Application("OpenRequestsByCustomerRecordAmount") = 500

  The maximum number of customer records that are returned in the customer drop-down list on the filter page for the Open Requests by Customer report.

Terminology mode

The mode is selected when ChangePoint is installed or upgraded. The only reason for changing this setting after installation is to switch terminology.

For ChangePoint PPM (Project Portfolio Management):

```
Application("CompanyProfile") = "ITD"
```

For ChangePoint SA (Services Automation):

```
Application("CompanyProfile") = "PSO"
```

> **Note:** Other changes are required to switch terminology. For more information, see "Running both ChangePoint SA and PPM websites on the same database" on page 231.

Time-out (ADO Commands)

To enable a global time-out value that will be used for all ADO commands, change "0" in the following setting to the number of seconds that you want to assign to the global time-out value:

```
Application("GlobalCommandTimeout") = 0
```

When set to zero, which is the default, the global time-out setting is disabled. In this case, the time-out utilized is either the ADO command value or the value that is supplied in connection string.

B. Troubleshooting

ChangePoint installer issues

* WARNING: Redis cache service could not be installed. Ensure that service (RedisService) and port (6379) is not in use. Please review the RedisCacheService.log file under the InstallLog folder and install and start the service manually.

During the ChangePoint 2022 installation, Redis cache service could not be installed and started. This would typically occur if there is already a Windows service, including an existing instance of Redis, that is using the Redis service name (RedisService), or the Redis port (6379) is currently assigned to another process.

To properly install the Redis service, you must assign a unique service and a port that is not currently assigned. Please refer to the "Installing and Configuring Redis" on page 33 for the manual Redis service installation and start up commands.

Database upgrade error

If the database upgrade fails, an error message appears. Do the following:

1. Check the log file for details. The log file path is specified in the error message.

2. Restore the database from the backup you made before upgrading.

3. Resolve the issues detailed in the log file.

4. Perform a manual database upgrade.

IIS error when installing ChangePoint websites

If you attempt to install the ChangePoint websites on a web server, but Internet Information Services (IIS) is missing, or the wrong version of IIS is installed, an error message appears.

Make sure that a supported version of IIS is installed on the web server and then try again.

Error: Operation failed with #X######X An attempt was made to load a program with an incorrect format

If this error occurs during the installation of the ChangePoint websites, ensure that the required components and roles have been installed on the web server. For more information, see the *ChangePoint Software Compatibility Matrix*.

Error Number: 0x80004005 Description: Unspecified error Setup will now terminate

This error might occur if you use Remote Desktop Protocol (RDP) to install ChangePoint.

Increase the colors setting to more than 256 colors (**Remote Desktop Connection > Display > Colors**.)

ChangePoint troubleshooting issues

Empty keys error in Event log

The NotificationProvider.Key1 and NotificationProvider.Key2 keys must be configured with valid license values to enable use of the ChangePoint Mobile app.

If you have not set up ChangePoint to use the Mobile app, then you must comment out the NotificationProvider.Key1 and NotificationProvider.Key2 keys in the `CPMail.exe.config` file.

HTTP 403 error
Project Planning Worksheet fails to save
Preferred resources cannot be edited

If you have enabled Request Filtering on the ChangePoint website or use tools such as URLScan to restrict HTTP verbs in HTTP traffic, you must do the following:

1. Add the following verbs to the [AllowVerbs] section:

    *   PUT

    *   PATCH

    *   DELETE

2. Remove the same verbs from the [DenyVerbs] section.

Blocking these verbs can result in unexpected HTTP errors and functional issues in ChangePoint. As of this service pack, ChangePoint deploys the new ChangePoint REST API internally (and externally as an option) to enable mobile app support and some internal product functionality. The REST API uses the HTTP verbs in its transactions.

3. Restart the web server or web application.

Project planning worksheet does not load
Error when accessing Manage Preferred Resources
"Access to registry key 'Global' is denied" in ChangePoint event log

Restart the web server. These errors can occur when registry permissions have been changed.

Users cannot upload large attachments

In order to upload attachments up to 40 MB in size to team folders, requests, and knowledge items, you might have to set the following in IIS Request Filtering and/or in URLScan.ini, depending on the versions of Windows Server and IIS that you are using:

```
maxAllowedContentLength=40000000
```

ChangePoint web pages do not render

Ensure that the required Windows components have been installed.

Browser not supported message in Internet Explorer (IE)

If users try to access ChangePoint using Internet Explorer and receive a message that the browser is not supported, they must do the following:

1. Disable the compatibility view setting.

2. Ensure that the ChangePoint website is not in the "Websites you've added to Compatibility View" list.

For more information about disabling the compatibility view setting, see the Internet Explorer online help.

ChangePoint web pages take a long time to render

The first time you access a page in ChangePoint, the page is compiled and takes longer than usual to render. If your antivirus software interferes with the compilation, a page error might occur. If a page error occurs, navigate to the page again. Some larger pages require re-navigating more than once. After the compilation is complete, the pages render more quickly.

Error message appears instead of the ChangePoint sign-in dialog box

Ensure that the Login Settings utility has been run to configure the ChangePoint configuration files and that the database server, database name and SQL account information entered is correct. For more information using the Login Settings utility, see "About configuring database connection settings" on page 65.

Error message: Please contact your system admin for this error!

Refer to the ChangePoint Section in the Event Viewer for the actual error message.

Error message: ChangePoint is not correctly registered

Ensure that the license file has been imported using ChangePoint Administration.

Application is restarting error in the web browser

Ensure that the ChangePoint application folder (<cp_root>) is excluded from antivirus scans. For more information, see:

JavaScript errors in Internet Explorer

After an upgrade, users must delete all browsing history in Internet Explorer. If users still encounter JavaScript errors after they have deleted the browsing history, they must delete the temporary Internet files manually. For more information about deleting browsing history and temporary Internet files, see the Internet Explorer online help.

Ajax errors

Ajax errors are typically a result of a configuration mismatch between the authentication configured for the website in IIS and the authentication settings configured in the Web.config file.

To resolve the errors, correct the mismatch. For more information, see the authentication sections in "Overview of configuration" on page 49 and "Web.config configuration file settings " on page 191.

ChangePoint Windows Services errors in the Event Viewer

Ensure that the database connection settings have been configured properly for the ChangePoint Windows Services. For more information, see "About configuring database connection settings" on page 65.

Repeated logon failures with "Your session is no longer active" message

This error can occur if the ChangePoint websites are sharing the same application pool, or if you attempted to install multiple website instances without specifying a unique name and port number for each website. To resolve the issue, ensure that the application pool, website name, and port number are unique for each website instance.

Knowledge search returns "No matches found" message

Do the following:

1. Verify that the user has the required permissions to view the records.

2. Verify that the "CPFullText" or "CPFullText using background updates" scheduled jobs are enabled and ran successfully.

If the user has the required permissions and the scheduled jobs ran successfully, then there might be a full text issue. Refer to the Microsoft website for information on troubleshooting full text issues.

Child workgroups not sorted correctly in standard reports that contain a Resource Workgroup selection field

Cannot expand workgroups in the User Setup tree view

If one or both of the above issues occur, you must regenerate the object breakdown structure (OBS) for workgroups:

1. From the **2020 Release Notes and Patches** team folder, download the **Workgroup OBS Utility.zip** file from the **Utility** subfolder

2. From the **Workgroup OBS Utility.zip** file, extract the CPRegenerateWGOBS.exe to any client machine that has a connection to the ChangePoint database server.

3. Execute `CPRegenerateWGOBS.exe`.

4. Enter the SQL server name, database name, SQL login, and password.

5. Click **Connect**.

6. From the **Global Workgroup** list, select the global workgroup.

7. Click **Generate OBS**.

SSO ADFS issues

Server Error in '/RP-STS_ADFS' Application

If users encounter an error similar to the following:

Server Error in '/RP-STS_ADFS' Application.

The data protection operation was unsuccessful. This may have been caused by not having the user profile loaded for the current thread's user context, which may be the case when the thread is impersonating.

Do the following on the ChangePoint web server:

1. In Internet Information Services (IIS) Manager, click **Application Pools**

2. Select the Application Pool used by the ChangePoint web site.

3. Click **Advanced Settings**

4. Set **Load User Profile** to True, then click **OK** to save and close **Advanced Settings**

5. Re-open **Advanced Settings**, set **Load User Profile** back to False, then click **OK**

ChangePoint Web Services API Issues

Errors related to .Net version when accessing Web Services API

If users encounter .Net version-related errors when accessing the Web Services API, and the API is installed on a web server other than the ChangePoint web server, ensure that the application pool for the hosting website is using the required version of the .NET framework.

ChangePoint Windows Services Issues

ChangePoint Windows Service does not appear in Add/Remove program in Windows Control Panel

If the Windows service you want to remove does not appear in the **Add/Remove Programs** in the Windows Control Panel, then you must do the following:

1. Run the installation program for the service from the ChangePoint product media for *the previous release*, and select **Repair**.

2. After the installation is repaired, you can remove the service using **Add/Remove Programs**.

ChangePoint Windows Service does not start

All ChangePoint Windows Services validate their version numbers against the version table in ChangePoint. The version numbers must match, otherwise the service will not start, and a message is recorded in the event log.

Emails remain queued

Due to startup timing issues, it is possible that services have been started but are not functioning properly, which may cause emails to remain queued instead of being sent.

You can fix this problem by creating a dependency for the ChangePoint Windows Services on the MSSQLServer service. For more information, see the Microsoft knowledge base article 193888 at: https://support.microsoft.com/en-us/help/193888/how-to-delay-loading-of-specific-services.

Exchange Server troubleshooting

Calendar items do not synchronize from ChangePoint to Outlook

- Ensure that the user has the Enable Calendar Synchronization feature.

- Ensure that the user has selected the correct calendar synchronization option in the **Preferences** view in ChangePoint.

Calendar items do not synchronize from Outlook to ChangePoint

- Ensure the ChangePoint Exchange Synchronization Service is running.

- Ensure that calendar items match the General Calendar Synchronization Options settings (Daily Start Time, Daily End Time and Time Zone) in the **Preferences** view in ChangePoint.

Event log

Check the event log for messages and errors. The following table lists the common events (EWS refers to the Exchange Web Service).

Event	Comments
Description: The primary SMTP address must be specified when referencing a mailbox.	*Error*. The message is returned via EWS. Users must have an Exchange primary email address in ChangePoint.
Description: Unable to create calendar item in Exchange for user: user@domain.com	*Error*. The message is returned via EWS. Calendar item add failed. This can happen for a number of reasons, for example, a user is synchronizing with an alternate email address.
Description: Unable to update calendar item in Exchange for user: user@domain.com	*Error*. The message is returned via EWS. Update to calendar item failed. This can happen for a number of reasons, for example, a user is synchronizing with an alternate email address.
Description: Unable to update calendar item in ChangePoint for user: user@domain.com	*Error*. The message is returned via ChangePoint. Update to calendar item failed.
Description: Unable to add calendar item in ChangePoint for user: user@domain.com	*Error*. The message is returned via ChangePoint. Calendar item add failed.
Description: Autodiscover exception occurred in DiscoverTryUrls. *Email Address*: user@domain.com *Exception*: The email address cannot be found.	*Warning*. The email address cannot be found.
Description: Autodiscover exception occurred in DiscoveryTryUrl. *Target url*: https://servername.domainname /autodiscover/autodiscover.xml	*Warning*. Autodiscovery failed when targeting the indicated URL.

Event	Comments
Description: Autodiscover exception occurred in GetRedirectUrl. *Target url*: https://servername.domainname /autodiscover/autodiscover.xml	*Warning*. Autodiscovery failed when targeting the indicated URL.
Description: Autodiscovery failed for user: user@domain.com	*Warning*. Autodiscovery failed for the indicated user.
Description: Calendar Synchronization Started - Version: XX.XX.XXX.XXX	*Information*. Documents the start of a synchronization cycle.
Description: Calendar Synchronization Finished	*Information*. Documents the completion of a synchronization cycle.
Function: Changepoint.Synchronization.Exchange .CreateCalendarItem *Response*: ErrorCalendarDurationIsTooLong *Extended Information*: Email address: user@domain.com	*Error*. EWS prevents calendar items from being created when duration is greater than five years. This is a limitation in Exchange .
Function: Changepoint.Synchronization.Exchange .UpdateCalendarItem *Response*: ErrorCalendarDurationIsTooLong *Extended Information*: Email address: user@domain.com	*Error*. EWS prevents calendar items from being updated when duration is greater than five years. This is a limitation in Exchange .

Event	Comments
Function: Changepoint.Synchronization.Exchange.GetItem *Response*: ErrorItemNotFound *Extended Information*: Id: AAMkADUxOWVlNTdjLWE2OW QtNDQwMC1hMTZmLTUyMWFk N2RmNDk4OQBGAAAAAAlhrFE 5hKpSK2C4OPkOtc/BwAAOrm5Pd RuTI2+olSwbXC4AAAAATSrAAD Bake3jpVuTLttXQS5sS3xAAzFdNI5AAA=	*Error*. An attempt was made to retrieve a deleted item from Exchange. This message can be ignored as the code responds by recreating the deleted item.
Function: Changepoint.Synchronization.Exchange.UpdateCalendarItem *Response*: ErrorOccurrenceTimeSpanTooBig *Extended Information*: Email address: user@domain.com	*Error*. The message is returned via EWS. Indicates that the time allotment for a given occurrence overlaps with another occurrence of the same recurring item.

SQL Server troubleshooting

SQL Server setup issues

The System Information script (SQLEnvironmentReport.sql) provides information that you can use to troubleshoot system setup issues.

1. Log on to the SQL server machine with the local administrator account.

2. Run the following script from the ChangePoint product media:

```
\Changepoint\Utilities\Changepoint System Information Script
\SQLEnvironmentReport.sql
```

The following information is reported:

•   General system information:

```
Host Name
OS Name
OS Version
OS Configuration
```

```
System Up Time
System Manufacturer
System Model
System Type
Processor(s)
BIOS Version
Windows Directory
Boot Device
System Locale
Input Locale
Time Zone
Total Physical Memory
Available Physical Memory
Page File
Page File Location(s)
Hotfix(s)
Network Card(s)
All Services Status
SQL Service Status
```

- Current SQL Instance information

```
Current SQL Instance
SQL Server Version
SQL Server Property
SQL Server Configure
```

- Database information (will list information for each database)

```
Database Name
Database Property
Database Files
```

ChangePoint database troubleshooting

Error "!!! MSDTC on server 'server_name' is unavailable" during manual database upgrade

Start the "Distributed Transaction Coordinator" service on the server where the database upgrade is being performed. Then repeat the manual database upgrade steps to complete the installation process.

Password validation error when running Porting Changepoint.sql

If you receive a password validation error when running the `Porting Changepoint.sql` script, reset the password to a password that conforms to your Windows security policy. If the database has already been attached successfully, run the script again starting from:

```
USE Changepoint
GO
```

Similarly, if you receive any other errors with this script and the database is already attached, fix the problem and be sure to choose an appropriate starting point beyond the attachment section when rerunning the script.

Restoring the database from a backup

When you restore the ChangePoint database on a server, the service broker is disabled. Run the following on the restored database to enable the service broker:

```
ALTER DATABASE <DatabaseName> SET SINGLE_USER WITH ROLLBACK IMMEDIATE
ALTER DATABASE <DatabaseName> SET ENABLE_BROKER
ALTER DATABASE <DatabaseName> SET MULTI_USER
```

Excessive table growth issues

If email notifications have been enabled in ChangePoint Administration, verify that both the ChangePoint Email Notification Service and the ChangePoint Mail service have been installed and configured to run at regular intervals. Otherwise, the EmailAuditStaging, EmailAuditNotification, and EmailQueue tables in the database can potentially grow to a very large size.

Archive database troubleshooting

Archive Aged Entities Job or Data archiving.dtsx fails

If the Archive Aged Entities job or `Data Archiving.dtsx` fails for any reason, and you do not want to proceed with the archiving, you must run the following script to re-enable triggers and foreign keys on the ChangePoint source database:

```
C:\Program Files\Changepoint\Changepoint\Data Archiving\EnableAllTRsNFKs.sql
```

If required, restore the archive database from backup.

Temporary Database available for troubleshooting

The Archive Aged Entities job automatically creates a temporary database named <database name>_ArcDistribution on the source database server. The temporary database is available for troubleshooting purposes until the next time that the job is run, when it is dropped and recreated.

Archive database performance issues

The following performance issues have opposing solutions:

- To improve performance of the archive database for end users, you can add indexes to the Archiving database.

- To improve the speed of the Archiving Aged Entities scheduled job, you can remove indexes from the Archiving database.

You can add indexes by applying the `Adding archiving indexes.sql` script, or remove indexes by applying the `Removing archiving indexes.sql` script from the following location on the ChangePoint product media:

`\Changepoint\Manual Install\Data Archiving\`

Cognos Analytics installation troubleshooting

"Invalid login response" message when signing into Analytics Portal from ChangePoint

This message appears when the security configuration has not been set up for Cognos. For more information, see "Setting the security settings in Cognos" on page 115.

Error: RQP-DEF-0177 appears in report or workspace area

Error: "RQP-DEF-0177 An error occurred while performing operation 'sqlPrepareWithOptions' status='-201'" in the report or workspace area, likely means that the database name in the SQL connection string for Cognos was not specified during installation.

Error: Invalid Web Content URI when configuring the Application Tier

If you get this error when trying to save the configuration of the Environment node in the **Explorer** pane during the configuration of the Application Tier, then you must reset the Web Content URI to the default as follows:

1. In the **Explorer** pane, select the Portal Services node.

2. Click in the Web Content URI field.

3. From the Cognos menu, select **Edit > Reset to Default**.

Connection test fails when testing the data source configuration

If the connection test fails for either SQL or the JDBC, it likely means that no SQL Server Native Client was installed on Application Tier server, or the wrong native client was installed.

On the Application Tier server, install the version of SQL Server Native Client that matches the SQL version on the server that hosts the Cognos content store. For more information, see the "Setting up the data source for IBM Cognos Analytics" on page 113.

Error: AAA-CFG-0008 in AppTier configuration

If the following message appears during the start of the Cognos service on Application Tier:

```
Error: "AAA-CFG-0008 The handler class 'com.changepoint.cap.CapControl '
cannot be loaded".
Error: "java.lang.ClassNotFoundException: com.changepoint.cap.CapControl".
```

Retest the ChangePoint namespace connection.

If the test passes, restart the service.

If the test fails, delete and recreate the ChangePoint namespace, then test again.

Web server error when embedding graphics that are hosted on a web server in reports

To embed graphics that are hosted on a web server in your reports, refer to the IBM Cognos Analytics product documentation.

If you are using URLScan, WebRequest Filtering or Application Filtering at your firewall to block WebDAV traffic, you must make the necessary security configuration changes.

ChangePoint-Cognos Sync utility troubleshooting

Timeout error when updating the model with a new revision

If there are a large number of configurable fields in the database, one or both of the following might occur when you update the Cognos model with a new revision:

- **New Revision** dialog box takes a long time to appear

- "Message: Timeout expired" error in the Cognos UI log file

You can increase the timeout setting in the CognosClientTools.exe.config file:

1. As administrator, open the `CognosClientTools.exe.config` file:

```
%programfiles%\Changepoint\Cognos Client Tools\CognosClientTools.exe.config
```

2. Edit the following key, then save the file. The default value is 300.

```
<add key="CommandTimeOut" value="1800" />
```

Error: BME-SP-0007 An unknown error occurred during execution

This error appears on the **Details** dialog box of the Sync Utility during the updating of the delta page content and configurable fields to create a new revision of the Cognos model.

Ensure that the same version of the SQL Server Native Client is installed on the ChangePoint Cognos administrator workstation, and the server that hosts the Cognos content store.

Error: BME-SP-0032 Your user id or password is incorrect. Re-enter your logon credentials

If you see this message when running the Sync Utility, ensure that the ChangePoint database is online by restarting the Cognos service on the Application Tier.

Troubleshooting scheduled jobs

Resource Demand Calculation scheduled job – performance issues or failure

By default, the Resource Demand Calculation scheduled job rolls up projects in batch processing mode.

However, if the job was not scheduled to be run daily, batch mode may not handle the load from accumulated changes. Or if there is an issue with one or more projects, the job might fail. In both cases you can switch the job to single mode processing as a workaround to roll up projects manually until the issues have been addressed.

To switch the Resource Demand Calculation job to single mode processing

1. In SQL Server Management Studio, append "0" to the step that calls the stored procedure RollupProjectsByFiscalPeriods as follows:

```
exec RollupProjectsByFiscalPeriods 0
```

2. You can then start and stop the job manually multiple times until all projects have been rolled up.

To revert to batch processing mode, either remove the "0", or change the "0" to "1".

Troubleshooting Intelligent Forms

How do I troubleshoot issues that I encounter while using forms?

The errors that are generated while using forms are listed in the **Management** tab of Infiniti Manage. If you do not have access to Infiniti Manage, contact your Infiniti administrator to do this for you.

When I access a submenu item in the Actions menu, a sign-in for Infiniti appears

To enable single-sign on for Intelligent Forms, the resource's email and password must be entered into their ChangePoint user account.

When I click Intelligent Forms > Infiniti Manage, an "Access denied" error appears

To access Infiniti Manage from ChangePoint Administration, a resource must be assigned the Global administrator role in Infiniti Manage. For more information, see "About security features for Intelligent Forms" on page 1.

C. Financial Analysis Information

Adding fiscal periods to group financial analysis data

Data in the Financial Analysis Data Providers is grouped by the default set of fiscal periods selected in the Funding and Scenario Comparison Setup in ChangePoint Administration.

To add other fiscal periods, insert a row into the database table FinAnnFiscalPeriod that contains the billingofficeid of the fiscal periods.

> **Note:** These changes must be done directly in the database table: there is no UI.

> **Note:** It is not necessary to add every billing office or every set of fiscal periods. It is only necessary to add one for each frequency (for example, weekly, monthly or quarterly) that is to be reported on.

Enabling financial analysis record types

The underlying financial analysis views rely on data that is calculated by the Financial Analysis Summary scheduled job and Calculate Project Costs scheduled jobs for specific record types. FinAnnRecType contains all the record types. The "enabled" field indicates which record types are enabled for calculation.

By default, only part of the record types are enabled.

Additional record types can be enabled. Existing record types can be disabled if they are not being used (for example, the types for forecast may be disabled if status updates are not being done and the information is not needed for reporting).

> **Note:** These changes must be made directly in the database table: there is no UI.

To enable a record type, mark the row as "enabled" in the FinAnnRecType table in the database.

> **Warning:** The more record types that are enabled, the longer the processing of the two jobs will take. This applies particularly to record types that group data at the task assignment level. For large databases, reporting at the task assignment level may result in performance issues. Ensure the grouped data providers are used (by month or fiscal period) and that the report is filtered sufficiently.

Dependencies among record types

- Types 0-26, which are enabled by default, should be left as enabled if the scenario comparisons functionality is being used.

- If you use funding sources, leave existing record types enabled. To start using funding sources after the upgrade, enable the appropriate record types:

  - If Projects are associated with funding sources, enable record types 28, 29, 42, 43.

  - If Requests are associated with funding sources, enable types 1, 3, 7, 9, 21, 22, 23.

  - If Opportunities (Candidates) are associated with funding sources, enable types 11, 12, 13, 14.

  - If any type that is related to invoiced items (type 1, 2, 20, 32, 37, 38, 39, 40, 41, 46) is enabled, enable type 0.

  - If type 12 is used, enable type 11.

  - If type 14 is used, enable type 13.

D. Administrator Information

Setting up OData access to ChangePoint data for reporting

OData is a standard open data protocol for consuming data through REST APIs. You can create an OData connection to a ChangePoint data model to access data for reporting and analysis.

To access ChangePoint data, you need to create a data set of the data required for your report.

Creating a data set in IBM Cognos Analytics

To create a data set in IBM Cognos Analytics, follow the instructions on the IBM website at:

https://www.ibm.com/docs/en/cognos-analytics/11.0.0?topic=data-creating-sets

> **Tip:** If you encounter a timeout when importing a data set, break the data up into smaller data sets and create OData connections to each of them. You can reduce the size of a data set by limiting the number of columns and queries, and adding filters to limit the amount of data being imported.

Creating the OData connection to PowerBI

Create the OData URL by appending the data set ID to the ChangePoint URL. Then use the OData URL to connect to the data set from PowerBI.

1. In ChangePoint Analytics, locate the data set.

2. Right-click the data set and click **Properties** (or click the Actions menu ⋮ >

   Properties).

3. In the **Properties** pane, expand the **Advanced** section, and then copy the ID.

4. Append the data set ID to the ChangePoint URL as follows:

```
http://[ChangePoint URL]/OData/Data('[data set ID]')
```

Creating the OData connection to a data set

1. In ChangePoint Administration (**Tools > Authentication token**):

   a. Add an authentication token to be used for the OData connection.

   b. Copy the authentication token to the clipboard.

For more information, see the *ChangePoint Administration Guide* or online help.

2. Open Power BI, and click **Get data > OData feed**.

3. In the **OData feed** dialog, select **Advanced** and enter the OData URL.

4. Select the **Include open type columns** check box.

5. Click **OK**.

6. In the next window, select **Basic**.

7. In the **User name** field, paste the authentication token.

8. Leave the **Password** field blank.

9. In **Select which level to apply these settings to** field, select the specific data set URL that you entered on the previous window.

   Tip: To avoid having to enter the token every time you change the data set, select the highest level (least specific) URL.

10. Click **Connect**.

11. Click **Transform Data**.

12. To view the imported data:

    a. Click the expand icon in the **More Columns** column heading.

    b. Select the **All Columns** check box. If all columns are not visible, click **Load more**.

    c. Click **OK**. The data set is loaded.

About creating and configuring an archive database

For more information on archive management and archive jobs, see the *ChangePoint Administration Guide*.

Before entities can be archived in ChangePoint, you must configure an archive database. The archive database does not have to be on the same server as the source database; however, you must configure the archive database by running the GenerateEmptyArcDestDB.dtsx on the server where the source database is located. This .dtsx package only needs to be run once.

   Warning: The GenerateEmptyArcDestDB.dtsx file drops the existing archive database (if any) and recreates it. You are responsible for backing up existing databases on the archive server before running the .dtsx file.

The minimum recommended size for the archiving processing on the source database is the *greater* of the following amounts:

- 10 GB, with an auto-growth rate of 10%

- three times the amount of data to be archived, with an auto-growth rate of 10%

This space is required for the transaction log of the Archive Aged Entities job.

Creating a new archive database

1. On the source database server, install or upgrade to the current ChangePoint version. SQL Server Management Studio and Integration Service must be installed on the machine where the Data Archiving folder is copied to.

2. Copy the Data Archiving folder and its contents from the ChangePoint product media:

   `\Changepoint\Manual Install\Data Archiving`

   to the the following folder on the database server:

   `C:\Program Files\Changepoint\Changepoint\Data Archiving`

   Note: Because this path is hard-coded in some of the required setup files, it is strongly recommended that you use this path. However, if you must use a different path, see "Changing the default location of the data archiving folder" on page 225.

3. Update the following file with the database information for the source production server and the destination archive server:

   `C:\Program Files\Changepoint\Changepoint\Data Archiving\Data Archiving.ini`

   For example:

```
[CPSQLServer]
ConnectionString=server=ServerName;database=Changepoint;uid=USERID;pwd=PASSWORD;

[ARCSQLServer]
ConnectionString=server=ServerName;database=Changepoint;uid=USERID;pwd=PASSWORD;
```

   Note: The connection settings for generating a new archive database are not encrypted.

4. Double-click the following file:

`C:\Program Files\Changepoint\Changepoint\Data Archiving\GenerateEmptyArcDestDB.dtsx`

   The **Execute Package Utility** dialog opens.

5. Do the following:

a. Click the **Connection Managers** page.

b. Select the check boxes for the Data Archiving.ini file and the GenerateEmptyArcDestDB.dtsx.log file.

c. Change the **Connection String** values for the selected files to the required path.

6. Click **Execute**.

   On successful completion, an empty archive database is created.

7. On completion, examine the following log file for any errors:

   ```
   C:\Program Files\Changepoint\Changepoint\Data Archiving\
   GenerateEmptyArcDestDB.dtsx.log
   ```

   Common errors are incorrect settings in the Data Archiving.ini file, and insufficient space.

8. From the ChangePoint product media, copy the files from the `\Manual Install\Upgrade` folder to a temp folder.

9. Remove the read-only attribute on the copied files, if set.

10. Import the database migration DLL:

    a. Run the SQL import utility: `SQLImport.exe`. The **ChangePoint SQL Update Utility** dialog box appears.

    b. Complete the fields as follows:

       • **Migration File** field – browse for and select **Changepoint.DatabaseServices.DBMigrations_CP2021_GA.dll**.
       • **SQL Server** field– name of the ChangePoint database server.
       • **Database** field – name of the ChangePoint database.
       • **Login ID** field – SQL account used to give the ChangePoint applications access to the database.
       • **Password** field – password for the SQL account.

11. Repeat the previous step for **Changepoint.DatabaseServices.DBMigrations.dll**.

Configuring the archive database

If you have a website set up to access the archive database, execute the following commands against the archiving database:

```
exec DBM_SetupCPTempDB
exec DBM_SetupCPExtended
```

```
exec DBM_EnableSqlDependency (with the user used in the Web.config files)
```

Changing the default location of the data archiving folder

It is recommended that you use the default path (`C:\Program Files\Changepoint\Changepoint\Data Archiving`) as the path for the Data Archiving folder on the source database server. However, if you must use a different path, the following are the changes that need to be made on the source database server to configure the path.

1. In SQL Server Management Studio, connect to the source database server.

2. In the **Object Explorer** tree view, expand:

    ServerName > SQL Server Agent > Jobs

3. Right-click the **Archive Aged Entities** job and select **Properties**.

    The **Job Properties** - **Archive Aged Entities** dialog displays.

4. Select the **Steps** page and double-click the **Delete DTSX Log** step.

    The **Job Step Properties** - **Delete DTSX Log** dialog displays.

5. In the **Command** field on the **General** page, replace the argument of the DEL command with the required path and click **OK**.

6. Double-click the **Run Archive DTSX** step.

    The **Job Step Properties** - **Run Archive DTSX** dialog displays.

7. On the **General** page, do the following:

    a. Click the **General** tab.

    b. In the **Package** field, select Data Archiving.dtsx.

8. Do the following:

    a. Click the **Data sources** tab.

    b. Select the check boxes for the Data Archive.dtsx.log and Data Archive.ini files.

    c. Change the Connection String values for the selected files to the required path.

    d. Click **OK**.

9. Click **OK**.

Setting up websites on the archive database

You can set up new archive websites or upgrade existing archive websites to point to the archive database and run reports from there. Use the InstallShield Wizard and when prompted for details, enter the details for the archive websites instead of the standard ChangePoint websites.

After running the InstallShield Wizard, use the Login Settings utility to configure the connection settings to the archive database, using the following configuration files:

- Global.asa for the archive ChangePoint website.

- Global.asa for the archive ChangePoint Administration website.

- WebAPI\web.config file

- WebSocket\web.config file

Creating a custom form

You can create a custom form by doing the following.

1. In Infiniti Manage:

   a. Create the form project.

   b. Configure the form project to use ChangePoint data.

   c. To create a form that creates or updates entities, configure the form project to push and pull ChangePoint data.

2. Make the form available to resources in ChangePoint. In ChangePoint Administration, create the **Actions** menu subheader and submenu item to make the form available to users in ChangePoint.

Configuring a form project to push and pull ChangePoint data

To enable a form project to push data to and pull data from ChangePoint, you must add three label questions to the form project in Infiniti Manage. The answer to the questions are parameters that are populated at run time and provide the information that is required for authentication and handshaking between Infiniti Launch and ChangePoint.

Question	Answer	Save by unique label
Session ID	Session ID	sno
Resource ID	Resource ID	rid
Entity ID	Entity ID	cpguid

1. In ChangePoint, click **Intelligent Forms > Manage**.

2. Click the **Projects** tab, and then select the project.

3. Add a question for each of the following IDs. Enter the same ID text for both the question and the answer:

   - Session ID

   - Resource ID

   - Entity ID

4. For each of the questions, do the following:

   a. Expand the question and then select the answer.

   b. In the **Properties** tab, expand the **Answer File Properties** section.

   c. Select the **Save to answer file** check box.

   d. Click the **Save by unique label** option.

   e. In the text field, enter the text as follows:

      - For Session ID, enter sno
      - For Resource ID, enter rid
      - For Entity ID, enter cpguid

About creating form projects that create or update entities

You can create an intelligent form that creates an entity record or updates an existing entity record. For example, you can create a form that guides resources through the process of creating or updating a request record.

You create a form project in Infiniti Manage (**Infiniti Manage > Design**), where there is a default set of ChangePoint actions for creating and updating each of the main entities. The

actions include the standard fields and configurable fields for the entity. For each field you can specify a fixed value or a reference to an answer value.

You add the actions to the final page in a forms project, and the actions are triggered when the form is submitted. When the forms project is complete, you can configure it to be used in ChangePoint.

Adding an Intelligent Forms form to the Actions menu

To make a forms project available to resources in ChangePoint, you must create a submenu header and submenu item for it to appear in the **Actions** menu.

> **Note:** The following instructions are specific to creating a submenu header and submenu item for an Intelligent Forms form.

1. In ChangePoint Administration, create the submenu header (**User Interface > Actions Menu Integration**).

2. From the submenu header, create the submenu item. In the **Parameter** field, you must enter the ID of the form project, which you obtain from the initial view of the form project in Infiniti Manage.

3. In the **Access control** section, you must restrict access to the form by security feature as follows:

   • If the form creates or updates an entity record, restrict access to the **Access Forms Generation** security feature that is in the **Intelligent Forms** category.

   • If the form creates a document, restrict access to the **Access Document Generation** security feature

4. In **User setup**, assign the security feature to each of the resources who require access to the form.

Adding logos for invoices/cross charges

Before a logo can be added to invoices for a billing office or cross charges for a cost structure, the image file for the logo must be placed in the `C:\Changepoint\Images\` folder on the ChangePoint web server.

Advise users that when they enter the path to the logo in ChangePoint Administration, they must exclude the default folder. For example, if the image file is located at:

`C:\Changepoint\Images\invoicelogo.jpg`

Users would enter:

```
/Images/invoicelogo.jpg
```

Adding a custom invoice/cross charge format

Before a custom invoice/cross charge format can be set up in ChangePoint Administration, the format must be created and then placed under `<cp_root>`.

1. Create the custom invoice/cross charge format in an ASP file.

2. Place the ASP file in the `<cp_root>\core\report` folder or another location under `<cp_ root>`.

3. Advise users that when they enter the path to the logo in ChangePoint Administration, they must exclude `<cp_root>`.

Adding a custom ASP report

Before a custom ASP report can be set up in ChangePoint Administration, you must add the report file to the ChangePoint web server.

As a best practice, add a `Custom` folder to the `Changepoint/Core/Report/` path for storing custom reports.

Advise users that when they specify the report URL in ChangePoint Administration, they must leave out the ChangePoint domain, but include the file name, for example: `Core\Report\Custom\MyReport.asp`.

Changing printers for batch printing

If you add or remove printers on the web server, you will likely need to reconfigure batch printing.

1. Run the htmlprint.exe file in the BatchPrint directory on the web server.

2. Make the necessary changes to the values of the PrintServername keys in the PrintInvoices.exe.config files.

3. In ChangePoint Administration, make the necessary changes to the following workgroup fields:

    *   **Print Server Name** field

    *   **Default Printer** field

For more information, see "Configuring batch printing" on page 146.

About switching between SA and PPM modes

ChangePoint runs in one of two modes: ChangePoint PPM (Project Portfolio Management) and ChangePoint SA (Services Automation). The mode is specified during installation, but you can switch modes after installation.

Database tables modified by the UpdateSystemDefaults stored procedure

For reference, the following is a list of the database tables that are modified when you run the UpdateSystemDefaults stored procedure.

```
AccountType
AutoNumberingSetup
CategoryDescription
Chart
ContactType
ContractType
CriteriaType
Dashboard
DialogDefault
Email
EmailParameters
ExchangeApplied
ExpenseCategory
ExpenseGLACenter
ExpPubTopic
FeatureDescription
GlobalWorkgroup
HelpDesk
InvoiceFormats
IPICategoryType
IPIMetricCalc
IPIMetricType
KMCategory
LineOfBusiness
LockType
OpportunityType
Report
ReportCategoryDescription
ReportDefinitionDescription
RequestBillingType
RequestStatus
RequestType
ResourceRequestType
ResourcesRequestInitiateLevel
```

```
RevenueTypeGLA
Role
SalesStatus
Section
SectionItem
SurveyTemplateS
SurveyTriggerType
TitleDefinitionDescription
Version
WorkflowEntity
WorkflowParticipants
WriteOffReasons
```

Switching between ChangePoint PSA and PPM (PSO mode and ITD mode)

If you installed one mode but later decide to switch to the other mode, you can do this by running a stored procedure and changing the appropriate configuration settings.

1. Open Microsoft SQL Server Management Studio and connect to the ChangePoint database using the sa account.

2. Run the UpdateSystemDefaults stored procedure using the ITDFlag value to set the mode:

   - To switch to PSA mode:

     ```
     exec UpdateSystemDefaults @ITDFlag = 0
     ```
   - To switch to PPM mode:

     ```
     exec UpdateSystemDefaults @ITDFlag = 1
     ```

3. In the Global.asa file, do the following:

   - For PSA, set CompanyProfile to "PSO"

   - For PPM, set CompanyProfile to "ITD"

4. In the Web.config file for each application (ChangePoint, WebAPI, etc.) do the following:

   - For PSA, set CompanyProfile to "PSO"

   - For PPM, set CompanyProfile to "ITD"

Running both ChangePoint SA and PPM websites on the same database

You can run both SA and PPM websites using the same ChangePoint database.

1. Start with a **PSO** mode installation.

2. Run the InstallShield Wizard to create another set of ChangePoint websites. When prompted, select the **Websites only** setup type, and select the **ITD** mode.

   For more information, see "Installing multiple ChangePoint instances" on page 26.

3. Distribute the URLs for the SA and PPM websites to your users according to the version that they require.

   Note: Most terms such as field and dialog box names in the ChangePoint websites display the correct values according to the specified mode. However, some terms (for example, report names, feature names, and drop-down values in some lists) may not match the ITDFlag setting.

ASP-based reports that support DSN

The ASP reports that can use a separate report server are:

- All Customers/All Clients

- Assigned Features by Resource

- Campaign Profitability

- Competitors by Frequency

- Customer Radar

- Expense Reports Approved By Me

- Expense Reports by Resource

- Expense Reports by Status

- Invoice/Cross Charge Details with Net Write-offs

- Invoiced/Cross Charged Hours by Resource

- List of AllContracts by Customer/Initiatives by Client

- Responsibility By Resource

- My Contacts

- My Expense Reports

- My Knowledge Items

- My Tasks

- Unbilled/Uncharged Time and Expenses

- Personal Vacation Time

- Project Progress All

- Project Summary by Resource

- Projects by Status and by Customer

- Projects by Status and by Project Manager

- Resources by Task

- Resource History

- Resources By Approver

- Resources by Function

- Task Status Compliance

- Tasks in Progress or Scheduled to Start

- Tasks Scheduled to Finish in Two Weeks

- Time and Expense by Billing Office/Cost Center

- Time and Expense by Invoice/Cross Charge Number

- Time and Expenses by Resource

- Time Submission Conformance

- Vacation Tracking

- Weekly Time Sheet

- Work Performed and Invoiced

- Workgroup Record History

Setting up access to ChangePoint portlets and reports in third-party portals

ChangePoint portlets and other specifically-enabled pages can be rendered directly in a browser or in third-party portal solutions such as IBM WebSphere, CA CleverPath, and Microsoft SharePoint, using a portlet-specific URL that is based on a common entry point.

To access portlets and reports from outside ChangePoint, use the common entry point, and pass additional parameters as required in the querystring:

The URL format is:

```
http://<entrypoint>&portletid=<PortletId>&params=<Params> …&url=<URL>
```

where:

- entrypoint – <ChangePointURL:port>/core/portlet.aspx?ui=p

  - ChangePointURL:port – the URL and port number of your ChangePoint website

- PortletId (required) – Id of the portlet to display (see list below)

- Params (optional) – Additional querystring parameters separated by ";"

- URL (optional) – Custom portlet URL

Notes

- If the website uses SSL, use the https protocol in place of http.

- If the website uses application authentication, portlet users are prompted for a user name and password for access to the portlet.

- If the website uses integrated Windows authentication, or one of the other Single Sign On (SSO) methods supported by ChangePoint, portlets are displayed to authenticated users without requiring further sign on.

- Links from a portlet to other areas of ChangePoint are not supported. For example, if you display the **My Reminders** portlet, then click on one of the links within the portlet (for example, "You have time to approve"), the link target might not render or function correctly.

- You are responsible for ensuring that the custom page renders correctly using UI=P.

ChangePoint portlet names and IDs

Portlet name	PortletId
Custom portlet url	*Custom See notes below.
Campaign/ Source	
Source/ Campaign Results	dshCampaign
Upcoming Sources / Campaigns	dshUpcomingCampaign
Client/ Customer & Contact	
Find Person	dshFindPerson
Contract/ Initiative	
Contract/ Initiative Warnings	dshEngagement
Expense	
Expense	Expense
ExpenseReport	ExpenseReport
Financial Management	
Financial Reminders	dshFinancialReminder
Intelligent Forms	
Intelligent form	iFORM See notes and examples, below.
Invoice/ Cross Charge	
Approved Cross Charges / Invoices	dshApprovedInvoice
Cross Charges / Invoices Pending Approval	dshPendingInvoice
Draft Cross Charges / Invoices	dshDraftInvoice

Portlet name	PortletId
Rejected Cross Charges / Invoices	dshRejectedInvoice
Knowledge Management	
Create Knowledge item	dcSubmitKM
Knowledge Management	dshKM
Opportunity/ Candidate	
Active Candidates / Opportunities	dshActiveOpportunity
Approved Candidates / Opportunities	dshOpportunityWin
Candidate / Opportunity Decision Summary	dshOpportunityOutcome
Candidate / Opportunity Decisions	dshCompetitiveOutcome
Candidate / Opportunity Rollups	dshOpportunityRollup
Personal portlets	
My Favorite Reports	dshFavoriteReport
My Links	dshMyLink
My Performance	dshMyPerformanceChart
My Reminders	dshReminder
My Utilization	dshMyUtilization
Requests Assigned To Me	dshRequestToMe
Requests Initiated By Me	dshRequestByMe
Performance Management	
Performance Management	dshPerformanceChart

Portlet name	PortletId
Project Management	
Project Status by Project Manager Report	rpProjectByStatus_PM
Project planning worksheet (Project Worksheet)	PPW See notes and examples, below.
Reporting	
ChangePoint Analytics reports	Cognos See notes and examples, below.
Requests	
Create request	dcrequest See notes below.
Edit Request	dcrequest See notes below.
Requests Summary	dshRequestSummary
Resource Management	
Find Person	dshFindPerson
Resource Planner)	RSW See notes and examples, below.
Underutilized Resources	dshUnderutilizedResource
Workgroup Utilization	dshWkgpUtilization
Surveys	
Survey Management	dshSurveyManagement
Timesheet	
Timesheet	Timesheet

Examples

My reminders:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=dshReminder
```

Create Request:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=dcrequest
```

Notes

Custom

To use a custom url:

- PortletId = "*Custom"

- Url = ~/Custom/Reports/{*your custom report here*}.asp

Example:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=*custom&url=~/Cu
stom/Reports/rpCustomRequestReport.asp
```

ChangePoint Analytics reports

ReportID is required.

- PortletID=Cognos

- Params = reportid=<ReportID>

  You can find the *ReportId* using ChangePoint Administration (see "Using ChangePoint Administration to get Report IDs" on page 240). For reports that are not in portlet format, you can use an SQL query or IE properties.

Example:

```
http://<ChangepointUrl:port>/core/portlet.aspx?ui=p&portletid=Cognos&Params=re
portid=<ReportId>
```

Intelligent Forms

- Portlet ID = iFORM

- Params = id=<Intelligent form ID>

Example:

```
http://mylocalweb/core/portlet.aspx?ui=p&portletid=iFORM&Params=id=<Intelligen
t Form Id>
```

Or if you need to pass in a ChangePoint Entity ID then:

```
http://mylocalweb/core/portlet.aspx?ui=p&portletid=iFORM&Params=id=<Intelligen
t Form Id>;CPGUID=< EntityId>
```

Project Worksheet

Project ID is required.

- Portlet ID = PPW

- Params = ProjectId=<Project ID>

Example:

```
http://mylocalweb/core/portlet.aspx?ui=p&portletid=PPW&Params=ProjectId=<Proje
ctId>
```

Resource Planner

- Portletid=RSW

Example:

```
http://mylocalweb/core/portlet.aspx?ui=p&portletid=RSW
```

Requests (dcrequest)

Create Request with a tabbed layout (default is inline):

If no template is specified, the default template is used. See "Create a request using a template" on page 239.

- PortletId = dcrequest

- Params = layout=tabbed

Example:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=
dcrequest&Params=layout=tabbed
```

Create a request using a template

- PortletId = dcrequest

- Params = templateid=<TemplateId>

You can find the TemplateId using a SQL query or IE properties.

Example:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=
dcrequest&Params=templateid=ff7e7079-9e0b-4856-9d7c-f9721437f737
```

Edit a request

RequestId is required

- PortletId = dcrequest

- Params = action=edit; reqnum=<request number>

Example:

```
http://<ChangepointURL:port>/core/portlet.aspx?ui=p&portletid=
dcrequest&Params=action=edit;reqnum=SR-2012-00157
```

Edit a request using a template

RequestId is required.

- PortletId = dcrequest

- Params = action=edit; reqnum=<request number>;selectedtemplateid=<EditTemplateId>

You can find the EditTemplateId using a SQL query or IE properties.

Example:

```
http://<ChangepointURL:port>/core/
portlet.aspx?ui=p&portletid=dcrequest&Params=action=edit;reqnum=SR-2012-
00157;selectedtemplateid= ff7e7079-9e0b-4856-9d7c-f9721437f773
```

Using ChangePoint Administration to get Report IDs

To get a report ID:

1. In ChangePoint Administration, go to **User Interface > Portlet Management**.

2. In the **Category** list, select **All portlets**.

3. From the list of portlets, select the report.

4. In the **URL** field, copy the reportid=<*ReportId*> from the end of the URL.

Index