



Upgrade Guide

Changepoint 2017 SP1

Copyright © 2018 Changepoint Canada ULC. All rights reserved.

U.S. GOVERNMENT RIGHTS-Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in Changepoint Canada ULC license agreement and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

This product contains confidential information and trade secrets of Changepoint Canada ULC. Disclosure is prohibited without the prior express written permission of Changepoint Canada ULC. Use of this product is subject to the terms and conditions of the user's License Agreement with Changepoint Canada ULC.

Documentation may only be reproduced by Licensee for internal use. The content of this document may not be altered, modified or changed without the express written consent of Changepoint Canada ULC. Changepoint Canada ULC may change the content specified herein at any time, with or without notice.

Contents

1. Upgrading to Changepoint 2017 SP1	7
About the service pack upgrade	7
Installing Changepoint 2017 SP1	7
Requirements for the service pack upgrade	7
Product media for the service pack upgrade	8
Changepoint documentation for the service pack upgrade	9
Preparing for the service pack upgrade	9
Filepath conventions	9
Assess the impact on customizations and product extensions	10
Perform backups	10
Upgrade in a test environment first	10
Pre-upgrade steps	11
Intelligent Forms installation parameters	13
Upgrading the Changepoint servers using the installer	14
Upgrading the Changepoint database server manually	15
Completing the service pack upgrade	16
Completing the service pack upgrade on the database server	17
Configuring the CPEffectiveDates scheduled job for access to the Redis cache	17
Completing the installation of Intelligent Forms	18
Running the script to prevent time entry on summary tasks	18
Completing the service pack upgrade on the web servers	19
Configuring Single Sign-on using WS-Federation (ADFS)	21
Upgrading Changepoint Windows services	22
Upgrading the online help	24
Setting up the Changepoint Mobile app	24
Upgrading the Changepoint API	25
Upgrading the Integration Framework	26
Upgrading the toolkits	26
Upgrading the Transport Tool	26
Upgrading the archive database and websites	27
Creating a new archive database after upgrading	27
Configuring the archive database	28
Verifying component versions	28
2. Upgrading Cognos	29
Upgrading to Cognos Analytics	29

Manually uninstalling Cognos	30
3. Installing and Configuring Cognos Analytics	33
Preparing to install Cognos Analytics	33
About roles and feature mapping between Cognos and Changepoint	33
Installation parameters for Cognos Analytics	34
Overview of Cognos Analytics installation and configuration	35
Stage 1. Creating the Cognos Content Store database	35
Stage 2. Installing the Cognos Application Tier	36
Stage 3. Configuring the Cognos Application Tier	37
Stage 4. Installing the Cognos web components	40
Stage 5. Configuring Changepoint server integration for Cognos Analytics	41
Stage 6. Assigning Changepoint security features for access to Cognos functionality	41
Stage 7. Importing the Changepoint metadata package	42
Stage 8. Setting up the data source for IBM Cognos Analytics	43
Stage 9. Setting the security settings in Cognos	45
About the Changepoint-Cognos Sync Utility	45
About using the Sync Utility with multiple Cognos Analytics instances	47
Upgrading the Sync Utility	47
Installing the Sync Utility	47
Importing the base data model	49
Adding customized field labels and configurable fields to the data model	49
Reverting to a previous version of the base data model	50
4. Installing additional instances of Cognos Application Tier and web components	51
About installing additional instances of Cognos Application Tier and web components	51
Installation parameters for additional instances of Cognos Application Tier and web components	51
Installing an additional Cognos Application Tier instance	52
Configuring an additional Cognos Application Tier component	53
Installing additional Cognos web component instances on a single server	56
Installing an additional Cognos web component	56
5. Porting the Changepoint database	59
Overview	59
Porting the Changepoint database	59
After porting the Changepoint database	60
Porting an archive database	61
6. Troubleshooting the service pack upgrade	63
Troubleshooting the upgrade	63

Execution timeout error in RSW.	63
Changepoint Mail Service error in event log	63
Access to the path '...\RP-STC_ADFS\Web.config' is denied" error when signing into Changepoint	63
Cognos report in a portal will not load	63
HTTP 403 errorProject Planning Worksheet fails to savePreferred resources cannot be edited	63
Errors in the Changepoint Installer.log	64
Server error in browser	64
Project planning worksheet does not loadError when accessing Manage Preferred Resources"Access to registry key 'Global' is denied" in Changepoint event log	65

1. Upgrading to Changepoint 2017 SP1

About the service pack upgrade

You can upgrade to Changepoint 2017 SP1 from Changepoint 2017 only.

The upgrade to Changepoint 2017 SP1 replaces *all website files*, but the Changepoint websites and configuration files (Web.config and Global.asa) are retained as-is.

The upgrade includes:

1. Ensuring that you meet all of the requirements.
2. Preparing for the upgrade.
3. Upgrading the Changepoint web and database servers.
4. Upgrading the optional Changepoint components.

Installing Changepoint 2017 SP1

You can do a new install of Changepoint2017 SP1.

1. Install Changepoint using the Changepoint2017 SP1 media, but following the instructions in the *Changepoint 2017 Installation Guide*.

Note: If you are installing the Changepoint Exchange Synchronization Service, and the service connection point is not configured in the environment, you must set `EnableScpLookup` to `false` in the service configuration file.

2. After installing, you must review the "Completing the service pack upgrade" on page 16. in this guide for additional configuration that is required for this service pack.

Requirements for the service pack upgrade

Obtain the latest patches

Check for general patches for the service pack in either of the following locations:

- *CP 2017 SP1 Patches* section in the [Changepoint Product Help Center](#)
- *2017 SP1 Release Notes and Patches* team folder, which is accessible through Client Portal

Required hardware and software

For details, see the *Changepoint 2017 SP1 Hardware Recommendations Guide* and the *Changepoint 2017 SP1 Product Architecture and Technology Matrix* document.

Note: You must download some third-party software from the vendor websites.

Required skills

To upgrade Changepoint, you must be familiar with the following software:

- Microsoft SQL Server
- Microsoft Windows Server
- Microsoft Internet Information Services (IIS)
- .NET
- Microsoft Windows PowerShell (for SSO configuration scripts)

If you require assistance with implementing Changepoint, contact your Changepoint customer representative.

Required accounts and permissions

You need credentials for the following accounts on each server:

- All servers – local or domain administrator account
- Database server:
 - For upgrading the Changepoint database :
 - the SQL account with “dbo” schema for databases (Changepoint, tempdb, master, MSDB)
 - the “sysadmin” server role. The MSDB access is required for scheduled job updates.
 - For configuring connections to the Changepoint database – the SQL account used to give the Changepoint applications access to the Changepoint database.

Product media for the service pack upgrade

Changepoint 2017 SP1 is available on the following product media:

- Changepoint 2017 SP1 – Used to upgrade the Changepoint websites, database, and online help. Referred to in this document as the Changepoint media.

- Changepoint 2017 SP1 COM and Web Services API
- Changepoint 2017 SP1 Cognos Analytics
- Changepoint 2017 SP1 Integration Framework
- Changepoint2017 SP1 Salesforce.com Integration Toolkit
- Changepoint2017 SP1 Transport Tool

Changepoint documentation for the service pack upgrade

This section lists the documentation that is referenced in this document by the team folder where the documentation is located. You access the team folders through Client Portal.

2017 SP1 Release Notes and Patches team folder

Changepoint 2017 SP1 Product Architecture and Technology Matrix

Changepoint 2017 SP1 Hardware Recommendations Guide

Changepoint 2017 SP1 Release Notes

CP2017 – CP 2017 SP1 Differences

2017 Release Notes and Patches team folder

Changepoint 2017 Installation Guide

Preparing for the service pack 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.

Filepath conventions

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

- <cp_root> – The root path of the Changepoint installation. The default path is:

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

- <cp_common> – The root location for common Changepoint utilities, such as the Login Settings utility. The default path is:

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

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 2017 SP1 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 pages or new pages added to the websites must be reapplied after the upgrade.

All customization 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 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 59. 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 2017 SP1 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)

Pre-upgrade steps

30 to 35 days before upgrading

(Web server) Change the content expiry of the Enterprise folders to expire in 1 day:

```
\images  
\css  
\Help  
\External\Help  
\External\images  
\Js
```

Changing content expiry settings and enabling caching of static files

You set content expiry in IIS Manager by changing the expiry options of the HTTP Response Headers for the Enterprise websites.

1. In IIS Manager, expand **servername** > **Sites** > **Enterprise**.
2. Select the folder.
3. In the **Home** screen, double-click the **HTTP Response Headers** icon.
4. Select **Actions** > **Set Common Headers**.
5. Change the settings as required.
6. Click **OK**.

One to two weeks before upgrading

1. Send an email message to users notifying them about the upgrade.

2. If you plan to install Intelligent Forms for the first time, determine the values for the installation parameters. For more information, see "Intelligent Forms installation parameters" on page 13.

One day before upgrading

(Web server) The day before the upgrade, change the content expiry setting to **Expire Immediately** for the Enterprise folders. For more information, see the "Changing content expiry settings and enabling caching of static files" section on page 11.

Changing this setting removes the need for users to clear their browser cache before signing into Changepoint after the upgrade.

Immediately before upgrading

1. Apply the applicable pre-upgrade patches according to the instructions in the patch release notes.
2. 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 Changepoint 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. For more information, see the "Changing content expiry settings and enabling caching of static files" section on page 11.
 - d. In IIS Manager, stop the Changepoint websites (Changepoint and Report Designer) that you are upgrading.
4. (Database server) Do the following:
 - a. Stop all scheduled jobs from running while you are performing the upgrade.
 - b. It is recommended that you drop custom full-text catalogs before the upgrade. You must recreate the catalogs after the upgrade is complete.
 - c. Back up the Changepoint database.
 - d. If required, port the Changepoint database.

e. Back up the Cognos content store 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
- transformation files in the Changepoint Data Mapper Service\Configuration folder
- `CPEXportPublishingService.exe.config` file from the Changepoint Export Publishing Service folder.

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	

Information needed	Notes	Your installation value
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		
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	

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 11.
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 13.
 - If you are upgrading Intelligent Forms:
 - only the website is updated (there is no change to the Infiniti database)
 - 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 service pack upgrade" section on page 16.

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. 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.
5. 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 18.01.075.000 completed
Configuration of CPTempDB database (Changepoint_CPTempDB) completed successfully
```

Completing the service pack upgrade

After you have upgraded the database and web servers, you must complete the upgrade by applying patches, restoring customizations, running scheduled jobs, and so on. For more information see:

1. "Completing the service pack upgrade on the database server" on page 17.
2. "Completing the service pack upgrade on the web servers" on page 19.
3. "Completing the installation of Intelligent Forms" on page 18.
4. "Upgrading Changepoint Windows services" on page 22.
5. Upgrade the following optional components as required:
 - "Upgrading the online help" on page 24
 - "Setting up the Changepoint Mobile app" on page 24
 - "Upgrading the Changepoint API" on page 25
 - "Upgrading the Integration Framework" on page 26
 - "Upgrading to Cognos Analytics" on page 29
 - "Upgrading the toolkits" on page 26
 - "Upgrading the archive database and websites" on page 27
6. Advise users that they must delete their browser history before signing into Changepoint for the first time after the upgrade.

Completing the service pack upgrade on the database server

1. Apply the applicable patches for the service pack, according to the instructions in the patch release notes.
2. Restore and test customizations (custom SQL code, accelerators, and extensions).
3. 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 17.
4. To prevent time entry on summary tasks, see "Running the script to prevent time entry on summary tasks" on the next page.
5. To optimize performance, follow the performance optimization recommendations in the *Changepoint 2017 Installation Guide*.
6. 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.
7. 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. For more information about scheduled jobs, see the *Changepoint 2017 Installation Guide*.

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.

8. If you dropped custom full-text catalogs before the upgrade, recreate the catalogs.
9. 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

For more information about the following steps, see the *Changepoint 2017 Installation Guide*.

1. Configure the database connection settings for Intelligent Forms according to the instructions in the "Configuring Database Connection Settings" chapter.
2. Configure Intelligent Forms according to the instructions in the "Configuring Intelligent Forms" section.

Note: Skip the first step. It is not necessary to apply the patch.

Running the script to prevent time entry on summary tasks

The default behavior for Changepoint 2017 SP1 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 company) 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 service pack upgrade on the web servers

1. Apply the applicable patches according to the instructions in the patch release notes.
2. Restore and test customizations (asp pages and extensions).
3. For optimum performance, the resource scheduling worksheet (RSW) has been set to a default maximum of 300 demand items that can be displayed. To increase this limit, change the value in the `WebAPI\Web.config` file for the following setting:

```
<add key="ResourceSchedulingWorksheet.DemandItemLimit" value="300" />
```

Note: 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 RSW.

4. To hide the resource management worksheet (RMW) or resource scheduling worksheet (RSW) so they are not available from the Changepoint user interface, change the settings in the `Enterprise\Web.config` file.

- To hide the resource management worksheet (RMW), set the value for the following setting to "false":

```
<add key="ResourceManagementWorksheet.EnableManagementWorksheet" value="false" />
```

- To hide the resource scheduling worksheet RSW, set the value for the following setting to "false":

```
<add key="ResourceSchedulingWorksheet.EnableSchedulingWorksheet" value="false" />
```

5. If you implemented single sign-on for Changepoint, and either Intelligent Forms or the Changepoint Integration Framework (Salesforce.com), you must reconfigure the `<cp_root>\API\CP Web Services\Web.config` file. For the previous settings, refer to the copy of the file that you backed up before upgrading.
6. If your environment is configured for single sign-on using WS-Federation (ADFS), verify that the **IIS_IUSRS** group has been granted **Modify** access to the `Enterprise\RP-STS_ADFS\Web.config` file. For information about granting the access, see "Configuring Single Sign-on using WS-Federation (ADFS)" on page 21.
7. To optimize performance, follow the performance optimization recommendations in the *Changepoint 2017 Installation Guide*.
8. 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 63.

9. Restart the Changepoint website.
10. 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**).
11. Restart all websites and check that you can sign in to each website.
12. Restore the content expiry settings of the Changepoint folders to the values before the upgrade:

```
\images
\css
\Help
\External\Help
\External\images
\Js
```

For more information, see the "Changing content expiry settings and enabling caching of static files" section on page 11.

13. Enable IIS caching of static files.
14. Restart IIS.
15. Restart the Redis cache service.

Configuring Single Sign-on using WS-Federation (ADFS)

There is a PowerShell script that must be run before you configure SSO using WS-Federation (ADFS). The upgrade clears the previous configuration in error, and this script reestablishes the previous configuration.

1. From the Changepoint product FTP site, at the root of the Changepoint folder, download the `Fix_ADFS_web_config_post_18_01_upgrade.ps1` script .
2. Copy the script to a location on the web server.
3. Start Windows PowerShell with the **Run as Administrator** option, and enable **running unsigned scripts** if required.
4. From the location on the web server, execute:

```
./ Fix_ADFS_web_config_post_18_01_upgrade.ps1
```
5. Follow the prompts to select the location of the Changepoint Enterprise website.

Grant the **IIS_IUSRS** group **Modify** access to the `Enterprise\RP-STIS_ADFS\Web.config` file.

1. Right-click the `Enterprise\RP-STIS_ADFS\Web.config` file, and then select **Properties**.
2. Click the **Security** tab, and then click **Edit**.
3. In the **Permissions** dialog box, click **Add**.
4. In the **Select Users, Computers, Service Accounts, or Groups** dialog box:
 - a. Click **Locations**.
 - b. Select the current local machine as the location (instead of the domain).
 - c. Click **OK**.
5. In the **Enter the object names to select** field, type: `IIS_IUSRS`.
6. Click **Check Names**. `IIS_IUSRS` is changed to `<local machine>IIS_IUSRS`.

7. Click **OK**.
8. In the **Groups or user names** field, click <local machine>\IIS_IUSRS.
9. In the **Permissions for <local machine>\IIS_IUSRS** section, select the **Allow** check box for **Modify** and then click **OK**.
10. Click **OK** to close the **Properties** dialog. Wait a moment before proceeding to allow for the security changes to be applied.

Upgrading Changepoint Windows services

The following standard Changepoint Windows services have been updated:

- Changepoint Email Notification Service
- Changepoint Exchange Synchronization Service
- Changepoint Mail Service
- Changepoint Report Prerender Service
- Changepoint Report Scheduler Service

The following Windows services for Integration Framework have been updated:

- Changepoint Data Mapper Service
- Changepoint Communication Dispatcher Service
- Changepoint Export Publishing Service

For more information about installing and configuring the Changepoint Windows services, see the *Changepoint 2017 Installation Guide*.

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 2017 SP1 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="" />
```

3. For the Changepoint Communication Dispatcher service:

- a. Copy the following key from the <appSettings> section of the backup configuration file, and replace the key in the <appSettings> section of the new configuration file:

```
< add key="Microsoft.ServiceBus.ConnectionString" ... />
```

- b. Add the following key to the < runtime > section of the new configuration file.

```
< AppContextSwitchOverrides
value="Switch.System.IdentityModel.DisableMultipleDNSEntriesInSANCertificate=true" />
```

4. For the Changepoint Data Mapper Service:

- a. Copy the following key from < appSettings > section of the backup configuration file, and then replace the key in the < appSettings > section of the new configuration file:

```
< add key="Microsoft.ServiceBus.ConnectionString" ... />
```

- b. Add the following key to the < runtime> section of the configuration file.

```
< AppContextSwitchOverrides
value="Switch.System.IdentityModel.DisableMultipleDNSEntriesInSANCertificate=true" />
```

5. For the Changepoint Export Publishing Service:

- a. In the < appSettings > section of the backup copy of the configuration file, copy the following key and replace the same key in the new configuration file.:

```
< add key="Microsoft.ServiceBus.ConnectionString" ... />
```

- b. In the < appSettings > section of the backup configuration file, copy the following key and then replace the same key in the new configuration file:

```
< add key="SQLSettings" ... />
```

- c. In the < appSettings > section of the new configuration file, delete the following key, which is redundant:

```
< add key="Microsoft.ServiceBus.ConnectionString" value="Endpoint=sb://[your
namespace].servicebus.windows.net; ... />
```

- d. Add the following key to the `< runtime>` section of the new configuration file.

```
< AppContextSwitchOverrides  
value="Switch.System.IdentityModel.DisableMultipleDNSEntriesInSANCertificate=true" />
```

Upgrading the online help

Install the online help files from the Changepoint 2017 SP1 media as documented in the *Changepoint 2017 Installation Guide*. It is not necessary to uninstall the previous help files.

There are no eLearning lessons available. .

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 2017 SP1 Product Architecture and Technology Matrix*.

1. Obtain the license from Changepoint Canada ULC 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 2017 SP1 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 2017 SP1 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 the Integration Framework

To upgrade the Integration Framework, you must upgrade the Windows services that were updated in this release. For more information, see "Upgrading Changepoint Windows services" on page 22

Upgrading a Salesforce.com integration

To upgrade a Salesforce.com integration, do the following:

1. Create a backup copy of the configuration files:

```
ExternalEndPoint\Web.config  
ExternalEndPoint\Configuration\Adapter.xml
```

2. On the SFDC Integration Toolkit media, copy the contents of the
Salesforce\ExternalEndPoint folder, and then paste the contents under the
ExternalEndpoint folder.

3. Move the backup copies of the configuration files back to the ExternalEndpoint folder.

Upgrading the toolkits

Upgrading the Transport Tool

To upgrade the Transport Tool, you must uninstall the previous version and then reinstall from the 2017 SP1 product media.

For more information, see the *Changepoint 2014 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. If the archiving solution is on a SQL Server 2016 environment:
 - a. Copy all files except the `Data Archiving.ini` file from the following folder on the Changepoint media:

`\Changepoint\Manual Install\Data Archiving`

Note: The `Data Archiving.ini` file contains the current configuration settings.

Paste the files into the `Data Archiving` folder on the archive environment.

3. If the archiving solution is on a SQL Server 2017 environment:
 - a. Obtain the 18.01.094 general patch.
 - b. Copy the `Data Archiving 2017.dtsx` and `GenerateEmptyArcDestDB 2017.dtsx` packages from the 18.01.094.000 general patch package.
 - c. Paste the files into the `Data Archiving` folder on the archive environment.

Creating a new archive database after upgrading

Follow this procedure to create an empty archive database to the patch level of the source database.

1. Create an empty archive database according to the instructions in the *Changepoint 2017 Installation Guide*.
2. From the Changepoint 2017 SP1 media, copy the files from the `\Manual Upgrade\Database\` folder to a temp folder.
3. Open the `SQLImport.exe.Config` file:
 - a. Set the value of the "VersionFrom" key to the same value that is set for the "VersionTo" key.
 - b. Search for and replace the following key:

```
< add key="FMExecOrder" value="--tag=PreMigration,--tag=CPScript,--tag=CPCode,
--tag=PostMigration"/>
```

with

```
< add key="FMExecOrder" value="--tag=CPArchiving,--tag=PostMigration"/>
```

4. Remove the read-only attribute on the copied files, if set.
5. Run the SQL import utility: `SQLImport.exe`. The **Changepoint SQL Update Utility** dialog box appears.
6. Complete the fields as follows:
 - a. **Migration File** field – browse for and select **Changepoint.DatabaseServices.DBMigrations.dll**.
 - b. **SQL Server** field– name of the Changepoint database server.
 - c. **Database** field – name of the Changepoint database.
 - d. **Login ID** field – SQL account used to give the Changepoint applications access to the database.
 - e. **Password** field – password for the SQL account

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 2017 SP1, the version for all components is: 18.01.075.000.

2. Upgrading Cognos

Upgrading to Cognos Analytics

You can upgrade to Cognos Analytics on the following Changepoint version only:

- Changepoint 2017

Upgrade notes for installing Cognos Analytics:

- Cognos Analytics 11 is a major release and requires a reinstall.
- The Cognos gateway server is no longer required. Only the Cognos application tier is required. The Changepoint installer removes the gateway server during the upgrade.

Upgrade notes for using Cognos Analytics:

- The Cognos Analytics 11 user interface is very different from the Cognos 10.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.
- Adding links from reports to Changepoint profile pages uses a different methodology for interactive reports, which are new in Cognos Analytics 11. Refer to the *Changepoint-Cognos Reference Guide* for more details.

Upgrading Cognos includes the following steps:

1. Upgrading Changepoint.
2. Backing up the content store database.

Note: The recommended method for backing up a content store database is to create a deployment archive by using IBM Cognos Administration. For more information, see [Creating a deployment archive](#) on the IBM Knowledge Center website

3. Backing up the Cognos startup configuration file (`cogstartup.xml`). The file is found under the `ibm\c10\configuration` folder. You might want to back up this file and other configuration files and use the configuration data with the new version.
4. Backing up the Cognos images folder. If the existing reports have images, back up the images folder: `C:\Program Files\ibm\cognos\c10\webcontent\samples\images`.
5. Installing Cognos Analytics. Perform the following steps:
 - "Stage 2. Installing the Cognos Application Tier" on page 36

- "Stage 3. Configuring the Cognos Application Tier" on page 37
 - "Stage 4. Installing the Cognos web components" on page 40
 - "Stage 5. Configuring Changepoint server integration for Cognos Analytics " on page 41
 - "Stage 6. Assigning Changepoint security features for access to Cognos functionality" on page 41
6. Copy the images from existing reports (that you backed up) to the images folder on the Cognos Application Tier server:


```
c:\Program Files\ibm\cognos\analytics\webcontent\bi\samples\images
```
 7. Remove the **Everyone** role from the following capabilities:
 - Data sets
 - Upload files
 - Web based modeling
 8. Ensure that the **Everyone** role has been removed from the Cognos System Administrators role.
 9. If Business Author licenses are to be granted full reporting capabilities, add the **Changepoint Query Users** role to the Cognos **Authors** role.
 10. By default, Cognos portlets and portals are opened inline in the Changepoint container. However, you can configure Cognos portlets and portals to open in a new browser window. In the `Enterprise\Web.config` file, set `Cognos.IE.LaunchPortletsInNewWindow` to "true."
 11. After you have verified that you do not require any files from the previous version, delete the Cognos IBM directory:


```
C:\Program Files\IBM\cognos\c10
```
 12. Upgrading the Changepoint-Cognos Sync Utility and importing the new base data model. For more information, see "About the Changepoint-Cognos Sync Utility " on page 45.
 13. Restarting the Cognos Application Tier server.

Manually uninstalling Cognos

You must uninstall Cognos Analytics 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\c10\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\c10
```


3. Installing and Configuring Cognos Analytics

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
Authors	Cognos Professional Author
Consumers	Base User License
Directory Administrators	Cognos Administrator
Portal Administrators	Cognos Administrator
Query Users	Cognos Business Author
Report Administrators	Cognos Professional Author
Server Administrators	Cognos Administrator
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	

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 35
- "Stage 2. Installing the Cognos Application Tier" on page 36
- "Stage 3. Configuring the Cognos Application Tier" on page 37
- "Stage 4. Installing the Cognos web components" on page 40
- "Stage 5. Configuring Changepoint server integration for Cognos Analytics " on page 41
- "Stage 6. Assigning Changepoint security features for access to Cognos functionality" on page 41
- "Stage 7. Importing the Changepoint metadata package" on page 42
- "Stage 8. Setting up the data source for IBM Cognos Analytics" on page 43
- "Stage 9. Setting the security settings in Cognos" on page 45

For information about installing the Changepoint-Cognos Sync Utility, see "About the Changepoint-Cognos Sync Utility " on page 45.

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 51.

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 51.

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.

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` as 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 34.
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, cogbootstrap.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), change localhost 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 35.
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 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, click the **Start**  button.
4. If the **IBM Cognos Configuration** dialog shows that the service could not be started but the details indicate the service has been started, do the following:
 - a. Close the **IBM Cognos Configuration** dialog box.
 - b. Click **Save** again in the configuration view.
 - c. Restart the IBM Cognos Analytics service.

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 to enable Cognos Analytics on the Changepoint website** and then follow the prompts.
5. Complete 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: 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 Cognos reporting functionality, you must assign the following Cognos-related features to resources or roles:

- **View Reports** feature – View Cognos reports and other Cognos content in the **Reports** tree view in Changepoint.
- **Cognos Business Author** feature and **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 > Analytics Portal**. The **IBM Cognos Analytics** portal appears.
3. Click **Manage**, then click **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**, then click **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**
 - b. Select all the **Content** check boxes.
 - c. In the **Report specification upgrade** option section, select **Keep the existing report specification versions**.
 - d. 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 > Analytics Portal**. The **IBM Cognos Analytics** portal appears.
3. Click **Manage**, then click **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** dialog box:
 - a. In the **Server name** field, enter the name of the database server.
 - b. In the **Database name** field, enter the name of the 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.
11. Complete the following fields in the **Specify the Microsoft SQL Server (JDBC) connection string** dialog box:
 - 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.

13. Click **Finish**.

The Changepoint data 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.

Optionally, you can grant Changepoint users the access rights to create their own portals in Cognos Workspace.

To remove the administrator role from Changepoint users

1. Sign in to Changepoint as Changepoint administrator.
2. Click **Analytics > Analytics Portal**. The **IBM Cognos Analytics** portal appears.
3. Click **Manage**, then click **Administration console**. The **IBM Cognos Administration** console appears.
4. Click **Security**, then click **Cognos**.
5. Scroll to the System Administrator role, and then click **More**.
6. Click **Set Members**, and select **Everyone**.
7. Click the **Remove** link.
8. Click **OK**.

About the Changepoint-Cognos Sync Utility

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

- you import a base data model that you received from Changepoint Canada ULC. 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 2017 SP1 Product Architecture and Technology Matrix* and the *Changepoint 2017 SP1 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-Cognos data model, 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, you must uninstall the previous release sync prerequisite and Sync Utility from the Windows Control Panel, and then install the current release version.

Installing the Sync Utility

By default, the Changepoint-Cognos Sync Utility is installed and configured for the PSA version of Changepoint. To configure the Sync Utility for Changepoint PPM, see step 11.

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. In the **Enterprise Website Server Name** field, enter the name of the Changepoint web server.
7. In the **Enterprise Port** field, enter the port used by the Changepoint website.
8. If the Changepoint website uses SSL, select the **SSL Enabled** check box.
9. Click **Next**, then click **Install**, then click **Finish**.
10. 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:

`<cp_common>\Cognos Client Tools\CognosClientTools.exe.config`

For more information, see Configuring database connection settings in the *Changepoint Installation Guide*.

A shortcut named **Changepoint Cognos Sync Utility** is added to the **Start** menu.
11. 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.
12. 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 PSA)
 - 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.

4. 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 Changepoint Canada ULC.

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 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 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. From the root of the Cognos Analytics media, run `setup.exe` as an administrator.
3. Click **Step 2: Install and Configure Cognos Application Tier**, and then follow the prompts.
4. To avoid damaging the existing installation, you must ensure that the installation directory is unique (for example, `C:\Program Files\ibm\cognos\analytics_at2`).
5. On the **Installation Completed** screen, click **Finish**.
6. 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 53.

4. Installing additional instances of Cognos Application Tier and web components

Note: The shortcut that was created for the second instance will replace the shortcut created for the first instance. You can launch the IBM Cognos Configuration from the following folder instead:

```
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
4. In the **Gateway Settings > Gateway URI** field, enter the URI and port of the Cognos Application Tier:

```
/p2pd/servlet/dispatch
```

For example:

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


5. In the **Explorer** pane, select **Logging**.
6. Complete the following fields in the **Logging - Component Properties** pane:
 - a. In the **Enable TCP?** field, select **True**.
 - b. In the **Local log server port** field, change **9362** to the port for the new application instance.
7. In the **Explorer** pane, select **IBM Cognos-1**.

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. Repeat all stages from "Stage 1. Creating the Cognos Content Store database" on page 35 to "Stage 9. Setting the security settings in Cognos" on page 45.
11. Import the base data model.

5. 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 `CPEExtended` 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 2017 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
```

6. Troubleshooting the service pack upgrade

Troubleshooting the upgrade

Execution timeout error in RSW.

If you are getting timeout errors in RSW, 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-STG_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-STG_ADFS\Web.config` file. For more information, see "Configuring Single Sign-on using WS-Federation (ADFS)" on page 21.

Cognos report in a portal will not load

The report version may be out of date. Regenerating the report in Cognos Analytics will update the report version.

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 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 and Report Designer websites 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 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.

