Gimmal
Information Management for Everyone®

Installation Guide
Compliance Suite

(Feature-Activated)

For SharePoint 2013/2016/2019

Software Version 4.14.0

December 2020

Title: *Compliance Suite (Feature-Activated) Installation Guide*

Gimmal LLC believes the information in this publication is accurate as of its publication date. The information in this publication is provided as is and is subject to change without notice. Gimmal LLC makes no representations or warranties of any kind with respect to the information contained in this publication, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose.

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmal.com. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

Contents

Chapter 1. Introduction...1

1.1 Who Should Use This Guide...1

1.2 About This Manual...1

Chapter 2. Implementing the SharePoint Environment...........2

2.1 Creating a New Web Application in SharePoint 2013/2016/2019..............2

2.2 Verifying the Fully Qualified Domain Name...4

2.3 Creating a Record Center in SharePoint 2013/2016/2019............................5

2.4 Make a Backup or Snapshot...6

Chapter 3. Installing Compliance Suite.....................................7

3.1 Prerequisites..7

3.2 Initiating the Installation Process...7

3.3 Deploying Bulk Task Processing...
17

Chapter 4. Performing Post-Installation Configuration Tasks
...20

4.1 Managing Event Service Application.. 20

4.2 Managing Email Service Application.. 20

4.3 Accessing File Plan Builder...21

4.3.1 Activating File Plan Builder...21

4.3.2 Applying File Plan Builder Settings...21

4.3.3 Setting up SSL Bindings for File Plan Builder Site..25

4.3.4 Verifying Windows Authentication..25

4.3.5 Adding Users to Groups...27

4.3.6 Launching File Plan Builder..27

4.4 Setting Up Localization... 28

4.4.1 Configuring Email Mapping..28

4.5 Activating Compliance Suite Ribbon Navigation for 2013/2016/2019... 29

4.6 Activating Compliance Suite Job Configuration.. 29

4.7 Activating Advanced Workflows..31

Chapter 5. Installing Compliance Suite in an ADFS Environment...32

Chapter 6. Describing Compliance Suite Features and Dependencies...40

Chapter 7. Performing an Uninstall of Compliance Suite Features 44

7.1 Using Gimmal Compliance Suite Installer... 44

7.2 Manually Deactivating Features.. 52

7 December 2020

1 Introduction

Gimmal delivers market leading content governance and compliant records solutions built on Microsoft® SharePoint®. Gimmal solutions drive user adoption and simplify information access by making information lifecycle management of content simple and transparent, ensuring consistent compliance and proactive litigation readiness enterprise-wide while lowering costs.

Gimmal's Compliance Suite for SharePoint 2013/2016/2019 combines with SharePoint to give your organization a reliable and centralized repository for collaboration and records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 Records Management Program.

Important!

For **SharePoint 2013**, Compliance Suite V4.14.0 can be upgraded from Compliance Suite V4.13.1.

For **SharePoint 2016**, Compliance Suite V4.14.0 can be upgraded from Compliance Suite V4.13.1.

For **SharePoint 2019**, Compliance Suite V4.14.0 can be upgraded from Compliance Suite V4.13.1.

Gimmal’s iGs Enhanced Search application is no longer bundled with the Compliance Suite installation/upgrade package. If you have an existing or older version of iGs Enhanced Search on your system, you must remove it manually prior to installing Compliance Suite.

1.1 Who Should Use This Guide

The intended audience for this document is SharePoint administrators. Administrators are considered to be SharePoint power users who are familiar with the enterprise's content management and retention policies.

1.2 About This Manual

This guide contains steps to install Gimmal Compliance Suite. These steps include configuring the desired base state for a SharePoint environment, running the Gimmal installer, performing postinstallation configuration tasks, and understanding the Compliance Suite features and dependencies.

2 Implementing the SharePoint Environment

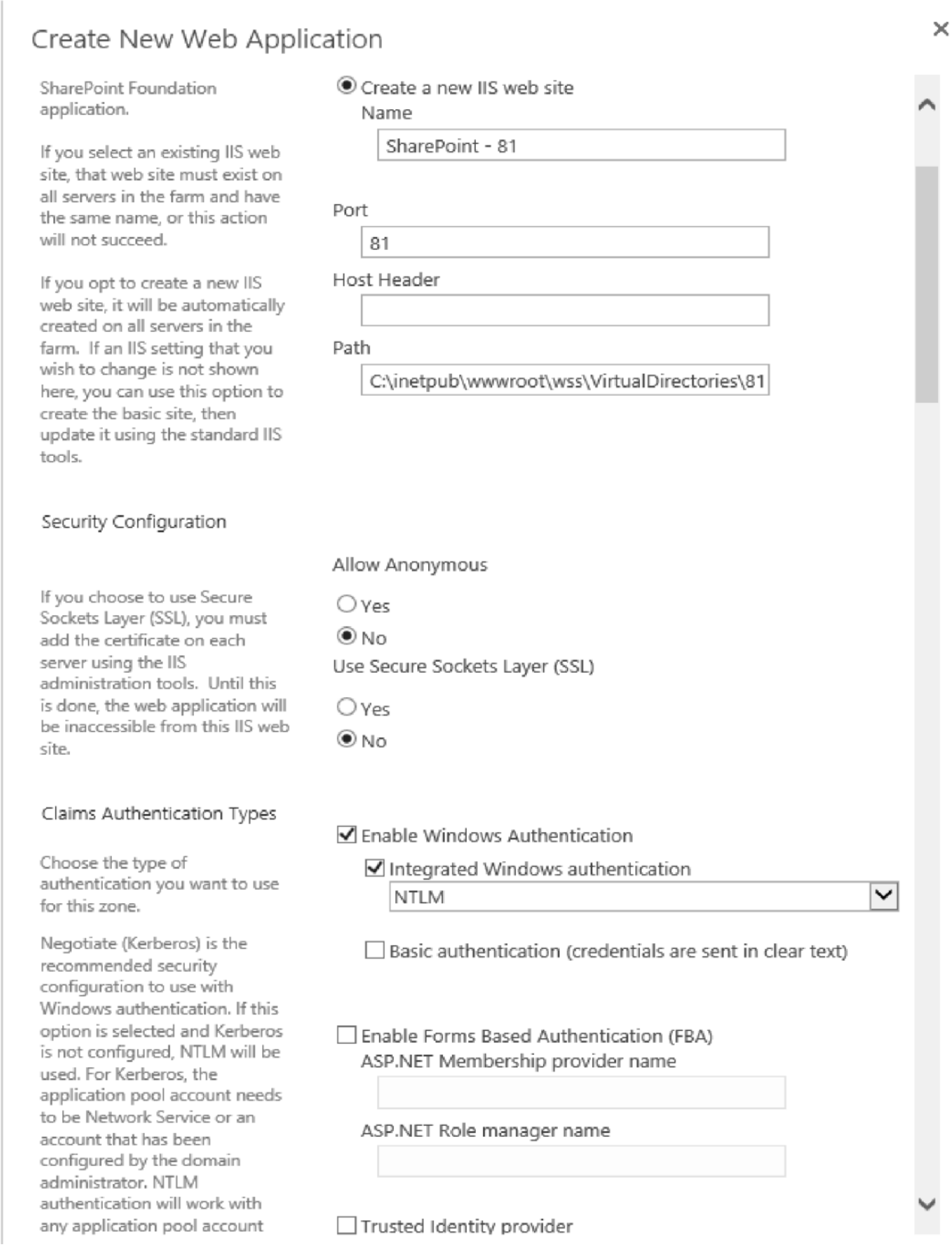
This chapter provides instructions for implementing the SharePoint environment in SharePoint 2013/2016/2019. You must have a SharePoint environment implemented to install, configure, and use the Gimmal Compliance Suite solution. The SharePoint environment provides the Fully Qualified Domain Names (FQDN). A FQDN consists of the host machine and the domain; for example, *http://machine.domain.com*.

2.1 Creating a New Web Application in SharePoint 2013/2016/2019

A Web application comprises an Internet Information Services (IIS) Web site that acts as a logical unit for the site collections that you create. Before you can create a site collection, you must first create a Web application. Web applications isolate content by creating a new content database and defining the authentication method used to connect to the database. If you do not have an existing web application, you'll need to create a new one by following the steps below.

1. Navigate to **Central Administration**.
2. Click **Application Management** in the left pane.
3. Click **Manage Web Applications**.
4. Click **New Web Applications**.
5. In the **IIS Website** section, click **Create a new IIS Web Site**.
    a. Type the name for your Web application.
    b. Select a port number that is currently not in use. The default port number for HTTP access is 80, and the default port number for HTTPS access is 443. If you want users to access the Web application without typing in a port number, they should use the appropriate default port number.
    c. In the **Path** box, type the path to the IIS Web site home directory for the server. This should be a path to your *inetpub* directory. For example: `C:\inetpub\wwwroot\wss\VirtualDirectories\80`.
6. In the **Security Configuration** section, configure security and encryption for your Web application.
7. In **Claims Authentication Types** section, select the mode of authentication from Windows Based (NTLM, Kerberos) or Trusted Identity Provider (Active Directory Federation Services (ADFS)).

8. In **Sign in Page URL** section, enter URL for your custom sign in page or use default.
9. In the **Public URL** section, type the **Fully Qualified Domain Name URL** for all sites that users will access in this Web application.
10. In the **Application Pool** section either select *Predefined* to use a predefined security account or *Configurable* to specify a new security account to be used for an existing application pool.
11. In the **Database Name and Authentication** section, choose the database server, database name, and authentication method for your new Web application.
12. If you use database mirroring, in the **Failover Server** section, in the **Failover Database Server** box, type the name of a specific failover database server that you want to associate with a content database.
13. In the **Service Application Connections** section, select the service application connections that will be available to the Web application.
14. Click **OK** to create the new Web application.



Create New Web Application

SharePoint Foundation application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

● Create a new IIS web site

Name: SharePoint - 81

Port: 81

Host Header:

Path: C:\inetpub\wwwroot\wss\VirtualDirectories\81

Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

○ Yes

● No

Use Secure Sockets Layer (SSL)

○ Yes

● No

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account

☑ Enable Windows Authentication

☑ Integrated Windows authentication: NTLM

☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name:

ASP.NET Role manager name:

☐ Trusted Identity provider

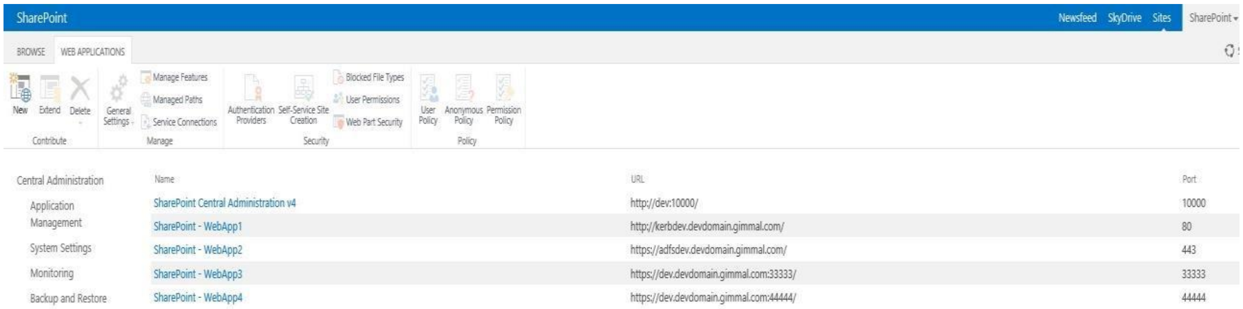
Figure 2-1 Creating a New Web Application in SharePoint 2013/2016

2.2 Verifying the Fully Qualified Domain Name

To verify that SharePoint is using a fully qualified domain name (FQDN) for the Web application, inspect the Web application using Central Administration with the following steps:

1. Go to **Central Administration**.
2. Click **Application Management** in the left pane.

3. Click **Web Applications/Manage Web Applications**.
4. Inspect the list to verify that FQDN is being used as follows.



Name	URL	Port
SharePoint Central Administration v4	http://dev:10000/	10000
SharePoint - WebApp1	http://kerbdev.devdomain.gimmal.com/	80
SharePoint - WebApp2	https://adfsdev.devdomain.gimmal.com/	443
SharePoint - WebApp3	https://dev.devdomain.gimmal.com:33333/	33333
SharePoint - WebApp4	https://dev.devdomain.gimmal.com:44444/	44444

Figure 2-2 Fully Qualified Domain Name in SharePoint 2013/2016

If you have verified that your web applications are not using FQDN, the following sections and steps assist in getting to the required base state. Note that the steps provided in the following instructions are intended for SharePoint Administrators and provide high level detail only.

Use these steps to configure Central Administration and the Web Application to use FQDN:

1. From **Central Administration**, click **Application Management**.
2. Under **Web Applications**, click **Configure alternate access mappings**.
3. Click the **Edit Public URLs** link.
4. From the **Alternate Access Mapping Collection** menu, select **Change Alternate Access Mapping Collection**.
5. Select the Web application that hosts Central Administration.
6. In the **Public URLs** section, type the URL protocol, host, and name field in the **Default** or **Custom** section; for example, *http://sharepointdev.spdev.com:8000*.
7. Verify that FQDN is used and click **Save**.
8. Close Internet Explorer.
9. Launch Internet Explorer.
10. Launch **Central Administration** using the FQDN.

2.3 Creating a Record Center in SharePoint 2013/2016/2019

A Records Center site is a specialized type of Web site in SharePoint that enables you to manage the documents and other files that you need to keep as records. If you do not have an existing Records Center site at the root of a site collection in SharePoint 2013/2016/2019, you must create a new one by following the steps in this section.

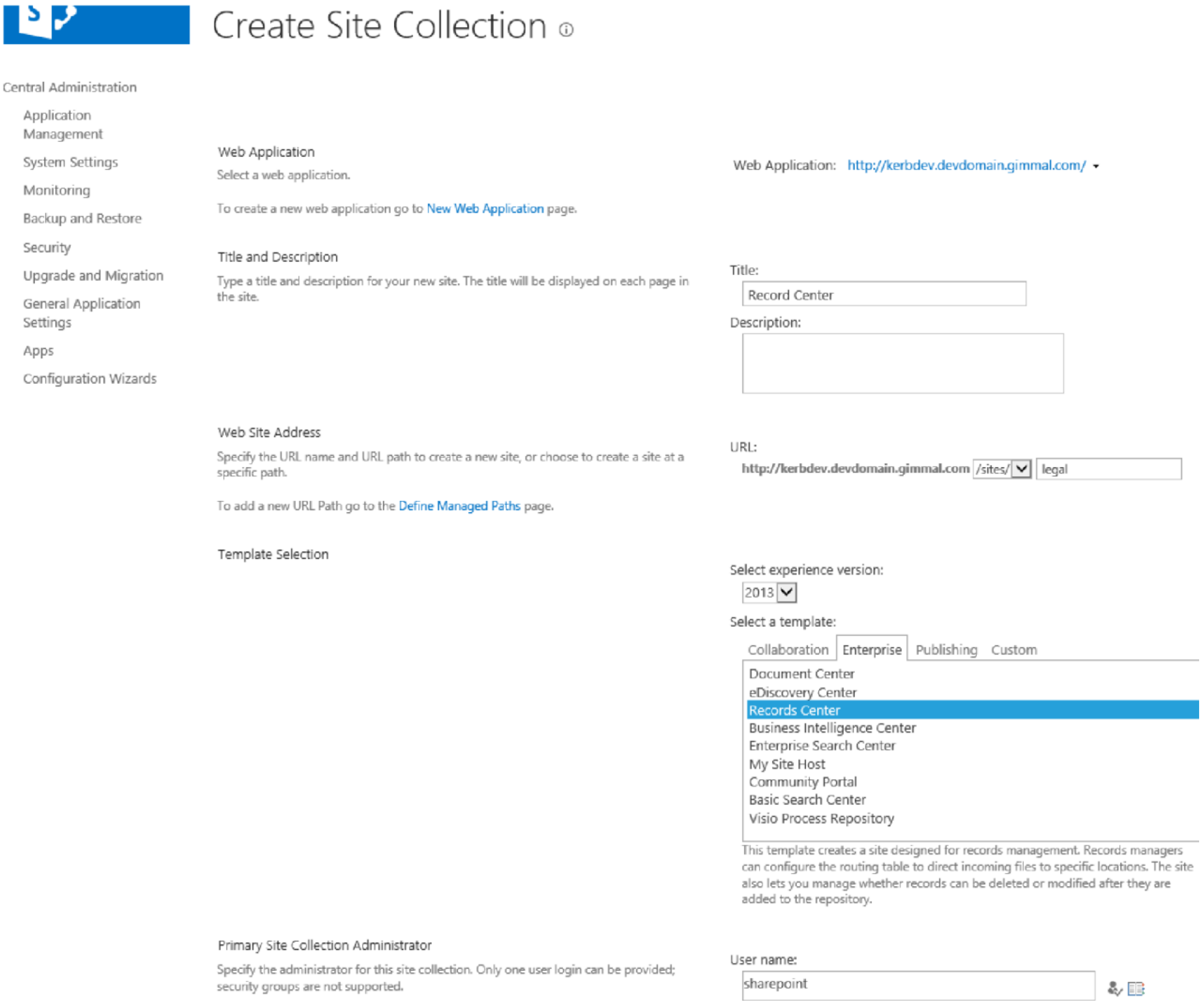
Create a Records Center as the root site by creating a new web application and site collection using the following steps:

1. From **Central Administration**, click **Application Management.**
2. Click **Create Site Collections** under **Site Collections**.
3. On the Create Site Collection page, in the **Web Application** section, if the Web application in which you want to create the site collection is not selected, click **Change Web Application** on the **Web Application** menu.
4. In the **Title** box, type a title for the Records Center site. The title will be displayed on each page in the site.

Note:

Changing the Record Center name after Compliance Suite has been installed can cause Compliance Suite to work improperly; therefore, it is advised to carefully decide on the Record Center name prior to installation.

5. Type a **Description** of the site.
6. In the **Web Site Address** section, specify the URL name and URL path to create a new site, or create a site at a specific path.
7. In the **Template Selection** section on the **Enterprise** tab, select **Records Center**.
8. In the **Primary Site Collection Administrator** section, type in the *Farm Account* or *Site Collection Administrator* name in the form DOMAIN\user name for the user who will be the site collection administrator.
9. Click **OK**.



Create Site Collection

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Apps
- Configuration Wizards

Web Application

Select a web application.

To create a new web application go to New Web Application page.

Web Application: http://kerbdev.devdomain.gimmal.com/

Title and Description

Type a title and description for your new site. The title will be displayed on each page in the site.

Title: Record Center

Description:

Web Site Address

Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

To add a new URL Path go to the Define Managed Paths page.

URL: http://kerbdev.devdomain.gimmal.com /sites/ legal

Template Selection

Select experience version: 2013

Select a template:

Collaboration | Enterprise | Publishing | Custom

- Document Center
- eDiscovery Center
- Records Center
- Business Intelligence Center
- Enterprise Search Center
- My Site Host
- Community Portal
- Basic Search Center
- Visio Process Repository

This template creates a site designed for records management. Records managers can configure the routing table to direct incoming files to specific locations. The site also lets you manage whether records can be deleted or modified after they are added to the repository.

Primary Site Collection Administrator

Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.

User name: sharepoint

Figure 2-3 Creating a Record Center in SharePoint 2013/2016

2.4 Make a Backup or Snapshot

At this point, Gimmal suggests taking a backup or snapshot to ensure that you have a reliable starting point to return to if problems occur.

3 Installing Compliance Suite

The Compliance Suite solution is installed using an installer. The installer operates on the Web Front-End (WFE) server of your system, so place it in an accessible location on the WFE server. The installation media consists of a single ISO that contains everything necessary to install and set up Compliance Suite and its components, and is described below.

3.1 Prerequisites

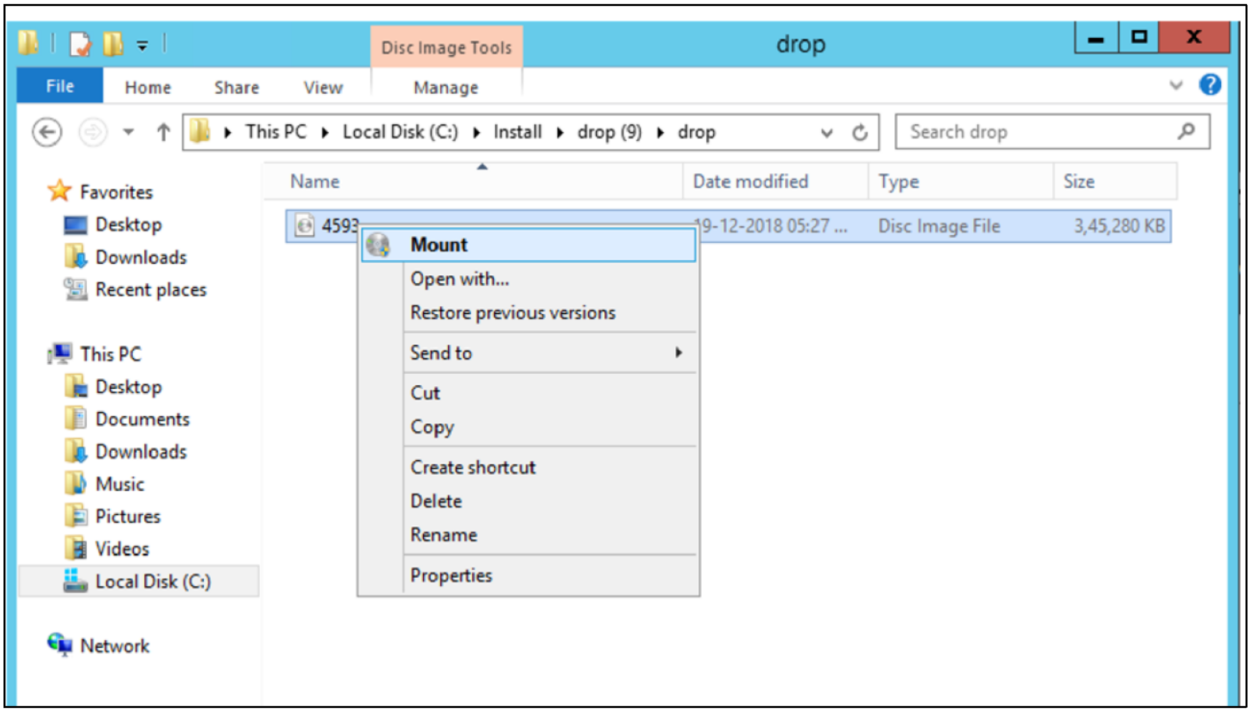
Before installing Compliance Suite, verify that:

- The user performing the installation is the administrator of a farm account and has local administrator rights on the Web front-end (WFE) server where the installation is being performed.
- Compliance Suite's File Plan Builder is installed on a Central Administration server, which must be a WFE-enabled server.
- SharePoint Server 2013/SharePoint 2016/SharePoint 2019 (Standard or Enterprise Edition) with Service Pack 1 has been installed.
- A Managed Metadata Term Store has been enabled and configured (see https://technet.microsoft.com/en-us/library/mt683863(v=office.16).aspx for instructions). The Gimmal Compliance Suite installer adds the terms that it needs to operate to the store if the store has been configured. If the store has not been configured, Gimmal Compliance Suite will not install.
- The Search Service application must be installed and configured on the SharePoint farm.
- The installing and activating user(s) must have the role of a term store administrator under the Managed Metadata Service.
- Microsoft .NET Framework 4.6 or higher is installed (https://www.microsoft.com/net/download/dotnet-framework-runtime/net46)
- One of the following authentication methods is installed: NTLM, Kerberos, or ADFS.
- If more than one instance of Compliance Suite is to be installed, then an equal number of SQL server instances must be available. A unique instance of the SQL server must be assigned to each instance of Compliance Suite.

3.2 Initiating the Installation Process

To initiate the Compliance Suite installation process, perform the following steps as a local Administrator:

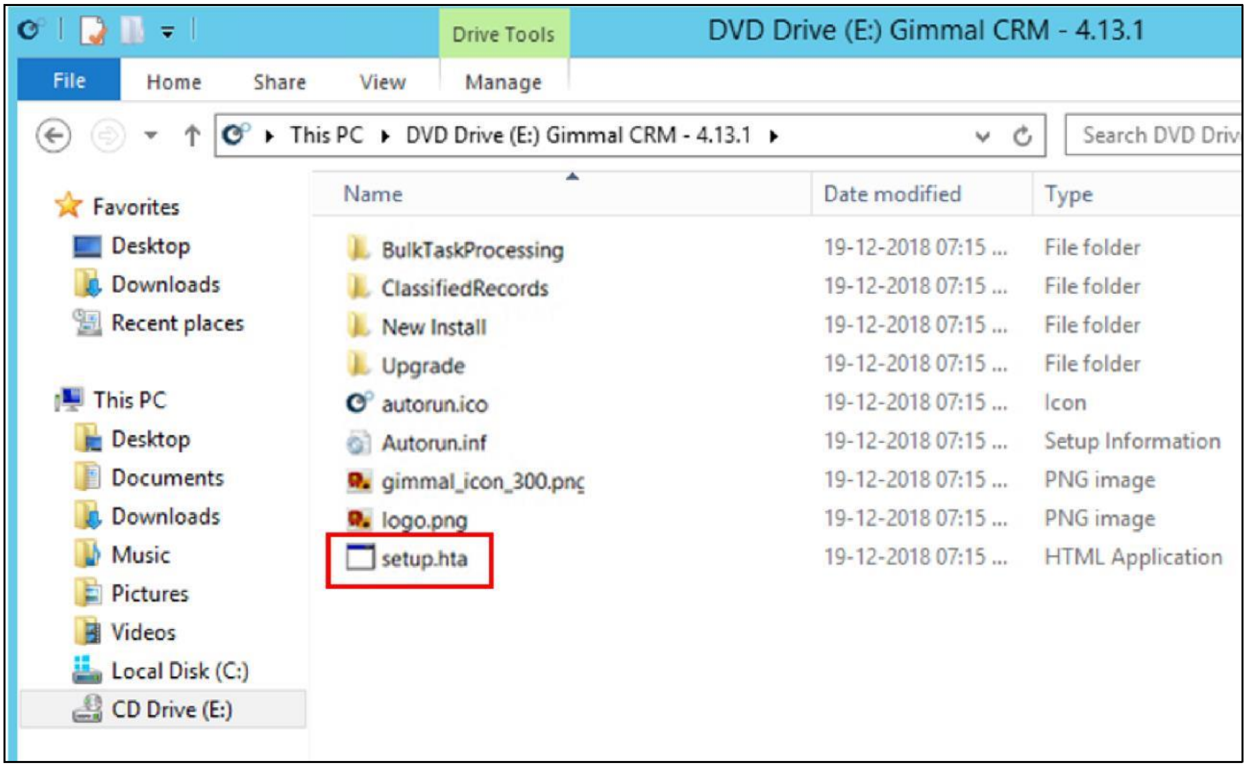
1. Download the zipped ISO package from the Gimmal software download site and extract it to a folder.
2. Navigate to the folder that contains the ISO file, right-click it, and select **Mount**.



Name	Date modified	Type	Size
4593	19-12-2018 05:27 ...	Disc Image File	3,45,280 KB

Figure 3-1 Mount ISO File

3. The installation setup should start automatically. If not, double-click the **setup.hta** file in the root folder of the ISO.



Name	Date modified	Type
BulkTaskProcessing	19-12-2018 07:15 ...	File folder
ClassifiedRecords	19-12-2018 07:15 ...	File folder
New Install	19-12-2018 07:15 ...	File folder
Upgrade	19-12-2018 07:15 ...	File folder
autorun.ico	19-12-2018 07:15 ...	Icon
Autorun.inf	19-12-2018 07:15 ...	Setup Information
gimmal_icon_300.pnc	19-12-2018 07:15 ...	PNG image
logo.png	19-12-2018 07:15 ...	PNG image
setup.hta	19-12-2018 07:15 ...	HTML Application

Figure 3-2 Setup File

The Certified Records Management splash screen launches, which provides a link to each component's respective installer, as well as some other helpful links.

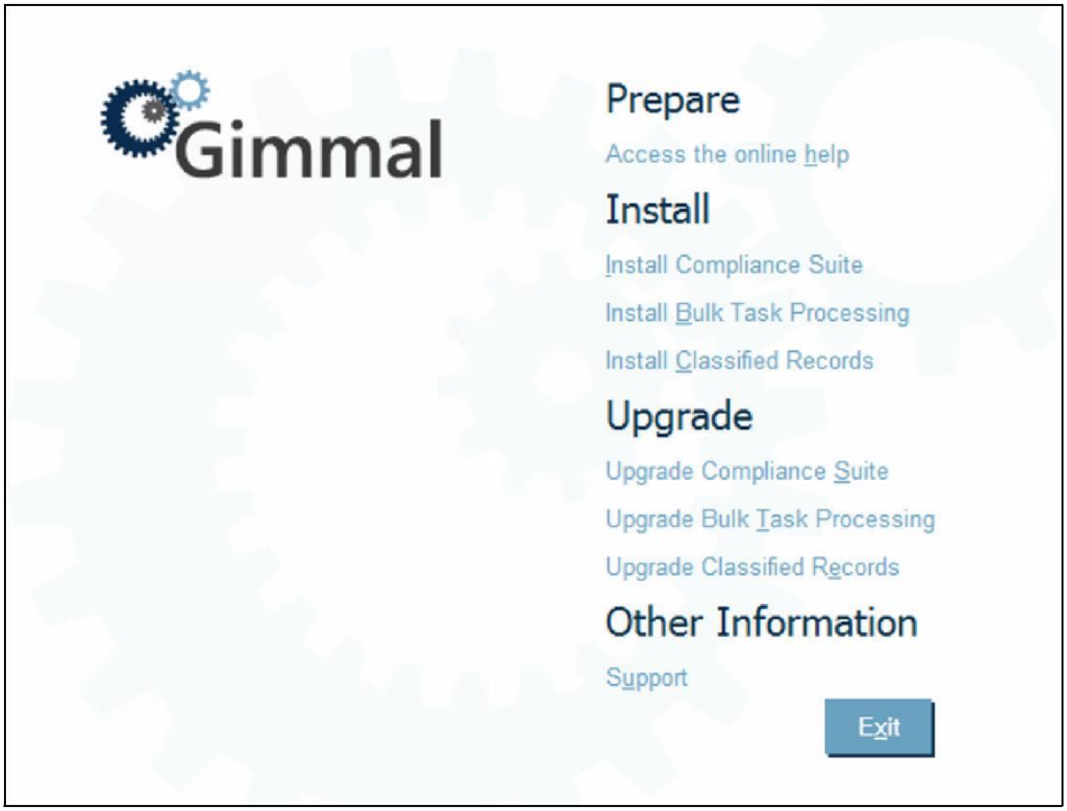
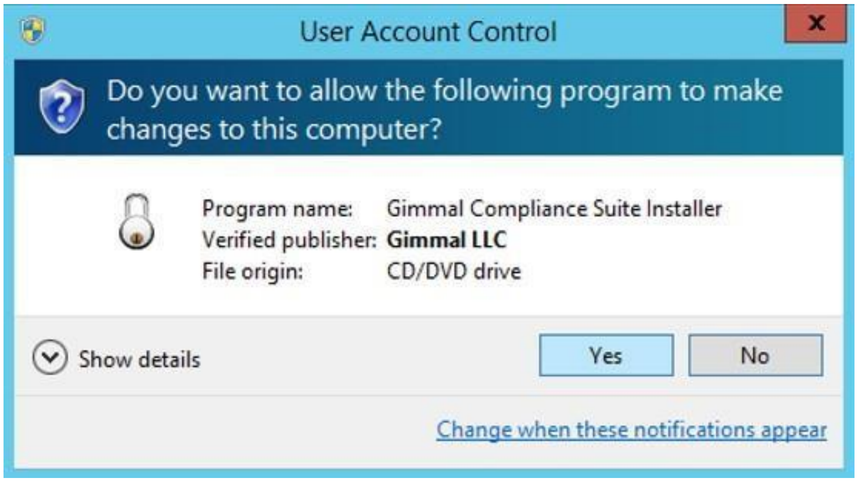


Figure 3-3 Splash Screen

4. Click **Install Compliance Suite**. A User Account Dialog opens.

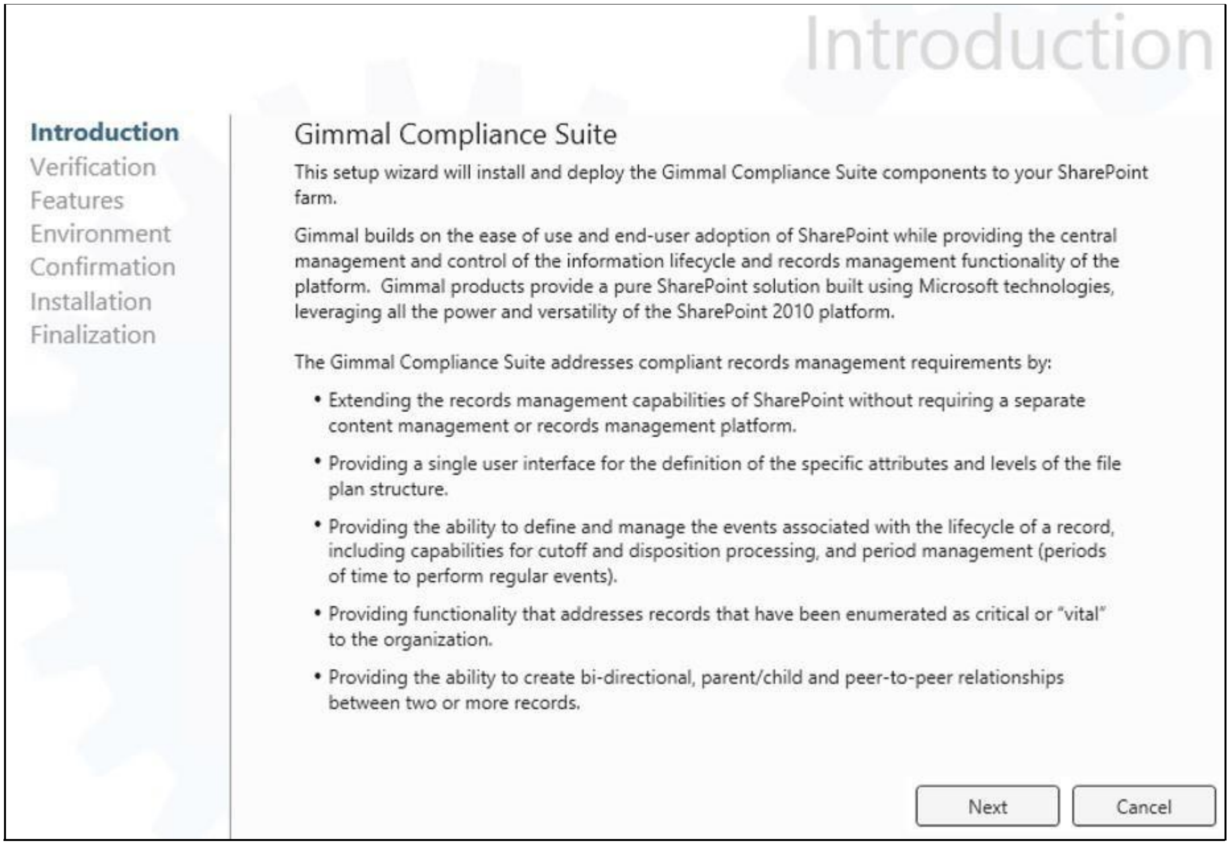


Do you want to allow the following program to make changes to this computer?

Program name: Gimmal Compliance Suite Installer
Verified publisher: **Gimmal LLC**
File origin: CD/DVD drive

Figure 3-4 User Account Dialog

5. Click **Yes** to continue. When the installer loads, the Gimmal Compliance Suite Introduction page displays.



Gimmal Compliance Suite

This setup wizard will install and deploy the Gimmal Compliance Suite components to your SharePoint farm.

Gimmal builds on the ease of use and end-user adoption of SharePoint while providing the central management and control of the information lifecycle and records management functionality of the platform. Gimmal products provide a pure SharePoint solution built using Microsoft technologies, leveraging all the power and versatility of the SharePoint 2010 platform.

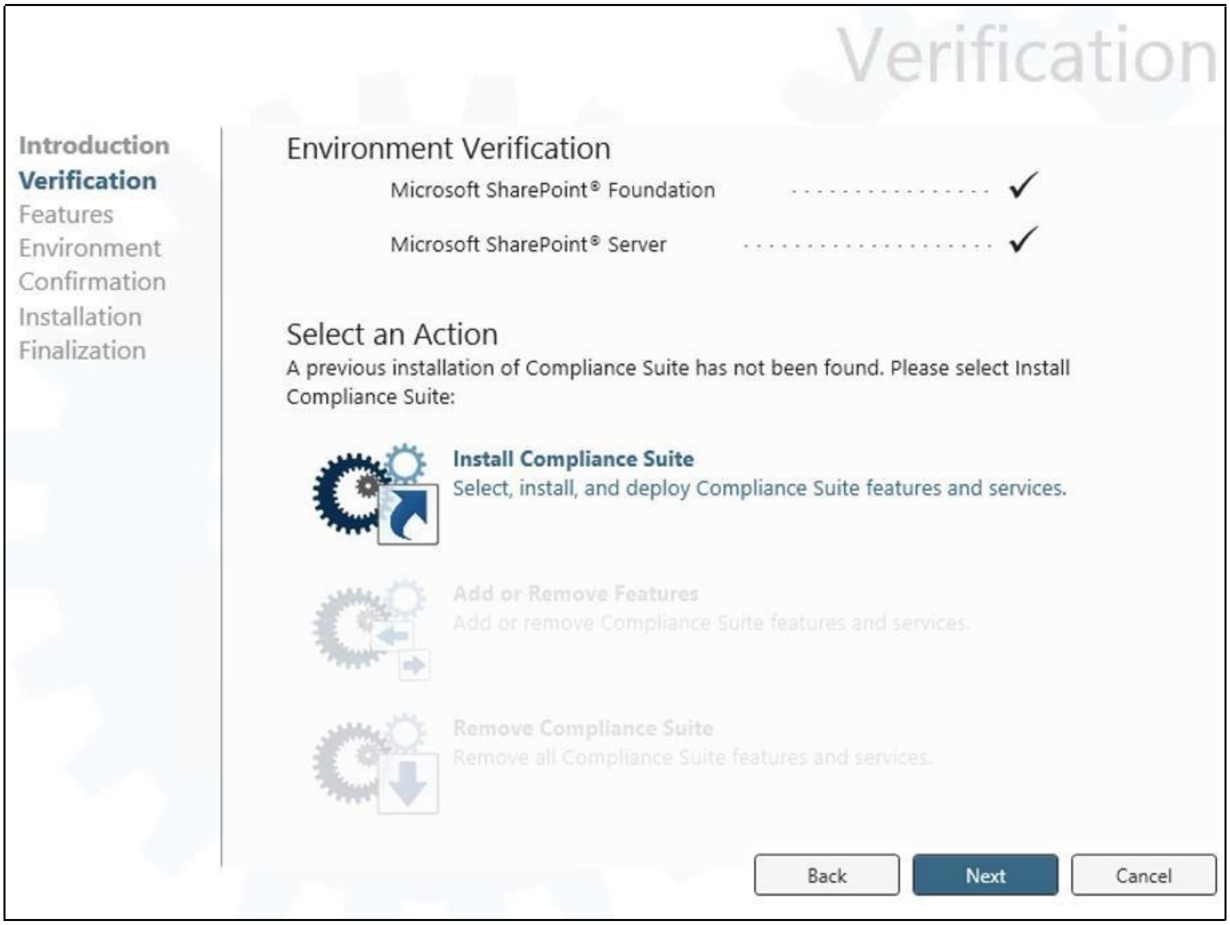
The Gimmal Compliance Suite addresses compliant records management requirements by:

- Extending the records management capabilities of SharePoint without requiring a separate content management or records management platform.
- Providing a single user interface for the definition of the specific attributes and levels of the file plan structure.
- Providing the ability to define and manage the events associated with the lifecycle of a record, including capabilities for cutoff and disposition processing, and period management (periods of time to perform regular events).
- Providing functionality that addresses records that have been enumerated as critical or "vital" to the organization.
- Providing the ability to create bi-directional, parent/child and peer-to-peer relationships between two or more records.

Figure 3-5 Installer Introduction Page

6. Click **Next**.

The Verification page displays, enabling the installer to verify that SharePoint Foundation and SharePoint Server are installed.



Environment Verification

Microsoft SharePoint® Foundation ✓

Microsoft SharePoint® Server ✓

Select an Action

A previous installation of Compliance Suite has not been found. Please select Install Compliance Suite:

Install Compliance Suite
Select, install, and deploy Compliance Suite features and services.

Add or Remove Features
Add or remove Compliance Suite features and services.

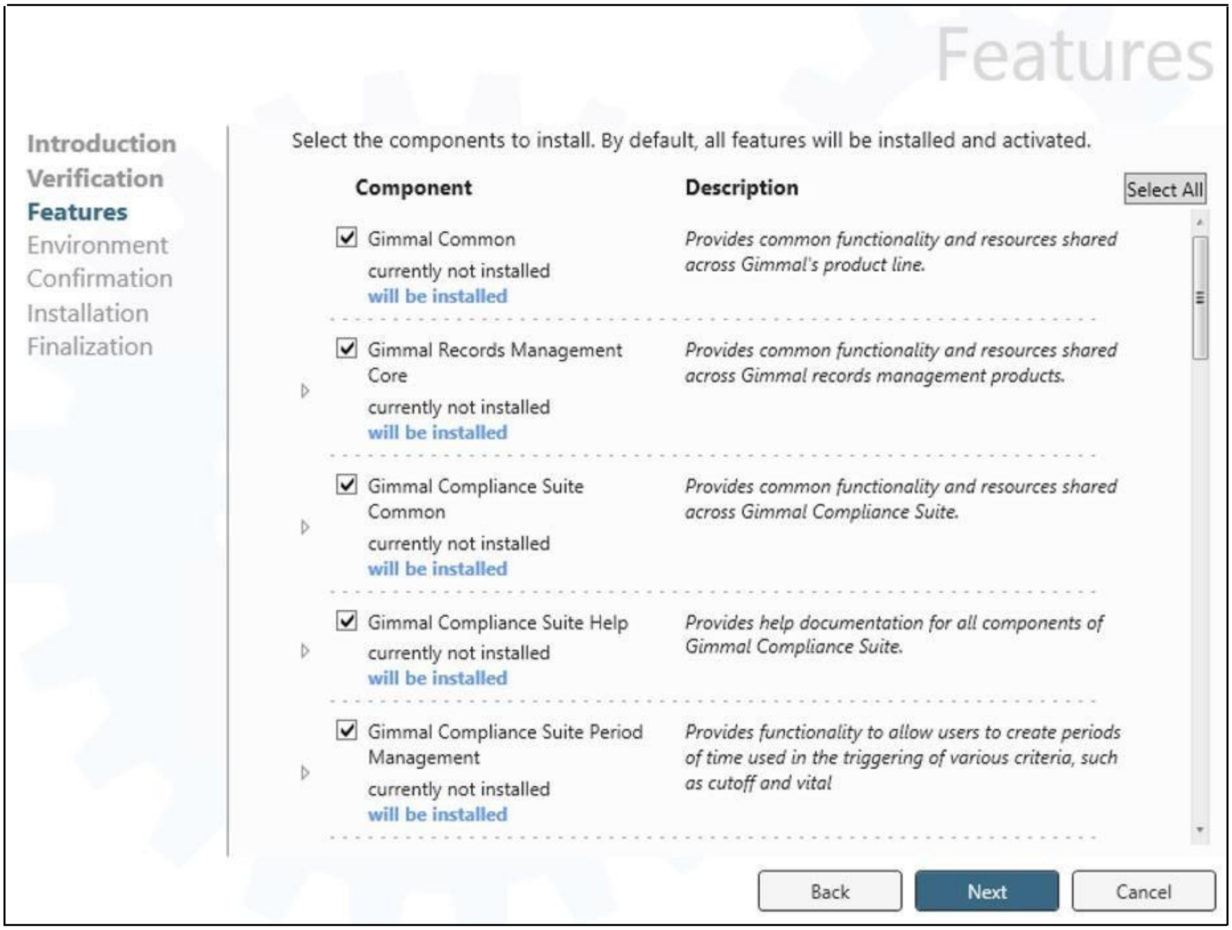
Remove Compliance Suite
Remove all Compliance Suite features and services.

Figure 3-6 Installer Verification Page

Note

If installing Compliance Suite for the first time, only the option to **Install Compliance Suite** displays. If Compliance Suite is currently installed, then the **Add or Remove Features** and **Remove Compliance Suite** options display.

7. Click **Next**. The Features page displays.



Select the components to install. By default, all features will be installed and activated.

Component	Description
☑ Gimmal Common currently not installed will be installed	*Provides common functionality and resources shared across Gimmal's product line.*
☑ Gimmal Records Management Core currently not installed will be installed	*Provides common functionality and resources shared across Gimmal records management products.*
☑ Gimmal Compliance Suite Common currently not installed will be installed	*Provides common functionality and resources shared across Gimmal Compliance Suite.*
☑ Gimmal Compliance Suite Help currently not installed will be installed	*Provides help documentation for all components of Gimmal Compliance Suite.*
☑ Gimmal Compliance Suite Period Management currently not installed will be installed	*Provides functionality to allow users to create periods of time used in the triggering of various criteria, such as cutoff and vital*

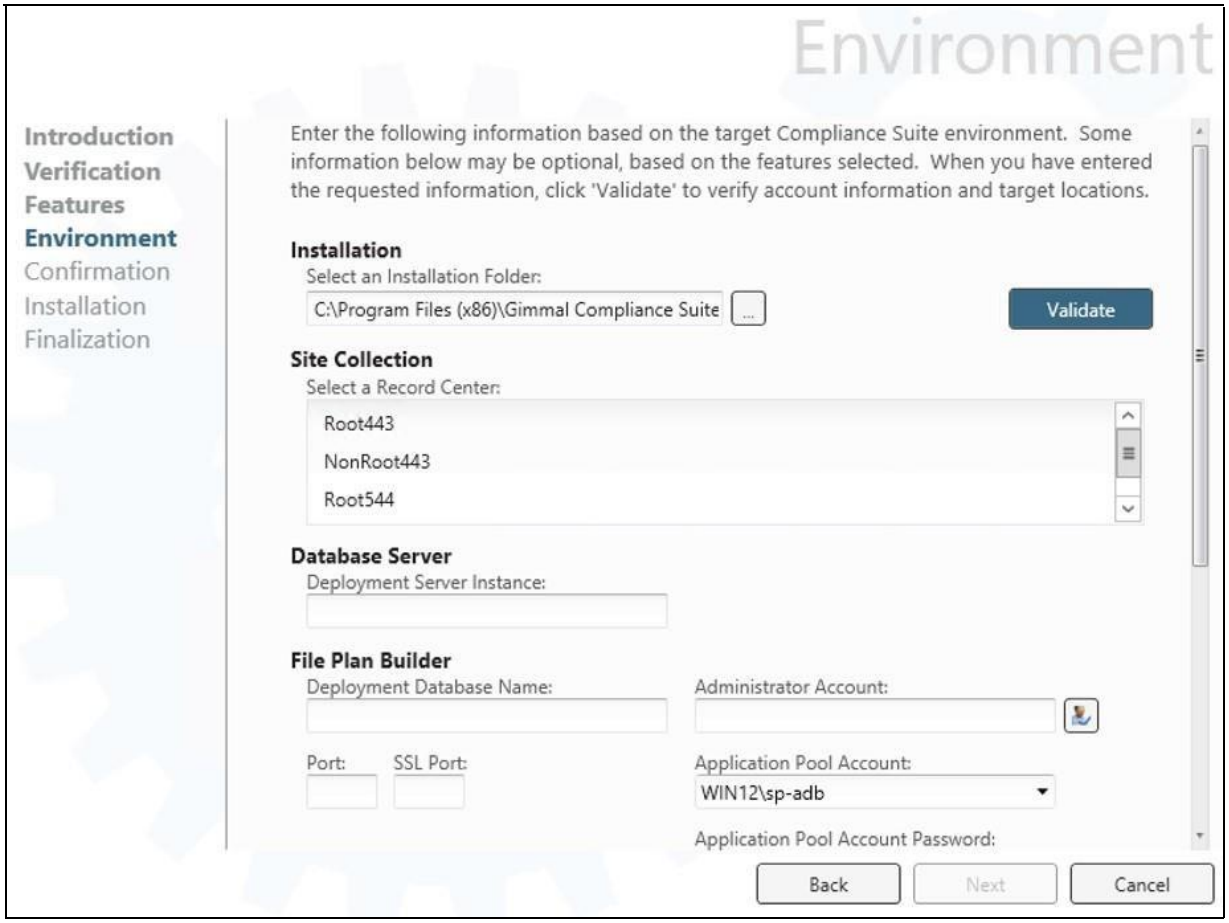
Figure 3-7 Installer Features Window

8. Select the **Gimmal Compliance Suite Features** that you want to install (or click **Select All** in the upper right corner to select all of the features. If you are installing for the first time, you can keep all the defaults.

Important!

If you are installing Cs in an ADFS environment, deselect the **File Plan Builder** check box because it must be installed manually (see the “5 Installing Compliance Suite in an ADFS Environment” on page 32).

9. Click **Next**. The Environment page displays.



Enter the following information based on the target Compliance Suite environment. Some information below may be optional, based on the features selected. When you have entered the requested information, click 'Validate' to verify account information and target locations.

Installation

Select an Installation Folder: C:\Program Files (x86)\Gimmal Compliance Suite

Site Collection

Select a Record Center:

Root443
NonRoot443
Root544

Database Server

Deployment Server Instance:

File Plan Builder

Deployment Database Name:

Administrator Account:

Port:

SSL Port:

Application Pool Account: WIN12\sp-adb

Application Pool Account Password:

Figure 3-8 Installer Environment Window

10. Provide the following installation parameters:

a. Select the folder where the **Installation** files will be installed, Gimmal recommends creating a folder on the C:\ or D:\ drive where there is enough empty disk space. (Around 15 MB).

b. Select the **Record Center** where you want to install Compliance Suite.

c. Enter the Fully Qualified Domain Name of your **Deployment Server Instance**.

d. If applicable, enter the **Deployment Database Name** for **File Plan Builder**. There is no restriction on the naming convention used for the File Plan Builder database in the Cs solution.

e. Select the **Application Pool Account** that the File Plan Builder web application should run under and enter the **Application Pool Account Password**.

f. Enter the **Port** and **SSL Port** that the File Plan Builder web application will run on. This port should be available and should *not* be used by any other sites.

g. If applicable, enter the **Service Instance Name** for Event Management.

h. Enter the **Deployment Database Name** for Event Management. There is no specific naming convention used for the Event Management database in the Cs solution.

i. Select the **Application Pool** that the Event Management service should run under.

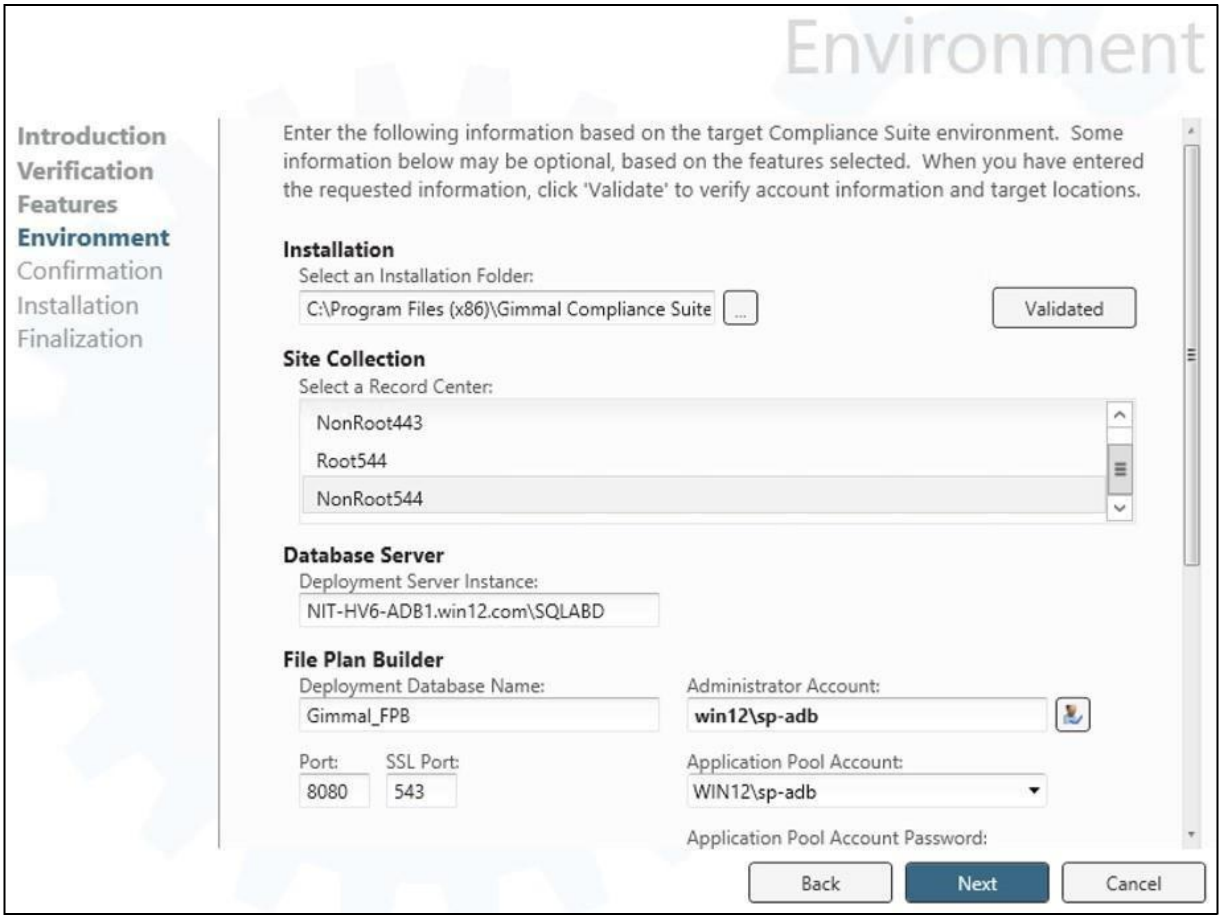
j. If applicable, enter the **Service Instance Name** for Email Management.

k. Enter the **Deployment Database Name** for Email Management. There is no restriction on the naming convention used for the Email Management database in the Cs solution.

l. Select the **Application Pool** that the Email Management service should run under.

m. Click **Validate** on the top right of the window. If there are any errors, a notification button with a Tool Tip displays.

11. When you enter valid settings, the **Next** button is enabled.



Enter the following information based on the target Compliance Suite environment. Some information below may be optional, based on the features selected. When you have entered the requested information, click 'Validate' to verify account information and target locations.

Installation

Select an Installation Folder: C:\Program Files (x86)\Gimmal Compliance Suite

Site Collection

Select a Record Center:

NonRoot443

Root544

NonRoot544

Database Server

Deployment Server Instance: NIT-HV6-ADB1.win12.com\SQLABD

File Plan Builder

Deployment Database Name: Gimmal_FPB

Administrator Account: win12\sp-adb

Port: 8080

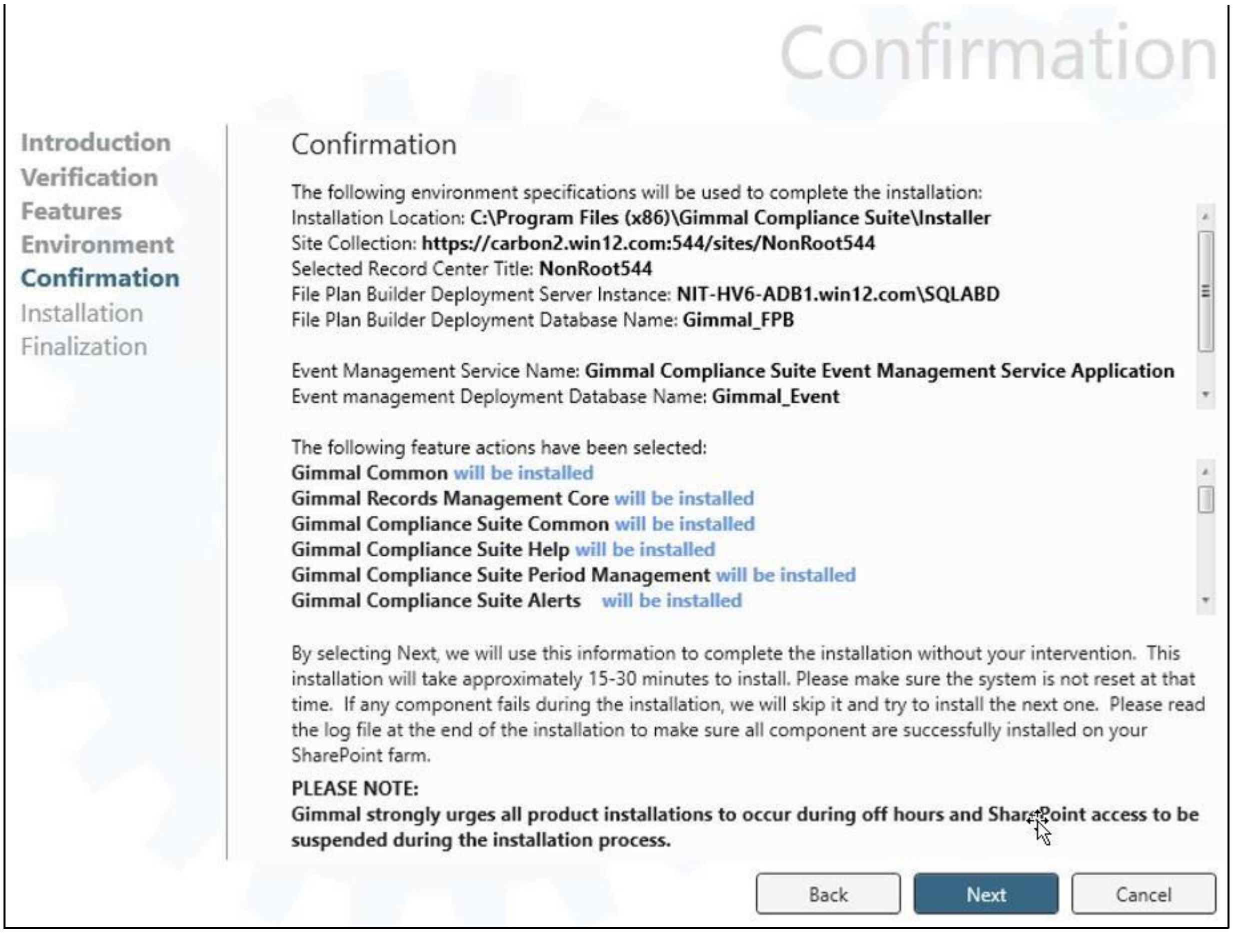
SSL Port: 543

Application Pool Account: WIN12\sp-adb

Application Pool Account Password:

Figure 3-9 Environment with Correct Settings

12. Click **Next** to proceed. The Confirmation page displays, confirming which Compliance Suite features will be installed.



Confirmation

The following environment specifications will be used to complete the installation:
Installation Location: **C:\Program Files (x86)\Gimmal Compliance Suite\Installer**
Site Collection: **https://carbon2.win12.com:544/sites/NonRoot544**
Selected Record Center Title: **NonRoot544**
File Plan Builder Deployment Server Instance: **NIT-HV6-ADB1.win12.com\SQLABD**
File Plan Builder Deployment Database Name: **Gimmal_FPB**

Event Management Service Name: **Gimmal Compliance Suite Event Management Service Application**
Event management Deployment Database Name: **Gimmal_Event**

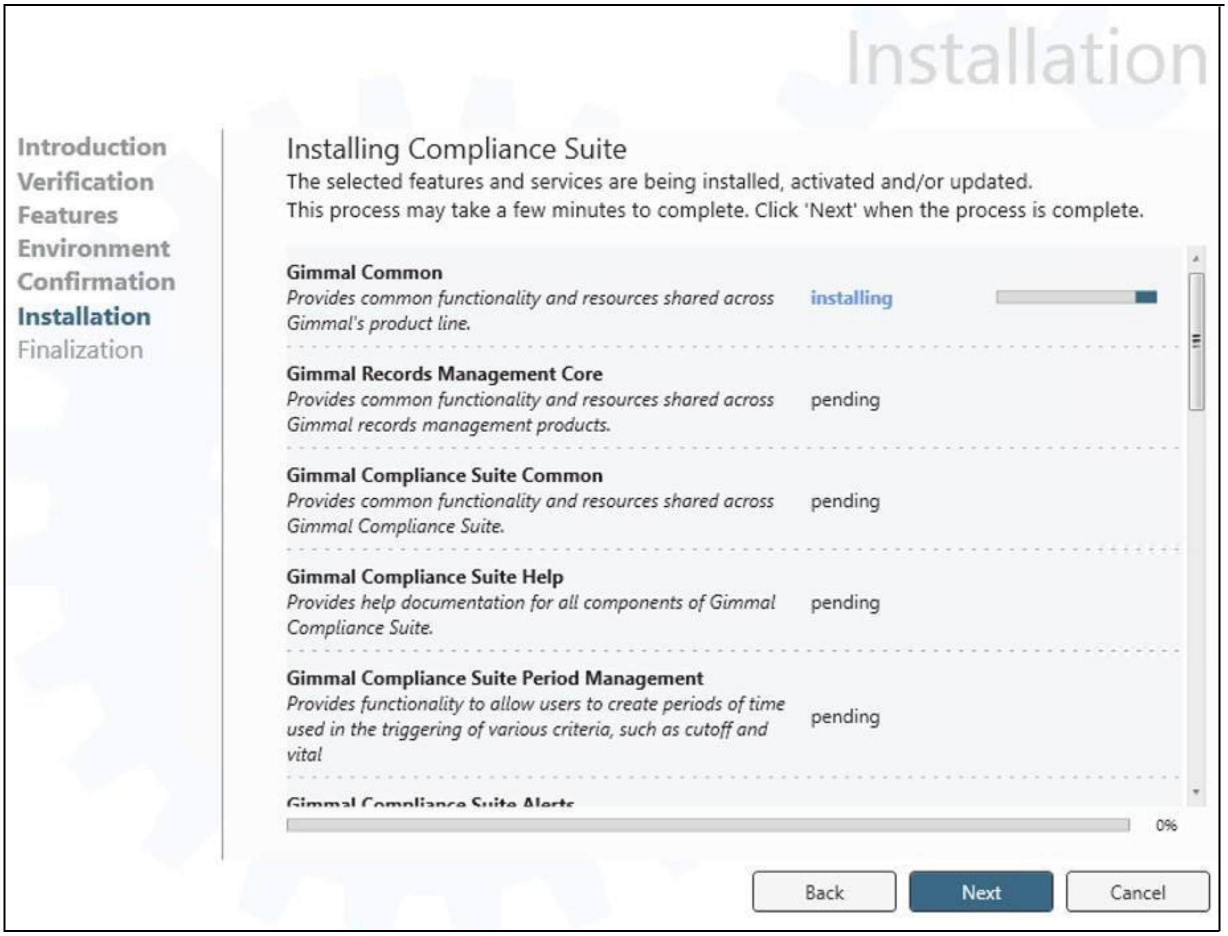
The following feature actions have been selected:
Gimmal Common will be installed
Gimmal Records Management Core will be installed
Gimmal Compliance Suite Common will be installed
Gimmal Compliance Suite Help will be installed
Gimmal Compliance Suite Period Management will be installed
Gimmal Compliance Suite Alerts will be installed

By selecting Next, we will use this information to complete the installation without your intervention. This installation will take approximately 15-30 minutes to install. Please make sure the system is not reset at that time. If any component fails during the installation, we will skip it and try to install the next one. Please read the log file at the end of the installation to make sure all component are successfully installed on your SharePoint farm.

PLEASE NOTE:
Gimmal strongly urges all product installations to occur during off hours and SharePoint access to be suspended during the installation process.

Figure 3-10 Installer Confirmation Window

13. Click **Next**. The installer begins installing the Compliance Suite features that you selected.



Installing Compliance Suite

The selected features and services are being installed, activated and/or updated.
This process may take a few minutes to complete. Click 'Next' when the process is complete.

Gimmal Common
Provides common functionality and resources shared across Gimmal's product line. installing

Gimmal Records Management Core
Provides common functionality and resources shared across Gimmal records management products. pending

Gimmal Compliance Suite Common
Provides common functionality and resources shared across Gimmal Compliance Suite. pending

Gimmal Compliance Suite Help
Provides help documentation for all components of Gimmal Compliance Suite. pending

Gimmal Compliance Suite Period Management
Provides functionality to allow users to create periods of time used in the triggering of various criteria, such as cutoff and vital pending

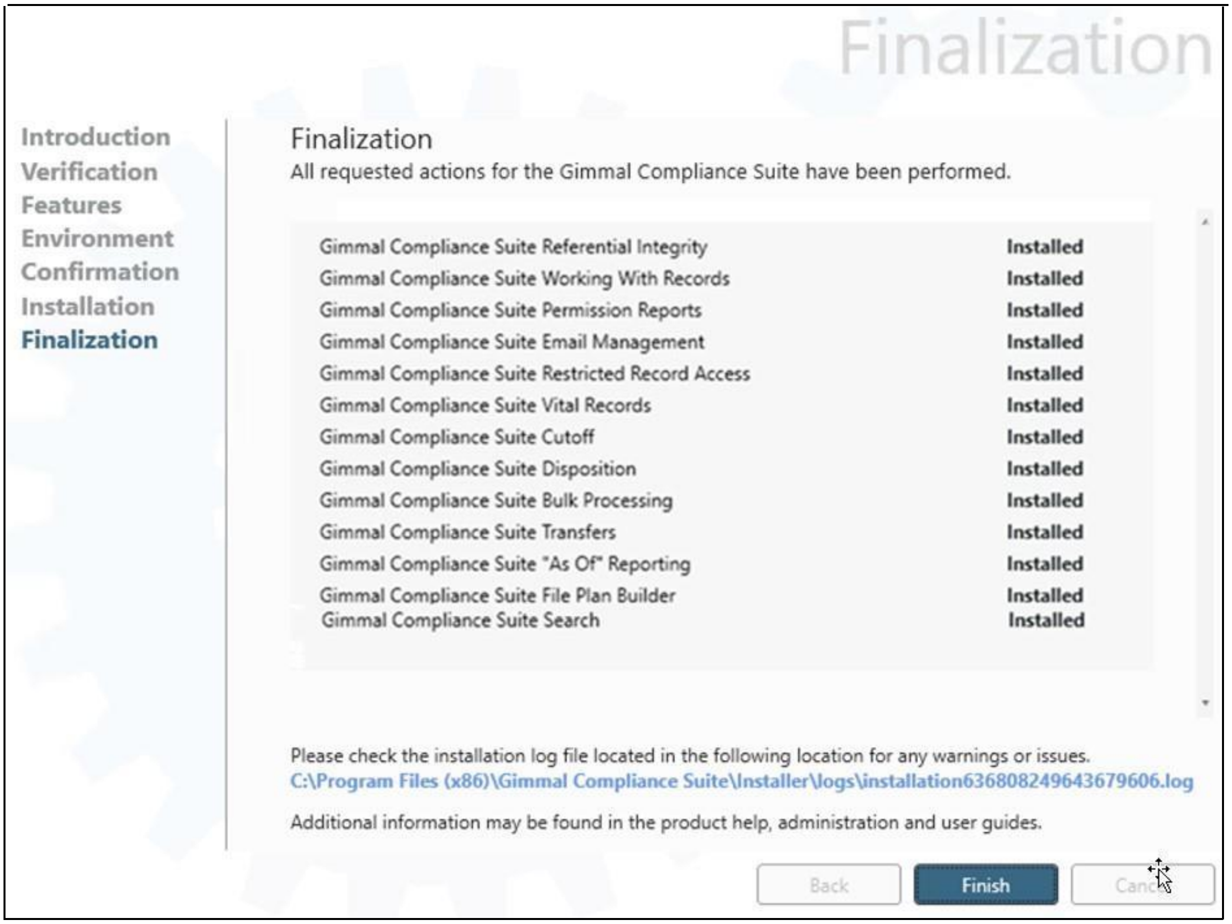
Gimmal Compliance Suite Alerts

0%

Figure 3-11 Installation Page

14. When the installation is finished, the **Next** button is enabled.

15. Click **Next**. The Finalization page displays.



Finalization

All requested actions for the Gimmal Compliance Suite have been performed.

Gimmal Compliance Suite Referential Integrity	Installed
Gimmal Compliance Suite Working With Records	Installed
Gimmal Compliance Suite Permission Reports	Installed
Gimmal Compliance Suite Email Management	Installed
Gimmal Compliance Suite Restricted Record Access	Installed
Gimmal Compliance Suite Vital Records	Installed
Gimmal Compliance Suite Cutoff	Installed
Gimmal Compliance Suite Disposition	Installed
Gimmal Compliance Suite Bulk Processing	Installed
Gimmal Compliance Suite Transfers	Installed
Gimmal Compliance Suite "As Of" Reporting	Installed
Gimmal Compliance Suite File Plan Builder	Installed
Gimmal Compliance Suite Search	Installed

Please check the installation log file located in the following location for any warnings or issues.
C:\Program Files (x86)\Gimmal Compliance Suite\Installer\logs\installation636808249643679606.log

Additional information may be found in the product help, administration and user guides.

Figure 3-12 Installer Finalization Page

16. If desired, click the installation log file link shown above, which enables you to view the log file generated as part of the installation process. The log file provides details on issues with feature installs that were unsuccessful.

17. When all Gimmal features are successfully installed, click **Finish**.

3.3 Deploying Bulk Task Processing

Bulk Task Processing is packaged with Compliance Suite, but must be separately deployed.

Follow these steps to deploy Bulk Task Processing:

1. Return to the Certified Records Management splash screen, described in section "3.2 Initiating the Installation Process" on page 7.

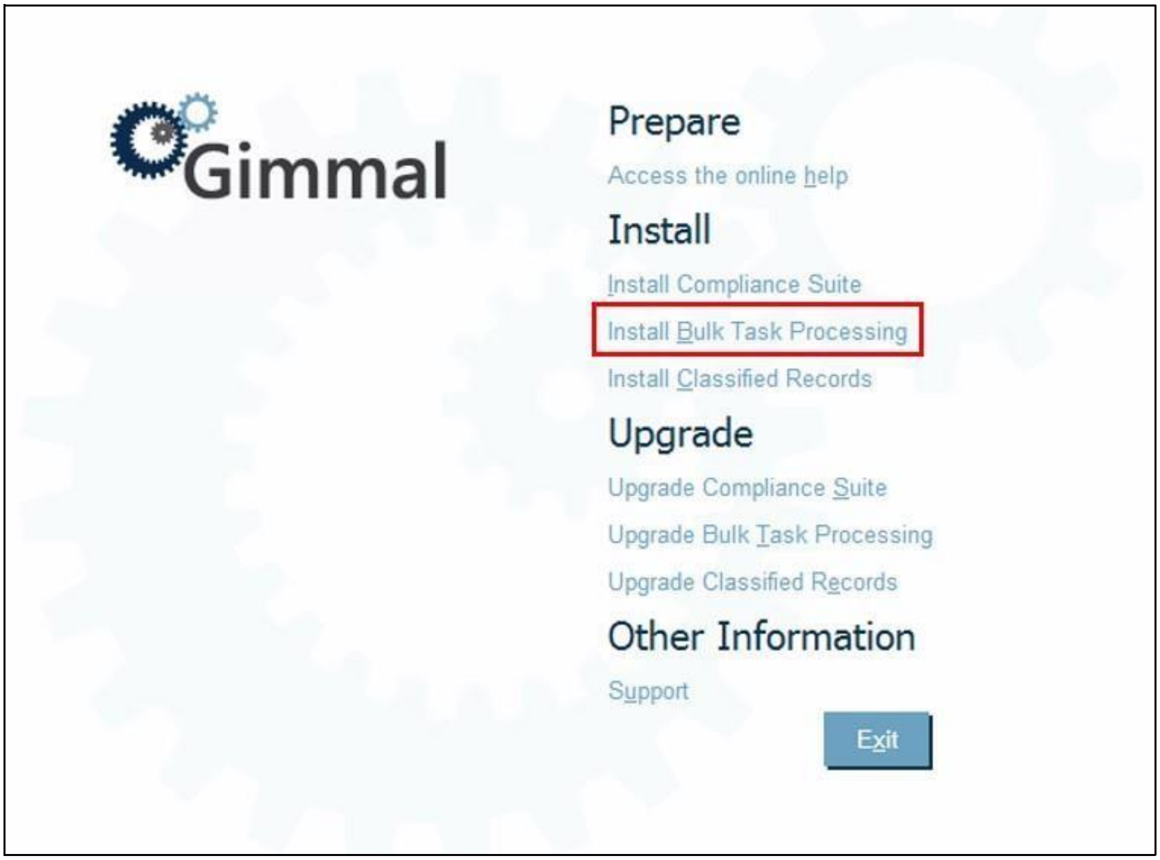


Figure 3-13 Certified Records Management Splash Screen

2. Click **Install Bulk Task Processing**. A Windows PowerShell opens and the .wsp file deploys automatically.

Note:

If the PowerShell window throws an error and closes, run PowerShell as Administrator, execute the command `Set-ExecutionPolicy Unrestricted`, and then click **Install Bulk Task Processing** again.

3. After the `.wsp` file deploys, Site Collection and Site features must be activated to enable Bulk Task Processing for every site collection where Compliance Suite is installed. You must first enable the Site Collection feature.
    a. From the root site where Compliance Suite has been installed, as a Site Collection Administrator, go to **Settings > Site settings > Site collection features** under the **Site Collection Administration** heading.
    b. Activate **Gimmal Compliance Suite - Bulk Task Processing Content Type**.

   c. You can now activate the site feature from **Settings > Site settings > Manage site features** under the **Site Actions** heading.

   d. Activate the following feature: **Gimmal Compliance Suite - Bulk Task Processing**.

4. The **Bulk Task Processing** button is now available on the Compliance Suite ribbon bar and is active when either the Disposition Tasks list or the Workflow Tasks list is selected.

5. Optional. You can activate the **Bulk Task Processing Settings** link in Central Administration. This link is only used if you have custom columns in the Disposition task list or the workflow task list.

   a. Launch Central Administration and select **Manage farm features** from **Farm Management** in **System Settings**.

   b. Activate the **Gimmal Compliance Suite - Bulk Task Processing** feature.

4 Performing Post-Installation Configuration Tasks

This chapter provides the procedures to configure Gimmal Compliance Suite after it is installed.

4.1 Managing Event Service Application

Note

The Event Service application is installed on the Central Administration server. If you want to run the Event Service on a different server, please contact Gimmal Support.

1. In Central Administration, click **Application Management**.
2. Click **Manage Service Applications**.
3. Select the **Gimmal Compliance Suite Event Management Service Application**.
4. Click **Administrators** and add the Records Management users who will need to add, modify, delete, and create Events.

   Administrators can also be added in the Event Management Service Application by clicking the **Gimmal Compliance Suite Event Management Service Application** link, and then clicking **Manage Administrators**. This list of administrators supports adding Claims identities for users in an ADFS environment. Both lists are respected by the application.

5. Select the check box and then click **Add**.
6. In the **Permissions** menu, select **Full Control**.
7. Click **OK**.
8. Click **Application Management**.
9. Navigate to **System Settings**, and click **Manage services on server**.
10. Locate **Gimmal Compliance Suite Event Management Service** and start it if it is not already running.

4.2 Managing Email Service Application

Note

The Email Service application is installed on the Central Administration server. If you want to run the Email Service on a different server, please contact Gimmal Support.

1. In **Central Administration**, click **Application Management**.
2. Click **Manage services** on server.
3. Locate **Gimmal Compliance Suite Email Management Service** and start it if it is not already running.

4.3 Accessing File Plan Builder

When the Cs installer has been run successfully with File Plan Builder selected, you must perform the following tasks to access it.

Note:

If you are installing in an ADFS environment, refer to “Installing Compliance Suite in an ADFS Environment” on page 32.

4.3.1 Activating File Plan Builder

You must activate File Plan Builder in SharePoint by following these steps.

1. Open your Records Center site and navigate to **Site Actions** and select **Site Settings**. Click **Manage site features** under **Site Actions**.
2. Locate and activate the **Gimmal Compliance Suite - File Plan Builder** feature.

4.3.2 Applying File Plan Builder Settings

To apply the File Plan Builder settings, perform the following steps:

1. Navigate to the Central Administration home page and click **File Plan Builder Settings** under the Compliance Suite category.

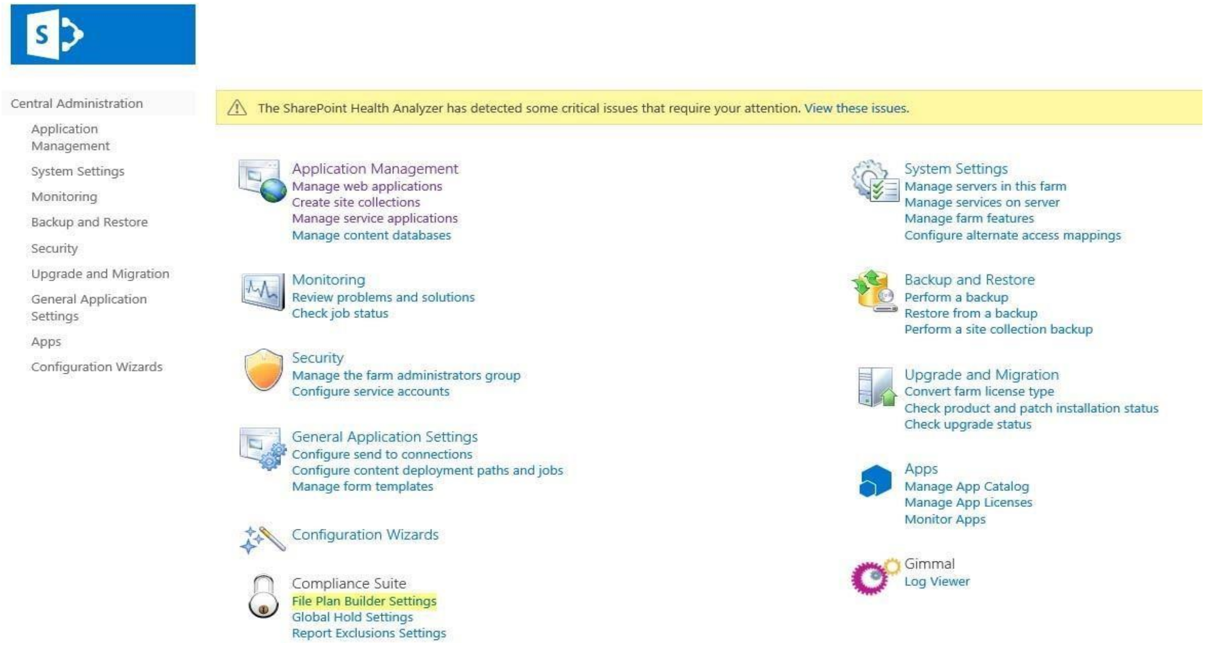

Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Apps
Configuration Wizards
The SharePoint Health Analyzer has detected some critical issues that require your attention. View these issues.
Application Management
Manage web applications
Create site collections
Manage service applications
Manage content databases
Monitoring
Review problems and solutions
Check job status
Security
Manage the farm administrators group
Configure service accounts
General Application Settings
Configure send to connections
Configure content deployment paths and jobs
Manage form templates
Configuration Wizards
Compliance Suite
File Plan Builder Settings
Global Hold Settings
Report Exclusions Settings
System Settings
Manage servers in this farm
Manage services on server
Manage farm features
Configure alternate access mappings
Backup and Restore
Perform a backup
Restore from a backup
Perform a site collection backup
Upgrade and Migration
Convert farm license type
Check product and patch installation status
Check upgrade status
Apps
Manage App Catalog
Manage App Licenses
Monitor Apps
Gimmal
Log Viewer

Figure 4-1 File Plan Builder Settings in Central Administration

2. Enter the following installation parameters:

Note

If you are performing a manual installation, a re-installation, or are moving File Plan Builder, you will need to select/enter these parameters. If you are performing a **new** installation using the installer, these parameters should already be set correctly and you simply need to verify the settings. See Figure 4-2 File Plan Builder Settings in SharePoint 2013/2016.

a. Enter the File Plan Builder Administrator user information. Do **not** a system account.

b. Enter the URL for the primary Record Center against which File Plan Builder will be installed.

c. In the **FPB Web Application Settings** section, enter the folder where the installation files will be installed. Gimmal recommends creating a folder in the C:\ or D:\ drive where there is enough empty disk space.

d. Ensure that the **Hostname** field has the correct fully qualified hostname for the WFE where File Plan Builder is installed. This field should point directly to the WFE where File Plan Builder is installed, not to a load-balancing URL. Note that the **Hostname** should **not** contain a port number or HTTP(S) prefix.

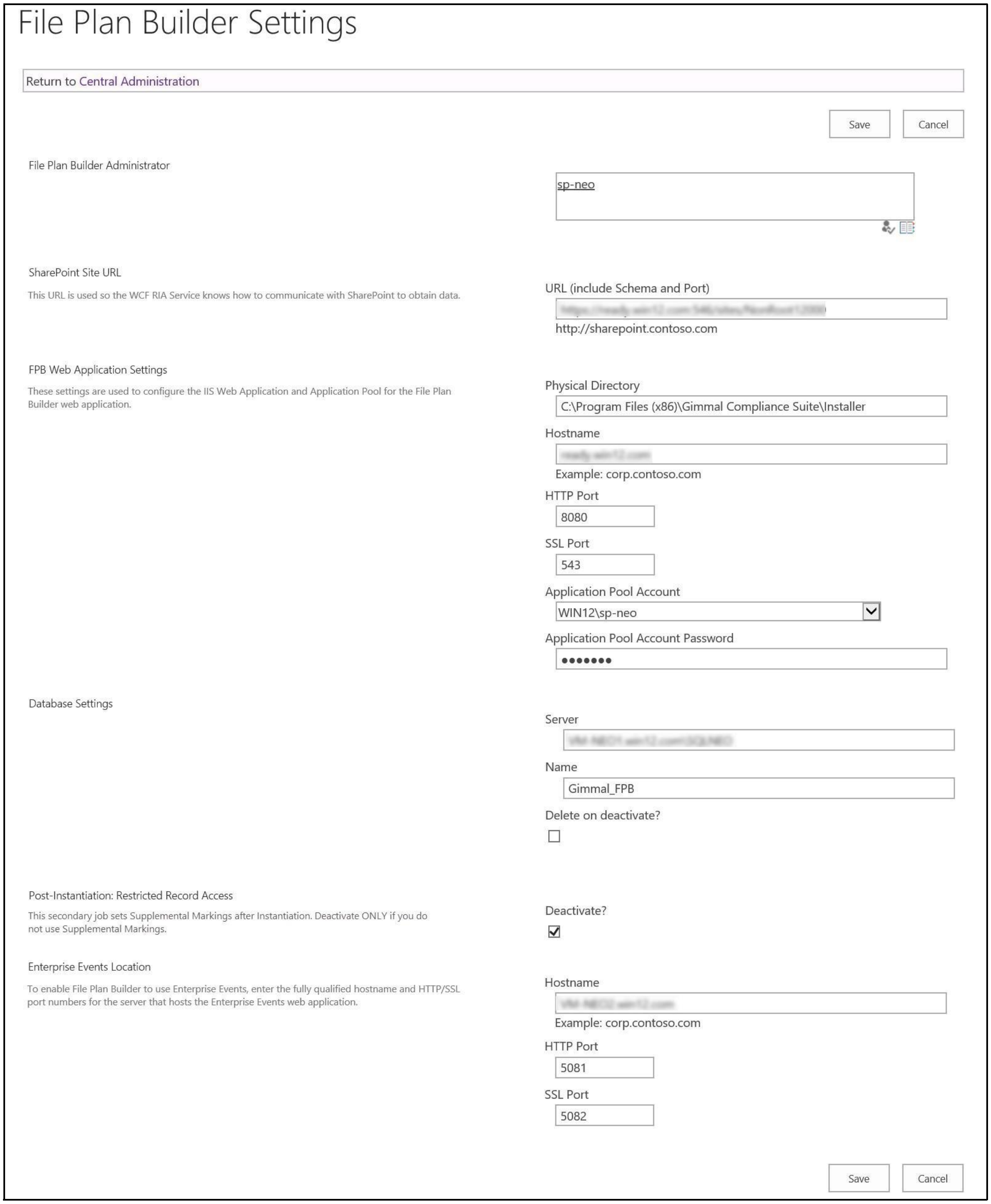
e. Enter the HTTP *Port* and *SSL Port* that the File Plan Builder web application should run on. This port should be available and should not be used by any other sites.

f. Select the *Application Pool Account* that the File Plan Builder web application should run under and enter the *Application Pool Account Password*.

g. In the **Database Settings** section, enter the hostname to the Database server.

h. Enter the database name for File Plan Builder. There is no restriction on the naming convention used for the File Plan Builder database in the Gimmal Compliance Suite solution.

i. Select the **Post Instantiation: Restricted Record Access** check box to enable a secondary job in support of Restricted Record Access. This is only required if using Supplemental Markings. If you are not using Supplemental Markings, do not select.



File Plan Builder Settings

Return to Central Administration

File Plan Builder Administrator

sp-neo

SharePoint Site URL

This URL is used so the WCF RIA Service knows how to communicate with SharePoint to obtain data.

URL (include Schema and Port)

[redacted]

http://sharepoint.contoso.com

FPB Web Application Settings

These settings are used to configure the IIS Web Application and Application Pool for the File Plan Builder web application.

Physical Directory

C:\Program Files (x86)\Gimmal Compliance Suite\Installer

Hostname

[redacted]

Example: corp.contoso.com

HTTP Port

8080

SSL Port

543

Application Pool Account

WIN12\sp-neo

Application Pool Account Password

●●●●●●●

Database Settings

Server

[redacted]

Name

Gimmal_FPB

Delete on deactivate?

☐

Post-Instantiation: Restricted Record Access

This secondary job sets Supplemental Markings after Instantiation. Deactivate ONLY if you do not use Supplemental Markings.

Deactivate?

☑

Enterprise Events Location

To enable File Plan Builder to use Enterprise Events, enter the fully qualified hostname and HTTP/SSL port numbers for the server that hosts the Enterprise Events web application.

Hostname

[redacted]

Example: corp.contoso.com

HTTP Port

5081

SSL Port

5082

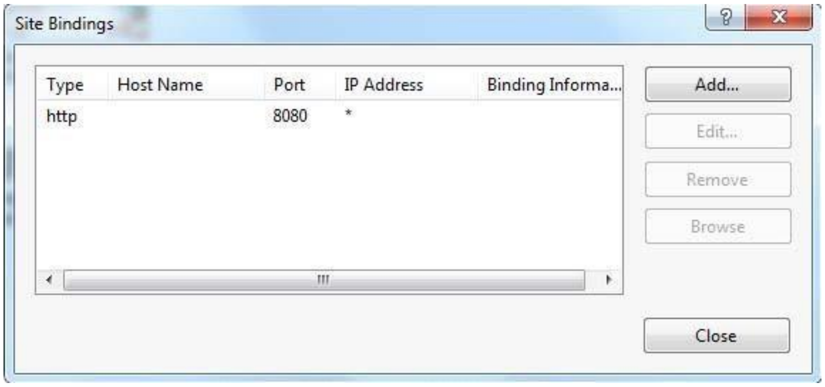
Figure 4-2 File Plan Builder Settings in SharePoint 2013/2016

j. Click **Save**.

4.3.3 Setting up SSL Bindings for File Plan Builder Site

If your installation is using SSL, set up SSL bindings for the File Plan Builder site:

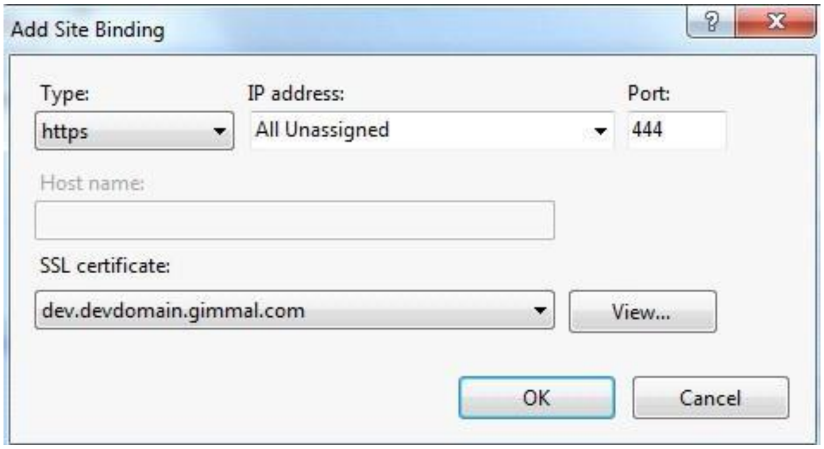
1. Open the IIS Manager from your WFE server and locate the FilePlanBuilder site. Right-click on it and select **Edit Bindings**. The **Site Binding** dialog box displays.



Type	Host Name	Port	IP Address	Binding Informa...
http		8080	*	

Figure 4-3 Site Bindings Dialog Box

2. Click **Add**. The **Add Site Binding** dialog box displays.



Type: https

IP address: All Unassigned

Port: 444

Host name:

SSL certificate: dev.devdomain.gimmal.com

Figure 4-4 Add a Site Binding Dialog Box

3. Select **Type https**, enter the same **Port** as specified in the File Plan Builder settings in step 10f in 3.2 Initiating the Installation Process, select an **SSL certificate** from the menu that is valid for the File Plan Builder site.
4. Click **OK**.

4.3.4 Verifying Windows Authentication

As a best practice, after you install Compliance Suite and activate File Plan Builder, but **before** File Plan Builder is launched through the browser, you must verify that Windows authentication is configured to use the application pool account.

1. Open the IIS Manager from your Web front end server.
2. Select the **FilePlanBuilder** site from the list of **Sites** in the left pane.

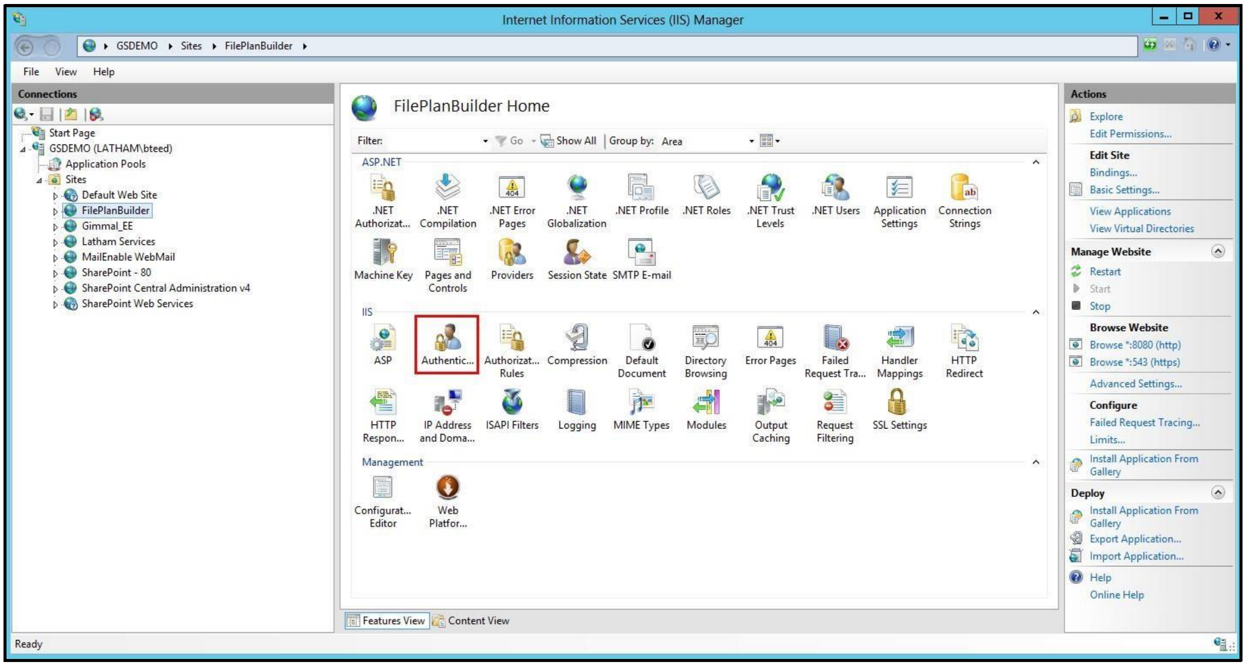
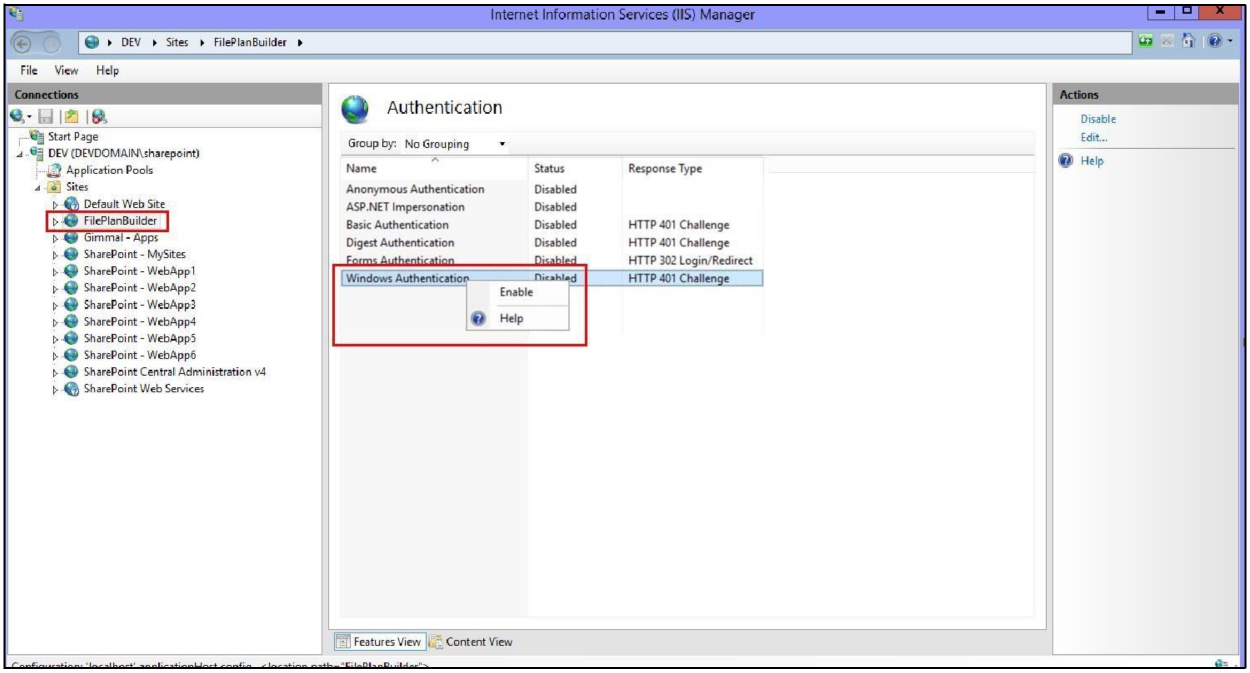


Figure 4-5 Authentication Button in IIS settings

3. Double-click the **Authentication** button in the **IIS** settings section.
4. To enable Windows authentication, right-click on the **Windows Authentication** button and select the **Enable** option from the context menu. The Status changes to "Enabled."



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Figure 4-6 Authentication Method Enabled

4.3.5 Adding Users to Groups

Add users to groups to access File Plan Builder.

1. Open the Records Center site and navigate to **Site Actions/Site Settings**. For SharePoint, click **Settings** and then click **Site Settings**.
2. Click **People and Groups** under **Users and Permissions**.
3. Click the **File Plan Builder Users** group and add the Records Management users that have access to use File Plan Builder.

Note:

Be sure these users are also part of the default SharePoint group members or owners (normally Records Administrators fall into this group).

4.3.6 Launching File Plan Builder

In SharePoint 2013/2016/2019, you have several options to launch File Plan Builder:

- ⋆ Activate the Gimmal Ribbon Navigation feature (select **Settings, Site Settings,** and then **Site Features**). File Plan Builder displays as a button when you select the Compliance Suite navigation tab. Click **File Plan Builder**.
- ⋆ Click **Settings,** click **Site Settings,** and then click the **File Plan Builder** link under the **Compliance Suite** section.
- ⋆ Manually add the link for File Plan Builder under **Navigation** in the **Site Settings Look and Feel** section. Click the link to launch File Plan Builder.

When using **Alternate Access Mappings** where the domain name differs from the domain name of the File Plan Builder Web Application, set the following in Internet Explorer:

1. Launch Internet Explorer and open **Internet Options**.
2. Click the **Security** tab.
3. Select **Local Intranet**.
4. Click the **Sites** button.
5. Click **Advanced**.
6. Enter the URL of the AAM SharePoint site name in **Add this website to the zone**; then click **Add**.

7. Click **Close**.
8. Click **OK** and then click **OK** again.

4.4 Setting Up Localization

Localization enables Compliance Suite to be presented in a Multilanguage User Interface (MUI) using SharePoint 2013/2016/2019. Localization currently supports only the French Canadian language. The Gimmal language pack installs with Compliance Suite.

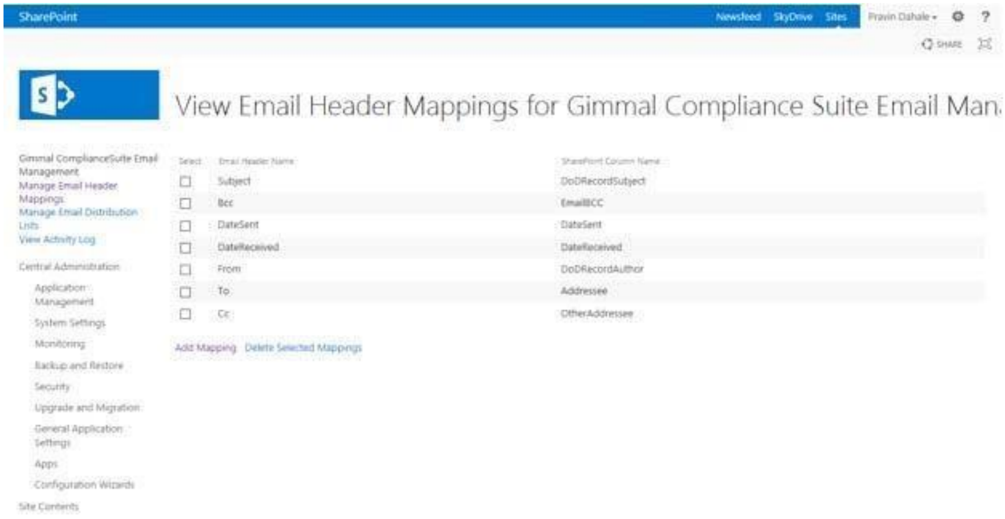
To use Localization, you must set the desired language so that it displays in the desired SharePoint site, in your personal settings, and in the browser. See the following article for information about multilingual SharePoint 2013/2016/2019 sites: http://technet.microsoft.com/en-us/library/cc262055(v=office.15).aspx

4.4.1 Configuring Email Mapping

You must change the Compliance Suite email mapping configuration to use internal names instead of display names.

Follow these steps to change the email mapping:

1. Navigate to Gimmal Compliance Suite Email Management.
2. Select **Manage Email Header Mappings**.



View Email Header Mappings for Gimmal Compliance Suite Email Man

Select	Email Header Name	SharePoint Column Name
□	Subject	DoDRecordSubject
□	Bcc	EmailBCC
□	DateSent	DateSent
□	DateReceived	DateReceived
□	From	DoDRecordAuthor
□	To	Addressee
□	Cc	OtherAddressee

Figure 4-7 View Email Header Mappings for Gimmal Compliance Suite Email Management Page

3. Change the configuration to use internal names instead of display names.

4.5 Activating Compliance Suite Ribbon Navigation for 2013/ 2016/2019

Although it is not required, you can activate the Compliance Suite ribbon navigation that installed with Common for easier access to Compliance Suite features in SharePoint 2013/2016/2019.

Follow these steps to activate the ribbon:

1. Go to **Settings,** select **Site Settings,** select **Site Actions**, and then select **Manage site features**.
2. Scroll down to **Gimmal - Ribbon Navigation**.
3. Click **Activate** to the right.
4. When you navigate to the SharePoint Records Center where Compliance Suite is installed, you can access Cs features via the ribbon.

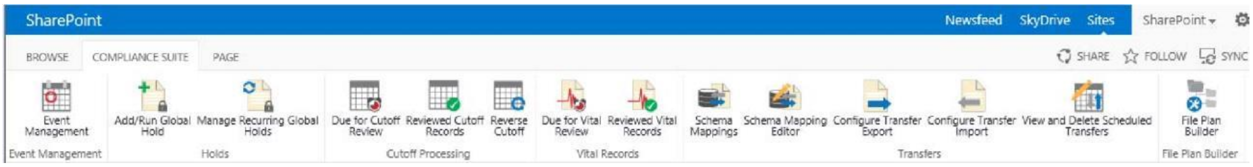


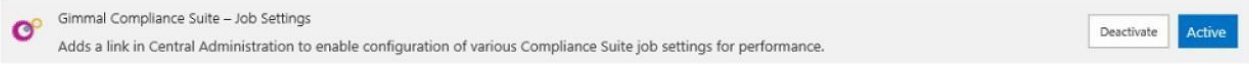
Figure 4-8 Compliance Suite Access via Ribbon

4.6 Activating Compliance Suite Job Configuration

The feature Compliance Suite Job Settings provides a way for users to manage Compliance Suite job configuration. This is a farm feature that, once activated, provides a link in the Compliance Suite section of Central Administration.

To activate the Compliance Suite Job Configuration feature, follow these steps.

1. When the package is deployed, navigate to **System Settings** and select **Manage Farm Features** in Central Administration.


Gimmal Compliance Suite – Job Settings

Adds a link in Central Administration to enable configuration of various Compliance Suite job settings for performance.

Figure 4-9 Activating Job Settings Feature in Central Administration

2. Click **Activate** for the **Gimmal Compliance Suite - Job Settings**. Now a **Job Settings** option is available in the Compliance Suite section of Central Administration.

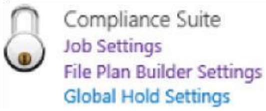
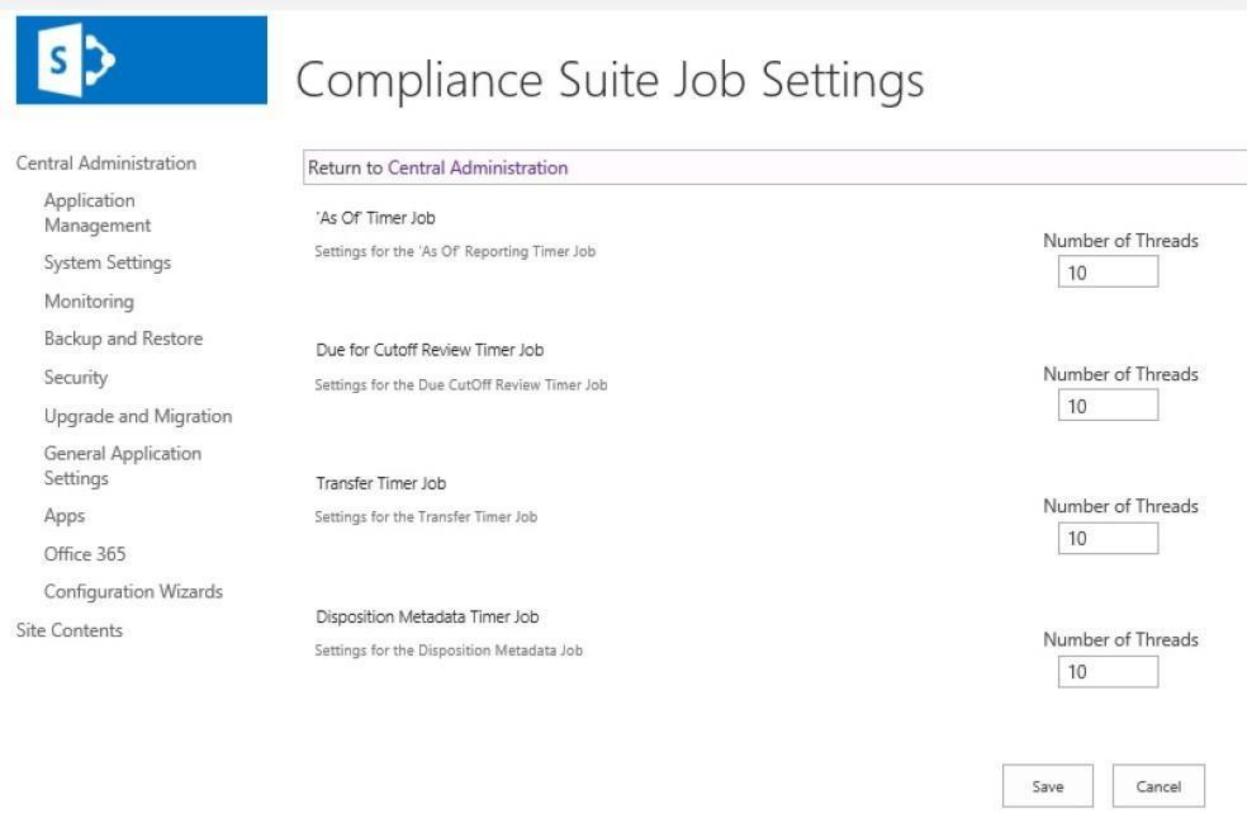


Figure 4-10 Job Settings Option in Compliance Suite Menu

3. Click **Job Settings** to display the view to set the number of threads for the jobs.



Compliance Suite Job Settings

'As Of' Timer Job

Settings for the 'As Of' Reporting Timer Job

Number of Threads: 10

Due for Cutoff Review Timer Job

Settings for the Due CutOff Review Timer Job

Number of Threads: 10

Transfer Timer Job

Settings for the Transfer Timer Job

Number of Threads: 10

Disposition Metadata Timer Job

Settings for the Disposition Metadata Job

Number of Threads: 10

Figure 4-11 Setting Number of Threads for Jobs

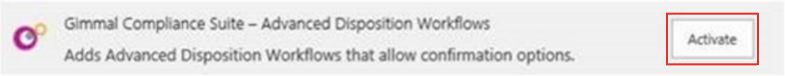
4. Set the number of threads for each job.
   - The default value is 10.
   - If you set the value for 0 or less, the system will automatically default to 10 again.
   - When the job runs, it processes items in a multi-threading fashion using the configured number of threads. Thus, if the thread count is set to 10, it will process 10 items (tasks) simultaneously instead of a single item or task.
   - Thread count is adjusted to optimize performance. *Within reason*, more threads equate to faster performance. There is no *right* number, and *within reason* depends on the environment. As the number of threads increase, more system resources are consumed, so there is an upper limit. The optimal number for any system can only be found by trial and error.
5. Click **Save**.

4.7 Activating Advanced Workflows

The advanced workflows must be activated before users can use them. For more information about these optional workflows, see "Compliance Suite Disposition Workflows" in the *Compliance Suite User Guide*.

To activate the advanced workflows, follow these steps.

1. As a Site Collection Administrator where Compliance Suite is installed, click the **Settings** button, select **Site settings**, and then select **Site collection features**.



Gimmal Compliance Suite – Advanced Disposition Workflows
Adds Advanced Disposition Workflows that allow confirmation options.

Figure 4-12 Activating Advanced Workflows in Central Administration

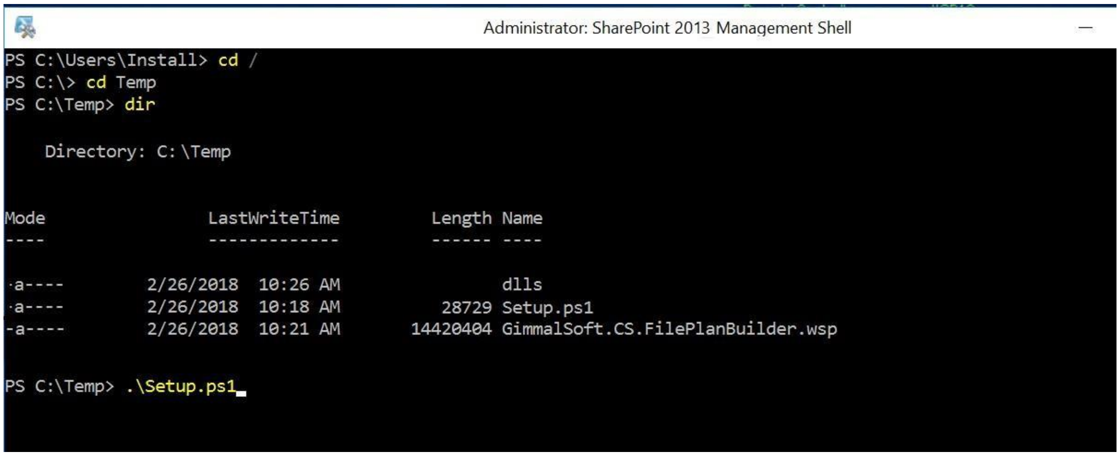
2. Click **Activate** for the **Gimmal Compliance Suite - Advanced Disposition Workflows**.

5 Installing Compliance Suite in an ADFS Environment

All Gimmal Compliance Suite components in an Active Directory Federation Services (ADFS) system are installed in the same manner as the NT LAN Manager (NTLM) environment with the exception of the File Plan Builder component.

To install Compliance Suite in an ADFS environment, follow these steps.

1. Follow the instructions in the "Installing Compliance Suite" chapter except that in Step 8 of Section 3.2, "Initiating the Installation Process" on page 7, deselect the **Gimmal Compliance Suite File Plan Builder** check box.
2. In "Performing Post-Installation Configuration Tasks", do **NOT** perform the File Plan Builder settings steps in "Accessing File Plan Builder".
3. When all components are installed except File Plan Builder, follow these steps to install File Plan Builder in an ADFS environment.
   a. Download the Upgrade packages for the version you are installing from the download site.
   b. Extract the files to a directory on the WFE.
   c. Navigate to the **Upgrade** directory and copy the following to a temporary folder:
      - `Setup.ps1`
      - `GimmalSoft.Cs.FilePlanBuilder.wsp`
      - dlls folder
   d. Open the **SharePoint 2013/2016/2019 Management Shell** as administrator, navigate to the temporary folder you created, and run `Setup.ps1`. This PowerShell script adds or upgrades all packages in the current directory to SharePoint's solution store. Alternatively, if you are familiar with the Add-SPSolution command, you can use it to add the package to SharePoint's solution store.



```
PS C:\Users\Install> cd /
PS C:\> cd Temp
PS C:\Temp> dir

    Directory: C:\Temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----

-a----        2/26/2018  10:26 AM                dlls
-a----        2/26/2018  10:18 AM          28729 Setup.ps1
-a----        2/26/2018  10:21 AM       14420404 GimmalSoft.CS.FilePlanBuilder.wsp


PS C:\Temp> .\Setup.ps1
```

Figure 5-1 Running Setup.ps1 Script in SharePoint 2013 Management Shell

e. Navigate to the Central Administration home page and click **System Settings**. Select **Manage Farm Solutions**.

4. Click `gimmalsoft.cs.fileplanbuilder.wsp`, select **deploy solution** on the following page, and click **OK**.
5. When the package is deployed, navigate to **System Settings** and select **Manage Farm Features** in Central Administration and activate the **Gimmal Compliance Suite - File Plan Builder Settings Editor**.
6. Navigate to the Central Administration home page and click **File Plan Builder Settings** under the Compliance Suite category.

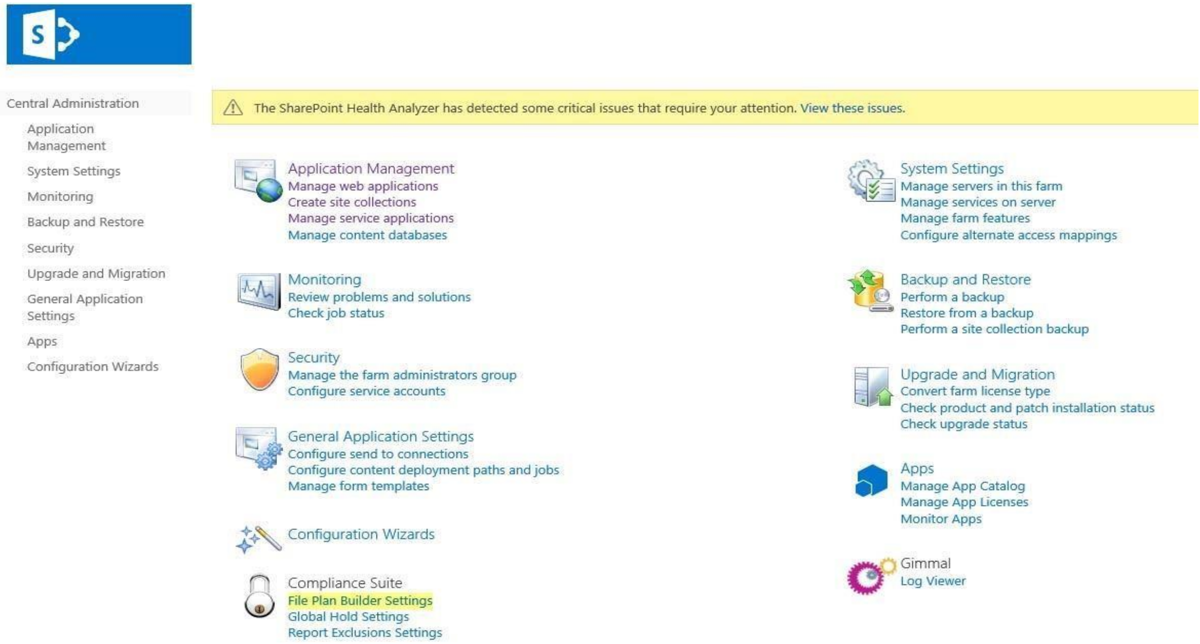

Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Apps
Configuration Wizards
The SharePoint Health Analyzer has detected some critical issues that require your attention. View these issues.
Application Management
Manage web applications
Create site collections
Manage service applications
Manage content databases
Monitoring
Review problems and solutions
Check job status
Security
Manage the farm administrators group
Configure service accounts
General Application Settings
Configure send to connections
Configure content deployment paths and jobs
Manage form templates
Configuration Wizards
Compliance Suite
File Plan Builder Settings
Global Hold Settings
Report Exclusions Settings
System Settings
Manage servers in this farm
Manage services on server
Manage farm features
Configure alternate access mappings
Backup and Restore
Perform a backup
Restore from a backup
Perform a site collection backup
Upgrade and Migration
Convert farm license type
Check product and patch installation status
Check upgrade status
Apps
Manage App Catalog
Manage App Licenses
Monitor Apps
Gimmal
Log Viewer

Figure 5-2 File Plan Builder Settings in SharePoint 2013/2016

7. Enter the following installation parameters:

   a. Enter the File Plan Builder Administrator user information.

   b. Select the site collection where you want File Plan Builder to be installed.

   c. Select the folder where the installation files will be installed, Gimmal recommends creating a folder in the C:\ or D:\ drive where there is enough empty disk space.

   d. Enter the URL where you'd like to host the File Plan Builder RIA services web application, not including the scheme (no http:// or https://, just the FQDN).

   e. Enter the *Port* and *SSL Port* that the File Plan Builder web application should run on. This port should be available and should not be used by any other sites.

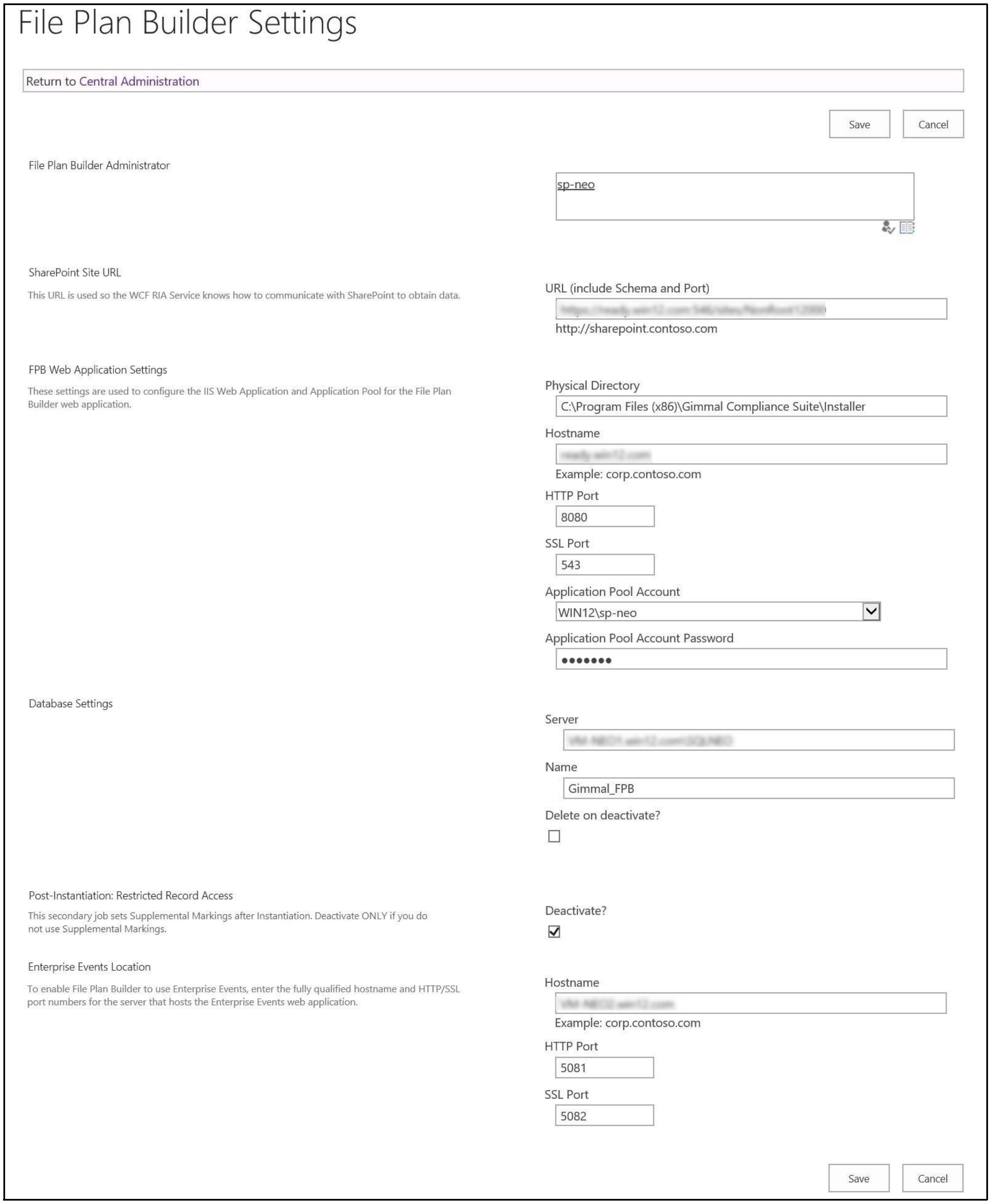
   f. Select the *Application Pool Account* that the File Plan Builder web application should run under and enter the *Application Pool Account Password*.

   g. Enter the URL to the ADFS server, including https://.

   h. Enter the Fully Qualified Domain name of your Database server instance.

   i. Enter the *Deployment Database Name* for File Plan Builder. There is no restriction on the naming convention used for the File Plan Builder database in the Gimmal Compliance Suite solution.

   j. Indicate whether you want to activate/deactivate *Post-Instantiation: Restricted Record Access*.



File Plan Builder Settings

Return to Central Administration

File Plan Builder Administrator

sp-neo

SharePoint Site URL

This URL is used so the WCF RIA Service knows how to communicate with SharePoint to obtain data.

URL (include Schema and Port)

[redacted]

http://sharepoint.contoso.com

FPB Web Application Settings

These settings are used to configure the IIS Web Application and Application Pool for the File Plan Builder web application.

Physical Directory

C:\Program Files (x86)\Gimmal Compliance Suite\Installer

Hostname

[redacted]

Example: corp.contoso.com

HTTP Port

8080

SSL Port

543

Application Pool Account

WIN12\sp-neo

Application Pool Account Password

●●●●●●●

Database Settings

Server

[redacted]

Name

Gimmal_FPB

Delete on deactivate?

☐

Post-Instantiation: Restricted Record Access

This secondary job sets Supplemental Markings after Instantiation. Deactivate ONLY if you do not use Supplemental Markings.

Deactivate?

☑

Enterprise Events Location

To enable File Plan Builder to use Enterprise Events, enter the fully qualified hostname and HTTP/SSL port numbers for the server that hosts the Enterprise Events web application.

Hostname

[redacted]

Example: corp.contoso.com

HTTP Port

5081

SSL Port

5082

Figure 5-3 File Plan Builder Settings in SharePoint 2013/2016

k. Click **Save**.

8. Navigate to **System Settings** and select **Manage Farm Features** in the Central Administration site. Activate **Gimmal Compliance Suite - File Plan Builder**.

9. Verify the successful install by checking:

a. Did the Web Application files extract? Check the physical directory that you entered in **Settings**.

b. Were the IIS Site and App Pool created? Check the IIS Manager.

c. Did the database provision? Check SQL Server Management Studio (SSMS) to see if the database name you entered in **Settings** now exists.

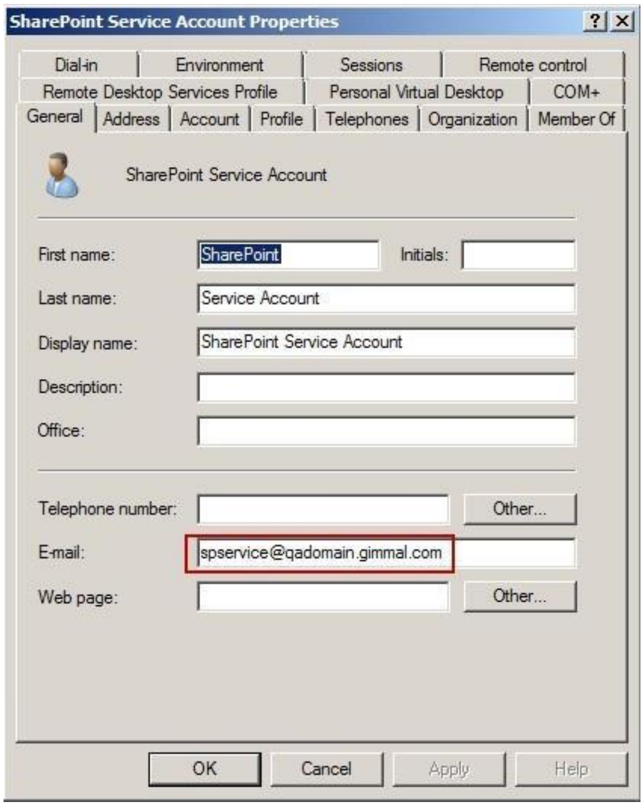
d. Is the app pool account on your web application the same as entered? Check **App Pool** in IIS Manager.

10. Open your Records Center site and navigate to **Site Actions** and select **Site Settings**. Click **Manage site features** under **Site Actions**.

11. Locate and activate the **Gimmal Compliance Suite - File Plan Builder** feature.

12. Follow the post installation steps for “Accessing File Plan Builder” on page 21 to create a binding for SSL and add users for File Plan Builder site access.

13. Ensure that the app pool account configured in Step 6a has an email address in the Active Directory.



SharePoint Service Account

First name: SharePoint
Initials:
Last name: Service Account
Display name: SharePoint Service Account
Description:
Office:

Telephone number:
E-mail: spservice@qadomain.gimmal.com
Web page:

Figure 5-4 Application Pool Account

14. Enable WS-Trust 1.3 for ADFS 2.0.

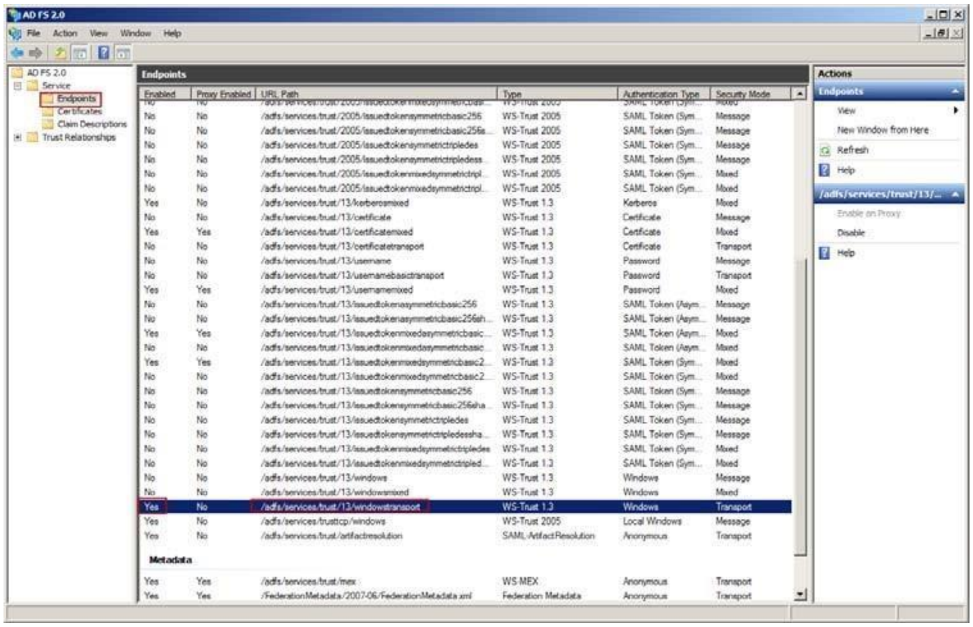
a. Open **AD FS 2.0**.

b. Expand **Service**.

c. Select **Endpoints**.

d. Select **/adfs/services/trust/13/windowstransport**.

e. Click **Enable** on the right tool pane.



Endpoints

Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasi...	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256s...	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledess...	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl...	WS-Trust 2005	SAML Token (Sym...	Mixed
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos	Mixed
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport
No	No	/adfs/services/trust/13/username	WS-Trust 1.3	Password	Message
No	No	/adfs/services/trust/13/usernamebasictransport	WS-Trust 1.3	Password	Transport
Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3	Password	Mixed
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Message
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh...	WS-Trust 1.3	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic...	WS-Trust 1.3	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic2...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha...	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripled...	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
Yes	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005	Local Windows	Message
Yes	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Metadata					
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport

Figure 5-5 Enabling WS-Trust

f. Expand **Trust Relationships**.

g. Select **Relying Party Trusts**.

h. Right-click on the **ADFS Site URL** that you want to configure and click **Properties**.

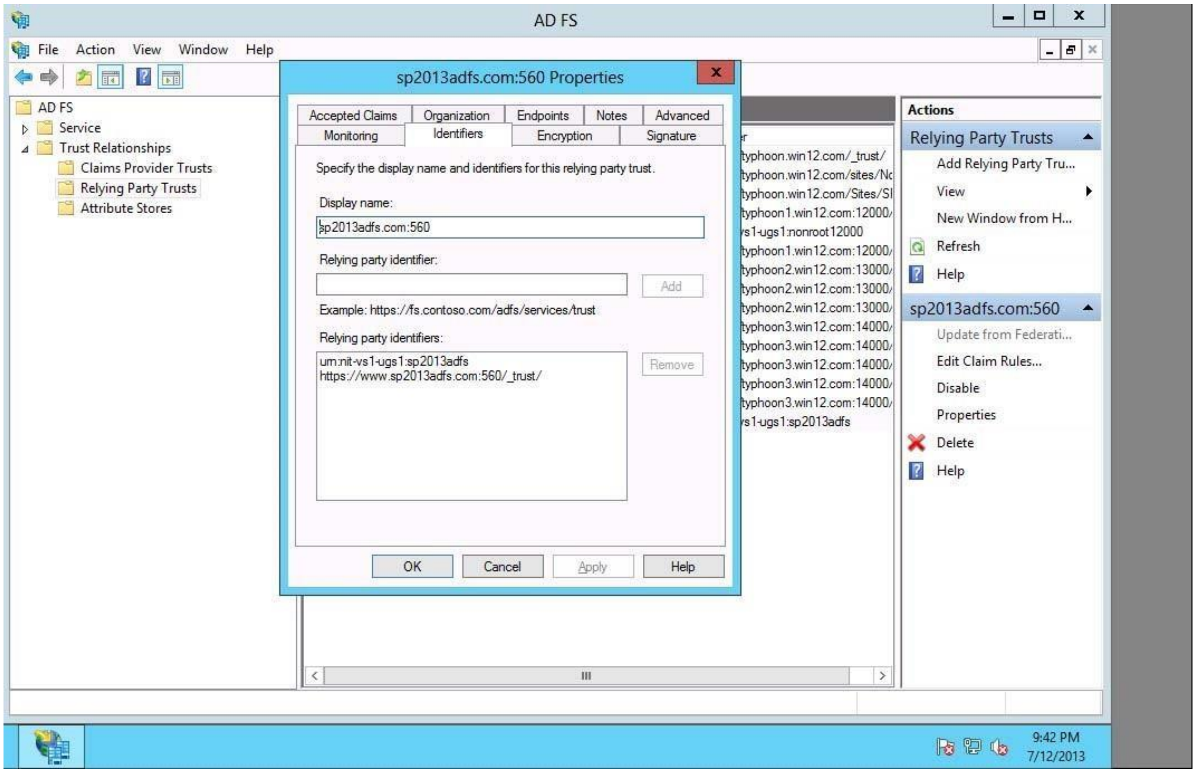
This is an entry in **Relying Party Trusts** for the Record Center Site where you are installing Compliance Suite.

i. Navigate to **Identifiers** tab.

j. Add the **Site URL** for the Records Center site where you are activating File Plan Builder to the Relying Party Identifier list box. The format should be *SiteURL/_trust/*. Be sure to include the ending forward slash after "trust"). For example:

https://www.sp2013adfs.com/_trust/

k. Click **Add.**



AD FS
File Action View Window Help
AD FS
Service
Trust Relationships
Claims Provider Trusts
Relying Party Trusts
Attribute Stores
typhoon.win12.com/_trust/
typhoon.win12.com/sites/Nc
typhoon.win12.com/Sites/SI
typhoon1.win12.com:12000/
s1-ugs1:nonroot12000
typhoon1.win12.com:12000/
typhoon2.win12.com:13000/
typhoon2.win12.com:13000/
typhoon2.win12.com:13000/
typhoon3.win12.com:14000/
typhoon3.win12.com:14000/
typhoon3.win12.com:14000/
typhoon3.win12.com:14000/
typhoon3.win12.com:14000/
s1-ugs1:sp2013adfs
Actions
Relying Party Trusts
Add Relying Party Tru...
View
New Window from H...
Refresh
Help
sp2013adfs.com:560
Update from Federati...
Edit Claim Rules...
Disable
Properties
Delete
Help
9:42 PM
7/12/2013

sp2013adfs.com:560 Properties

Accepted Claims | Organization | Endpoints | Notes | Advanced | Monitoring | Identifiers | Encryption | Signature

Specify the display name and identifiers for this relying party trust.

Display name:
sp2013adfs.com:560

Relying party identifier:

Add

Example: https://fs.contoso.com/adfs/services/trust

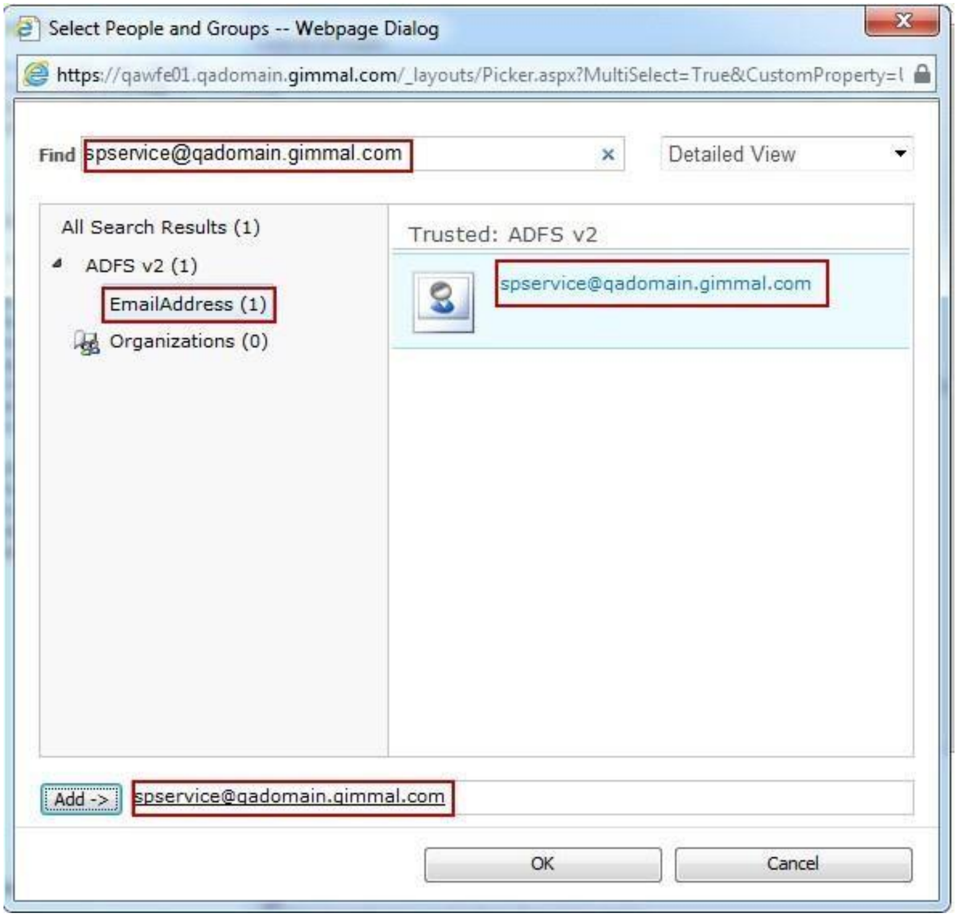
Relying party identifiers:
urn:nit-vs1-ugs1:sp2013adfs
https://www.sp2013adfs.com:560/_trust/

Remove

OK Cancel Apply Help

Figure 5-6 Adding File Plan Builder Site URL to Relying Identifier List

15. Ensure that the app pool account specified in Step 6f has read access to the **Relationship Types** list in your Record Center site.



Select People and Groups -- Webpage Dialog

https://qawfe01.qadomain.gimmal.com/_layouts/Picker.aspx?MultiSelect=True&CustomProperty=l

Find spservice@qadomain.gimmal.com

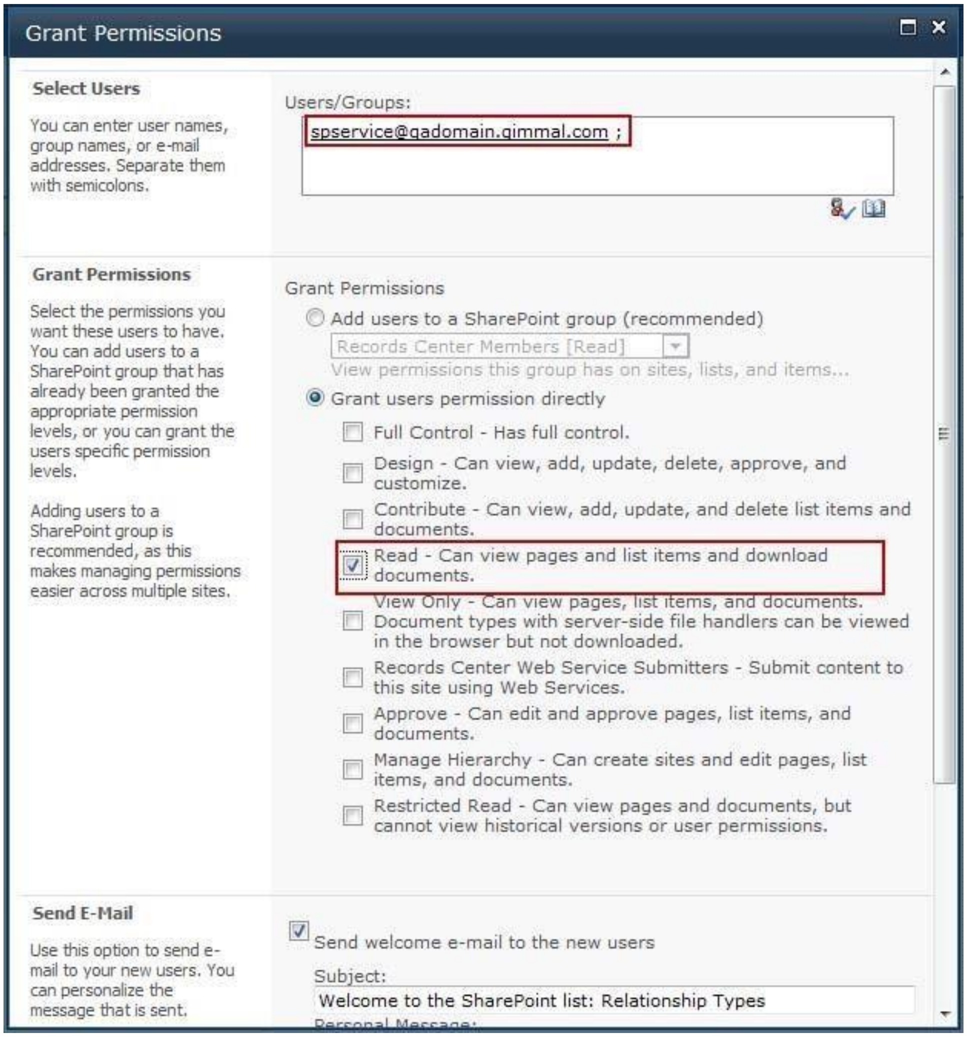
Trusted: ADFS v2

spservice@qadomain.gimmal.com

Add -> spservice@qadomain.gimmal.com

Figure 5-7 Relationship Types

16. Click **OK**.



Grant Permissions

Select Users

You can enter user names, group names, or e-mail addresses. Separate them with semicolons.

Users/Groups: spservice@qadomain.gimmal.com ;

Grant Permissions

Select the permissions you want these users to have. You can add users to a SharePoint group that has already been granted the appropriate permission levels, or you can grant the users specific permission levels.

Adding users to a SharePoint group is recommended, as this makes managing permissions easier across multiple sites.

Grant Permissions

○ Add users to a SharePoint group (recommended)

Records Center Members [Read]

View permissions this group has on sites, lists, and items...

● Grant users permission directly

- □ Full Control - Has full control.
- □ Design - Can view, add, update, delete, approve, and customize.
- □ Contribute - Can view, add, update, and delete list items and documents.
- ☑ Read - Can view pages and list items and download documents.
- □ View Only - Can view pages, list items, and documents. Document types with server-side file handlers can be viewed in the browser but not downloaded.
- □ Records Center Web Service Submitters - Submit content to this site using Web Services.
- □ Approve - Can edit and approve pages, list items, and documents.
- □ Manage Hierarchy - Can create sites and edit pages, list items, and documents.
- □ Restricted Read - Can view pages and documents, but cannot view historical versions or user permissions.

Send E-Mail

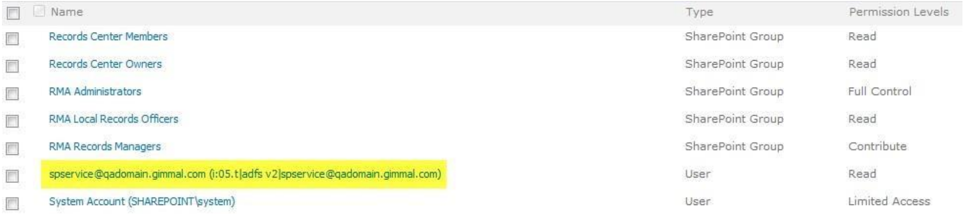
Use this option to send e-mail to your new users. You can personalize the message that is sent.

☑ Send welcome e-mail to the new users

Subject: Welcome to the SharePoint list: Relationship Types

Personal Message:

Figure 5-8 Grant Permissions



□	Name	Type	Permission Levels
□	Records Center Members	SharePoint Group	Read
□	Records Center Owners	SharePoint Group	Read
□	RMA Administrators	SharePoint Group	Full Control
□	RMA Local Records Officers	SharePoint Group	Read
□	RMA Records Managers	SharePoint Group	Contribute
□	spservice@qadomain.gimmal.com (i:05.t|adfs v2|spservice@qadomain.gimmal.com)	User	Read
□	System Account (SHAREPOINT\system)	User	Limited Access

Figure 5-9 Updated Permissions

6 Describing Compliance Suite Features and Dependencies

This section describes the features added by the Gimmal Compliance Suite installer and the internal dependencies between features and solutions.

1. Common
    a. Installs **Gimmal - Common** at farm level.
    b. Installs **Gimmal - Ribbon Navigation** at web level.
2. Record Core
    a. Installs **Gimmal - Record Core - Site Content Types** at site collection level. Dependent on 1: Common.
3. Compliance Suite Common
    a. Installs **Gimmal Compliance Suite - Common** at farm level. Dependent on 1: Common.
    b. Installs **Gimmal Compliance Suite - Base Content Types** at site collection level. Dependent on 1: Common and 2: Record Core. The installing and activating user(s) must have the role of a term store administrator under the Managed Metadata Service (https://technet.microsoft.com/en-us/library/mt683863(v=office.16).aspx).
    c. Installs **Gimmal Compliance Suite - Security Configuration** at site collection level. Dependent on 3: Compliance Suite Common (a) and SharePoint Server Publishing Infrastructure.

Note:

Search Service Application is a requirement for Compliance Suite Common to be activated. Navigate to **Central Administration > Application Management > Configure service application associations > (your web app)** to make sure that **Search Service Application** is selected.

4. Event Management Service
    a. Installs **Gimmal Compliance Suite - Event Management Service Installer** at farm level. Dependent on 1: Common.
    b. Installs **Gimmal Compliance Suite - Event Management** at web level. Dependent on 1: Common and 4 (a).
5. Period Management
    a. Installs **Gimmal Compliance Suite - Period Management** at site collection level. Dependent on 1: Common and 3: Compliance Suite Common (c).
6. Record Relationships

   a. Installs **Gimmal Compliance Suite - Record Relationship Content Types** at site collection level. Dependent on 1: Common, 3: Compliance Suite Common (c), and the Document ID Service.
   b. Installs **Gimmal Compliance Suite - Record Relationship Functionality** at web level and is dependent on 3: Compliance Suite Common (a) and 6: Record Relationships (a).
   c. Installs **Gimmal Compliance Suite - Restricted Records Cleanup Timer Job** at web application level.

7. Working With Records
   a. Installs **Gimmal Compliance Suite - Working with Records Site Columns** at site collection level. Dependent on 3: Compliance Suite Common.
   a. Installs **Gimmal Compliance Suite - Working with Records** at web level. This depends on 6: Record Relationships, 3: Compliance Suite Common, and 7 (a).
8. Restricted Record Access
   a. Installs **Gimmal Compliance Suite - Restricted Record Access Content Types** at site collection level. Dependent on 3: Compliance Suite Common (a and b).
   b. Installs **Gimmal Compliance Suite - Restricted Record Access** at web level. Dependent on 3: Compliance Suite Common and 8 (a).
9. Referential Integrity
   a. Installs **Gimmal Compliance Suite - Referential Integrity** at web application level. Dependent on 3: Compliance Suite Common (a),
   b. Adds **Compliance Suite Referential Integrity Synchronizatio**n timer job.
10. Alerts
    a. Installs **Gimmal Compliance Suite - Alert Content Types** at site collection level. Dependent on 3: Compliance Suite Common (a).
    b. Installs **Gimmal Compliance Suite - Alerts and Notification** at web level. Dependent on 3: Compliance Suite Common (a and c) and 10 (a).
11. Holds
    a. Installs **Gimmal Compliance Suite - Holds Infrastructure** at farm level. No dependencies.
    b. Installs **Gimmal Compliance Suite - Holds Site Columns** at site collection level. No dependencies.

   c. Installs **Gimmal Compliance Suite - Holds Management** at web level. Dependent on 3: Compliance Suite Common (a), and 11 (a and b).

12. User Permissions Reports

    a. Installs **Gimmal Compliance Suite - User Permission Reports** at web level. Dependent on 3: Compliance Suite Common (a).

13. Metadata Editing

    a. Installs **Gimmal Compliance Suite - Metadata Editing** at web level.

14. Vital Records

    a. Installs **Gimmal Compliance Suite - Vital Records Content Types** at site collection level. Dependent on 3: Compliance Suite Common (a).

    b. Installs **Gimmal Compliance Suite - Vital Records Management** at web level. Dependent on 3: Compliance Suite Common, 5: Period Management, and 14 (a).

    c. Installs **Gimmal Compliance Suite - Vital Records Timer Job** at web application level. Dependent on 3: Compliance Suite Common (a).

15. Email Management

    a. Installs **Gimmal Compliance Suite - Email Management Service Installer** at farm level. Dependent on 3: Compliance Suite Common (a).

    b. Installs **Gimmal Compliance Suite - Email Management** at web level. Dependent on 3: Compliance Suite Common (a and b), 6: Record Relationships (b), and 7: Working with Records (b).

16. Disposition

    a. Installs **Gimmal Compliance Suite - Disposition Metadata Timer Job** at web application level. Dependent on 3: Compliance Suite Common (a).

       i. Adds **Gimmal Compliance Suite Disposition Metadata Timer Job**

    b. Installs **Gimmal Compliance Suite - Disposition Content Types** at site collection level. Dependent on 3: Compliance Suite Common (a and b).

    c. Installs **Gimmal Compliance Suite - Disposition View for Record Libraries** at site collection level and is dependent on 3: Compliance Suite Common (a) and 17: Cutoff (b).

Note:

Disposition is not fully installed until after its workflows are activated in step 18.

17. Cutoff
    a. Installs **Gimmal Compliance Suite - Cutoff Content Types** at site collection level. Dependent on 3: Compliance Suite Common (a).
    b. Installs **Gimmal Compliance Suite - Cutoff Management** at web level. Dependent on 3: Compliance Suite Common (a) and 17 (a).
18. Transfers
    a. Installs **Gimmal Compliance Suite - Transfer Timer Job** at web application level. Dependent on 3: Compliance Suite Common (a).
        i. Adds **Gimmal Compliance Suite Transfers Timer** Job
    b. Installs **Gimmal Compliance Suite - Transfers Content Types** at site collection level. Dependent on 3: Compliance Suite Common.
    c. Installs **Gimmal Compliance Suite - Transfers** at web level. Dependent on Document ID Service, 3: Compliance Suite Common, 6: Record Relationships, and 18 (b).
    d. Installs **Gimmal Compliance Suite - Disposition Workflows** at site collection level. Dependent on 3: Compliance Suite Common (a), 16: Disposition (b), and 17: Cutoff (a).
19. Bulk Processing
    a. Installs **Gimmal Compliance Suite - Bulk Processing Administration** at web application level. Dependent on 3: Compliance Suite Common (a).
    b. Installs **Gimmal Compliance Suite - Bulk Processing Site Columns** at site collection level. Dependent on 3: Compliance Suite Common (a).
    c. Installs **Gimmal Compliance Suite - Bulk Processing Timer Job** at web application level. Dependent on 19 (b).
20. As Of Reporting
    a. Installs **Gimmal Compliance Suite - "As Of" Reports** at web level. Dependent on 3: Compliance Suite Common (a) and 16: Disposition (b).
21. File Plan Builder
    a. Installs **Gimmal Compliance Suite - File Plan Builder Settings Editor** at farm level. Dependent on 3: Compliance Suite Common (a).
    b. Installs **Gimmal Compliance Suite - File Plan Builder** at farm level. Dependent on 3: Compliance Suite Common (a) and 21 (a).
    c. Installs **Gimmal Compliance Suite - File Plan Builder** at web level. Dependent on 3: Compliance Suite Common (a), 6: Disposition (b), 14: Vital Records, 21 (a and b).

22. Help

    a. Installs **Gimmal Compliance Suite - Help** at farm level. No dependencies.

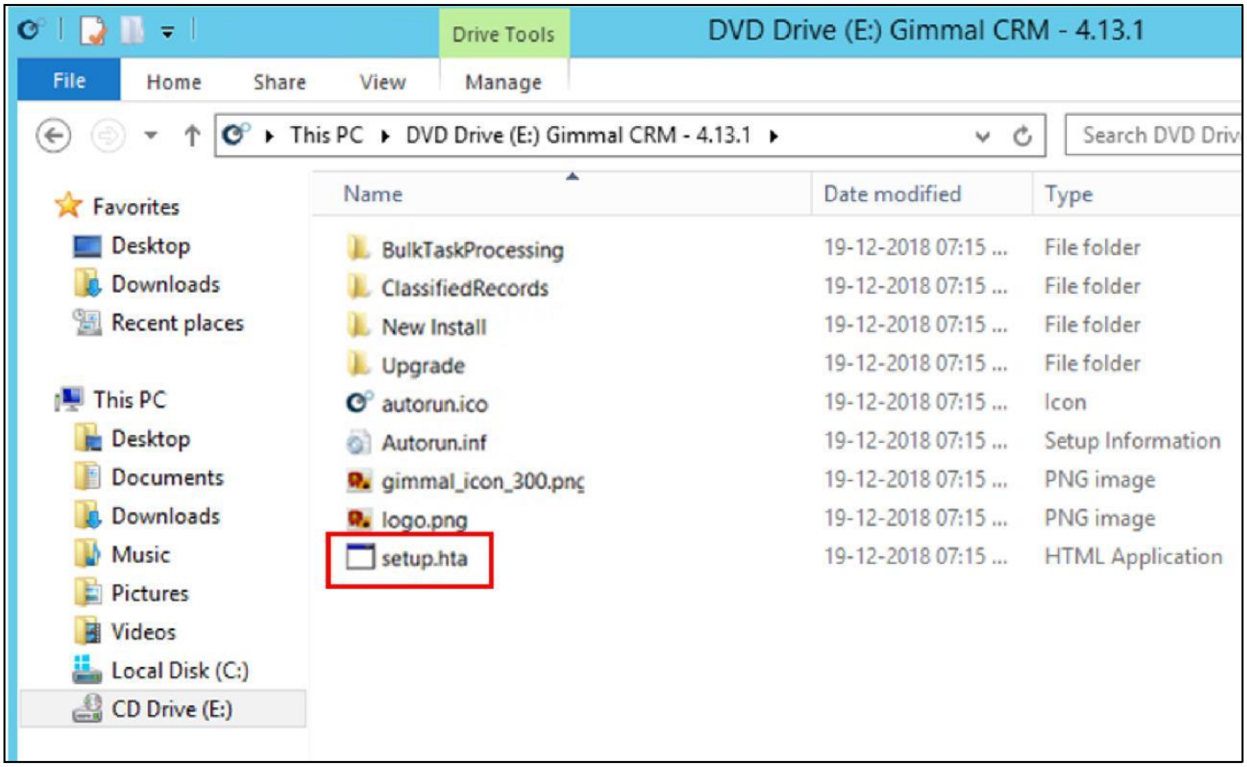
7 Performing an Uninstall of Compliance Suite Features

This section guides you on uninstalling Compliance Suite features.

7.1 Using Gimmal Compliance Suite Installer

To uninstall Compliance Suite using the installer, follow these steps:

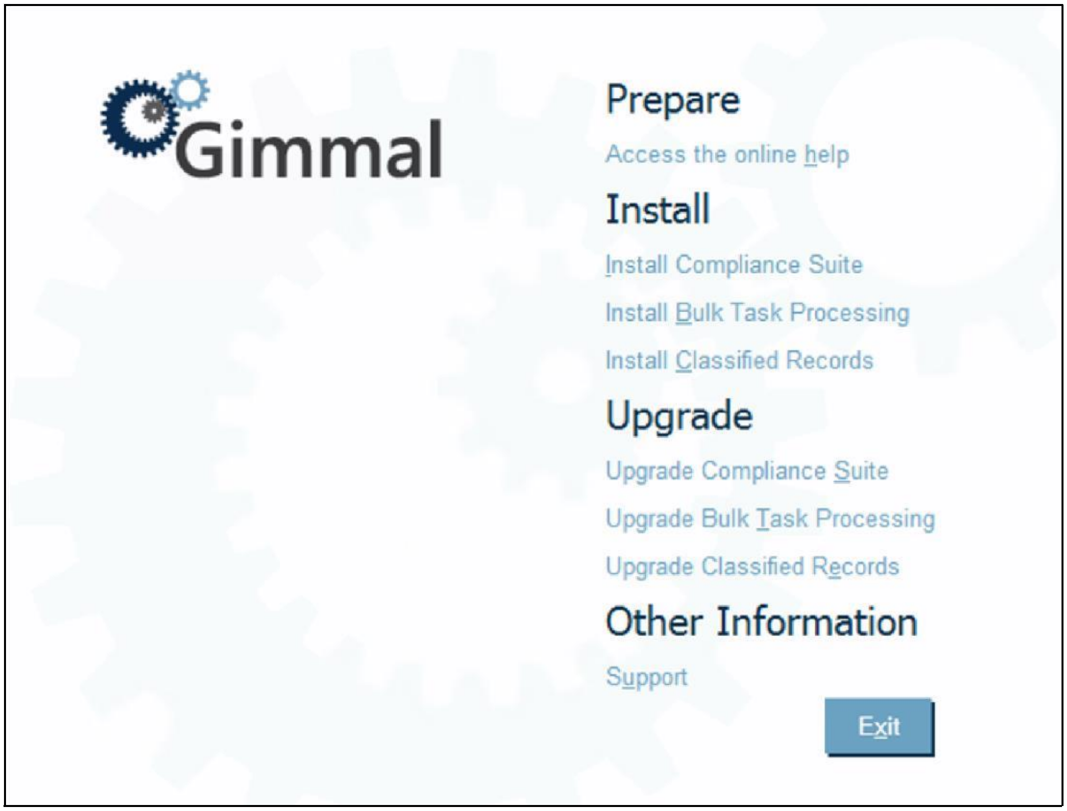
1. Navigate to the GRM 4.14.0 installation folder and double-click the **setup.hta** file in the root folder of the ISO.



Name	Date modified	Type
BulkTaskProcessing	19-12-2018 07:15 ...	File folder
ClassifiedRecords	19-12-2018 07:15 ...	File folder
New Install	19-12-2018 07:15 ...	File folder
Upgrade	19-12-2018 07:15 ...	File folder
autorun.ico	19-12-2018 07:15 ...	Icon
Autorun.inf	19-12-2018 07:15 ...	Setup Information
gimmal_icon_300.pnc	19-12-2018 07:15 ...	PNG image
logo.png	19-12-2018 07:15 ...	PNG image
setup.hta	19-12-2018 07:15 ...	HTML Application

Figure 7-1 Setup File

The Certified Records Management splash screen launches, which provides a link to each component's respective installer, as well as some other helpful links.



Gimmal

Prepare

Access the online help

Install

Install Compliance Suite

Install Bulk Task Processing

Install Classified Records

Upgrade

Upgrade Compliance Suite

Upgrade Bulk Task Processing

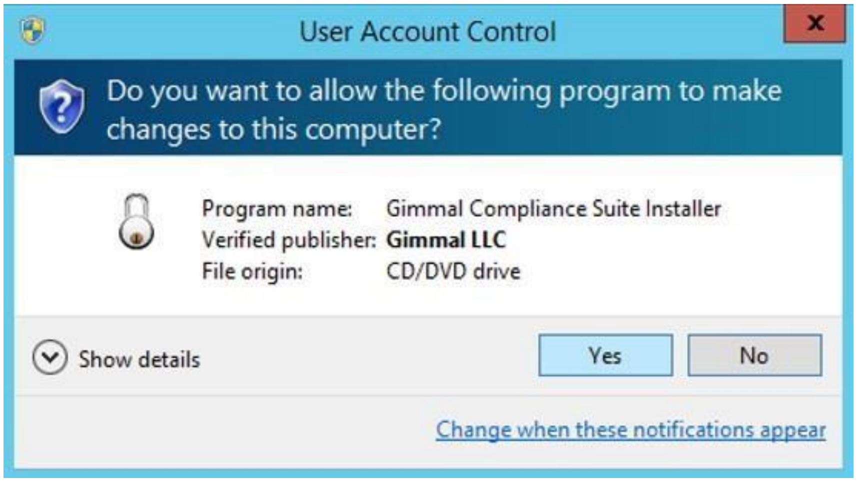
Upgrade Classified Records

Other Information

Support

Figure 7-2 Splash Screen

2. Click **Install Compliance Suite**. A User Account Dialog opens.



User Account Control

Do you want to allow the following program to make changes to this computer?

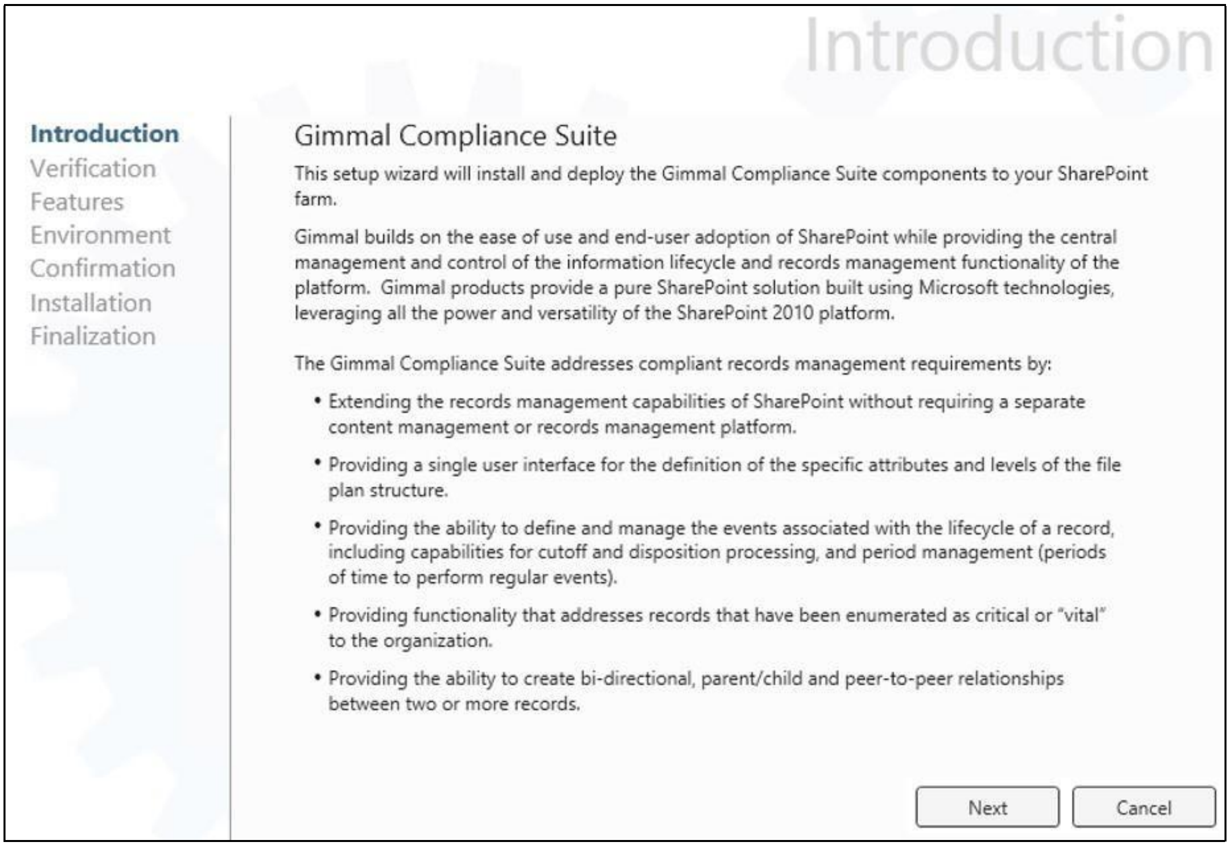
Program name: Gimmal Compliance Suite Installer

Verified publisher: **Gimmal LLC**

File origin: CD/DVD drive

Figure 7-3 User Account Dialog

3. Click **Yes** to continue. When the installer loads, the Gimmal Compliance Suite Introduction page displays.



Gimmal Compliance Suite

This setup wizard will install and deploy the Gimmal Compliance Suite components to your SharePoint farm.

Gimmal builds on the ease of use and end-user adoption of SharePoint while providing the central management and control of the information lifecycle and records management functionality of the platform. Gimmal products provide a pure SharePoint solution built using Microsoft technologies, leveraging all the power and versatility of the SharePoint 2010 platform.

The Gimmal Compliance Suite addresses compliant records management requirements by:

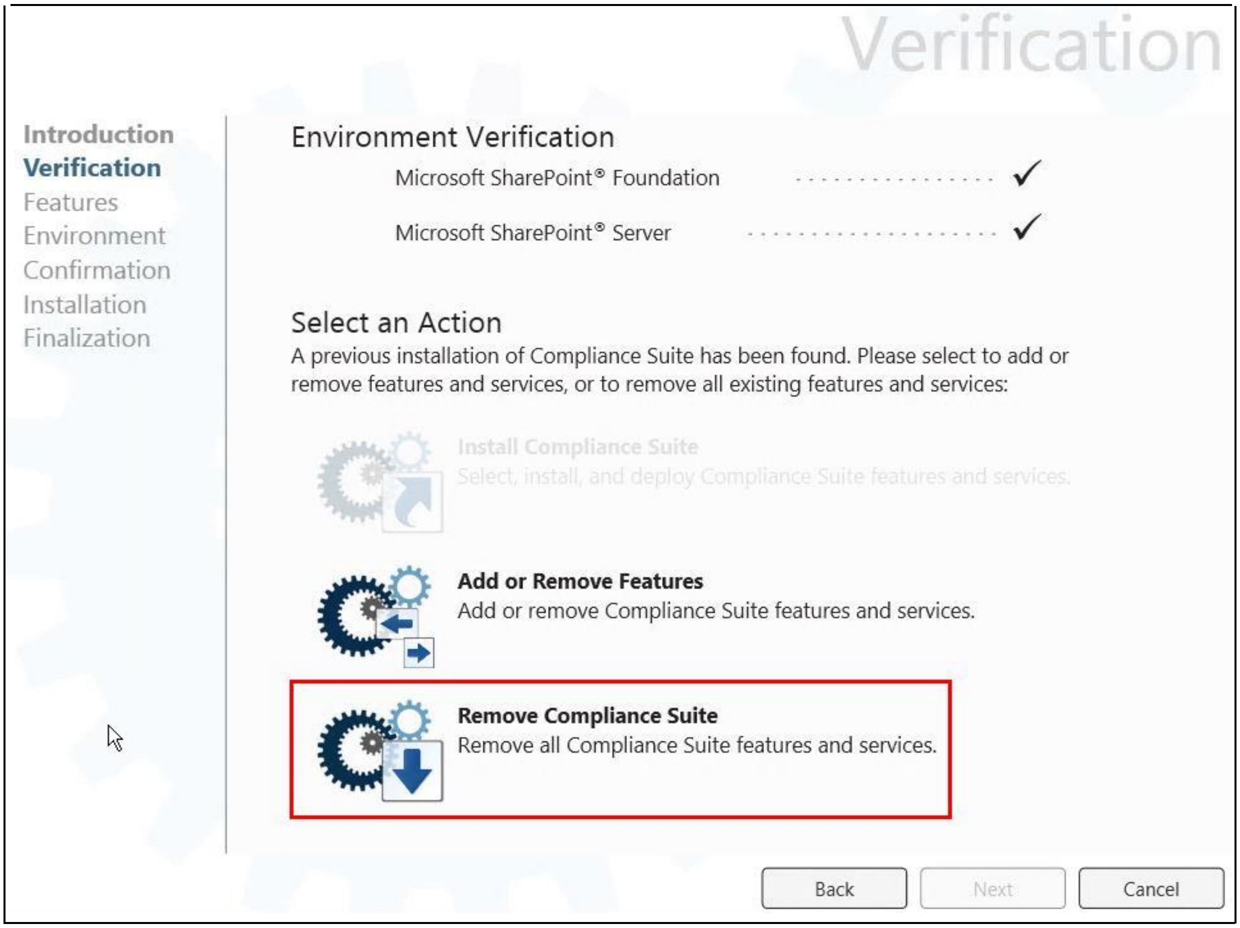
- Extending the records management capabilities of SharePoint without requiring a separate content management or records management platform.
- Providing a single user interface for the definition of the specific attributes and levels of the file plan structure.
- Providing the ability to define and manage the events associated with the lifecycle of a record, including capabilities for cutoff and disposition processing, and period management (periods of time to perform regular events).
- Providing functionality that addresses records that have been enumerated as critical or "vital" to the organization.
- Providing the ability to create bi-directional, parent/child and peer-to-peer relationships between two or more records.

Figure 7-4 Installer Introduction Page

4. Click **Next**. The Verification page displays.

Note

If Gimmal Compliance Suite was previously installed on the farm, the **Add or Remove Features** and **Remove Compliance Suite** are enabled. Selecting either option enables the **Next** button.



Environment Verification

Microsoft SharePoint® Foundation ✓

Microsoft SharePoint® Server ✓

Select an Action

A previous installation of Compliance Suite has been found. Please select to add or remove features and services, or to remove all existing features and services:

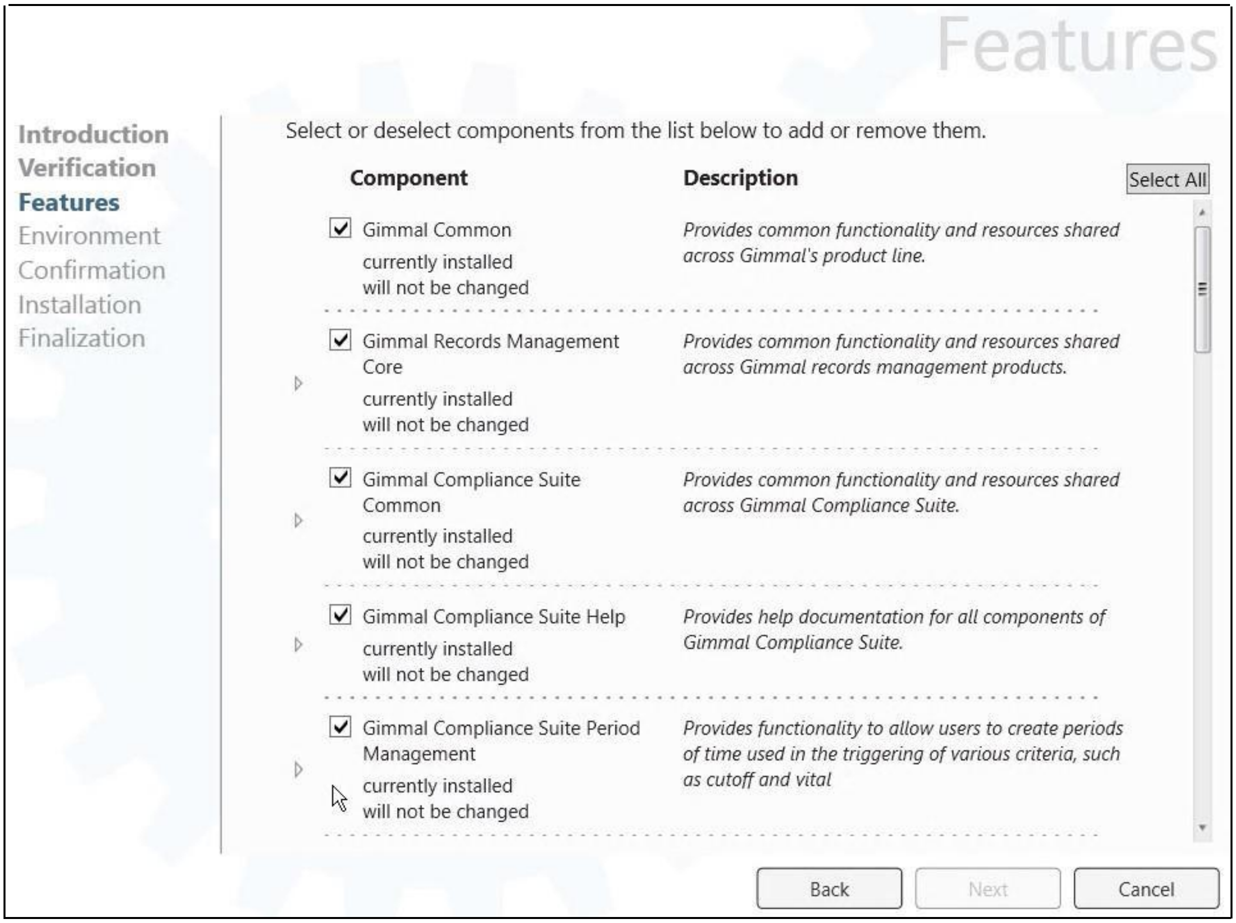
Install Compliance Suite
Select, install, and deploy Compliance Suite features and services.

Add or Remove Features
Add or remove Compliance Suite features and services.

Remove Compliance Suite
Remove all Compliance Suite features and services.

Figure 7-5 Installer Verification Page

5. Under Select an Action, click **Remove Compliance Suite**.
6. Click **Next**. The Features page displays. If other features depend upon the selected feature (i.e., Compliance Suite), those other features are automatically selected. See the following figure.



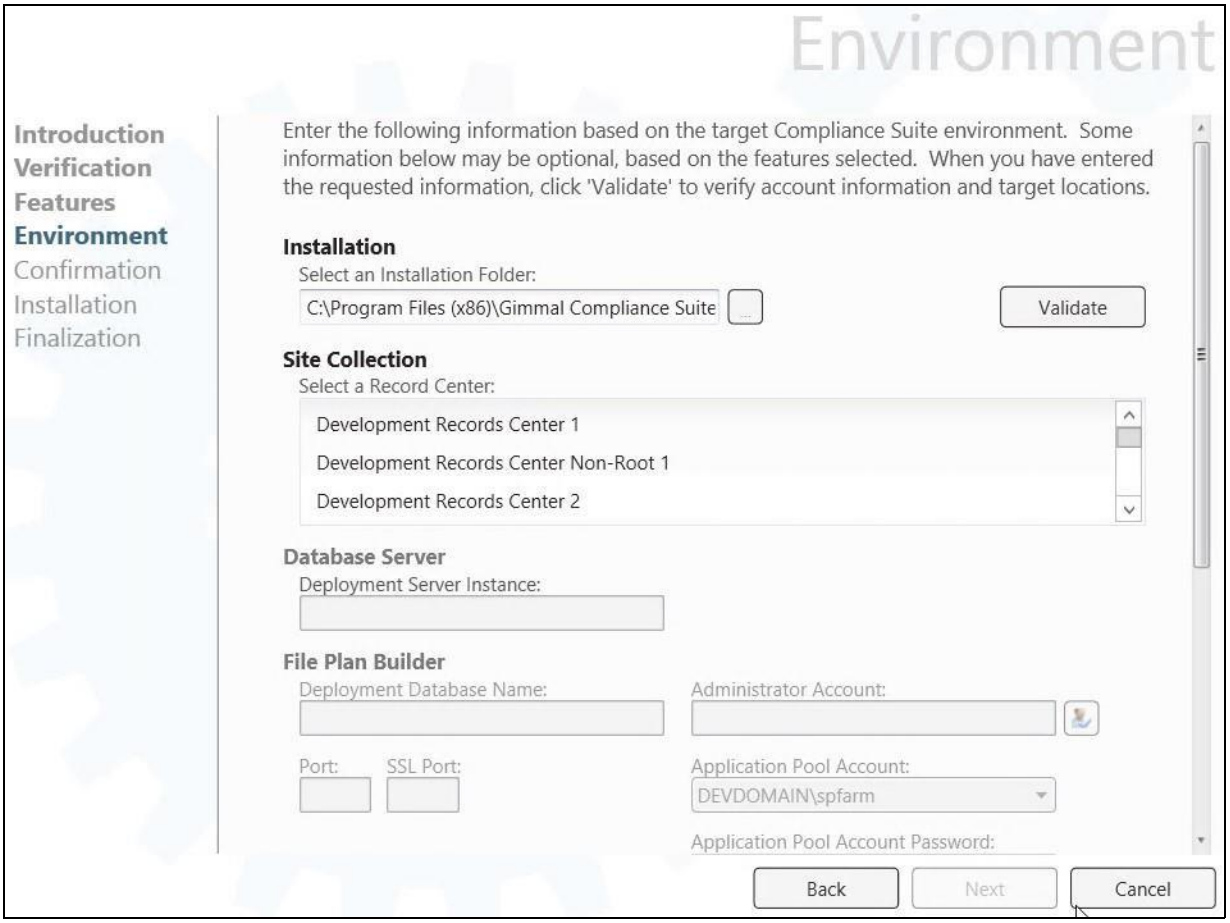
Select or deselect components from the list below to add or remove them.

Component	Description
☑ Gimmal Common currently installed will not be changed	*Provides common functionality and resources shared across Gimmal's product line.*
☑ Gimmal Records Management Core currently installed will not be changed	*Provides common functionality and resources shared across Gimmal records management products.*
☑ Gimmal Compliance Suite Common currently installed will not be changed	*Provides common functionality and resources shared across Gimmal Compliance Suite.*
☑ Gimmal Compliance Suite Help currently installed will not be changed	*Provides help documentation for all components of Gimmal Compliance Suite.*
☑ Gimmal Compliance Suite Period Management currently installed will not be changed	*Provides functionality to allow users to create periods of time used in the triggering of various criteria, such as cutoff and vital*

Figure 7-6 Installer Features Page

7. Verify the selected components, and then click **Next**. If **Remove Compliance Suite** was selected in step 5, everything is uninstalled.

8. Click **Next**. The Environment page displays.



Enter the following information based on the target Compliance Suite environment. Some information below may be optional, based on the features selected. When you have entered the requested information, click 'Validate' to verify account information and target locations.

Installation

Select an Installation Folder: C:\Program Files (x86)\Gimmal Compliance Suite

Site Collection

Select a Record Center:

- Development Records Center 1
- Development Records Center Non-Root 1
- Development Records Center 2

Database Server

Deployment Server Instance:

File Plan Builder

Deployment Database Name:

Administrator Account:

Port:

SSL Port:

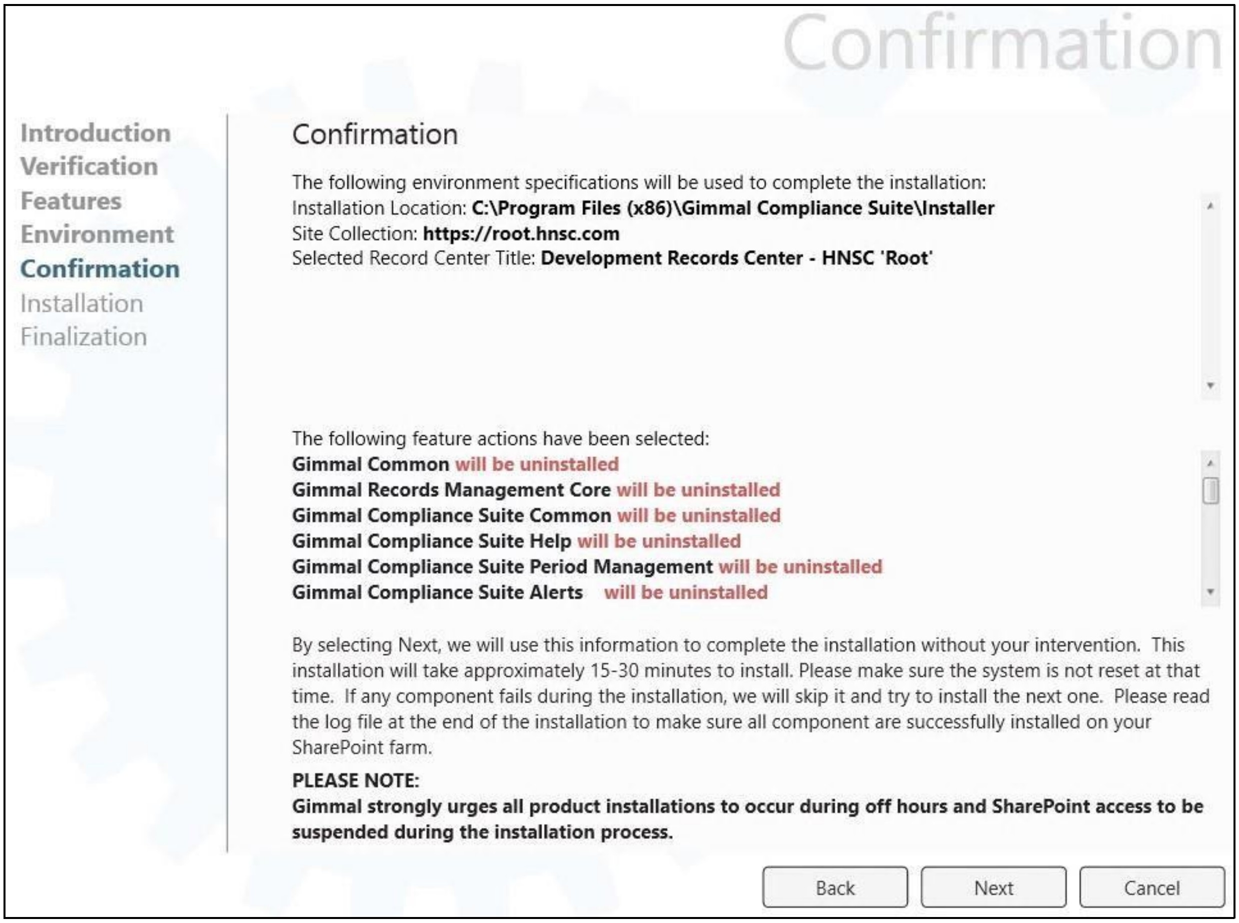
Application Pool Account: DEVDOMAIN\spfarm

Application Pool Account Password:

Figure 7-7 Uninstaller Environment Window

9. Click **Validate** to validate the installation directory location and Site Collection settings.

10. Once validated, the **Next** button is enabled. The Confirmation page displays, confirming your selections.



Confirmation

The following environment specifications will be used to complete the installation:
Installation Location: **C:\Program Files (x86)\Gimmal Compliance Suite\Installer**
Site Collection: **https://root.hnsc.com**
Selected Record Center Title: **Development Records Center - HNSC 'Root'**

The following feature actions have been selected:
Gimmal Common will be uninstalled
Gimmal Records Management Core will be uninstalled
Gimmal Compliance Suite Common will be uninstalled
Gimmal Compliance Suite Help will be uninstalled
Gimmal Compliance Suite Period Management will be uninstalled
Gimmal Compliance Suite Alerts will be uninstalled

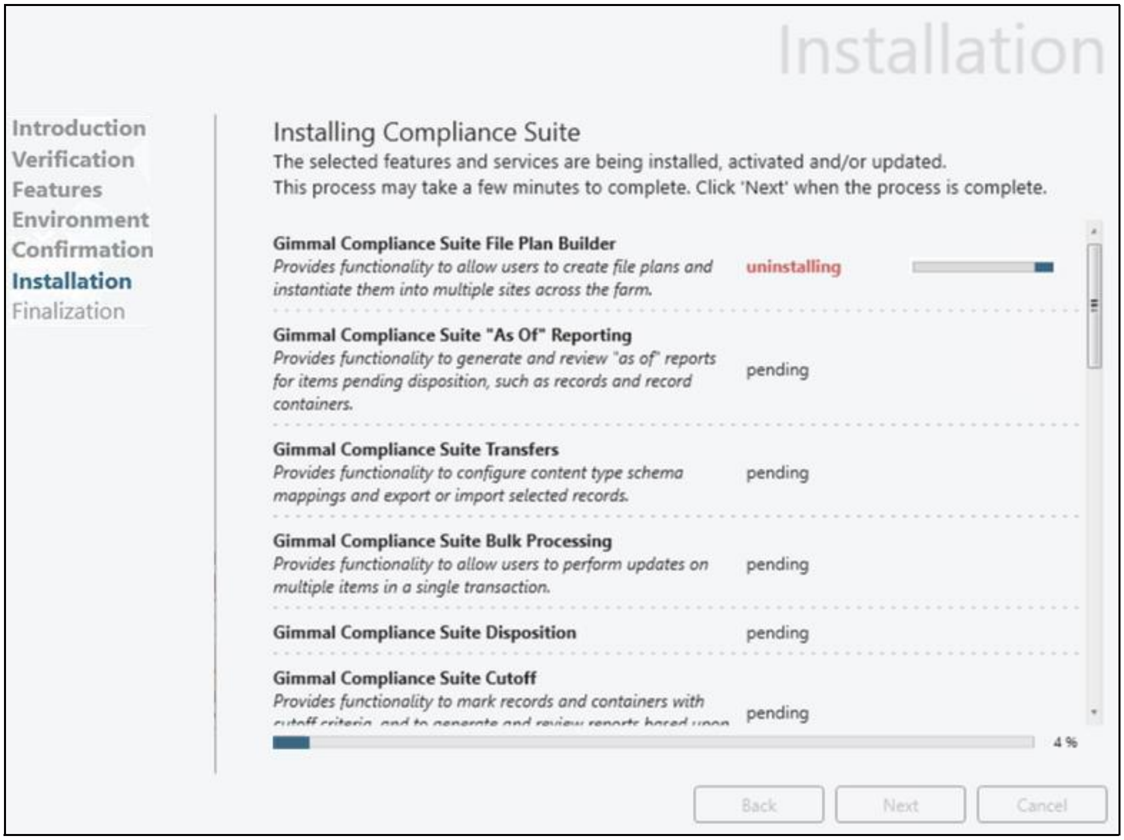
By selecting Next, we will use this information to complete the installation without your intervention. This installation will take approximately 15-30 minutes to install. Please make sure the system is not reset at that time. If any component fails during the installation, we will skip it and try to install the next one. Please read the log file at the end of the installation to make sure all component are successfully installed on your SharePoint farm.

PLEASE NOTE:
Gimmal strongly urges all product installations to occur during off hours and SharePoint access to be suspended during the installation process.

Figure 7-8 Uninstaller Confirmation Window

11. Click **Next**.

    The uninstallation program now uninstalls the Compliance Suite features that were previously selected.



Installing Compliance Suite

The selected features and services are being installed, activated and/or updated.
This process may take a few minutes to complete. Click 'Next' when the process is complete.

Gimmal Compliance Suite File Plan Builder
Provides functionality to allow users to create file plans and instantiate them into multiple sites across the farm. uninstalling

Gimmal Compliance Suite "As Of" Reporting
Provides functionality to generate and review "as of" reports for items pending disposition, such as records and record containers. pending

Gimmal Compliance Suite Transfers
Provides functionality to configure content type schema mappings and export or import selected records. pending

Gimmal Compliance Suite Bulk Processing
Provides functionality to allow users to perform updates on multiple items in a single transaction. pending

Gimmal Compliance Suite Disposition pending

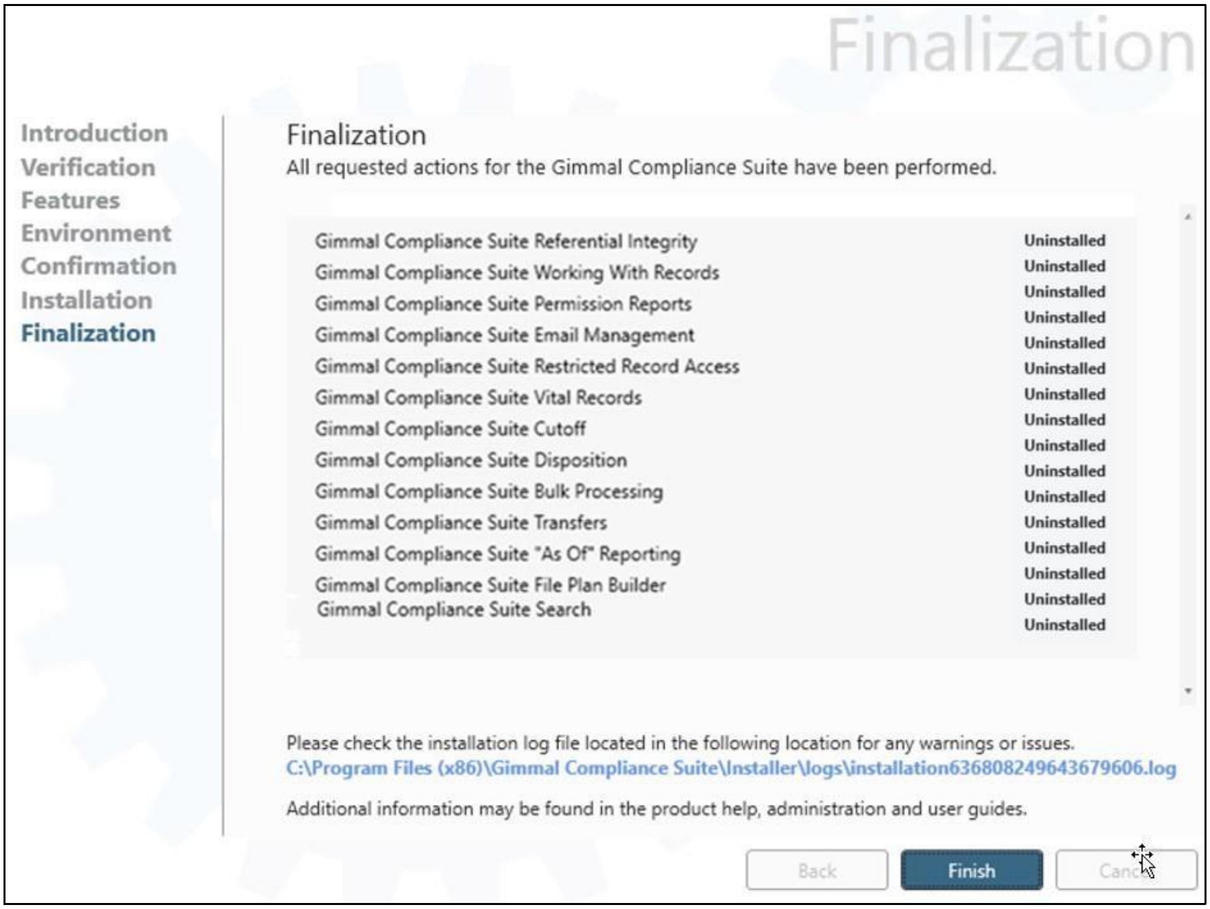
Gimmal Compliance Suite Cutoff
Provides functionality to mark records and containers with cutoff criteria, and to generate and review reports based upon pending

Figure 7-9 Uninstallation Window 1

12. If the uninstall was successful, you should see "**complete**" next to each uninstalled component. If the uninstall was not successful, an error displays and the **Next** button is enabled without uninstalling everything.

13. Click **Next**. The Finalization page displays.

    You can view the log file generated as part of the uninstallation by clicking the link that displays at the bottom of the Finalization screen, as shown below. The log file provides details on issues with feature uninstalls that were unsuccessful.



Finalization

All requested actions for the Gimmal Compliance Suite have been performed.

Gimmal Compliance Suite Referential Integrity	Uninstalled
Gimmal Compliance Suite Working With Records	Uninstalled
Gimmal Compliance Suite Permission Reports	Uninstalled
Gimmal Compliance Suite Email Management	Uninstalled
Gimmal Compliance Suite Restricted Record Access	Uninstalled
Gimmal Compliance Suite Vital Records	Uninstalled
Gimmal Compliance Suite Cutoff	Uninstalled
Gimmal Compliance Suite Disposition	Uninstalled
Gimmal Compliance Suite Bulk Processing	Uninstalled
Gimmal Compliance Suite Transfers	Uninstalled
Gimmal Compliance Suite "As Of" Reporting	Uninstalled
Gimmal Compliance Suite File Plan Builder	Uninstalled
Gimmal Compliance Suite Search	Uninstalled
	Uninstalled
	Uninstalled

Please check the installation log file located in the following location for any warnings or issues.
C:\Program Files (x86)\Gimmal Compliance Suite\Installer\logs\installation636808249643679606.log

Additional information may be found in the product help, administration and user guides.

Figure 7-10 Uninstaller Finalization Window

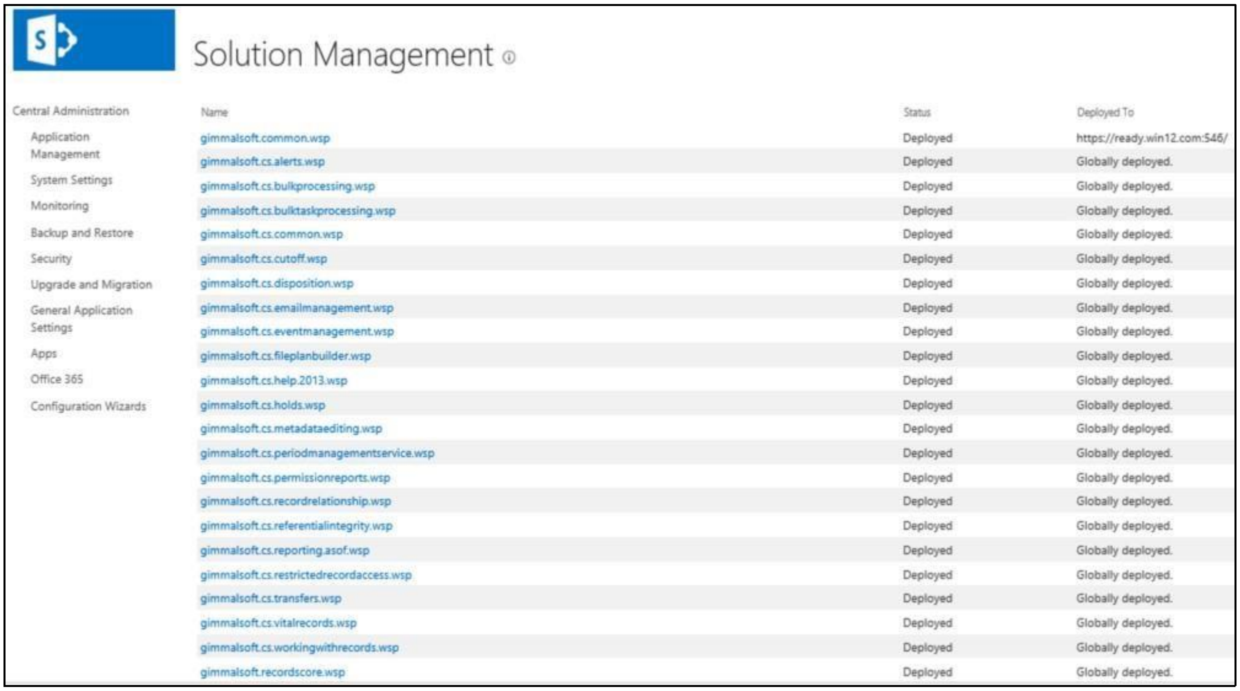
14. When all Gimmal features have been uninstalled successfully, click **Finish**.

7.2 Manually Deactivating Features

To manually uninstall Compliance Suite features, start deactivating features in inverse order in Gimmal Compliance Suite dependency list mentioned previously (i.e., start deactivating from feature 23 to 1).

Once all features are deactivated, next step is to retract and remove all WSPs from central administration. To uninstall WSPs, follow these steps:

1. Login to Central Administration Site.
2. Navigate to Farm Solutions under **System Settings** → **Farm Management.**



Solution Management

Name	Status	Deployed To
gimmalsoft.common.wsp	Deployed	https://ready.win12.com:546/
gimmalsoft.cs.alerts.wsp	Deployed	Globally deployed.
gimmalsoft.cs.bulkprocessing.wsp	Deployed	Globally deployed.
gimmalsoft.cs.bulktaskprocessing.wsp	Deployed	Globally deployed.
gimmalsoft.cs.common.wsp	Deployed	Globally deployed.
gimmalsoft.cs.cutoff.wsp	Deployed	Globally deployed.
gimmalsoft.cs.disposition.wsp	Deployed	Globally deployed.
gimmalsoft.cs.emailmanagement.wsp	Deployed	Globally deployed.
gimmalsoft.cs.eventmanagement.wsp	Deployed	Globally deployed.
gimmalsoft.cs.fileplanbuilder.wsp	Deployed	Globally deployed.
gimmalsoft.cs.help.2013.wsp	Deployed	Globally deployed.
gimmalsoft.cs.holds.wsp	Deployed	Globally deployed.
gimmalsoft.cs.metadataediting.wsp	Deployed	Globally deployed.
gimmalsoft.cs.periodmanagementservice.wsp	Deployed	Globally deployed.
gimmalsoft.cs.permissionreports.wsp	Deployed	Globally deployed.
gimmalsoft.cs.recordrelationship.wsp	Deployed	Globally deployed.
gimmalsoft.cs.referentialintegrity.wsp	Deployed	Globally deployed.
gimmalsoft.cs.reporting.asof.wsp	Deployed	Globally deployed.
gimmalsoft.cs.restrictedrecordaccess.wsp	Deployed	Globally deployed.
gimmalsoft.cs.transfers.wsp	Deployed	Globally deployed.
gimmalsoft.cs.vitalrecords.wsp	Deployed	Globally deployed.
gimmalsoft.cs.workingwithrecords.wsp	Deployed	Globally deployed.
gimmalsoft.recordscore.wsp	Deployed	Globally deployed.

Figure 7-11 List of All Compliance Suite Solutions

3. Click on WSP related to Compliance Suite and start retracting.
4. Refresh your browser until you see Not Deployed as the status on the WSP.
5. Select the WSP retracted in previous step and click **Remove Solution**.
6. Repeat steps 3-6 until all Compliance Suite Related WSPs are removed.

Even after entire uninstallation, you see some compliance suite related content present in site collection and central administration. The following items are preserved or removed after entire manual uninstallation:

1. Email and Event Management Service is deleted after deactivation.
2. Following Databases are not deleted:
    a. Gimmal Compliance Suite Database
    b. Email Management Database
    c. Event Management Database
    d. File Plan Builder Database
3. Following Databases are deleted:
    a. Gimmal Common Database

4. All Custom Managed Property related to Compliance Suite remain in Search Schema.
5. All Terms created in Term Store remain intact.
6. Following Libraries remain intact:
    a. Access Rules
    b. Cutoff Reviews
    c. Cutoff Search Reports
    d. Disposition Tasks
    e. Filing Locations
    f. GimmalSoft Column Access Control
    g. Period Definitions
    h. Related Records
    i. Relationship Types
    j. Schema Mappings
    k. Vital Record Reports
    l. Vital Record Reviews

Note:

Users can delete these libraries if they want to, but the libraries are not deleted as part of the uninstallation process.

Note:

Uninstall does not remove users from the groups on the sites. An administrator can delete the users manually from the groups if desired.