



# Install Guide

**Gimmel Apps**

**Version 5.1.0**

**February 2016**

Title: *Gimmal Apps Install Guide*

© 2016 Gimmal LLC

Gimmal® is a registered trademark of Gimmal Group.

Microsoft® and SharePoint® are registered trademarks of Microsoft.

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.

Use, copying, and distribution of any Gimmal software described in this publication requires an applicable software license. For the most up-to-date listing of Gimmal product names and information, visit [www.gimmal.com](http://www.gimmal.com). All other trademarks used herein are the property of their respective owners.

### Document Revision History

Publication Date	Document Version #	Description
October 2017	2.1	Improved instructions on how to properly remove/uninstall an app from a farm
February 2016	2.0	Updated Guide
February 2015	1.0	Initial Guide

If you have questions or comments about this publication, you can email [TechnicalPublications@Gimmal.com](mailto: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

<b>Preface .....</b>	<b>4</b>
Who Should Use This Guide .....	4
<b>Introduction .....</b>	<b>5</b>
<b>Deployment Scenarios .....</b>	<b>6</b>
SharePoint 2013 (On-premises) and O365.....	6
App Components.....	6
Before You Begin .....	7
<i>System Prerequisites</i> .....	7
<i>Prerequisite for Single Server Environment</i> .....	7
<i>SharePoint Configuration</i> .....	8
<b>Installing Web Deploy on the IIS .....</b>	<b>9</b>
Installing Web Deploy .....	9
<b>Running the Gimmel App Installer .....</b>	<b>11</b>
Information Needed for Configuration.....	11
Downloading and Running the App Installer .....	12
<b>Upgrading Gimmel Apps .....</b>	<b>6</b>
Downloading the Latest Version of the App Installer.....	6
Upgrading an App Using the Installer.....	6
Upgrading an App in SharePoint.....	13
<b>Configuring IIS Settings for High Trust Apps .....</b>	<b>15</b>
<b>Uninstalling an App.....</b>	<b>18</b>
Removing an App from a Site .....	18
Removing an App from the App Catalog .....	18
Removing an App's Remote Web from Internet Information Server (IIS).....	18

## Preface

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

## Who Should Use This Guide

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

## Introduction

This manual contains the instructions for running the Gimmel App Installer and deploying a Gimmel app using the App Installer. The manual also provides additional procedures that are necessary before running the installer or deploying an app.

Use these instructions for each Gimmel app you deploy. To configure an app after you deploy it, refer to that app's specific configuration manual.

## Deployment Scenarios

This section describes app deployment scenarios, as well as the prerequisites for deploying an app. You must determine which scenario is appropriate for your site before deployment.

### SharePoint 2013 (On-premises) and O365

Gimmel apps can be deployed into SharePoint 2013 on-premises or O365 environments. Each app may consist of a SharePoint app, a remote web, a database, or any combination of those. The app components you choose to deploy, and where you choose to deploy them, depend on your environment and SharePoint topology. If a remote web or database are required, you must choose the configuration that best fits your deployment scenario.

Possible *standard* scenarios include:

- **Single farm (on-prem)** – Deploy from Web Front End (WFFE)
- **Multi farm (on-prem)** – Deploy to each farm once, possibly needing to pick a single web server and database server, if required by the app (one single server for the farm)
- **O365** – Deploy to O365 from any computer. Likely need the CSOM SDK installed on the computer from which you are installing. You also need a local (i.e., not O365) web server that can be reached by O365 and database server, if required by the app.
- **Multi-farm hybrid** (O365 + on-prem - rare, but supported) – Similar to the Multi farm install where one farm is an O365 install. You must deploy to each O365 and on-prem farm once. You need two web servers (one for O365 and one for on-prem that can be shared by the on-prem farms), but the two web servers can share a single database.

### App Components

You must successfully deploy two components for the SharePoint app to work properly – the app itself and the remote web. Some Gimmel apps also use the app installer to install a required database. The app installer reads an app's configuration file and displays the correct components for installation according to those file settings.

You must deploy the app to the SharePoint App Catalog. You may deploy the remote web either to a single Internet Information Services (IIS) server, or to multiple IIS servers, if load balancing is desired. The following common deployment scenarios cover most situations:

- **Single-Server** – Applies when the SharePoint Web Front End (WFE) and IIS server are the same server; typically, this deployment scenario is used only in a developer’s virtual machine (VM) environment. You simultaneously deploy the app and remote web in this scenario.
- **Multi-Server** – Applies when the SharePoint WFE and IIS server are on different servers, but there is only one IIS server; typically, this deployment scenario is used in a DEV or TEST environment. In this scenario, you run the App Installer once to install the app and again to install the remote web.
- **Load-Balanced Multi-Server** – Applies when the SharePoint WFE and IIS server are on different servers and there is more than one IIS server; typically, this deployment scenario is used in a TEST, STAGING, or PRODUCTION environment. In this scenario, you run the App Installer once to install the app and once for each IIS server participating as a remote web

## Before You Begin

Before installing apps, you must confirm the following system prerequisites. You must also configure the SharePoint 2013 server for app deployment, create an app catalog, and configure SharePoint for apps.

### System Prerequisites

The Gimmel App Installer requires the following software:

- SharePoint Server 2013 (Standard or Enterprise Edition with Service Pack 1)
- Microsoft .NET Framework 4.5.2

### Prerequisite for Single Server Environment

If you are installing a provider-hosted app in an environment where the provider-hosted web is located on a SharePoint WFE and you have already installed any of Gimmel’s feature-activated (.WSP) software, then you must download and install the most recent version of Gimmel Common. This situation does not apply to the following previously installed products:

- Drop Zone (FA)
- Content Loader (FA)
- Metadata Inheritance Rules (FA)
- Enhanced Template Manager (FA)
- Site Provisioning (FA)
- Enhanced Search (FA)
- Content Organizer Manager (FA)
- Site Decommissioning (FA)

## SharePoint Configuration

Refer to the following hyperlinked MSDN articles to prepare the system before attempting to install the apps:

Follow these steps to configure a SharePoint **on-premises** environment:

1. [Configure an environment for apps for SharePoint.](#)
2. [Set up an App Catalog for SharePoint.](#)
3. [Configure SharePoint for High Trust Apps.](#)
4. If the app requires a remote web, [install Web Deploy](#) (msdeploy.exe) on the machine(s) where you plan to host a remote web. Refer to "Installing Web Deploy."
5. [Install SharePoint Server 2013 Client Components SDK](#) (optional). Do this if you want to deploy an app by running the App Installer from a server that does not have SharePoint installed.

Follow these steps to configure a SharePoint Office 365 environment:

1. [Set up a SharePoint App Catalog](#) (step 1 only).
2. If the app requires a remote web, [install Web Deploy](#) (msdeploy.exe) on the machine(s) where you plan to host a remote web. Refer to "Installing Web Deploy."
3. [Install SharePoint Server 2013 Client Components SDK](#) to deploy an app with the App Installer on a server that does not have SharePoint installed



## Installing Web Deploy on the IIS

Before deploying the app, you must install Web Deploy on the IIS machines on which you are running the installer to install the remote web. This section provides instructions for installing Web Deploy.

### Important!

When installing on O365, the IIS machine must be accessible to the O365 environment.

## Installing Web Deploy

You must install Web Deploy on each server where the apps (remote web) will be used.

Follow these steps to install the most recent version of Web Deploy:

1. On the Web Server, run the WebPlatformInstaller.exe usually located in C:\Program Files\Microsoft\Web Platform Installer. You also can download the most recent version of the Microsoft Web Platform Installer from <http://www.microsoft.com/web/downloads/platform.aspx>
2. Download and run the Web Deploy package.
3. Launch the Web Platform Installer. The installer dialog displays:

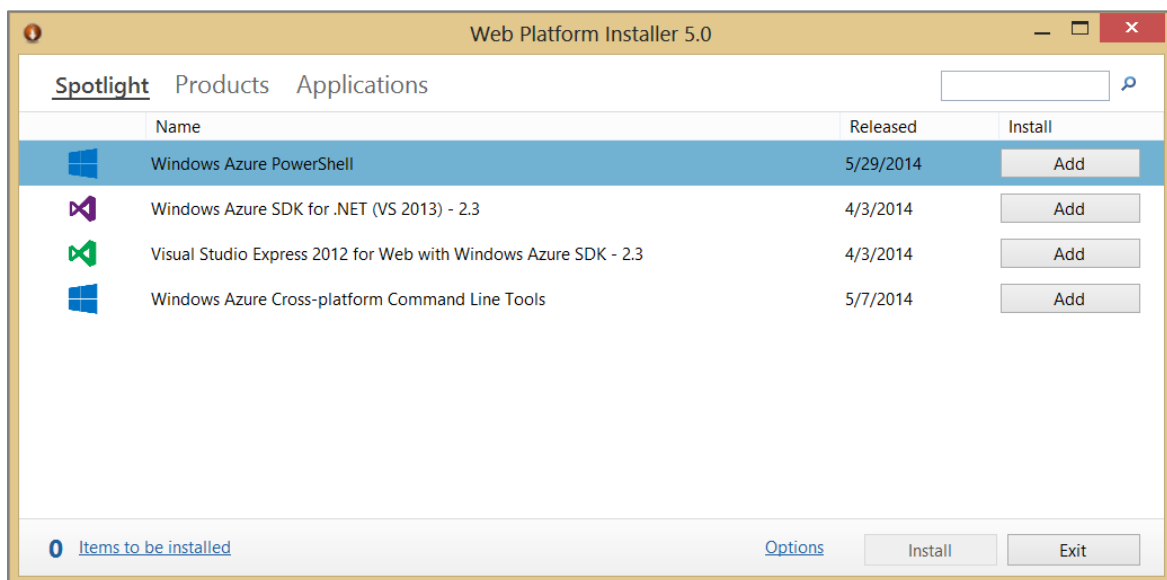


Figure 1 Web Platform Installer Dialog

4. In the search box to the right at the top of the page, type Web Deploy, then press **Enter**.

- Next to the Web Deploy entry, click **Add** and then **Install** at the bottom of the page. If the component is already installed, you will not be able to add it, and it displays as **Installed**.

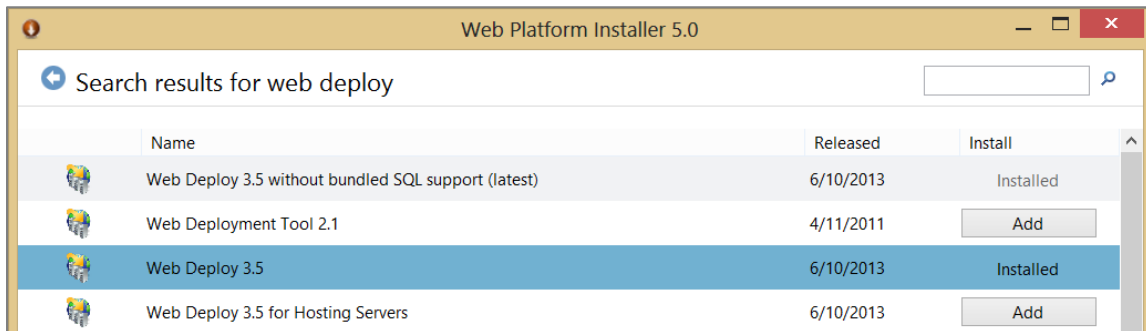


Figure 2 Web Platform Installed

## Running the Gimmel App Installer

This section provides step-by-step instructions for downloading Gimmel App Installer and deploying an app. You must copy the App Installer and app on each server where they will be used.

### Important!

Determine the type of deployment scenario needed for your site, as described in [Deployment Scenarios](#), and then deploy the app in the required locations for that scenario.

In a single server scenario, simultaneously deploy the app and remote web as described in this section. To deploy a SharePoint app and remote web in a multi-server scenario, use these instructions to deploy the app and deploy the remote web. To deploy a SharePoint app in a load-balanced multi-server scenario, use the installer once to deploy the app and once to deploy the remote web on each remote web.

If you are installing apps into multiple app catalogs, configure them to point to the same remote web(s) and database. In most cases, a single remote web must be used for all web applications. You must use two separate remote webs if using both High Trust and ACS SharePoint sites.

## Information Needed for Configuration

In addition to web and database configuration information, you need the following information at hand to deploy high trust apps in SharePoint:

- Certificate file location
- Certificate password
- Certificate issuer ID

### Important!

If you are installing only on O365 and are not targeting sites on a high trust environment, you do not need the certificate information.

## Downloading and Running the App Installer

Gimmel App Installer is distributed separately from other Gimmel products. You must have System Administrator privileges to install apps. If using SharePoint 2013 (on-prem), log into a WFE server using an account that is a member of the Farm Administrators group in the SharePoint Farm.

Follow these steps to download and run the app installer:

1. Download the app you plan to deploy from the Gimmel Software Download site at: <https://clients.gimmel.com/sites/gimmalsoftdownload/SitePages/Home.aspx>
2. Once downloaded, right-click on the .zip file and select **Properties** from the menu. The Properties dialog displays.
3. On the **General** tab, ensure that **Unblock** is selected so that the zip file is not blocked when you try to unzip it. This setting depends on the server's security configuration.
4. Unzip the package.
5. Follow steps 1 through 4 for the app installer package.
6. Open the App Installer folder you previously downloaded (refer to ""), right-click `GimmelAppInstaller.exe`, and then select **Run as administrator** from the menu. The Gimmel App Installation Wizard displays.

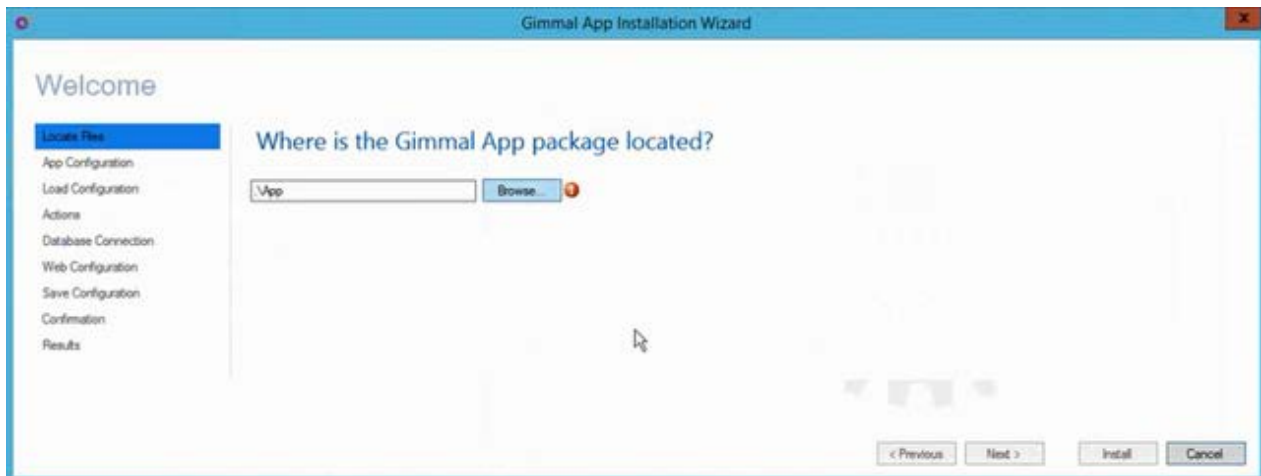


Figure 3 Locate Files Page

### Important!

The installer window is not resizable.

7. On the Locate Files page, click **Browse** and select the folder for the app that you want to deploy.
8. Click **Next**. The App Configuration page displays.

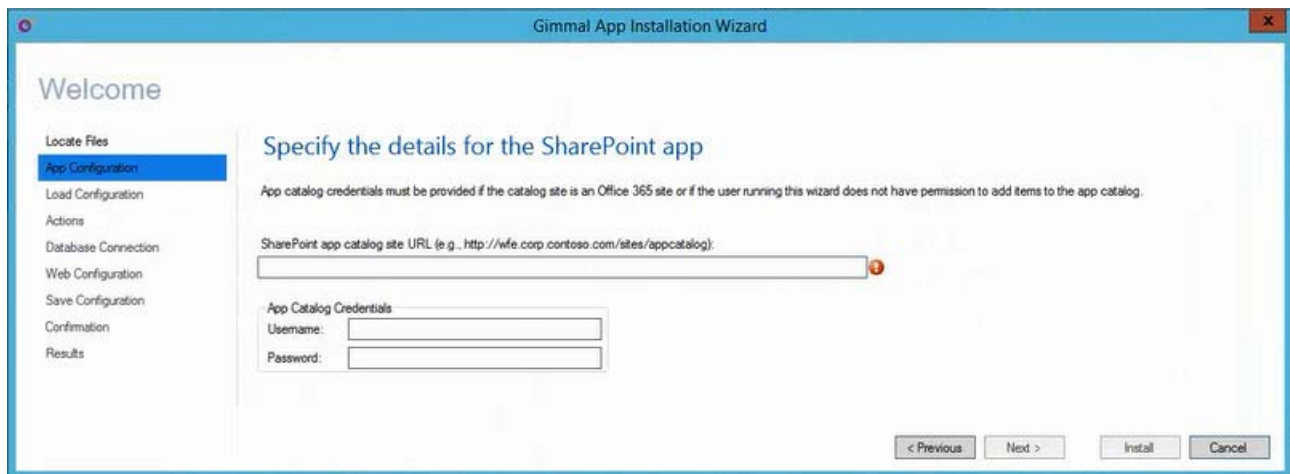


Figure 4 App Configuration Page

9. In the **App Configuration** page:
  - a. In **SharePoint app catalog site URL**, provide the app catalog URL. To find the URL, follow these steps:
    - i. If using SharePoint 2013 (on-prem), from the main page in Central Administration. If using O365, go to the SharePoint Admin Center. Click **Apps** in the left menu pane. The Apps page displays.
    - ii. In SharePoint 2013 (on-prem), under **App Management**, select **Manage App Catalog**. In O365, select **App Catalog**. The URL displays next to **Web Application** on the right side.
  - b. If you are installing as a user that does not have permission to add items in the app catalog, enter the **Username** and **Password** for the site in **App Catalog Credentials**.
10. Click **Next**. The **Actions** page displays.

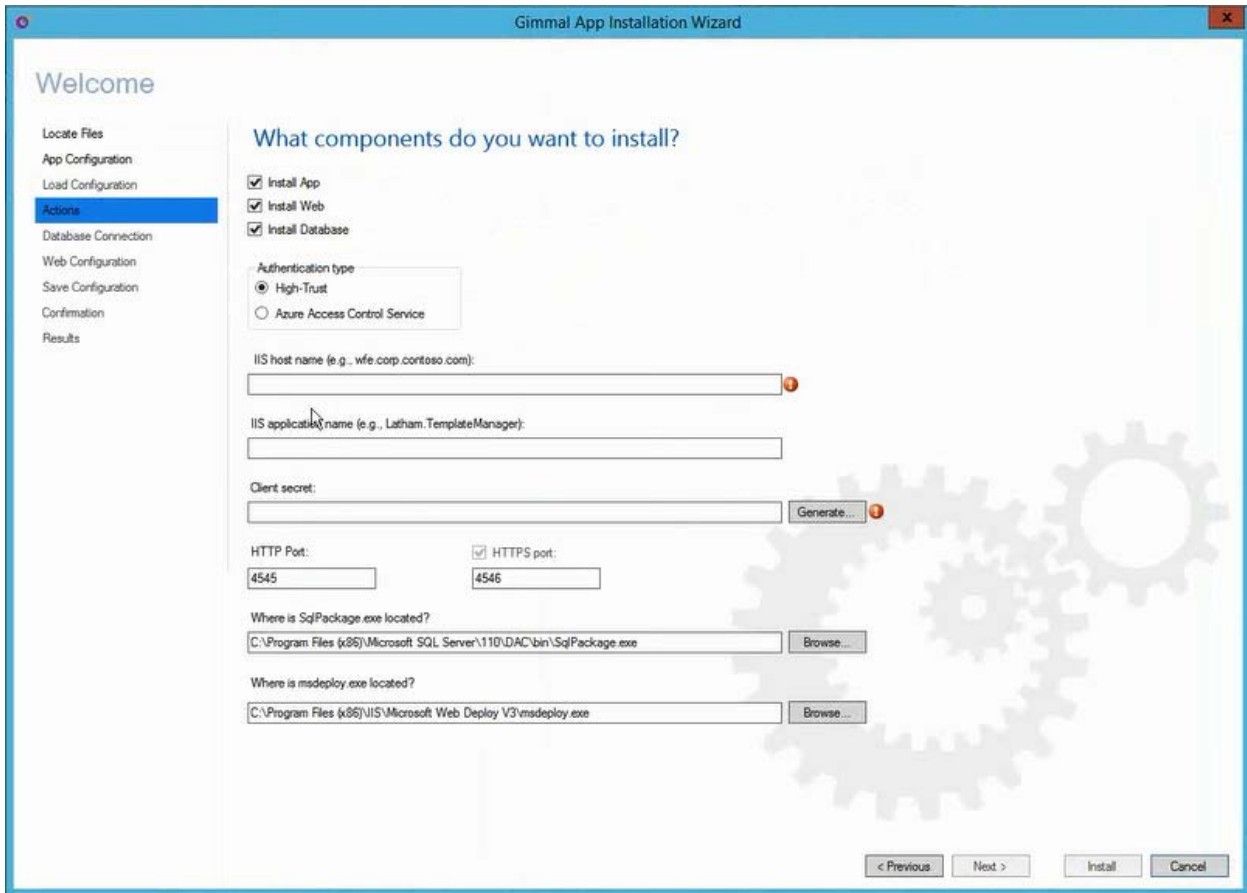


Figure 5 Actions Page

11. In the Actions page:

- a. Select the checkboxes for **Install App**, **Install Web**, and **Install Database**, according to your installation scenario. If an install option is not required for the app's configuration, it is grayed out.

### Important!

If SQL Server or [SQL Server Data Tools](#) is not installed on the web server, you can first run the installer on the database server, choosing to only **Install Database**. Then, when installing on the web server, uncheck **Install Database** and configure the existing connection string on the Database Connection tab.

- b. Select **High-Trust** as **Authentication type** if the web will be used for a high-trust, on-premises installation. Select **Azure Access Control Service** if the web will be used for an O365 installation.

## Important!

If you are using both on-premises and O365 installations, you must have two separate webs; one to service high trust and one to service ACS/O365. You must run the installer for each web, selecting the appropriate Authentication type.

- c. In **IIS host name**, provide the name of the corresponding Web Server where you intend to install the remote web.
- d. If you are installing the web into a folder/application in a website, enter the **IIS application name**. You can leave **IIS application name** blank if you are installing in the root of a website.
- e. Click **Generate** next to the **Client Secret** field, if it is required for your app scenario.
- f. Verify the port numbers (automatically populated):
  - **HTTP Port** – Port used for HTTP requests
  - **HTTPS Port** – Port used for HTTPS requests

## Important!

HTTPS must be checked before you can select **Next**. You must use HTTPS to install apps.

- g. Verify the **Where is SqlPackage.exe located?** field. It should automatically populate.
  - h. Verify the **Where is msdeploy.exe located?** field. It should automatically populate.
12. Click **Next**. The **Database Connection** tab displays if you selected to Install Database in step 9. If you are not installing a database, go to step 14.



Figure 6 Database Connection Tab

13. In the **Database Connection** tab:

- a. Click **Build** displayed next to the **Database connection string** field. The Connection Properties window displays.

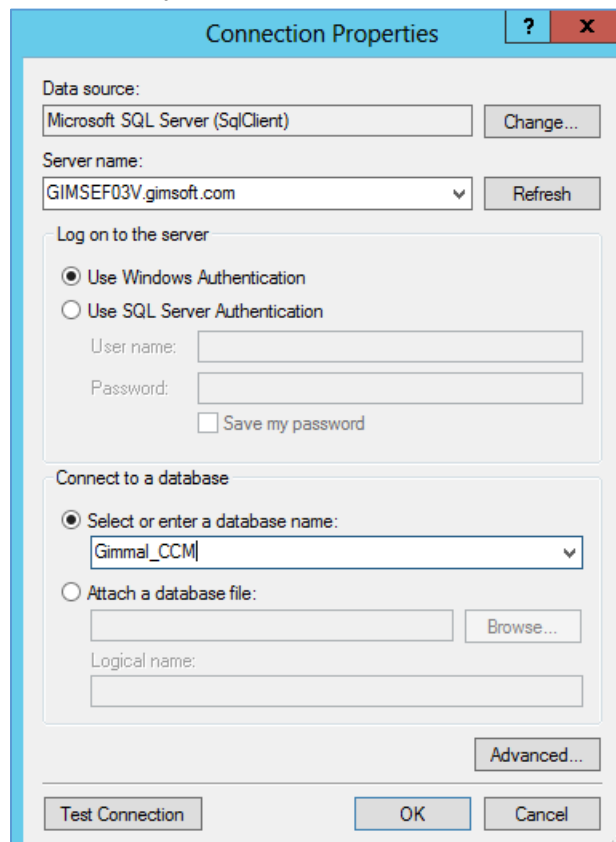


Figure 7 Connection Properties Window

- b. Enter the following in the Connection Properties window:
  - i. **Data source:** Microsoft SQL Server (SqlClient) is selected.
  - ii. **Server name:** Select the name of the SQL Server (if it is not displayed in the list). Then click **Refresh**.
  - iii. **Log on to the server:** Select the type of authentication.
  - iv. **Connect to a database:** Provide the name of a database that you intend to use (i.e., Gimma1\_CCM). If you type in a name that does not exist, the installer creates it for you.
  - v. Click **Test Connection** to verify the connection. If the connection is successfully established, click **OK** on the successful message. If it is not successful, check your entries in the Connection Properties window.
  - vi. Click **OK** to save the changes made on the Connection Properties window.
- c. Click **Next** on the **Database Connection** tab. The **Web Configuration** tab displays.



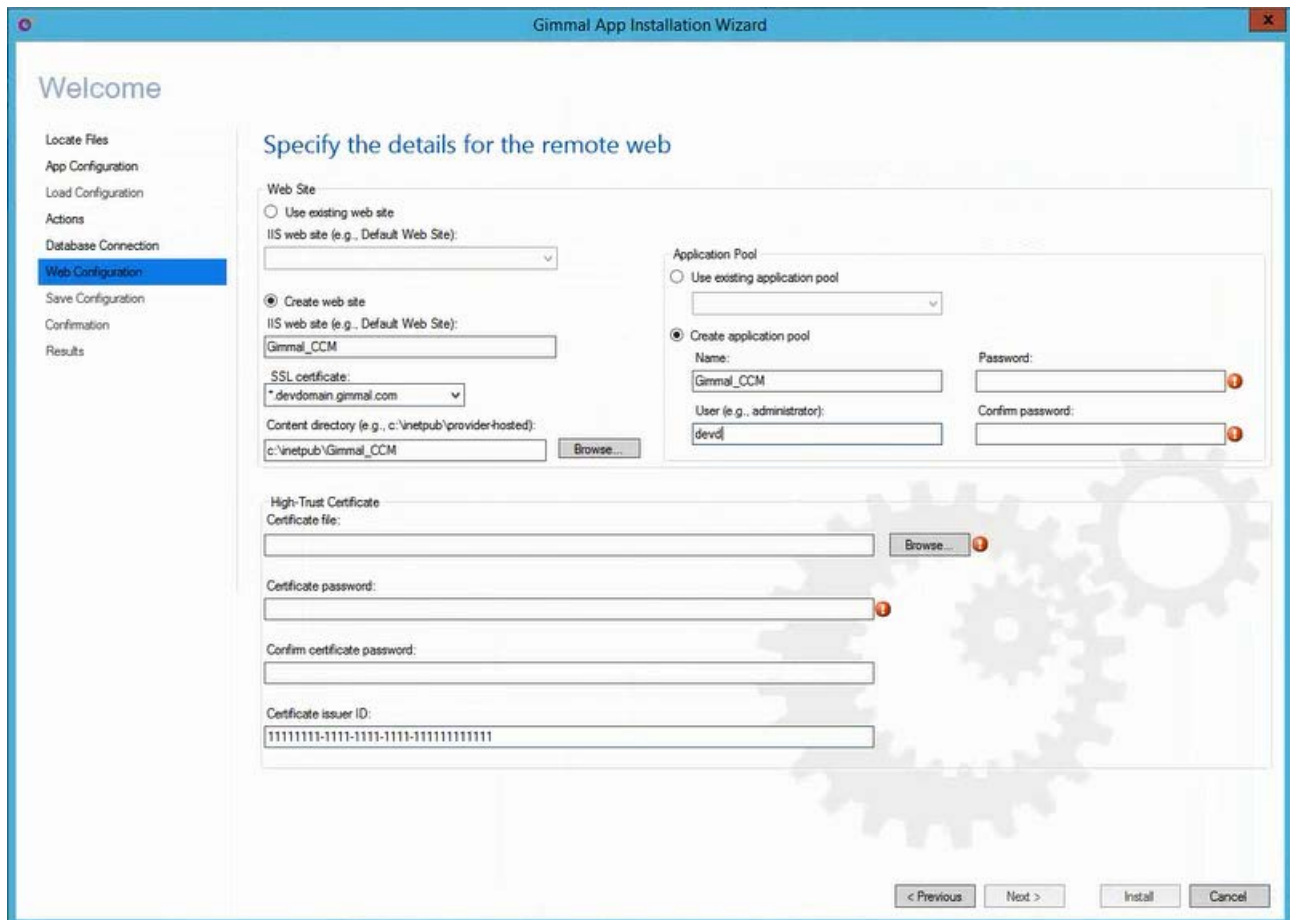


Figure 8 Web Configuration Tab

14. In the **Web Configuration** tab:

- a. Either select **Use existing web site** and select the existing website or select **Create web site**. If you create a new website, select a **SSL certificate** and enter an existing **Content directory**. You can **Browse** and select a different **Content directory**.

### Important!

The Content directory must already exist. A new folder is not created for the deployed content.

- b. In the **Application Pool** section, you can select **Use existing application pool** to use an application pool that currently exists. If you created a web site in the previous step, you can also select **Create application pool** and enter the **Name**, **User**, and **Password** if not already populated.

## Important!

User and Password are the credentials that the application pool runs as.

- c. Select **Certificate file** by clicking **Browse**.

## Important!

If you are installing only on O365 and are not targeting sites on a high trust environment, leave the **Certificate file**, **Certificate Password**, and **Certificate issuer ID** fields blank and go to step 13.

- d. Provide valid **Certificate Password**.
- e. Provide valid **Certificate Issuer ID**.

15. Click **Next**. The Save Configuration page displays.

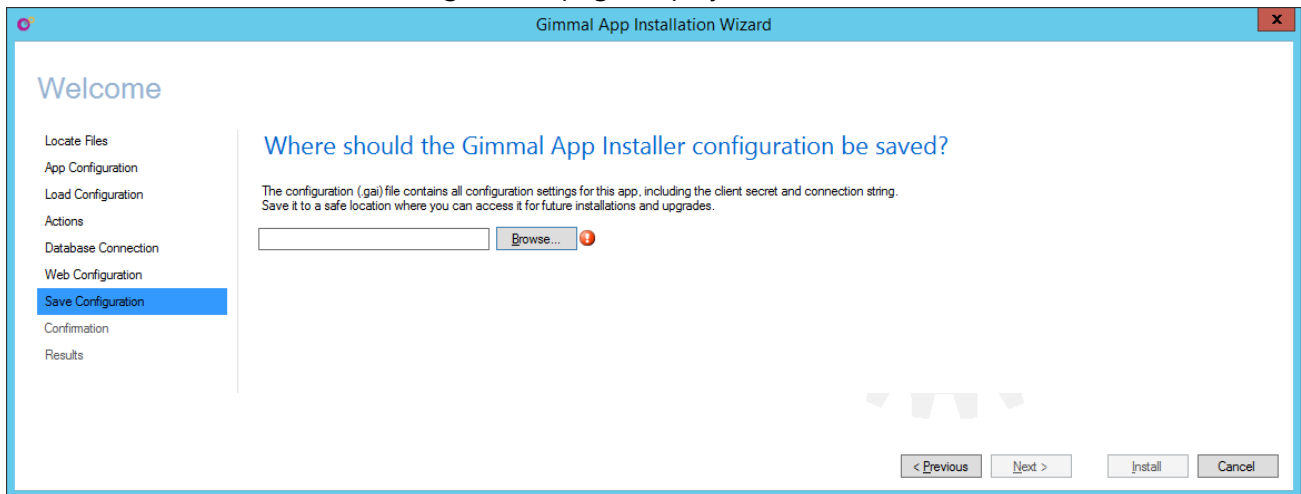


Figure 9 Save Configuration Page

16. Specify a **.gai** file where you want to save the configuration as a text file.

## Important!

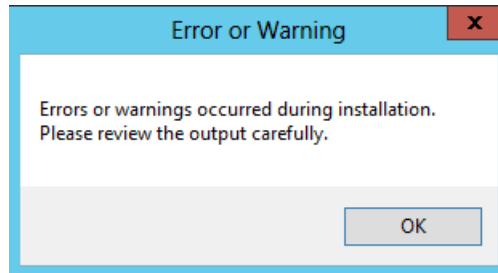
The **.gai** file contains sensitive information, such as the client secret, connection string, etc., but is not read-only and can be modified. Therefore, save it to a secure location to avoid errors when trying to re-install or upgrade!

17. Click **Next**. The Review the configuration page displays.

18. Confirm all the information provided, then click **Install**.

19. Wait until the **Success** message displays indicating that the App installer is successfully completed.

If you receive an error message like the one that follows, review the information you entered in the configuration to ensure it is correct. If the information is correct, copy the output to a text file, which can be sent to Gimmel Support Services, if required.



*Figure 10 Installation Error Message*

### Important!

You can also review the results of the installation in the `GimmelAppInstaller.log` file in the same directory where you accessed the `GimmelAppInstaller.exe` file. Every installation is appended to this log file.

## Upgrading Gimmel Apps

This section provides step-by-step instructions for using the Gimmel App Installer to upgrade a Gimmel App. You must copy the App Installer and app on each server where they will be used.

### Downloading the Latest Version of the App Installer

Gimmel App Installer is distributed separately from other Gimmel products. You must have System Administrator privileges to install apps.

#### Important!

The installer window is not resizable.

Follow these steps to download the app installer:

1. Download the app you plan to deploy from the Gimmel Software Download site at: <https://clients.gimmel.com/sites/gimmalsoftdownload/SitePages/Home.aspx>
2. Once downloaded, right-click on the .zip file and select **Properties** from the menu. The Properties dialog displays.
3. On the **General** tab, ensure that **Unblock** is selected so that the zip file is not blocked when you try to unzip it. This setting depends on the server's security configuration.
4. Unzip the package.
5. Follow steps 1 through 4 for the app installer package.
6. Select the appropriate deployment scenario and deploy the app installer according to your scenario.

### Upgrading an App Using the Installer

This section provides the steps for upgrading an app using the app installer. You must perform these steps on the WFE server where the previous app was installed using an account that is a member of the Farm Administrators group in the SharePoint Farm.

Follow these steps to upgrade a Gimmel app using the installer:

1. Open the App Installer folder you previously downloaded (refer to "Downloading the Latest Version of the App Installer"), right-click `GimmelAppInstaller.exe`, and then select **Run as administrator** from the menu. The Gimmel App Installation Wizard displays.

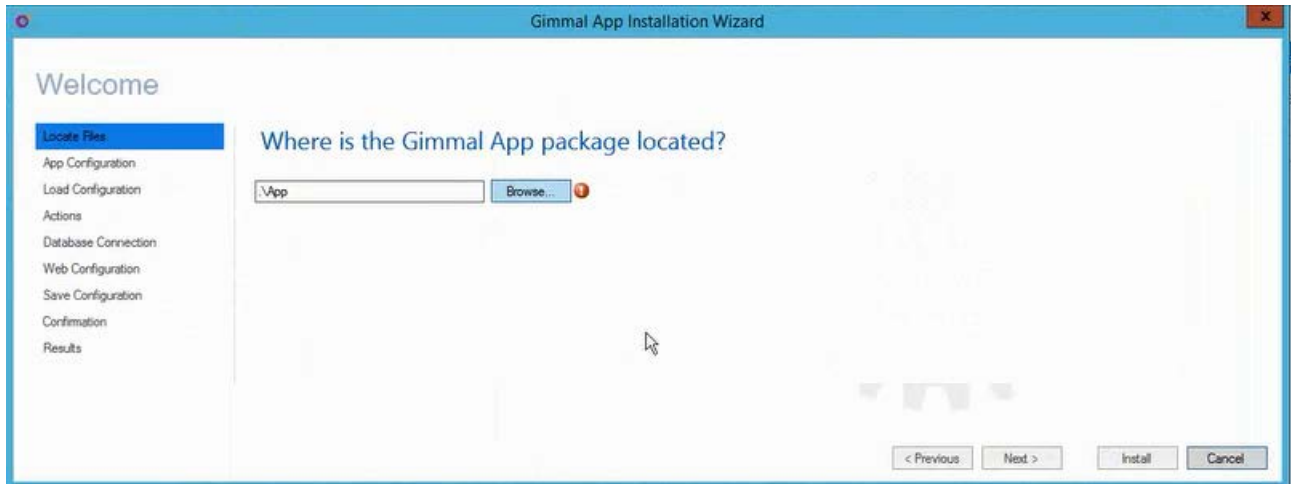


Figure 11 Locate Files Page

2. On the Locate Files page, click **Browse** and select the folder for the app that you want to deploy.
3. Click **Next**. The App Configuration page displays if the app contains a SharePoint app. If the app does not contain a SharePoint App, go to step 5.

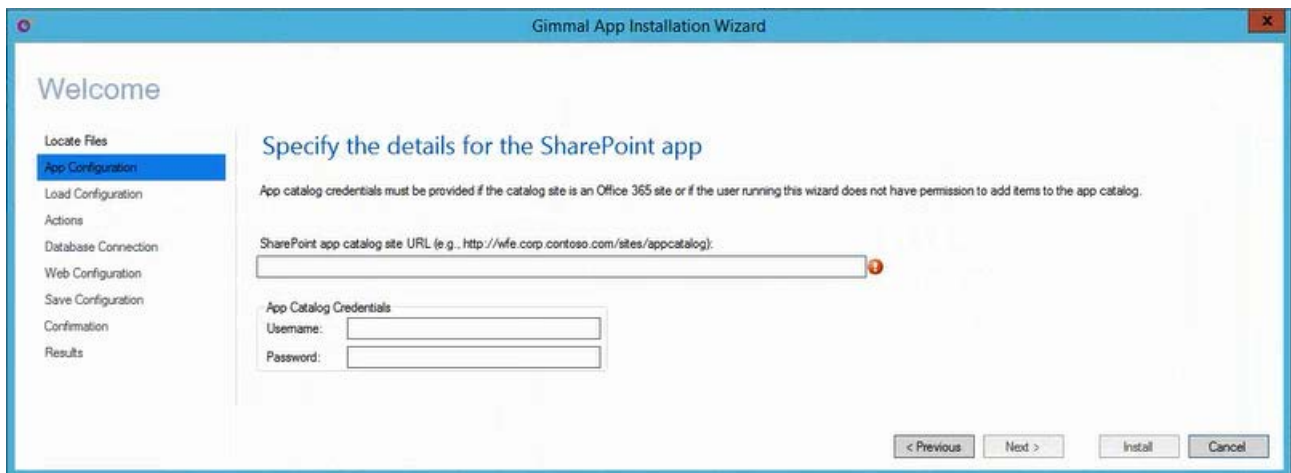


Figure 12 App Configuration Page

4. In the **App Configuration** page:
  - a. In **SharePoint app catalog site URL**, provide the app catalog URL. To find the URL, follow these steps:
    - i. From the main page in Central Administration, click on **Apps** in the left navigation. The Apps page displays.
    - ii. Under **App Management**, select **Manage App Catalog**. The URL displays next to **Web Application** on the right side.

- b. If you are installing as a user that does not have permission to add items in the app catalog, enter the **Username** and **Password** for the site in **App Catalog Credentials**.
5. Click **Next**. The app installer verifies the app catalog and the Load Configuration page displays with the information for the previously installed app.



Figure 13 Load Configuration Page

### Important!

If you are upgrading an app that does not require an app catalog, the Load Configuration page is optional. Leave the configuration file location field blank and click **Next** if this is the case.

6. Click **Browse** to locate the load configuration (.gai) file that was saved from the previous install.
7. Click **Next**. The **Actions** page displays with the previous install's information prepopulated.

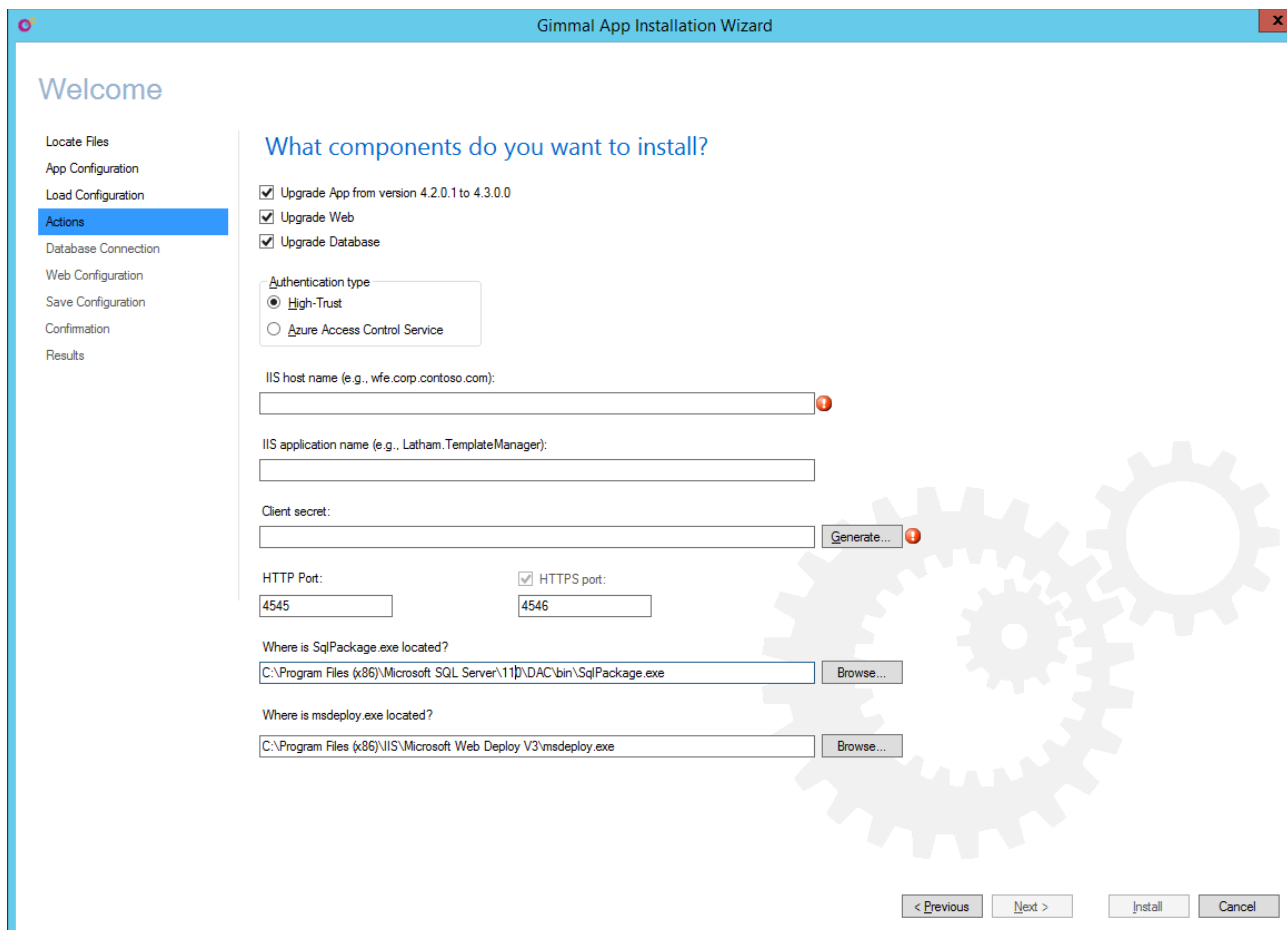


Figure 14 Actions Page

8. In the Actions page:
  - a. Verify that the **Update App from version <X.X.X.X> to <X.X.X.X>** and **Upgrade Web** checkboxes are checked. The **Upgrade Database** checkbox should only be checked if the app you are going to install requires access to a database.
  - b. Ensure that the correct **Authentication type** is selected.

### Important!

If you are using both on-premises and O365 installations, you must have two separate webs; one to service high trust and one to service ACS/O365. You must run the installer for each web, selecting the appropriate **Authentication type**.

- c. Verify the **IIS host name** and **Client Secret**. You can leave **IIS application name** blank if you are installing in the root of a website.
- d. Verify the port numbers (automatically populated):

- **HTTP Port** – Port used for HTTP requests
- **HTTPS Port** – Port used for HTTPS requests

## Important!

HTTPS must be checked before you can select **Next**. You must use HTTPS to install apps.

- e. Verify the **Where is SqlPackage.exe located?** field. It should automatically populate.
  - f. Verify the **Where is msdeploy.exe located?** field. It should automatically populate.
9. Click **Next**. The **Database Connection** tab displays if you selected to **Upgrade Database** in the previous step. If you are not installing a database, go to step 12.



Figure 15 Database Connection Tab

The correct **Database connection string** from the previous install should display. If it does not, follow the steps for building a connection in the previous section.

10. Click **Next** on the Database Connection tab. The Web Configuration tab displays.



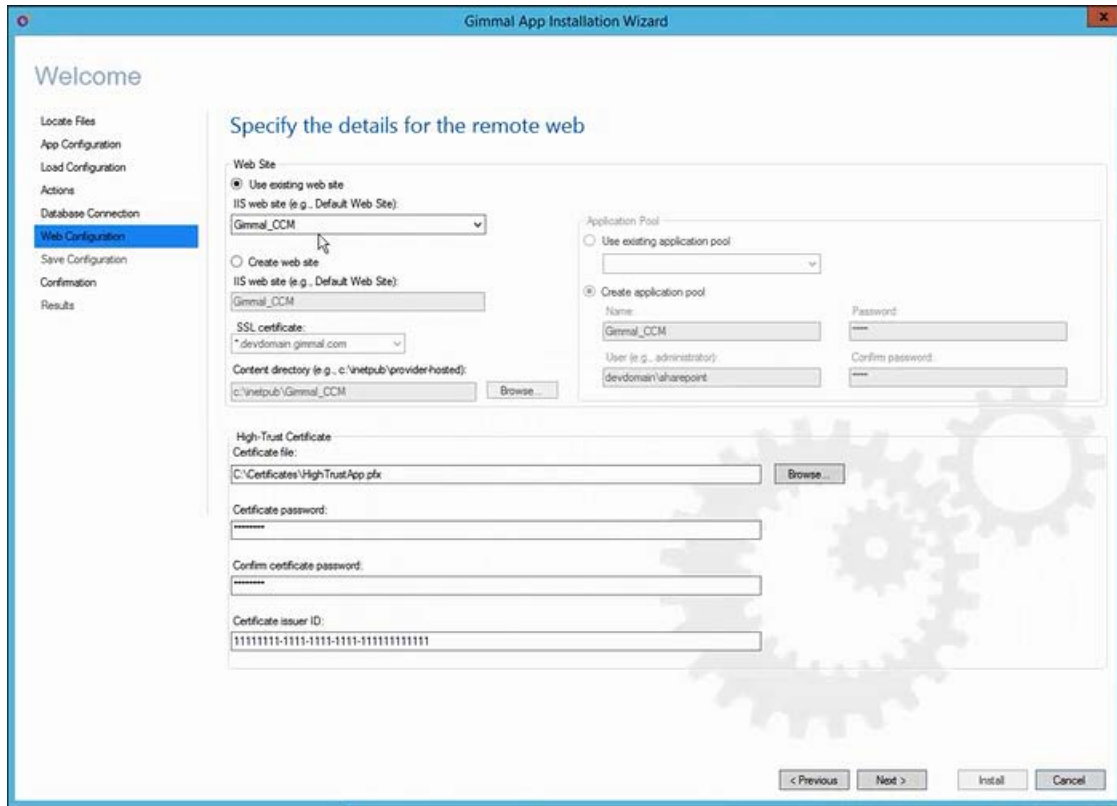


Figure 16 Web Configuration Tab

11. Select **Use existing web site**. The previously used website, certificate, and password information are automatically selected. By using the existing web site, the existing app pool is used.
12. Click **Next**. The Review the configuration page displays.

### Important!

If you changed any configuration information, the Save Configuration page displays asking where to save the configuration. The selection defaults to the previous .gai file and warns you that it will overwrite it. Either **Browse** to select a new location or click **Next** to overwrite it.

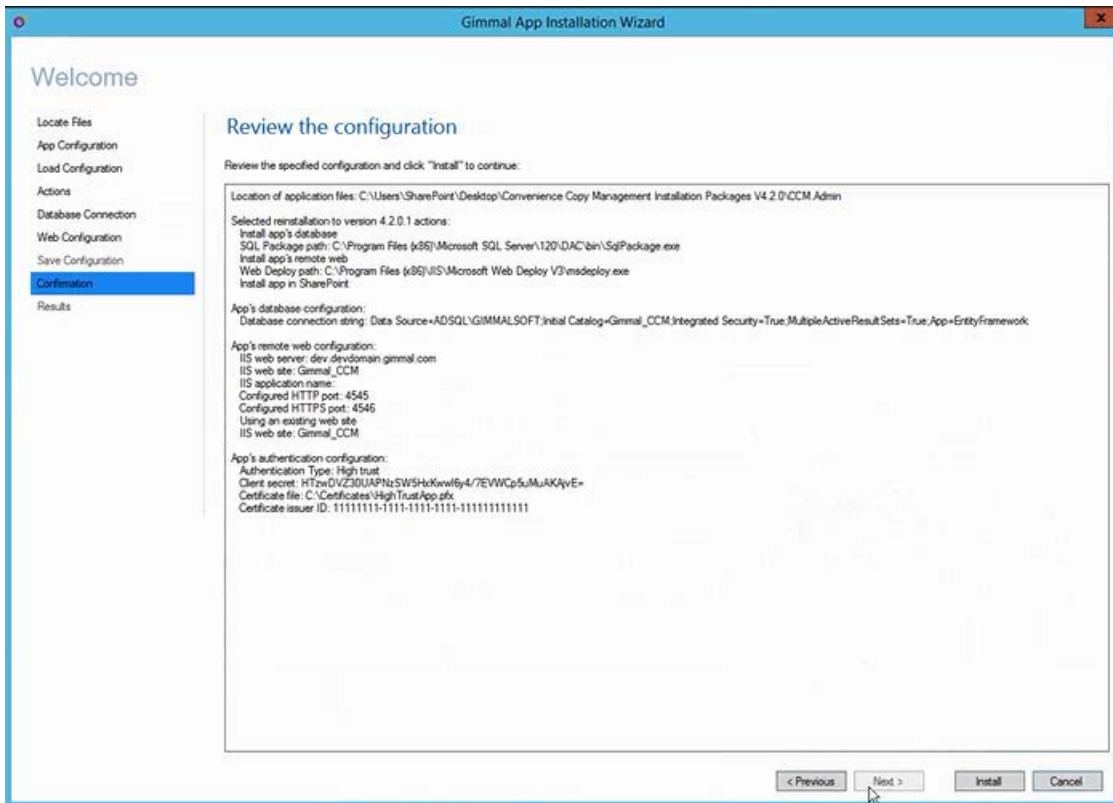


Figure 17 Review the Configuration Page

### Important!

Notice that the version number increased from 4.2.0.0 to 4.2.0.1. For every installation of the same app version, the last (fourth) digit increments by one. You must upgrade the app in SharePoint to reflect any configuration changes you made during the app upgrade using the installer.

13. Confirm all the information provided, then click **Install**.

14. Wait until the **Success** message displays indicating that the App installer is successfully completed.

If you receive an error message like the one that follows, review the information you entered in the configuration to ensure it is correct. If the information is correct, copy the output to a text file, which can be sent to Gimmel Support Services, if required.

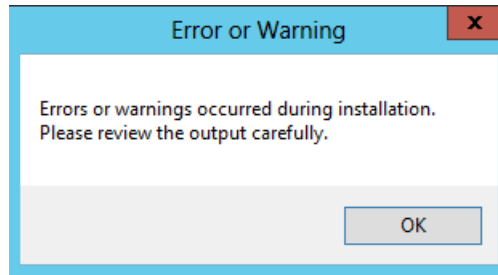


Figure 18 Installation Error Message

## Important!

You can also review the results of the installation in the `GimmelAppInstaller.log` file in the same directory where you accessed the `GimmelAppInstaller.exe` file. Every installation is appended to this log file.

## Upgrading an App in SharePoint

If you want the changes you made by upgrading the app using the app installer to be reflected in SharePoint, you must follow these steps.

Follow these steps to upgrade the app:

1. Using SharePoint, go to the installation site where you installed the original app.
2. Go to Site Contents and select the app you are upgrading.
3. From the app settings that display, click **ABOUT**. The app's details display.

**Gimmel Drop Zone**  
from Gimmel, LLC

**Details**

The Drop Zone app extends SharePoint's drag and drop capabilities, both in document libraries and as a stand-alone web part. It is intended as a component for team collaboration or department sites. For other Gimmel SharePoint apps to accelerate your SharePoint deployments and provide governance, check out the Gimmel App Store.

ADD IT

There is a new version of this app. Get it now.

GET IT

VERSION	4.3.0.1
RELEASE DATE	November 2014
CATEGORY	Gimmel
SUPPORT	<a href="#">App Website</a>

Figure 19 App Details

You can see that there is a new version of this app on the right side.

4. Click **GET IT**. A dialog displays asking if you want to trust the app.
5. Click **Trust It**. The app updates, which you can verify by viewing the app settings and the updated version number.

## Configuring IIS Settings for High Trust Apps

If the remote web is configured for high trust, you must set the authentication type to **NTLM** in the IIS manager. By default, **Negotiate authentication** is selected. You must set the authentication type for all apps.

Follow these steps to configure IIS settings for high trust:

1. Launch IIS as the administrator. In the **Connections** pane on the left, expand the tree under Sites and select the Site that you created or used during the installation (**App Webs** in the following figure).
2. Double-click **Authentication** in the right-hand pane.

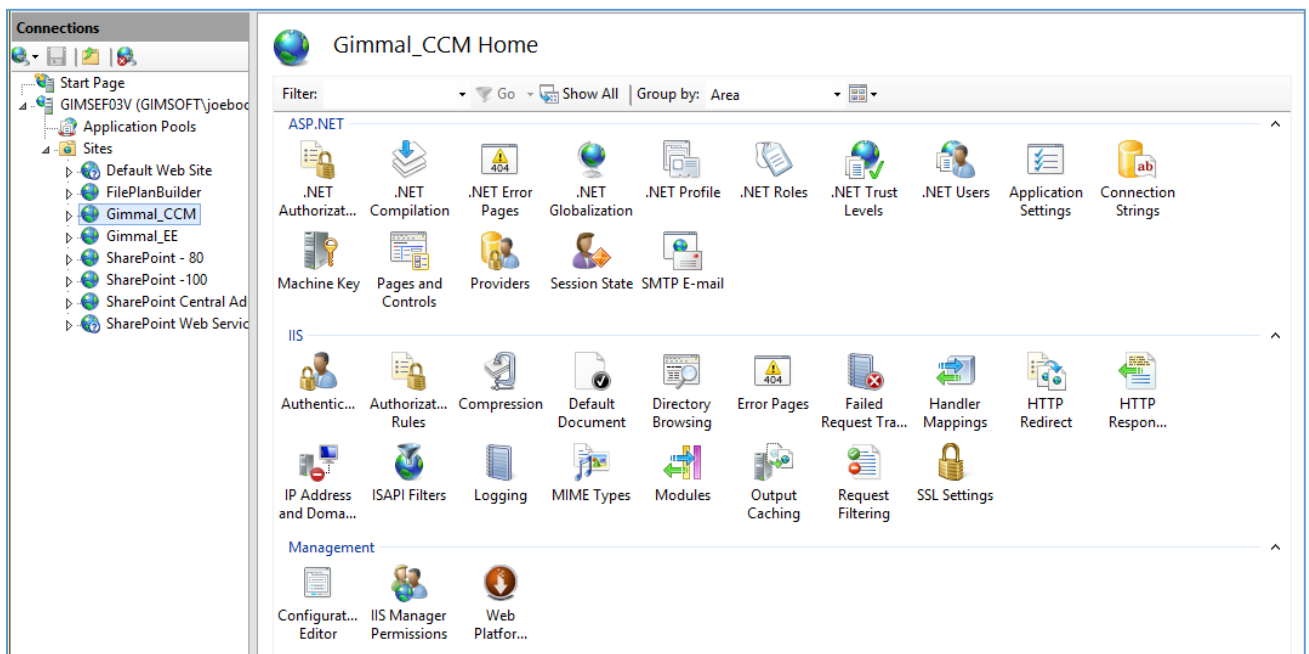


Figure 20 Selecting an App for Configuration

3. Ensure that the Windows Authentication entry is enabled. If not, right-click the entry and select **Enable**.

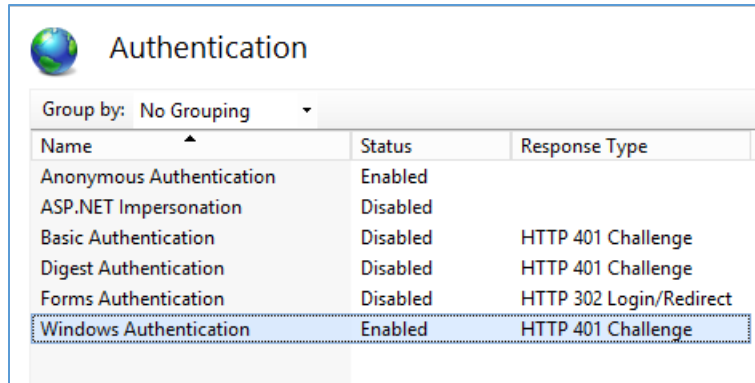


Figure 21 Enabling Authentication

- Click **Providers...** under **Actions** in the right-hand pane. This option is available from the right-click context menu.

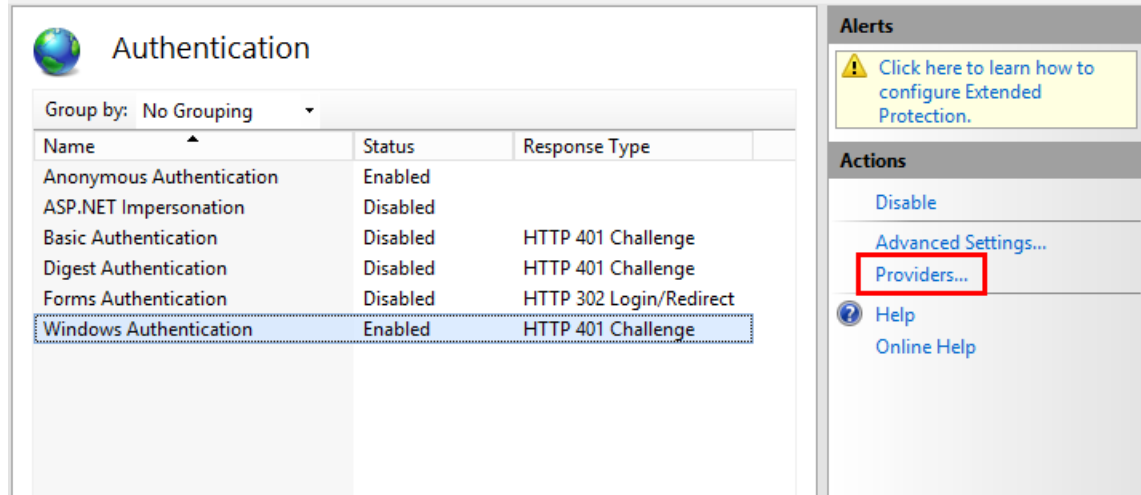


Figure 22 Selecting Providers

- Highlight **NTLM** and make sure it displays as the first entry by clicking **Move Up**. Click **OK**.

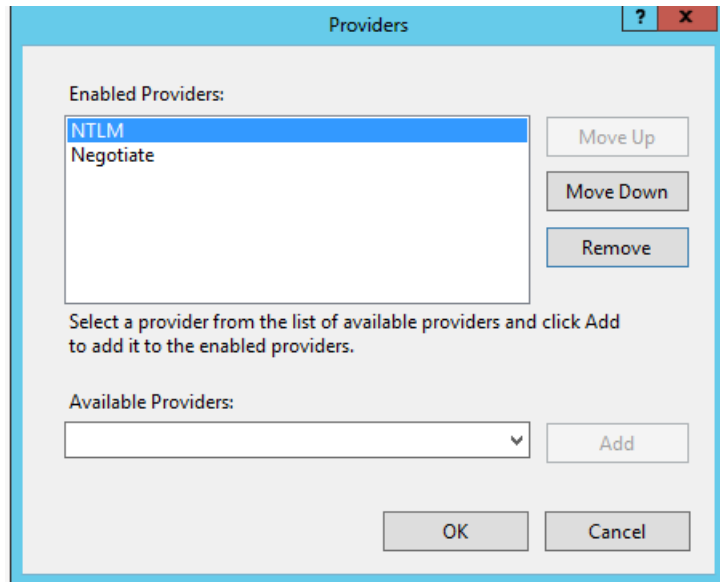


Figure 23 Selecting NTLM

## Uninstalling an App

This section describes how to uninstall Gimmel apps from a SharePoint environment.

To remove an app, you must remove it from a site(s), the SharePoint 2013 or Office 365 App Catalog, remove the remote web from the IIS server, and then remove the app principal (removing the app principal applies only to O365/SharePoint Online).

### Removing an App from a Site

See the “Uninstallation” section in each app’s configuration guide for detailed steps on how to remove an app from a site.

Note
<p>To completely remove an app from a site, you must:</p> <ul style="list-style-type: none"><li>• Navigate to the Site Contents page and remove the app.</li><li>• Remove the app from the first-stage recycle bin.</li><li>• Remove the app from the second-stage recycle bin.</li></ul>

### Removing an App from the App Catalog

Perform the following steps to remove apps from the SharePoint 2013 or Office 365 App Catalog site:

1. Navigate to the SharePoint 2013 or Office 365 App Catalog site. The App Catalog page displays.
2. Select **Apps for SharePoint** from the left navigation. The Apps for SharePoint page displays showing the list of installed apps.
3. Select the ellipsis (...) next to the app you want to delete. The app’s context menu displays.
4. Select the ellipsis (...) on the app’s context menu. Another menu displays.
5. Select **Delete**. You are prompted to confirm the deletion.
6. Click **OK**. The app is removed from the App Catalog.

### Removing an App’s Remote Web from Internet Information Server (IIS)

Perform the following steps to remove an app’s remote web from IIS.



## Note

The following steps show how to remove the News app's remote web, as an example, but the steps apply to any of the Gimmel apps.

1. Open Internet Information Server Manager.
2. Navigate to the News remote web under the Sites folder.
3. Right-click on the News remote web and select **Deploy > Delete Application and Content**. You are prompted to confirm the deletion.

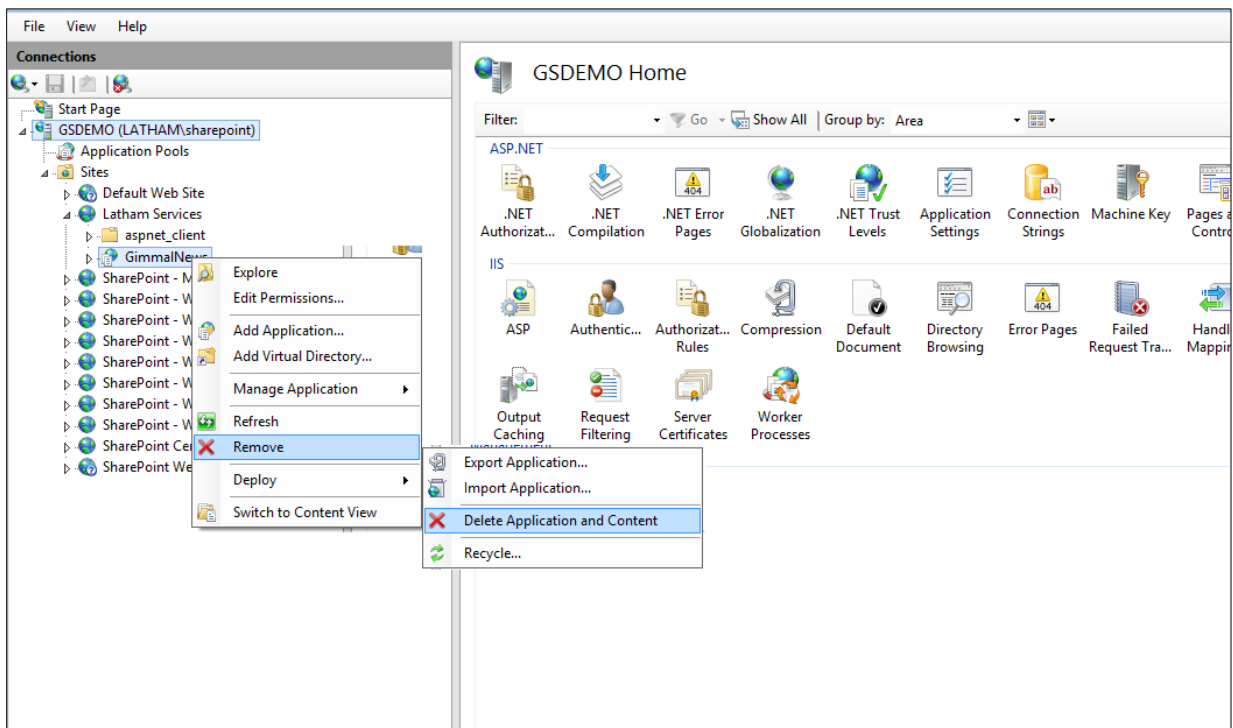


Figure 24 Deleting the Remote Web from IIS

4. Click **OK**. The News remote web is deleted.