BeyondTrust

Privileged Identity Upgrade Guide

TC:3/26/2020

Table of Contents

Upgrade Privileged Identity

This guide describes how to upgrade Privileged Identity from a previous installation.

Please visit the Product Change Log to get the details of each release of BeyondTrust remote support software.

For versions prior to 5.5.3.0, you can upgrade from a previous version to version 5.5.3.0 without first having to upgrade to an intermediate version. For versions after 5.5.3.0, you must upgrade to 5.5.3.0 before upgrading to the latest version.

Note: *Upgrading causes some saved preferences to reset to default values. If you configured the management console to hide certain account store types, plan on reapplying those settings following the upgrade.*

Prior to upgrading, be sure to back up the program's database. During the upgrade, structures within the database are updated and may not be compatible with older versions of the product.

If the program database is still running on SQL Server 2005 or older, the database will need to be re-hosted to SQL Server 2012 or newer prior to upgrade.

- If upgrading from version 4.83.4 or older and you are running the solution on a Windows 2003 Server, you must migrate the installation to a Windows Server 2012 or later operating system. Privileged Identity is not supported on any version of Windows Server prior to Windows Server 2012. Contact a BeyondTrust account representative for more information.
- Versions of the product prior to version 4.83.4 did not use ASP.NET. The ASP.NET IIS role must be installed and enabled prior to upgrading to this version.
- Starting with version 5.5.2 of the product, Microsoft .NET Framework version 4.5.2 is a requirement for all components of the solution.
- Starting with version 5.5.2 of the product, the web service is a requirement for the web application to function. This also adds new requirements to the host servers.

For more information on prerequisites prior to upgrading, please see Install Privileged Identity Prerequisites at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/index.htm.

Upgrade Roadmap

The following roadmap outlines the steps to follow to install Privileged Identity.

1. **Back up the solution's data store and encryption key.**
    - If there are any difficulties during or after upgrade and a rollback is required, the upgraded database may prevent previous functionality from working. The database and encryption key (or related settings) are required for disaster recovery purposes.
2. **Understand the product requirements prior to installation.**
    - Check the release notes for important information on this release of the product.
    - Ensure you are prepared for the installation.

    For more information, please see Install Privileged Identity Prerequisites at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/index.htm.

3. **Stop the existing Deferred Processing Service.**
    - Use the management console or Windows Services snap-in to stop the existing deferred processing service.

    Note: *In product versions 5.5.2 and earlier, the Deferred Processing Service was called "Enterprise Random Password Manager Deferred Processing Service".*

4. **Stop and remove any existing zone processors.**
    - If upgrading from version 5.5.0 or later, it is sufficient to re-copy and replace the updated zone processor files and upgrade the integration components and cross-platform support library. Be sure to take notes on the current configuration.
    - If upgrading from version 5.4.0 or earlier, zone processors should be removed first, then re-installed due to file and registration differences. Failure to do so will render the zone processors inoperable. Be sure to take notes on the current configuration.
5. **Remove existing web sites.**
    - If upgrading from version 5.5.2 or earlier, the web site registration and naming process follows a different process than 5.5.2.1 or later. Failure to remove existing web sites will cause multiple registrations with different names to appear in the web site registration dialog and can cause your security and other settings not to take effect.
6. **Install the base Privileged Identity program.**
    - This step will install the management console.

    For more information, please see Install the Management Console at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/index.htm.

7. **Configure and Register Privileged Identity.**

- **Complete the setup wizard.**

  The first time Privileged Identity is run, a mini-setup wizard will run through a series of pages that handle the configuration of the various components of the product, such as database connections and encryption settings. Don't worry if you do not yet have all information required at this point, as all configurations may be performed or changed after the installation, as well.

  > For more information, please see the setup wizard at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/program-database.htm.

- **Register Privileged Identity.**

  Completing the **Registration** dialog enables switching from demo mode to extended demo mode or switching from demo mode to commercial mode.

  > For more information, please see Register the Privilege Identity Instance at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/registration.htm.

- **Configure permissions to launch the management console (optional.**

  Following installation, any user who is an administrator of the system where the management console is installed and who also has access to the program data store will have the ability to launch the application. Configuring these permissions allows you to enable MFA requirements for launching the console as well, as define what aspects of the management console are available to users of the console.

- **Configure database settings (optional).**

  If necessary, reconfigure database settings such as provider, connection limits, or connection strings for high-availability configurations.

  > For more information, please see Configure Database Settings in the admin guide at https://www.beyondtrust.com/docs/privileged-identity/documents/5-5-5/pi-admin-5-5-5.pdf.

- **Configure encryption settings (optional).**

  Passwords managed by Privileged Identity are encrypted and then stored in the secure data store. The use of HSM or software-based encryption is supported at all times and may be changed at any point in time.

  > For more information, see the Configuring Encryption Settings in the admin guide at https://www.beyondtrust.com/docs/privileged-identity/documents/5-5-5/pi-admin-5-5-5.pdf.

8. **Install the web application.**

   - The web application is used by consumers and auditors. Consumers will retrieve secured passwords or establish sessions through a delegated and audited process. Auditors will be able to generate reports and audit settings.

> For more information, please see Install the Web Application at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/web-application.htm.

9. **Install the web service.**

   - The web service provides API-based functionality via a SOAP or REST-based URI and is required by the web application, PowerShell, federated logins (SAML/OAUTH), and application launcher modules. The web service is deployed from a separate installer or can be pushed from the management console with version 5.5.2.1 of the product or later.

   > For more information, please see Install the Web Service at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/web-service.htm.

10. **Install one or more zone processors (optional).**

    - A zone processor is a remotely deployed scheduling service designated to perform specific jobs against a specific list (management set) of systems and devices. Conversely, the default deferred processor is installed with the management console and will handle any configured jobs against any and all lists of systems. Zone processors are typically used in DMZs or distributed networks where normal communication may not be allowed. Zone processors are also used to improve the job processing throughput of the entire solution. Zone processors may also require secondary installations of integration components and the cross-platform support library.

    > For more information, please see Deploy Zone Processorsat https://www.beyondtrust.com/docs/privileged-identity/deployment/deploy-zone-processors.htm.

11. **Install the PowerShell cmdlets (optional).**

    - PowerShell cmdlets extend the management of Privileged Identity to a command line scripting environment.

    > For more information, please see Installing the PowerShell Cmdlets in the Privileged Identity PowerShell API Guide, pages 8-11 at https://www.beyondtrust.com/docs/privileged-identity/documents/5-5-5/pi-powershell-api-5-5-5.pdf.

12. **Install the application launching and session recording components (optional).**

    - Application launching allows users to enter a privileged session without gaining access to the underlying credentials (password, key, etc.) using a secured host where session recording may also be enabled for the session.

    > For more information, please see Installing the Application Launcher and Session Recording at https://www.beyondtrust.com/docs/privileged-identity/app-launcher-and-recording/installation/index.htm.

13. **Install the Syslog Forwarder Service (optional).**

- This service is listed for syslog UDP traffic and retransmits it using SSL or TCP on the same or different port for greater security and reliability when forwarding events to loggers and SIEM products.

  For more information, please see *Using the Syslog Forwarder to Forward Syslog & MSMQ* in the Privileged Identity Admin Guide, at https://www.beyondtrust.com/docs/privileged-identity/documents/5-5-5/pi-admin-5-5-5.pdf, page 468.

If you are ready to begin your upgrade to the latest version of Privileged Identity, be sure to first visit Install Privileged Identity Prerequisites at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/index.htm.

Prepare for Upgrade

As a best practice, back up the system prior to performing an upgrade. If, after upgrade, you should need to restore the previous installation, you must have:

- A recent backup of the database prior to the upgrade. This is performed within SQL Server, not in Privileged Identity.
- The encryption key. This can be found in the management console by going to **Settings > Encryption Settings**, then clicking the **Export** button and saving the file to a secure location. If using a hardware security module (HSM), be sure you know the key store and PIN to access your HSM.
- The previous installation software.

> ***Note:*** *If the management console is installed on a virtual machine, it may be prudent to simply snapshot the virtual machine.*

Upgrade Outline

1. Stop the deferred processing and zone processor services. This ensures that jobs will not be processed during the database upgrade and helps prevent any data loss or corruption.
2. Stop the web application and web services. This ensures users will not be able to generate new database activity (jobs, auditing, etc.) while the upgrade takes place.
3. Upgrade the console.
4. Deploy the upgraded web application and web service.
5. Deploy the upgraded deferred and zone processor services.
6. Deploy ancillary components such as PowerShell, application launcher, etc.

Stop the Existing Deferred Processing Services

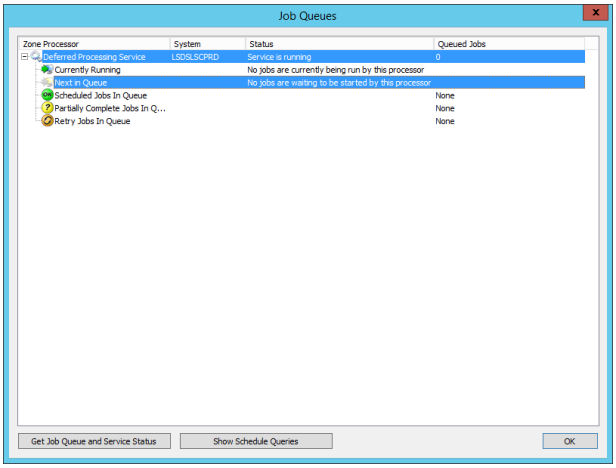
1. From the management console, click **Jobs** from the left action pane.
2. On the **Stored Jobs** dialog, click **Job Queues**.
3. On the **Job Queues** dialog, select all items of type **Deferred Processing Service** and click **Get Job Queue and Service Status**.
4. Immediately expand each **Deferred Processing Service** and check the status column for **Currently Running**. The status should indicate **No jobs are currently being run by this processor**.
5. If the status indicates a job is running, it is best to wait for the job to finish or you may damage the job or cause other problems in your network due to a partially complete job. Further, if a job is running, also check the **Queued Jobs** column for the deferred processor and note how many jobs are in the queue to process. It will be best to wait for the jobs to finish or to take note of their Job IDs and disable them before they are run so you may perform the upgrade. When you start the processors post-upgrade, all past-due jobs will be run as soon as possible.
6. If the jobs list is empty, go to the Services snap-in within Windows, locate **RED Identity Management Deferred Processing Service**and stop the service.

> ***Note:*** *This service was called* ***Enterprise Random Password Manager Deferred Processing Service*** *in version 5.5.2 of the software.*

1. Repeat step 5 for each management console installed.

Stop Existing Zone Processors

1. From the management console, click **Jobs** from the left action pane.
2. On the **Stored Jobs** dialog, click **Job Queues**.
3. On the **Job Queues** dialog, select all items where the zone processor column is NOT listed as **Deferred Processing Service** and click **Get Job Queue and Service Status**.
4. Immediately expand each zone processor service and check the status column for **Currently Running**. The status should indicate **No jobs are currently being run by this processor**.
    - If the status indicates a job is running, it is best to wait for the job to finish or you may damage the job or cause other problems in your network due to a partially complete job. Further, if a job is running, also check the **Queued Jobs** column for the deferred processor and note how many jobs are in the queue to process. If will be best to wait for the jobs to finish or take not of their Job IDs and disable them before they get run so you may perform the upgrade. Don't worry, when you start the processors post-upgrade, all past due jobs will be run as soon as possible.
5. If the jobs list is empty, cancel the **Job Queues** dialog and click on **Zone Processors** from the **Stored Jobs** dialog.
6. Right click on each zone processor and select **Stop Service**. If there are any problems communicating with the services control manager on the remote systems, you will need to go to each system, open the **Services** snap-in within Windows, locate **RouletteSked${ZONE-NAME}** and stop the service.
7. Repeat step 6 for each zone processor.



Remove any Existing Deferred Processing Services if Necessary

IMPORTANT!

If you are upgrading from version 5.5.0 or later of the solution, you may simply replace key files on the zone processor host, or you may follow the removal/re-deploy steps that follow. If simply replacing the files, the file list is provided later in this process. If upgrading from version 5.4.0 or earlier, all previous zone processor installations should be removed. The required files and registry configurations have changed.

The method for removing zone processors depends on whether the remote zone processor host can be managed remotely from the management console or not.

> ***Note:*** *There is no way to tell in the console how a zone processor was deployed. If you are unsure, start by trying to remove the zone processor from the console. If there are any failures to communicate or perform the first action (file removal), stop and follow the steps in the alternate subsection below.*

If the remote zone processor host can be managed remotely from the management console and was deployed by the management console:

1. From the management console, click **Jobs** from the left action pane.
2. From the **Stored Jobs** dialog, click **Zone Processors**.
3. From the **Zone Processors** dialog, right-click the zone processors in question and select **Remove**.
4. You will be prompted to remove the service files, service registry settings, and finally the service registration. Select **Yes** for each prompt.

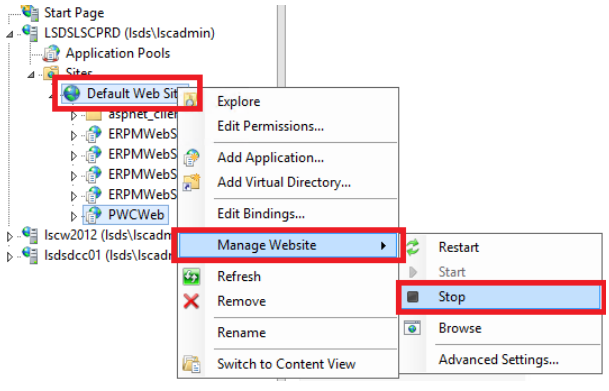
If the remote zone processor host was not deployed by the management console:

> ***Note:*** *There is no way to tell in the console how a zone processor was deployed. If you are unsure, start by trying to remove the zone processor from the console. If there are any failures to communicate or perform the first action (file removal), stop and follow the steps below.*

1. Log into the zone processor host.
2. Open **Programs and Features**.
3. Find the Zone Processor installer and remove it. It will have a name similar to **BeyondTrust Zone Processor**.
4. From the management console, click **Jobs** from the left action pane.
5. From the **Stored Jobs** dialog, click **Zone Processors**.
6. From the **Zone Processors** dialog, right-click the zone processors in question and select **Delete Registration**.

Stop the Web Application and Web Service in IIS

1. Open IIS on the web application and web service hosts.
2. Expand the host server.
3. Expand Sites.
4. Right-click on the parent root web site, and then click **Manage Web Site > Stop**.
5. Repeat this step for each web application and web service host.



Stop the Web Application and Web Service COM+ Applications

1. Open **Component Services** (dcomcnfg.exe) on the web application and web service hosts.
2. Expand **Component Services**.

3. Expand **Computers**.
4. Expand **My Computer**.
5. Select the **COM+ Applications** folder.
6. Shut down the COM+ application:
    - For the web application, right click on **PWCWebComApp**, and then select **Shutdown**.
    - For the web service application, right-click on the web service, and then select **Shutdown**.

Upgrade the Management Console

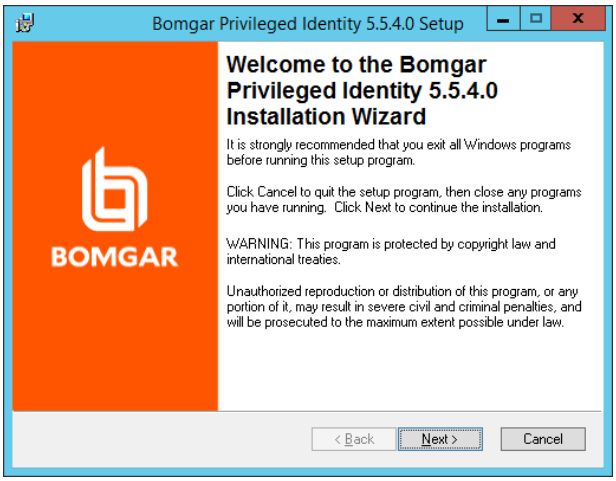
An upgrade installation is very much like an initial installation with the exception that things like email database configurations, and registration configurations have already been performed.

Before installing the management console, ensure your host server meets the prerequisites as defined in Host System Requirements at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/host-system.htm.

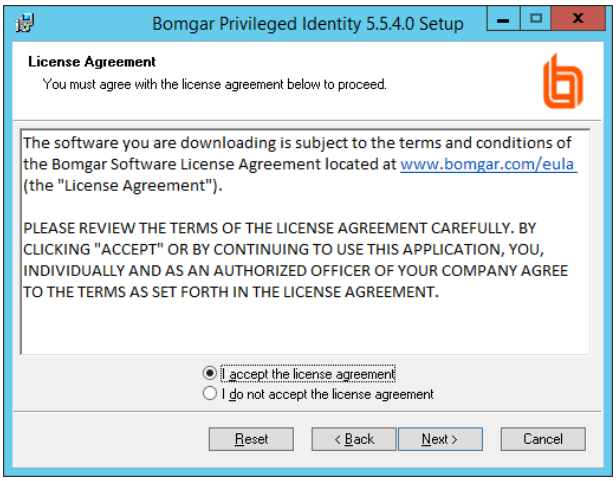
After upgrading the management console and before performing any other steps, be sure to launch the management console at least once. This step is required to upgrade the database.

If you have multiple management consoles, upgrade your primary licensed management console first, launch that console, then upgrade any other management consoles.

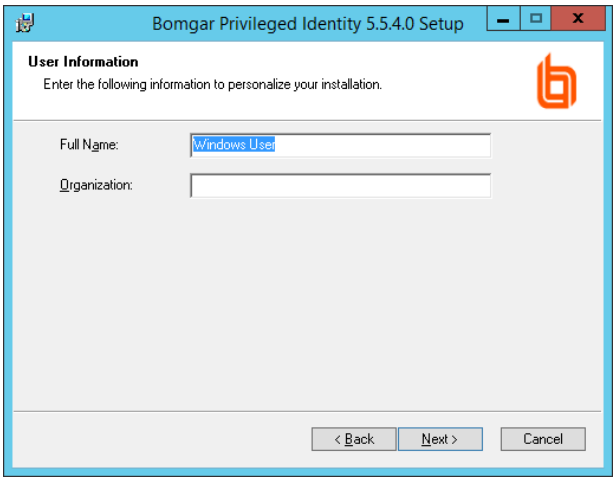
1. Launch the Privileged Identity installer.
2. On the **Welcome** screen, click **Next**.



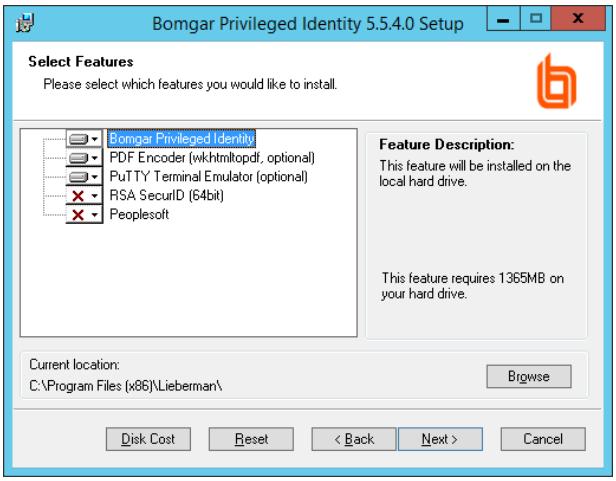
3. Read the entire license agreement. If you agree, select **I accept the license agreement**, then click **Next**.



4. Enter your name and organization name, then click **Next**.

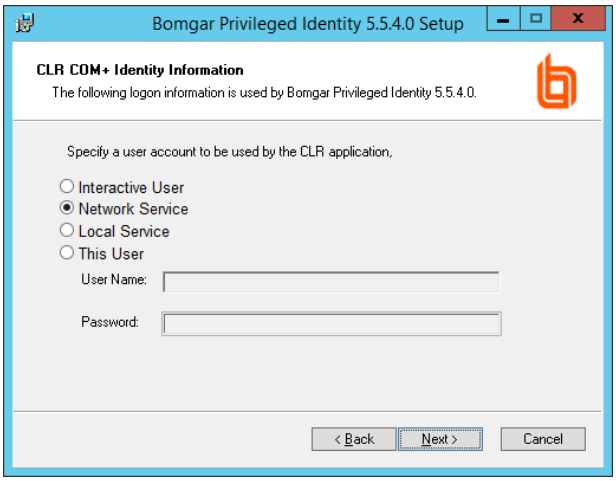


5. Select the features to install:
   - **Privileged Identity** is the only required element.
   - **PuTTY Terminal Emulator**: installs the open source PuTTY software.
   - **PDF Encoder** (recommended): provides Privileged Identity the ability to turn its compliance reports into PDF documents.
   - **RSA SecureID**: install this option if RSA multi-factor authentication will be required to access the management console, but this machine will NOT host the web application. If this machine will host the web application, leave this option unselected, as the application will be installed automatically when the web application is installed.

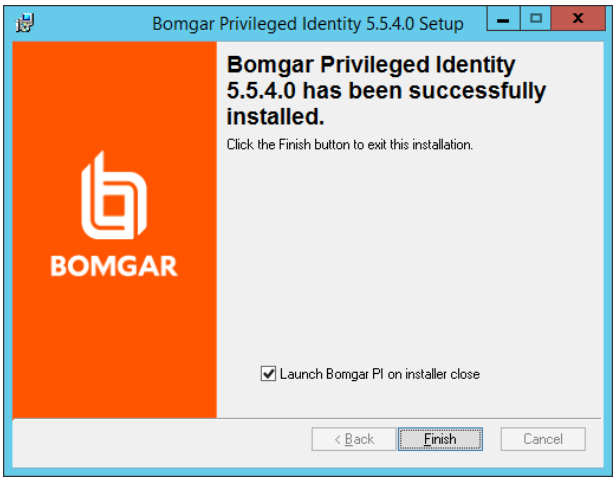


6. If necessary, click **Browse** to change the default installation folder. If you have doubts about your available disk space, click **Disk Cost**.
7. Click **Next**.

8. Choose the identity to run the CLR COM application. The default is **Network Service**. The CLR COM Identity is used to provide network and local system access for the solution to various cloud services. Individual account stores (Azure, AWS, ESX, etc.) will be configured with specific connection credentials when they are enrolled. Options for the identity are:



   - **Interactive User**: Use the same logon information as the calling identity. This is an administrator-level account because the calling identity will either be the admin running the console or the deferred processor service account. This option requires the least configuration but provides significantly more privileges than is required.
   - **Network Service** (recommended): Use the network service account. For this option you do not have to manage a password or grant additional rights, although in some cloud management cases, you may need to grant additional permissions on the file system.
   - **Local Service**: Use the local service account. For this option you do not have to manage a password or grant additional rights, although in some cloud management cases, you may need to grant additional permissions on the file system. The local service account has many more rights and privileges than the network service.
   - **This User**: Use a specified username and password. This user could be a local account that is configured to never authenticate to any other machine in the network (unlike network service or local service), but it does represent another account to manage a credential for. In some cloud management cases, you may need to grant additional permission to it on the file system. This account also needs **Logon as a batch** rights granted to it.
9. Click **Next**.
10. Once the basic configurations are complete, click **Next**.
11. When you receive confirmation that the application has been successfully installed, click **Back** to make any needed changes or **Next** to complete the installation.



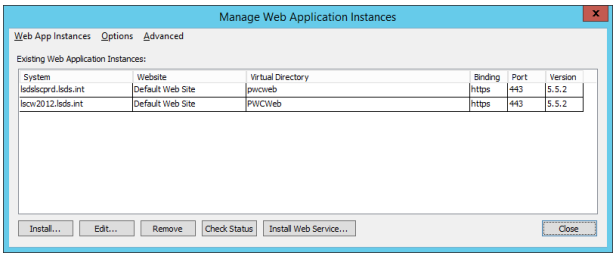
12. Launch the program to perform the database upgrade. After this step is complete, repeat steps 1-12 for all other management consoles.
13. Continue the installation by upgrading the web application, then web service, then deferred and zone processors.

Upgrade the Web Application

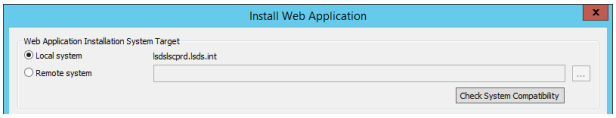
The web application is the primary mechanism for users to gain access to the credentials stored in the solution, whether managed or static, as well as to audit access to those credentials. The web application also performs other functions as well such as a secure file store, privilege escalation, and secure personal password store. This section shows how to install the web application from the management console.

> For more information on the web application host prerequisites prior to installation, please see Web Application Host Requirements at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/host-system.htm#WebApp.

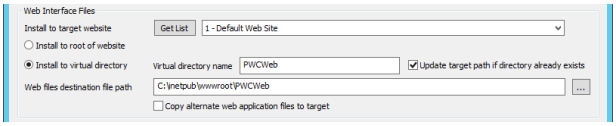
1. In the management console, click the **Manage Web App** button from the left action pane.
2. If upgrading from version 5.5.1 or earlier, select your web application from the list and click **Remove**. This step is necessary because the system name and registry settings have changed.
3. On the **Manage Web Application Instances** dialog, click **Install**, located in the lower left corner.



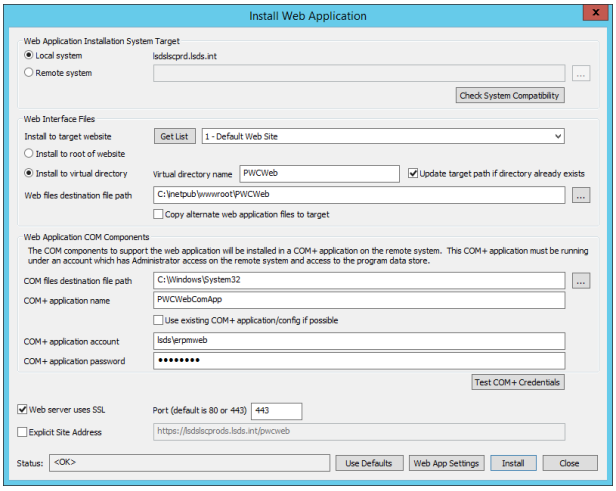
4. On the **Install Web Application** dialog, select the target installation system. **Local system** is the system you are on now. If installing to a remote system, supply the remote system name as fully qualified domain name.



5. Click **Check System Compatibility**. This will perform a check of the target system to validate IIS is accessible, the file system is accessible, and remote registry and remote COM+ access are possible. Fix any access errors before continuing. If the check proceeds without incident, the **Web Interface Files** section will be filled in automatically.
6. In the **Web Interface Files** section, supply the following information:
   - **Install to target web site**: any and all root web sites on the target server will be listed here. Choose the root web site to host the web application.

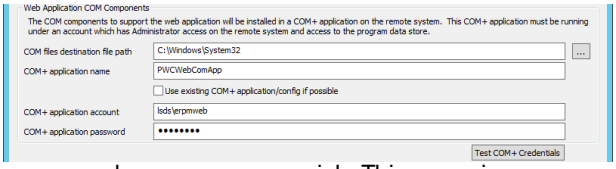


- Choose **Install to root of web site** or **Install to virtual directory**:
  - Installing to root of web site will replace the existing web site configuration at the targeted web site. The URL of the web application will simply target the name of the server. This makes it easier for end users torecall and type. If the web server is a shared server, you could inadvertently overwrite another web application.
  - Installing to a virtual directory is the safest option, as you will not overwrite any other applications if the target is a shared server. The default virtual directory name is *PWCWeb*. This name can be changed to any value permitted by IIS. The name supplied here will be appended to the server name. In the default case, the URL will target **https://serverName/pwcweb**.



- **Web files destination path**: this is where the web application files will be copied on the target server. The path is resolved from IIS on the target server, which defaults to **%inetpub%\wwwroot**. When installing to a virtual directory (default), the path is appended with the name of the virtual directory.
- **Copy alternate web application files to target** (not recommended): version 5.5.2 was the last version to provide official support for the legacy web application. Although it is still present in the current installer, it will be removed without notice from future iterations.

7. **Web Application COM Components** defines information for the COM application that will be responsible for data access from the web application to the solution data store. Supply the following information:



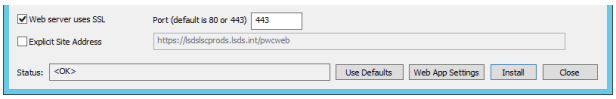
   - **COM+ files destination files path** - defaults to **C:\Windows\System32** and will install to \\serverName\admin$\syswow64 (**c:\windows\syswow64**). It is typically not necessary to change this setting.
   - **COM+ application name** - defaults to **PWCWebComApp**. You may supply any name you wish. This name is never visible to end users and is purely for identification when using the **Windows Components** snap-in.
   - **Use existing COM application/config if possible** - if upgrading from an existing installation, this will attempt to leave the existing COM application configurations intact and simply replace the required COM component files (**rouletteweb.dll**).
   - **COM+ application account** - this is the identity that will actually run the COM application. When using Integrated Windows Authentication, this is the account that will be responsible for data access from the database server on the web application's behalf. Enter the username as **DomainName\UserName**.

> For more information, please see Service Account Requirements at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/service-account.htm.

   - **COM+ application password** - this is the password for the COM application account.

8. Click **Test COM+ Credentials**. This will attempt to validate the credentials defined that are in fact valid credentials.

9. In the bottom section of the **Install Web Application** dialog, identify the use of SSL, provide a custom port if needed, or identify an explicit site address. Use an explicit site address when the URL to access the web application will be different than the **serverName** (or **serverName/virtualDirectoryName**). This would be the case when using a load balancer or if the server name will be aliased in DNS.



   - The information entered here has no functional effect on the web site regarding end users. It affects only the web application auto-launch capability from the **Manage Web Application Instances** dialog in the management console.

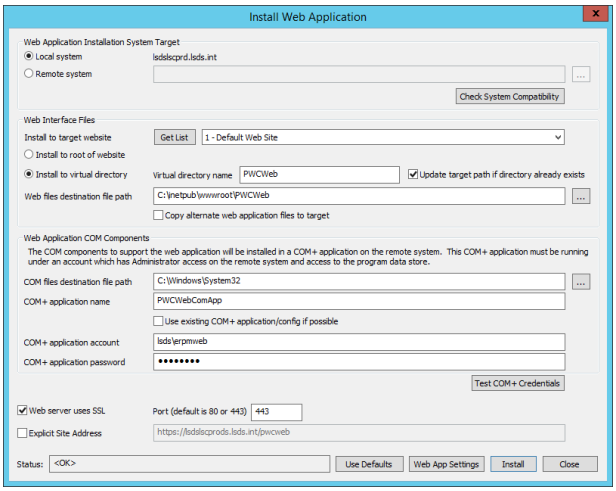
10. Click **Web App Settings** to configure additional web application options. These options affect security, sessions, and other integrations. For more information, please see Install the Web Application at https://www.beyondtrust.com/docs/privileged-identity/install/install-software/web-application.htm.

   - The one option you must specify is the **Web Service URI for REST web service endpoint** on the **App Options** tab. At this point, the web service is not yet installed. However, if the web service will be installed onto the same machine using default settings, the URI will be virtually the same as the URL mentioned above. For example, if the server is defined to use SSL in the previous step on the default port (443) and your SSL cert uses the FQDN of the server (e.g. example.int), then the URI to enter will be **https://servername.example.int/erpmwebservice/authservice.svc/REST**. Everything after your server name is **standard: /erpmwebservice/authservice.svc/REST**. If you were behind a load balancer and the name of the load balanced cluster was **secureidmstore.example.com** the URI to enter would be: **https://secureidmstore.example.com/erpmwebservice/authservice.svc/REST**.

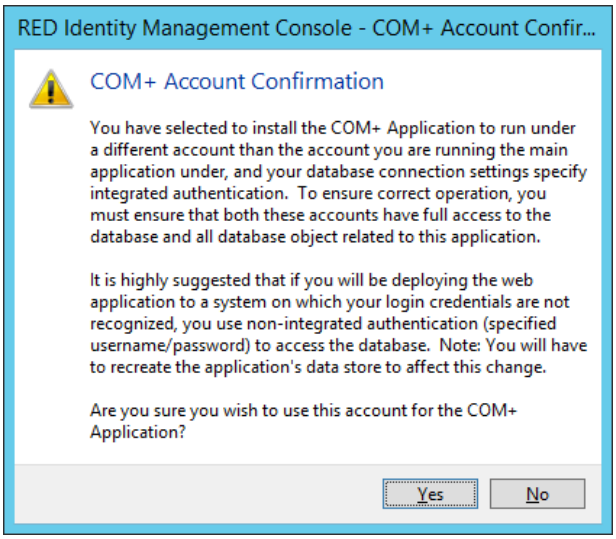
   - If any information changes, the information can be updated at any time.

11. Click **Install**.

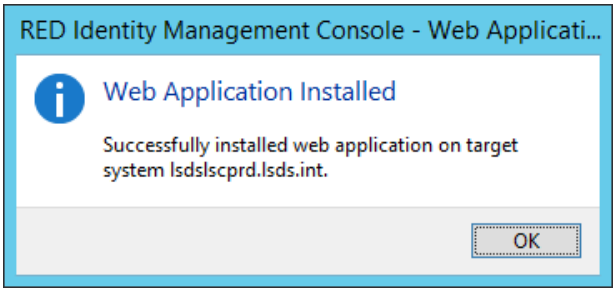
12. You may receive a **COM Account Confirmation** warning after clicking. This dialog will appear if the COM account specified on the installation dialog is different than the currently logged in user. The warning asks you to be sure that the account specified has data store access or the web application will fail to function until the access issue is resolved.



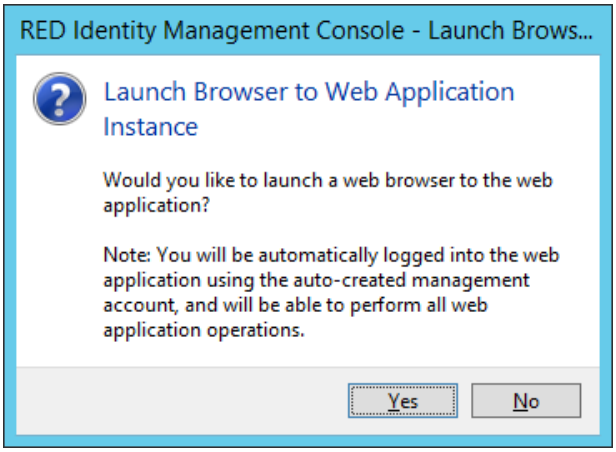
13. If you are sure about the account information, click **Yes** to continue or **No** to change to a different account.



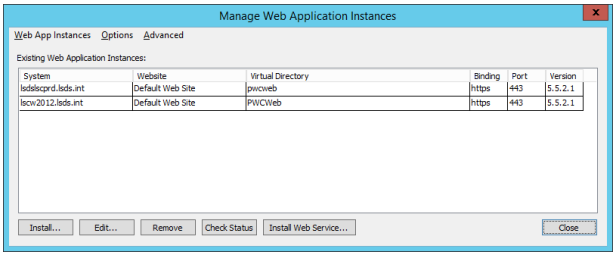
14. When the web application installation is complete, a dialog indicating a successful install will appear. Click **OK**.
15. You will next be prompted to launch the web application. Clicking **Yes** will open your default browser to the URL specified in step 9 above.



16. Click **Yes** to launch the web application. You will be logged into the web application as **[WebApplicationManager]**. This is a built-in account. Its password is randomly generated with each installation of this product.



17. Once the installation of the web applications is complete, the **Manage Web Application Instances** dialog will be populated with a list of all known web applications.
18. If the web service is hosted on the same machine, continue to Upgrading the Web Service. If the web service is hosted on a different machine, then start the parent web site in IIS on the web application hosts only.



For more information please see Post Installation or Upgrade Steps for additional steps and verifications.

Upgrade the Web Service

Starting with Privileged Identity version 5.5.2, the web service is a requirement for the web application to function. In prior versions, the web service was an optional component used only for PowerShell cmdlets, application launcher, session recording, and API access.

IMPORTANT!

If the web service is installed on a machine that is NOT also hosting the web application, the web service will fail to load unless additional actions are taken. In this scenario, export the web application settings from the management console, then import them onto the web service host.

1. To export the settings from the management console, follow the steps below.
2. Click **Manage Web App** from the left action pane.
3. Select the desired web application instance from the list.
4. Go to **Advanced** and select **Export web app registry config**. This will export a regedit file.
5. You will be prompted to generate the file for 64-bit Windows. Click **Yes**.
6. Copy the registry export to the target web service host and double-click the file to import it.

Note: *These steps provide the web service with the necessary information to connect to the data store, the hardware security module, if configured, and the encryption key, as well as other settings. Any time these options change, it will be necessary to repeat these steps.*

IMPORTANT!

If the web service is hosted on a different machine than the web application host and the systems are accessed through a URL is different (specifically with regards to the protocol, server name, or port), your web browser will block access to the web service and many things will not function correctly. The basic steps to resolve this are to open the ***web.config*** *file for the web service after installation, and to set* ***EnableCORS*** *to* ***true****. Additional configurations may be required in your specific browser and may not work in all configurations (non-Microsoft browsers especially).*

Please refer to your browser's specific documentation for more information on enabling CORS support.

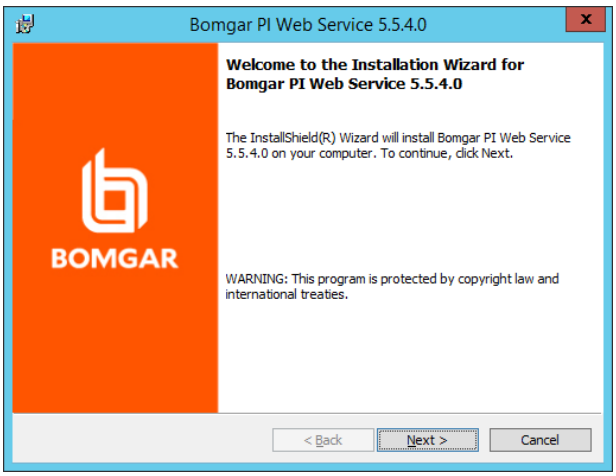
Web service prerequisites are outlined in Web Application Host Requirements at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/host-system.htm#WebApp, and its service account requirements are outlined in Service Account Requirements at https://www.beyondtrust.com/docs/privileged-identity/install/prerequisites/service-account.htm.

The web service cannot be pushed to a target system from the management console; it must be installed locally at this time. If installing the web service on the same machine as the management console, the installation of the web service package may be initiated from the management console, by clicking **Manage Web App > Install Web Service** at the bottom of the **Manage Web**

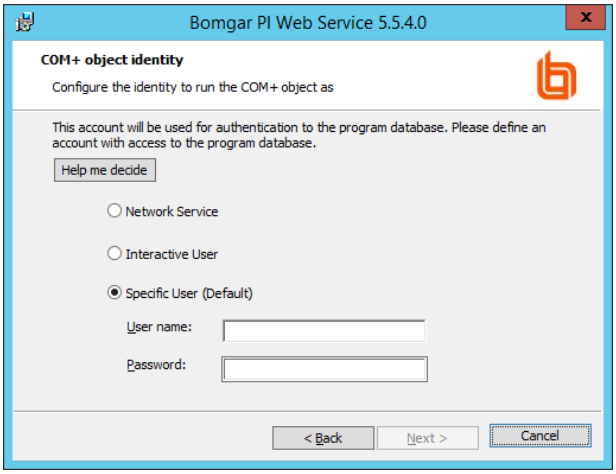
Application Instances dialog. For remote systems, copy and use the manual installer **(ERPMWebService.exe)** found in the **SupplementalInstallers** sub-folder in the installation directory, typically **%programfiles(x86)%\Lieberman\Roulette**.

During an upgrade, your previous settings will be remembered and will already be selected. You will, however, need to re-enter the password for the COM identity.

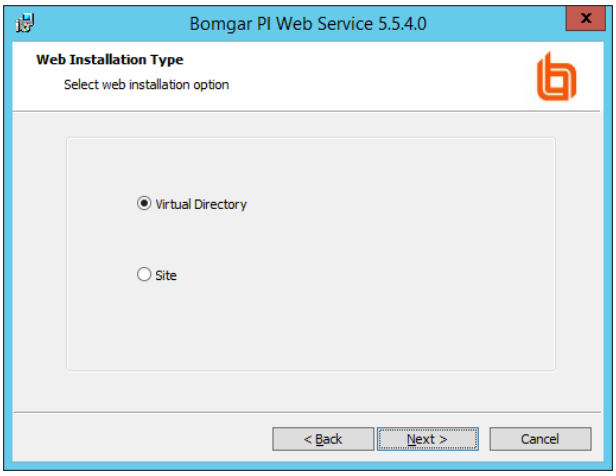
1. Launch the web service installer.
2. On the welcome page, click **Next**.



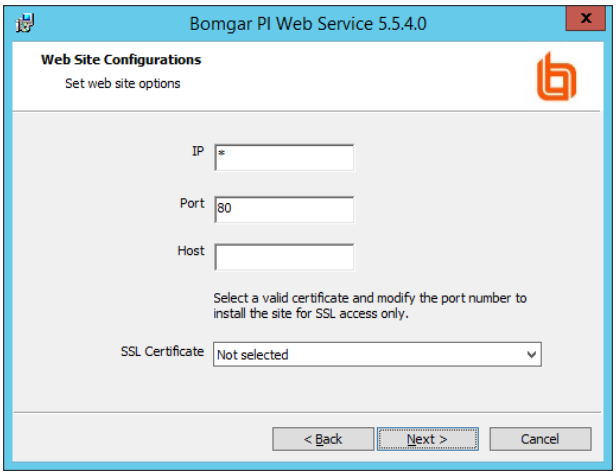
3. On the **COM+ Object Identity**, choose an appropriate identity and click **Next**. Valid identity options are:
   - **Network Service**: use this option when using database native authentication mode to connect to the database (e.g. SA).
   - **Interactive User** (not recommended): use this option when it is desired for the user calling the web service to pass their authentication token as the authentication token to the database. This is valid when using Integrated Windows Authentication but will require considerably more security configurations in the program data store.
   - **Specific User** (default, recommended): use this option when using Integrated Windows Authentication to the database or when it is desired to minimize any rights granted to the COM application. This is the most compatible option. Usernames should be supplied in the format of **DomainName\Username**.



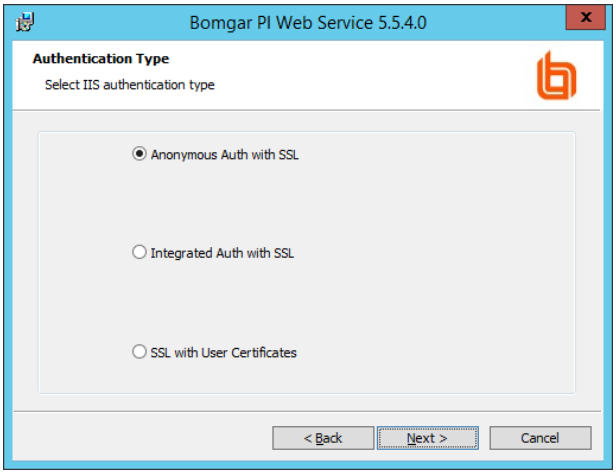
4. On **Web Installation Type**, select the location in the local IIS instance to install the web service to, and click **Next**. Valid options are:
    - **Virtual Directory** (default, recommended): will install the web service to a virtual directory called **ERPMWebService** located under the parent web site you select. This is the safest option to choose for both security and configuration reasons.
    - **Site**: use this option to install the web service to the root web site. If there are multiple root web sites configured on the host, you will also be presented with a selection of root web sites to choose from.



5. If you chose **Virtual Directory** on **Web Installation Type**, select a web site on **Parent Site**, and then click **Next**.



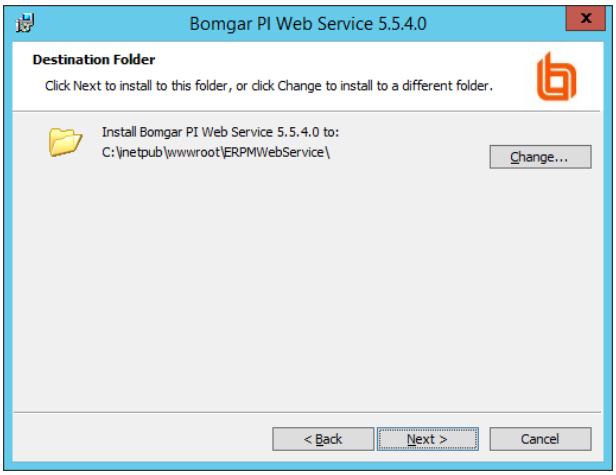
6. If you chose **Site** on **Web Installation Type**, configure site options on **Web Site Configuration**.
7. Select the authentication method for connecting to the web service, then click **Next**. Only methods available to the target parent web site will be displayed. Valid methods include:
    - **Anonymous Auth with SSL**: use this option when SSL is configured but Integrated Windows Authentication will not be used.
    - **Anonymous Auth without SSL** (not recommended): use this option when neither Integrated Windows Authentication nor SSL will be used. Application Launcher will not work with this configuration.
    - **Integrated Auth with SSL**: use this option when SSL and Integrated Windows Authentication will be used.



    - **Integrated Auth without SSL**: use this option when Integrated Windows Authentication will be used without SSL. Application Launcher will not work with this configuration.
    - **SSL with User Certificates** - use this option when users must supply a user-based certificate (smart card, biometrics, etc.) to authenticate to the web site and web service. This will incur much more overhead in the overall configuration

and may cause problems with Application Launcher.

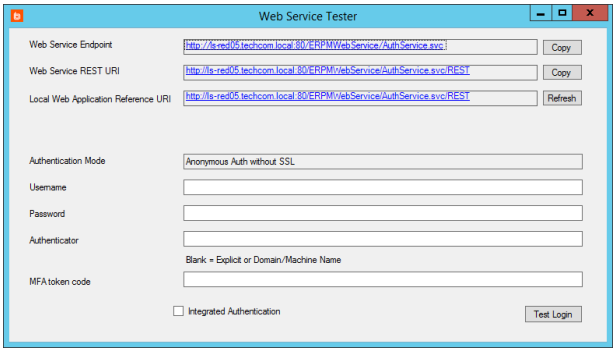
8. Select the destination folder for the web service to be installed to and, click **Next**. The default location is **%inetpub%\wwwroot\ERPMWebService**, which already grants all required permissions to be properly hosted. Changing the location may require additional configurations on the web server.
9. When ready, click **Install**.



IMPORTANT!

*If you chose to create a virtual directory, this process will create a virtual directory called **ERPMWebService**. This will inherit the authentication settings, SSL settings, and other settings from the parent web site. This is important because if the parent web site is configured to use anonymous authentication and the installer was configured to use Integrated Windows Authentication, the virtual directory will be created with incorrect settings, and it will be necessary to open IIS and reconfigure the authentication settings post install.*

10. Click **Finish** when the installer is done.
11. Clicking **Finish** launches the web service page and web service tester. Make note of the **Web Service REST URI** as it will be required when configuring the web application. At this point, the web service will be non-functional, as it also requires settings from the web application to function. If the web site is installed on the same host as the web service, no further configuration actions will be required for the web service.



IMPORTANT!

If you install the web service on a machine that is NOT also hosting the web app, you must export the web app settings from the management console and import them onto the web service host. Otherwise, the web service will fail to load.

To export the settings from the management console, follow the steps outlined below:

1. Click **Manage Web App** from the left action pane.
2. Select the desired web application instance from the list.
3. From the top tools menu, select **Advanced > Export web app registry config**. This exports a regedit file, which you will save locally.
4. When prompted to generate the file for 64-bit Windows, click **Yes**.
5. slcCopy the registry export to the target web service host and double-click the file to import it.

These steps provide the web service with the necessary information to connect to the data store, the hardware security module, the encryption key, and other settings. Any time these settings change on the web app host, you must repeat these steps.

If the web service and web app have different host systems, and if the systems are accessed through different URLs (specifically the protocol, server name, or port), your web browser will block access to the web service, causing processes to malfunction.

To resolve this, enable cross-origin resource sharing (CORS). After you have installed the web service, open **web.config** and set **EnableCORS** to **true**.

Your specific browser may require additional configuration and may not work in all configurations. Please refer to your browser's documentation for more information on enabling CORS support.

Please see Post Installation or Upgrade Steps for additional steps and verifications.

Upgrade Scheduling Services

This section covers upgrading the Deferred Processing Services as well as zone processors. Not all methods below will necessarily apply to your installation. Please choose the sub-headings that apply to your situation and upgrade accordingly.

Deferred Processing Services

Follow these steps if the deferred processor was previously installed.

1. Once the management console has been upgraded, open the management console and navigate to **Settings > Application Components**.
2. Note the component version. It should match the build date of the management console as noted in **Help > About** (see the build number in parenthesis, e.g. 170123).
3. Once verified, click **Jobs** from the left action pane.
4. Click **Deferred Processor**, then click **Start**.
5. There should be no errors when starting the deferred processor, as no settings will have changed. The deferred processor will begin polling the database looking for work.

Zone Processors - Upgrading from 5.5.0 and later, Manual Method

1. Assuming the zone processors were not installed using the Zone Processor Standalone installer (check **Programs and Features** on the zone processor host), if upgrading zone processors on existing zone processor hosts that were running version 5.5.0 and later, it is not necessary to uninstall and remove the previous files (though you certainly may). Rather, simply re-copy the following files from the program installation directory to the zone processor installation directory (typically **C:\LiebermanZoneProcessor**):
    - ipworks9.dll
    - ipworksauth9.dll
    - ipworkssmime9.dll
    - ipworksssl9.dll
    - ipworksssnmp9.dll
    - msvcp120.dll
    - msvcr120.dll
    - RouletteProc.exe
    - RouletteSked.exe
    - wkhtmltopdf.exe
    - zlibwapi.dll
2. If previously installed, copy **IntegrationComponents.msi** (installer for ticketing systems, email, etc.) and/or **CrossPlatformSupportLibrary.msi** (installer for SSH, Telnet, and other non-Windows support) from the **SupplementalInstallers** subdirectory to the target zone processor host.
3. On the zone processor host, open **Programs and Features**.
4. If upgrading from any version of the **CrossPlatformSupportLibrary** or **IntegrationComponents** prior to version 5.5.2, uninstall the existing **Cross Platform Support Library** and/or **Integration Components** programs.
5. Run the installers for **Integration Components** and/or **CrossPlatformSupportLibrary**.
6. Start the zone processor (this will cause database re-registration for this zone processor) using the **Windows Services** snap-in. The service will be named **RouletteSked${ZoneName}**. The service should start without any problems. Typical errors at

this point include:

a. **Inability to connect to the program data store** - check connectivity to database using the service account credentials and the current database provider is installed on the zone processor host (the management console does not push database providers to the remote system).

b. **Bad service account information** - examine the Logon tab of the service in the Windows Services snap-in and validate the username and password.

7. Repeat this processor for all zone processor hosts.

Zone Processors - Console Push Method

In Prepare for Upgrade, it is noted to remove the zone processors using the management console if the zone processor host can be reached from the console (remote registry and file system) and/or you are upgrading from version 5.4.0 or earlier.

1. From the management console, click **Jobs** from the left action pane.
2. Click **Zone Processors** from the **Stored Jobs** dialog left action pane.
3. Click **Install**.
4. **Supply all necessary information to fully reconfigure the service** - zone ID, service account, job types, and management set affinity.
5. Click **OK**.
6. If previously installed, copy **IntegrationComponents.msi** (installer ticketing systems, email, etc.) and/or **CrossPlatformSupportLibrary.msi** (installer for SSH, Telnet and other non-Windows support) from the SupplementalInstallers subdirectory to the target zone processor host.
7. On the zone processor host, open **Programs and Features**.
8. If upgrading from any version of the **CrossPlatformSupportLibrary** or **IntegrationComponents** prior to version 5.5.2, uninstall the existing **Cross Platform Support Library** and/or **Integration Components** programs.
9. Run the installers for **Integration Components** and/or **CrossPlatformSupportLibrary**.
10. Start the zone processor (this will cause database re-registration for this zone processor) by right-clicking on the service registration and selecting **Start**. The service should start without any problems. Typical errors at this point include:
    - **Inability to connect to the program data store**: check connectivity to database using the service account credentials and the current database provider is installed on the zone processor host (the management console does not push database providers to the remote system).
    - **Bad service account information**: examine the Logon tab of the service in the Windows Services snap-in and validate the username and password.
11. Repeat this processor for all zone processor hosts.

Zone Processors - Standalone Installer

If zone processors were previously deployed using the **Standalone Zone Processor Installer** (typically due to inability to connect to the zone processor host from the management console), open **Windows Explorer**, and navigate to the program installation directory, and open the **SupplementalInstallers** sub-directory.

1. Launch **CreateZoneInstaller.exe**.
2. Supply the necessary information to the installer and click **Create**.
3. Copy the created file to the target zone processor hosts and run the package to update installed zone processors.
4. If previously installed, copy **IntegrationComponents.msi** (installer ticketing systems, email, etc.) and/or **CrossPlatformSupportLibrary.msi** (installer for SSH, Telnet and other non-Windows support) from the **SupplementalInstallers** subdirectory to the target zone processor host.

5. On the zone processor host, open **Programs and Features**.
6. If upgrading from any version of the **CrossPlatformSupportLibrary** or **IntegrationComponents** prior to version 5.5.2, uninstall the existing **Cross Platform Support Library** and/or **Integration Components** programs.
7. Run the installers for **Integration Components** and/or **CrossPlatformSupportLibrary**.
8. Start the zone processor (this will cause database re-registration for this zone processor) by right-clicking on the service registration and selecting **Start**. The service should start without any problems. Typical errors at this point include:
    - **Inability to connect to the program data store** - check connectivity to database using the service account credentials and the current database provider is installed on the zone processor host (the management console does not push database providers to the remote system).
    - **Bad service account information** - examine the Logon tab of the service in the Windows Services snap-in and validate the username and password.
9. Repeat this entire process for zone processors hosts managing different zones or having different configurations.

Upgrade PowerShell

For the users leveraging the PowerShell cmdlets, the PowerShell upgrade is simply a matter of distributing the updated cmdlet DLLs.

1. On the management console host, open **Windows Explorer**.
2. Navigate to the **SupplementalInstallers** folder from the program installation directory.
3. Open the **LSCPowerShellCmdlets** folder.
4. Open **LSClientAgentCommandlets**.
5. Distribute **LSClientAgentCommandlets.dll** to the users who use the PowerShell cmdlets.
6. Replace **LSCClientAgentCommandlets.dll** on the client systems. The default recommended location is **%userprofile%\Documents\WindowsPowerShell\Modules\LSClientAgentCommandlets**.
7. Version 5.5.2 introduced two new sets of cmdlets called **LSClientUpdateConfiguration** and **LSClientUpdatePassword**. For any users leveraging these additional cmdlets, copy and replace those DLLs into their respective folders, as well.

Post Installation or Upgrade Steps

After the web application and web service are installed, there may be additional steps to take depending on the options enabled or desired. Additional actions may be required for the following scenarios:

- Use of Integrated Windows Authentication for web application access.
- Required use of SSL.
- Use of IIS redirects.
- Use of user certificates, required for web application access.
- Use of File Store.

CORS Support

If the web service and web app have different host systems, and if the systems are accessed through different URLs (specifically the protocol, server name, or port), your web browser will block access to the web service, causing processes to malfunction.

To resolve this, enable cross-origin resource sharing (CORS). After installing the web service, open its **web.config** file (typically found at **C:\Program Files (x86)\Lieberman\Roulette\ERPMWebService\web.config**), and set **EnableCORS** to **true**.

CORSDomain is used to control the source domain allowed for CORS support. The initial value is set to an asterisk (*), which means the web service will allow references from any web server. To limit communication to a particular domain, change * to **domain.name**. For example:

```
<add key="CORSDomain" value="lsds.int" />
```

The above example will set **Access-Control-Allow-Origin** to **lsds.int**, and requests from servers in other domains will not be allowed.

***Note:** Only one **CORSDomain** value can be specified at a time.*

Additional configurations may be required in your specific browser and may not work in all configurations (non-Microsoft browsers especially).

About CORS

CORS is defined in RFC6454 (https://www.ietf.org/rfc/rfc6454.txt). This specification defines that a resource is considered the same origin if it uses the same scheme (protocol), host, and port. If your web application and web service are installed on the same host, both accessed by HTTPS and both running on the same default port (443), they are considered to be of the same origin, and your browser will not block communication to either component. If any of those elements is different, the browser will by default block communication to the web service via the web application, which will prevent many operations from working, such as password retrieval through the web application. Controls for browser behavior surrounding CORS varies by browser.

For more information, please see your browser's specific documentation on enabling CORS support.

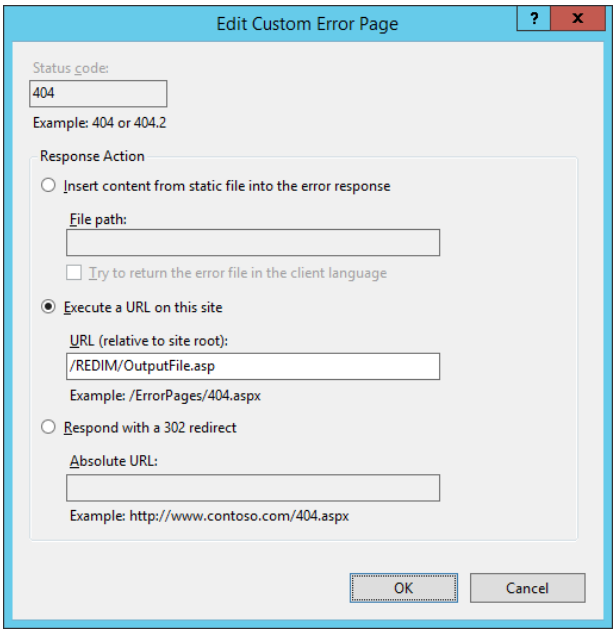
File Store

The web application does not dynamically create the **web.config** configuration file for the file store. Rather, the **web.config** file is pre-configured to always point to a virtual directory called **PWCWeb**. As a result, if the installation of the web application is instead directed to a root directory or a virtual directory other than **PWCWeb**, the file store will not function.

If the installation performed does not point to a virtual directory called **PWCWeb** directly off of a root web site in IIS, take the following corrective actions:

1. Open IIS and locate the root web site or virtual directory where the web application was installed.
2. Expand this object and select the application called **FileVault**.
3. On **FileVault**, open **Error Pages**.
4. Edit the **404** error handler.
5. Edit the **URL (relative to site root)** field and update the correct path. If you installed the web application to a root directory, set the URL to **/OutputFile.asp**.

   If you installed the web application to a virtual directory under a root other than **PWCWeb** immediately off the root (e.g., **/REDIM**), set the URL to that path (e.g., **/REDIM/OutputFile.asp**).

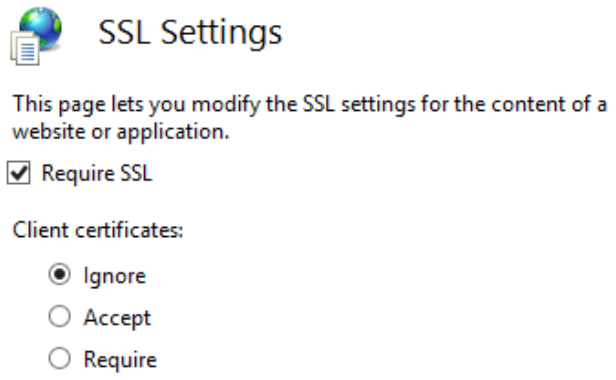


SSL

When installing to a virtual directory (or upgrading an existing installation), the virtual directory will inherit the settings of the parent web site. That means if the parent web site has certain settings, the virtual directory will automatically inherit those settings. Thus, if the parent web site is not configured to require SSL, then your virtual directory will not be configured to require SSL.

To require SSL on your virtual directory, assuming your parent web site already has a proper SSL certificate and binding, follow these steps:

1. On the host server, open **Internet Information Services (IIS) Manager**.
2. Expand your server node, then **Sites**, and then your web site.
3. Select your virtual directory. The default for the web app is **PWCWeb**, and the default for the web service is **ERPMWebService**.
4. From the center pane, open **SSL Settings**.
5. Select the check box **Require SSL**.
6. Click **Apply**.

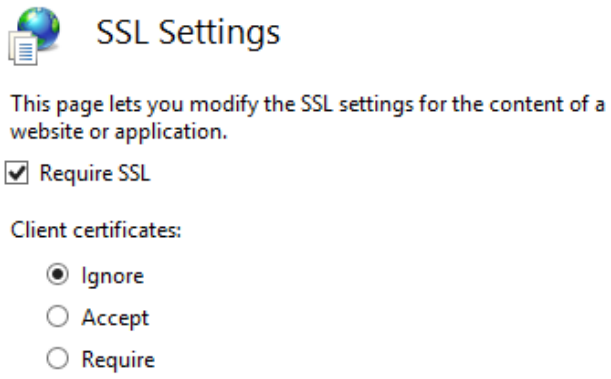


User Certificates

When installing to a virtual directory (or upgrading an existing installation), the virtual directory will inherit the settings of the parent web site. That means if the parent web site has certain settings, the virtual directory will automatically inherit those settings. Thus, if the parent web site is not configured to require user certificates, then your virtual directory will not be configured to require user certificates.

To require user certificates on your virtual directory, assuming your parent web site already has a proper SSL certificate and binding and user certificates are properly configured, follow these steps:

1. On the host server, open **Internet Information Services (IIS) Manager**.
2. Expand your server node, then **Sites**, and then your web site.
3. Select your virtual directory. The default for the web app is **PWCWeb**, and the default for the web service is **ERPMWebService**.
4. From the center pane, open **SSL Settings**.
5. Select the check box **Require SSL**.
6. Under **Client Certificates**, select one of the following options:
    - **Accept**: allows users to pass a user certificate but will also allow users who do not have a user certificate. Select this option if some users will require certificates but you are unsure if ALL users will be using certificates.
    - **Require**: all users accessing this site must supply a valid user certificate.
7. Click **Apply**.



URL Redirects

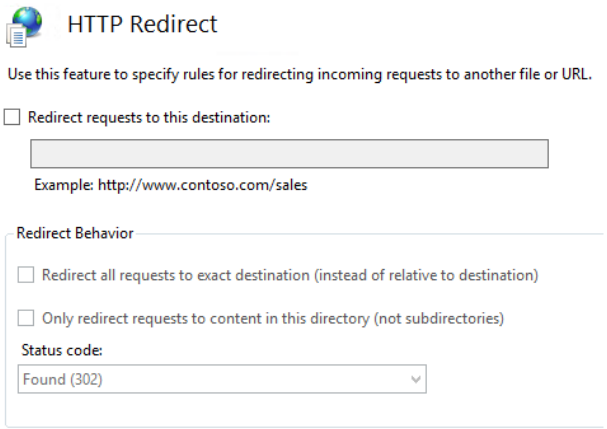
URL redirects are not configured by default in IIS. In fact, they are not even available in a default installation of IIS and must be enabled. URL redirects are typically used so that when a user connects to a particular address, such as a root web site using HTTP, they may be redirected to the proper virtual directory with HTTPS.

When installing to a virtual directory (or upgrading an existing installation), the virtual directory will inherit the settings of the parent web site. That means if the parent web site has certain settings, the virtual directory will automatically inherit those settings. Thus, if the parent web site is configured with a redirect, the virtual directory will be configured with a redirect. In this particular case, this can cause a redirect loop which will cause the user to never be able to connect to the web application or web service. In short, the redirect needs to be removed from the virtual directory.

When installing to a root web site, the same incorrect behavior can occur where it keeps redirecting to itself.

To rectify the problem when dealing with a virtual directory, use the following steps. For root directories, see further down this page.

1. On the host server, open **Internet Information Services (IIS) Manager**.
2. Expand your server node, then **Sites**, and then your web site.
3. Select your virtual directory. The default for the web app is **PWCWeb**, and the default for the web service is **ERPMWebService**.
4. From the center pane, open **HTTP Redirect**.
5. Clear all redirect options.
6. Click **Apply**.



Other options to control switching from HTTP to HTTPS include:

- Using the **Microsoft IIS URL Rewrite Module**.
- Crafting a new default login page and configuring that new page as the **Default Document** for the web site or virtual directory

Integrated Windows Authentication

When installing to a virtual directory (or upgrading an existing installation), the virtual directory will inherit the settings of the parent web site. That means if the parent web site has certain settings, the virtual directory will automatically inherit those settings. Thus, if the parent web site is not configured to use Integrated Windows Authentication (or is mis-configured by also enabling another form of authentication), then your virtual directory will inherit the same incorrect settings.

To require Integrated Windows Authentication on your virtual directory, assuming the IIS module for Integrated Windows Authentication is already installed, follow these steps:

1. On the host server, open **Internet Information Services (IIS) Manager**.
2. Expand your server node, then **Sites**, and then your web site.
3. Select your virtual directory. The default for the web app is **PWCWeb**, and the default for the web service is **ERPMWebService**.
4. From the center pane, select **Authentication**.
5. Right-click on **Windows Authentication** and select **Enable** (note that the status column changes to **Enabled**).
6. If any other forms of authentication are enabled, right-click on those methods and disable them.

Next, your browsers may require additional configuration.

Internet Explorer

For Internet Explorer to willingly use Integrated Windows Authentication, the URL connected to must be seen as being part of the local intranet rather than the internet or trusted network. Internet Explorer will only automatically treat locations entered with their short name (as opposed to an FQDN) as being in the intranet zone. If you are accessing the web application and web service via their short names,you should be able to connect without error, SSL certificates permitting. If you are accessing the web application and web service via an FQDN, Internet Explorer will not treat these URLS as intranet zone items, and Integrated Windows Authentication will fail.

To rectify this when using FQDNs, either you may have every user add the web application and web service FQDN into the intranet zone in IE, or you may use group policy to push out the proper settings. To configure group policy, configure the following group policy to add the FQDN (wildcards allowed) as a trusted site:

- For Kerberos authentication: **network.negotiate-auth.trusted-uris**
- Define if Kerberos ticket passing is required: **network.negotiate.auth.delegation-uris**

- Define if NTLM authentication is allowed: **network.automatic-ntlm-auth.trusted-uris**

In each policy, define the domain name. If your domain name were **example.int**, you would enter **.example.int** for the Kerberos exchange (notice the leading dot).

> ***Note:*** *Firefox may not function properly when working with cross-origin requests (CORS) where the web service is located on a machine separate from the web application and called by a different URL when using Integrated Windows Authentication. These settings have also been noted to be lost between Firefox upgrades.*

Chrome

Recent versions of Chrome will support Integrated Windows Authentication when run from a Windows host without further configuration required. Refer to your Google Chrome documentation for more information or additional settings.

> ***Note:*** *Chrome may still not work properly when working with cross-origin requests (CORS) where the web service is located on a machine separate from the web application and called by a different URL when using Integrated Windows Authentication.*

Upgrade Application Launcher and Session Recording Software

The upgrade process for the application launcher software and session recording software are straightforward: simply re-run the installation routines on the host servers. Your previous settings will be remembered with one notable exception: you will need to re-enter the service account credentials that are asked for during the session recording installation routine.

These upgrade routines should be performed after the core BeyondTrust Privileged Identity software (console, web application and web service) have already been upgraded.

There is no need to re-establish previously configured applications or application settings.

> If you have deployed Application Launcher and Session Recording in your previous version, please refer to the Application Launcher and Session Recording guide at https://www.beyondtrust.com/docs/privileged-identity/app-launcher-and-recording/index.htm and follow the installation protocols to perform the upgrade.

Final Setup Steps

After the web app and web service are installed, you may need to take additional steps, depending on the options enabled or desired.

> Please refer to the Installation Guide at https://www.beyondtrust.com/docs/privileged-identity/install/final-setup/index.htm for a discussion of the available options and instructions.