Gimmal

Technical Users Installation Guide

Gimmal Physical

Contents

Version History

Version	Approved By	Effective Date	Product Version	Description of Change
1	Terry Butler	03/28/2022	3.11	Created for Gimmal Version 3.11
2	Marta Farensbach	12/1/2022	3.12	Minor formatting updates

Technical Users Installation GUide

Gimmal

For Windows 2016

1. Open Server, click **Manage** at the top and then click **Add Roles and Features.**

2. Click **Next** three times to reach the 'Select Server Roles' screen and open **Web Server**.

3. Be sure the following options are selected:

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
.NET Framework 4.6 Features
    ASP.NET 4.6
Web Server (IIS)
    Management Tools
        IIS 6 Management Compatibility
            IIS 6 Scripting Tools
            IIS 6 Metabase Compatibility
            IIS 6 WMI Compatibility
        IIS Management Console
    Web Server
        Application Development
            Application Initialization
            ASP.NET 4.6
            ISAPI Extensions
            ISAPI Filters
            .NET Extensibility 3.5
            .NET Extensibility 4.6
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
            HTTP Redirection
            Static Content
        Health and Diagnostics
            HTTP Logging
        Performance
            Static Content Compression
        Security
            Basic Authentication
            Request Filtering
            Windows Authentication

Technical Users Installation GUide

![Gimmal]

Installation

Gimmal Physical will provide the following files for on-premises installations:

> 1) A backup file to be restored in SQL Server database (.bak or backpac)
>
> 2) A setup file to install the main application on the Web Server (exe)
>
> 3) Hangfire.zip. The Hangfire service is responsible for running all the batch processes and large imports/exports.
>
> 4) CRUD (Create, Read, Update and Delete) folder

The first step in installing Gimmal Physical is to restore the database backup on the SQL Server.

Restore Database

1. Open the SQL Server Management Studio and right-click **Databases** and choose the **Restore Database** option in Object Explorer.

2. Select the **Device** option.

3. Select the database backup file downloaded from the FTP site (button to the right of text field).

4. Select or type the name of a new or existing database in the Database drop down field. (Continued on next page.)

Technical Users Installation GUide
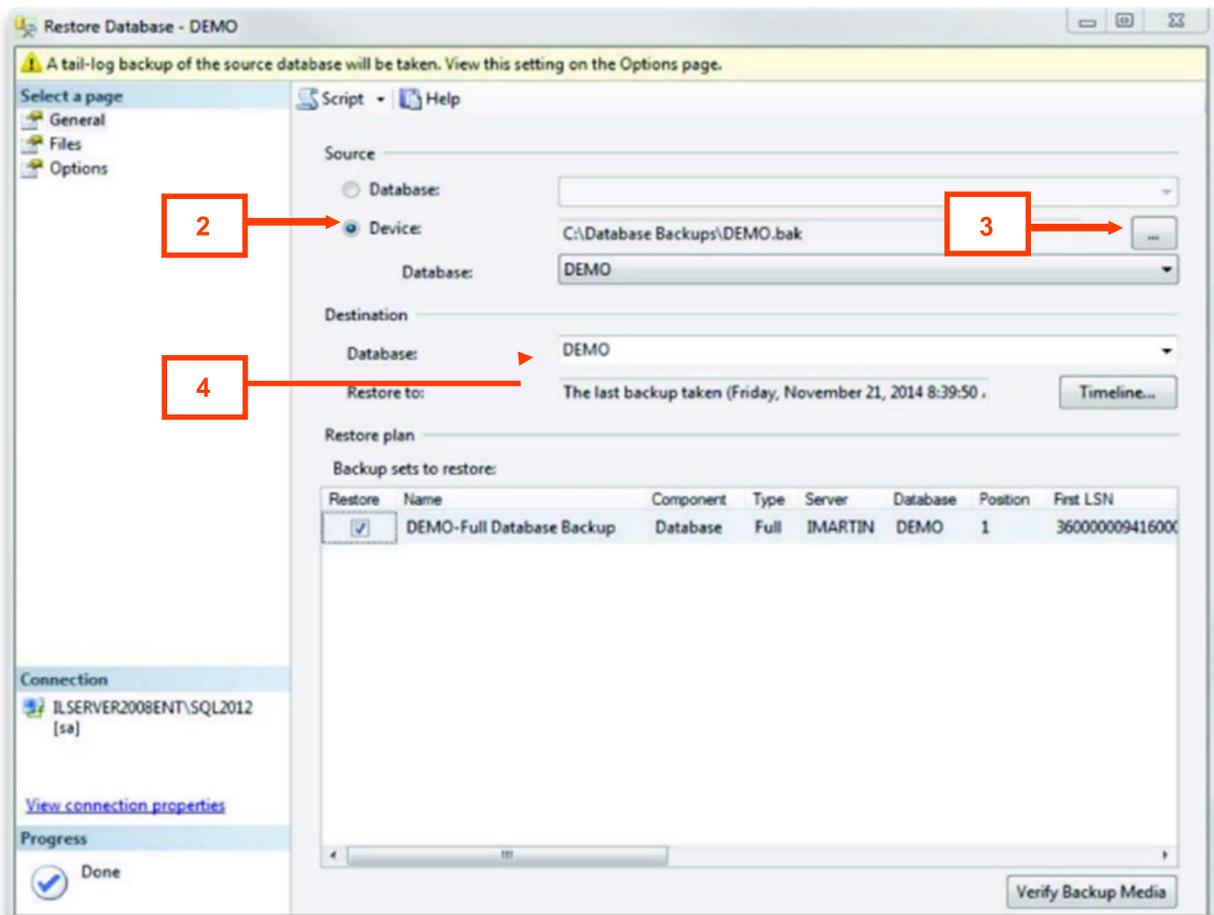
5. Click the **Files** tab to verify the file paths are valid.
6. Click **OK** to perform the restore.
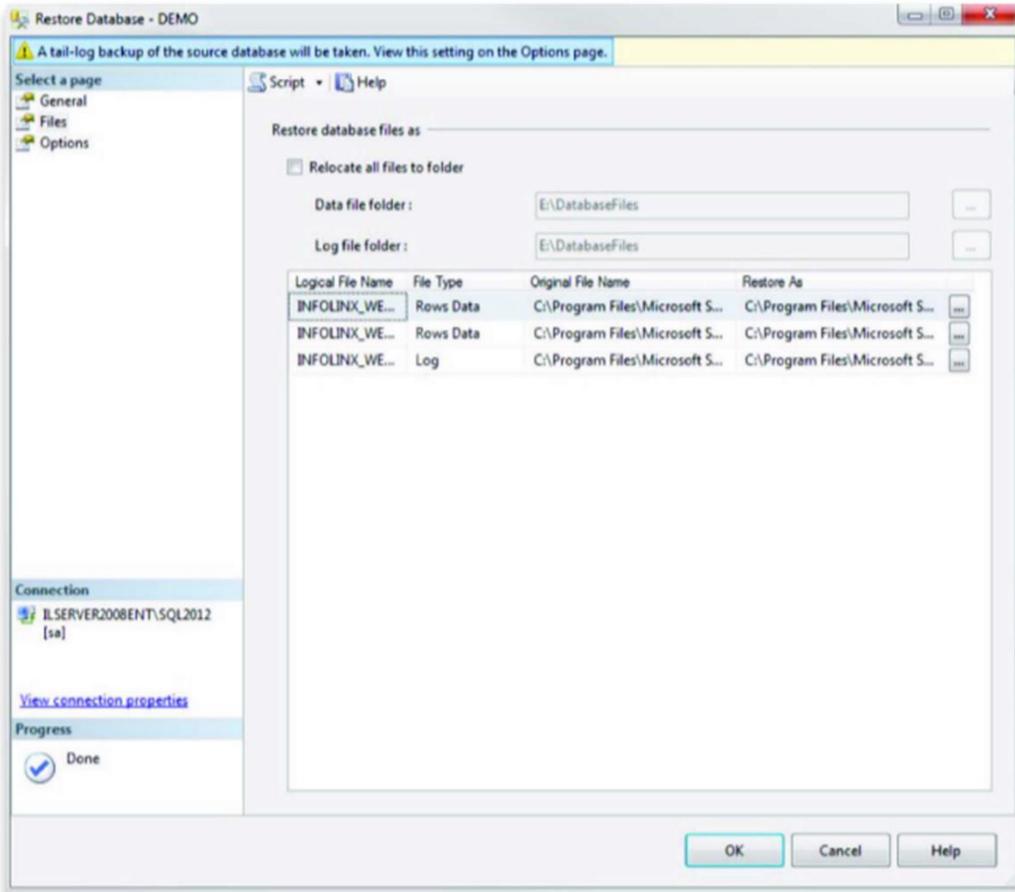
Install Application

On the Web server, follow these steps to install the application.

1. **Open** the install file.

2. If you agree to the license agreement, click through until you reach the 'Installation Type' page.

3. Choose the **Installation Type** that is most appropriate for your organization. In most cases, this is 'Typical' or 'Complete'.   Click **Next**.

4. Enter the Website and Web Service Name you want to use with IIS.

5. Enter the database information and then click **Next**.
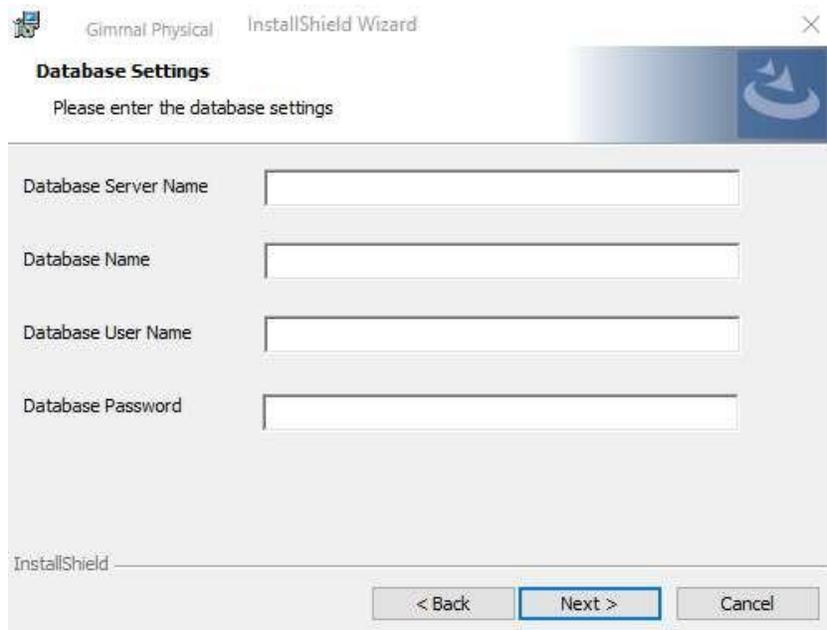
The Gimmal Physical application is now installed**. If you are using Windows Authentication for your Gimmal Physical system, please read the next paragraph as well as the Windows Authentication section at the end of this document.**

Windows Authentication

Before you can access the Gimmal Physical application one or more valid windows security groups must exist in the Gimmal Physical roles table. If no roles in the roles table match any of your network windows security groups, you will get an HTTP 403 Forbidden message. To temporarily get the system up and running, it is recommended to rename the Gimmal Physical administrator role in the Gimmal Physical database to match a valid windows security group on your network. To do this, open the ROLES table in the Gimmal Physical database and update the ROLE_NAME field for the role with ROLE_ID 1 to DOMAIN\Domain Users where DOMAIN is your network domain name.

Gimmal Physical as its own web site

In some organizations, the desired configuration is to create a new web site in the IIS manager that uses port 80 but utilizes HTTP headers to route traffic to the correct site (i.e., gimmalphysical.yourdomain.com).   This configuration is supported and Gimmal Physical works fine.   However, the Gimmal Physical setup program does not currently install to a separate web site on port 80 with an http header.   If this is the desired environment, install Gimmal Physical to a virtual directory and then copy all the files using Windows Explorer into your separate Gimmal Physical web site.

Installing CRUD pages

Copy the provided CRUD folder under the Application/ItemTypesCRUD folder. The default path is:
C:\inetpub\wwwroot\Gimmal\3.11\Application\ItemTypesCRUD\

Installing Hangfire

Included with the installation files is the Hangfire.zip file. To install this:

1. Unzip the Hangfire.zip file.
2. Copy the Hangfire folder into Application folder that was created during the installation of the Gimmal Physical software. Note if you have changed the default install directory the InstallHangfire.cmd will need to be updated accordingly.
3. Update InfolinxHangfire.exe.config with correct database connection string after installing.
4. Run the InstallHangfire.cmd
5. Open Services and set properties for the Hangfire service. If using integrated security in the database connection string, the service will need to run under a service account that can access the database. The recovery options should all be set to Restart the Service.
6. In the Gimmal Physical web site go to Admin/Application settings and select the value for the setting Hour to run background jobs in UTC time.

Quick Start Guide
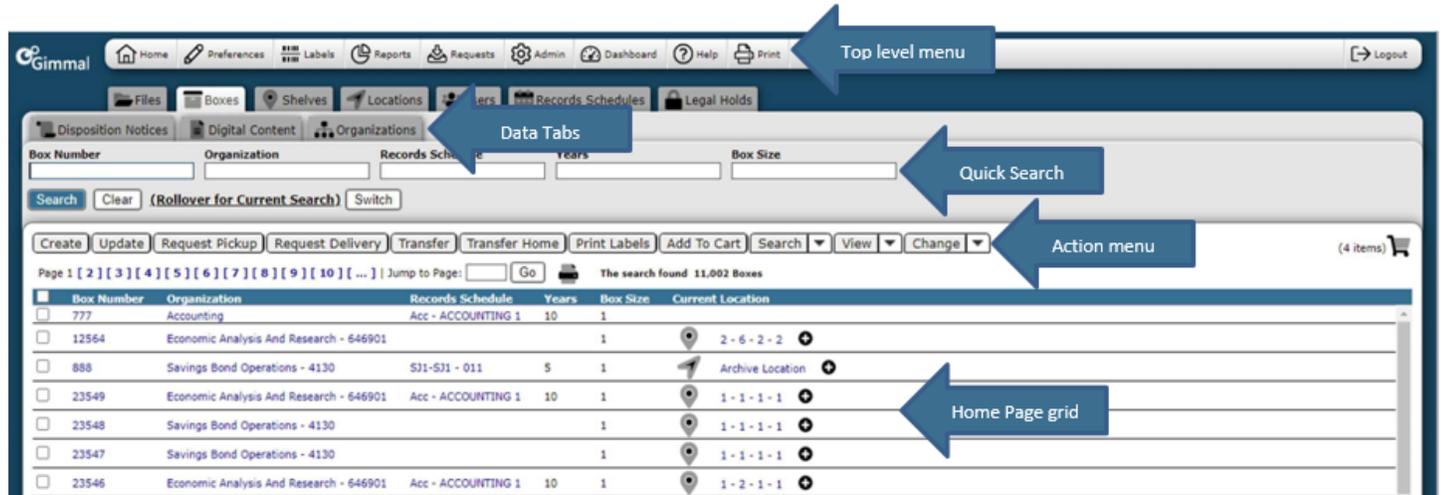
1. **Top Level Menu** – provides access to the various indicated functions

2. **Data Tabs** – used to access the various items being tracked

3. **Quick Search** – used to query within tabs

4. **Action Menu** – provides access to listed actions

5. **Home Page Grid** – displays queried results

User Administration

Gimmal Physical operates in **two modes for user authentication**:
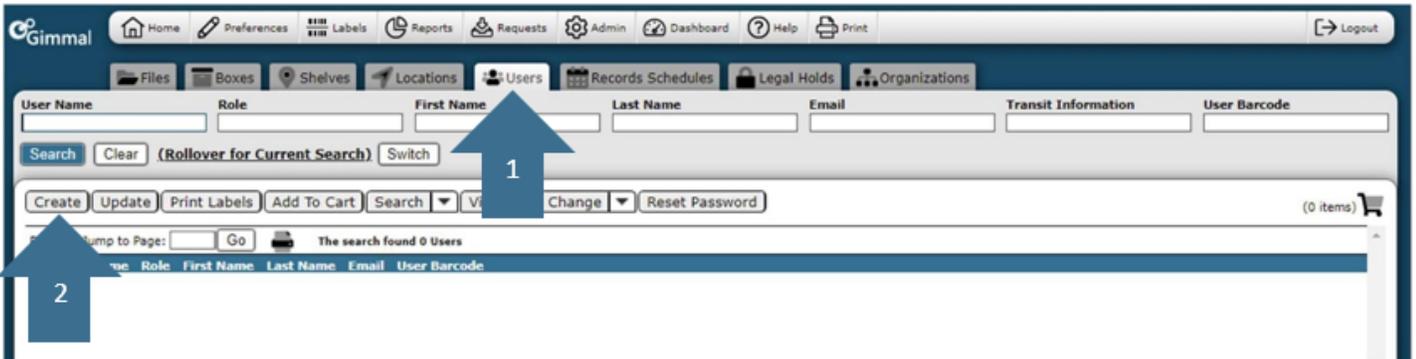
- ☐ **Forms Authentication**: the username and password are managed by the Gimmal Physical database.
- ☐ **Windows Authentication**: the username and password are managed in the Windows NT Domain or Windows Active Directory

Forms Authentication

When using Forms Authentication, the user is prompted with an Gimmal Physical login screen where they must enter valid credentials to access the system.

Add Users to Gimmal Physical:

1. Click the **Users** tab on the Home Page.
2. Click **Create** in the Action Menu.

3. Enter the user's information and click **Save & New** to create a new user.
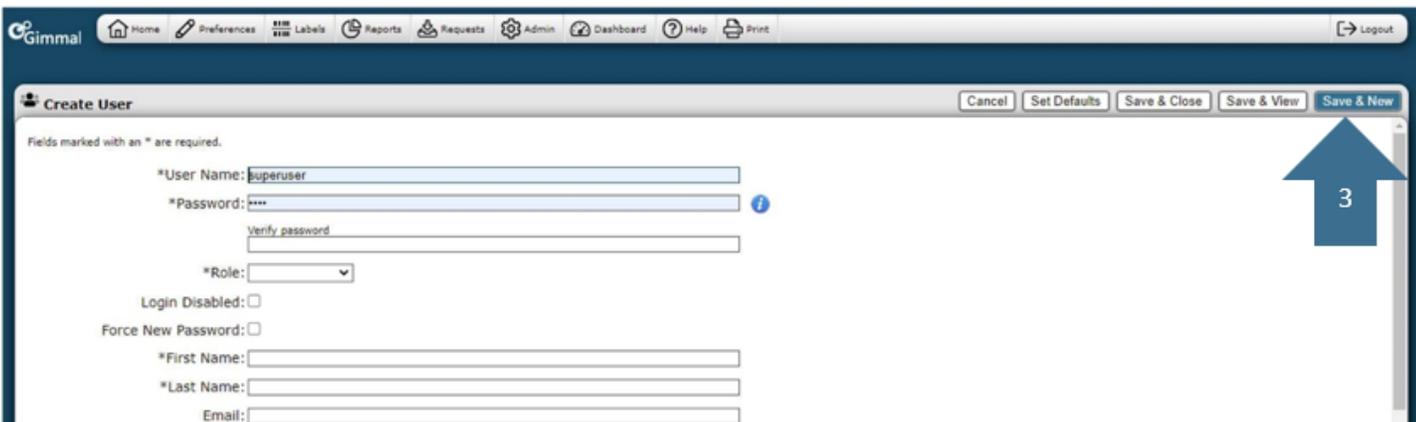
Windows Authentication

When using Windows Authentication, the user is prompted with a Windows login dialog where they enter their network username and password.

Once a user is authenticated, Gimmal Physical compares the Role Name to see if the user is a member of any of the Gimmal Physical Roles.

If the user is not a member of any of the Roles assigned in Gimmal Physical, an **HTTP 403 (Forbidden)** error is generated. Gimmal Physical Roles must exist as Security Groups in the Windows domain.

For example, if SSI is the domain name.

1. Create a Windows Security Group in the Domain called **Gimmal Physical Administrators**.

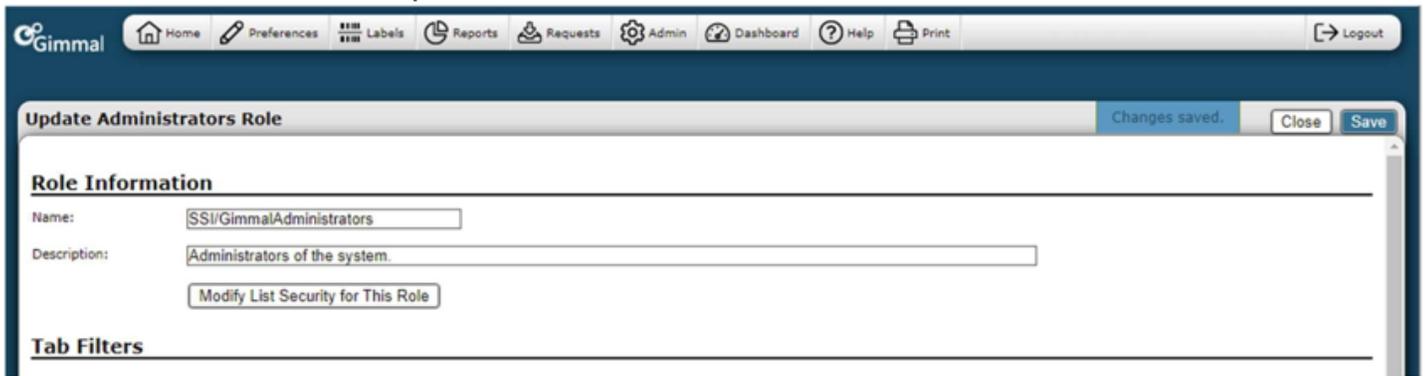| Gimmal Physical Administrators	Security Group - Global
Gimmal File Room Users	Security Group - Global
Gimmal General Users	Security Group - Global

2. On the top menu, click **Admin.** Click **Roles and Permissions** and click **Edit.** Edit the name of the Gimmal Physical Administrator Role with the name SSI\ Gimmal Physical Administrators.

3. Change the name to match the syntax DOMAIN NAME\Security Group Name (i.e., SSI\ Gimmal Physical Administrators) and click **Save** toupdate the role name.
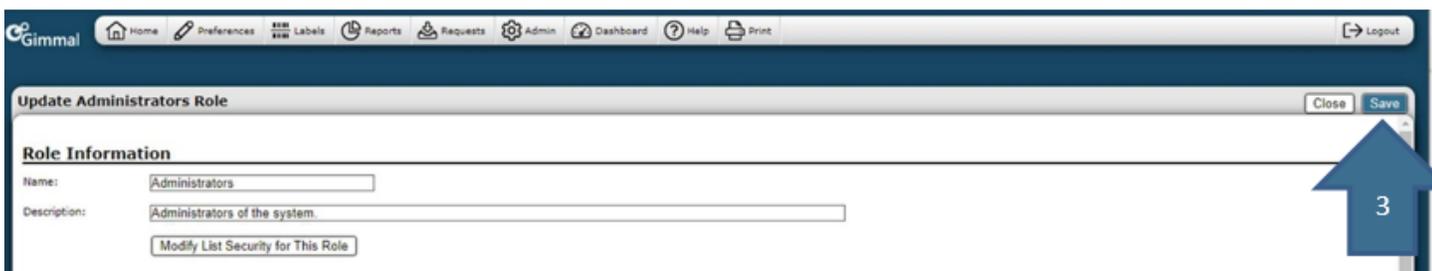
4. The role name will be updated to the new role name entered.

Note: The existing Security groups such as Domain Admins and Domain Users can be used if desired.

Refer to the Gimmal Physical on-line Help within the Gimmal Physical application.