iWD Deployment Guide

IWD Manager Configuration

5/9/2025

Contents

IWD Manager Configuration

Logging in

User Login

Anyone who needs access to iWD Manager must be configured as a $Person$ or in Genesys Administrator (GA) or Genesys Administrator Extension (GAX) and also must have the required privileges (usually defined as iWD roles) assigned either in GA or GAX.

The login screen prompts for the following information:

- **Username**—The username for the Person or User as configured in GA/GAX.
- **Password**—The password for the Person or User as configured in GA/GAX.

Programmatic Login

You can log into iWD Manager programmatically by providing the URL for iWD Manager login page along with a valid username and password. This can facilitate a single sign-on process.

The URL format to use is:

```
http://<appserverhost>:<appserverport>/<iwdmanagerapplication>/ui/login.jsf?username=<username>
&password=<password>&passwordEncoded
```

Where:

- `<appserverhost>` and `<appserverport>` are the host and port for the application server where iWD Manager is deployed.
- `<iwdmanagerapplication>` is the iWD Manager application running on the application server (for example, `iwd_manager`).
- `<username>` and `<password>` are a valid username and password combination for the user logging into iWD Manager.

Important

If you want to include the &passwordEncoded at the end of the URL, then the value for <password> should be encoded using the BASE64 algorithm. Otherwise, you can pass a plain-text password in the **<password>** parameter and omit &passwordEncoded.

An example URL is:

```
<http://myTomcatHost:8080/iwd_manager/ui/login.jsf?username=jsmith&password=myPassword&ConfigApplication=iWDManager
```

General Conditions for Configuring an iWD Manager User

To access the Global Task List, the Person must be associated with a Place in Genesys Configuration. If the Person is not an Agent, the Place can be configured as an option on the **Annex** tab of the Person/User object. Create a section called **[iWD]** (if it does not already exist) and within it, create an option **iWDManagerPlace** with the value of a valid Place name.

If you want a user to have access to a specific managed tenant in iWD, that user must have at least Read access to the Configuration Server tenant that is linked to that iWD managed tenant—either directly or by being a member of an Access Group that does. The user must have at least Read and Execute permissions to the iWD Manager application in Configuration Server, and Read permissions to the Configuration Server Host object where the Interaction Server is running, either directly or by being a member of an Access Group that does.

If the user is going to have access to the Global Task List, then the user must have at least Read and Execute permissions to these application objects in Configuration Server:

- Interaction Server
- The Database Access Point for the Interaction Server database
- The Database Access Point for the History Node database.

These permissions may be applied directly to the user, or by the user being a member of an Access Group that has such permissions.

The Place that must be associated with the user must be a Place configured under the Configuration Server tenant that maps to the iWD managed tenant. (This presumes that the Interaction Server application also has an association with this Configuration Server tenant.) The Place is only used to give the user access to the Global Task List.

If you want to restrict what the user can do in iWD Manager, use roles and privileges as described in Role-Based Access Control.

If the user is created under a Configuration Server child tenant, then the following additional conditions must be met:

- If you want the user to have access to both the iWD SYSTEM tenant as well as the iWD managed tenant to which the Configuration Server tenant maps, then this user must be either be a member of at least two Access Groups with the relevant permissions, or must have permissions granted directly to them.

Such Access Groups must have at least Read permission to the tenants.

If the user has no role privilege in a Tenant, then the Tenant is hidden from that user.

If the user is created under the Environment tenant (for example, such as the default user that is in the Configuration Server database when it is initially deployed) then in order for this user to have full control of the Global Task List (not just read-only access), two conditions must be met:

- The user must have a valid Place configured, where the Place is created under a child Configuration Server tenant to which the Interaction Server is associated.

- The user must have an Employee ID that also belongs to a user who is created under a child Configuration Server tenant to which the Interaction Server is associated.
- The user must have all role privileges from all the "iWD*" groups.

Importing Media Icons

Prerequisites

- iWD Manager, iWD Runtime Node are installed.
- Application servers are started (if running on WebSphere).

Procedure

1. Log in to iWD Manager.
2. Select "Media Icons" from the main menu.
3. Select Import from the top right toolbar.
4. Import the relevant media icons file: for example;
     - ***<iWD Manager installation directory>*\config\iwd_mediaicons.xml**.

> **Important**
>
> The XML file is saved to the installation directory where the iWD Manager supporting files were installed.

5. After each import a message appears at the bottom of the screen to indicate whether the import was successful.

Media Icons View in iWD Manager
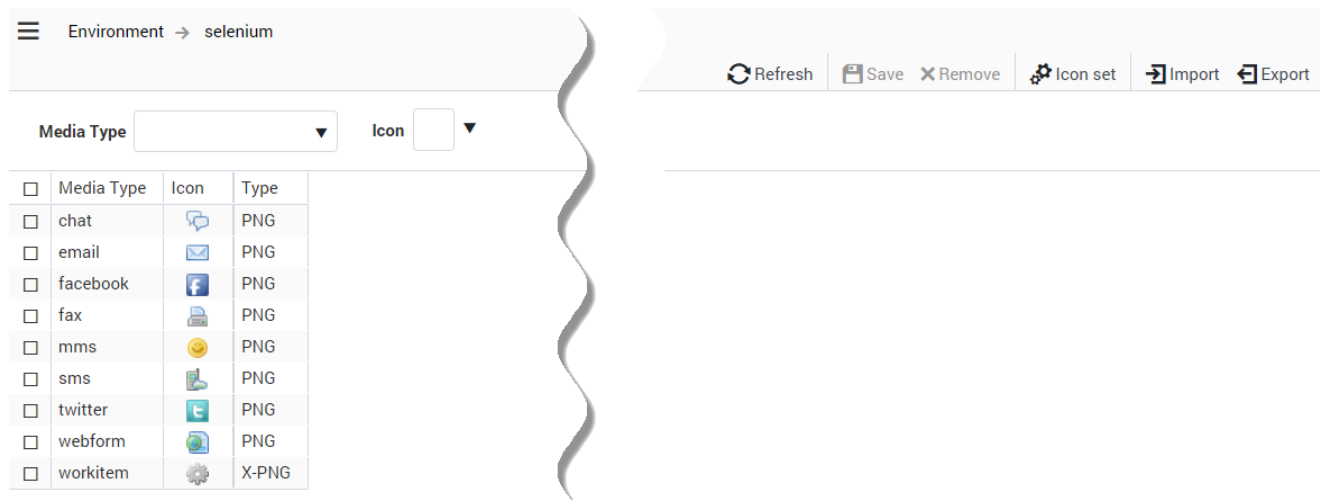
The **Media Icons** view lets you map graphical icons to media types for display in the GTL. iWD comes with some pre-loaded icons, but you can import additional icons and map them to existing media types, or new media types. You can also export the icon set to an XML file.

Basic data

- **Media Type**— The media type to which the icon will be mapped. This list of media types is retrieved dynamically from Genesys Configuration Server. Media types are a type of **Business Attribute** in Configuration Server. Genesys provides out-of-the-box media types but new custom media types can be added.

- **Icon**—The graphical 16x16 icon that will be displayed in the GTL when a task is of the media type to which the icon is mapped.

- **Type**—The icon's file type. Icons must be 16x16, but can be in any of the following file formats:
  - GIF
  - JPG
  - BMP
  - PNG
  - X-PNG

Actions

Use the toolbar commands to do the following:

- **Remove**—Remove a selected icon.
- **Save**—Save changes.
- **Refresh**—Refresh the display.
- **Icon set**—Add new icons from a local file system.

- **Import**—Allows you to import the iWD Media Icons configuration from an XML file. Click Import, select a file on your local drive, select it and and click Open.

- **Export**—Export the iWD Media Icons configuration to a local XML file.

Filters

Configuration of Filters is performed in iWD Manager. Filters let you refine the list of tasks displayed in the GTL. Each filter is defined by a set of filter criteria (optional) and a list of table columns (Filter columns) that will be displayed in the GTL.

Some filters are preconfigured for iWD Manager, and you can create custom filters. Full details are in the **Filters** (new document) topic of iWD Manager Help.