iWD Deployment Guide

Installing IWD Manager

5/9/2025

Installing IWD Manager

Prerequisites

Prerequisites

- The environment meets the requirements that are described in *Installation Prerequisites*
- The computer on which the iWD Manager is going to be installed has network access to the computer that is hosting Genesys Configuration Server. Users of iWD Manager will be authenticated through Genesys Configuration Server.
- You have access rights to execute `install.sh` or `setup.exe`, depending on the operating system.
- For upgrades from 8.5.0 to 8.5.1+:
  - The servlet container (for example, Tomcat) is stopped.
  - The previous version of iWD Manager is uninstalled—the `iwd_manager` directory from the web server is removed.

On Windows

On Windows

Prerequisites

- Installation Packages have been installed.

Purpose

To install the iWD Manager application on the Windows platform.

Summary

Installation of iWD Manager saves the required database scripts in the working directory. These scripts must be run against the iWD Configuration database and the Interaction Server database. iWD Manager does this automatically after a user's successful login and authentication, when it detects a different database schema than expected. For Iteration Server synchronization, there is a dedicated option `Configure Ixn Custom Properties` in iWD Manager. The current procedure assumes that the application already exists in Configuration Server—the required steps are described in *iWD Manager Application Definition*.

> ### Important
> If you are upgrading, ensure that you have uninstalled the previous version and proceed with the current installation procedure. Also make sure not to skip the Application Definition step, because new versions might deliver new options.

Procedure

1. Locate and double-click setup.exe in the iWD Manager directory eg. of the iWD DVD.
2. The iWD Manager Installation Wizard opens. Click **Next** in the Welcome screen.
3. Select the web container (for example, Tomcat or WebSphere) and click **Next**.
4. If you selected WebSphere in Step 7, select the appropriate JDK from the list.

   > ### Important
   > This is not the JDK which will be used by WebSphere. This is necessary to properly configure the scripts which will be used to build the WAR archive.

5. If you selected Apache Tomcat in Step 7, browse to the Home directory for your Apache Tomcat installation (for example, `C:\ProgramFiles\Apache\Tomcat7\`). The iWD Manager components will be installed in the selected directory, under the `webapps/` subdirectory.
6. Click **Next**.
7. In the **Connection Parameters** to the Configuration Server screen, enter the login details to connect to Genesys Configuration Server and then click **Next**:
   - `Host name`—The host of Genesys Configuration Server
   - `Port`—The port that is used by Genesys Configuration Server
   - `User name`—The user name of the Person (or User) as defined in Genesys Configuration Manager or Genesys Administrator.
   - `Password`—The password that is associated with the Person (or User).

8. (Post-8.5.101.03 only) From the list of available choices, choose the iWD Manager application that you want to install and click `Next`.
9. Choose the destination location for iWD Manager. If you selected Websphere in Step 7, both supporting files and iWD Manager Java application part will be installed in that location. If you selected Tomcat in Step 7, only supporting files for iWD Manager will be installation in that location. The iWD Manager web application will be installed directly into the `webapps` folder under your Tomcat home directory.
10. Click **Next**.
11. Select the database type that will be used by the iWD Configuration database.
12. Enter the parameters that are used to connect to the iWD Configuration database in the next screen. Enter the following information:
    - `DB Server Host`—The name of the computer on which the database is located.
    - `Database Name`—The name of the iWD Configuration database.
    - `User Name`—The name of the user that is used to connect to the database.
    - `Password`—The password that is used to connect to the database.
13. Click **Next**.
14. Enter the host name and port of the computer on which the backup Genesys Configuration Server is running. If there is no backup Configuration Server in your environment, specify the primary Configuration Server host and port. Click **Next**.
15. In the **Ready to Install** screen, click **Install** to begin the installation of iWD Manager.
16. When installation has been completed, click **Finish**.
17. Perform any optional steps or install localization if needed.

For WebSphere configuration after installation of iWD Manager, build the WAR archive as described in *Post-Installation Steps For WebSphere* and install the generated WAR file by using the WebSphere Integrated Solutions Console.

End of procedure

On UNIX

On Unix

Prerequisites

- Installation Packages have been installed.

Purpose

To install the iWD Manager application on the UNIX platform.

Summary

Installation of iWD Manager saves the required database scripts in the working directory. These scripts must be run against the iWD Configuration database and the Interaction Server database. iWD Manager does this automatically after a user's successful authentication in the login every time that it detects a different database schema than expected. For Interation Server synchronization there is a dedicated option `Configure Ixn Custom Properties`. The current procedure assumes that the application already exists in Configuration Server—the required steps are described in *iWD Manager Application Definition*.

> **Important**
>
> If you are upgrading, ensure that you have uninstalled the previous version and proceed with the current installation procedure. Also make sure not to skip the Application Definition step, because new versions might deliver new options.

Procedure

1. Locate the install directory and enter `./install.sh`.
2. When the following output is displayed, enter the required information, as indicated at each prompt.

> **Important**
>
> In this procedure Websphere is selected for the servlet container. When asked to provide the destination directory, enter an arbitrary location. iWD Manager Java application and supporting files will be installed in this directory.
>
> Othercase you can select Tomcat option. Then you will be asked additionally for you tomcat installation path: `Please enter the full path to your Tomcat installation`
>
> And java application will be installed directly into Tomcat as `iwd_manager` and rest of supporting files in location that you provided.

```
************************************************
* Welcome to the Genesys 8.5 Installation Script *
************************************************

Installing iWD Manager, version 8.5.101.XX
```

```
Please select your servlet container type by number:
1. Tomcat
2. WebSphere
=>1

Please specify the type of used Database Server:
1) MS SQL Server
2) Oracle Server
=>2

Please enter the Database Server hostname or IP address =>X.X.X.X

Please enter the Database name =>XE

Please enter the Database Server user name =>iWD

Please specify the Database Server user password =>

Please enter the Configuration Server Host Name =>X.X.X.X

Please enter the Configuration Server Port =>2020

Please enter the Configuration Server Backup Host Name =>X.X.X.X

Please enter the Configuration Server Backup Port =>2020

Please enter the Configuration Server Application Name =>iWD Manager (Note:
Post-8.5.101.03 only)

Please enter full path of the destination directory for installation =>/var/iwd85/manager

Extracting tarfile: data.tar.gz to directory: /var/iwd85/manager
...
webapp/
...
webapp/WEB-INF/
webapp/WEB-INF/application.properties
webapp/WEB-INF/web.xml
webapp/WEB-INF/faces-config.xml
webapp/WEB-INF/lib/
webapp/WEB-INF/lib/hibernate.jar
webapp/WEB-INF/lib/packagedstatisticsdeprecated.jar
webapp/WEB-INF/lib/commons-lang.jar
webapp/WEB-INF/lib/commons-logging.jar
...
webapp/META-INF/MANIFEST.MF

Installation of iWD Manager, version 8.5.XXX.XX has completed successfully.
```

3. Perform any optional steps or install localization if needed.

For WebSphere configuration after installation of iWD Manager, build the WAR archive as described in *Post-Installation Steps For WebSphere* and install the generated WAR file by using the WebSphere Integrated Solutions Console.

iWD Manager Application Definition

Procedure

1. Log into Genesys Administrator or GAX and import the iWD Manager Application template eg. from the iWD DVD. Since 8.5.0, the iWD Manager template also includes privileges. Double-check to see whether metadata were correctly imported. This is important for definition of roles in Genesys Administrator. For GAX, importing the IP automatically also imports privileges. In that case, metadata are options since you would manage roles using GAX in those circumstances.
2. Create a new **Application** object based on the template. For upgrades from 8.5.0 to 8.5.1 you can either create a new application in place of the previous one or simply update the application by using the new template. As for second option be careful with privileges part.

> **Important**
>
> The must be only one iWD Manager application on the Configuration Server. Additional ones will be ignored.

3. To begin create procedure navigate to **Configuration > Environment > Applications** and click **New**.
4. On the **General** tab:
   a. Enter a name for the iWD Manager.
   b. Select the application **Template**—This must of type `iWD Manager`.
   c. **Version**, **Tenant** and **Is Application Server** boxes are pre-selected according to the template type.
   d. **State Enabled**—If selected, indicates that the object is in regular operating condition and can be used without any restrictions.
5. On the **Connections** tab, add the connections to the Interaction Server and to Universal Contact Server (UCS) that your iWD Solution will use. If you need to:
   a. Add the **Port ID** on the Interaction Server that iWD Manager will connect to.
   b. Specify the **Connection Protocol**: `simple` or `addp`.
   c. Specify the **Local Timeout** and the **Remote Timeout**—These values are required only if you specified addp in Connection Protocol. This value specifies the heartbeat polling interval, measured in seconds, on a client side. This indicates how often the client application sends polling signals to the server application. To enable this functionality, specify any integer as the value.
   d. Specify a Trace Mode—The connection trace mode used between a server and its client.
      - `Trace Is Turned Off`—Select if you do not want either the client or the server application to print ADDP-related messages in its log.
      - `Trace On Client Side`—Select if you want the client application to print ADDP-related messages in its log.
      - `Trace On Server Side`—Select if you want the server application to print ADDP-related messages in its log.
      - `Trace On Both Sides`—Select if you want both the client and server applications to print ADDP-related messages in their log.
6. Specify **Transport Protocol Paramters**—Any text, usually key=value pairs, separated by a semicolon (;). This property is application-specific.

7. Specify **Application Parameters**—Any text, usually key=value pairs, separated by a semicolon (;). This property is application-specific.

- The **Ports** tab lists communication ports used by the clients of an application to connect to a server. To support specific high-availability configurations, more than one server can be registered on the same port within the same host. Otherwise, do not assign the port number to any other server on the same host. Click **Add** to add a connection.
- Ignore the **Options** tab.
- Ignore the **Application Options** tab.
- Click **Save** to save the Application object.

Additional Configuration for Database Cluster Solutions

Additional Configuration for Oracle RAC and MS SQL

After a standard installation of iWD Manager, you must do one of the following to correctly configure iWD Manager for either Oracle RAC or MS SQL clusters:

- Edit the `iwd.properties` file

1. Edit the iWD Manager configuration file (`iwd.properties`) and replace the `iwd.configDatabase.url` property value with a valid JDBC URL for either Oracle RAC or MS SQL.
2. Start iWD Manager.

See also **here** for differences between the Oracle RAC SCAN-on and SCAN-off URLs.

Post-Installation Steps for WebSphere

Post-Installation Steps for WebSphere

After the installation of iWD Manager it is necessary to build the WAR archives and install them into WebSphere using Integrated Solutions Console.

Building WAR archives for iWD Manager

1. Browse to the directory which was specified during installation of iWD Manager and continue to

subdirectory \webapps.

2. Launch the `iWD_Manager.bat` or `iWD_Manager.sh` file, depending on your operating system. This will create the `iwd_manager.war` file. For example, for UNIX the following output will be displayed:

```
bash-3.00# cd /var/iwd85
bash-3.00# ls
manager
bash-3.00# cd manager/webapps
bash-3.00# ls
iWD_Manager.sh iwd_manager
bash-3.00# ./iWD_Manager.sh
added manifest
...
adding: ui/lib/codepress/images/line-numbers.png(in = 16556) (out=
16556)(stored 0%)
bash-3.00#
```

3. Log in to Websphere Integrated Solutions Console.
4. Uninstall the existing iWD Manager applications, if they are present.
5. Install iWD applications, and select the prepared WAR files when prompted.
6. When installation is completed, adjust the order of classloaders for each installed iWD application. By default, classloader order is Parent first, then Application. iWD requires the order to be Application first, then Parent.
7. To change the order of the classloaders, in WebSphere Integrated Solutions Console, click on **Application**, click **Manage Modules**, click on **Module** (one per application), then change the `classloader` order to Application, then Parent.
8. Click **Save**.
9. From the installed application list:
   a. Click on the application.
   b. Click on the [JSP and JSF options] link.

> **Important**
>
> When deploying on Websphere 8.x, the JSF implementation must be set to SunRI1.2 for the iwd_manager application.

   c. Select SunRI1.2 from the drop-down list.
   d. Click **Save**.
   e. Set the WebSphere cookie path to `/iwd_manager` with the session management override enabled. This setting is located in **iwd_manager_war> Session Management> Enable Cookies**.
   f. Click **Save**.
10. Start the application.

Encode your database password

Encode your database password

Purpose

An optional step that allows you encrypt the database password, because it is held in configuration files.

Procedure

A file named `passwordEncoder.cmd` (or `passwordEncoder.sh` for UNIX-based operating systems) file is included when you install iWD Manager. This utility can be run to encode the database password that appears in the `iwd.properties` file, which is located in `<web application server directory>/webapps/iwd_manager/WEB-INF/classes` (the password is in plain text in the `iwd.properties` file by default).

1. On Windows open command-line window (go to **Start -> Run** and enter `cmd` in the **Run** dialog box). On other systems, open the console.
2. Navigate to the directory where iWD Manager has been installed (for example, `cd C:\Program Files (x86)\GCTI\iWDManager\passwordEncoder`). Navigate to directory `passwordEncoder`.
3. Enter `passwordEncoder <unencoded password>` (for example, if the password is `genesys` you would type in `passwordEncoder genesys`).
4. The command-line window will display the encoded version of the password.
5. In the `iwd.properties` file, replace the unencoded version of the password string with the encoded version (`iwd.configDatabase.password=`).
6. Change the value of the `iwd.configDatabase.passwordEncoded` property to `true`.
7. Save the `iwd.properties` file.

Below are two sample files. The first shows an `iwd.properties` file before the password was encoded. The example shows the same file after the password was encoded.

In order for the password encoder to work, the JRE bin directory must be added to the PATH system environment variable for users that handle iWD Manager server. For example, if the JRE is installed in `C:\Java\jre1.7.0_45_x64` then `c:\Java\jre1.7.0_45_x64\bin` should be in the PATH system environment variable.

Sample file with unencoded password

```
iwd.configDatabase.url=jdbc:sqlserver://iwd80vm;
databaseName=iwdmanagerdb
iwd.configDatabase.username=genesys
```

```
iwd.configDatabase.password=genesys
iwd.configDatabase.passwordEncoded=false
iwd.configDatabase.driverClassName=
com.microsoft.sqlserver.jdbc.SQLServerDriver
iwd.configDatabase.hibernateDialect=
org.hibernate.dialect.SQLServerDialect
iwd.configDatabase.type=mssql
iwd.cfgServerHost=localhost
iwd.cfgServerPort=2020
iwd.cfgServerBackupHost=localhost
iwd.cfgServerBackupPort=2020
iwd.host=maestro_01
```

Sample file with encoded password

```
iwd.configDatabase.url=jdbc:sqlserver:
//iwd80vm;databaseName=iwdmanagerdb
iwd.configDatabase.username=genesys
iwd.configDatabase.password=********
iwd.configDatabase.passwordEncoded=true
iwd.configDatabase.driverClassName=
com.microsoft.sqlserver.jdbc.SQLServerDriver
iwd.configDatabase.hibernateDialect=
org.hibernate.dialect.SQLServerDialect
iwd.configDatabase.type=mssql
iwd.cfgServerHost=localhost
iwd.cfgServerPort=2020
iwd.cfgServerBackupHost=localhost
iwd.cfgServerBackupPort=2020
iwd.host=maestro_01.
```

> **Important**
>
> You can use other Base64 encoders to encode your password as well. These can be found easily on the Web. One example is: http://www.motobit.com/util/base64-decoder-encoder.asp.

End of procedure

Implementing Single Sign-On and Single Log-Out

Implementing Single Sign-On & Log-Out

To configure single sign-on (SSO), the following additional configuration is required:

1. Edit the `sso.properties` section and set the following properties:
   - `iwd.saml.enabled`—Set to `true`
   - `iwd.saml_entityid`—Set to a value that is unique within the SSO circle (the full URL path, for

example)

- `iwd.saml_idp_metadata`—The URL from which to obtain the IDP's metadata file (a locally stored metadata file could be used as an alternative)
- `iwd.saml_sp_metadata`—The path to the locally stored metadata file for the current SP (iWD Manager). The default value is `metadata/iwdmanager_sp.xml` .
- `iwd.saml.iwd_url`—Set to the full URL of the local SP.

2. In order to confgure Single Log-Out set following attributes in the `sso.properties` :
   - `iwd.saml.sloEnabled`—Set to `true`.
   - `iwd.saml.sloAppName`—Set to application name.
   - `iwd.saml.sloRegEndpoint`—Set to `<activity-monitor-url>/v01/slo/registration/sp`.
   - `iwd.saml.sloUnregEndpoint`—Set to `<activity-monitor-url>/v01/slo/unregistration/sp`.
   - `iwd.saml.spSloEndpoint`—Set to `<iwd-manager-url>/saml/logout`.
   - `iwd.saml.spHeartbeatHandlerEndpoint`—Set to `<activity-monitor-url>/v01/server/activities`.
   - `iwd.saml.sloLogoutUrl`—Set to `/saml/logout`.
   - `iwd.saml.postLogoutUrl`—Set to `<hub-landing-page-url>` or `/ui/blank.jsf`.
3. Obtain encryption keys and store them in the local keystore file. The Java keystore is managed using the JDK keytool command. iWD needs to know the location of the keystore file, key name and passwords which are provided using the following properties:
   - `iwd.saml.keystore`—`/security/samlKeystore.jks`
   - `iwd.saml.keyname`—`iwdmanager`
   - `iwd.saml.keypass`—`ChangeIt`
   - `iwd.saml.keystorepass`—`ChangeIt`
4. To encrypt password fields, use the `passwordEncoder` tool and set `iwd.saml.keystorePasswordsEncoded` as follows:
   - `iwd.saml.keypass`—`********`
   - `iwd.saml.keystorepass`—`********`
   - `iwd.saml.keystorePasswordsEncoded`—`true`
5. Generate the metadata file if it is not present:

Before 8.5.103.04

   a. Set the `iwd.saml.generate_metadata` property to `true`.
   b. Set the `iwd.saml.iwd_url` property to `<iwd-manager-url>/saml/metadata`. in the `iwd.properties` file. In case missing of such atribute, please add it.
   c. Restart iWD Manager and go to the `<iwd-manager-url>/saml/metadata` URL.
   d. Rollback `generate_matadata` to `false`.

After 8.5.103.04

a. Go to the `<iwd-manager-url>/saml/metadata` URL, no additional configuation modification is required.

b. Save the downloaded metadata file.

6. Provide the SP's metadata file to your IDP.
7. Enable concurrent former logging to iWD Manager in the HUB environment by setting the `iwd.saml.formLoginEnabled` property to `true` in `sso.property` file.

Configuring UCS over TLS (Win)

Configuring UCS over TLS (Win)

When UCS has Transport Layer Security (TLS) configured, either as a server on its ESP port, or as a client in its connection to Message Server, there are two ways to enable it as a Windows Service:

-Log on As a Local Host User

1. Select the Windows service related to UCS.
2. Select the **Log On** tab. The default setting is `Log on as local system account`.
3. Select `Log on as this account` and provide the login/password of a local host user.

-Import a Certificate to the Local System Account

1. Do one of the following:
   - Run `psexec.exe -i -s mmc.exe`, then import a certificate for a user that is the local system account.
   - Run `psexec.exe -i -s certutil -f -user -p` *`[password]`* `-importpfx` *`[path to the certificate]`*

> **Important**
>
> With the flag `-s`, `psexec.exe` executes the specified program under the system account. `psexec` is part of PSTools, which can be downloaded from http://technet.microsoft.com/en-US/sysinternals