



GroupID

by *Imanami* | NOW PART OF *netwrix*

Version 10



GroupID
Authenticate



GroupID
Automate



GroupID
Self-Service



GroupID
Synchronize



GroupID
Password Center



GroupID
Insights



GroupID
Mobile App



GroupID
Reports

Installation & Configuration Guide

Microsoft Windows Servers 2012, 2016 & 2019 Families

Installation & Configuration Guide

This publication applies to GroupID Version 10 and subsequent releases until otherwise indicated in new editions.

© 2022 Imanami | Now Part of Netwrix. Trademarks are the property of their respective owners.

Contents

About GroupID 10	1	Connect to a different server.....	45
The GroupID Installer	1	Convert a client to a server.....	46
Part 1 - GroupID Prerequisites	2	Chapter 3 - Uninstalling GroupID	48
Chapter 1 - GroupID Prerequisites.....	3	Uninstall GroupID for Upgrade	48
Hardware Requirements.....	3	Complete Uninstall	49
Supported Microsoft® Windows Servers	3	Part 4 - GroupID Upgrade.....	53
Supported Microsoft® Exchange Servers.....	4	Chapter 1 - Upgrading to GroupID 10.....	54
Database Requirements.....	4	Upgrade to GroupID 10	54
Part 2 - GroupID Installation	6	Part 5 - Appendices.....	69
Chapter 1 - GroupID Installer	7	Appendix A.....	70
GroupID Installation Package.....	7	Setting up Authentication modes.....	70
Who can install GroupID.....	7	SQL Server Authentication	70
Installation Cases.....	8	Windows Authentication.....	71
Chapter 2 - Installing GroupID	9	Appendix B.....	72
Preparation Tool.....	9	The do's and don'ts of the Upgrade wizard	72
Installation Tool	13	Multi-domain upgrade	74
Chapter 3 - What does the Preparation Tool Install	17	Appendix C.....	76
Part 3 - GroupID Configuration	21	Authorizing additional users/groups as GroupID administrators.....	76
Chapter 1 - Configuring GroupID	22	Appendix D.....	79
Configuration Tool.....	22	Backing Up and Restoring GroupID Data.....	79
How to Configure a GroupID Server.....	24		
How to Configure a GroupID Client.....	35		
Configure a GroupID server with existing database.....	36		
Chapter 2 - Modifying GroupID Configurations..	39		
Modifying a GroupID Server	40		
Change Server Configurations.....	40		
Convert the server to a client	45		
Modifying a GroupID Client.....	45		

About GroupID 10

GroupID 10 has been designed to work with any identity store, such as a generic LDAP provider, G Suite, Microsoft Azure, and more.

The GroupID Installer

The GroupID Installer redefines GroupID installation as an efficient shift from a manual, time-consuming job.

Till GroupID 7, users had to manually install software and enable Windows features required by GroupID. The task was made more complex when these prerequisites varied slightly for different modules and portals.

With the GroupID Installer, you just have to specify the GroupID modules and the messaging provider you want to use. Based on this information, the Installer not only auto detects the prerequisite software and Windows features that GroupID requires, it also installs them without any manual intervention. This has practically simplified GroupID installation, reduced workloads, and diminished installation times from hours to just a few minutes.

Furthermore, GroupID configuration is no more a distinct task; rather, it has been seamlessly integrated into the installation experience. Once you've run the Installer, launch GroupID and start using it.

Part 1 - GroupID Prerequisites

Chapter 1 - GroupID Prerequisites

This chapter covers the operating system, Exchange, database and hardware required to run GroupID 10. The prerequisites may vary depending on your environment.

Hardware Requirements

Minimum hardware requirements for GroupID are:

- x64 Processor / Intel® Pentium® IV (2.4 GHz or higher)
- 8 GB of RAM (for up to 250,000 objects in the directory)
- 1024 MB hard drive space (for installation only)

Space requirement is relative to the provider's data size growth for Elasticsearch data.

Supported Microsoft® Windows Servers

GroupID supports the following Microsoft® Windows Servers:

Microsoft® Windows Server 2012 Family

- Windows Server 2012 Standard
- Windows Server 2012 Datacenter

Microsoft® Windows Server 2016 Family

- Windows Server 2016 Standard
- Windows Server 2016 Datacenter

Microsoft® Windows Server 2019 Family

- Windows Server 2019 Standard
- Windows Server 2019 Datacenter

Supported Microsoft® Exchange Servers

GroupID supports the following Microsoft® Exchange Servers:

- Microsoft® Exchange Server 2010
- Microsoft® Exchange Server 2013
- Microsoft® Exchange Server 2016
- Microsoft® Exchange Server 2019

Database Requirements

GroupID requires an SQL Server database to store and retrieve data.

The SQL database may reside on any SQL Server in your environment. GroupID supports the following versions of SQL Servers:

Database Server	Editions
Microsoft® SQL Server 2008	Express, Standard, Enterprise <i>Express edition available at:</i> Microsoft® SQL Server® 2008 Express
Microsoft® SQL Server 2008 R2	Express, Standard, Enterprise <i>Express edition available at:</i> Microsoft® SQL Server® 2008 R2 SP2 - Express Edition
Microsoft® SQL Server 2012	Express, Standard, Enterprise <i>Express edition available at:</i> Microsoft® SQL Server® 2012 Express
Microsoft® SQL Server 2014	Express, Standard, Enterprise <i>Express edition available at:</i> Microsoft® SQL Server® 2014 Express

Database Server	Editions
Microsoft® SQL Server 2016	Express, Standard, Enterprise <i>Express edition available at:</i> SQL Server 2016 Express edition
Microsoft® SQL Server 2017	Express, Standard, Enterprise <i>Express edition available at:</i> SQL Server 2017 Express edition
Microsoft® SQL Server 2019	Express, Standard, Enterprise <i>Express edition available at:</i> SQL Server 2019 Express edition

The SQL Server Browser service is required and during the installation of SQL Server, you can set its start mode either as *Automatic*, *Disabled* or *Manual*. If it is disabled, SQL Servers are not listed in the **SQL Server** box on the **Database settings** page (Figure 15) of the Configuration Tool. In that case, you have to type the server name in the **SQL Server** box to select the required server manually.

To enable the SQL Server Browser service, see [How to: Start and Stop the SQL Server Browser Service](#).

Part 2 - GroupID Installation

Chapter 1 - GroupID Installer

After ensuring that all prerequisites have been set in the environment, you can proceed to install GroupID.

The GroupID Installer installs GroupID without any manual configuration. It comprises of:

- [Preparation Tool](#)
This tool not only detects prerequisite software and Windows features required by GroupID; it also installs them automatically.
- [Installation Tool](#)
When prerequisites are installed, the Installation Tool installs GroupID.
- [Configuration Tool](#)
This tool carries out the GroupID services and database configurations.

GroupID Installation Package

The GroupID installation package consists of:

- Core Installer (file folder)
- Diagnostics (file folder)
- Guides (file folder)
- Preparation Tool (file folder)
- Setup.exe (application)

Who can install GroupID

Before installing GroupID, make sure that the logged-in user is a member of the local Administrators group on that machine.



There is a dedicated server for GroupID.

- Do not install GroupID on the domain controller.
- Do not install GroupID and Microsoft® Exchange Server on the same machine.

Installation Cases

Choose one of the four installation cases for GroupID 10:

- **Case # 1:** GroupID 10 to co-exist with GroupID 9 on the same machine
- **Case # 2:** GroupID 10 to co-exist with GroupID 7.0/ 8.0/ 8.1/ 9.0 in the same environment
- **Case # 3:** In-place installation of GroupID 10 on the same machine
- **Case # 4:** In-place installation of GroupID 10 in the environment

The GroupID 10 installation and configuration process is the same for all four cases. You must create a copy of the database being used with the previous GroupID version and bind the copy with GroupID 10. The database can be copied when you configure GroupID 10 (Figure 15).

Next, run the Upgrade wizard it to make the copied database compatible with GroupID 10. Once upgraded, the database schema changes, making it incompatible with the previous GroupID version.



When GroupID 10 co-exists with a previous GroupID version (case # 1 and 2), the two must have separate databases. Data is not replicated between these databases.



This section does not apply to a fresh GroupID installation.

Chapter 2 - Installing GroupID

To use GroupID, the first step is to install the prerequisite software and then proceed to install GroupID.

Double-click the **setup.exe** file available in the GroupID installation package to launch the GroupID Installer.



Figure 1: The GroupID Installer

Preparation Tool

Run the Preparation Tool on a machine to prepare it for GroupID.



GroupID requires [Microsoft® .NET Framework 4.7.2](#). You must install it on the machine before you run the Preparation Tool.

1. Click **Install pre-requisite softwares** on the GroupID Installer (Figure 1) to launch the Preparation Tool.

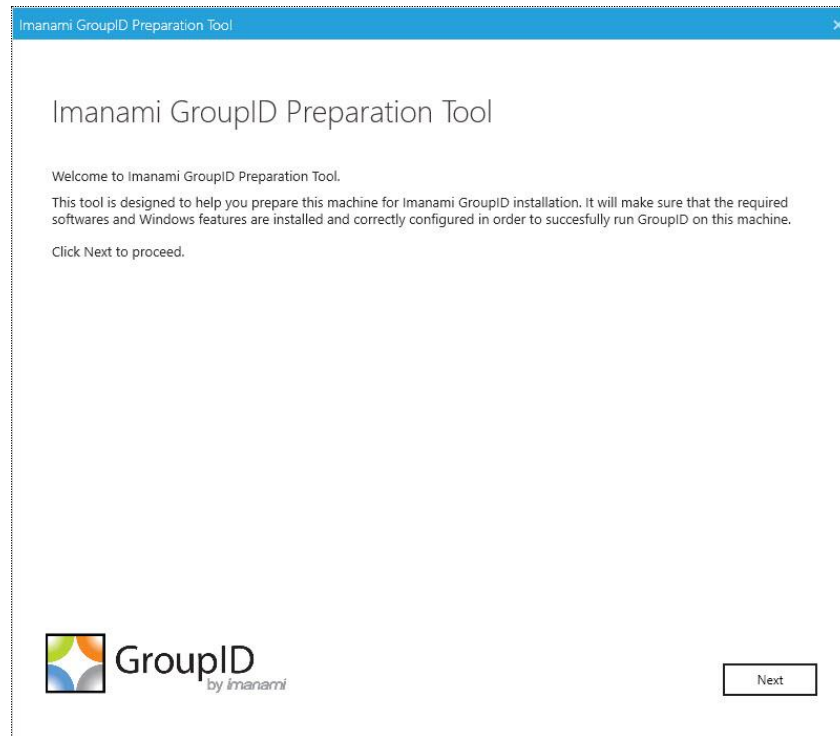


Figure 2: Welcome page

2. Read the welcome message and click **Next**.

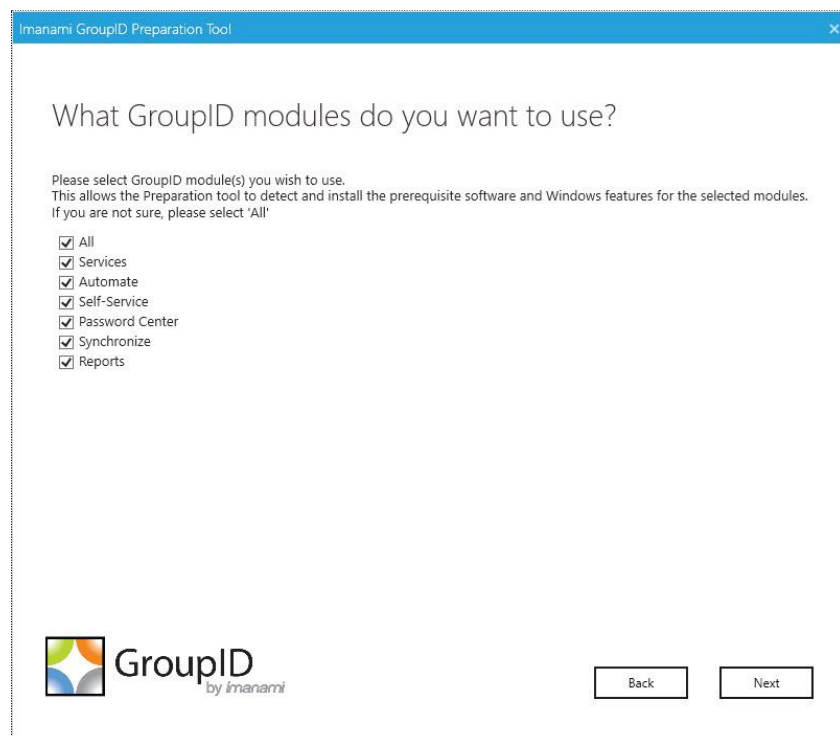


Figure 3: GroupID Modules page

3. Select the check boxes for the GroupID modules you want to use. This allows the Preparation Tool to detect and install the prerequisite software and Windows features for the selected modules.
4. Click **Next**.

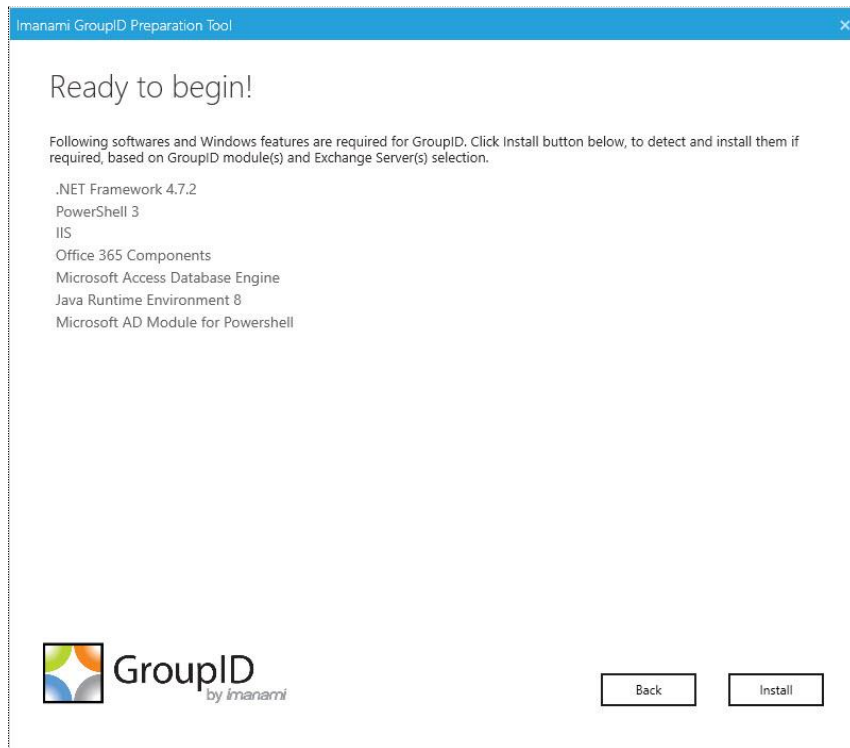


Figure 4: Ready to begin page

Based on the modules and Exchange Servers selected, the **Ready to begin** page lists the required software and Windows features that the Preparation Tool has identified for GroupID.

5. Click **Install** to begin.

The progress bar shows the installation progress while prerequisites are installed.

- On installation, the next page displays the status of each prerequisite software and Windows feature as *Passed* or *Failed*.

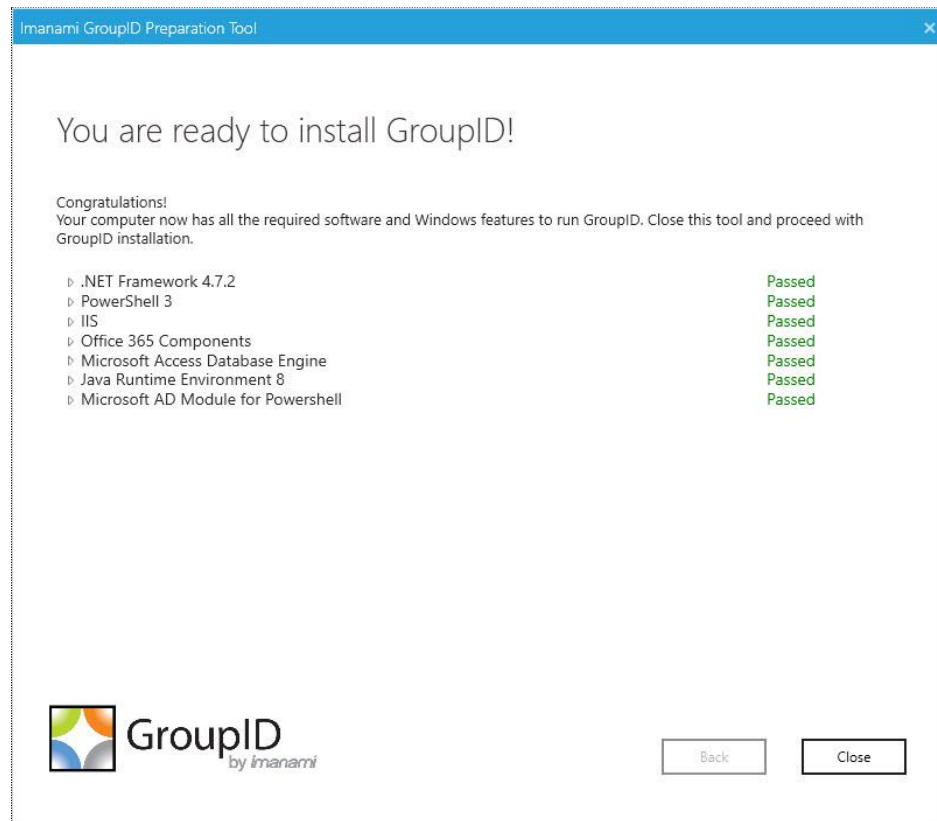


Figure 5: Prerequisite Installation Status page

Expand the node for a prerequisite to view its details.

- A *Passed* prerequisite has one of these statuses:
 - was already installed (no action taken)
 - Configured Successfully
- For a *Failed* prerequisite, read the given message and take appropriate action. That done, click **Retry** to verify whether the prerequisite has been installed.

- After viewing the information, click **Close**.

If you are installing the prerequisites for the first time, a message to restart the machine is displayed. Click **OK** to restart.

To view the list of installed software and Windows features, refer to Chapter 3 - What does the Preparation Tool Install.

Installation Tool

Installing GroupID is a two-step process; agree to the license agreement and specify the path where GroupID should be installed.

1. Click **Install GroupID** on the GroupID Installer (Figure 1).

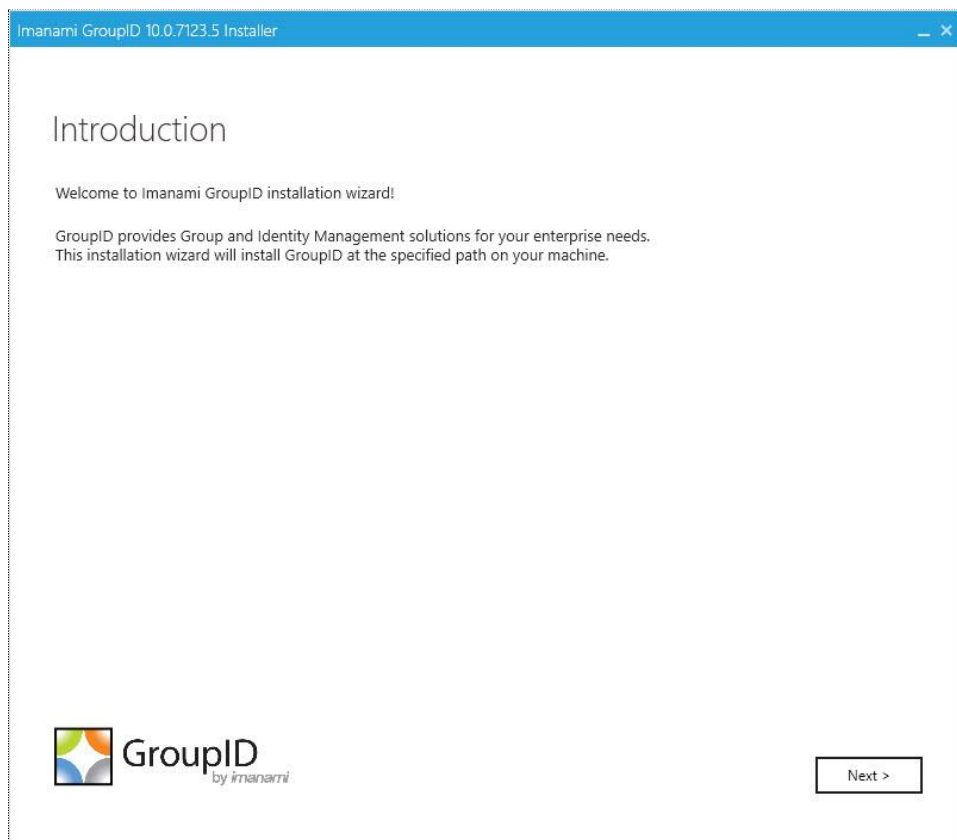


Figure 6: Introduction page

2. Read the welcome message and click **Next**.

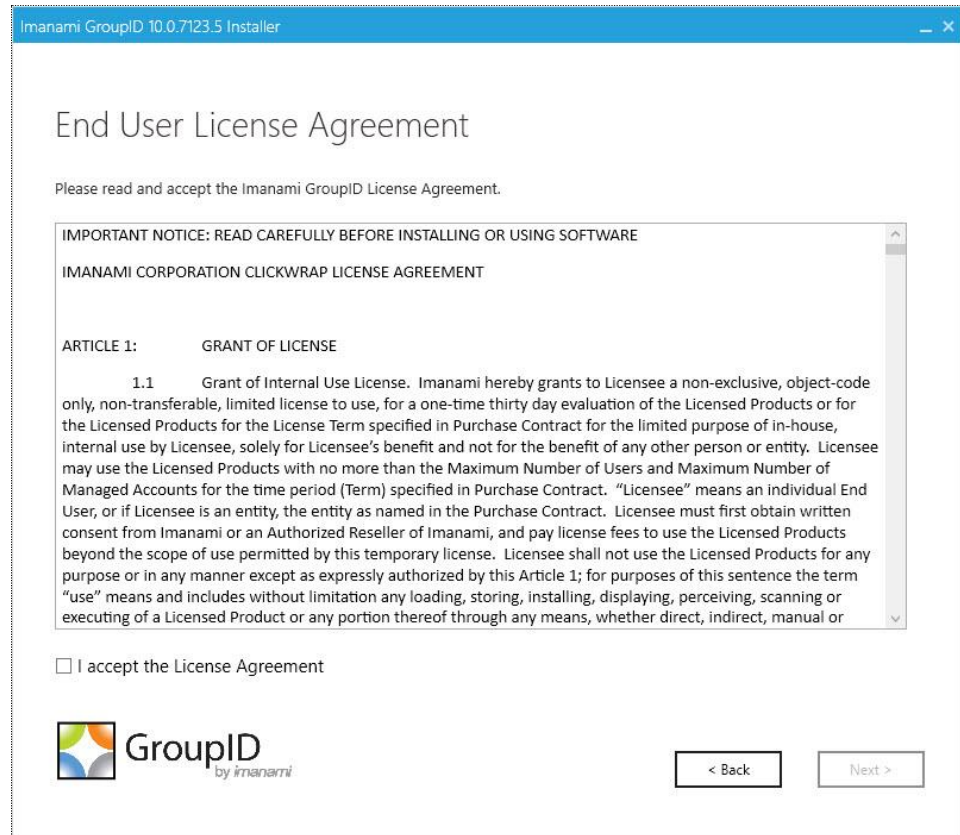


Figure 7: End User License Agreement page

3. On the **End User License Agreement** page, review and accept the licensing agreement and click **Next**.

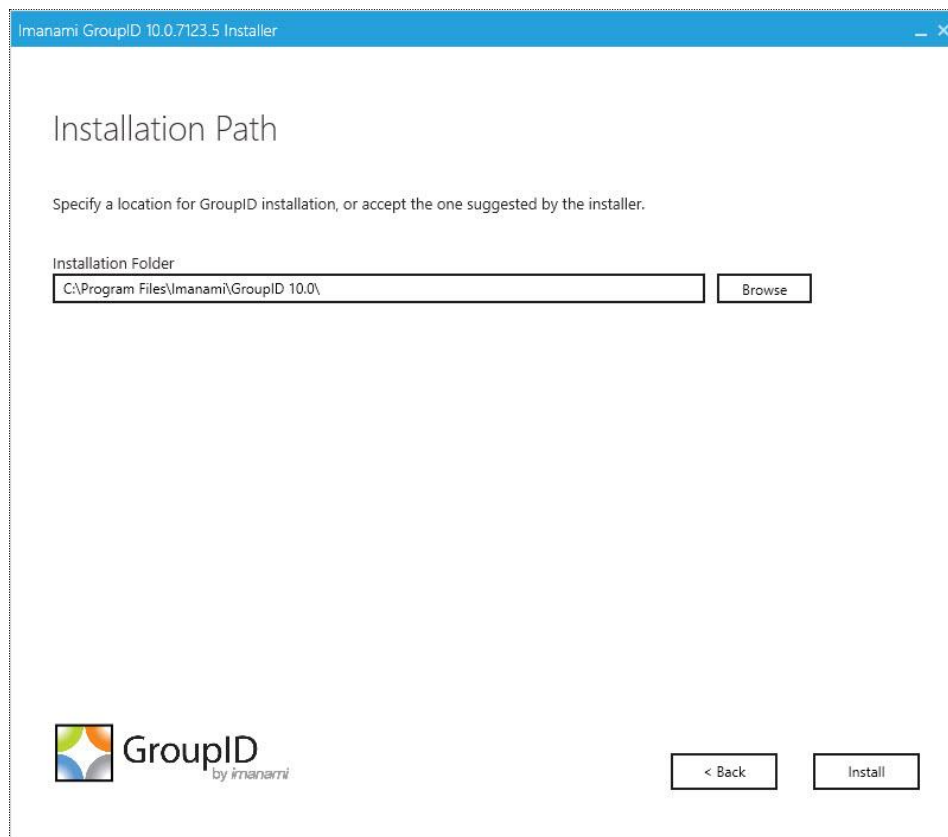


Figure 8: Installation Path page

4. In the **Installation Folder** box, specify the location where you want to install GroupID or accept the one suggested by the Installer. Click **Install**.

The progress bar shows the installation progress while all files are copied to the specified location and GroupID is installed.



When GroupID 9 and GroupID 10 co-exist on the same machine, the **GroupID 9.0** and **GroupID 10.0** folders at the path, C:\Program Files\Imanami\, relate to the GroupID 9 and GroupID 10 installations respectively.

5. On successful installation, the **Run Configuration Tool** page is displayed. Use the Configuration Tool to configure GroupID.

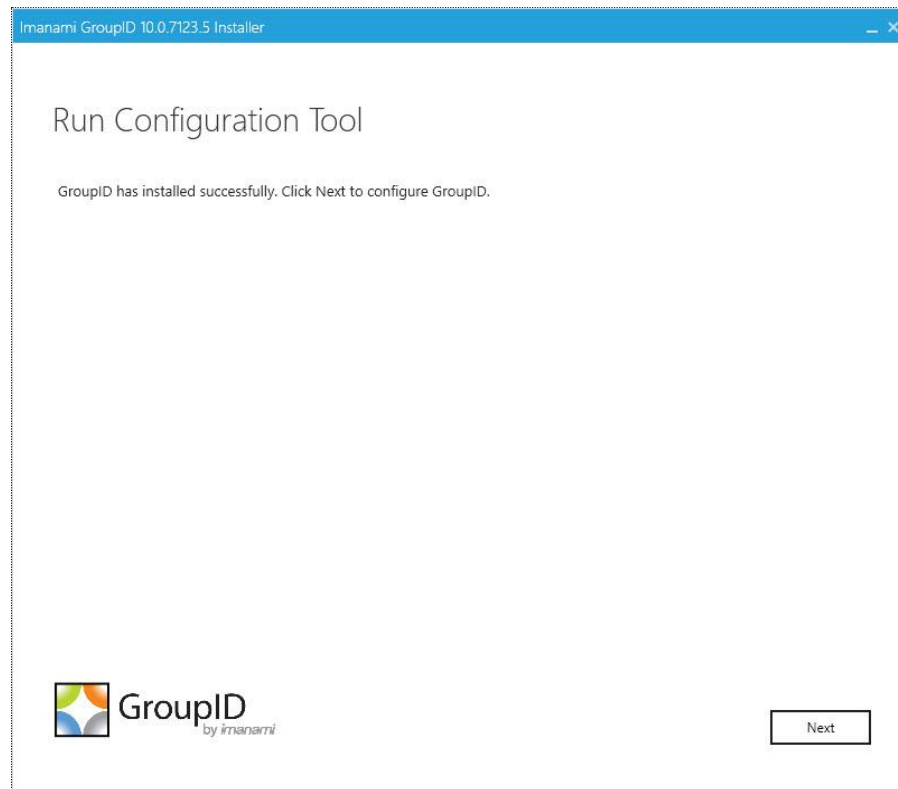


Figure 9: Run Configuration Tool page

6. GroupID is installed on your machine. You can choose to configure GroupID now or later.

- Click **Next** to proceed with configuring GroupID.

OR


- Click **Close** (X) on the Title bar to close the GroupID Installer and configure GroupID later.

To configure GroupID, refer to Chapter 1 - Configuring GroupID in Part 3 - GroupID Configuration.

Chapter 3 - What does the Preparation Tool Install

When the [GroupID Preparation Tool](#) runs, it installs the following software and Windows features:

Software	Comments
Required by all modules of GroupID	
<p>Microsoft® Internet Information Services (IIS) with the following role services:</p> <ul style="list-style-type: none">▪ Common HTTP Features<ul style="list-style-type: none">✓ Default Document✓ Directory Browsing✓ HTTP Errors✓ Static Content✓ WebDAV Publishing▪ Application Development<ul style="list-style-type: none">✓ NET Extensibility✓ ASP.NET✓ ISAPI Extensions✓ ISAPI Filters▪ Health and Diagnostics<ul style="list-style-type: none">✓ HTTP Logging▪ Security<ul style="list-style-type: none">✓ Request Filtering✓ Windows Authentication▪ Performance<ul style="list-style-type: none">✓ Static Content Compression▪ Management Tools<ul style="list-style-type: none">✓ IIS Management Console✓ IIS 6 Metabase Compatibility under IIS 6 Management Compatibility	

Software	Comments
Windows server features: <ul style="list-style-type: none"> ▪ Windows Process Activation Service <ul style="list-style-type: none"> ✓ Process Model ✓ Configuration APIs 	
Microsoft® .NET Framework 4.7.2 features: <ul style="list-style-type: none"> ▪ WCF Services <ul style="list-style-type: none"> ✓ Http Activation and its dependent features Click here to download.	GroupID only supports this specific version of .Net Framework.
Microsoft® Distributed Transaction Coordinator	The Microsoft® Distributed Transaction Coordinator service (MSDTC) is installed during the installation of the Windows OS. Errors that occur during installation may stop the component from working properly. Any errors that occur during an upgrade process may also stop the component from working properly <i>More information:</i> <u>Microsoft® Distributed Transaction Coordinator Service Installation and Setup</u>
Windows PowerShell 3.0	Windows Server 2012 includes PowerShell 3.0 by default.
Java Runtime Environment 8	The Java Runtime Environment version may vary, depending on the OS.
Elasticsearch 6.2.4	If 95% of space is consumed on C drive, Elasticsearch will stop responding intermittently and will require a restart after more than 95% space is available. When Elasticsearch is locked, any object created or modified in GroupID will be committed in provider but not in the Elasticsearch repository.  While configuring an Elasticsearch cluster on all GroupID Instances,

Software	Comments
	<p>make sure that port TCP IP 9305 or a custom port (configured in the yml file for the Elasticsearch cluster) is unblocked and remains the same on each GroupID instance that is part of the master-slave cluster.</p>
Microsoft AD module for PowerShell	
WinRM IIS Extension	<p>For GroupID to make a connection to Exchange, configure WinRM in one of the following ways.</p> <ul style="list-style-type: none"> ▪ Option 1: intra-Domain Both GroupID and the destination Exchange host must be in the same domain. Both systems must have WinRM configured (use the PowerShell command <code>winrm /quickconfig</code> for this). The default value for the necessary listener(s) is * and that is all that is necessary to make a remote connection when the “-authentication” parameter is not specified. ▪ Option 2: Inter-Domain Both systems must have WinRM configured (use the PowerShell command <code>winrm /quickconfig</code> for this). Design the hosts to trust each other by configuring “Trusted Hosts” either by GPO or locally. <ul style="list-style-type: none"> ✓ By GPO: Computer > Windows > Admin Templates > Windows Components > Windows Remote Management > WinRM Client > Trusted Hosts ✓ Use this PowerShell command to configure locally: <code>Set-Item wsman:\localhost\Client\Trus</code>

Software	Comments
	tedHosts -Value <servername.domain.com>
Required by Password Center	
Microsoft® ASP .NET MVC 5	This is automatically installed with .NET Framework 4.7.2.
Required by Synchronize	
Microsoft® Access Database Engine 2010 Redistributable <i>Click here to download.</i>	Required if Microsoft® Office Access 2010 or Microsoft® Office Excel 2010 is used in a Synchronize job, either as a source or a destination. Install manually since the Preparation tool will not detect and install it automatically.
2007 Office System Driver <i>Click here to download.</i>	Required if Microsoft® Office Access 2007 or Microsoft® Office Excel 2007 is used in a Synchronize job, either as a source or a destination. Install manually since the Preparation tool will not detect and install it automatically.

Part 3 - GroupID Configuration

Chapter 1 - Configuring GroupID

Use the Configuration Tool to configure a new GroupID server or a new GroupID client. In either case, the tool configures:

- A valid license for GroupID
- Connection with GroupID Data Service and GroupID Security Service
- An encryption key to encrypt GroupID data
- An SQL Server and database



When the IP of a GroupID server machine changes, you must run the Configuration Tool again.

Configuration Tool

You can configure GroupID immediately after installing it or later.

1. Run the Configuration Tool in one of the following ways:
 - To configure GroupID right after installation, click **Next** on the **Run Configuration Tool** page (Figure 9).
 - When GroupID is installed, the Configuration Tool is also installed as a separate program on the machine.

Launch the GroupID Configuration Tool from the Windows Start screen or from GroupID Management Console > Configurations node > Configure GroupID.

In either case, the tool opens to the **Introduction** page.

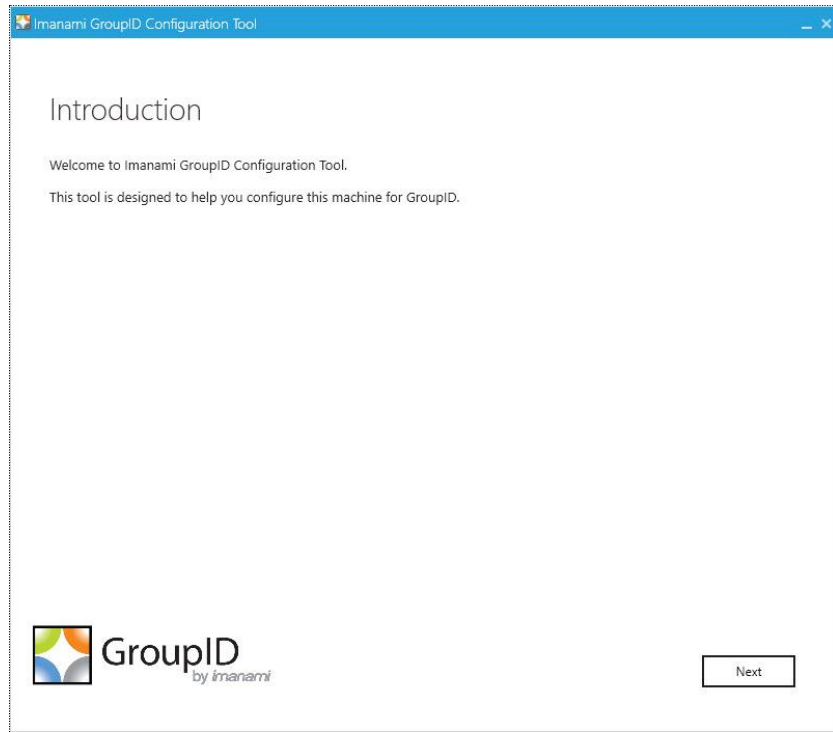


Figure 10: Introduction page

2. Read the welcome message and click **Next**.

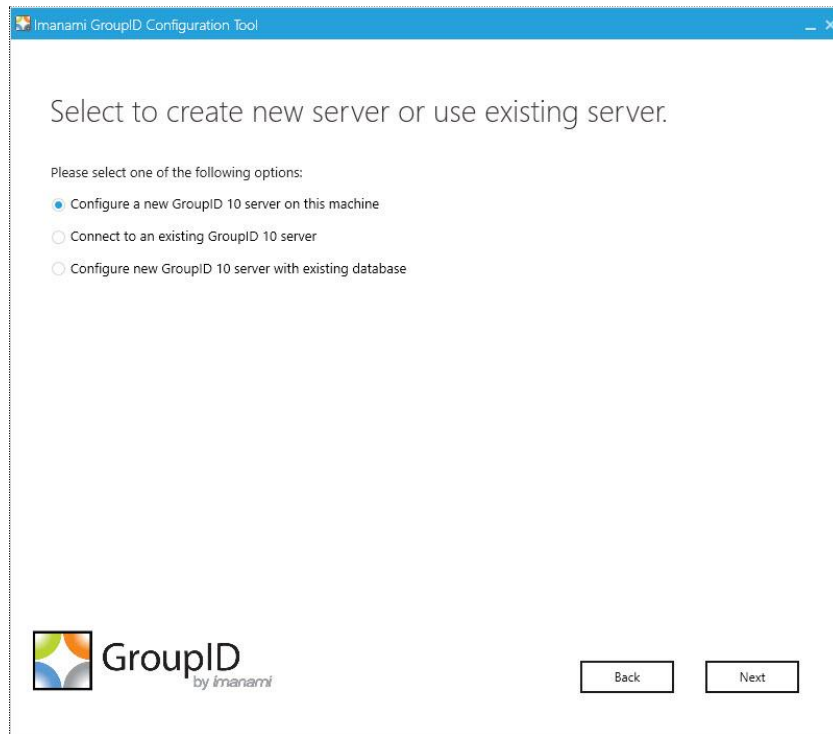


Figure 11: GroupID Server Configuration page

3. To configure a GroupID server or a GroupID client, select the relevant option.
 - **Configure a new GroupID 10 server on this machine** – configures the GroupID server and the GroupID Data Service on the machine where GroupID is being installed.

It also configures the GroupID Elasticsearch Service as a master node for the Elasticsearch service cluster to support load balancing.

Follow the instructions in How to Configure a GroupID Server to configure a new GroupID server.

- **Connect to an existing GroupID 10 server** – configures a GroupID client that connects to a GroupID server already configured in your environment.

Follow the instructions in How to Configure a GroupID Client to configure a GroupID client.



All GroupID clients connected to a GroupID server share the same database. Hence, any change made to GroupID using the server or any client are reflected in the Management Console of the server and all connected clients.

- **Configure new GroupID 10 Server with existing database** – configures a GroupID server that has its own Data Service, but this Data Service uses the configurations (paraphrase and database settings) of the Data Service deployed for another GroupID server in your environment.

This option also configures the GroupID Elasticsearch Service as a slave node to the master node for the Elasticsearch Service cluster configured on the GroupID server.

Follow the instructions in Configure a GroupID server with existing database to configure a GroupID server with load balancing support.

How to Configure a GroupID Server

Configuring a new GroupID server involves:

- A valid license for GroupID
- Connection with GroupID Data Service and GroupID Security Service
- An encryption key to encrypt GroupID data
- An SQL Server and database

- Service accounts for GroupID App Pool, scheduled jobs and Windows services

To configure a new GroupID server:

1. On the **GroupID Server Configuration** page (Figure 11), select **Configure a new GroupID 10 server on this machine** to configure the GroupID server on the machine where GroupID is currently being installed.

This also configures the GroupID Elasticsearch Service as a master node for the Elasticsearch service cluster to support load balancing.

2. Click **Next**.

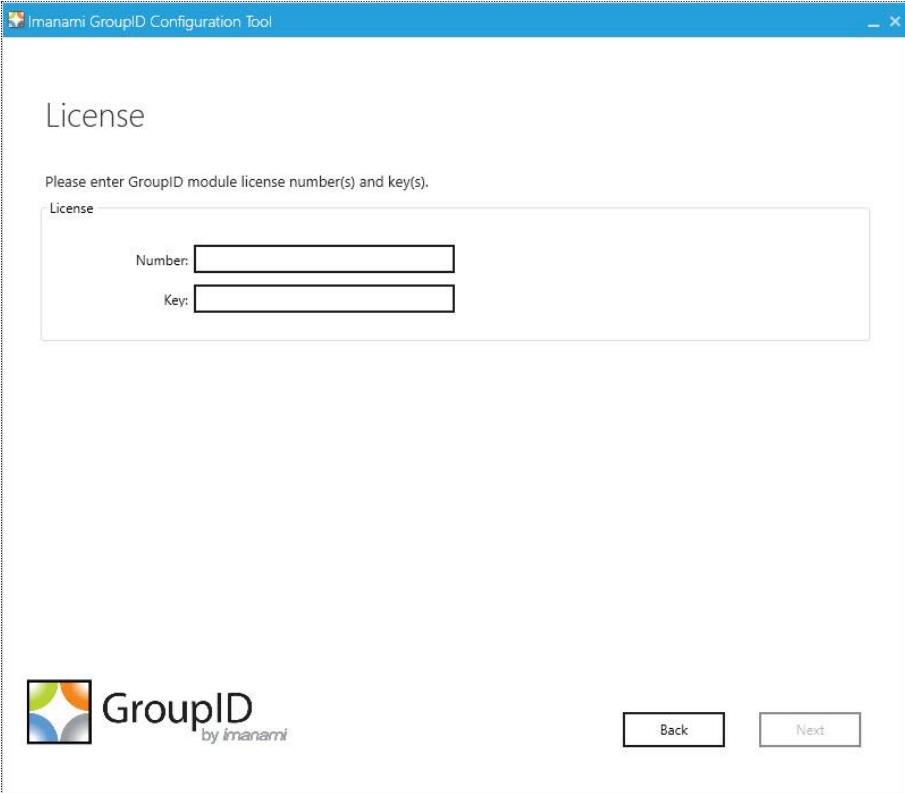
The screenshot shows a window titled "Imanami GroupID Configuration Tool". The main heading is "License". Below it, the text reads "Please enter GroupID module license number(s) and key(s)". There is a large text area labeled "License" containing two input fields: "Number:" and "Key:". At the bottom left is the GroupID logo with the text "by imanami". At the bottom right are two buttons: "Back" and "Next".

Figure 12: License page

3. On the **License** page, enter a valid license number and key in the respective boxes. A valid license and key enable the **Next** button. If the **Next** button remains disabled, check your entries for errors.

If you have licensed GroupID by module, provide any one license here. To enter another license, do one of the following:

- After completing the GroupID configurations, launch the Configuration Tool from the Windows Start screen and proceed to enter another license (Figure 26).

- Launch GroupID Management Console, run the Configuration Tool from the Configuration node, and proceed to enter another license.
4. Click **Next**.

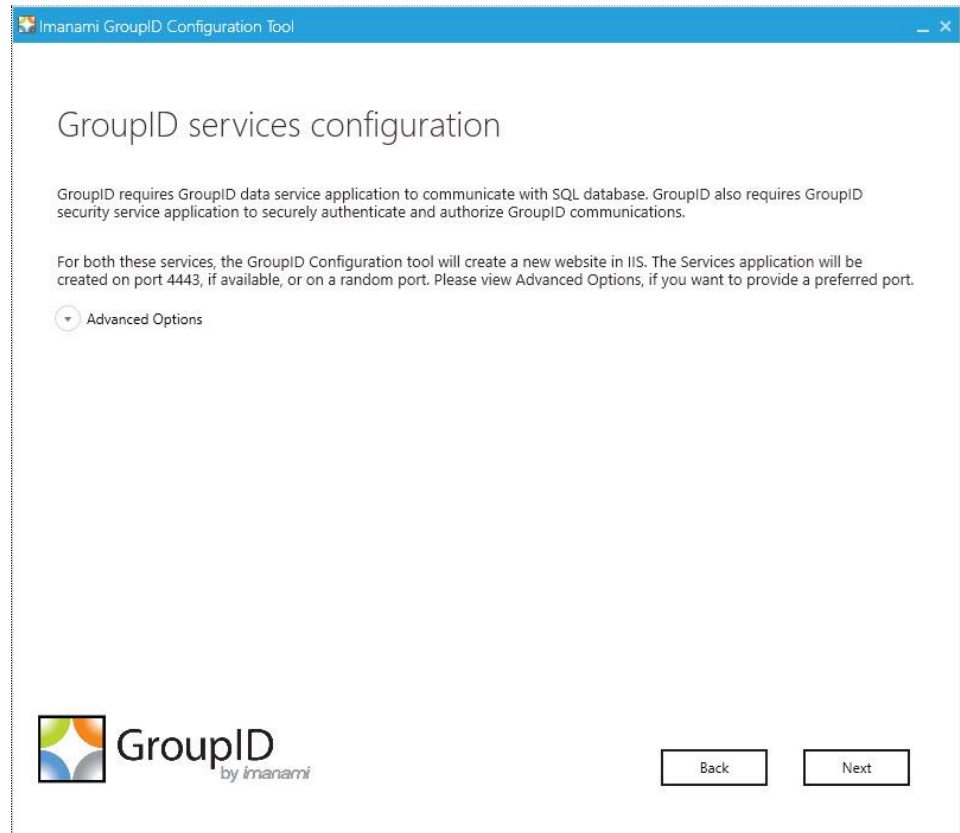


Figure 13: Service Configuration page

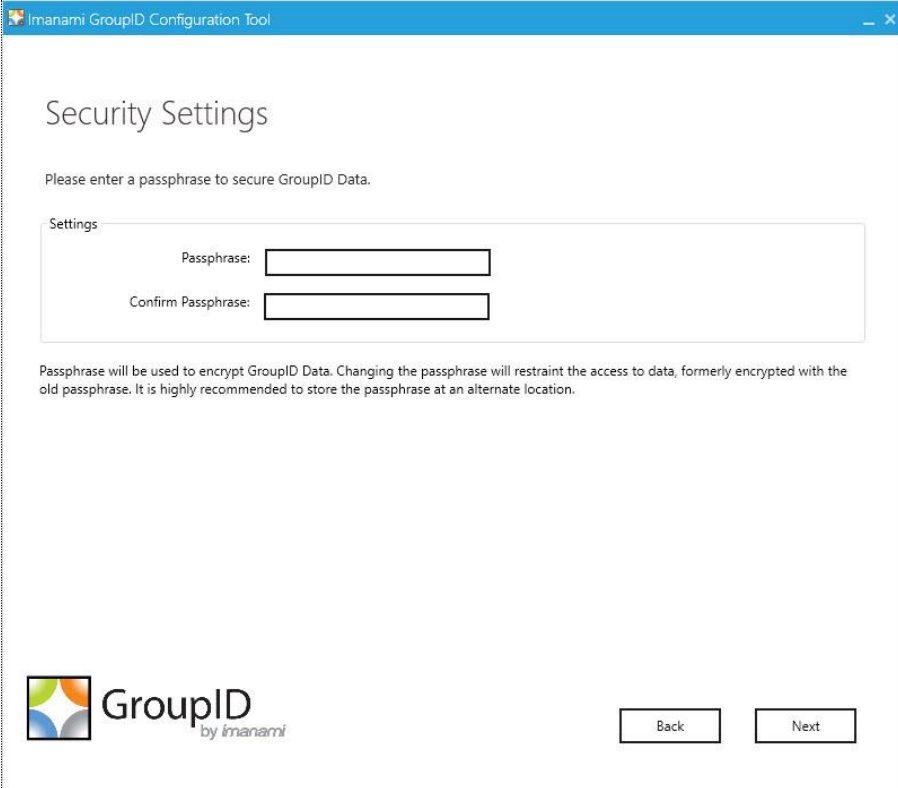
GroupID requires two services:

- **GroupID Data Service**
This is a web-based service that GroupID uses to communicate with Microsoft® SQL Server for storing and fetching data in the database.
- **GroupID Security Service**
This is also a web-based service that GroupID uses to:
 - Authenticate and authorize users on different GroupID functionalities in accordance with their roles.
 - Encrypt and decrypt data that GroupID Data Service stores and fetches from the SQL database.

To deploy these services, the Configuration Tool creates and configures a new website in IIS with the name GroupIDSite10. By default, it binds this site to any of the available ports. However, if you have a different preference, you can change the port.

Click **Advanced Options** and enter the port in the **Port Number** box.

5. Click **Next**.



The screenshot shows a window titled "Imanami GroupID Configuration Tool" with a "Security Settings" page. The page instructs the user to "Please enter a passphrase to secure GroupID Data." Below this, there is a "Settings" box containing two input fields: "Passphrase:" and "Confirm Passphrase:". A note below the fields states: "Passphrase will be used to encrypt GroupID Data. Changing the passphrase will restrain the access to data, formerly encrypted with the old passphrase. It is highly recommended to store the passphrase at an alternate location." At the bottom of the window, there is the GroupID logo (by Imanami) and two buttons: "Back" and "Next".

Figure 14: Security Settings page

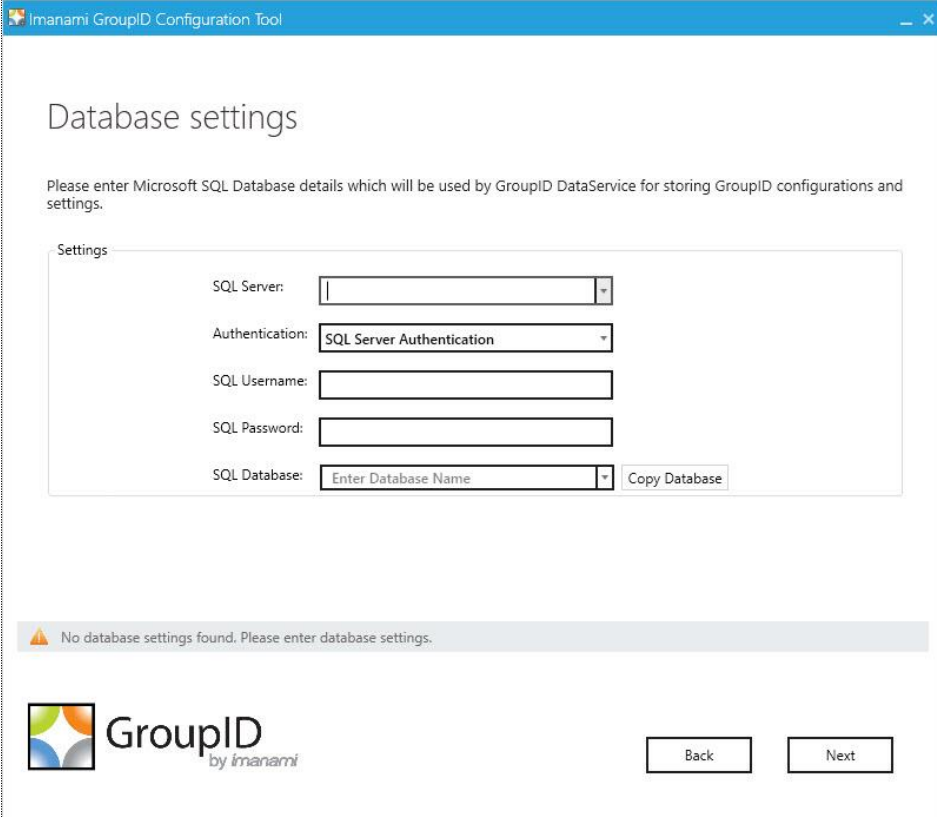
6. On the **Security Settings** page, enter an encryption key in the **Passphrase** and **Confirm Passphrase** boxes to secure GroupID data.

GroupID Data Service uses this key to encrypt and decrypt the data that it stores in, and retrieves from, the SQL Server database.



- The passphrase must have at least eight characters.
- If you are upgrading to GroupID 10 from a previous GroupID version, provide the encryption key you used in that product; else, you would not be able to upgrade.
- Be sure to save this passphrase with you. Providing an incorrect passphrase at any later point will result in the loss of GroupID data.

7. Click **Next**.




The screenshot shows the 'Database settings' page of the 'Imanami GroupID Configuration Tool'. The page title is 'Database settings'. Below the title, there is a message: 'Please enter Microsoft SQL Database details which will be used by GroupID DataService for storing GroupID configurations and settings.' The main form area is titled 'Settings' and contains the following fields:

- SQL Server: A dropdown menu.
- Authentication: A dropdown menu with 'SQL Server Authentication' selected.
- SQL Username: A text input field.
- SQL Password: A text input field.
- SQL Database: A dropdown menu with 'Enter Database Name' selected, and a 'Copy Database' button to its right.

Below the form, there is a warning message: 'No database settings found. Please enter database settings.' At the bottom of the page, there is the GroupID logo (by Imanami) and two buttons: 'Back' and 'Next'.

Figure 15: Database Settings page

8. In the **SQL Server** list, select the SQL Server to use with GroupID.

If the required server does not appear in the list, make sure that the **SQL Server Browser service** is running on the SQL Server machine and then click the **Refresh**  button.

9. In the **Authentication** list, select an authentication mode to be used when connecting to the SQL Server database. Modes are:

- **SQL Server Authentication**
To set SQL Server to work with GroupID using an SQL Server account.

For details, see [SQL Authentication](#) in Appendix A.

- **Windows Authentication**
To set SQL Server to work with GroupID using a Windows user account.

For details, see [Windows Authentication](#) in Appendix A.

10. Depending on the authentication mode selected, do the following:
 - For SQL Server Authentication, enter the user name and password of the selected SQL Server in the **SQL Username** and **SQL Password** boxes.
 - For Windows Authentication, provide the credentials of a domain account or a Windows local account that GroupID will use to connect with SQL Server. On clicking **OK**, the system authenticates with that account on SQL Server via Windows authentication.
11. Specify the SQL database to use for GroupID by doing one of the following:
 - Use an existing database - click the **SQL Database** drop-down list to get a list of all databases that reside on the selected server. Select the required database to connect it to GroupID.
 - Use a copy of an existing database - You may want to create a copy of the database you used with the previous GroupID version and use the copied database with GroupID 10.

Select the required database from the **SQL Database** drop-down list and click **Copy Database** to create a copy of it.

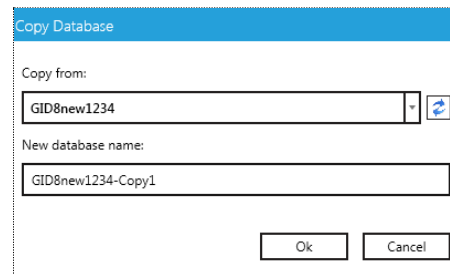


Figure 16: Copy Database dialog box

The **Copy from** list displays the database you want to create a copy of, while the **New database name** box displays a name for the copy. Click **OK**.

- Create a new database - type the name of the new database in the **SQL Database** box.



Create a copy of the database you used with the previous GroupID version and bind the copy with GroupID 10. Refer to Installation Cases for more information.

For a fresh GroupID installation, create a new database.

12. Click **Next**.

In case of a new database, a message is displayed to inform that the database does not exist. Click **Yes** to create it.

Imanami GroupID Configuration Tool

Service Account settings

Please select service accounts for GroupID services on local machine.

Service Accounts

App Pool Account: ...
 Password:
 Configure same account for all

Scheduled Jobs Account: ...
 Password:

Windows Services Account: ...
 Password:

✓ Keys Distribution Service (KDS) is running.



 **GroupID**
by imanami

Figure 17: Service Account Settings page

GroupID enables you to specify the service accounts to use for the GroupID app pool, scheduled jobs, and Windows services.

Services	Service Account Description
GroupID App Pool	<p>Use a domain account or a Group Managed Service Account (gMSA).</p> <p>The account must be a member of the Administrators group or both the Backup Operators and IIS_IUSRS groups.</p> <p>The account you specify will be used to manage the GroupID app pool in IIS. GroupID Data Service, Mobile Service, Security Service, and the portals run under the app pool.</p> <p>By default, a local account, GroupIDSSuser, is set for the GroupID app pool, but you cannot proceed unless you change it to a domain account or gMSA.</p>

Services	Service Account Description
	 You can specify a local account (with local administrator rights) in app pool for a machine that is not joined to any domain (this applies to an Azure AD identity store only).
Scheduled jobs	<p>Use a domain account, local account, or Group Managed Service Account.</p> <p>The account you specify will be used to run GroupID scheduled jobs on the machine.</p> <p>By default, the GroupIDSSuser account is used for scheduled jobs, which is a local account.</p>
Windows services	<p>Use a domain account, system user account, or Group Managed Service Account.</p> <p>The account must be a member of the Backup Operators group.</p> <p>The account you specify will be used to run Windows services created by GroupID.</p> <p>By default, the LocalSystem account is used for Windows services, which is a Group Managed Service Account. You must change it in order to proceed.</p>



For GroupID App Pool and Windows services, only a domain account can be used for a machine joined to a domain. To use a local account, you will have to add a registry key under GroupID 10 on the GroupID server.

Launch the Registry Editor. Select Local Machine > Software > Imanami > GroupID > Version 10.0 > ServiceAccount, and add the string value: key name = AllowLocal, value = True.

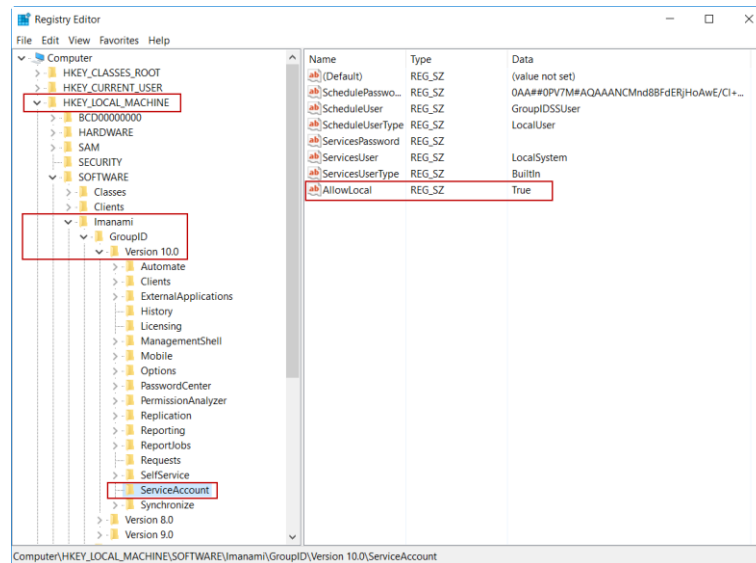


Figure 18: Registry Editor



Before you use a Group Managed Service Account, make sure that:

- Key Distribution Service (KDS) is enabled on the GroupID machine.
- Microsoft AD module for PowerShell is installed on the machine.

13. You can specify service accounts for the app pool, scheduled jobs, and Windows services in any of the following ways:

- Use the default account
- Use an existing account

Click . On the **Find Service Account** dialog box, search and select the required account and click **OK**.

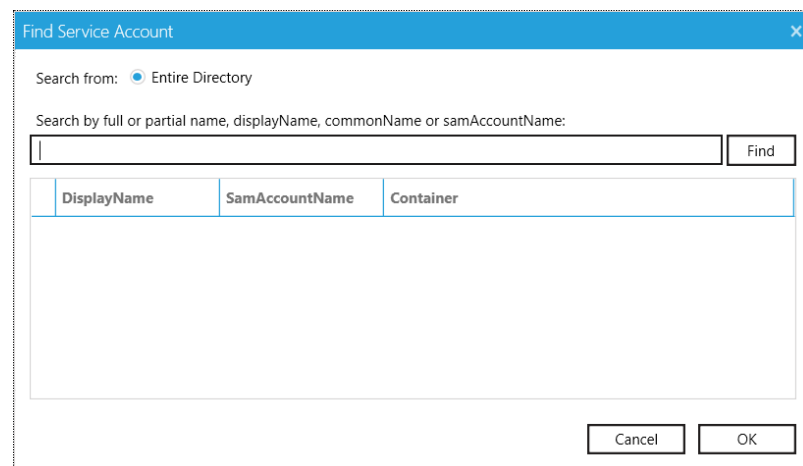


Figure 19: Find Service Account dialog box

- Create a new service account
Click the **Create New** button.

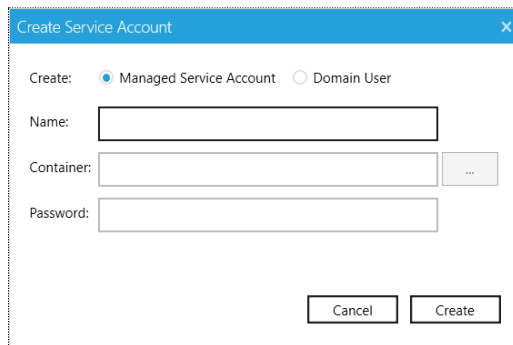


Figure 20: Create Service Account dialog box

On the **Create Service Account** dialog box, select the kind of account you want to create. Then enter a name and password for the account. Select a container to create the account in, and click **Create**.



The logged-in user must have appropriate rights to create a new account.



If Key Distribution Service (KDS) is not configured in the environment, a warning will be displayed that you cannot use a Group Managed Service Account.

14. Provide passwords for the service accounts (except for a Group Managed Service Account) in the **Password** box.
15. Click **Configure**.
16. The next page displays the progress while a GroupID server is configured on the machine. On successful configuration, the **GroupID is successfully configured** page opens.

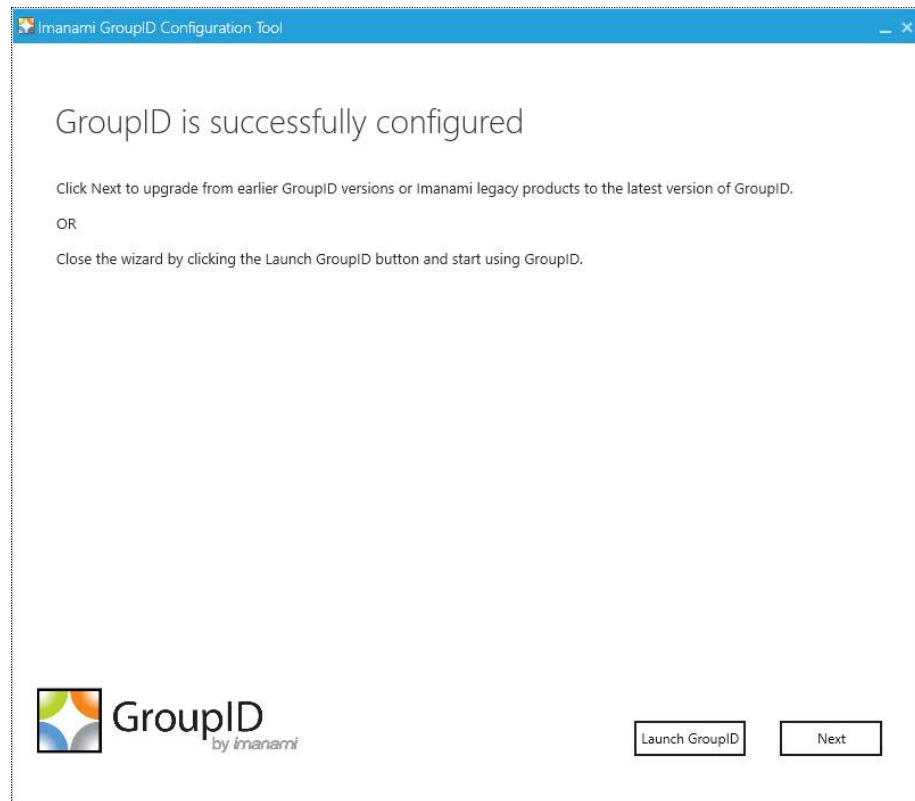


Figure 21: GroupID Successfully Configured page

17. GroupID is configured on your machine. You can choose to upgrade it now or later.

- Click **Next** to launch the [Upgrade wizard](#) and proceed to upgrade GroupID.

OR

- Click **Launch GroupID** to start using GroupID 10 and upgrade it later.

To upgrade GroupID, refer to Chapter 1 - Upgrading to GroupID 10 in Part 4 - GroupID Upgrade.



The Configuration Tool is also installed as a separate program on the machine. You can rerun it to modify GroupID configurations.

How to Configure a GroupID Client

While installing GroupID, you can choose to create a GroupID client that connects to a GroupID server already configured in the environment.

To configure a client, specify either the GroupID server name or the complete URL of GroupID Data Service. This completes the GroupID configuration and connects the new client to the specific server.

To configure a new GroupID client:

1. On the **GroupID Server Configuration** page (Figure 11), select **Connect to an existing GroupID 10 server** to configure a GroupID client.
2. Click **Next**.

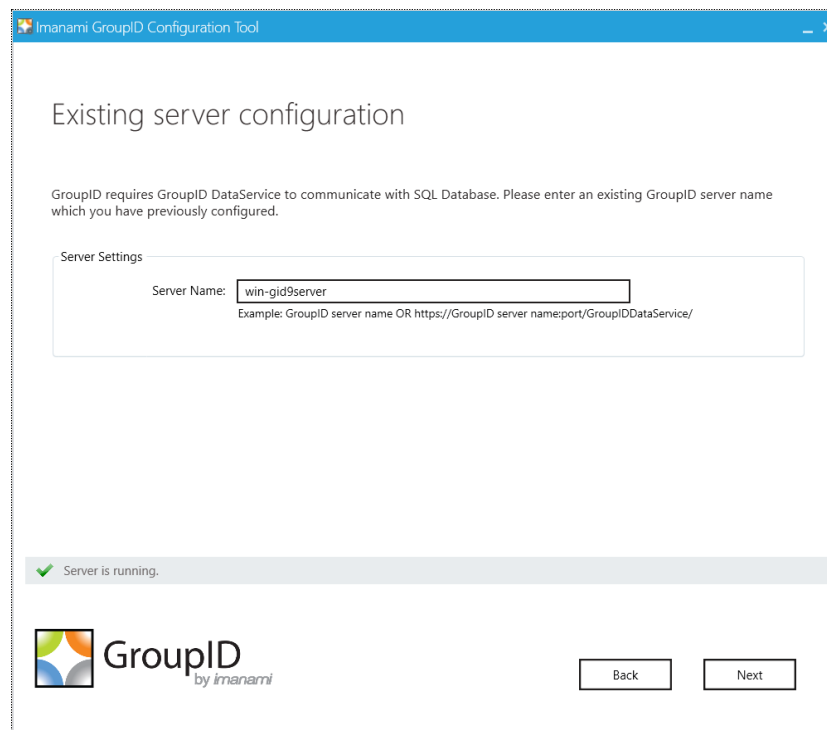


Figure 22: Existing Server Configuration page

3. In the **Server Name** box, either type the name of the server to which you want to connect this client or the complete URL of the Data Service deployed on that server.

The Data Service URL should be in the following format:
`https://<GroupID server>:<port number>/GroupIDDataService/`

where *GroupID server* is the name of the server and *port number* is the port that was used for configuring the Data Service.

4. Click **Next**.
5. The **Service Account Settings** page (Figure 17) is displayed, where you can view and remap service accounts for the GroupID app pool in IIS, scheduled jobs, and Windows services.
6. Click **Configure**.
7. The next page displays the progress while a GroupID client is configured on the machine. This client uses the same SQL Server and database as used by the specified server.

On successful configuration, the **GroupID is successfully configured** page opens (Figure 21).

8. Click **Launch GroupID** to start using GroupID 10 or click **Next** to launch the [Upgrade wizard](#) for upgrading GroupID.

Configure a GroupID server with existing database

While installing GroupID, you can choose to create a GroupID server with load balancing support, where load will be balanced in real time with multiple Data Services, portals and Elasticsearch instances.

To configure this server, you have to specify either the GroupID server name or the complete URL of GroupID Data Service that is already deployed in the environment. The new GroupID server will have its own Data Service, but that service will use the paraphrase and database settings of the specified Data Service to connect to the existing database.

This option also configures the GroupID Elasticsearch Service as a slave node to the master node for the Elasticsearch Service cluster configured on the GroupID server.



You may need to add the SPN of the GroupID server/master node in the context of the user account being used for GroupID client-server / master-slave node connectivity. Visit [Set spn](#) for help on adding the SPN.

The following example shows how you can add an SPN for a server with GroupID Data Service deployed on it.

Server name: msvr02
User: Demo1\administrator

Run the following command in Command Prompt on the server, msvr02 (GroupID server or master node) with FQDN of msvr02:

```
SetSPN -s HTTP/msvr02.demo1.com demo1\administrator
```

To configure a GroupID server with existing database:

1. On the **GroupID Server Configuration** page (Figure 11), select **Configure new GroupID 10 Server with existing database**.
2. Click **Next**.

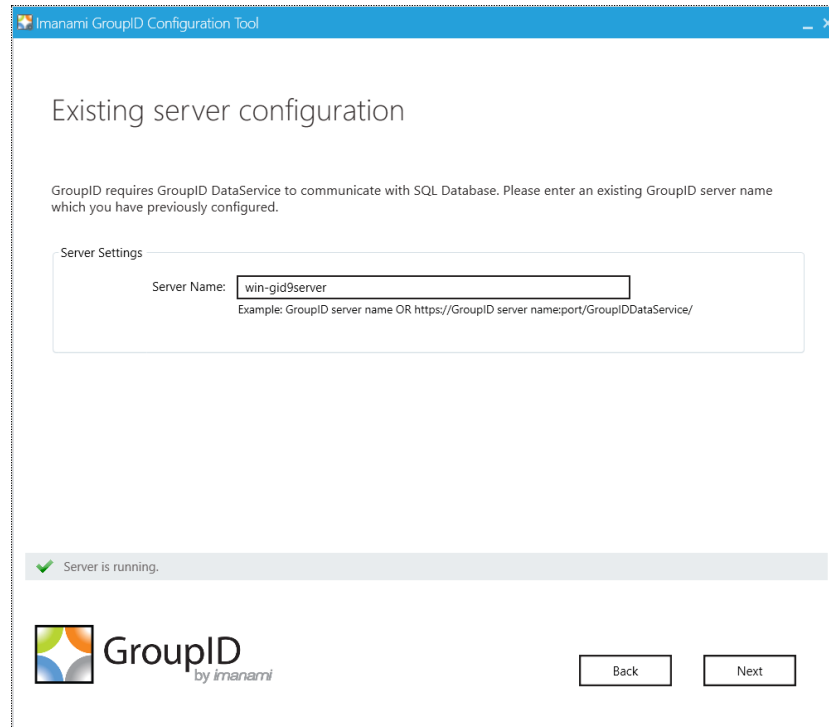


Figure 23: Existing Server Configuration page

3. In the **Server Name** box, either type the name of the GroupID Server or the complete URL of the Data Service deployed on that server.

The Data Service URL should be in the following format:
`https://<GroupID server>:<port number>/GroupIDDataService/`

where *GroupID server* is the name of the server and *port number* is the port that was used for configuring the Data Service.

4. Click **Next**.
5. The **Service Account Settings** page (Figure 17) is displayed, where you can view and remap service accounts for the GroupID app pool in IIS, scheduled jobs, and Windows services.
6. Click **Configure**.

7. The next page displays the progress while a GroupID server is configured on the machine.
On successful configuration, the **GroupID is successfully configured** page opens (Figure 21).
8. Click **Launch GroupID** to start using GroupID 10 or click **Next** to launch the [Upgrade wizard](#) for upgrading GroupID.

Chapter 2 - Modifying GroupID Configurations

When GroupID is installed, the Configuration Tool is also installed as a separate program on the machine. You can rerun it to modify GroupID configurations. Depending on whether the machine is a GroupID server or client, the tool displays different modification options.

On a GroupID server machine

Run the Configuration Tool to:

- Modify the existing server configurations
OR
Connect to a different server (in which case this server converts to a client)
OR
Modify current GroupID server with existing database configurations
- Enter multiple GroupID licenses

On a GroupID client machine

Run the Configuration Tool to:

- Connect this client to a different server
OR
- Configure this machine as a GroupID server (in which case this GroupID client converts to a server)

Launch the Configuration Tool from the Windows Start screen or from GroupID Management Console (Configurations node > Configure GroupID).

The tool opens to the **Introduction** page.

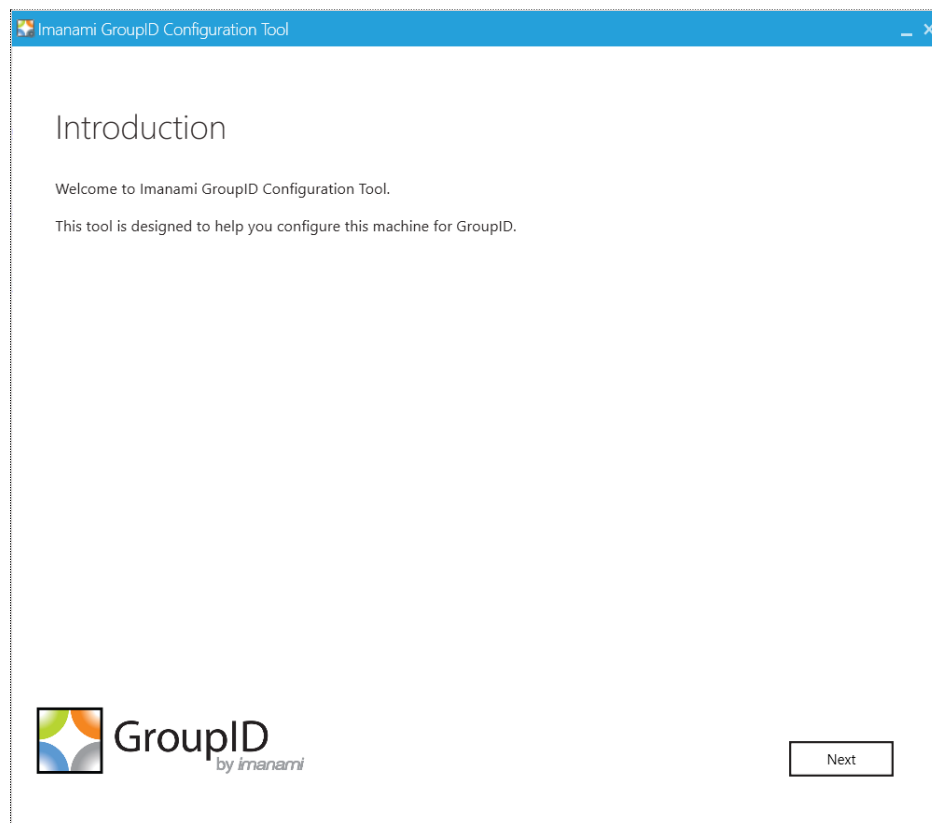


Figure 24: Configuration Tool - Introduction page

Modifying a GroupID Server

Change Server Configurations

You can modify a GroupID server for any of the following reasons:

- Change the GroupID license
- Add another license
- Change the port for GroupIDSite10 (GroupID Data Service and GroupID Security Service are deployed in this website in IIS)
- Change the encryption key used to encrypt GroupID data
- Connect the GroupID server to a different SQL database residing on the same SQL server or on a different server.
- Change the authentication mode to use when connecting GroupID to the SQL Server database.

- Change the service accounts configured for GroupID app pool, scheduled jobs, and Windows services.

To change GroupID license or add another license

You must replace the GroupID license with a new one when the existing license expires.

If you have licensed GroupID by module, you would also have to provide multiple licenses.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.

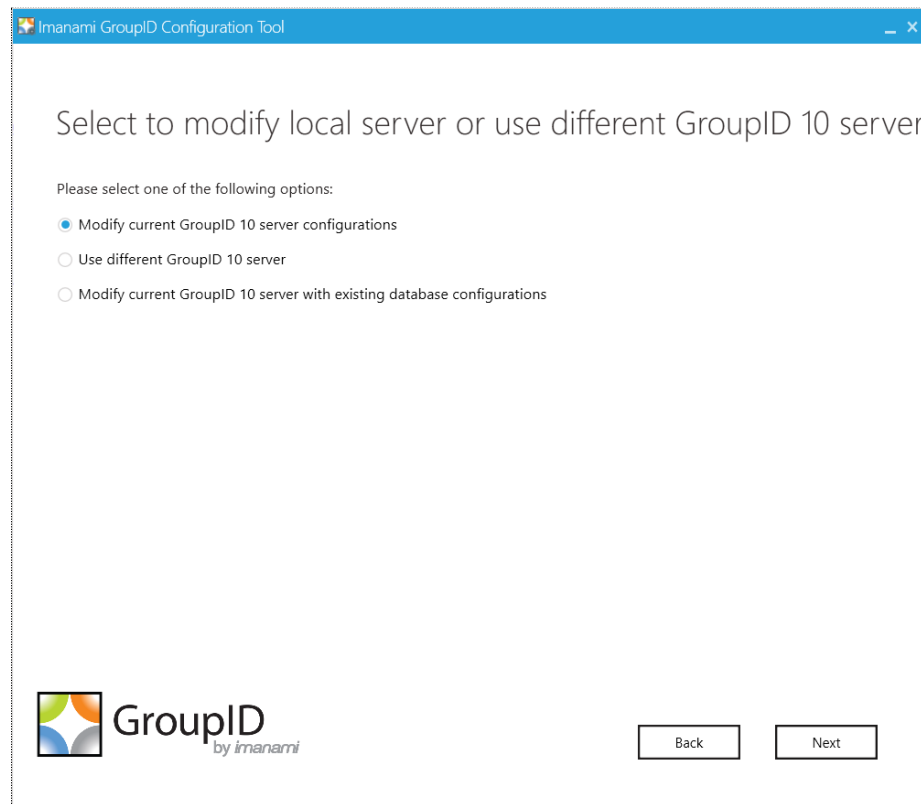


Figure 25: Server options

- The **Modify current GroupID 10 server configurations** option is selected by default. Click **Next**.

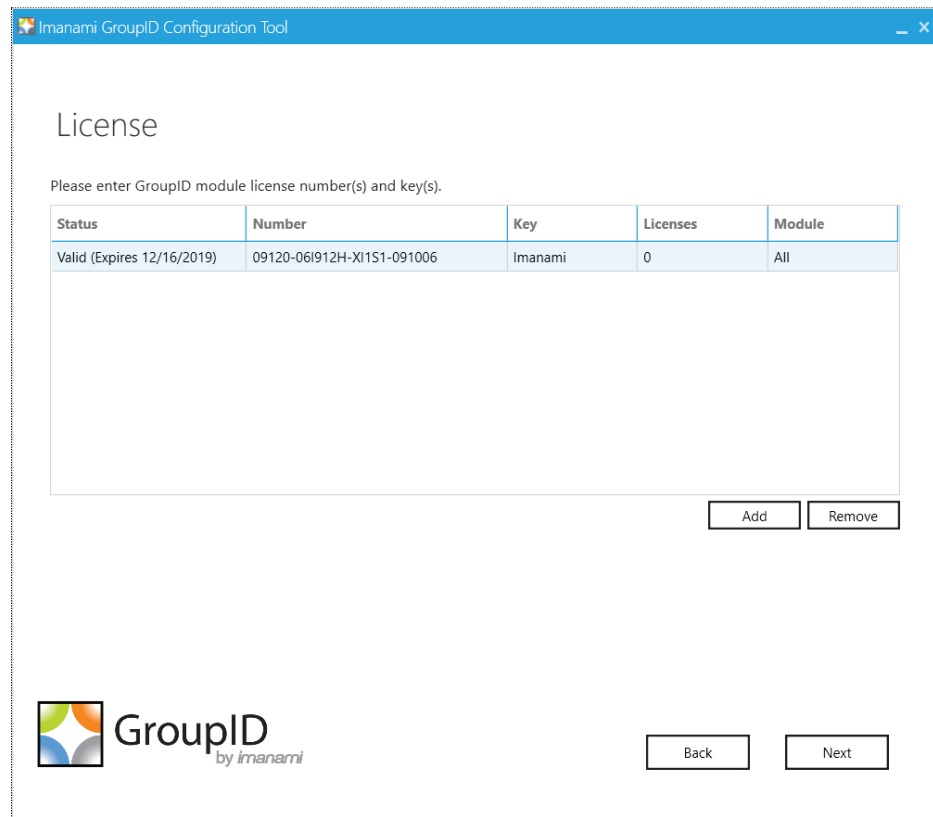


Figure 26: License page

- The GroupID license you provided earlier is displayed on the **License** page. When it expires, you can simply edit it to provide a new license.

Add multiple licenses here if you have licensed GroupID by module.

- **Edit the existing license** – On double-clicking the license row, the **Add/Edit License** dialog box is displayed with the license and key populated in the respective boxes. Edit the license and click **OK**.
 - **Add another license** - Click **Add**; the **Add/Edit License** dialog box is displayed, where you can provide a valid license and key.
 - **Remove a license** - Click **Remove** to remove any existing licenses.
- Click **Next**.

Go through the remaining pages of the tool to complete the process.

To change the port for GroupIDSite10

For GroupID 10, the GroupID Data Service and GroupID Security Service are deployed in the website named GroupIDSite10 in IIS. You can change the binding port for this site.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
2. The **Modify current GroupID 10 server configurations** option is selected by default (Figure 25). Click **Next** until you reach the **Service Configuration** page, which is similar to Figure 13.

Follow the instructions under the figure to change the port.

3. Go through the remaining pages of the tool to complete the process.

To change the encryption key

You can change the encryption key that GroupID Data Service uses to encrypt and decrypt the data that it stores in, and retrieves from, the SQL Server database.

When you change the key, GroupID Data Service will not be able to decrypt any data that was encrypted with the previous key.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
The **Modify current GroupID 10 server configurations** option is selected by default (Figure 25). Click **Next** until you reach the **Security Settings** page, which is similar to Figure 14.

Follow the step under the figure to change the encryption key. A warning is displayed since it isn't recommended that you change it.

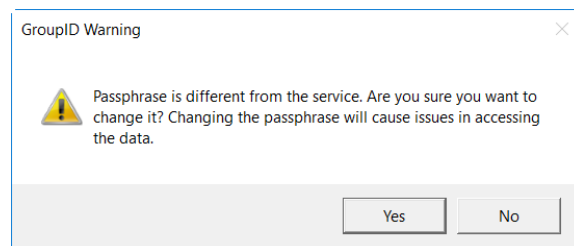


Figure 27: Warning message

2. Click **Yes** to change the encryption key or **No** to cancel the change.
3. Go through the remaining pages of the tool to complete the process.

To change the SQL Server and database

You can change the SQL database you are using with GroupID. You can even select a different SQL Server and then select or create a database on that server. However, data from the previous database would not be available in the database you select or create.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
2. The **Modify current GroupID 10 server configurations** option is selected by default (Figure 25). Click **Next** until you reach the **Database Settings** page, which is similar to Figure 15.

Follow the instructions under the figure to change the GroupID database.

3. Go through the remaining pages of the tool to complete the process.

To change the authentication mode

You can change the authentication mode that GroupID uses to connect to the SQL Server database. Options are, SQL server authentication and Windows authentication.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
2. The **Modify current GroupID 10 server configurations** option is selected by default (Figure 25). Click **Next** until you reach the **Database Settings** page, which is similar to Figure 15.

Use the **Authentication** list to select the authentication mode to use when connecting GroupID to the SQL Server database.

3. Go through the remaining pages of the tool to complete the process.

To change the service accounts

You can change the service accounts configured for the GroupID app pool in IIS, GroupID scheduled jobs, and Windows Services.

Moreover, if the password of a service account has changed, you can provide the new password.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
2. The **Modify current GroupID 10 server configurations** option is selected by default (Figure 25). Click **Next** until you reach the **Service Account Settings** page, which is similar to Figure 17.

Follow the instructions under the figure to change the service account for the GroupID app pool, scheduled jobs, or Windows services. In case the password of a service account has changed, you can also provide the new password.

3. Go through the remaining pages of the tool to complete the process.

Convert the server to a client

You can convert this machine from a GroupID server to a GroupID client. This requires that you already have another GroupID server configured in the environment, so you can connect to that when rendering this server to a client.

On conversion, the client will use the GroupID license, services (Data Service and Security Service), and SQL database configured for the server you connect to.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.
2. Select the **Use different GroupID 10 server** option (Figure 25) and click **Next**.
3. The **Existing Server Configurations** page (Figure 22) is displayed, where you have to specify the server to connect the client to.

Follow the instructions under the figure to connect to a server.

4. Go through the remaining pages of the tool to complete the process.



When you convert a GroupID server to a client, all server-related configurations, though deactivated, remain intact. In case you convert this machine back to a GroupID server, you will find all previous configurations available for reuse.

Modifying a GroupID Client

Connect to a different server

You can connect a GroupID client to a different GroupID server in the environment. This done, the client would be using the GroupID license, services (Data Service and Security Service), and SQL database configured for the server you connect to.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.

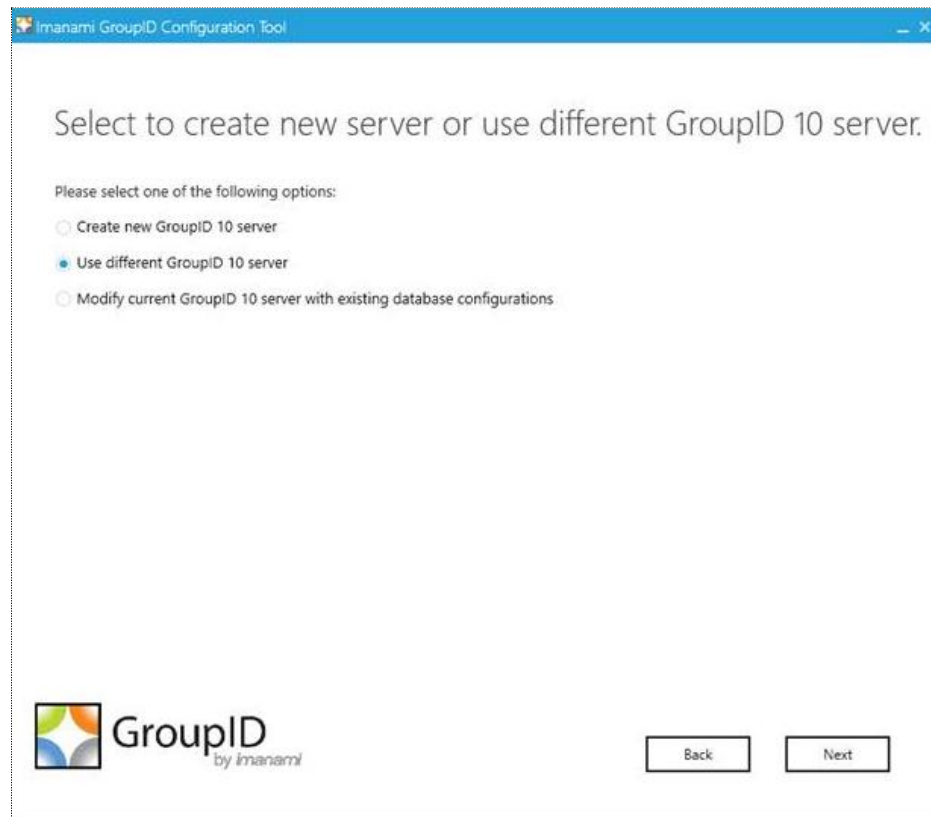


Figure 28: Options on a GroupID client machine

2. The **Use different GroupID 10 server** option is selected by default. Click **Next**.
3. The **Existing Server Configurations** page (Figure 22) is displayed, with the **Server Name** box displaying the name of the GroupID server this client is currently connected to.

Follow the instructions under the figure to connect to a different server.

Convert a client to a server

You can convert a machine from a GroupID client to a GroupID server. Creating a server requires that you provide a GroupID license, connect to Data Service and Security Service, and specify an SQL server and database for the GroupID server to connect to.

1. On the **Introduction** page of the Configuration Tool (Figure 24), click **Next**.

2. Select the **Create new GroupID 10 server** option (Figure 28) and click **Next**.

The remaining process is the same as discussed in the section, How to Configure a GroupID Server. Follow the instructions from step 3 onwards to convert a GroupID client to a server.



When you convert a GroupID client to a server, you must restart Elasticsearch for each node.

Chapter 3 - Uninstalling GroupID

GroupID can be uninstalled at two levels:

- Uninstall the current GroupID version to upgrade to a newer version.
- Uninstall GroupID completely from the machine.



Before you uninstall GroupID, make sure that the logged-in user is a member of the local Administrators group on that machine.

Uninstall GroupID for Upgrade

To uninstall the current GroupID version to upgrade to a newer version, follow the steps below:

1. Double-click the **setup.exe** file available in the GroupID installation package to launch the GroupID Installer.



Figure 29: The GroupID Installer

2. Click **Uninstall GroupID**. This uninstalls the GroupID application files from your computer.

Now proceed to upgrade to a newer version of GroupID. For this,

1. Click the **Install GroupID** link on the GroupID Installer to install the latest version of GroupID.
2. After installation, run the **Upgrade** wizard to make the data created with an earlier GroupID version compatible with the new version.

Complete Uninstall

To uninstall GroupID completely, remove the GroupID folders and registry keys from your machine. This done, you do not have the option to upgrade to a newer version of GroupID.

Click **Uninstall GroupID** on the GroupID Installer (Figure 29) to uninstall the GroupID application files from your computer.

Next, follow the instructions given below to completely uninstall GroupID from your machine.

For complete uninstallation, remove:

- The GroupID installation directory
- Other relevant directories
- GroupID DLLs
- Registry keys
- Services files
- Self-Service and Password Center portal files
- GroupID application pool
- GroupID certificates

Remove the GroupID installation directory

- 1 Go to the location **X:\Program Files\Imanami** (where X represents the GroupID installation drive).
- 2 Delete the directory named **GroupID 10.0**.

Remove other relevant directories

- 1 On the Windows **Run** dialog box, type the following command:
%ALLUSERSPROFILE%\Imanami
- 2 From the location referenced by the given command, delete the folder:
GroupID 10.0.

GroupID DLLs

3. Go to C:\Windows.
4. Search all DLL files having names starting with *Imanami*.

You can find the files by typing *Imanami*.dll* in the Windows Explorer Search box.

5. Delete these files.

Remove registry keys

- 1 Open the **Registry Editor** by typing **regedit** in the Windows **Run** dialog box.
- 2 Delete the following registry keys:
 - HKEY_CURRENT_USER\Software\Imanami\GroupID\Version 10.0
 - HKEY_LOCAL_MACHINE\Software\Imanami\GroupID\Version 10.0

Remove GroupID Services files

Follow these steps to remove GroupID Data Service and GroupID Security Service files:

- 1 Go to the following location:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- 2 Delete these folders:
 - groupiddataservice
 - groupidsecurityservice

Remove portal files

Follow these steps to remove GroupID Self-Service and GroupID Password Center portal files:

- 1 Open the Internet Information Service console by typing *inetmgr* in the Windows **Run** dialog box.
- 2 Under the **GroupIDSite10** node in the console tree, locate the portals that you have created using the Self-Service or Password Center module.
- 3 Delete each portal one-by-one by right-clicking it and clicking **Remove** in the shortcut menu.
- 4 After removing the portals, go to the following location:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- 5 Delete each portal folder one-by-one.



If you have installed Password Center Client on your machine(s) and want to uninstall it too, refer to **GroupID 10 Password Center Client Configuration Guide**.

Remove the GroupID application pool

Follow these steps to remove the GroupID app pool from IIS:

- 1 Open the Internet Information Service console by typing *inetmgr* in the Windows **Run** dialog box.
- 2 Expand the *<machine name>* node in the console tree and click **Applications Pools**.
- 3 On the **Application Pools** page, delete GroupIDAppPool10.

Remove GroupID Certificates

Follow these steps to remove GroupID certificates from IIS:

6. Open the Internet Information Service console by typing inetmgr in the Windows **Run** dialog box.
7. Click the <machine name> node in the console tree. On the **Features View** tab, select **Server Certificates** in the **IIS** section.
8. Delete these certificates bound to GroupIDSite10 (the site deploying GroupID Data Service):
 - GroupIDSecurityService
 - Imanami GroupID Certificate



Do not remove these certificates if another GroupID version is installed on the machine.

Part 4 - GroupID Upgrade

Chapter 1 - Upgrading to GroupID 10

If you are updating to GroupID 10 from an earlier GroupID version, data created with the earlier version must be upgraded to make it compatible with GroupID 10.

GroupID 10 supports upgrade from the following:

- GroupID 9.0
- GroupID 8.0
- GroupID 7.0

Two log files are created on upgrade:

- UpgradeLog, in the GroupID installation package folder.
- ~GroupID10_Upgrade, in a temporary folder for the logged-on user. Access using the %TEMP% environment variable.

Upgrade to GroupID 10

Before you upgrade to GroupID 10, you must know the kind of installation you have chosen for GroupID 10. Refer to Installation Cases for more information.



If you are using the database of an earlier GroupID version with GroupID 10, it is recommended that you take a backup of the database before upgrade. Follow the instructions in Appendix D for backing up and restoring a database.

The upgrade process involves the following:

- Specify the features to upgrade from the previous GroupID version to GroupID 10.
- Create an identity store for the domain running for the previous GroupID version (required when you are upgrading from GroupID 7).
- Specify a source database (required when you are upgrading from GroupID 7):
- For Self-Service and Password Center portals, verify details such as the portal names and the IIS site where they are to exist.

To Upgrade:

1. To launch the Upgrade wizard, click **Next** on the **GroupID Successfully Configured** page (Figure 21) of the Configuration Tool.

OR

In GroupID Management Console, select the **Configuration** node and click the **Upgrade GroupID** link.

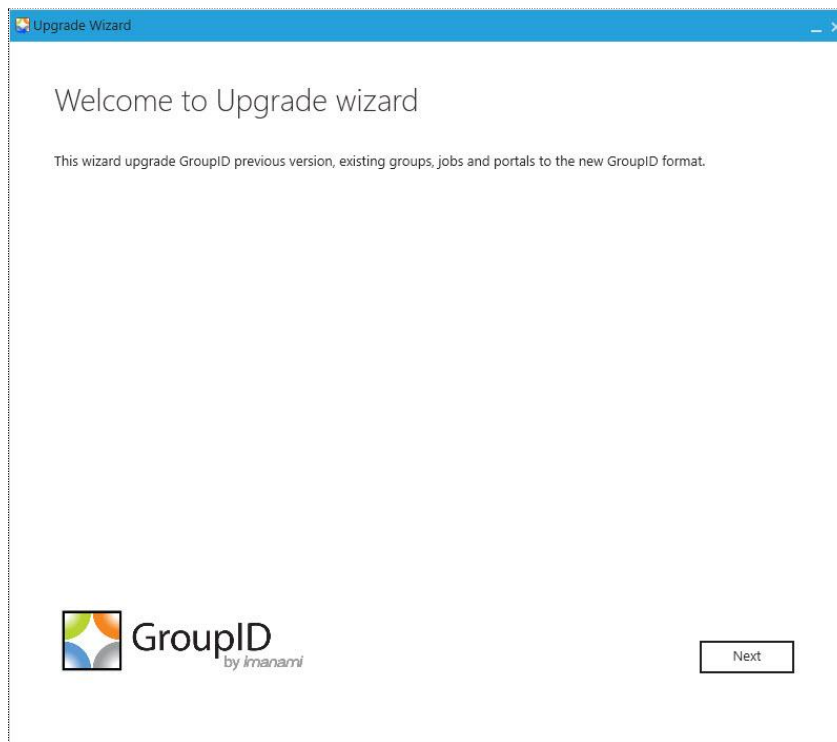


Figure 30: Upgrade wizard - Welcome page

2. Read the welcome message and click **Next**.

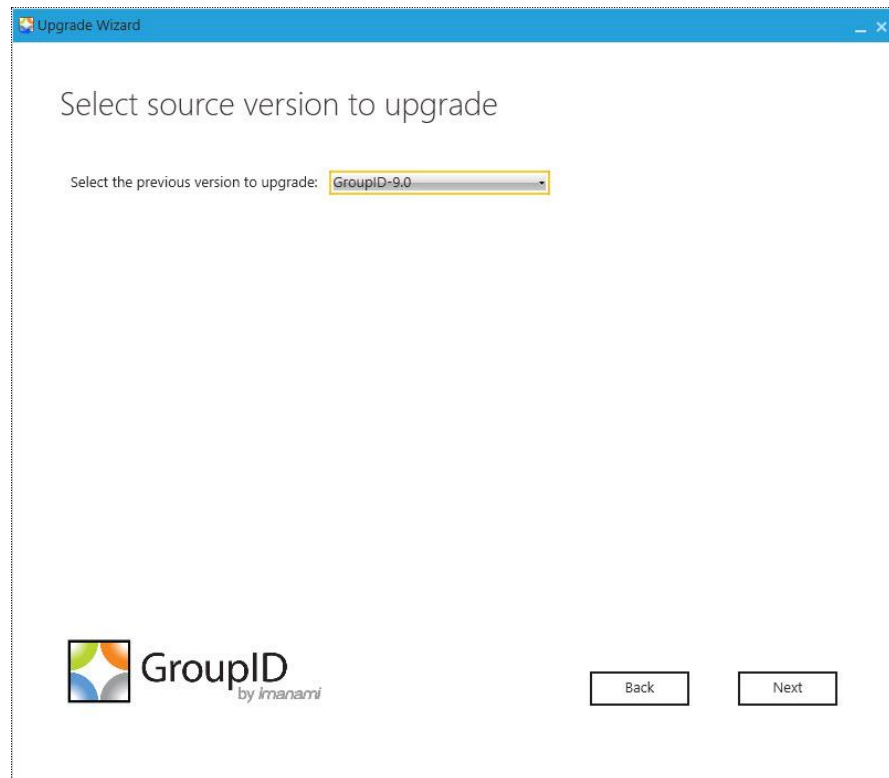


Figure 31: Select Source version/product page



The following steps discuss the upgrade process with GroupID 9.0 as the source version. The process may vary for different source versions.

3. From the **Select the previous version to upgrade** list, select the GroupID version to upgrade from.
4. Click **Next**.

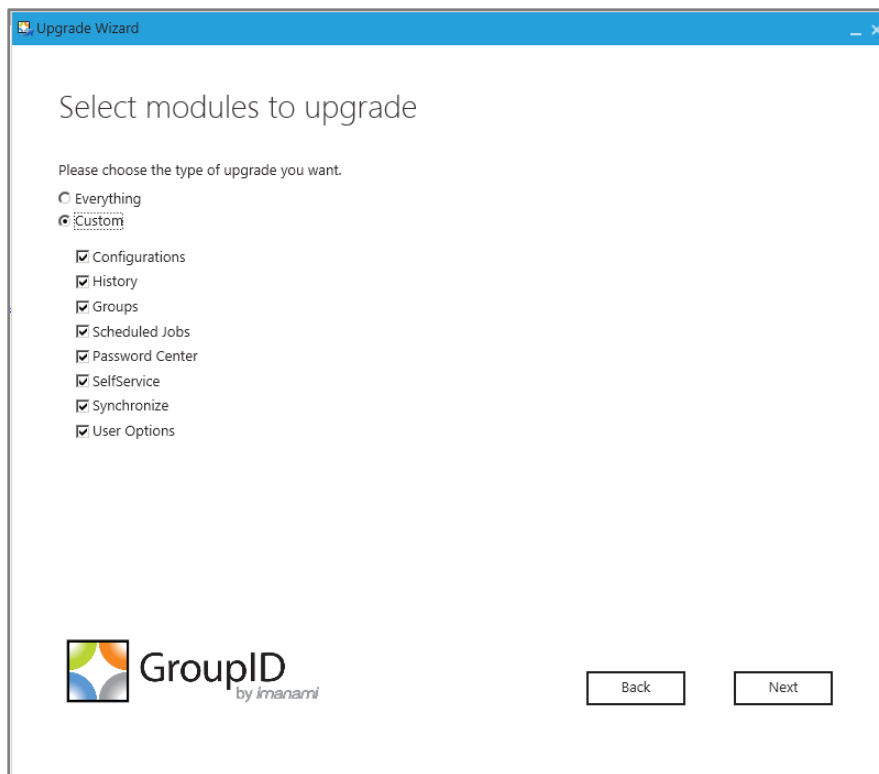


Figure 32: Select modules page

You can choose to upgrade all or selective data of the previous version.

If you have created a new database or a copy of an existing database for GroupID 10, data will be upgraded in the new/copy database. If you are using the database of an earlier GroupID version with GroupID 10, the same database will be upgraded.

On upgrade, the database schema changes, making it compatible with GroupID 10, but incompatible with the previous GroupID version.

On the **Select Modules** page, select the type of GroupID data for upgrade. Options are:

- **Everything** – upgrades all data, which covers all options discussed under **Custom**.
- **Custom** – choose what data you want to upgrade. On selecting it, the following options are listed, from where you can choose the data to upgrade.

Data type	Description
Configurations	This upgrades all GroupID global configurations that are available against the Configuration node in GroupID Management Console.
History	<p>This upgrades all history data in GroupID. It includes the history data of the modules and all data available against the History Summary node in GroupID Management Console.</p> <p>History data examples are:</p> <ul style="list-style-type: none"> • User creation, modification, and deletion logs • Group creation, modification, and deletion logs • Group membership update logs • ExtensionData changes (Group, User, Lifecycle) <p>History data includes all user and group attributes, including password changes.</p>
Groups	<ul style="list-style-type: none"> • This upgrades Active Directory's ExtensionData attribute. • It upgrades membership lifecycle data. • When a security group expires, its membership data is stored in the database. This data is also upgraded. • All scripts for Dynasties and Smart Groups, defined in the Query Designer window in Automate, are also upgraded.
Scheduled Jobs	<ul style="list-style-type: none"> • This upgrades the scheduled jobs defined in the Automate and Self-Service modules. • Scheduled jobs in the Reports and Synchronize modules are upgraded only when GroupID 10 in-place installation is done on the same machine or when GroupID 10 co-exists with GroupID 9 on the same machine.
Password Center	This upgrades all Password Center (user and Helpdesk) portals. However, any customizations made to the source portals are lost in this process.

Data type	Description
Self-Service	This upgrades all Self-Service portals. However, any customizations made to the source portals are lost in this process.
Synchronize	<p>This upgrades all Synchronize jobs. In this process, these jobs are reformatted for management through GroupID 10.</p> <p>History is only upgraded for jobs having Active Directory-only destinations, with an identity store already configured in GroupID 10 for that domain.</p>
User Options	<p>Data upgraded for the above options is server-related data. However, data upgraded for this option is machine-specific (registry based). It relates to what a specific user does, for example,</p> <ul style="list-style-type: none"> • Other than licensing, all information entered for Configuration > Modify User Options in GroupID Management Console. • All data entered in the Recipient Scope dialog box (expand the Automate node, right-click All Groups and select Modify Group Scope). • The number of items to display on a page in Automate, as specified in the Page Size of Items to be Displayed dialog box (on a group listing in Automate, select the Other option in the pagination bar at the bottom). <p>User Options data is only upgraded when GroupID 10 in-place installation is done on the same machine or when GroupID 10 co-exists with GroupID 9 on the same machine.</p>



In case of any conflict in data, data generated by the earlier GroupID version is given priority.

The situation would arise when GroupID 10 co-exists with an earlier GroupID version before you upgrade. Later, when you upgrade, for example, a group that is active in the earlier GroupID version but expired in GroupID 10, would not be expired in GroupID 10 after upgrade. This also applies when you rerun the upgrade process.

5. Click **Next**.

Figure 33: Create Identity Store page



The **Create Identity Store** page is displayed when you are upgrading from GroupID 7. For upgrade from GroupID 8 and 9, the wizard skips this page as it automatically connects to the identity store present in the respective version for upgrade.

For upgrade from GroupID 7, the wizard requires to connect to the Active Directory domain running for GroupID 7. Use the **Create Identity Store** page to create an identity store for this Active Directory domain (say, Demo1.com).

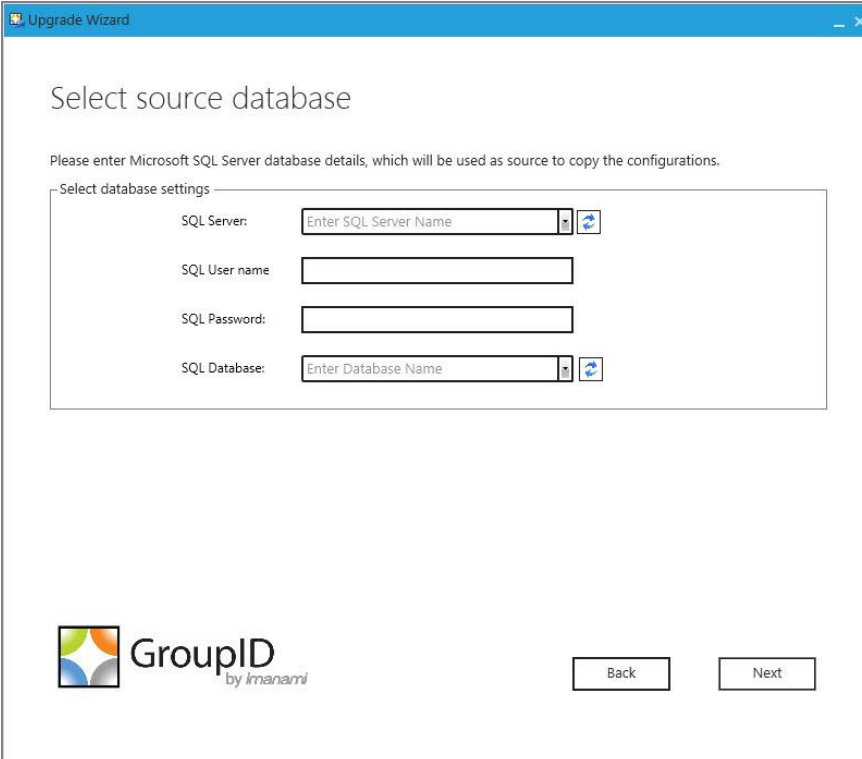
However, this page is not displayed if the Upgrade wizard finds an identity store for Demo1 (as in the following instances), in which case it automatically connects to it for upgrade.

- when you create an identity store for Demo1 in GroupID 10 Management Console before you upgrade from GroupID 7.
- when an identity store for Demo1 exists in the GroupID 7 Password Center module. The wizard upgrades this identity store before upgrading data to it.

See Appendix B for a detailed discussion of the possible scenarios.

When the **Create Identity Store** page (Figure 33) is displayed, provide the domain name and credentials to connect to it. The wizard creates an identity store for this domain to upgrade GroupID 7 data to it. The identity store is also available in GroupID 10 Management Console.

6. In the **Name** and **Domain Name** boxes, enter the fully qualified domain name of the domain running for GroupID 7.
7. Provide a user name and password to connect to the domain in the **User Name** and **Password** boxes respectively.
8. Click **Next**.



The screenshot shows a window titled "Upgrade Wizard" with a blue header. The main content area is titled "Select source database" and contains the following text: "Please enter Microsoft SQL Server database details, which will be used as source to copy the configurations." Below this is a section titled "Select database settings" containing four input fields: "SQL Server:" with a dropdown menu and a refresh icon, "SQL User name:" with a text box, "SQL Password:" with a text box, and "SQL Database:" with a dropdown menu and a refresh icon. At the bottom left is the GroupID logo with the text "GroupID by imanami". At the bottom right are two buttons labeled "Back" and "Next".


Figure 34: Select Source Database page

The **Select Source Database** page is displayed when you are upgrading from GroupID 7.

Specify the GroupID 7 database as the source database. The upgrade process copies data from this database to the GroupID 10 database and then upgrades the GroupID 10 database by reformatting the old tables and adding new ones. Once this database is made compatible with GroupID 10, it cannot be used with GroupID 7.

Data selected for upgrade on the **Select modules to upgrade** page (Figure 32) is fetched from the source database.

9. Provide information of the GroupID 7 database.
 - a. In the **SQL Server** list, select the SQL Server where the source database resides.

If the required server is not displayed in the list, make sure that the **SQL Server Browser service** is running on the SQL Server machine and then click the **Refresh**  button.

- b. Enter the user name and password of the selected SQL Server in the **SQL Username** and **SQL Password** boxes.
 - c. Click the **SQL Database** drop-down list to get a list of all databases that reside on the selected server. Select the source database.



GroupID uses [SQL authentication](#) when connecting to the SQL Server database for upgrade. This sets the upgrade process to work with SQL Server using the SQL Server account you provided on the **Select Source Database** page (Figure 34).

The upgrade process does not support [Windows authentication](#).

10. Click **Next**.
11. The wizard displays a module-wise summary of the data that will be copied/updated, using a separate page for each module.

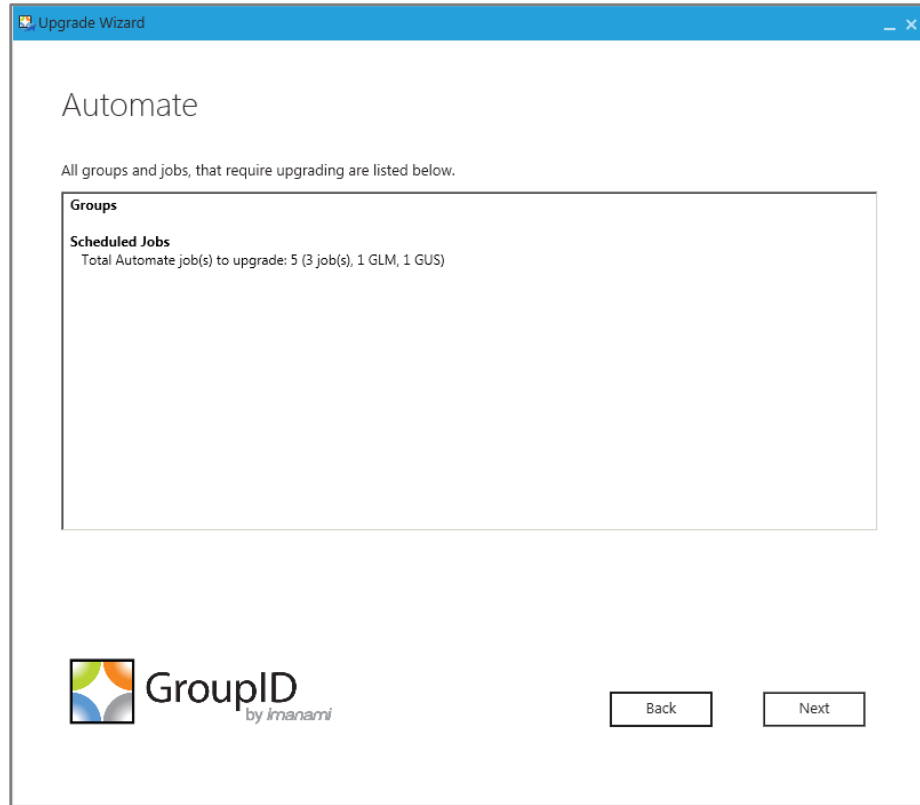


Figure 35: Automate Upgrade Summary page

For Automate, the page displays information about the groups and scheduled jobs to be copied/upgraded.

12. Click **Next**.

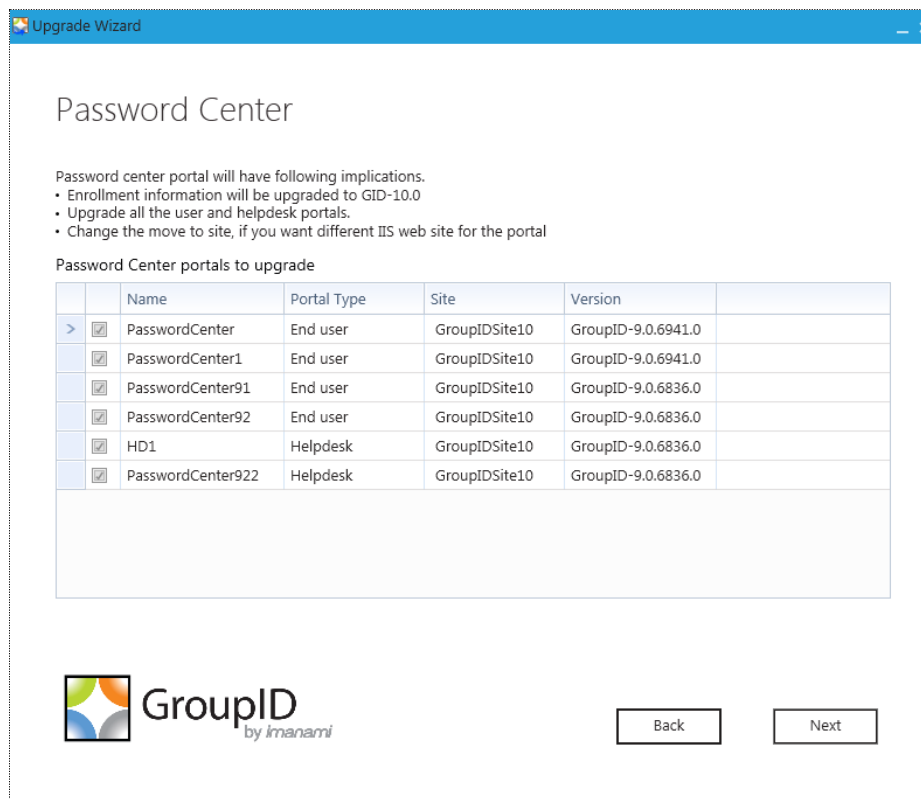


Figure 36: Password Center Upgrade Summary page

For Password Center, the page lists the Password Center portals (user and Helpdesk) to be copied/upgraded.

Consider the following:

- When GroupID 10 is to co-exist with an earlier GroupID version, do not upgrade these very portals, since upgrading them would make them work with GroupID 10 but unavailable for the earlier GroupID version.

Create a copy of the portals and upgrade the copy for GroupID 10.

- For GroupID 10 only, you can choose to upgrade the same portals or create a copy for upgrade.

13. Select the check box for the portals you want to copy/upgrade.

14. To upgrade these very portals, simply click **Next**.

OR

To create a copy of the portals and upgrade the copy, change the portals' names or the IIS site hosting the portals, or both.

- To change a portal's name, double-click the name in the **Name** column and provide a new name. A copy of the portal with the new name will be created in the IIS site appearing in the **Site** column.
- To create a copy of the portal under a different IIS site, select the required site from the **Site** list.

The **Site** list contains all websites defined in IIS. For GroupID 10, you can choose to copy the portals to GroupIDSite10 or any other site of your choice.

15. Click **Next**.

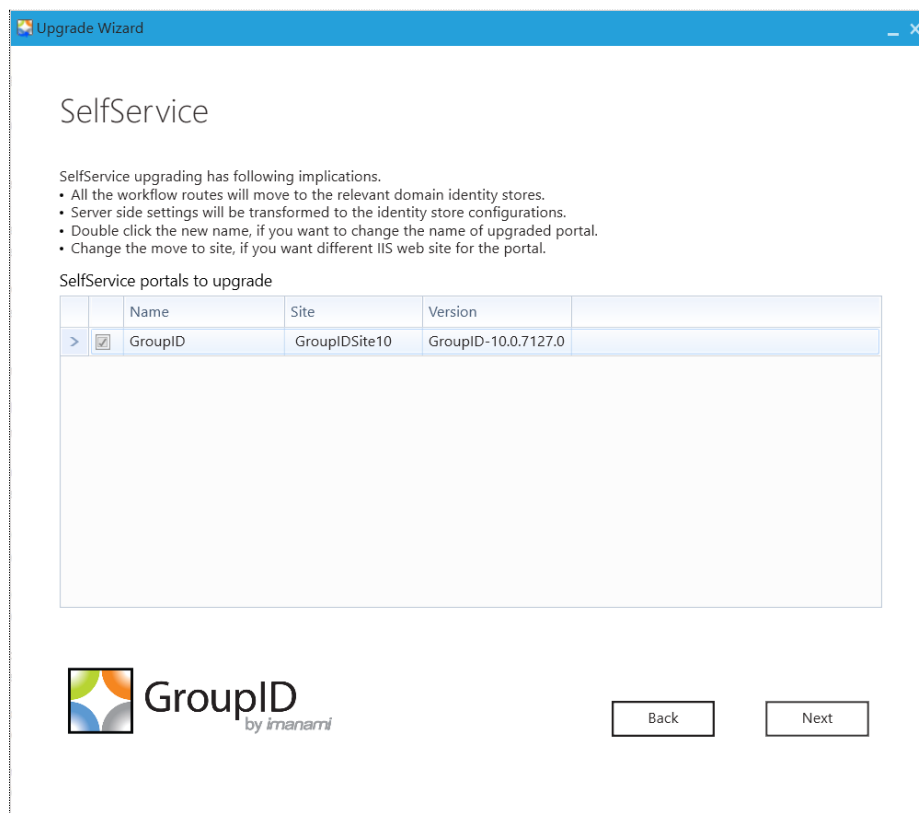


Figure 37: Self-Service Upgrade Summary page

For Self-Service, the page lists the Self-Service portals to be copied/upgraded.

For upgrade from GroupID 7, workflow routes are also upgraded. This involves a merging of all system-defined routes and user-defined routes in GroupID 7 with those in GroupID 10.

However, workflow requests are not merged. You can view requests in individual identity stores.

Before you copy/upgrade the portals, consider the following:

- When GroupID 10 is to co-exist with an earlier GroupID version, do not upgrade these very portals, since upgrading them would make them work with GroupID 10 but unavailable for the earlier GroupID version.

Create a copy of the portals and upgrade the copy for GroupID 10.

- For GroupID 10 only, you can choose to upgrade the same portals or make a copy for upgrade.

16. Follow steps 13 and 14 under Figure 36 to copy/upgrade the portals.

17. Click **Next**.

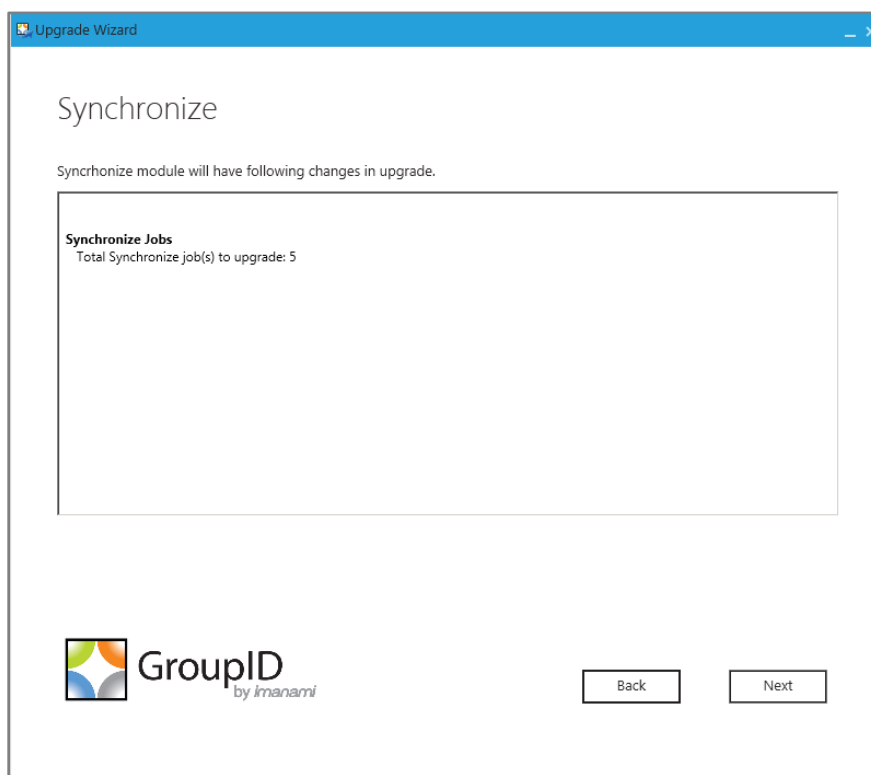


Figure 38: Synchronize Update Summary page

For Synchronize, the page displays information about the Synchronize jobs to be copied/upgraded.

18. Click **Next**.

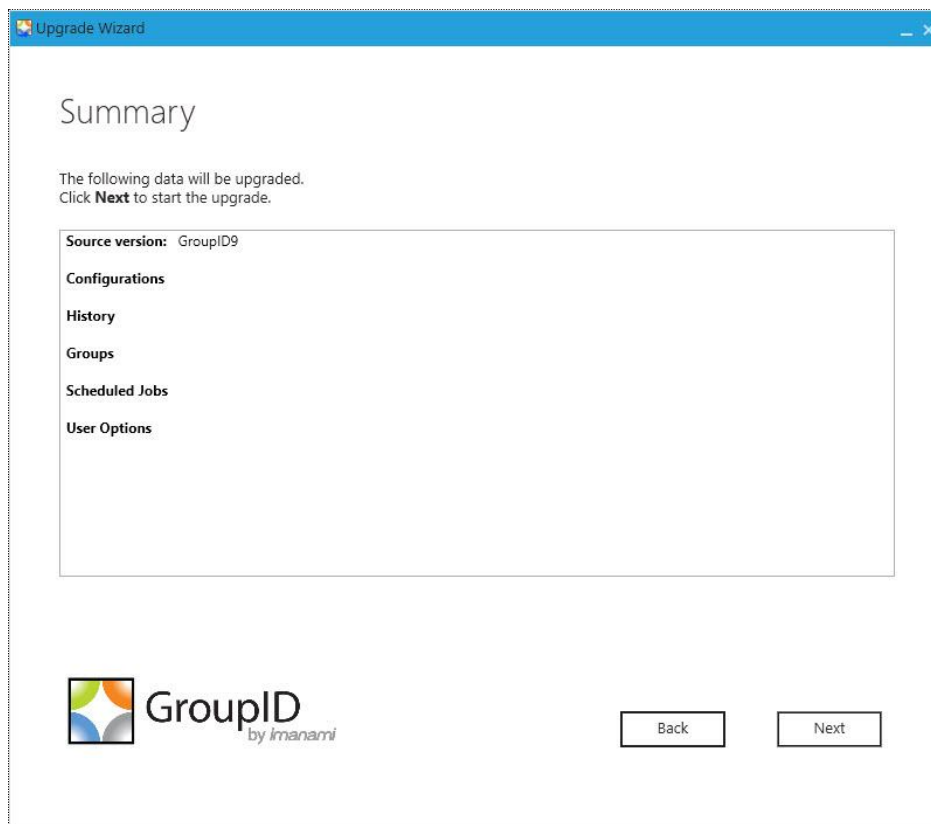


Figure 39: Upgrade Summary page

This page displays a complete summary of the data to be copied/ upgraded for your selected options. These options were selected on the **Select modules to upgrade** page (Figure 32).

19. Review the summary and click **Next**.
20. GroupID is upgraded while the next page displays the upgrade progress.

On successful upgrade, the **Upgrade Completed** page is displayed.

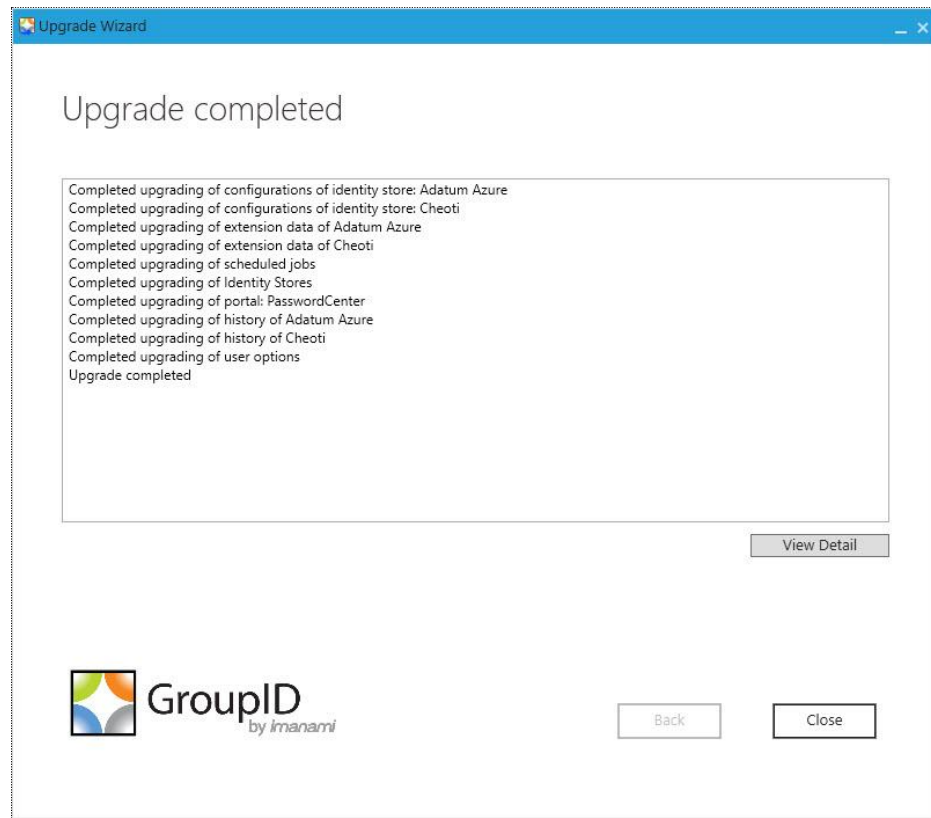


Figure 40: Upgrade Completed page

21. Click **Launch GroupID** to start using GroupID 10 or click **Close** to close the Upgrade wizard.

Part 5 - Appendices

Appendix A

Setting up Authentication modes

While setting up GroupID, you must select an authentication mode for connecting to SQL Server (that hosts the GroupID database). There are two possible modes:

- SQL Server Authentication
- Windows Authentication

SQL Server Authentication

It is recommended that you create a new SQL Server account for GroupID. You must add the account to the *db_creator* server role so that it can create and maintain the GroupID database.

The account must also be part of the *db_owner* database role, so that it can execute DDL (Data Definition Language) and DML (Data Manipulation Language) commands. However, unlike Windows Authentication mode setup, you do not need to add the account to the *db_owner* role because SQL Server *db_creator* is mapped to the *db_owner* database role by default.



For SQL Server 2008, 2012, 2014, 2016, and 2017 families, every SQL Server account is assigned the *public* role. Therefore, the GroupID SQL account belongs to two server roles: *db_creator* and *public*.

To add the GroupID SQL account to the *db_creator* role

1. Launch SQL Server Management Console.
2. Create a new account for GroupID 10, if needed.
3. Connect to the server using your new GroupID SQL account.
4. Right-click the database server node and click **Properties**.
5. On the **Properties** dialog box, select the **Permissions** page.
6. Scroll down on the **Explicit** tab to the **Connect SQL** permission.
7. Select the **Grant** check box.

8. Click the **Effective** tab. You should have the following permissions listed here:
 - Connect SQL
 - Create any database
 - View any database
9. Click **OK**.

Windows Authentication

GroupID works with SQL Server (which hosts the GroupID database) using the Windows Authentication mode in context of the account configured in GroupIDAppPool10 (when SQL Server is available locally or remotely). GroupID detects this account and authenticates with it on SQL Server via Windows authentication.

You can configure a domain account in GroupIDAppPool10 and use it to connect GroupID to SQL Server, provided that it has the following permissions on SQL Server.

- The user account type on SQL Server must be a Windows account with db_owner permissions on the GroupID database.
- For creating a new database, the user account must have the db_creator role and db_owner permissions on the master database.

Use a domain account when SQL Server is available remotely or locally. A local Windows account will work only when GroupID and SQL Server are running on the same machine).

The domain account used to connect GroupID with SQL Server must:

- Be a member of the IIS_IUSR and Backup Operators groups.
- Have read/write permissions on the GroupID 10 installation folder: [GroupID installation drive]:\Program Files\Imanami\GroupID 10.0.

Appendix B

The do's and don'ts of the Upgrade wizard

This appendix provides additional information on the behavior of the Upgrade wizard.

In the following text, the term 'source version' refers to the GroupID version from which you are upgrading to GroupID 10.

1. (Applies to upgrade from GroupID 7 only) When you create an identity store in GroupID 10 Management Console before upgrade, it has the following impact upon upgrade:

The settings configured for the identity store in GroupID 10 are not upgraded when the same settings are configured differently for the same identity store in the source version. Examples of such settings are: advanced settings for Self-Service portals, global configurations, out of bound settings, and user roles for Password Center (User and Helpdesk) portals.

2. User options and scheduled jobs are only upgraded when the GroupID 10 co-exist or in-place installation is done on the machine where the source version was installed.
3. When GroupID 10 co-exists with GroupID 8.1 or 9.0 in the environment, you must copy the whole GroupID 8.1/9.0 installation directory to the GroupID 10 machine (to keep the design files for all portals and the attributes to replicate list for an identity store intact).
4. When GroupID 10 co-exists with an earlier GroupID version in the environment, you have to manually copy the Self-Service portals and Password Center (User and Helpdesk) portals from the source version installation folder to the GroupID 10 installation folder.

For GroupID 9, for example, the portal directories are available at the following locations:

Self-Service

[installation drive]:\Program Files\Imanami\GroupID
9.0\SelfService\inetpub\portal_name\

Password Center user portal

```
[installation drive]:\Program Files\Imanami\GroupID  
9.0\PasswordCenter\Inetpub\User_portal_name\
```

Password Center Helpdesk portal

```
[installation drive]:\Program Files\Imanami\GroupID  
9.0\PasswordCenter\Helpdesk\Inetpub\helpdesk_portal_name\
```

For the Self-Service portals, you also need to manually create the directory structure of GroupID 9 on the GroupID 10 machine. This will enable the Upgrade wizard to read the portals of the previous version.

Create the directory structure at the following path on the GroupID 10 machine::

```
[installation drive]:\Program Files\Imanami
```

It should look like:

```
[installation drive]:\Program Files\Imanami\GroupID  
9.0\SelfService\Inetpub>
```

5. When you copy a Self-Service portal for upgrade from one machine to another, you must change the server name in GroupID 10 Management Console (Self-Service > Portals > [required portal] > Server > IIS tab.) after upgrade. For example:

Previous version portal URL after upgrade: <https://msvr02:4443/GroupID>
Required change: <https://msrv1:4443/GroupID>

Here, 'msvr02' is the previous GroupID version machine and 'msrv1' is the GroupID 10 machine.

6. When GroupID 10 co-exists with an earlier GroupID version in the environment, you have to manually copy Synchronize jobs from the source version installation folder to the GroupID 10 installation folder.

For GroupID 9, for example, Synchronize jobs are available at the following location

```
[installation drive]:\ProgramData\Imanami\GroupID 9.0\Synchronize\Jobs
```

Copy the jobs to the following location in GroupID 10:

```
[installation drive]:\ProgramData\Imanami\GroupID 10.0\Synchronize\Jobs
```

7. For Synchronize, history is only upgraded for jobs having Active Directory-only destinations, with an identity store already configured in GroupID 10 for that domain.

8. The Upgrade wizard does not upgrade the Reports module. You have to manually copy the reports from the source version reports directory to the GroupID 10 reports directory.

Reports directory in GroupID 9:

[installation drive]:\ProgramData\Imanami\GroupID 9.0\Reports

Reports directory in GroupID 10:

[installation drive]:\ProgramData\Imanami\GroupID 10.0\Reports

9. In GroupID 7, GMS and GUS were under global configurations. In GroupID 8 and above, they would be upgraded as scheduled jobs with their respective credentials and scope, and would be available under the Scheduling node.

However, when GroupID 10 is installed (co-exist or in-place) on a different machine than the source version machine, you would have to manually create all scheduled jobs.

10. When GroupID 10 co-exists with an earlier GroupID version in the environment, external database Smart Groups with ODBC connection (for example, Oracle, SQL connection) requires that you create a system DSN with the same name on the GroupID 10 machine first and then update Smart Group queries manually for each Smart Group or via GroupID Management Shell.
11. Health Meter in GroupID 7 was configured locally on the GroupID machine. With GroupID 8 and above, it has been moved to the cloud as SaaS.



GroupID 9.0 and 10 should not co-exist on the same machine.

Multi-domain upgrade

The following scenarios for multi-domain upgrade apply when you upgrade from Group 7.0.

In GroupID 7, a Self-Service portal could be configured with a domain other than the one GroupID Management Console was connected to.

In GroupID 8 and above, such a portal will only work when an identity store for its connected domain exists in GroupID Management Console.

Consider that you are upgrading from GroupID 7 to GroupID 10. The Upgrade wizard encounters the following scenarios with respect to Self-Service portals and resolves them as discussed below:

1. **GroupID 7 connected to a domain (e.g. Adatum.local) and Self-Service portals (e.g. portal1 and portal2) configured with child domains, namely east.adatum.local and south.adatum.local respectively.**

When the Upgrade wizard runs, it displays the Create Identity Store page (Figure 33), where you have to create an identity store for the Adatum.local domain. The Upgrade wizard then upgrades source version data to it.

For Self-Service portals - portal1 and portal2 – the Upgrade wizard automatically creates identity stores for east.adatum.local and so0uth.adatum.local and configures them with the respective portals. GroupID 7 global configurations are upgraded to these identity stores.

2. **GroupID 7 connected to a domain (e.g. Adatum.local) with an identity store existing for this domain in the Password Center module, and Self-Service portals (e.g. portal1 and portal2) configured with child domains, namely east.adatum.local and south.adatum.local respectively.**

When the Upgrade wizard runs, it does not display the Create Identity Store page (Figure 33); rather, it automatically upgrades the identity store for the Adatum.local domain and then upgrades source version data to it.

For Self-Service portals - portal1 and portal2 – the Upgrade wizard automatically creates identity stores for east.adatum.local and south.adatum.local and configures them with the respective portals. GroupID 7 global configurations are upgraded to these identity stores.

3. **GroupID 7 connected to a domain (e.g. Adatum.local) with an identity store existing in the Password Center module for the west.Adatum.local domain, and Self-Service portals (e.g. portal1 and portal2) configured with child domains, namely east.adatum.local and south.adatum.local respectively.**

When the Upgrade wizard runs, it displays the Create Identity Store page (Figure 33), where you have to create an identity store for the Adatum.local domain. The Upgrade wizard then upgrades source version data to it.

The Upgrade wizard will also upgrade the identity store for the west.Adatum.local domain and bind the respective Password Center portals with it.

For Self-Service portals - portal1 and portal2 – the Upgrade wizard automatically creates identity stores for east.adatum.local and south.adatum.local and configures them with the respective portals. GroupID 7 global configurations are upgraded to these identity stores.



For the above scenarios to apply, the service account for the domain the source version is connected to (adatum.local), must have permissions on the whole forest to upgrade groups in all domains (adatum.local, east.adatum.local, south.adatum.local, and west.adatum.local).

Appendix C

Authorizing additional users/groups as GroupID administrators

This topic provides instructions on how other users/groups - in addition to the user account with which the Data Service is configured for the first time and the Domain Admins groups of the domain the user account belongs to - can be designated as GroupID administrators, so that they can change the encryption key and SQL database settings, as well as perform administrative tasks related to GroupID.

The GroupID administrative permissions are controlled through the Authorization Manager (AzMan) console. For detailed information about the AzMan console, visit [Windows Authorization Manager](#).

In AzMan, the authorization policies are defined in the form of authorization stores that are stored in Active Directory or XML files and apply authorization policy at runtime. The authorization policy of GroupID is stored in a separate authorization store. This store comes with two default user roles: GroupID Administrators and GroupID Helpdesk. Users/groups under the GroupID Administrators role have the following permissions:

- Configure database settings on the GroupID Configuration Tool
- Perform administrative tasks for Password Center User portals
- Manipulate Password Center Helpdesk portals
- Perform all other administrative tasks for GroupID

Users/groups under the GroupID Helpdesk role have the following permissions:

- Manipulate Password Center Helpdesk portals

The following steps will guide you through the process of adding users/groups to the GroupID Administrators role:

1. On the GroupID Data Service machine, click Windows **Start** button, click **Run**, and then type: **AzMan.msc**. The Authorization Manager opens without any authorization store added.

2. To open GroupID authorization store, right click **Authorization Manager** and click **Open Authorization Store**.

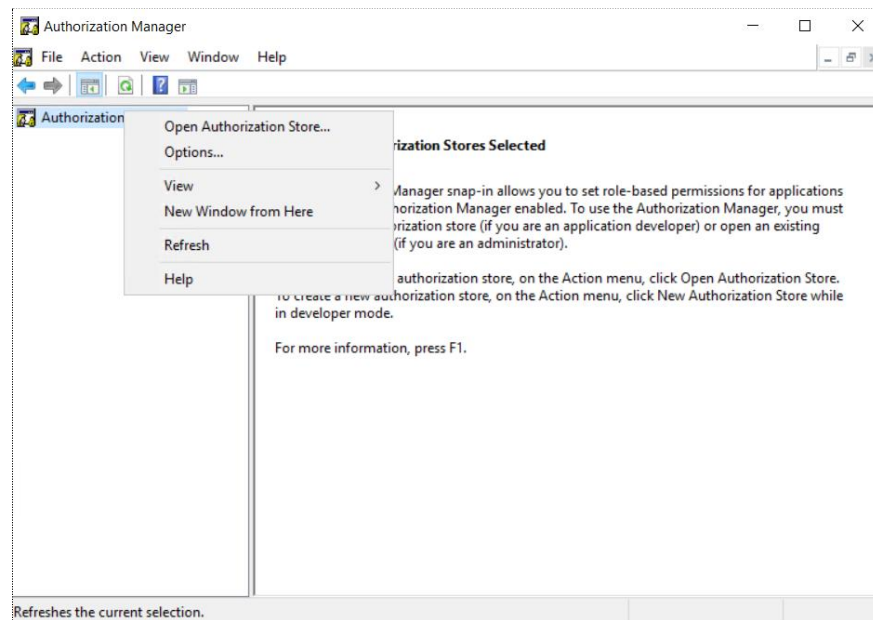


Figure 41: Authorization Manager Console

3. On the **Open Authorization Store** dialog box, make sure that the XML file option is selected for **Select the authorization store type**.

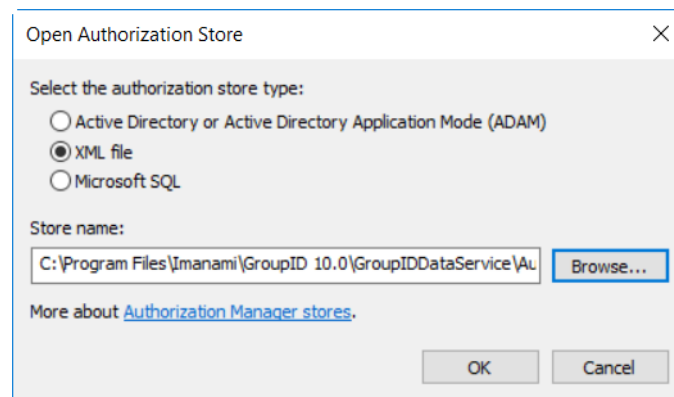


Figure 42: Open Authorization Store dialog box

4. Click **Browse** next to the **Store name** box and browse to the location: X:\Program Files\Imanami\GroupID 10.0\GroupIDDataService\AuthStore; (X represents the GroupID installation drive).

The AuthStore folder is empty by default. In the File Name box, type **GroupIDAuthStore.config** and click **Open**. Click **OK** to close the Open Authorization Store dialog box.

5. *GroupIDAuthStore.config* is displayed below the **Authorization Manager** node in the left pane. Expand the GroupIDAuthApplication node and click **Role Assignments**. Right-click GroupID Administrators in the middle pane, point to **Assign Users and Groups** and click **From Windows and Active Directory**.

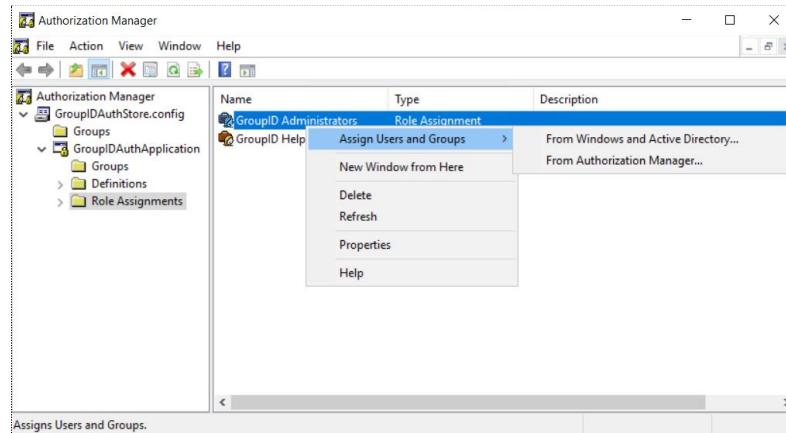


Figure 43: Authorization Manager window

6. On the Select User, Computers or Groups dialog box, type the name of the user or group that you want to assign to the role. Click **Check Names**, and then click **OK**.

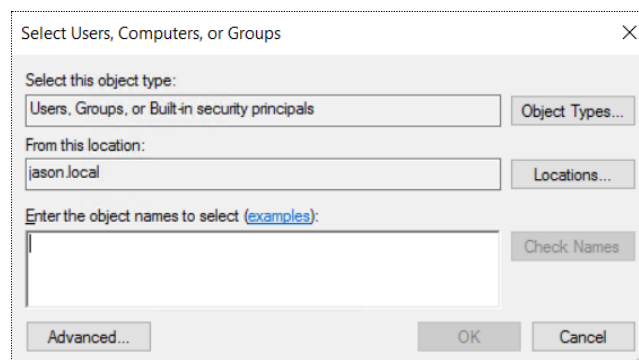


Figure 44: Select Users, Computers, or Groups dialog box

7. Repeat steps 5 and 6 to add more users and groups to the administrator role.

Appendix D

Backing Up and Restoring GroupID Data

This appendix provides instructions for backing up and restoring the data from previous versions of GroupID.

- GroupID database on SQL Server
- Elasticsearch data
- Group Usage Service, and GroupID groups
- GroupID Self-Service Portals
- GroupID Password Center Portals
- GroupID Synchronize Jobs
- GroupID Reports

GroupID database on SQL Server

Take a backup of the GroupID database that you will use to upgrade to GroupID 10.

Follow Microsoft standards to back up this SQL Server database.

Whenever this database is restored, any changes you made using GroupID 10 would be lost.

Elasticsearch data

Before you upgrade from GroupID 9 to 10, take a backup of the Elasticsearch data folder. The default folder location is:

C:/ProgramData/Imanami/GroupID 10.0/Replication/data/

Group Usage Service, and GroupID groups

Back Up

Use the following unsupported script as a guide for creating a backup for:

- Groups created using GroupID 7.0
- Distribution groups for which last-used information is stamped by Group Usage Service

From the domain controller, execute the following command:

```
ldifde -f c:\groupinfobeforeGroupID.ldf -r
"(&(objectClass=group)(objectCategory=group)(|(extensionData=*)(extensionAttribute15=*)(extensionAttribute14=*)(extensionAttribute13=*)(extensionAttribute12=*)))" -p Subtree -l
extensionData,extensionAttribute15,extensionAttribute14,extensionAttribute13,extensionAttribute12
```

This command creates a file named **groupinfobeforeGroupID.ldf** on the **C** drive of the domain controller. To create the file with a different name or at a different location, replace the pathname in the first line with your desired name.

Restore

To restore group data, open the file you created in the preceding steps in a text editor and modify it as follows:

- 1 Replace **changetype: add** with **changetype: modify**.
- 2 Add **replace: extensiondata** before the first **extensiondata** line for each record.
- 3 At the end of each object record, type a hyphen (-) followed by a blank line. For example:

```
dn: CN=sSDL,OU=test,DC=w2k8-64,DC=com
changetype: modify
replace: extensiondata
extensionData::
U0Q0PTE7MTslQU5ZU0VSVkVSJTtEQz13Mms4LTY0LERDPWNvbTs3Oz
syOyo7Kjs7Ozs7OzsKCgoKCg
o2MzM1OTMwOTgwNzMzODgzMzg7UUFYUDQ1OzE=
-

dn: CN=ssd,OU=test,DC=w2k8-64,DC=com
changetype: modify
replace: extensiondata
extensionData:: U0Q0PTE7MTslQU5ZU0VSVkVSJTtHQz1kYy53M
```

```
ms4LTY0LmNvbTs3OzsyOyo7Kjs7Ozs7OzsKCgoKCg  
o2MzM1OTMyMjQ1MDE3NjAxOTk7UUFYUDQ1OzE=  
-
```

- 4 Type and run the following command from the domain controller:

```
ldifde -i -f c:\groupinfobeforeGroupID.ldf
```

GroupID Self-Service Portals

Back Up

Follow these steps to back up the Self-Service portals created using GroupID 7.0, 8.0/8.1, and 9.0:

- 1 Go to the Inetpub folder of the product for which you want to take a backup.
 - **GroupID 7** – X:\Program Files\Imanami\GroupID\SelfService\Inetpub
 - **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\SelfService\Inetpub
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\SelfService\Inetpub
- 2 Copy the folders for each virtual server or portal.
- 3 Create a new folder (ideally on a different drive) and paste the copied data into that folder.

Restore

Follow these steps to restore GroupID Self-Service portals:

- 1 Copy the folders containing the portals from the backup folder you created in the previous steps.
- 2 Go to the Inetpub\ folder of the product's installation directory:
 - **GroupID 7** – X:\Program Files\Imanami\GroupID\SelfService\Inetpub
 - **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\SelfService\Inetpub
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\SelfService\Inetpub
- 3 Paste the copied data in the location, replacing any existing files.

GroupID Password Center Portals

Back Up

Follow these steps to back up Password Center User and Helpdesk portals created using GroupID 7.0, 8.0/8.1, and 9.0:

- 1 Go to the PasswordCenter\ folder of the product's installation directory:
 - **GroupID 7** – X:\Program Files\Imanami\GroupID\PasswordCenter\Inetpub
X is the drive that GroupID is installed on.
 - **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\PasswordCenter\Inetpub
(for Password Center User portals)
 - **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\PasswordCenter\Helpdesk
(for Password Center Helpdesk portals)
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\PasswordCenter\Inetpub
(for Password Center User portals)
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\PasswordCenter\Helpdesk\Inetpub
(for Password Center Helpdesk portals)
- 2 Copy the folders of each portal.
- 3 Create a new folder (on a different drive) and paste the copied data into that folder.

Restore

Follow these steps to restore Password Center portals to GroupID:

- 1 Copy the folders containing the Password Center portals from the backup folder you created in the previous steps.
- 2 Go to the PasswordCenter\ folder of the product's installation directory:
 - **GroupID 7** – X:\Program Files\Imanami\GroupID\PasswordCenter\Inetpub
X is the drive that GroupID is installed on.

- **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\PasswordCenter\Inetpub
(for Password Center User portals)
 - **GroupID 8** – X:\Program Files\Imanami\GroupID 8.0\PasswordCenter\Helpdesk
(for Password Center Helpdesk portals)
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\PasswordCenter\Inetpub
(for Password Center User portals)
 - **GroupID 9** – X:\Program Files\Imanami\GroupID 9.0\PasswordCenter\Helpdesk\Inetpub
(for Password Center Helpdesk portals)
- 3 Paste the copied data into the location, replacing any existing files.

GroupID Synchronize Jobs

Back Up

Follow these steps to create a backup of jobs created with GroupID 7.0, 8.0/8.1, and 9.0 Synchronize:

- 1 On the Windows **Run** dialog box, type one of the following paths and run the command:
 - **GroupID 7** – %ALLUSERSPROFILE%\Imanami\GroupID\Synchronize
 - **GroupID 8** – %ALLUSERSPROFILE%\Imanami\GroupID 8.0\Synchronize
 - **GroupID 9** – %ALLUSERSPROFILE%\Imanami\GroupID 9.0\Synchronize
- 2 Copy the **Jobs** folder.
- 3 Create a new folder (ideally on a different drive) and paste the **Jobs** folder into it.



If some scheduled tasks are defined for Synchronize jobs, you do not need to create their backup. On restoring, the scheduled tasks remain functional for Synchronize jobs.

Restore

Follow these steps to restore jobs from GroupID 7.0, 8.0/8.1, and 9.0:

- 1 Copy the **Jobs** folder from the backup folder you created in the preceding steps.
- 2 On the Windows **Run** dialog box, type one of the following paths and run the command:
 - **GroupID 7** – %ALLUSERSPROFILE%\Imanami\GroupID\Synchronize
 - **GroupID 8** – %ALLUSERSPROFILE%\Imanami\GroupID 8.0\Synchronize
 - **GroupID 9** – %ALLUSERSPROFILE%\Imanami\GroupID 9.0\Synchronize
- 3 Paste the **Jobs** folder into the location, replacing any existing files.

GroupID Reports

Back Up

Follow these steps to create a backup of GroupID 7.0, 8.0/8.1, and 9.0 Reports:

- 1 Browse to the location where the reports generated by these products are saved. The default locations are:
 - **GroupID 7** – X:\ProgramData\Imanami\GroupID\Reports
X is the drive that GroupID is installed on.
 - **GroupID 8** – X:\ProgramData\Imanami\GroupID 8.0\Reports
 - **GroupID 9** – X:\ProgramData\Imanami\GroupID 9.0\Reports
- 2 Copy all data at the location.
- 3 Create a new folder (ideally on a different drive) and paste the copied data into that folder.



You do not need to create a backup of scheduled tasks that include report criteria. On restoring, the scheduled tasks remain functional for these reports.

Restore

Follow these steps to restore GroupID 7.0, 8.0/8.1, and 9.0 Reports:

- 1 Copy the data from the backup folder you created in the previous steps.
- 2 On the Windows **Run** dialog box, type the path of the location where the reports are saved and run the command:
 - **GroupID 7** – X:\ProgramData\Imanami\GroupID\Reports
X is the drive that GroupID is installed on.
 - **GroupID 8** – X:\ProgramData\Imanami\GroupID 8.0\Reports
 - **GroupID 9** – X:\ProgramData\Imanami\GroupID 9.0\Reports

Paste the copied data in the location, replacing any existing file.



GroupID

by *imanami* | NOW PART OF **netwrix**

Imanami | Now part of Netwrix

6160 Warren Parkway, Suite 100,
Frisco, TX 75034,
United States.

<https://www.imanami.com/>

Support: (925) 371-3000, Opt. 3
support@imanami.com

Sales: (925) 371-3000, Opt. 1
sales@imanami.com

Toll-Free: (800) 684-8515

Phone: (925) 371-3000

Fax: (925) 371-3001