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**

User Guide
Password Center

GroupID
by *imanami* | NOW PART OF netwrix

Contents

Chapter 1 – Introduction to Password Center

Using GroupID Password Center, you can reduce your administrative workload by setting up two types of portals:

- User portal

  Create a web-based Password Center user portal and link it to one or more identity stores. Users of these identity stores can use the portal to perform account unlock, password change and password reset operations for their identity store accounts.

- Helpdesk portal

  Create a Password Center Helpdesk portal where Helpdesk users can perform account unlock and password reset operations on behalf of end users of the connected identity store. Like a user portal, a Helpdesk portal can also serve multiple identity stores.

  The Dashboard, History, and Live Updates features of the portal enable Helpdesk users to audit and analyze the functions performed by end users on the user portal.

Password Center portals can also send notification emails to designated recipients when a user makes any change to an object in the directory.

Localization

A Password Center portal (user and Helpdesk) detects the language settings of the web browser that is accessing it and attempts to serve the portal's content in the same language.

Supported languages are:

- Danish

- Dutch

- English

- Finnish

- French

- German

- Icelandic

- Italian

- Portuguese

- Spanish

- Swedish

- Turkish

However, if the portal does not support the browser's language set or if it cannot detect them, it loads the portal with the default language that is English.

Role-based security

To manage access in GroupID, security roles are defined for an identity store. Each role is granted a set of permissions that enable role members to access specific GroupID functions.

Priority value

Each security role is assigned a priority value in the 1-99 range, where 1 is the highest and 99 is the lowest value. Role priority is unique for each role in an identity store, and determines which role is higher than the other.

Chapter 2 – Creating Password Center Portals

Using Password Center you can create the following portals;

- **User portal** for end users to access account unlock and password change services.

- **Helpdesk portal** to facilitate Helpdesk role members to perform account unlocks and password-reset operations on behalf of end users.

Portals are linked to one or more identity stores, which you can add or remove as needed in the course of portal maintenance.

GroupID does not support account unlock in an Azure-based identity store.

If the portal you are going to create has settings similar to an existing helpdesk or user portal, you can copy that portal to create a new one, instead of entering all settings from scratch.

Prerequisites for a portal

The following must be defined in GroupID before a Password Center user or Helpdesk portal can be created:

- An identity store
  A portal cannot be created unless an identity store is defined in GroupID. An identity store must be associated with a portal to enable users to carry the account unlock, password change and reset services of the portal for that identity store.

- An SMS Gateway account
  An SMS gateway is required to be created and associated with the required identity store for Password Center user portals to use it for SMS authentication and Password Center Helpdesk portals to use it for sending new passwords and password reset links to the users' mobile numbers.

- An SMTP server and a messaging system
  These must be configured for each identity store you want to associate with your portal, so that notification emails can be sent using the portal.

- Role-based permissions
Grant Password Center permissions to end users and Helpdesk users of each identity store to empower them to perform different functions (such as account unlock and password reset), using the portal.

- Workflow (optional)
If **Workflow to reset password** is enabled for the identity store, then a password reset operation must be approved before the password is actually reset.

Role policies

Additionally, the following policies, defined separately for each role in an identity store, also impact the portal:

Authentication policy

The authentication policy consists of two parts:

- If the GroupID administrator enables second factor authentication for a user role in an identity store, then members of that role must authenticate their identity store accounts against a second factor authentication type while logging into the portal.

- Role members must authenticate their identity store accounts while resetting their accounts passwords or unlocking their identity store accounts against the authentication type(s) they enrolled their account with.

Password policy

Password policy is role-specific and applies to Password Center user portals. The policy:

- Specifies settings relevant to user authentication on the Password Center user portal.

- Specifies password validation checks for passwords that role members create for their identity store accounts.

Helpdesk policy

The Helpdesk policy is specific to the Helpdesk role in an identity store and applies to the Password Center Helpdesk portal.

Create a user or Helpdesk portal

You can create a portal using the portal creation wizard or by copying an existing portal.

Create a portal using the wizard

1. In GroupID Management Console, expand the **Password Center** node.

2. Right-click **User Portals** or **Helpdesk Portals** and select **Create**.

3. The **New Password Center User Portal** or **New Password Center Helpdesk Portal** wizard opens to the **Introduction** page.
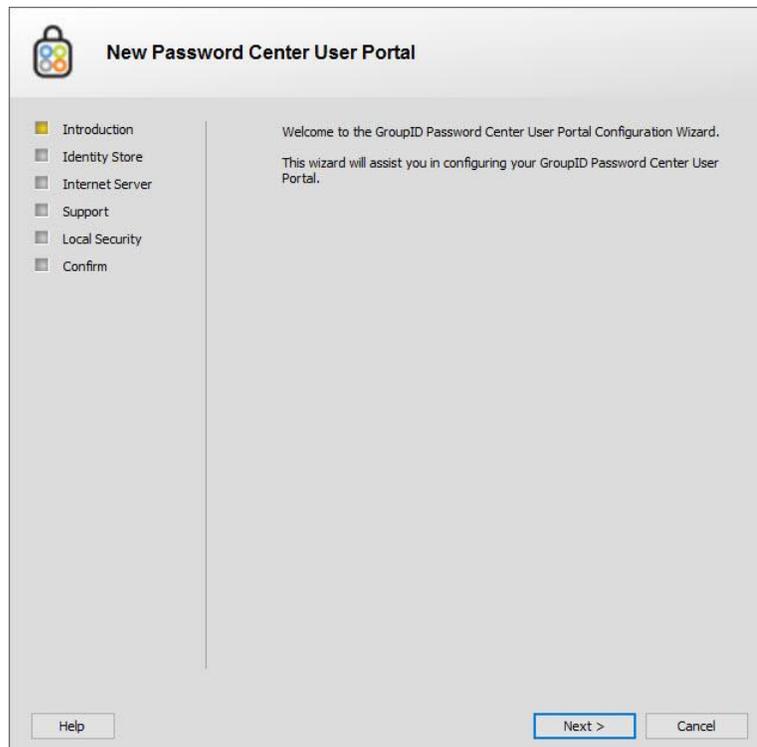
Figure 1: Introduction page

4. Read the welcome message and click **Next**.
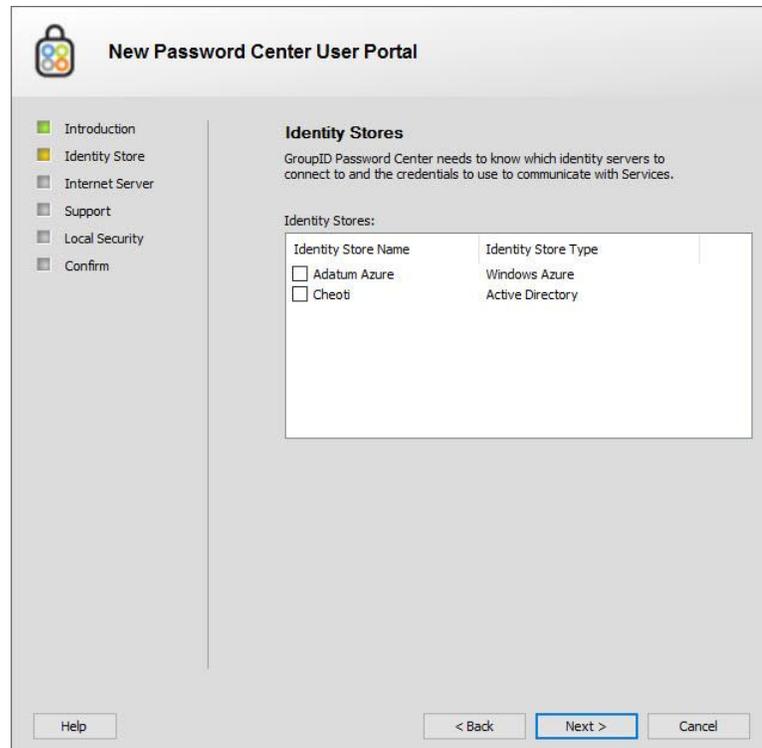
Figure 2: Identity Stores page

5. On the **Identity Stores** page, select the check box for an identity store to associate it the Password Center user or Helpdesk portal. Users of this identity store can log into the portal to perform Password Center user or Helpdesk operations.

   You can select associate multiple identity stores with a portal.

   This page displays a list of all identity stores defined in GroupID.

6. Click **Next**.
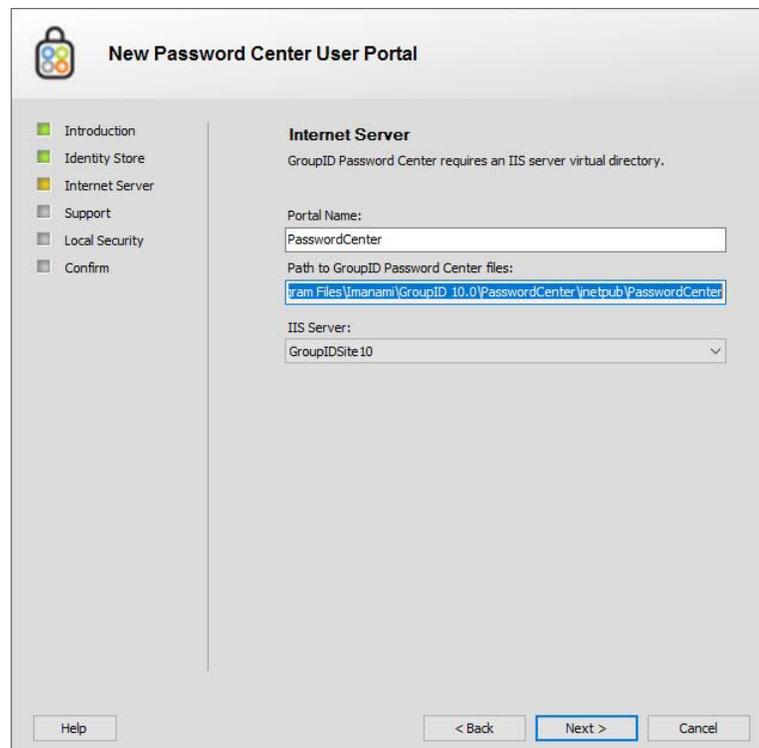
Figure 3: Internet Server page

7. In the **Portal Name** box, modify the name of the portal (if desired).

8. The Password Center portals run within a virtual directory on Internet Information Server (IIS). On the **Internet Server** page, you can view the location where portal files are physically located on disk, and specify settings for the IIS virtual directory that will host the portal.

   When you create the portal, Group ID creates a directory after the portal's name at the given path and copies the portal files from its template directory to the file system path. It also creates a virtual directory on the selected IIS website.

   a. The **Path to GroupID Password Center files** field displays the path to the directory where the portal files are located on disk. The path is read-only.

   a. In the **IIS Server** drop-down list, select the website to host the portal files.

      The list displays the websites defined on the local IIS server. **GroupIDSite9** is the default selection.

9. Click **Next**.

Figure 4: Support page

10. On the **Support Information** page, enter internal contact information and resource links for the portal's users to obtain help using the portal.

    A Password Center portal includes two links, **Feedback** and **Help** ⓧ, on its web interface. The **Feedback** link launches an email application to send an email to the administrator or Helpdesk for inquiries or feedback. The **Help** ⓧ link launches the online help for the portal in a new browser window. Both links are customizable and their target email address or web address is specified on the **Support Information** page.

    a. In the **Support group/administrator's e-mail address** box, type the e-mail address of the group, user or contact to whom the users' queries will be directed.

        This email address is mapped to the **Feedback** link in the portal

    b. In the **Help URL** box, specify the address of your company's internal support website or the portal's help page, where portal users can find support material or report their problems. By default, this box displays the URL of the portal's help page.

        This URL is mapped to the **Help** link in the portal.

11. Click **Next**.
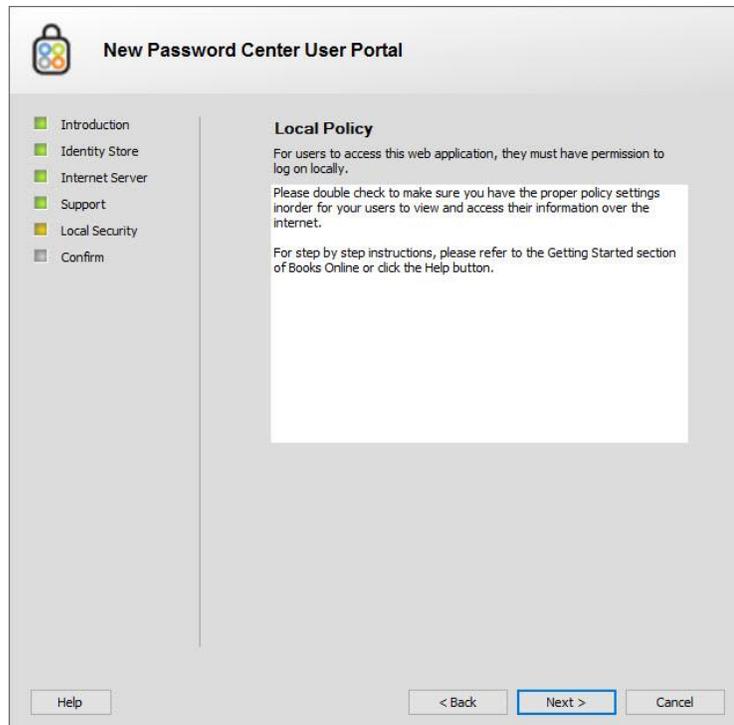
Figure 5: Local Policy page

12. The **Local Security** page displays information about the permissions that users must have to log on to the portal.
Review the information displayed and then click **Next**.
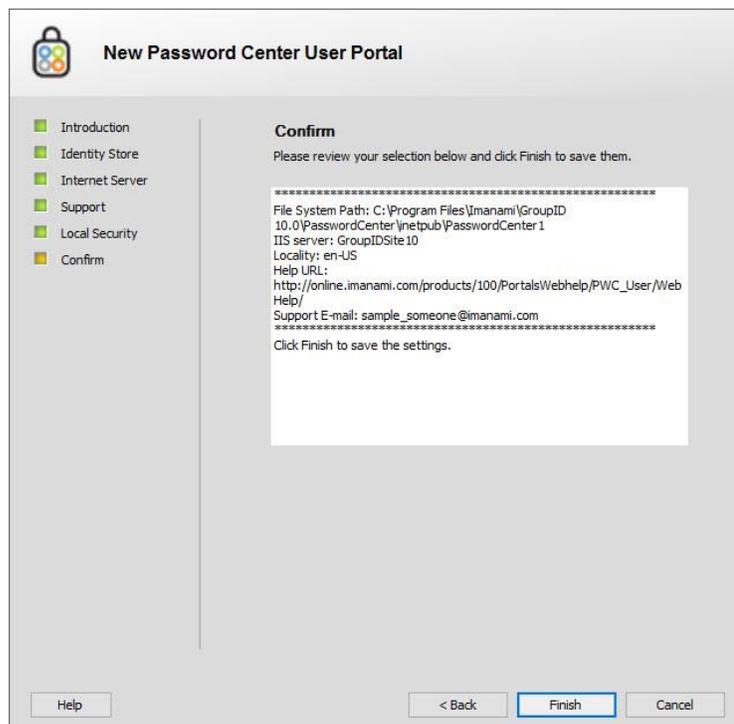
Figure 6: Confirm page

13. On the **Confirm** page, check the accuracy of the values you have entered for the portal's settings, and if necessary, click **Back** to return to the pages of any incorrect entries.

14. After reviewing the information, click **Finish**.

The user or Helpdesk portal is created and the portal's URL is displayed on the **General** tab against the Password Center > User Portals or Helpdesk Portals > *portal name* node. End users and Helpdesk users of the associated identity stores will be able to avail the account unlock, password-related services of the portal only if you enable **user portal permissions** for end users and **Helpdesk portal permissions** for Helpdesk users on the **Permissions** page:

Users of the connected identity store that have been linked with the portal can now use the portal.

Create a user or Helpdesk portal by copying an existing portal

You can create a new portal by copying an existing portal. All server and design configurations of the copied portal are duplicated to the new portal.

1. In GroupID Management Console, expand the Password Center node and then expand the **User Portal** or **Helpdesk Portals** node.

2. Right-click the portal you want to copy and select **Copy Portal** > **User Portal** or **Helpdesk Portal**.

3. The **New Password Center User Portal / New Password Center Helpdesk Portal** wizard is displayed, its pages are populated with the settings of the copied portal.

4. To modify any setting, follow the instructions in Create a portal using the wizard.

Launch a user or Helpdesk portal

Click **Password Center** > **User Portals** or **Helpdesk Portals**> [*portal name*]. The **General** tab lists the portal URL.

Click the URL to launch the portal.

Provide the portal's URL to your users so that they can access it through their browsers.

Notifications in the Password Center portals

Password Center user and Helpdesk portals can send notification emails to designated recipients when an end user or Helpdesk members perform a functions using the portals, provided that notifications are configured for those identity store in GroupID Management Console that are associated with the portals.

The administrator can specify notification recipients that can be:

- individual recipients.

- the user who performs Password Center related functions on user or Helpdesk portals.

Deleting a portal

Deleting a portal removes:

- the portal directories under the following locations on the disk:

  For user portals: *X*:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub)

  For Helpdesk portals: *X*:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Helpdesk\Inetpub)

  (where **X** represents the GroupID installation drive).

- the portal's virtual directory from the website in IIS.

  This website was selected for hosting the portal web application on the Internet Server page of the portal creation wizard.

Delete a portal

1. In GroupID Management Console, expand the **Password Center** node.

2. Expand the **User Portals** or **Helpdesk Portals** node.

3. Right-click the portal that you want to delete and select **Delete Portal**.

Chapter 3 – Modifying Portals' Settings

This chapter provides information to modify configurations of a Password Center user and Helpdesk portals. These configurations were mainly specified during portals' creation and include:

- Change a portal's display name; guides you on how to change a portal's name.

- Modify web server settings; explains how to manage settings for the IIS server that hosts the portal.

- Manage support settings; describes how you can change the email address of the portal's support team and the URL of the portal's online help.

- Link a portal to Identity Stores; explains how to associate a portal with one or more identity stores.

- Specify a different logo for portal, guides you on how to change a portal's logo.

NOTE   When any of the above configurations change, the portal's session ends and all connected users are logged out. When accessed again, the portal runs according to the new configurations

Change a portal's display name

Each portal is assigned a display name during creation. This name uniquely identifies the portal, and is used to name the portal's virtual directory in IIS and its physical directory under.

- **For user portals**:
  X:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub

- **For Helpdesk portals**:
  X:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Helpdesk\Inetpub

  (where **X** represents the GroupID installation drive).

You can change the portal name, but the change propagates only to the IIS directory; the physical directory name remains unchanged.

View a portal's display name

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **General** tab.
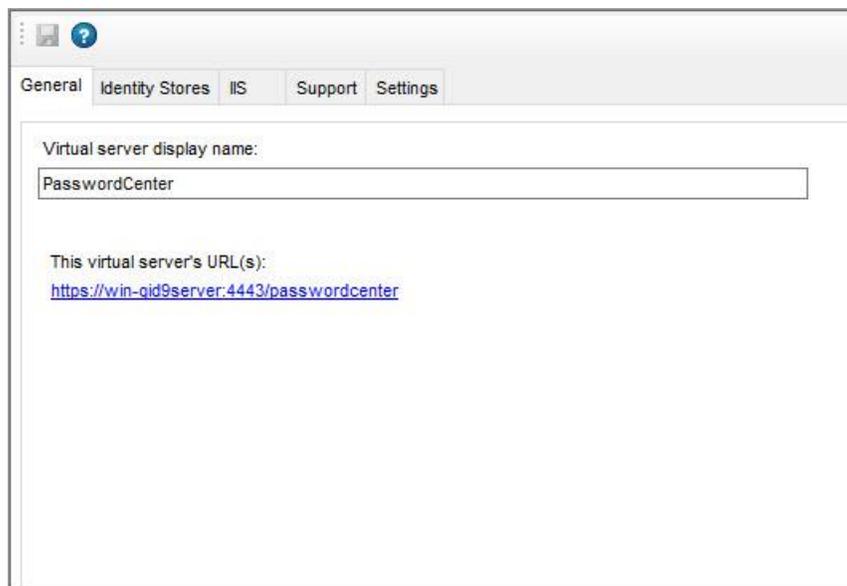
Figure 7: General tab

4. The **Virtual server display name** box displays the name of the portal.

Change a portal's display name

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **General** tab (Figure 7).

   In the **Virtual server display name** box, type the new name of the portal.

   This name will append with the web server address to construct the address which will be used for accessing the portal.

4. On the toolbar, click **Save** .

Link a portal to Identity Stores

End users and Helpdesk users of an identity store get access to a portal when their identity store is linked to a user portal and Helpdesk portal. End users belonging to the linked identity store can change, unlock and reset their password using the user portal and Helpdesk users can use the Helpdesk portal to reset the passwords and unlock accounts for users of the linked identity store(s).

If you want to link more identity stores with a portal or remove a linked identity store, use the **Identity Stores** tab.

On the **Identity Stores** tab, you can:

- View the identity stores associated with the portal. You can also view the data store type the identity store is created for.

- Modify the list of associated identity store(s) with the portal.

Associate an identity store with a portal

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **Identity Stores** tab.
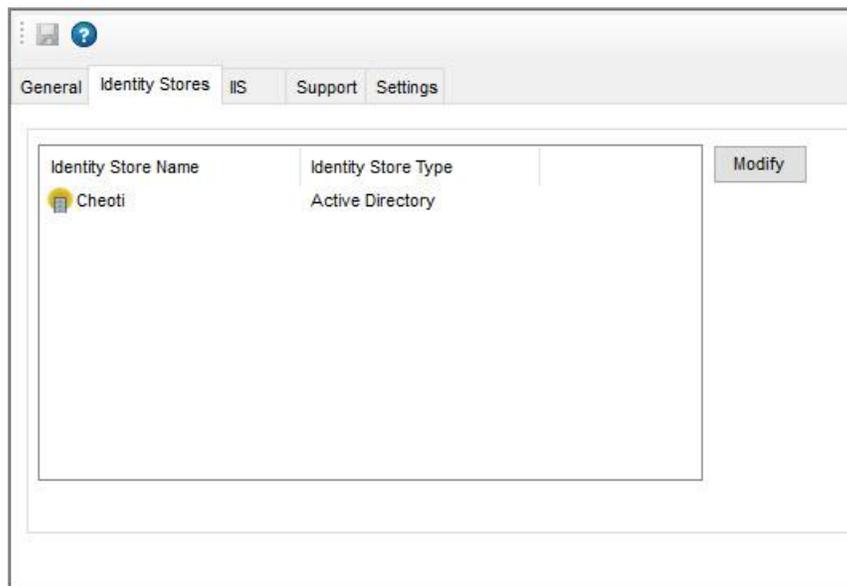
Figure 8: Identity Stores tab

4. Click **Modify** to modify the list of identity stores that are linked to this portal.

   The **Edit Identity Stores** dialog box is displayed.
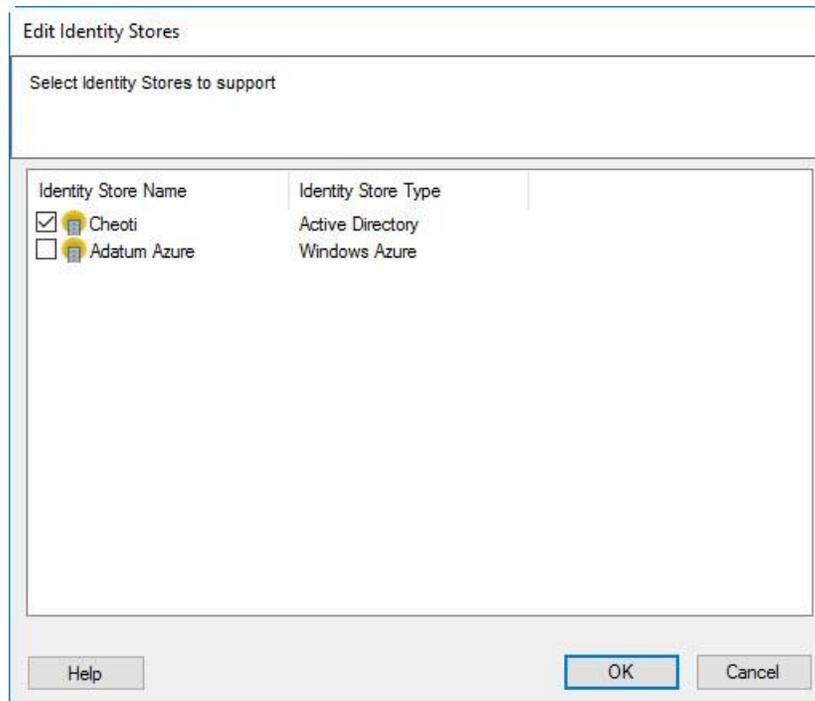
Figure 9: Edit Identity Stores dialog box

5. From the **Identity Store Name** list, select check box of one or more identity stores that you want to link and click **OK**.

6. On the toolbar, click **Save** .

Disassociate an identity store from a portal

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **Identity Stores** tab (Figure 8).

4. Click **Modify** to modify the list of identity stores that are linked to this portal.

   This displays the **Edit Identity Stores** dialog box (Figure 9).

5. From the **Identity Store Name** list, clear check box of one or more identity stores that you want to unlink.

6. Click **OK**.

7. On the toolbar, click **Save** 💾.

Modify web server settings

Each Password Center portal is hosted as a web application on the local IIS server.

Using the **IIS** tab, you can change:

- The IIS website that hosts the portal

- The URL of the IIS server

You can also view the physical path to the portal's folder.

View the physical path to a portal's folder

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **IIS** tab.
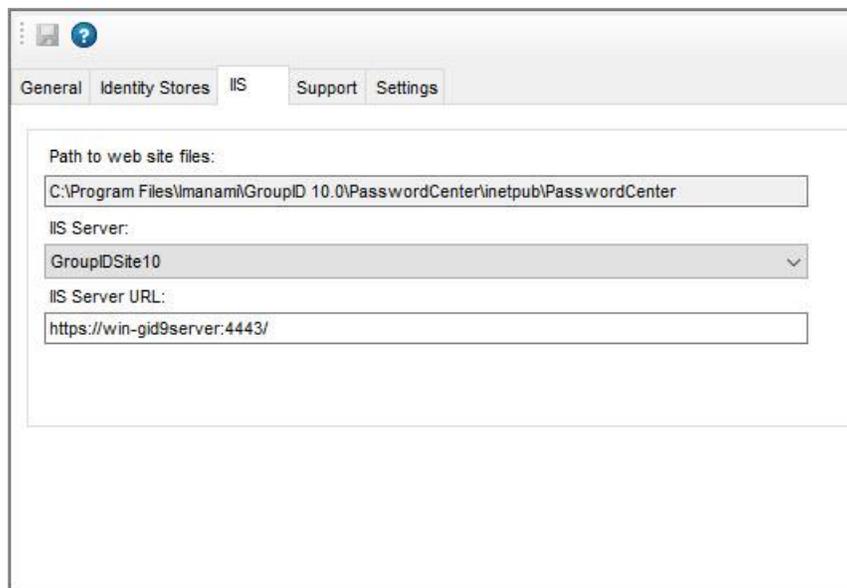
Figure 10: IIS tab

4. The **Path to web site files** box displays the physical path to the portal's folder. This field is read-only.

Change the IIS site for a portal

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **IIS** tab (Figure 10).

4. The **IIS Server** list displays the IIS site that hosts the portal. You can select a different IIS site from the list to move the portal's directory under it.

    The list displays the websites defined on the local IIS server. The default is *GroupIDSite9*.

5. On the toolbar, click **Save** .

Change the base server URL for a portal

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **IIS** tab (Figure 10).

4. The **IIS Server URL** box displays the URL of the IIS web server. This URL is used in email notifications for linking back to portal pages.

    If the name of the IIS web server has been changed, you can edit the URL in this box.

5. On the toolbar, click **Save** .

Manage support settings

Portals include a **Help** icon and a **Contact** link on their web interface. The **Help** icon launches the online help for the portal in a new browser window. The **Contact** link launches an email application to send an email to the administrator or Helpdesk for inquiries or feedback. Both links are customizable and their target email address or web address can be changed using the Support tab (Figure 13).

Figure 11: Help icon in the top right corner of the portal

Copyright © 2001-2019 Imanami Corporation. All Rights Reserved   Contact

Figure 12: Contact link at the bottom of the portal

Both links are customizable and their target email address or web address can be changed using the **Support** tab (Figure 13).

You can also configure the log settings for portal events. The logged events can be viewed in **Windows Event Viewer**.

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **Support** tab.
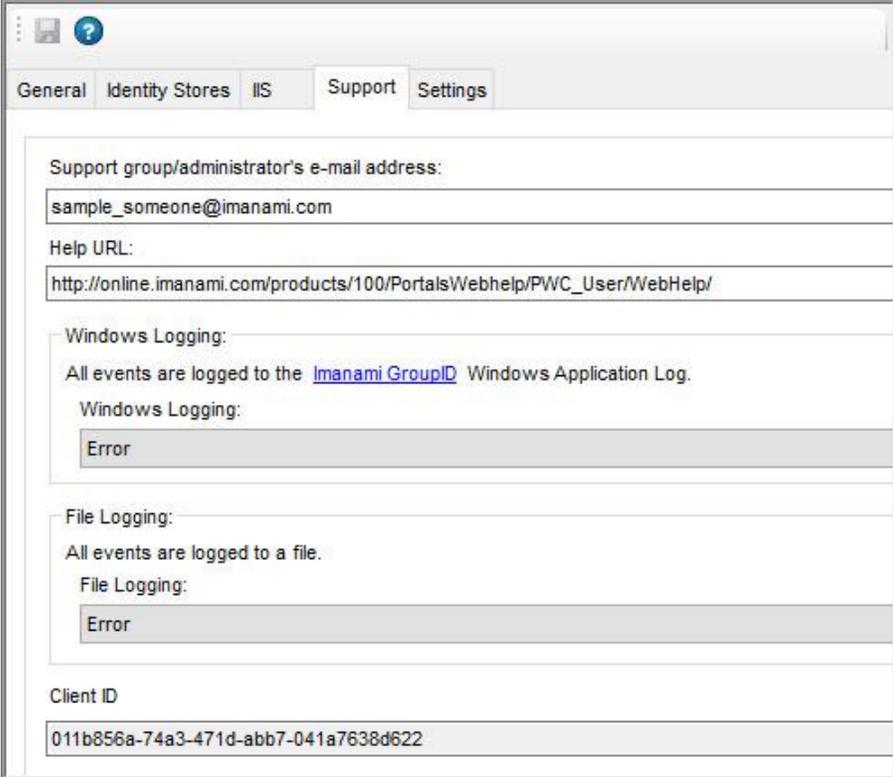
Figure 13: Support tab

On the Support tab, you can:

- Specify a different e-mail address for the support group or administrator

- Change the Help URL for a portal

- Configure Windows logging for a portal

- Configure File logging for a portal

- View the client ID assigned to the portal

Specify a different e-mail address for the support group or administrator

1. In the **Support group/administrator's email address** box, type the email address for the group, user, or contact that will be responsible for responding to requests or inquiries from portal users.

   This box shows the support email address specified during portal creation.

   This email address is mapped to the **Contact** link in the portal.

2. On the toolbar, click **Save** .

Change the Help URL for a portal

1. In the **Help URL** box, change the address of your company's internal support website or the portal's Help page, where portal users can find support material or report their problems.

   This box shows the help URL specified during portal creation.

   This URL is mapped to the **Help** link in the portal.

2. On the toolbar, click **Save** .

Configure Windows logging for a portal

1. From the **Windows Logging** drop down, select a level for the Windows logging.

   Windows Logging records five levels of events from Password Center in a centralized event log named **Imanami GroupID**. The logged events can be viewed in **Windows Event Viewer**.

Each successive event level incorporates the events of the preceding levels. The following table describes the five event levels.

	Level	Description
1.	Error	This is the default event level for Windows logging. This level logs problems such as loss of data or loss of functionality.
2.	Warn	This level logs events that are not necessarily significant, but may indicate a possible future problem.
3.	Info	Setting this level logs events that describe the successful operation of a module or functionality.
4.	Success Audit	Setting this level logs events that record an audited security access attempt that is successful.
5.	Failure Audit	Setting this level logs event that records an audited security access attempt that fails.

Click the **Imanami GroupID** link in this section to launch Windows **Event Viewer** and view the GroupID log entries.

2. On the toolbar, click **Save** 📙.

Configure File logging for a portal

1. From the **File Logging** drop down, select a level for the file logging.

File Logging records Password Center events in log files saved on the file system. These log files are created in a subfolder within the root directory of each portal:

[*Installation drive*]:\Program Files\Imanami\GroupID 10.0\PasswordCenter\Inetpub\[*Portal Name*]\Log

File Logging uses the **Rollover Logging** mechanism to log events. This mechanism logs events in a text file named **GroupID10.0-PasswordCenter**. When the file size reaches 100MB, the rollover archives the log file in the same directory by replacing the file extension with the suffix **.Log.X** and then creating a new text file named **GroupID10.0-PasswordCenter**. *X* in .Log.X is a number from 1 to 10 representing the archiving order; the lower the number, the more recently the file was archived.

File Logging groups events into seven levels depending on the type of information being captured. Each event level incorporates the events of the preceding levels. The following table describes the event levels.

	Level	Description
1.	All	This is the highest level of logging and logs every possible event in the log file.
2.	Debug	Setting the debug level designates fine-grained informational events that are most useful to debug the application.
3.	Info	Setting this level logs events that describe the successful operation of a module or functionality.
4.	Warn	Setting this level logs events that are not necessarily significant, but may indicate a possible future problem.
5.	Error	This is the default event level for file logging. Setting this level logs error events that might still allow the application to continue running.
6.	Fatal	Setting this level logs very severe error events that will presumably lead the application to abort.
7.	Off	Set this event level to turn-off file logging.

2. On the toolbar, click **Save** .

View the client ID assigned to the portal

Every GroupID client (such as Automate, Management Shell, a Password Center portal, etc.) is registered with a unique ID in the database, known as client ID.

This client ID is required while integrating a third-party single sign-on solution that support the SAML standard, into GroupID via any of its clients.

The **Client ID** box displays the client ID assigned to the portal. It is read-only and can be copied for use.

Specify a different logo for portal

You can use the default Password-Center logo or a logo of your choice for display in the portal.

1. In GroupID Management Console, expand the **Password Center** node.

2. Select the **User Portals** or **Helpdesk Portals** node and click the required portal.

3. Click the **Settings** tab.
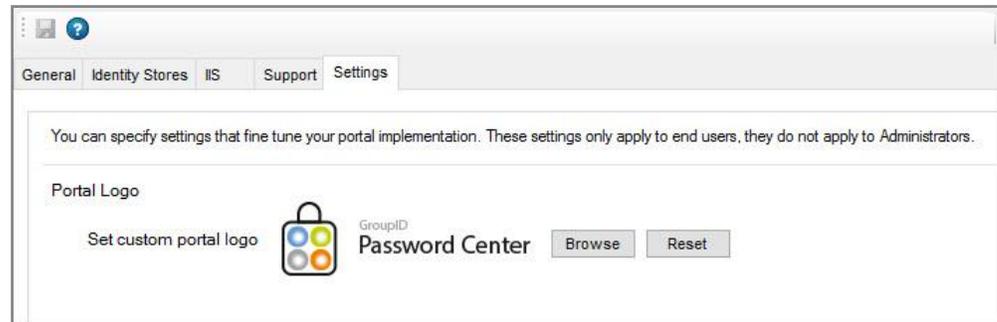
Figure 14: Settings tab

4. Use **Browse** to select and upload a logo of your choice for display in the portal.

5. Use **Reset** to revert to the default logo.