User Guide

Corporate Administrator

5.6

Galaxkey Limited
2 Falcon Gate, Shire Park,
Welwyn Garden City AL7 1TW
www.galaxkey.com

Table of Contents

Section 1. Version History

Version Number	Revision Date	Summary of Changes	Changed by
V 5.0	28 May 2018	Updated new functionalities	AK
V 5.1	05 Sept 2018	Updated the Digital Document Sign functionality	AK
V 5.2	10 Nov 2018	Review Changes	AK
V 5.3	09 Apr 2019	Updates with respect to new theme and licensing	AK
V 5.6	01 Jun 2020	Updates with new features and functionality Platform version: 5.6.7	AK

Section 2. Copyright

Section 3. About Galaxkey

Galaxkey is a data protection company providing a portfolio of corporate data protection products to secure all data and support multinational data compliance regulations. Galaxkey is a global company with its headquarters in the UK. Our Galaxkey team has vast experience working with large multinational organisations across a variety of sectors and Galaxkey has select partners globally to provide local support and service to our customers across the globe. Our robust and experienced team offers exceptional customer service as well as quick response and turnaround times.

3.1. Disclaimer

The information contained in this document is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Galaxkey Ltd.

While every care has been taken in preparing this document, Galaxkey Ltd cannot be held responsible for any errors or omissions. The information in this document is subject to change without prior notice.

Galaxkey is a registered trademark of Galaxkey Ltd., registered in the U.K. and other countries. All other trademarks belong to their respective owners.

3.2. Corporate Administrator Guide

This document, the Corporate Administrator Guide, outlines the functionalities for a Galaxkey Corporate Administrator. The intended audience for this document is the users with administrative rights and with access to the Galaxkey Manager.

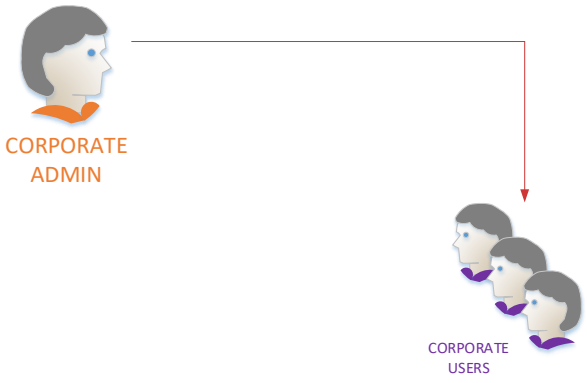
Section 4. Roles

4.1. Overview

The Corporate Administrator is an admin role in the deployment and management of Galaxkey in a corporate environment. The functions of the Corporate Administrator are

1. Domain Management
2. Configuration Management
3. Corporate Identity Management

This document outlines these functions in detail and provides guidelines for the effective management of security in a corporate infrastructure.



The **Partner** is responsible for the creation of the **corporate account** and assigning the licences for the trial.

The **Corporate Administrator** is responsible for the creation of **Individual Users** within the Corporate.

The Individual Users are the actual Galaxkey users.

4.2. URL for Management

The Corporate Administrator can perform these functions from the Galaxkey Manager Portal. The URL to the portal is https://manager.galaxkey.com.

If the company has an in-house customised portal, the URL to the portal is https://**company**.galaxkey.com, where the **company** is the designated sub-domain provided by Galaxkey.

4.3. Administrative Access Delegation

Galaxkey lets the corporate administrator to delegate one or more of the administrative tasks to other individual users in the organisation by configuring **Service Accounts.**

For details refer *Active - Service Accounts & Administrative Rights*

Section 5. Domain Management

Domain Management in Galaxkey is the process of managing the existing domains and registering one or more additional domains for secured communication.

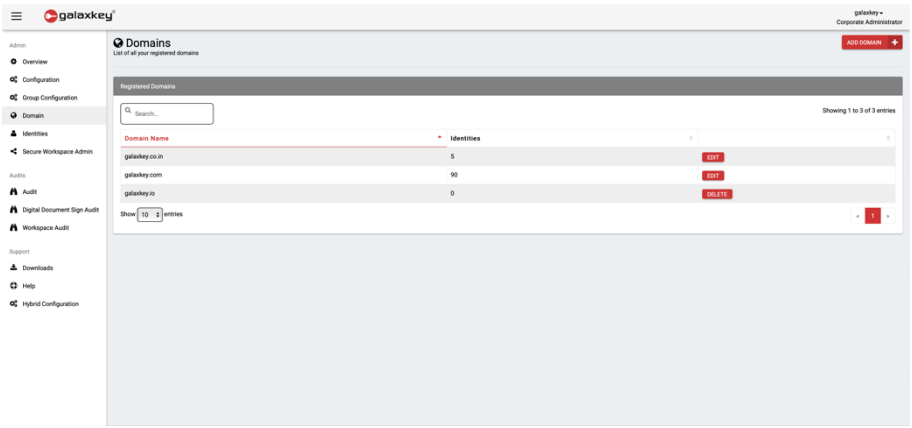
A corporate licensee with licence type Enterprise Self Hosted can also configure the web access for the domain to enable a web-based reader and keeping track of the domain's web access installation type.

A default domain is registered with Galaxkey when your organisation subscribes for the Galaxkey Licence. To start using Galaxkey in a corporate environment, the Corporate Administrator must first register a domain. It is the first step towards ensuring that the domain is exclusively owned by the Corporate and cannot be re-registered in the Galaxkey ecosystem.

If the Corporate Administrator is unable to register a domain because the domain has already been registered, send an email to the Galaxkey support team at *support@galaxkey.com*, and we will investigate and resolve the issue as soon as possible.

5.1. Process

The **Domains** module of the Galaxkey Manager provides the interface for Domain Management.



The primary purpose of this module is to enable the Corporate Administrator to register other domains owned by the organisation and extend Galaxkey security across the organisation.

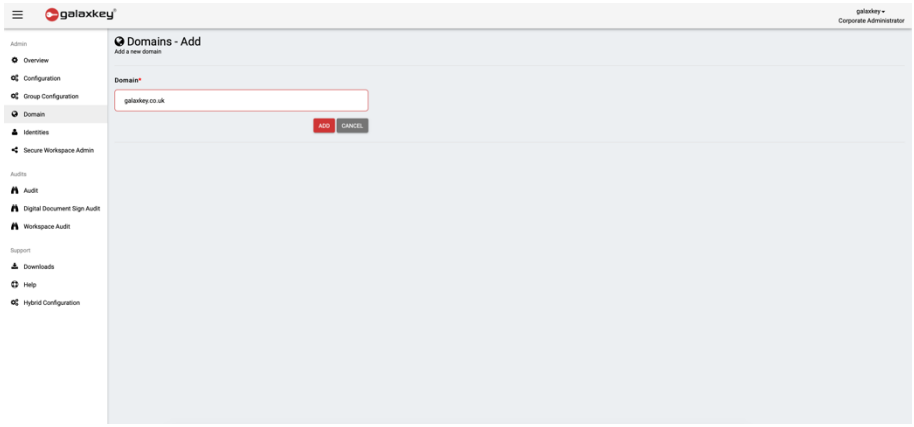
The home page of the Domains module lists all the email domains of the organisation registered with Galaxkey. When you first log in, this page lists only the domain registered while engaging with Galaxkey.

You can use this module to:

1. Add a new domain
2. Manage the web access options for the existing as well as the new domain

5.1.1. Add Domain

The primary domain of your organisation is added at the time of deal registration. You can register additional domains with Galaxkey using this portal. Click the "**ADD NEW DOMAIN**" button on the home page to register a new domain.



Enter the domain name in the **Domain** field and click the **'ADD'** button. Once registered, your domain will be listed on the home page.

Galaxkey support team will run background checks to ensure the domain is owned by your organisation. If the domain is not owned, then the administrator will be informed accordingly and the domain will be removed from your account.

You can now add the identities of this domain from the '**Identities**' module. A domain **cannot be deleted** once identities are associated with it. It can **only be edited** after that.

Note:

This new domain is in addition to the default domain registered with Galaxkey at the time of registration.

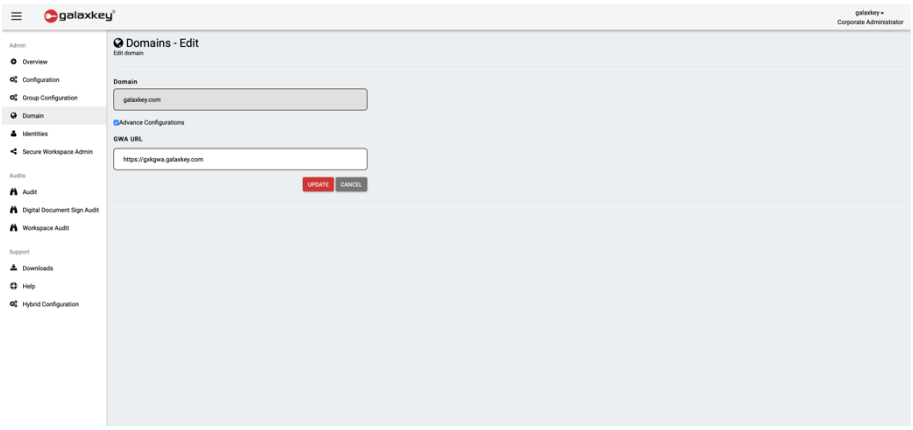
5.1.2. Managing Galaxkey Web Access Option

Galaxkey Web Access (GWA) is the Galaxkey Web Client for viewing and sending Galaxkey secured emails.

As the client is web-based, the user can easily access it via any browser.

The GWA client can be installed in a corporate environment as well. The link to the local copy of GWA can be configured using this section.

On the home page, click the '**EDIT**' button to configure the Galaxkey Web Access for the domain.



This is the process to enable GWA for a corporate domain

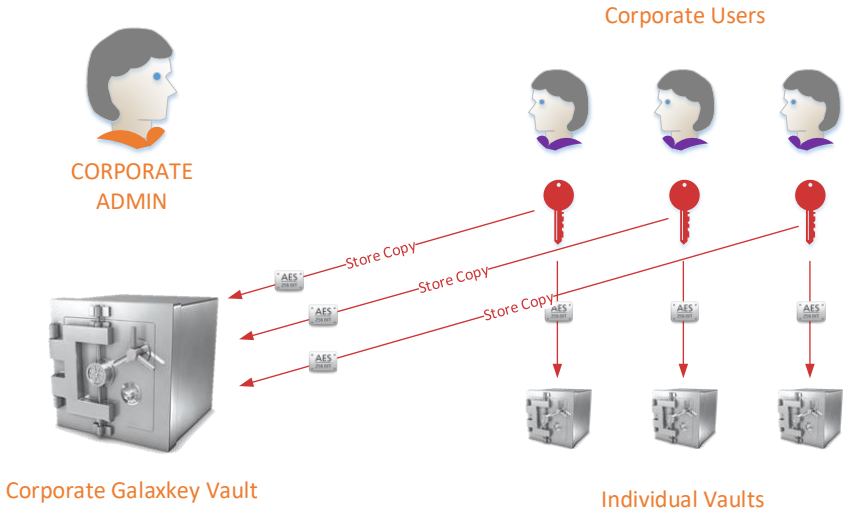
1. On the '**Edit Domain**' page, check the '**Advanced Configurations**' check-box.
2. In the GWA URL, enter the URL to the GWA server installed on your premises.
3. In case, there is no in-house GWA installation; the emails can be accessed over the web via *https://gwa.galaxkey.com*.

   Note:

   *To access the Galaxkey Secured emails over the web, the **CONFIGURATION > Group Policies > Galaxkey Secure Share** must be appropriately set.*

Section 6. Corporate Identity Management

The identities of the users in the Corporate are stored in the Corporate Administrator's Vault which is secured using the Corporate Administrator's password.



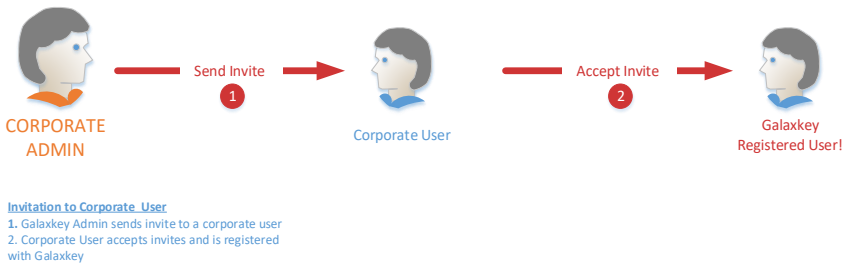
Corporate Identity Management encompasses the following:

1. Adding identities of new corporate users
    a. To add multiple identities simultaneously use the **Galaxkey Active Directory Connector (GADC)**
    b. To add identities one at a time, use the **Identities** module of the Galaxkey Manager.
2. Managing existing Users

6.1. Adding New Identity

As a Corporate Administrator, you can create Galaxkey identities in one of the following two ways

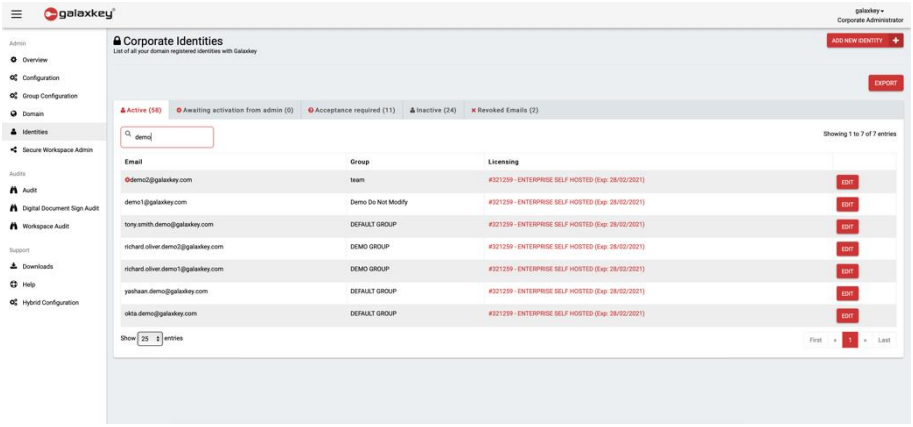
1. By registering via the **Identities** module



2. By registering via the Galaxkey Active Directory Connector (GADC)

6.1.1. Registering via Identities Module

The **Identities** module gives you a bird's eye view of the individual identities, their statuses, groups and the licence validity thereof.

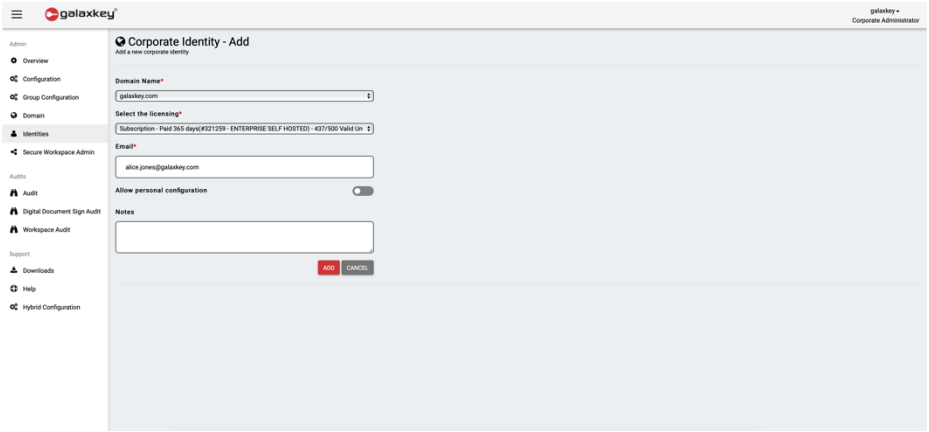


The Identities module lists the existing identities with their licence details. You can add new identities, one at a time.

Following is the process for adding individual corporate identities to the Galaxkey Manager, **one at a time.**

1. Log on to the Galaxkey Manager and go to the **Identities** module.
2. Under the Identities tab, click on the Add New Identity button to open the Add New Email Identity page.
3. The **'Domain Name'** drop-down is populated with the domain added while registering the company with Galaxkey. If you have added other domains, you can select the domain from the available list.
4. The **'Select the licensing'** drop-down by default displays the valid licence.
5. In the **'Email'** field, enter the email ID of the individual user to be registered. The email you enter must be of the same domain you have selected in the Domain Name drop-down.
6. Enter your admin password in the '**Please re-enter your login password**' field.
7. Enabling the **'Allow personal configuration'** will allow the individual user to **override corporate settings** for his/her identity. Enter special comments, if any, in the **'Notes'** field.

Click the **'ADD'** button. The newly added user is listed under the **'Acceptance Required'** tab on the list page.



An **invitation email** is sent to the individual user directing the user to register with Galaxkey.

After the user accepts the Galaxkey invitation, the **DEFAULT GROUP** is assigned to the user. You can then change or assign more groups to the user.

6.1.2. Registering via Galaxkey Active Directory Connector (GADC)

Adding individual corporate identities to the Galaxkey Manager, one at a time, is a tedious and time-consuming task. The GADC enables you to add multiple identities to the Galaxkey Manager simultaneously. This is the process for adding multiple corporate identities to the Galaxkey Manager all at once.

1. Log on to Galaxkey Manager. Go to the Downloads module. Download the GADC which is available under the **'Additional Downloads'** tab.
2. Run the GADC application on a network machine. This will automatically add all your corporate identities to the Galaxkey Manager. All the identities will be displayed under the **'Acceptance Required'** tab on the list page.

An **invitation email** will be sent to all the individual users directing them to register with Galaxkey.

Please refer to the GADC Manual for more details

6.2. Managing Existing Identities

Identity management is another key function of the Identities module, which includes managing the access rights, status and passwords of the corporate users.

The identities are grouped and displayed in tabs depending on their statuses. The statuses are defined as follows;

1. **Active**: The identities listed in this tab are all the active identities, which have a valid licence assigned to them.
2. **Inactive:** The identities listed in this tab are all the identities which are rendered inactive. The users using these identities cannot access their secured documents – emails and files since the licence for such users is released. This licence can then be assigned to other users.
3. **Acceptance Required:** The identities listed in this tab are all the identities awaiting acceptance by the users to whom the identities have been assigned.

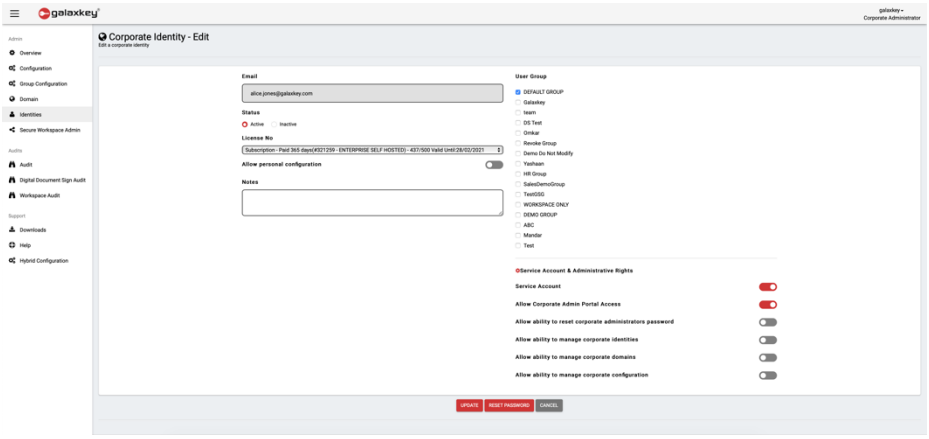
The tabs are only shown when there is at least one identity with the given status. The functionalities of the identities differ for each tab.

6.2.1. Active Identities

The listing of the identities in this tab displays the email address, group, the licensing and the ability to edit the identity.

The identity can be in one or more groups which are displayed in comma separated listings.

If the licence is assigned to the identity, it is displayed with the licence number and the expiry date. If the identity licence is expired, a button appears that allows you to assign a new licence to the identity. You can also click on the existing licence and change the licence if required.



The **Edit** button lets you edit the following identity details

1. **Change status from Active to Inactive** – When you change the status from **active to inactive**, the licence is released, and the user is unable to access secured documents.
2. **Change licensing** – This is particularly required when applying new licence after revising your subscription.
3. **Enter notes** – You can enter any details, instructions or relevant information in this field.
4. **Enable Allow Personal Configuration** – If you enable this option, the user can manage his/her own configuration, and the corporate configuration policy is not applicable to the user.
5. **User Groups**-Assign appropriate pre-defined user groups to the users. You can assign multiple groups to a user. The Galaxkey configuration is group-based. Thus, the security features change as per the assigned groups. In the case of multiple groups, the maximum-security settings override. Refer *Groups* for details.
6. **Reset password** – Ability to reset user passwords. Refer *Active – Reset Password* for details.
7. **Enable Service Account & Administrative Rights**-This enables you to delegate some of your Galaxkey management responsibilities to other users. Refer *Active – Service Accounts & Administrative Rights* for details.

6.2.2. Active - Reset Password

The Edit Mode facilitates with changing a user password using the **RESET PASSWORD**. Since Galaxkey does not store any passwords, the process for resetting a password is as follows;

1. Enter the Corporate Administrator's password, which is used to extract the user's key from the admin's password store.
2. The extracted key is then secured using a temporary password which is emailed to the user.

   Note: In case of Single Sign-On [SSO – e.g., AD authentication], the temporary password will be used directly in conjunction with the Network password and will not be communicated with the user.
3. Once the user logs on to the portal, the user must reset the password.

Note: The user is not required to change password in case of SSO.

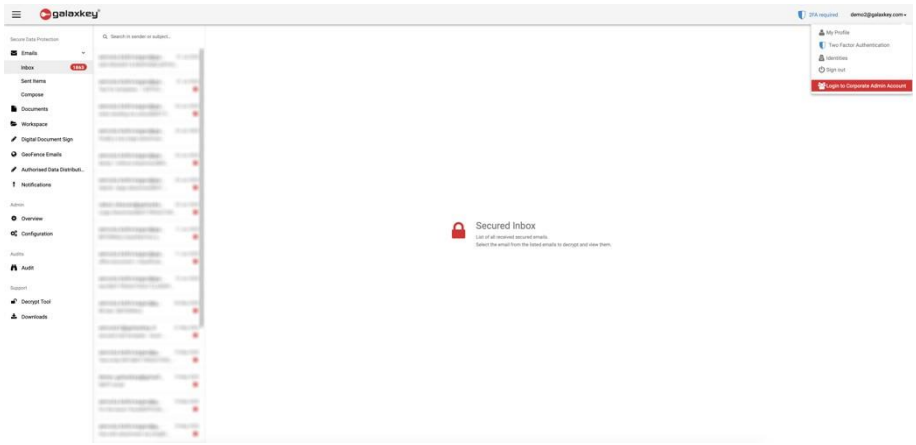
6.2.3. Active – Service Accounts & Administrative Rights

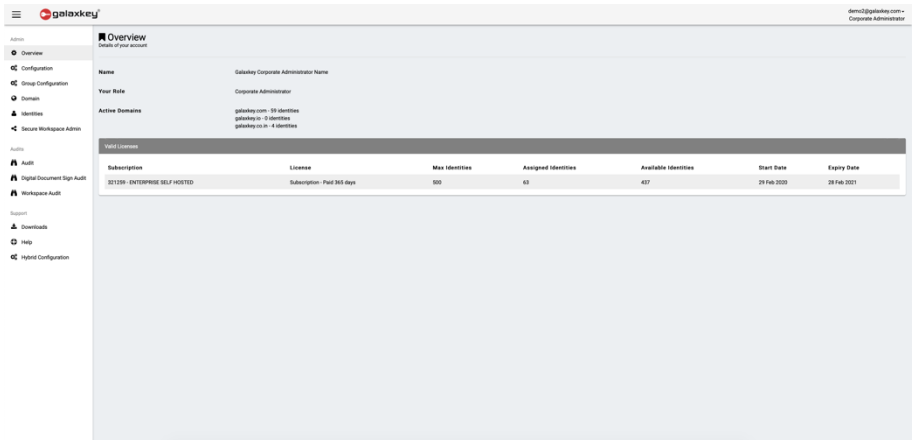
This section enables the Corporate Administrator to delegate administrative rights to a non-admin Galaxkey user. The account to which administrative rights is granted is the '**Service Account**'.

Once you select the **'Service Account'** checkbox, the **'Allow Corporate Admin Portal Access'** checkbox is displayed. On selecting this, the following options become available

1. **Allow ability to reset corporate administrator password**: Selecting this option enables the user to reset the administrator account password.
2. **Allow ability to manage corporate identities**: Selecting this option grants the user access to the Identities module and thus to the Corporate Identity Management.
3. **Allow ability to manage corporate domains**: Selecting this option grants the user access to the Domains module and thus to the Domain Management.
4. **Allow ability to manage corporate configuration**: Selecting this option grants the user access to the Configuration module and thus to the Corporate Configuration Management.

You, as an administrator, can choose which administrative rights to grant to the selected user. You can choose to set an account as service account and yet NOT grant access to the Manager Portal.





The user with the Service Account can then see an additional button in the Galaxkey Manager which lets her switch between accounts.

Note: A user, when logged in as Service account, cannot edit own identity.

In addition to the administrative rights, this Service Account is used in Galaxkey Secure Gateway (GSG) for encrypting and decrypting the emails.

6.3. Inactive Identities

The identities in this tab are identities rendered inactive either by GADC or manually by the Corporate Administrator.

When you mark an identity '**inactive**', the Galaxkey user account is deactivated and access to all the secure data is revoked. Yet, the keys are retained, such that you can reactivate the account.

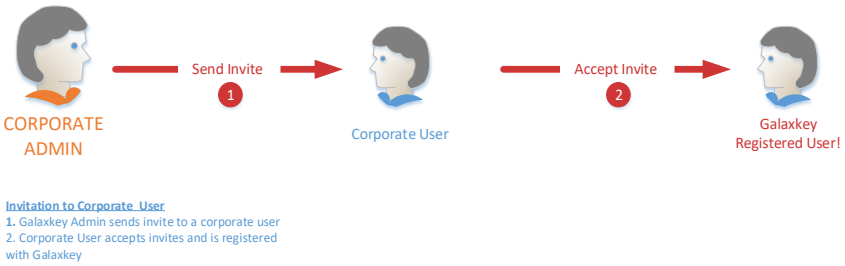
In marking inactive, the licences of inactive users are released and are available to assign to other corporate users.

You can revert the inactive identities to active by reassigning the license.

You cannot reset the passwords when an identity is inactive.

6.4. Acceptance Required

When the Corporate Administrator adds a new identity, the user must accept it.



An identity is in the '**Acceptance Required**' stage from the time of receipt of the invitation to the time the user accepts the invitation. An identity in this stage cannot be edited. You can either **resend** the invite using the '**RESEND INVITES**' button or **delete** the identity.

Section 7. Galaxkey Configuration

Galaxkey Configuration is done at two levels – at a Corporate and a Group level. While the corporate configurations mainly deal with the look and feel of Galaxkey, the group configurations help to set up Galaxkey to suit an organisation's security requirements.

Accordingly there are two modules to manage Galaxkey configuration

1. Configuration
2. Group Configuration

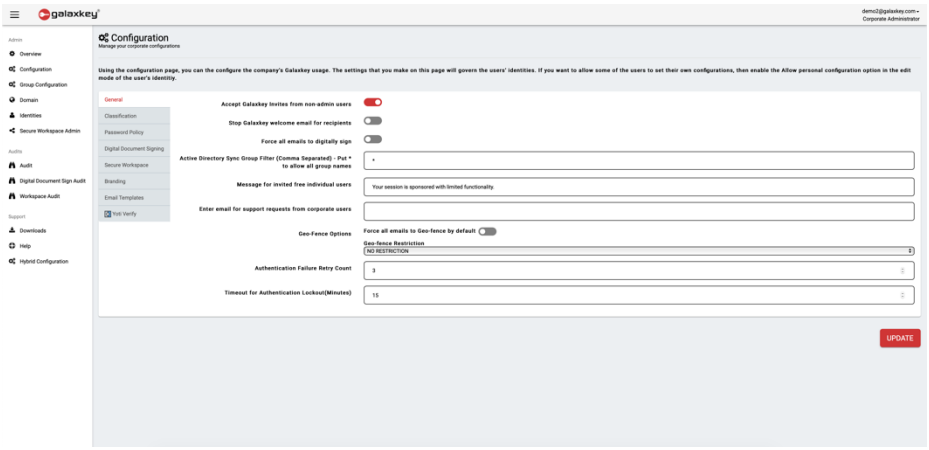
7.1. Configuration

The options in the **Configuration** module govern the global policies and the look and feel of Galaxkey for the Corporate. The configurations in this module can be defined as

1. General Configurations
2. Classification
3. Password Policy
4. Secure Workspace
5. Branding
6. Email Template Configurations

The following sections consider each of these in greater detail.

7.1.1. General Configuration



7.1.1.1. Accept Invites from Non-Admin Users

Galaxkey works on an invitation model. Thus, a new user is invited to join the Galaxkey network when you send an email to a new user.

The '**Accept Galaxkey Invites from non-admin users'** option, lets you control whether users in your organisation can receive invitations from other Galaxkey users. This attribute allows you, the administrator, to manage your licensing and subscription with Galaxkey.

If you **disable** this option, users in this domain will be able to receive invitations ONLY from the corporate administrator.

If you **enable**, users from this domain can receive invitations from any of the Galaxkey registered users. Licences will be assigned to these users when they accept the invite and complete the registration process.

If the number of '**Registered Users**' exceeds the number of subscribed licences, all the invited identities will be listed under the '**Awaiting activation from admin**' tab. For these users to be able to use Galaxkey, you must purchase additional licences OR manage from the existing ones.

For example, you have purchased 10 Galaxkey licences. If you **disable** this option, no user other than the 10 you have assigned the licences to will receive Galaxkey invitations. If this option is enabled, new users in your organisation with the domain email address can receive invitations, and you must assign them licences accordingly.

Select the '**Accept Galaxkey Invites from non-admin users**' checkbox to enable domain users to receive invites to join the Galaxkey network.

7.1.1.2. Stop sending welcome emails

Select the '**Stop Galaxkey welcome emails for recipients**' checkbox to disable the system sending the welcome email to any user invited by a member of the corporate account.

7.1.1.3. Enforce digital sign

Select the '**Force all emails to digitally sign**' checkbox to auto check the Sign option in the confirmation dialog before a user sends an encrypted.

7.1.1.4. Active Directory Sync Group Filter (Comma Separated) - Put * to allow all group names

You can synchronise the groups in the Active Directory with Galaxkey. This setting aids with the synchronisation of groups in the AD with Galaxkey.

7.1.1.5. Message for Invited free individual users

Galaxkey works on an invitation model, i.e., invites are sent to people to join the Galaxkey network. This setting lets you configure a message to be displayed when your invitee's login after successful registration.

7.1.1.6. Enter email for support requests from corporate users

When an end-user from your organisation raises a Galaxkey support request, it must be addressed within the organisation at the first level.

You can configure an email address (Galaxkey user) which will receive all such internal requests using the '**Enter email for support requests from corporate users**' setting.

7.1.1.7. Geo fence options

Galaxkey lets you geo-fence, i.e., restrict the '.gxk' attachments from leaving your organisation's premises or the server located therein.

The '**Force all emails to Geo-fence by default**' option lets you enforce geo-fencing of secured emails for the enterprise. Thus, when this option is enabled, all the secured emails sent from the domain users are geofenced. This setting is disabled, by default.

The **Geo-fence Restriction** option lets you create a whitelist of sorts. You can select the geographical regions (and thus, IP addresses) from which the secured files can be accessed using this option. The default setting for this is '**No Restriction**', which makes the secured file available in all the regions.

7.1.1.8. Authentication Retry

When a user fails to authenticate for a set count of times, the system blocks the user to again authenticate for 15 minutes. Set the value in the "**Authentication Failure Retry Count**" to set the count before the user is blocked for 15 minutes.

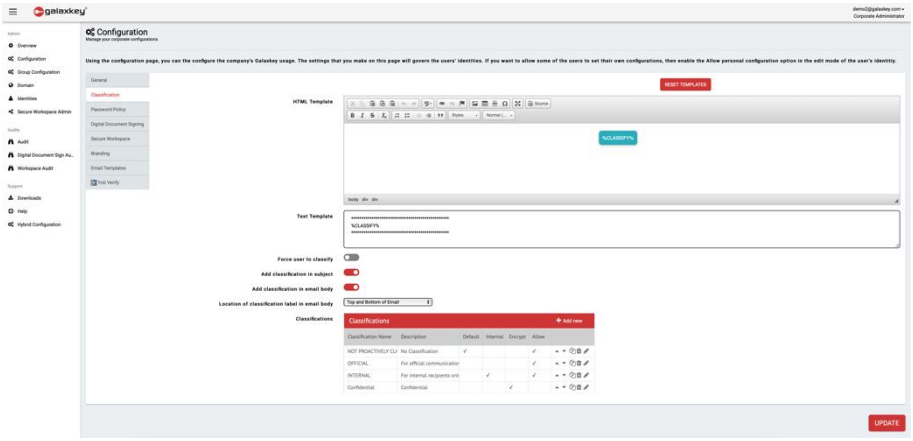
7.1.1.9. Timeout before re-authentication is allowed

If the user fails authentication, he is blocked for 15 minutes by default. This 15 minutes can be configured to required minutes as per corporate policy. Set the value for "**Timeout for Authentication Lockout(Minutes)"** in minutes.

7.1.2. Classification

The corporate configuration for Classification includes

1. Email configuration & force classification
2. Visual label configuration
3. Review and reconfigure the classification definition



7.1.2.1. Email configuration & force classification

On the Configuration menu, go to the Classification Section. This section lets you

Configure Email Template

1. Galaxkey provides a preconfigured email template, both in **text** and **HTML** format, which are used when the end-user sends a Galaxkey classified email.
2. You can make changes to the template to suit your requirement

The placeholder %CLASSIFY% is required to fetch the classification set by the user.

3. Click the Update button after all the changes are done.

Force User to Classify

1. By enabling the Force User to Classify setting, you make it mandatory for users to classify every email exchanged in the organisation.
2. By enabling this option, end-users are prompted to classify emails before sending them.

7.1.2.2. Configuring Labels

Add classification in subject: You must enable this setting if you want the email subject to be prefixed with the set classification.

Add classification in email body: You must enable this setting if you want the classification label to be added in the email.

Location of classification label in email body: You can configure the position of the label in the classified email. To do this, you must select one of the following

1. Top of email (default position)
2. Bottom of email
3. Top and bottom of email

7.1.2.3. Classification Definition

Galaxkey comes with a set of pre-configured classification titles viz.

1. NOT PROACTIVELY MARKED
2. INTERNAL ONLY
3. PROTECT
4. RESTRICTED
5. CONFIDENTIAL

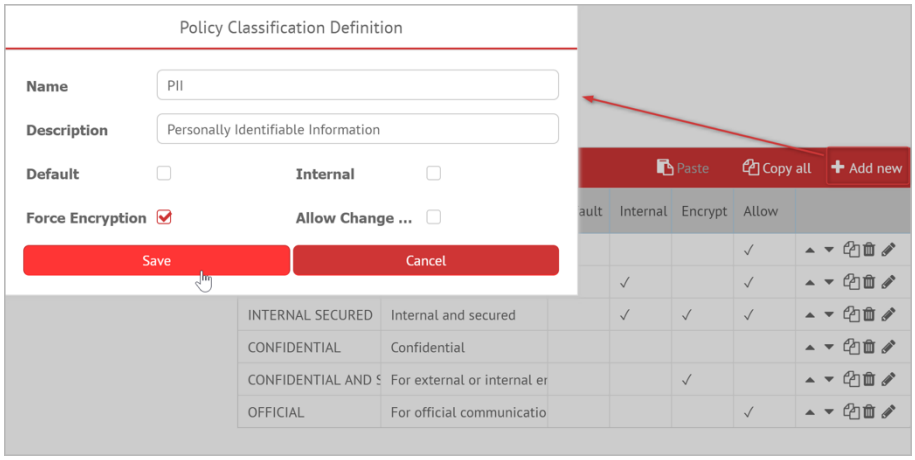
You can use these or edit them to suit your requirements. You can also create a new set of classification definitions.

The Classification table provides the information including classification name, description and classification attributes such as Default, Internal, Force Encryption, Allow Change Down.

The Action column gives you the options to reposition, copy, delete and edit the classification.

Add New Classification

1. Click the **Add New** button to create a new classification.
2. On the pop-up screen, enter the following information:



a. **Classification Name**: Enter a suitable name in this field. This is the label that will be displayed in the clients while classifying the email.

b. **Classification Description**: Enter a brief explanation for the classification. The description should reflect the purpose for setting the classification.

c. **Default**: Select this checkbox to set the classification as the default classification to be applied to the emails.

There can be only one Default classification.

d. **Internal**: Select this check box if you want to restrict the emails with this classification to your domain.

e. **Force Encryption**: Select this option if you want the email to be encrypted when this classification is applied.

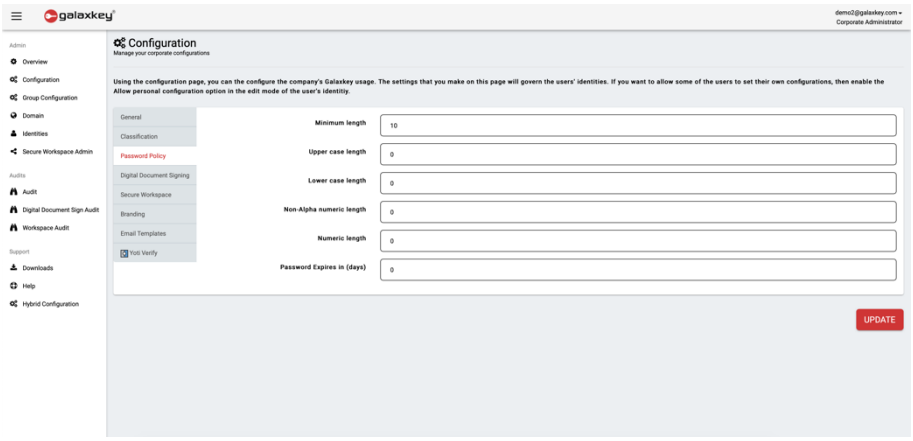
f. **Allow Change Down**: Select this option if you want to allow the users to change the classification to a lower sensitivity level.

3. Click the **Save** button once you have set the classification definition to suit your requirements.
4. Click the **Update** button to apply and save the additions and changes.

This completes the corporate classification definition. You can modify the definitions at a later stage.

7.1.3. Password Policy

Galaxkey provides an option that enables you to create a template for all users to create a strong Galaxkey password.



The password policy can mandate users to use at least one numeric, uppercase and special character in their password. You can also enforce a minimum password length.

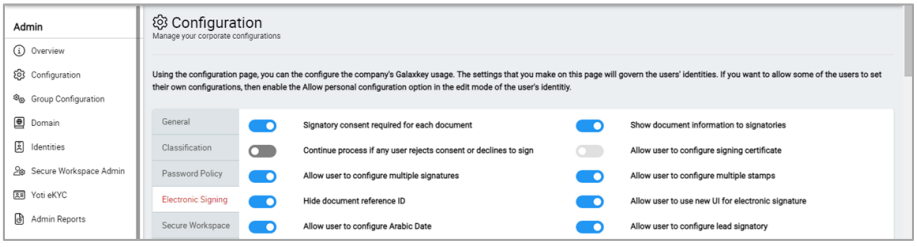
7.1.4. Electronic Signing

The corporate administrator can configure Electronic Signing from the **Configuration > Electronic Signing** menu of the admin portal.

7.1.4.1. Configuring Signing Options

The following settings affect the signing experience of the document owner and signatory. When these settings are enabled

1. **Signatory consent required for each document**: Signatories must consent to signing for every document they sign.
2. **Continue process if any user rejects consent or declines to sign**: Signing process continues even if one of the signatories declines to sign a document or rejects the document consent.
3. **Allow user to configure multiple signatures**: Grants ability to the users to configure more than one signatures
4. **Allow user to configure Arabic Date**: Grants ability to the document owner to capture date of signing in Arabic
5. **Show document information to signatories**: Grants ability to all the signatories to view the document information
6. **Allow user to configure multiple stamps**: Grants ability to the users to configure more than one stamps
7. **Allow user to use new UI for electronic signature:** Option to enable the new UX

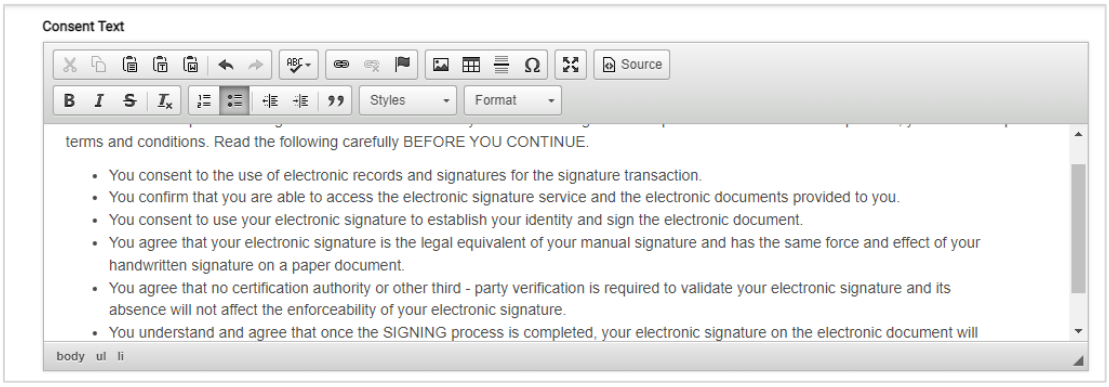


8. **Hide document reference ID**: Document id (gxk id) not displayed on the document
9. **Location of document reference ID in PDF**: Decide the positioning of document id
10. **Document reference ID colour**: Text Colour in which document id is printed
11. **Document reference ID font size**: Text size in which document id is printed
12. **Company logo width and Company logo height**: Ability to configure the size of corporate stamp. The size range is between 60 – 300px

7.1.4.2. Configuring Consent text & Metadata

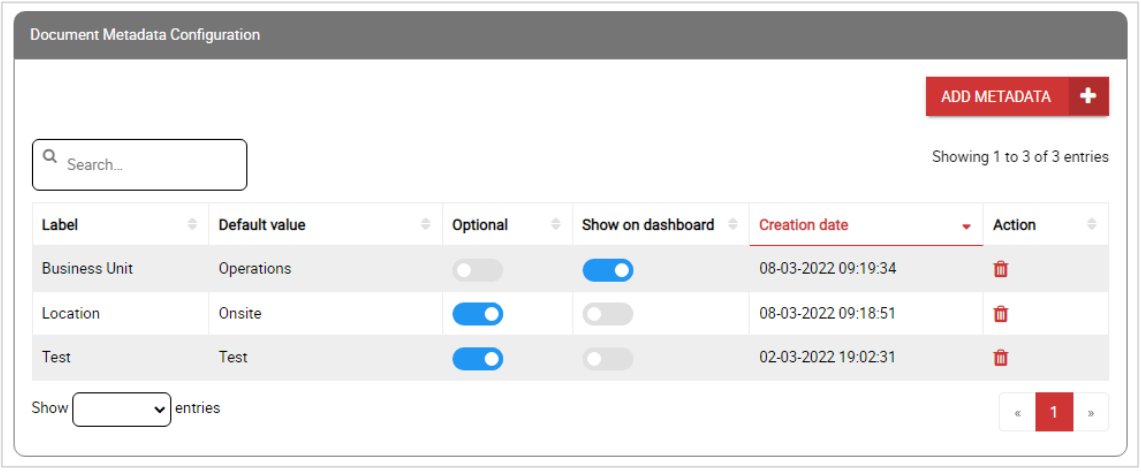
1. Configuring Consent Text

Galaxkey provides a standard consent statement for signing the documents. However, you can use consent text in line with the corporate policy.

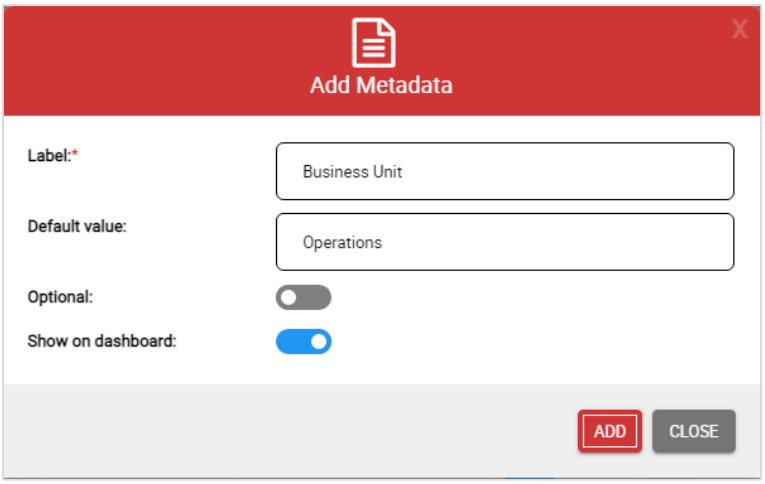


2. Configuring Metadata fields

You can capture additional information about a document using the predefined Metadata fields. In the Document Metadata Configuration section, click, Add Metadata button. On the pop-up form enter:



1. **Label**: Name of the field to be displayed while adding document.
2. **Default Value**: This optional fields is used to configure a default value to be displayed in the field.

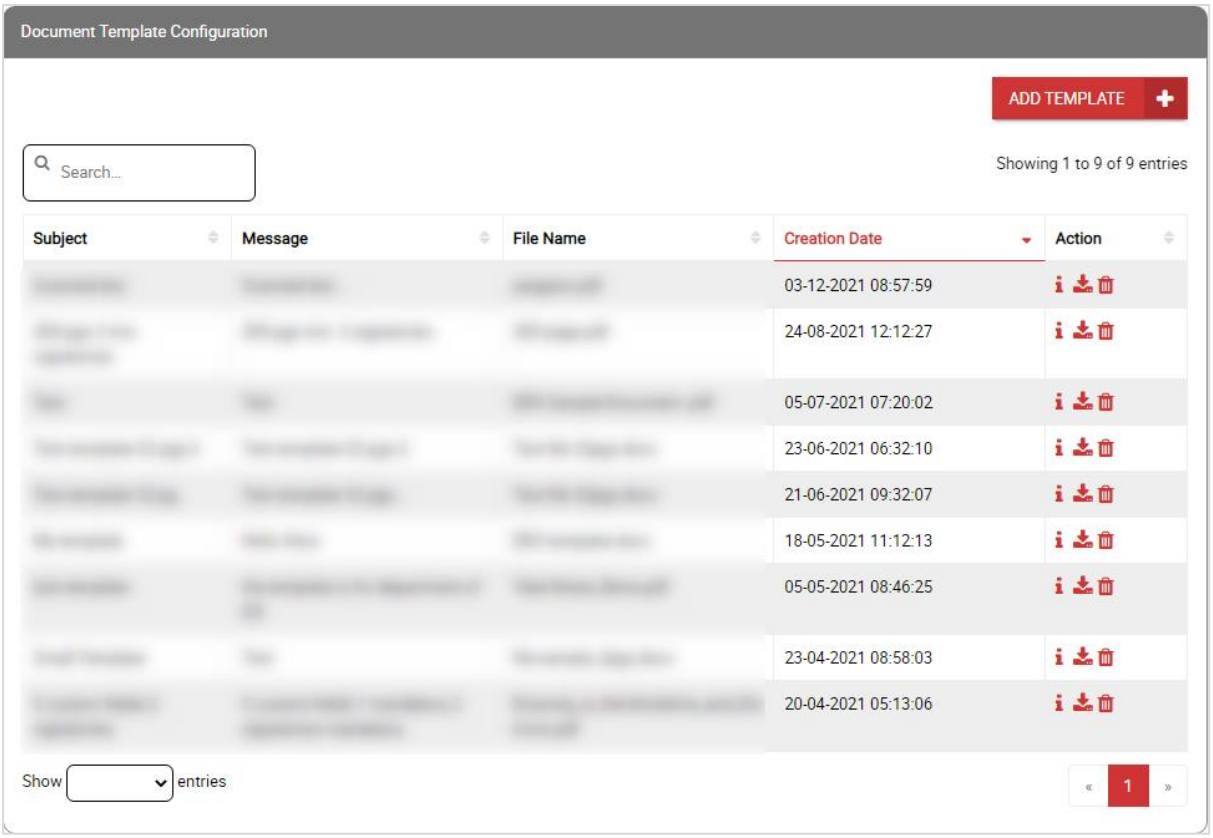


3. **Optional**: Enabled by default, use this slider button to make the field optional or mandatory.
4. **Show on dashboard**: Disabled by default, use this slider button to decide if the information is to be shown on the My documents list page.

Upon saving, the field is enlisted in the Document Metadata Configuration section. You can delete the field from here.

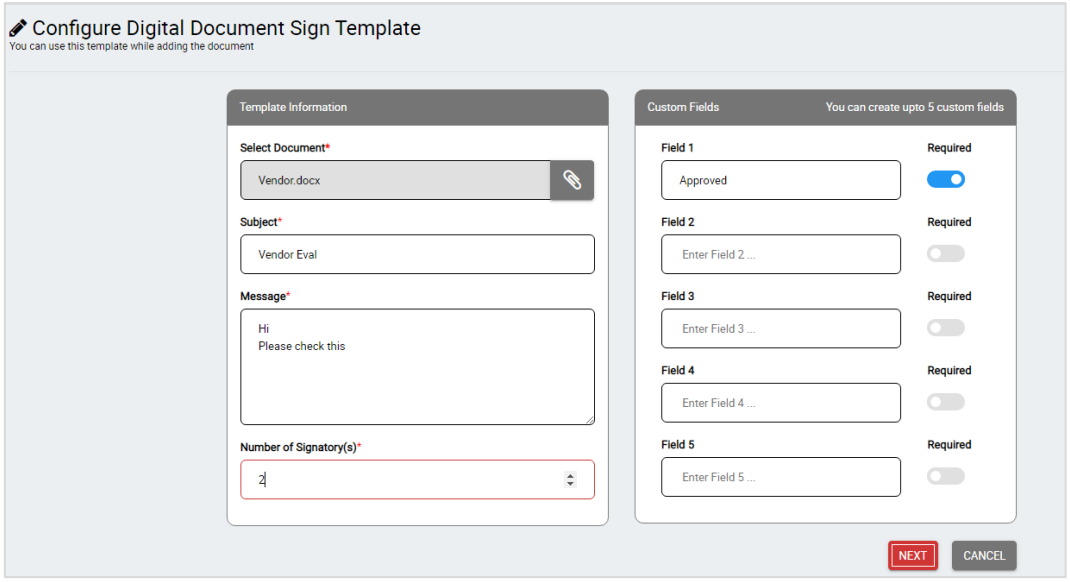
7.1.4.3. Adding Templates

The Configure Document templates section lets you add and configure templates to be used for document signing.



1. **Adding Templates**

Click the Add template button. The add template page is comprised of two sections –



a. **Template Information**

1. **Select Document**: Click the 'Pin' icon, browse, and select the required document.
2. **Subject**: Enter the appropriate subject for the template.
3. **Message**: Can contain any additional instructions for the signatories.
4. **Number of Signatories**: Enter minimum number of signatories required to sign a document created from the template

b. **Custom Fields**

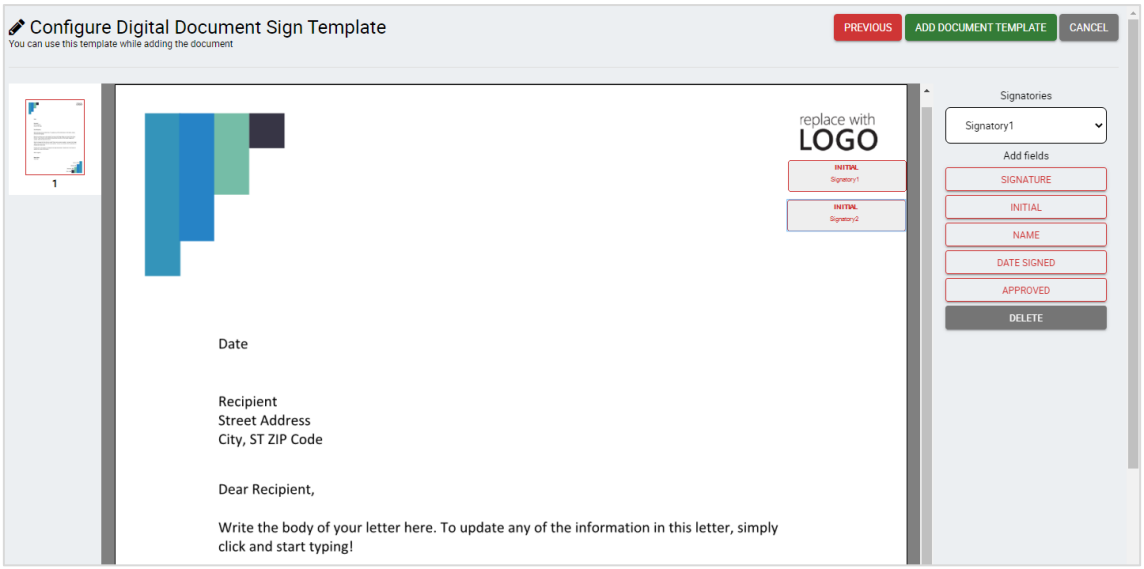
For every template you can configure up to 5 custom fields

1. **Field Name**: Name as users will see while adding document using template
2. **Required**: Enable this slider button to make the field mandatory

Once you have updated the basic document information, click **Next**

c. **Configuring Templates**

After you click Next, the uploaded document is shown in a read-only format.

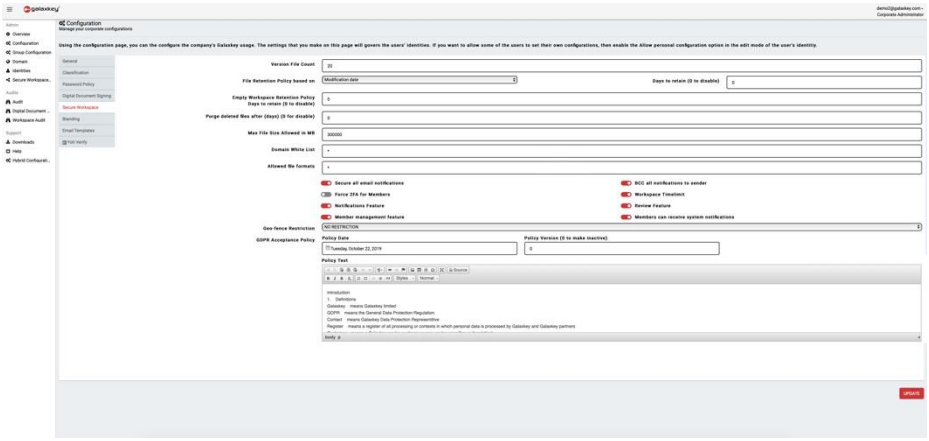


1. The panel on the extreme right of the page provides you with
2. List of signatories (dropdown) as per the count set on the previous page
3. List of placeholders to put on the document
4. Placeholders define the signing positions on the document.
5. For every signatory you must add at least one signature or initial placeholder and the placeholders for mandatory fields
6. All other placeholders are optional
7. Use the **Previous** button to go back to the previous page and make changes
8. Once you have added placeholders, click the Add document template button.
9. The template will now be listed in the Configure Templates section. You can
    a. Download the template
    b. Delete the template
    c. View template information

d. View Template Information

1. Click the '*i*' button to view the template information
2. The information page has two sections -
3. Document – Provides template details like the Template name, id, subject and message.
4. Custom Fields – Provides the details custom fields defined for the template.

7.1.5. Secure Workspaces



This section lets you set up your secure workspaces. The configurations include:

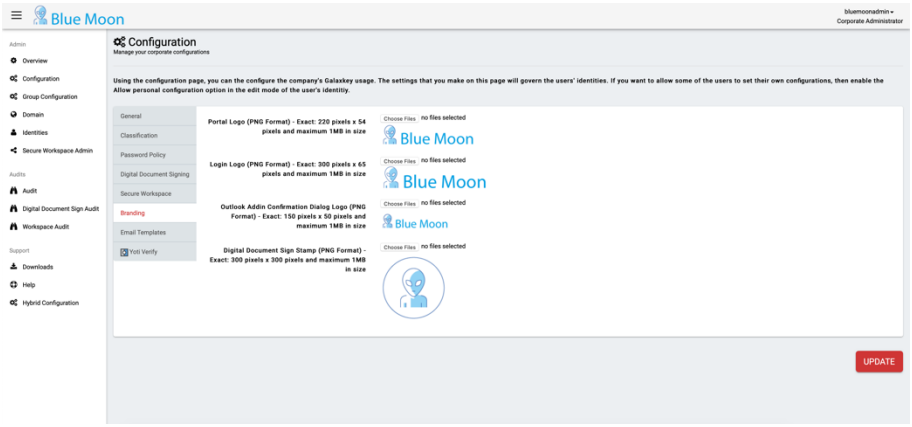
1. **Version File Count**: This setting lets you configure the maximum count of versions of a document that will be maintained in the workspace. When the count exceeds the value set here, the oldest version is removed.
2. **Retention Policy**: The next three settings deal with the retention of files and workspaces in the system.
    a. **File Retention Policy Based on**: This setting lets you define the criterion for maintaining a file in the system. Select one of – **Modification Date** or **Creation Date** from the dropdown list.
    b. **Days to retain (0 to disable)**: Enter the number of days for which the file will be retained in the system before being deleted permanently. This auto-deletion can be disabled by entering 0 (ZERO).
    c. **Empty Workspace Retention Policy Days to retain (0 to disable):** A workspace where no files are present can be retained for the number of days set using this setting. Enter 0 (ZERO) to disable the auto-deletion of the empty workspaces.
3. **Purge deleted files after (days)**: This setting lets you define the number of days after which deleted files are automatically purged. Please note once the files are purged, all history associated with the file is completed purged and not recoverable.
4. **Max File Size Allowed in MB**: This setting lets you define the maximum size of files that can be uploaded in your corporate workspaces.
5. **Domain White List**: This setting lets you create a list of domains (and thus domain users) which can access the files in your workspaces. Enter * (STAR) to allow access to all the domains. Creating a domain whitelist automatically creates a domain blacklist – all domains not listed are in the blacklist.
6. **Allowed file formats**: This setting lets you create a comma-separated list of extensions or file formats that can be uploaded to your corporate workspaces. This is a pre-populated list that can be modified to suit your requirements.

7. **Secure All Email Notifications**: Galaxkey lets you send notification emails to the Workspace members whenever there is a significant activity, e.g., new file uploaded. This setting lets you configure if these notifications should be sent as secured emails. When this setting is enabled, the 'Secured' check box at the bottom of the email is selected by default. Users can uncheck it, as per their liking. This setting is enabled, by default.
8. **Bcc all notifications to sender**: This setting lets you configure whether the sender of the notifications receive a copy. When enabled, the Bcc check box on the email form is selected by default. The sender can reset it to their liking.
9. **Force 2FA for members**: This setting lets you force workspace members be authenticated with 2FA before they can access any workspace that is shared with them.
10. **Workspace time limits:** This setting will enable the option in workspace definition to set time limits. Time limits are used to configure time after which the workspace is not visible to members. The workspace would still be accessible to the workspace owner.
11. **Notifications Feature:** Enable this option if you would like to enable the notifications features for workspaces. Notifications are system generated messages when members perform actions in workspace.
12. **Review Feature:** Enable this option to enable review functionality for workspaces. Workspace members can then add members to the workspaces who can only review. After the files are added, the have to be manually enabled for review even if the workspace owner adds a member with review functionality.
13. **Member Management Feature:** Enable this option if the workspace owner wants to delegate member management rights to members in the workspace. With this option enabled, workspace owners can enable members who can further add members from their same domain with their same access rights. This feature is useful when members from another company are invited and they want to delegate some other member in their organisation to access this workspace.
14. **Members can receive notification emails:** This option provides the ability for members to be enabled to receive system notifications.
15. **Geo-fence Restriction**: The **Geo-fence Restriction** option lets you create a whitelist of sorts. You can select the geographical regions (and thus, IP addresses) from which the secured files can be accessed. The default setting for this is '**No Restriction**', which makes the secured file available in all the regions.
16. **GDPR Acceptance Policy**: This section lets you upload and edit your corporate GDPR policy. When a user logs in for the first time to the corporate workspaces, the user will have to read and accept the GDPR policy. The policy review and acceptance will also be shown on subsequent updates to the policy version number.
    a. **Policy Date:** This setting lets you select the date on which the GDPR policy is added or modified.
    b. **Policy Version (0 to make inactive)**: Enter the version number of the policy. This setting is particularly important when the policy is edited overtime.

c. **Policy text**: This is the option to enter and format your GDPR policy.

7.1.6. Corporate Branding

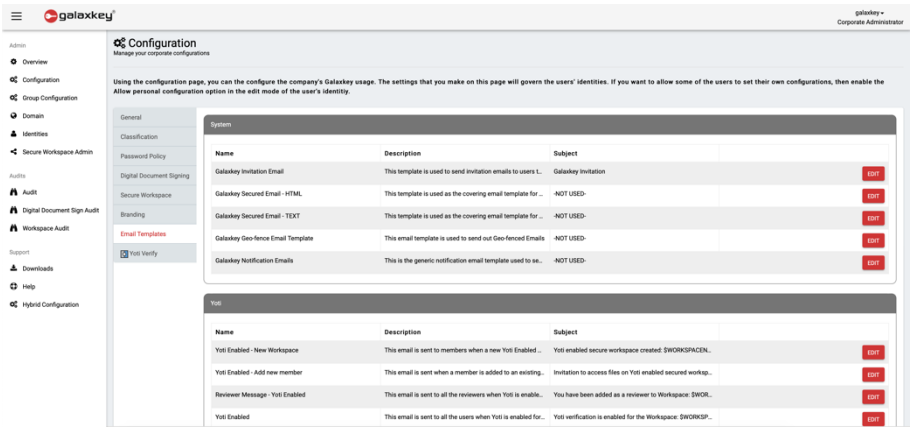
Galaxkey can be deployed with your corporate branding. This benefits the organisation from a marketing and security perspective. You can completely white-label Galaxkey by uploading your corporate logo in the following fields.



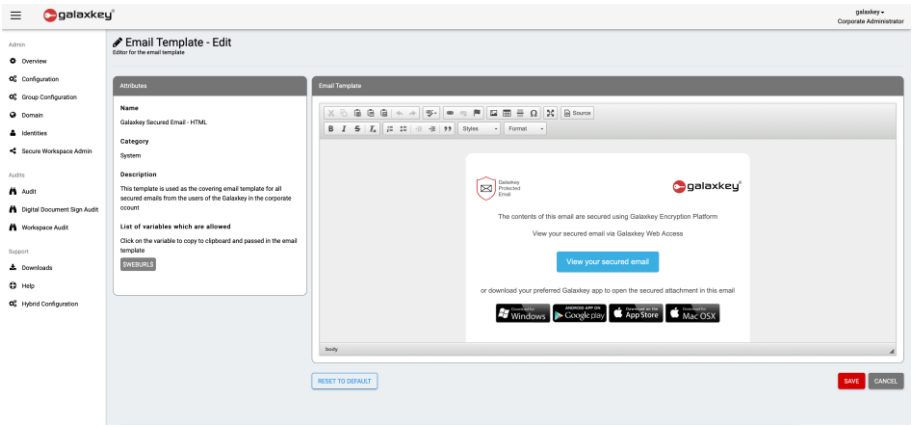
1. **Portal Logo**: The logo uploaded here will be displayed in the top left side corner after the user logs in. Upload a '**.png**' file with a size up to 1 Mb and a dimension of exactly 220 pixels x 54 pixels.
2. **Login Logo**: The logo uploaded here will be displayed on the login page and the confirmation pages on the portal. Upload a '**.png**' file with a size up to 1 Mb and a dimension of exactly 300 pixels x 65 pixels
3. **Outlook Add-in Confirmation Dialog Logo**: The logo uploaded here will be displayed in the left bottom of the **Confirmation** dialog box when the user sends a secured email using Galaxkey Add-in for MS Outlook. Upload a '**.png**' file with a size up to 1 Mb and a dimension of exactly 150 pixels x 50 pixels.
4. **Digital Document Sign Stamp**: You can insert corporate stamp while signing documents using Galaxkey Digital Document Sign. Upload the stamp image with a size up to 1MB and dimensions exactly 300 pixels x 300 pixels here.

7.1.7. Email Template Configuration

This section helps you to configure certain emails, including the content and the look of the system emails. You can configure the following emails.



Galaxkey provides all the emails sent out to their users and customers to be configured as per the corporate branding. The Email templates section lists all the emails as per functionality. The description of all the email templates provide the purpose of the template and using the EDIT button, the template can be configured as per requirement.

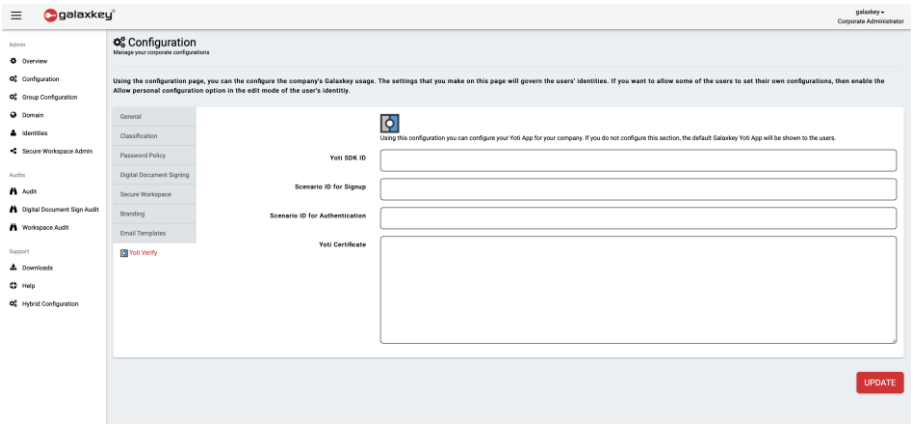


When the user selects the EDIT button, he is shown with an html editor where the complete look and feel of the email change be changed. On the left of the editor panel is the list of variables that are required to be used in the template. These variables are mandatory for the template shown. Using the Source button on the tool bar of the template, the administrator can use HTML code to tweak the template as desired.

There is a button called “RESET TO DEFAULT”. If this button is clicked, the system defined default template is reset into the template and the administrator can modify as required. Once all modifications are completed, press the SAVE button to complete the editing of the template.

7.1.8. Yoti Verify

This option is shown only if your company has purchased the license of Yoti. This section lets you define your Yoti account details.



The Yoti business account details that are specified in this section are used for verifying and authenticating users to your corporate account. This section is optional. If you do not configure, the default Galaxkey Yoti Business account is used to authenticate and verify users. The configured Yoti business account is also used in Workspaces when a workspace is enabled for Yoti verification. It is important that corporates configure this section as the users will see your corporate logo when they are verifying themselves when verifying for Yoti Emails and Yoti enabled workspaces.

7.2. Group Configuration

Galaxkey is configured to allow the Corporate Administrator to define corporate policies centrally, based on User Groups. A system generated 'DEFAULT GROUP' is created by default.

This feature enables the corporate to control the client behaviour based on user roles, accessibility and the assigned licences.

7.2.1. Groups

The access management in Galaxkey is based on **User Groups** created in the system. Galaxkey comes with a pre-defined group – DEFAULT GROUP. You can add more groups as per your organisational requirements.

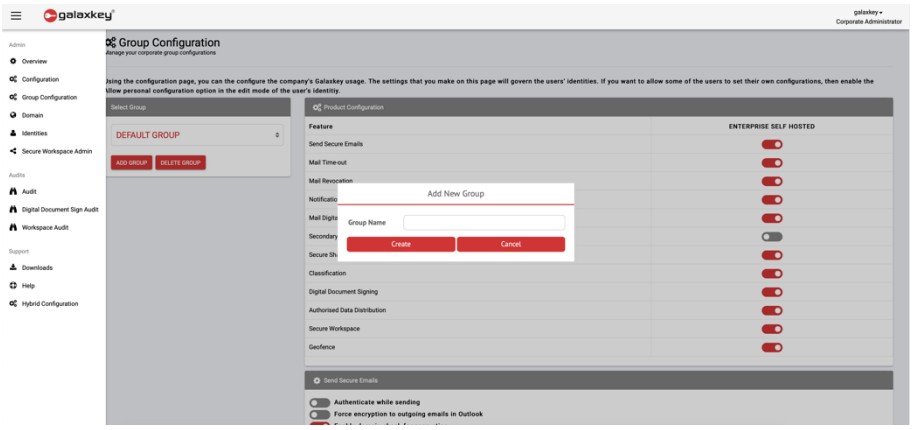
If you have implemented SSO, you can import the groups defined in your Active Directory and manage Galaxkey access rights using the AD groups.

7.2.1.1. Adding New Groups

In addition to the system generated '**DEFAULT GROUP**', you can add other groups manually via Group Configuration.

To add a new group:

1. Click the '**Add**' button.



2. On the pop-up window, enter the group name and click ‘Create’.
3. Click ‘Update’ at the bottom of the Group Configuration page.

This newly created group is then listed in the **Identities** module and is available for mapping with the new and existing users.

In case of AD Integration with Galaxkey, you can import the AD Groups using the Galaxkey Active Directory Connector (GADC) during synchronisation.

7.2.1.2. Access Control using Groups

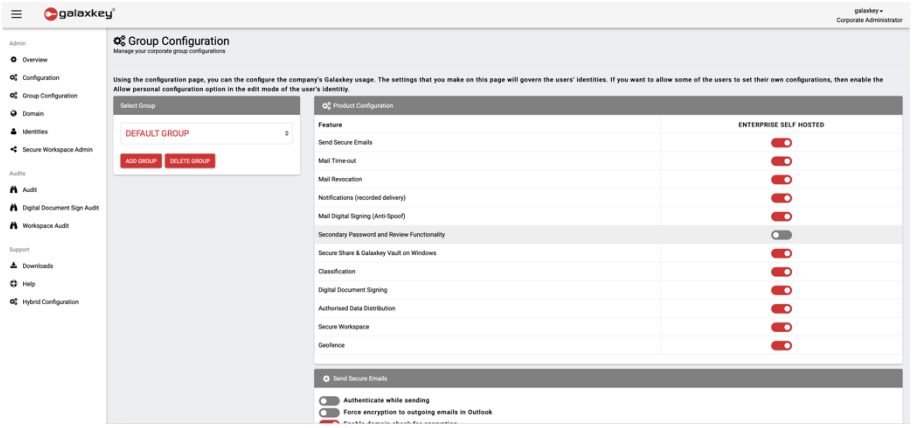
The groups, thus created, can be associated with every active Galaxkey Identity [Galaxkey Manager > Identities] while adding a new identity or at a later stage.

All these groups are available in the ‘**Select Group**’ drop-down on the Group Configuration page.

You can select the required group and configure Galaxkey for each group as described in the following sections.

7.2.2. Product Configuration

Every Galaxkey Subscription licence has a **Product** associated with it. Every product offers a set of features. Using this section of the Group Configuration, you can configure whether the members of a selected group can use these features.



All these features can be enabled or disabled using the slider buttons. The list of features is as follows: (Please note the display of the features are dependent on the licenses you have purchased)

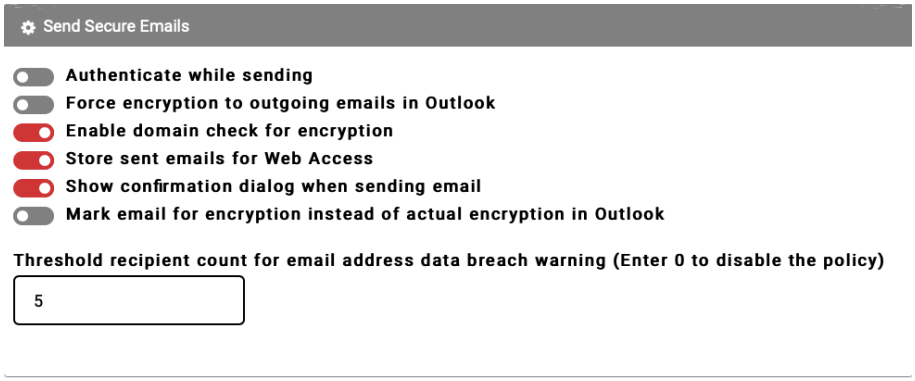
Feature	Description	Effect
Send Secure Email	Send secured emails from the clients. This setting is enabled by default.	When enabled, you can configure more security settings under the '*Send Secure Mails*' section.
Mail Time-out	Set a validity duration and expiry date for the secured emails. This setting is enabled by default.	When enabled, the members of this group can set the 'Valid From' and 'Valid To' time while sending a secured email.
Mail Revocation	A Galaxkey secured email can be recalled, i.e., revoked by the owner (sender) of the email. When this option is selected, all the secured emails are marked as 'Revocable' by default.	When enabled, the user can use the 'Revoke' option from the Galaxkey toolbar or the Galaxkey context menu to revoke an email.
Notifications (recorded delivery)	Users can request a read-receipt for a secured email they send.	When enabled, the users can see a Notification checkbox on the Confirmation dialog box while sending secured emails.
Mail Digital Signing (Anti-Spoof)	Users can insert a Digital Signature to establish the authenticity of the sender's identity.	When enabled, 1. The **administrator** must configure '**Subject prefix for digitally signed emails**' under the *Mail Digital Signing (Anti-Spoof)* section that is enabled by the same name. 2. The **sender** can see a Sign checkbox on the

		confirmation dialog box while sending secured emails.
Secondary Password and Review Functionality	Users can review attachments and enable two-factor authentication for emails with attachments.	When enabled, 1. The **administrator** must configure the '**Message for the secondary password prompt**' under the *Secondary Password and Review Functionality* section. 2. The **sender** can see a list of attachments and a 'Password Protect' checkbox on the confirmation dialog box while sending secured emails. 3. The **recipient** must provide the secondary password to open the secured email in addition to the Galaxkey password.
Secure Share & Galaxkey Vault on Windows	Enables secure file sharing and storage.	When enabled, 1. Under the section *Secure Share & Galaxkey Vault on Windows* the **administrator** must manage access rights (grant or revoke) of users to a. Cloud Synchronisation b. Secure (files on desktop) c. Restore (files on desktop) d. Secure for (selected users) e. Galaxkey Vault Users can secure, share and store files securely based on the access rights granted.
Classification	Allows manual classification of emails based on the data's sensitivity.	Users can view the Classification button on the Compose window and a drop-down to select the classification from the confirmation dialog box.
Digital Document Signing	Enables the Secure Wet Signing of digital documents.	The Secure Sign menu option is enabled in the Galaxkey manager for the users to sign documents electronically.

Authorised Data Distribution	Enables the Forward block (and permission cycle) and Reply block features when sending secured emails.	Users can set Forward block and Reply Block for the secured email from the confirmation dialog box.
Secure Workspace	Enables the access to corporate Secure Workspaces	Users can see the Secure Workspaces menu option in the left-hand tree menu. The *Secure Workspace* section also allows you to manage the rights to create and delete the corporate workspaces.
Geofence	Enables the option for Geofencing.	Users can see a Geofence checkbox on the confirmation dialog box. This is a Hybrid-only feature.

A few other sections are enabled and disabled based on the settings in this section. These are as follows:

7.2.2.1. Send Secure Email



This section is enabled when the **Send Secure Emails** feature is enabled for the selected group. This section allows you to configure the Galaxkey Add-in.

1. Authenticate while sending

When this setting is enabled, a field '**Enter password**' is enabled on the confirmation dialog box. The users of the group will have to enter their Galaxkey password while sending secured emails.

2. Force encryption to outgoing emails in Outlook

When this setting is enabled, the users of the group will be forced to send secured emails irrespective of whether the Outlook "Send" or Galaxkey "Secure and Send" button is used.

3. Enable domain check for encryption

When this setting is enabled, the Add-in checks if at least one of the recipients is NOT from the sender's domain and alerts the user to send a secured email.

4. Store sent emails for Web Access

When this setting is enabled, a copy of the encrypted file (.gxk) is stored on the designated Galaxkey server (The Galaxkey cloud, in the case of a cloud set up and the appliance, in the case of a hybrid set up). Thus, the emails are available for the Galaxkey Web Access.

5. Show confirmation dialog when sending email

This setting is enabled, by default.

When this setting is enabled, the users of the group will be able to see the confirmation dialog while sending a secured mail. The confirmation dialog allows the user to edit the security options to be associated with the secured email.

If disabled, the secured email will be sent directly without an option for assigning any of the security options.

6. Mark email for encryption instead of actual encryption in Outlook

When this setting is enabled, a tag is inserted in the email header instead of securing the email in Outlook.

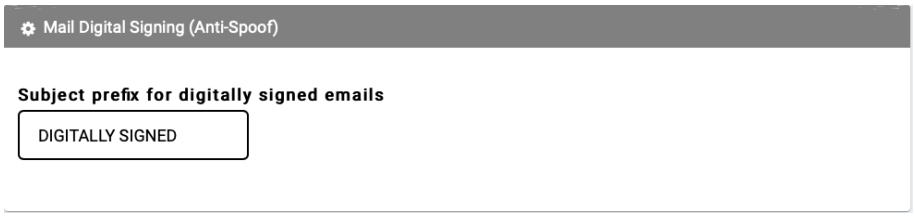
These mails are then secured in the Gateway component (Galaxkey Secure Gateway).

7. Threshold recipient count for email address

This setting monitors the count of recipients from other domains when sending an email. If the count exceeds the number set here, the sender will be alerted and suggested to move the recipients in Bcc.

You can disable this setting by entering ZERO (0).

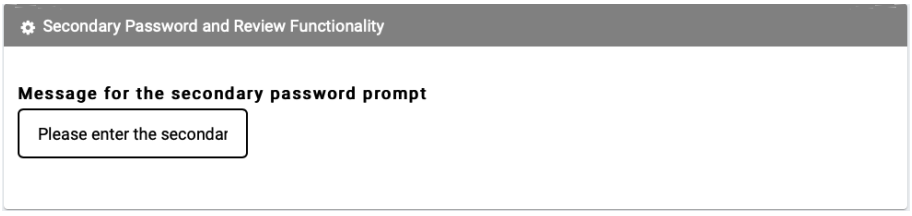
7.2.2.2. Mail Digital Signing (Anti-Spoof)



This section lets you configure the visual label in the subject line of a digitally signed email.

In the **Subject prefix for digitally signed emails** text box, enter the text prefix that must be shown in the email subject when users insert digital signature in the secured email.

7.2.2.3. Secondary Password and Review Functionality



This section lets you configure the message to be shown on the password prompt when users (recipients) try to open the secured email secured using the secondary password.

Enter a suitable message in the '**Message for secondary password prompt**' text box.

7.2.2.4. Secure Share & Galaxkey Vault on Windows

This section lets you configure the file sharing access rights to be granted to the users. Use the slider buttons to grant or revoke the access to file sharing options.

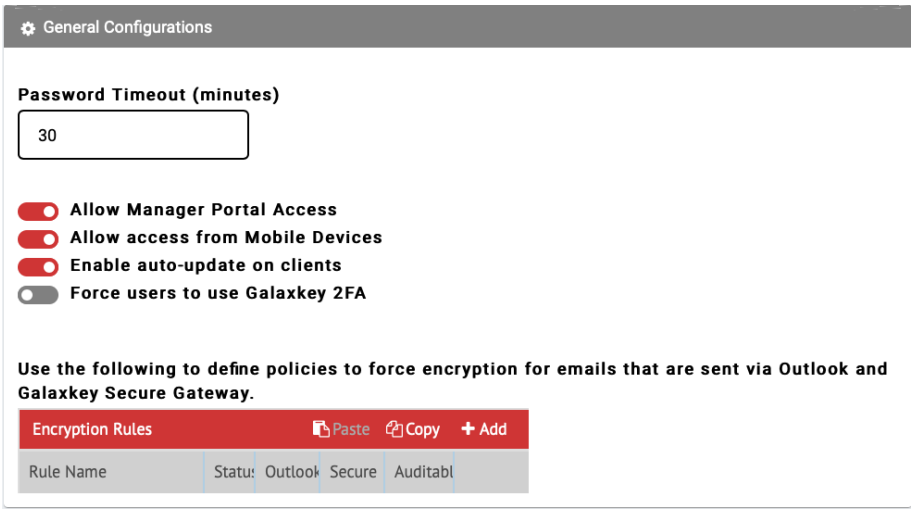
7.2.2.5. Secure Workspace

This section lets you define if the users of the selected group can create or delete a workspace. Use the slider buttons to change the preferences.

7.2.2.6. Yoti Verify

This section lets you enable or disable Yoti verify functionality for users in Workspace and Email clients.

7.2.3. General Configuration



This section lets you configure the advanced access security to Galaxkey.

7.2.3.1. Password Timeout

The Password Timeout defines the time for which the password is stored in memory before the user must re-authenticate to use the functionality in the clients.

This is an important security feature which prevents any unauthorised use of your Galaxkey account.

The default timeout is set to thirty (30) minutes but can be changed to anything below or above this default time. Please note that the time you enter here should be in minutes.

Thus, if you set the timeout to 30 minutes, the user will have to re-authenticate after every 30 minutes of idle time.

The setting is disabled if you enter ZERO (0).

7.2.3.2. Allow Manager Portal Access

The Corporate Administrator can grant (or revoke) user privileges to access secured emails and documents over the web using the Galaxkey Manager Portal.

This setting is enabled by default. Move the slider button to the **left** to revoke the access.

The members of the group for which the access is revoked will not be able to access the secure emails and documents via Galaxkey Manager Portal and will have to rely on the clients to access their secured data.

7.2.3.3. Allow Access from Mobile Devices

The Corporate Administrator can grant (or revoke) user privileges to access secured emails and documents using the Galaxkey clients on hand-held devices.

This setting is enabled by default. Move the slider button to the **left** to revoke the access.

Thus, the members of the group for which the access is revoked will not be able to access the Galaxkey clients on the hand-held devices, viz., iOS and Android. Such users will have to rely on the web, Galaxkey Add-in for Outlook and Galaxkey for Mac clients to access their secured data.

7.2.3.4. Enable Auto-updates on clients

If this option is enabled, the Galaxkey clients installed on the machines of the corporate users will automatically update whenever Galaxkey releases a new version.

The Corporate Administrator can enable this option if the Corporate prefers centralised installation.

This option is disabled, by default.

7.2.3.5. Encryption Rules

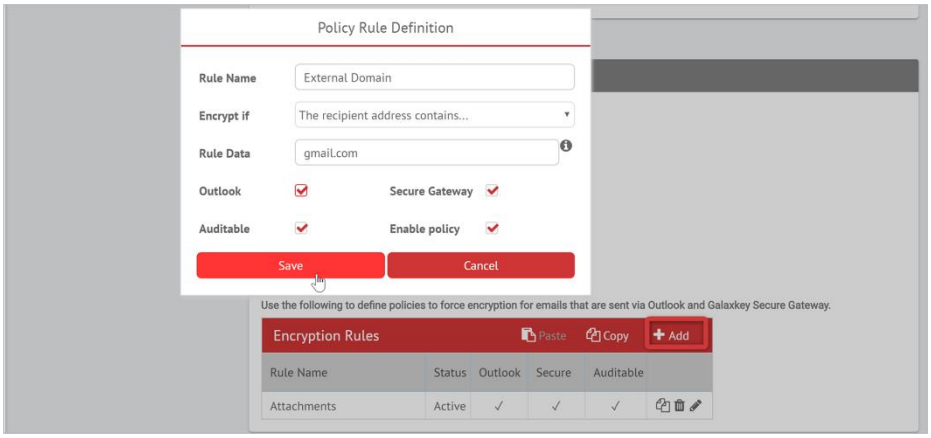
Email is widely used to share personal and official information which must be safeguarded. Galaxkey provides a robust solution for this.

Galaxkey provides an option to encrypt emails based on specific conditions (conditional encryption of emails). You can create a set of rules, which will be evaluated whenever an email is sent using the Outlook '**SEND**' button.

These policies are based on multiple attributes like

1. Sender
2. Recipient
3. Subject of the email
4. Content (body) of the email
5. Number and types (extensions) of attachments
6. Certain attributes of the MS Office attachments

Defining a Policy



1. Click 'Add new' to add a new encryption rule.
2. In the pop-up window, furnish all the details as follows:
    a. **Rule Name**: Enter a name of your choice that best describes the rule.
    b. **Encrypt If**: Select the appropriate condition from this drop-down list of twelve conditions.
    c. **Rule Data**: Enter valid data to match the selected rule condition.

The following table outlines the rule conditions available in Galaxkey and the expected rule data for each.

Rule Condition	Rule Data
The Sender is	Enter a valid email address
The Sender address contains	Enter a valid part of an email Id or a regular expression for email address.
The Recipient is	Enter a valid email address
The Recipient address contains	Enter a valid part of an email Id or a regular expression for email address.
GSG only - The email header contains	The rule data here is implied. This condition is applicable exclusively to Galaxkey Secure Gateway (GSG).
The subject contains	Enter any text or a regular expression, which if matched, the email should be encrypted.

The body contains	Enter any text or a regular expression, which if matched, the email should be encrypted.
The body contains any credit card number	The rule data, in this case, is implied. Galaxkey validates most of the standard credit cards.
The email contains one or more attachments	The rule data, in this case, is implied. Galaxkey will secure the email if there is at least one attachment to the email.
Office attachment classification contains	Enter the Property Name and value separated by a colon. (Group: Galaxkey)
Any email attachment file name contains	Enter any text or a file extension, which if matched, the email will be secured.
Triggered by classification software	This rule is exclusively applicable to Galaxkey Add-in for Outlook only.

The simple text rule data is case insensitive.

When the rule data is a regular expression, prefix the search expression with the word 'REG:' e.g. REG:^[A-Z0-9._%+-]+@[A-Z0-9.-]+.[A-Z]{2,}$

The form displays the following four checkboxes

1. **Outlook**: You can select whether the rule will be evaluated in Galaxkey Add-in for Outlook.
2. **Secure Gateway**: You can select whether the rule will be evaluated in Galaxkey Secure Gateway.
3. **Auditable**: When selected, logs for successful evaluation and application of the rules will be generated.
4. **Enable Policy**: You can decide whether the policy will be active and available for evaluation in the clients.

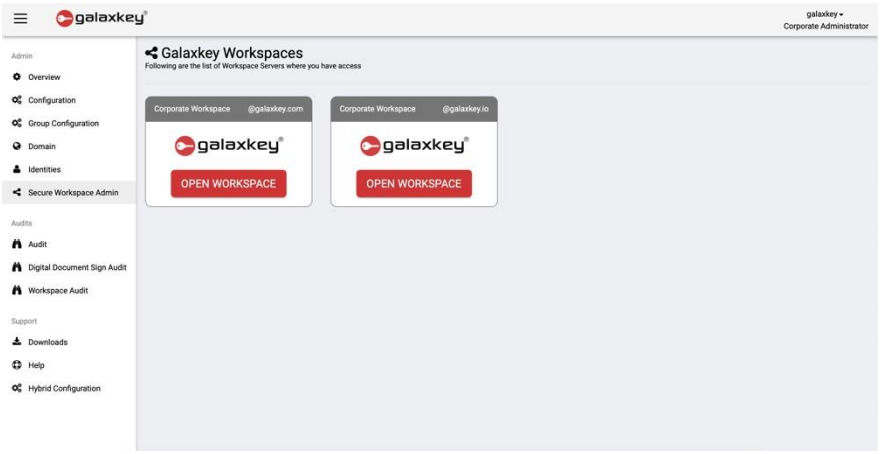
All the checkboxes are selected by default.

Once you have completed the configurations, save the data on the form and click the 'UPDATE' button to save all your configurations.

The configurations will take effect only when you restart the client applications.

Section 8. Secure Workspace Admin

Using the secure workspace admin, administrators can manage workspaces that are configured for the corporate account. This option is available only if the Workspace licenses is enabled for the corporate account.



The page lists all the workspaces configure for the corporate admin for the domains.

The administrator has only limited functionality for each workspace.

When the user clicks the **OPEN WORKSPACE** button, the administrator is taken to the administrative portal of the workspace for the domain shown on the top right corner of the Workspace box.

Section 9. Downloads

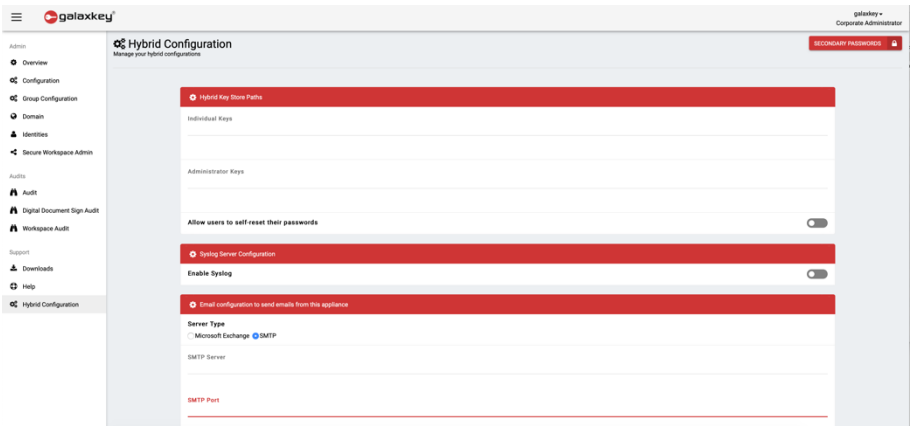
The **Downloads** module serves as the download centre for all the standard Galaxkey software.

For the Corporate Administrator, there is an additional tab under the Downloads called **Additional Downloads.** The additional downloads section provides additional resources which you can use in accordance with the copyrights of Galaxkey.

Apart from additional binaries, there are PowerPoint Presentations and Datasheets. We suggest you use these for evaluation purposes.

Section 10. Hybrid

The Hybrid module is available only for corporate customers who have installed the Galaxkey Appliance in Hybrid mode.



The Hybrid menu allows the Corporate Administrator to configure the hybrid appliance. It lets the Corporate Administrator configure the path to the keys store and the syslog server.

10.1. Hybrid Key Store Path

Galaxkey in hybrid mode stores the private keys inside the corporate users' network. The keys never leave the network. The appliance accesses the keys locally. This option lets you configure the path where the keys will be stored.

The **Individual Keys** is the path to the keys folder where the individual users' keys are stored.

The Administrator keys is the path to the keys folder where the administrator's keys are stored.

Enable authentication is the NTLM authentication to access the keys folders. This is optional.

10.2. Syslog Server Configuration

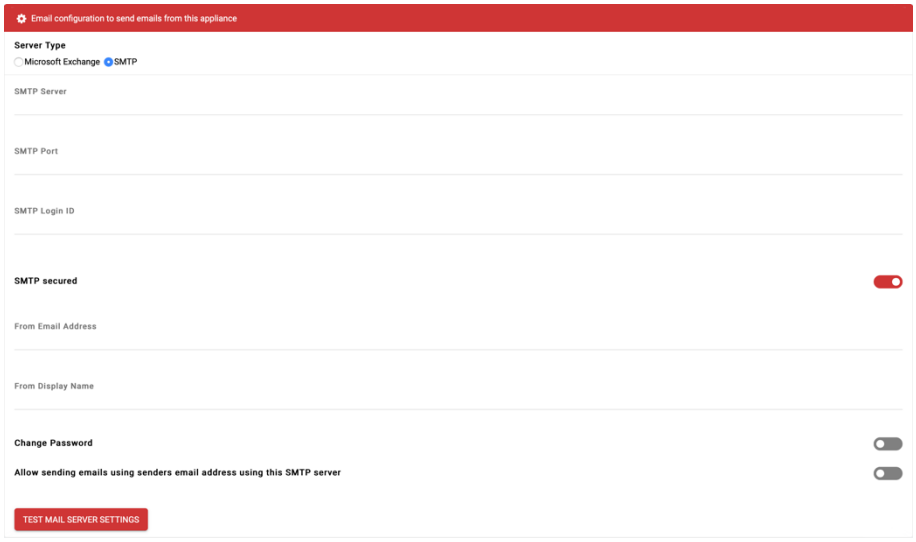
The Syslog Server Configuration lets you configure auditing to the syslog server. The option lets you configure the IP address to the syslog server and the listening port.

Using this option, you can configure Galaxkey to record live audits to any SIEM server which supports Syslogs.

10.3. Email Configuration to Send emails from this appliance

This email configuration enables the hybrid configuration to set an email server that will be used to send out emails and Galaxkey Notifications. The settings are as follows.

1. **Mail Server Type**: Select one of the two server types – **Microsoft Exchange** or **IMAP**. Based on this selection, you must set-up the following:



2. In the case of Microsoft Exchange, enter the Exchange Webservices URL in the format ***https://mail.acme.com/EWS/Exchange.asmx***.
3. In the case of **IMAP**, enter the **IMAP Server**, **IMAP Server Port**, and enable the **SMTP Secured** setting to opt for a secure connection.
4. Enter the email Id from which you want to send the system emails in '**From Email Address**' and the display name in the '**From Display Name**' fields.
5. In both cases, you must provide your **Login ID** and **Password** to the email server. You can change the password at a later stage.
6. The "**Allow sending emails using senders email address using SMTP server**" setting is used to enable emails to be sent directly by the sender's email address. This option should not be used if the server does not support relay of emails for domain users.

Use the '**Test Mail Server Settings**' to ensure the settings are correct before updating.

10.4. Galaxkey Secure Storage

Galaxkey supports the upload of emails to a local appliance folder instead of AWS. You can use this section to configure the local secure storage.

You should update the following settings

1. **Private Key**: Enter the value as provided by Galaxkey.
2. **Private Value**: Enter the value as provided by Galaxkey.

3. **Folder for Galaxkey Secure Share**: Path of the appliance folder where your emails will be stored.
4. **Enable Authentication**: Select this checkbox if you want to enable additional authentication, like
    a. Domain / Host Name
    b. Username
    c. Password

10.5. Digital Document Sign

Galaxkey supports applications where users can electronically sign a secured digital document. The electronic signatures are saved in the database. You can choose to associate one of the following database server types with Galaxkey.

1. MySQL
2. MS SQL

After you have selected the appropriate DB Server, enter the connection string in the '**Connection String for Secure Sign Audit Logs**'. The connection is disabled when this field is blank.

10.6. Secure Collaboration

Galaxkey Secure Workspace allows for the secure collaboration. This section lets you configure the server folder settings for the enterprise.

Enter the path where the fields are stored for editing in the **Path to store temporary checked out collaboration files.**

The **Secure Collaboration Server Folder Settings** section lets you configure the path where files will be uploaded and assembled. This path will be different for each domain in the corporate.

10.7. Authentication Options

Galaxkey supports integration with Active Directory, Azure and Okta. When either of these is enabled, users need not remember multiple passwords. Additionally, users can by-pass repeated authentication to access secured emails.

10.7.1. Active Directory Integration

You can enable **LDAP** authentication for Galaxkey so that the user does not need to remember multiple passwords and need not repeatedly authenticate to access Galaxkey secured emails.

The following options are available when you select the Active Directory option

1. **Path to Active Directory**: Enter the path to Active Directory in the format – LDAP://DC=onecity,DC=Corp,DC=Fabrikam,DC=com
2. **Email property Name in Active Directory**: Enter the appropriate property name to be mapped with the Galaxkey identity.
3. **Prompt to ask for AD credentials**: Enter the text to be shown when the system asks for AD credentials.
4. **AD Service Account**: Enter the Service Account identity.
5. **AD Service Account Password**: Enter the password for the Service Account.

10.7.2. Okta Integration

You can enable Okta authentication for Galaxkey so that the user does not need to remember multiple passwords and need not repeatedly authenticate to access Galaxkey secured emails.

The following options are available when you select the Okta option

1. **Okta URL for JSON Authentication**: Enter the appropriate Okta URL for authentication
2. **Path to Active Directory**: Enter the path to Active Directory in the format – LDAP://DC=onecity,DC=Corp,DC=Fabrikam,DC=com
3. Email property Name in Active Directory: Enter the appropriate property name.
4. **Prompt to ask for AD credentials**: Enter the text to be shown when the system asks for AD credentials.
5. **AD Service Account**: Enter the Service Account identity.
6. **AD Service Account Password**: Enter the password for the Service Account.
7. **Okta Single Sign On URL**: Enter the appropriate URL for signing.
8. **Okta provider Issuer**: Enter the name of your issuer.
9. **Okta x**.509 Certificate: Enter the path of the certificate.
10. **Okta IDP metadata** (Optional): Enter the metadata.
11. Service Provider PKI Certificate Password: Enter the path of the PKI certificate.

10.7.3. Azure AD Integration

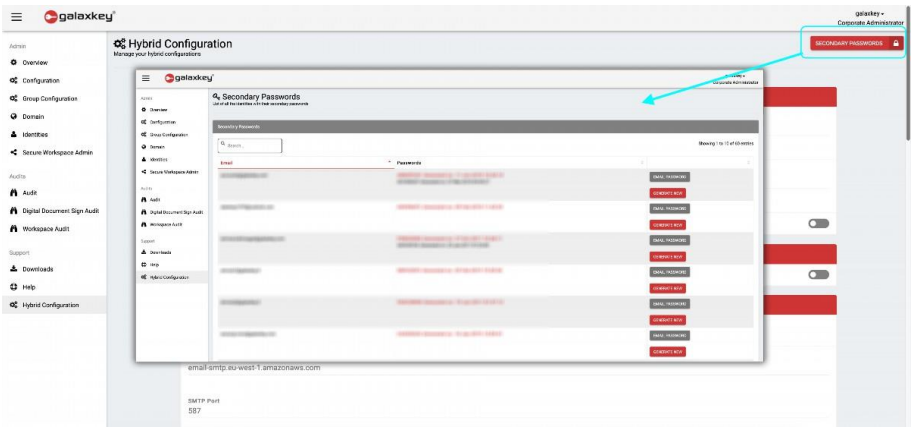
You can enable Azure AD authentication for Galaxkey so that the user does not need to remember multiple passwords and need not repeatedly authenticate to access Galaxkey secured emails.

The following options are available when you select the Azure AD option

1. **Azure AD URL for JSON Authentication**: Enter the appropriate Okta URL for authentication
2. **API Token**: Enter the API token.
3. **Azure AD Single Sign On URL**: Enter the appropriate URL for signing.
4. **Azure AD provider Issuer**: Enter the name of your issuer.
5. **Azure AD x**.509 Certificate: Enter the path of the certificate.
6. **Azure AD IDP metadata** (Optional): Enter the metadata.
7. Service Provider PKI Certificate Password: Enter the path of the PKI certificate.

10.8. Secondary Password

Secondary Password is an integral part of the two-tier authentication for emails with attachments.



This section stores the system generated Secondary Passwords. You can change the Secondary Password using the '**Generate New**' button.

You can also email the password to the recipient using the '**Email Password**' link.