



Galaxkey

User Guide: Corporate Administrator

Version 5.0

Table of Contents

[Section 1. Copyright 4](#_Toc484101381)

[Section 2. Executive Summary 5](#_Toc484101382)

[2.1. About Galaxkey 5](#_Toc484101383)

[2.2. Corporate Administrator Guide 5](#_Toc484101384)

[Section 3. Corporate Administrator 6](#_Toc484101385)

[3.1. Overview 6](#_Toc484101386)

[3.2. URL for Management 6](#_Toc484101387)

[Section 4. Domain Management 7](#_Toc484101388)

[4.1. Domain Module 7](#_Toc484101389)

[4.1.1. Adding New Domain 7](#_Toc484101390)

[4.1.2. Managing Galaxkey Web Access Option 8](#_Toc484101391)

[Section 5. Corporate Identity Management 9](#_Toc484101392)

[5.1. Adding New Identities 9](#_Toc484101393)

[5.1.1. Registering via Identities Module 10](#_Toc484101394)

[5.1.2. Registering via Galaxkey Active Directory Connector 11](#_Toc484101395)

[5.2. Managing Existing Identities 11](#_Toc484101396)

[5.2.1. Active 12](#_Toc484101397)

[5.2.2. Active – Reset Password 12](#_Toc484101398)

[5.2.3. Active – Service Account & Administrative Rights 13](#_Toc484101399)

[5.2.4. Inactive 13](#_Toc484101400)

[5.2.5. Acceptance Required 14](#_Toc484101401)

[5.3. Identity Backup and Maintenance 14](#_Toc484101402)

[Section 6. Galaxkey Configuration 15](#_Toc484101403)

[6.1. Configuration 15](#_Toc484101404)

[6.1.1. General Configurations 15](#_Toc484101405)

[6.1.2. Password Policy 17](#_Toc484101406)

[6.1.3. Corporate Logo 17](#_Toc484101407)

[6.1.4. Email Template Configuration 18](#_Toc484101408)

[6.2. Group Configuration 19](#_Toc484101409)

[6.2.1. Microsoft Windows & Outlook Add-in Configuration 19](#_Toc484101410)

[6.2.2. Galaxkey Client Policy 22](#_Toc484101411)

[6.2.3. Galaxkey Secure Share 23](#_Toc484101412)

[6.2.4. Policy Manager 23](#_Toc484101413)

[Section 7. Downloads 26](#_Toc484101414)

[Section 8. Hybrid 27](#_Toc484101415)

[8.1. Hybrid Key Store Path 27](#_Toc484101416)

[8.2. Syslog Server Configuration 27](#_Toc484101417)

[8.3. Email Configuration to send emails from this appliance 27](#_Toc484101418)

[8.4. Galaxkey Secure Storage 28](#_Toc484101419)

[8.5. Secure Sign 28](#_Toc484101420)

[8.6. Authentication Options 29](#_Toc484101421)

[8.7. Secondary Password 30](#_Toc484101422)

# Copyright

© Copyright Galaxkey® Limited. All rights reserved. Galaxkey Limited, the Galaxkey logo, Galaxkey are registered trademarks of Galaxkey Limited in the Europe and other countries. All other Trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Galaxkey Limited assumes no responsibility for any inaccuracies in this document. Galaxkey Limited reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

# Executive Summary

## About Galaxkey

Galaxkey provides an identity based email content security solution. When a user registers with Galaxkey, a security identity is created which is associated with the user’s email address. This identity is managed and stored by Galaxkey in the cloud and is accessible to any Galaxkey enabled client on proper authorisation and authentication. The identities on the platform are completely secured with user provided unique credentials; ensuring secure user access. The administrators of corporate users have full control of their corporate user’s identities and data.

With advances of networking and communication technologies, e-mail has established itself as a formal communication medium. E-mail as a medium has gone past the mere communication tool and is being used for communicating confidential information including official documents ranging from notices, invoices and confirmations to name a few. These developments also raise issues surrounding email security and privacy of data. E-mail is highly susceptible to various forms of attack, starting at the e-mail source point, onto the corporate server, including the stages in between, to the recipient’s server and finally the destination point. The risk of attack increases multi-fold at each point. There are various solutions offered to counteract these vulnerabilities at various points. These solutions offer a partial solution. However, a robust solution that addresses all the vulnerabilities and still maintains ultimate control with the end user, the sender and receiver is desirable. This is the solution Galaxkey provides.

Galaxkey offers security solutions using state of the art technology to secure e-mail end-to-end and not only in transit but at the source and at the destination while maintaining control with the end user through proper authentication.

## Corporate Administrator Guide

This document, the Corporate Administrator Guide, outlines the functionalities for a Corporate Administrator. The intended audience for this document are the Corporate Administrators.

# Corporate Administrator

## Overview

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

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

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



## 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.

# Domain Management

Domain management in Galaxkey is the process of registering a domain for secured communication, configuring web access for the domain to enable a web-based reader and keeping track of domain's web access installation type.

To start using Galaxkey in a corporate environment, the corporate administrator must first register his 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.

In case the administrator is unable to register a domain due to reasons which mention that the domain is already registered, then send an email to the support team at [support@galaxkey.com](mailto:support@galaxkey.com) and we will investigate and resolve this issue as soon as possible.

## Domain Module

The **Domains** module of Galaxkey Manager provides the interface for domain management.

The primary purpose of this module is to help the corporate register any other domain owned by them and extend Galaxkey security across the organisation.

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

Using this module, you can

1. Add new domain
2. Manage the web access options for the domain

### Adding New Domain

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.

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

Note:

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

### Managing Galaxkey Web Access Option

Galaxkey Web Access is the Galaxkey Web client for viewing and sending Galaxkey secured mails.

The client being web based, the user can easily access it via any of the browsers.

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

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

To enable GWA for a corporate domain:

On the ‘**Edit Domain**’ page, check the ‘**Advance Configurations**’ check-box.

In the GWA URL, enter the URL to the GWA server that is installed on your premises.

In case, there is no in-house GWA installation, the mails can be accessed over the web via <https://gwa.galaxkey.com> .

Note:

In order to access the Galaxkey Secured e-mails over the web, the **CONFIGURATION > Group Policies > 3.Galaxkey Secure Share** must be appropriately set.

If you have **NOT** opted for this, your corporate users can save the '.GXK' file locally and open it using the ‘**BROWSE**’ option on the GWA portal.

# Corporate Identity Management

The identities of the users in the corporate are stored in the corporate administrator’s vault which is secured using the administrator’s password.



Corporate identity management encompasses the following

1. Adding Identities of new corporate users.
   1. You can add multiple identities in one go using the **Galaxkey Active Directory Connector (GADC)**
   2. Use the **Identities** module of the Galaxkey Manager to add one identity at a time.
2. Managing existing Users

## Adding New Identities

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

1. Registering via **Identities** module



1. Registering via the Galaxkey Active Directory Connector (GADC)

### Registering via Identities Module

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

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

This is the process of adding individual corporate identities to Galaxkey Manager, **one by one**. For this:

1. Log on to Galaxkey Manager. Go to **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'** dropdown is populated with the domain added while registering the company with Galaxkey. If you have added other domains, you can select the domain from available list.
4. The **'Select the licensing'** dropdown by default displays the valid license.
5. In the **'Email'** field, enter the e-mail 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 dropdown.
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 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 e-mail** is sent to the individual user directing her 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.

### Registering via Galaxkey Active Directory Connector

Adding individual corporate identity to Galaxkey Manager, one by one is a tedious and time consuming task. The GADC, helps you to add to Galaxkey Manager in one go. For this:

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

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

Please refer to the GADC Manual for more details

## Managing Existing Identities

The identities key management is the module where the administrator can manage all the identities. The identities are grouped and displayed in tabs depending on their statuses. Following are the statuses

1. **Active**: Identities listed in this tab are all active and they have a valid license assigned to them.
2. **Inactive:** Identities listed in this tab are all identities which are rendered inactive and the user using this identity cannot open secured emails.
3. **Acceptance Required:** These are identities which are awaiting acceptance from the users to whom the identities have been assigned.

The tabs are shown only if there are valid identities in them. The functionalities on the identities differ on each tab.

### Active

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

The identity can be in one or more than one group which are displayed in comma separated listing.

If the license is assigned to the identity, it is display with the license number and the date when it is expiring. If the identity license is expired, a button appears which allows you to assign a new license to the identity. You can also click on the existing license and change the license if required.

The edit button lets you edit the following identity details

1. Change status from Active to Inactive
2. Change licensing
3. Enter some notes
4. **Enable Allow Personal Configuration** – If you enable this option, the user can manage his 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 case of multiple groups, the maximum security settings override.
6. **Reset password** – explained in later sections
7. **Enable Service Account & Administrative Rights**: With this you can delegate some of your Galaxkey management responsibilities to other users.

### Active – Reset Password

The edit mode facilitates you change the user password using the **RESET PASSWORD**. Since Galaxkey does not store any password, the process of resetting the password is as follows

1. You, the corporate administrator enters his own password
2. Using the admin password, the users’ key is extracted from the admin’s password store.
3. The extracted key is then secured using a temporary password which is emailed to the user.
4. The user must first reset the password once he logins to the portal.

### Active – Service Account & Administrative Rights

This section helps you to delegate administrative rights to a non-admin Galaxkey user. The account to which administrative rights are granted is the '**Service Account**'.

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

1. **Allow ability to reset corporate administrator password**: With this the user, can reset the administrator account password.
2. **Allow ability to manage corporate identities**: Selecting this grants access to the Identities module and thus corporate identity management.
3. **Allow ability to manage corporate domains**: Selecting this grants access to the Domains module and thus Domain management.
4. **Allow ability to manage corporate configuration**: Selecting this grants access to the Configuration module and thus corporate configuration management.

You can choose the administrative rights to be granted to the selected user. The user with Service Account can then see an additional button in the Galaxkey Manager to switch between accounts.

In addition to the administrative rights, this service account is used in Galaxkey Secure Gateway (GSG) for encrypting and decrypting the mails.

### Inactive

The identities in this tab are ones rendered inactive either by GADC or manually by the corporate administrator.

The licenses of inactive users are released and are available for assigning to other corporate users.

You can revert the inactive identities to active. While doing so, license must be reassigned.

You cannot reset password for the inactive identities.

### Acceptance Required

When the corporate administrator adds a new identity, it must be accepted by the user.



An identity is in the ‘**Acceptance Required**’ stage from the time of receipt of 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.

## Identity Backup and Maintenance

The maintenance tab is very crucial for identities management. Using this tab, the administrator can create a backup of all the identities.

It is strongly advised that the administrators take regular backups of the identities.

To perform backup of the identities, the administrator must enter his existing Galaxkey Password and a password to secure the backup files. Once this information is entered, the portal provides a button to download the secured backup file which ends with the extension ‘.GXB’. Please store this backup file securely

Since Galaxkey does not store any passwords, in case the administrator forgets his password, he will need the identities backup to regenerate new password. So it’s advised to do regular backups.

# Galaxkey Configuration

Galaxkey Configuration are made at two levels – corporate and group. While the corporate configurations mainly deal with the look and feel of Galaxkey, the group configurations help you set up Galaxkey to suit your organisation’s security requirements.

Thus, there are two modules:

1. Configuration
2. Group Configuration

## Configuration

The options in the **Configuration** module govern the global policies and look and feel of Galaxkey for the corporate. The configurations in this module can be classified as under:

1. General Configurations
2. Password Policy
3. Logo configurations
4. Email template configurations

The following sections consider each of these in greater details.

### General Configurations

#### Accept Galaxkey 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 such a user.

Using the ‘**Accept Galaxkey Invites from non-admin users’** option, you can control if the users in your organisation are eligible to receive invitations. If you **disable** this option, no user under this domain will be able to receive invitations.

This attribute allows administrators to control their licensing and subscription with Galaxkey.

For example, you have purchased 10 Galaxkey licenses. If you have **disabled** this option, no user other than the 10 you have assigned the licenses 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 licenses accordingly.

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

Galaxkey allows in-house set-up of the appliance and the SMTP server can also be configured on it.

You can now send the invites from this server by checking this option.

#### 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 helps you with the synchronisation.

#### Auto invite functionality for users

Galaxkey works on an invitation model, i.e., invites are sent to people to join the Galaxkey network. Accordingly, Galaxkey can invite all your contacts stored in the ‘Contacts’ folder of Outlook. This auto-invite functionality can be configured under this section.

Select the ‘**Auto invite functionality for users**’ checkbox to enable Galaxkey to invite your contacts.

#### Send Galaxkey invites using SMTP configured on the Hybrid Appliance

When a Galaxkey registered user sends an email to a non-registered user, the latter is invited to join Galaxkey. The sender of this invite is Galaxkey Security. You can opt to send this from your own domain instead.

When this setting is enabled, all the Galaxkey invites sent out by the users in your organisation are sent from your registered domain instead of Galaxkey Security.

#### Enter email for support requests from corporate users

You can restrict the corporate users from resetting their own password. In this case, the password reset request is sent to the corporate administrator.

You can delegate this to any other user by entering the user’s email in the ‘Enter Email for password manager’ text box.

This way all the password reset requests will be redirected to this user. You can choose to keep this blank, so that all the password reset requests will be sent to the corporate manager.

#### Enter the message for Secondary Password

Galaxkey provides a two-tier security to emails with attachments. This is achieved by associating a system-generated password to the email when there is an attachment to the mail.

This setting allows you to configure the message to be shown on the message box for entering the secondary password.

#### Subject prefix for digitally signed emails

Enter your preferred prefix in the ‘**Subject prefix for digitally signed emails**’ text box and save.

This text is added to the subject line of the users’ Galaxkey secured mail when they opt to send a digitally signed mail.

### Password Policy

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

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

Note:

*The Password Policy can be set only when you have an in-house (hybrid) installation.*

### Corporate Logo

Out of the box, Galaxkey can be deployed with your corporate branding. This greatly benefits the organization from a marketing and security perspective. You can completely white label Galaxkey by uploading your corporate logo in the following field:

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 of size upto 1 Mb and dimension 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 of size upto 1 Mb and dimension 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 when the user send a secured email using Galaxkey Add-in for MS Outlook. Upload a ‘**.png**’ file of size upto 1 Mb and dimension exactly 150 pixels x 50 pixels

### Email Template Configuration

This section, as the name suggests, helps you to configure the emails – content and look of the system emails. You can configure the following emails -

#### Email Template for Invitation Email

Galaxkey allows you to send custom message to your invitees.

This option enables you to customise text of the invitation email that is sent out when someone from your organisation sends a secured email to a non-registered user.

Please ensure that the template contains the **$WEBURL$** placeholder**.**

#### Template for Galaxkey Secured Email

The ‘Template for Galaxkey Secure Email’ is used to customise and create a corporate template to be used as the cover page or envelope of the secured mail.

When you check this option, Galaxkey prompts you with an HTML and text editor to create your secured email templates.

You can create any template to suit your needs.

Please ensure that the template contains the **$WEBURL$** placeholder**.** This place holder is replaced with the link to the GWA for the recipient. You need two versions of the template – one (HTML) for Outlook Add-in and iOS and one (Text) for Mac OS X and Android. Hence you have to define the HTML template and the text template.

#### Email Design Template for Geo-fencing Email

Geo-fencing in Galaxkey is a set-up for restricting a secured mail within your premises. The shared users (recipients) of the secured email receive a link to the mail. Using this link the mail can be accessed over the internet via a browser.

Using the HTML editor, you can design a template of your choice. This template will be sent to the recipient(s) of a Geo-fenced mail.

#### Email Design Template for Notification Email

Galaxkey has its own read receipt system in the form of Notifications. When the owner of an email asks for notifications from the shared users, two of the three notifications are sent in the form of formatted emails. The notification emails can be customized using this section.

Please ensure that the template contains the **$EMAIL\_MESSAGE$** placeholder**.**

Click the ‘**UPDATE**’ button once all you have configured Galaxkey to your liking.

## Group Configuration

Galaxkey is configured to allow Administrators to define corporate policies centrally based on user Groups. A system generated ‘DEFAULT GROUP’ is created by default.

You can add other groups manually via Group Configuration.

Groups are also imported by GADC automatically during synchronisation.

This is a very useful feature as it allows the corporates control the client behaviour based on the customer roles.

### Microsoft Windows & Outlook Add-in Configuration

The settings under this section define the behaviour of Galaxkey Add-in for Microsoft Outlook and Galaxkey for Windows. These can be broadly grouped as follows:

1. Related to updates: Enable Auto-updates on Windows
2. Related to display of options: These include:
   1. Confirm before sending secured emails (Confirmation Dialog)
3. Related to how encryption will take place in Galaxkey Add-in: These include –
   1. Force Encryption to outgoing emails in Outlook
   2. Enable domain check for encryption
4. Related to additional security features of the mail: These include –
   1. Authenticate user when sending email
   2. Display valid from when sending encrypted emails from Outlook
   3. Provide option for Geo-fencing
   4. Enable attachment review and secondary password functionality
   5. Mark email for encryption instead of actual encryption in Outlook
   6. Enable revoke functionality

These are explained in details in the following sections:

#### Enable auto-updates on Windows

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 disable this option in case they prefer centralised GPO installation.

#### Force Encryption to Outgoing mails

This option is enabled to force the user to encrypt all the emails when they are sent. This option is useful to set the security policy for accounts that must send encrypted emails.

When you select this option, even the mails sent using the native ‘**Send**’ button of MS Outlook will also be encrypted.

#### Enable domain check for encryption

This option enables you to opt for sending secured (or non-secured) mails using the default ‘**SEND**’ button. When this option is selected, and user uses ‘Send’ button to send mails to recipients outside your domain, the user will be prompted to send a secured mail

#### Confirm before sending secured mails (Confirmation dialog)

This option is enabled by default. If this option is disabled, the user will not be prompted with a confirmation dialog when sending emails.

When this option is enabled, following options are enabled as well

1. Authenticate user when sending email:
2. Display valid from when sending encrypted emails from Outlook
3. Provide option for Geo-fencing
4. Enable attachment review and secondary password functionality
5. Mark email for encryption instead of actual encryption in Outlook

#### Authenticate user when sending email:

If this option is enabled, users will be prompted to enter their Galaxkey password every time they send out a secured email.

This attribute is useful in business environment where the company wants to ensure that the user sending encrypted emails is genuine.

#### Display valid from when sending encrypted emails from Outlook

This options enables you to set the time from which the email will be valid. When the user sets this time, recipients will not be able to access the secured email until the set time.

This setting in conjunction with the ‘Valid Till’ option, helps the user to restrict the availability of the email.

#### Provide option for Geo-fencing:

This option enables you to set-up the geo-fencing for your corporate. When you select this option, a Geo-fencing check box will be displayed on the Confirmation dialog of Outlook Add-in.

When the user will select this option a geo-fenced mail, the actual secured file, the GXK will be stored at a secured location within your premises. The geo-fenced mail will send a link to the secured document instead of the actual document.

The advantage of sending a geo-fenced mail is that the secured emails are physically restricted within your premises.

Note:

You can send additional attachments in a geo-fenced mail. The best viewed format of the attachments is PDF.

#### Enable attachments review and secondary password functionality

Email is a common mode of exchanging documents in the form of attachments. Galaxkey offers additional security to such emails in the form of secondary password.

When this option is enabled, a list of all the attachments of the mail is displayed in the confirmation dialog along with the option to review them. Reviewing the attachments ensures that the right attachment is sent to the right recipient.

User can also select whether the secondary password should be assigned to the email. Secondary password is generated by the system and stored in the Hybrid > SECONDARY PASSWORD. You can share it with the recipients via email or any other mode.

#### Mark email for encryption instead of actual encryption in outlook

Galaxkey can be configured such that the mail in Sent items of the sender is non-encrypted but the recipient receives a secured mail. This can be achieved by routing the mail via Galaxkey Secure Gateway (GSG).

When this option is selected, the Galaxkey Add-in will insert a header in the mail and send it as a plain mail.

Such mails will then be secured by the Galaxkey Secured Gateway (GSG) based on the policy definition.

Note: All the options (6.2.1.5 to 6.2.1.9) will be available only if you have enabled the ‘**Confirm before sending secured mail (Confirmation dialog)**’.

#### Enable Revoke Functionality

A Galaxkey secured mail can be recalled, i.e., revoked by the owner (sender) of the mail.

When you select this option all the secured mails are marked as ‘Revocable’, by default.

The user can then use the ‘Revoke’ option from the Galaxkey toolbar or the Galaxkey context menu to revoke the mail. Please note that the mails can be revoked only from the Sent Items folder of your Outlook.

### Galaxkey Client Policy

The configurations in this section are applicable to all the Galaxkey clients which include the Galaxkey Add-in for Microsoft Outlook, Galaxkey for iOS, Galaxkey for Blackberry, Galaxkey Web Access and Galaxkey for Mac OS. The two options are as follows:

1. Password Timeout
2. Enable Digital Signature

#### 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 usage of your Galaxkey account.

The default timeout is set to Thirty (30) minutes but can be changed to anything lesser or more. Please note that the time you enter here should be in minutes.

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

#### Enable Digital Signature

Digital signature is the standard mode of ensuring the sender’s identity.

When this option is selected, the option of sending a digitally signed mail is available to the users.

When a user selects this checkbox, digital signature of the user is inserted in the mail.

The recipient can verify this signature using the ‘Verify’ option in the decrypted mail.

### Galaxkey Secure Share

The configurations in this section are applicable to the Galaxkey Secure Share.

1. Enable Galaxkey Secure Share File Synchronisation:

If this option is disabled, the Galaxkey Cloud Synchronisation will be unavailable for your users, thus, not allowing them to store and share files securely.

1. Store sent email to GSS folder:

This option is used to enable the option where a copy of the sent email is stored in the users GSS folder. This is a very useful feature when you send emails to a new user. The encrypted copy of the email is stored in your GSS folder and when the recipient opens the email via Galaxkey Web Access, they are able to access the emails. The retention policies are used to define until when the mails are stored in your GSS folder.

### Policy Manager

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

Galaxkey provides for conditional encryption of an email. You can create a set of rules, which will be evaluated whenever you send a mail 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

Click ‘Add new’ to add a new encryption rule as shown below;

In the pop-up window, furnish all the details as follows;

1. **Rule Name**: Enter a name of your choice that best describes the rule.
2. **Encrypt if**: Select the appropriate condition from this drop down list of twelve conditions.
3. **Rule Data**: Enter valid data to match the selected rule condition.

The following table outlines the rule conditions available in Galaxkey and 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 mail should be encrypted |
| The body contains… | Enter any text or a regular expression, which if matched, the mail 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 mail if there is atleast one attachment to the mail |
| 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 mail will be secured |
| Triggered by classification software | This rule is exclusively applicable to Galaxkey Add-in for Outlook only. |

Note:

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 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.

By default, all the checkboxes are selected.

Save the data on form once you have configured it and then click the ‘UPDATE’ button to save all your configurations.

Note:

The configurations will take effect only when you restart the clients.

# Downloads

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

For the Corporate Administrators 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 Power Point Presentations and Data Sheets. We suggest you to use these for evaluation purposes.

# Hybrid

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

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

## 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 would be stored.

The individual Keys is the path to the keys folder where the individual users’ keys are stored

Administrator keys is the path to the keys folder where the administrative keys are stored.

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

## 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.

## Email Configuration to send emails from this appliance

The email configuration lets the hybrid configurations to set a mail 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 type – **Microsoft Exchange** or **IMAP**. Based on this selection, you must set-up the following:
2. In case of **Microsoft Exchange**, enter the **Exchange Webservices URL** in the format [**https://mail.acme.com/EWS/Exchange.asmx**](https://mail.acme.com/EWS/Exchange.asmx).
3. In 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 the cases, you must provide your **Login ID** and **Password** to the mail server. You can change the password at a later stage.

Use the ‘**Test Mail Server Settings**’ to ensure the correctness if the settings before updating.

## Galaxkey Secure Storage

Galaxkey now supports 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
   1. Domain / Host Name
   2. Username
   3. Password

## Secure Sign

Galaxkey supports applications where users can sign a secure document. This signature is saved in the database. You have a choice of associating 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.

## Authentication Options

Galaxkey now supports integration with Active Directory and Okta. When either of these is enabled, user need not remember multiple passwords. Also, the users can by-pass the repeated authentication to access secured mails.

#### Active Directory Integration

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

Following options are available on selecting 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.
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 he password for the service account.

#### OKTA Integration

You can enable OKTA authentication for Galaxkey so that the user does not need to remember multiple password and need not authenticate repeatedly to access Galaxkey secured mail.

Following options are available on selecting 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 he 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 certficate

## 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.