



Galaxkey

User Guide: Corporate Administrator

Author: Galaxkey Team

Table of Contents

[Section 1. Copyright 4](#_Toc448357186)

[Section 2. Executive Summary 5](#_Toc448357187)

[2.1. About Galaxkey 5](#_Toc448357188)

[2.2. Corporate Administrator Guide 5](#_Toc448357189)

[Section 3. Corporate Administrator 6](#_Toc448357190)

[3.1. Overview 6](#_Toc448357191)

[3.2. URL for Management 6](#_Toc448357192)

[Section 4. Domain Management 7](#_Toc448357193)

[4.1. Adding New Domain 7](#_Toc448357194)

[4.2. Managing Galaxkey Web Access Option 8](#_Toc448357195)

[Section 5. Galaxkey Configuration 9](#_Toc448357196)

[5.1. Corporate Configurations 9](#_Toc448357197)

[5.1.1. Accept Galaxkey Invites from Non-Admin Users 9](#_Toc448357198)

[5.1.2. Enable custom header for Galaxkey Invite (Invitation) 10](#_Toc448357199)

[5.1.3. Template for Galaxkey Secured Email 10](#_Toc448357200)

[5.1.4. Custom Amazon S3 Cloud Credentials 10](#_Toc448357201)

[5.1.5. Password Policy 10](#_Toc448357202)

[5.1.6. Geo-fencing 11](#_Toc448357203)

[5.1.7. Invitations 11](#_Toc448357204)

[5.1.8. Digital Signature 11](#_Toc448357205)

[5.2. Group Policies 12](#_Toc448357206)

[5.2.1. Microsoft Windows & Outlook Add-in Configuration 13](#_Toc448357207)

[5.2.2. Galaxkey Client Policy 15](#_Toc448357208)

[5.2.3. Galaxkey Secure Share 15](#_Toc448357209)

[5.2.4. Policy Manager 15](#_Toc448357210)

[Section 6. Corporate Identity Management 20](#_Toc448357211)

[6.1. Adding New Identities 20](#_Toc448357212)

[6.1.1. Registering via Identities Module 21](#_Toc448357213)

[6.1.2. Registering via Galaxkey Active Directory Connector 22](#_Toc448357214)

[6.2. Managing Existing Identities 22](#_Toc448357215)

[6.2.1. Active 23](#_Toc448357216)

[6.2.2. Active – Reset Password 24](#_Toc448357217)

[6.2.3. Active – Service Account & Administrative Rights 25](#_Toc448357218)

[6.2.4. Inactive 26](#_Toc448357219)

[6.2.5. Awaiting Activation from Admin 26](#_Toc448357220)

[6.2.6. Acceptance Required 27](#_Toc448357221)

[6.3. Identity Backup and Maintenance 27](#_Toc448357222)

[Section 7. Downloads 29](#_Toc448357223)

[Section 8. Hybrid 30](#_Toc448357224)

[8.1. Hybrid Key Store Path 31](#_Toc448357225)

[8.2. Syslog Server Configuration 31](#_Toc448357226)

[8.3. Email Configuration 31](#_Toc448357227)

[8.4. Custom Template for Email Header and Footer 31](#_Toc448357228)

[8.5. Geo-Fencing 31](#_Toc448357229)

[8.6. Galaxkey Secure Storage 32](#_Toc448357230)

# 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 is able to address all the vulnerabilities and still maintain 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.

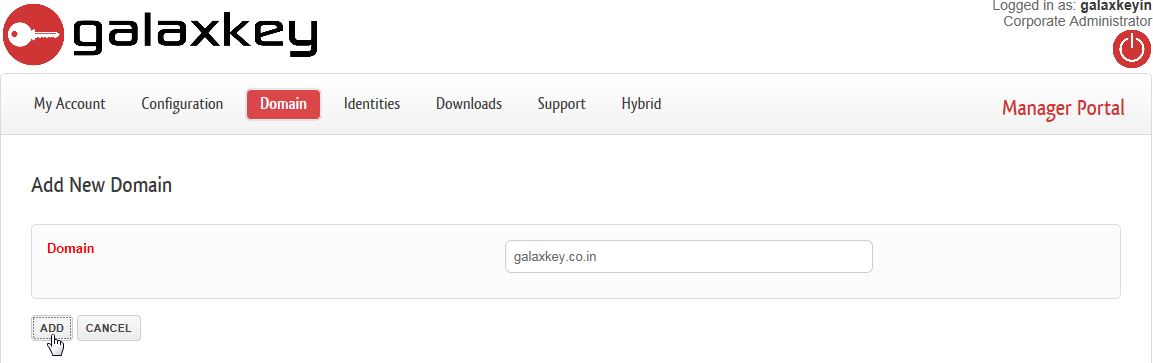
# Domain Management

Domain management in Galaxkey is the process of registering a domain for secured communication, configuring web access for the domain in order 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. The domain registration is the first step towards ensuring that the domain is exclusively owned by the Corporate and no one else in the Galaxkey Eco-system can register the domain. In case the administrator is not able to register a domain due to reasons which mention that the domain is already registered, then the administrator needs to 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.

The **Domains** module of Galaxkey Manager provides the interface for domain management. Using this module, you can

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

## Adding New Domain

The home page of the Domains module lists all the registered domains. Click the **‘ADD NEW DOMAIN’** button to register another 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 then manage this domain.

Note:

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

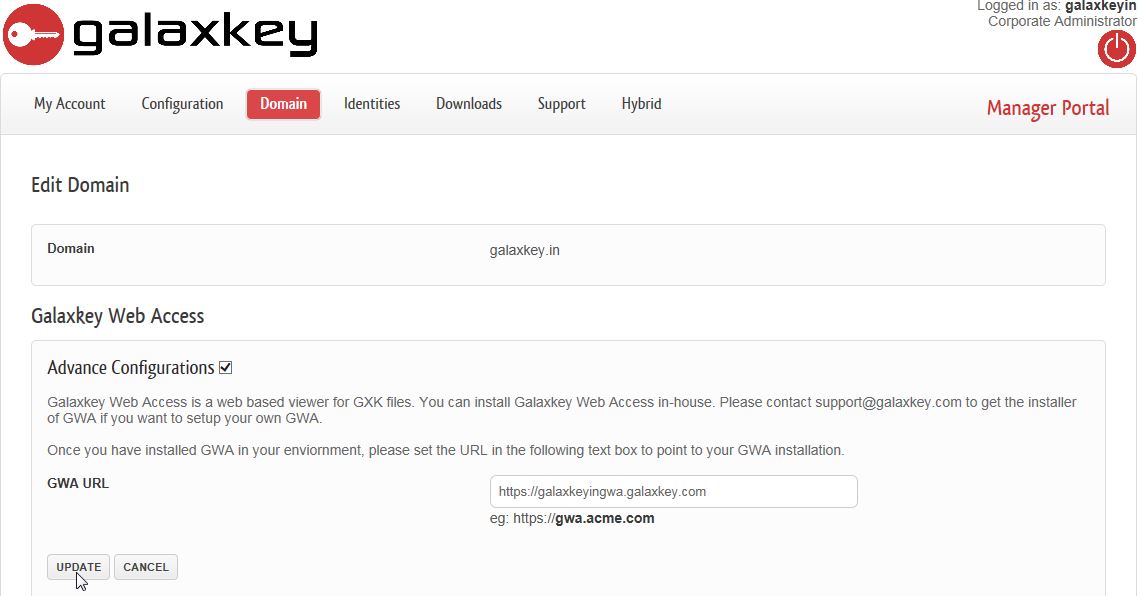
## Managing Galaxkey Web Access Option

Galaxkey Web Access is a Web client for Galaxkey. The client is web based hence the user does not need to install any Galaxkey client in house. You can get more details about GWA from <https://help.galaxkey.com/GalaxkeyWebAccessGWA.html>. The GWA client can be installed in a corporate environment as well. So 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.

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 'Drag-Drop' option on the GWA portal.

# Galaxkey Configuration

The **Configuration** module aids you in setting up Galaxkey to suit to the organisation’s security requirements.

The settings that you make on this page will govern the users' identities. If you want to allow some of the users to set their own configurations, then enable the **Allow personal configuration** option in the edit mode of the user's identity.

The Configuration module comprises of two sections:

1. Corporate Configurations
2. Group Policies

## Corporate Configurations

The configuration options in this section, govern the global policies for the corporate.

### Accept Galaxkey Invites from Non-Admin Users

This is an important configuration option. Galaxkey works on an invitation model. So when you send an email to a new user, Galaxkey sends an invitation to that 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 only 10 licenses with Galaxkey, and 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 will have to 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.

### Enable custom header for Galaxkey Invite (Invitation)

Galaxkey allows you to send custom text in to your invitees. Select the ‘**Enable Custom header for Galaxkey Invite (Invitation)**’ checkbox to enable the custom text.

This option enables you to prepend custom text to the email that is sent out as an invitation when someone from your organisation sends out an invite.

Please enter the text in HTML as it will be formatted and placed at the start of the email.

### 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 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 version of the template and hence you have to define the HTML template and the text template.

### Custom Amazon S3 Cloud Credentials

Galaxkey provides a very powerful framework for corporate customers to configure their own Amazon S3 Cloud Storage. All the data in the cloud is stored in secured form. Thus, a file is always encrypted before it is copied to the cloud.

The corporate accounts can configure their own cloud storage, by specifying the Amazon S3 storage.

### Password Policy

Galaxkey provides a very powerful framework for corporate customers to configure their own Amazon S3 Cloud Storage. All the data in the cloud is stored in secured form. Thus, a file is always encrypted before it is copied to the cloud.

The corporate accounts can configure their own cloud storage, by specifying the Amazon S3 storage.

Note:

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

### Geo-fencing

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.

The geo-fencing settings made here are as follows:

Select the ‘**Enable Geo fencing**’ checkbox to enable the Geo-fencing feature for your organisation. The following parameters should be configured before this feature can be implemented effectively.

**E-mail Template for Geo-fencing Email (sent to recipient):**

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.

### Invitations

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.

### Digital Signature

This section helps you to add a prefix to the subject of emails digitally signed using Galaxkey.

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

### 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 upload your logo using the ‘**Corporate logo**’ section of the Corporate Configurations section.

### Invite Settings

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

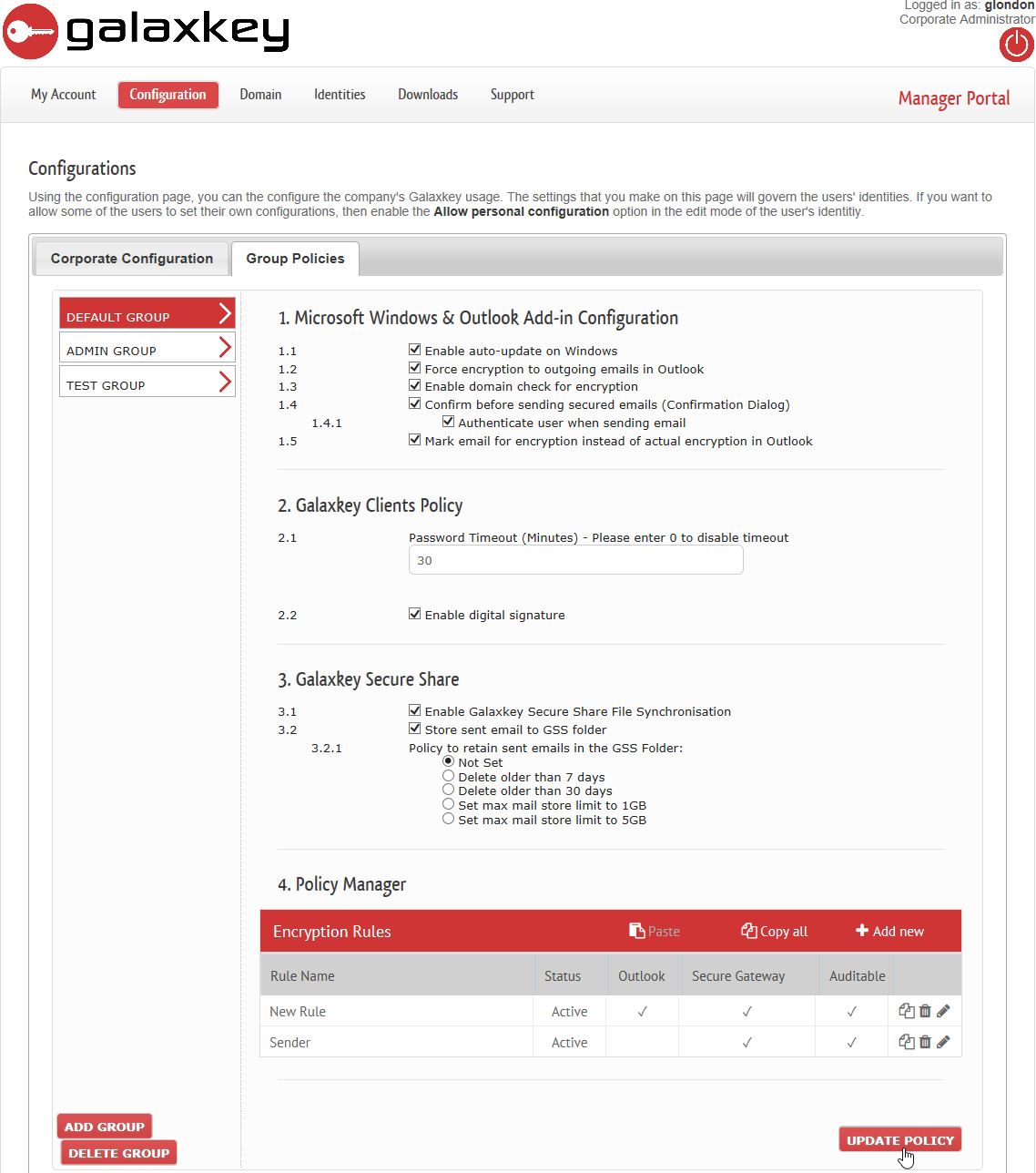
You can now send the invites from this server by checking this option.

## Group Policies

Galaxkey is configured to allow Administrators to define corporate policies centrally based on user Groups. There is always one DEFAULT GROUP and the other groups can be added manually. The groups are also filled by the GADC automatically during synchronisation.

The Corporate Administrator can configure different configurations for different groups. 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 pertain only to the Microsoft Outlook Galaxkey Add-in users. Following are the options available

#### 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 two options are enabled as well

1. **Authenticate user when sending email**: If this option is enabled, each time the user sends out emails, he will be prompted for authentication.

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

1. **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.

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

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: This option will be available only if your reseller has selected the ‘**Allow mark only encryption capability**’ checkbox in your corporate settings.

### 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.

1. **Password Timeout:** The Password Timeout defines the time the password is stored in memory before the user has to re-authenticate to use the functionality in the clients
2. **Enable Digital Signature**: When this is selected, all the users in your organisation can digitally sign a secured email.

### 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

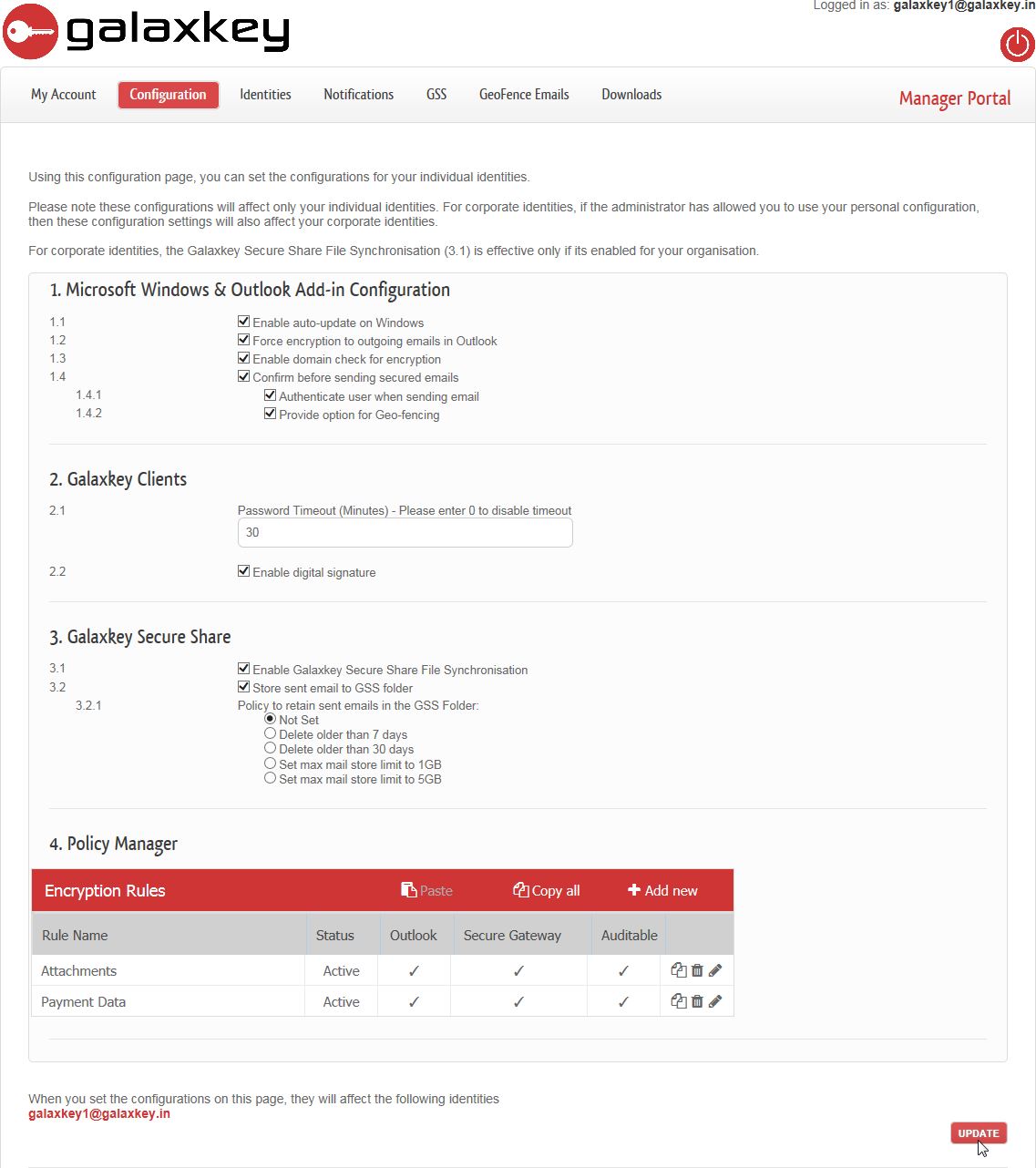
Email is widely used to share personal and official information which must be safeguarded. Galaxkey provides a robust solution for this.

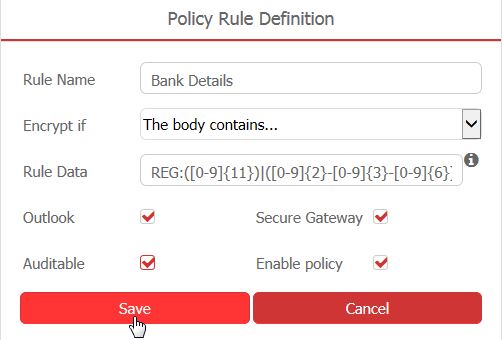
Galaxkey provides for conditional encryption of an email. You can create a set of rules, which will be evaluated whenever you send a mail using the Outlook ‘**SEND**’ button.

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.

# Corporate Identity Management

As a corporate administrator, the identities of the users in the corporate are all stored in the administrator’s vault which is secured using the administrator’s password.



Corporate identity management encompasses the following

1. Adding Identities: New Corporate Users
   1. Bulk Addition: Using Galaxkey Active Directory Connector (GADC)
   2. Via Galaxkey Manager: Using the Identities module
2. Managing existing Users
3. Identity Back-up and Maintenance

## Adding New Identities

As a Corporate administrator, one of your main tasks is to **add** and **manage** individual corporate identities.

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.

To manage these individual identities, you must login to the Galaxkey Manager. The Identities module lists the existing identities and also provides to add new identities.

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 later on, 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.
6. Enter your **admin password** in the **'Please re-enter your login password'** field.
7. Selecting 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 will be listed under the **'Acceptance Required'** tab on the list page.

An **invitation e-mail** will be sent to the individual user directing her to register with Galaxkey.

### 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.

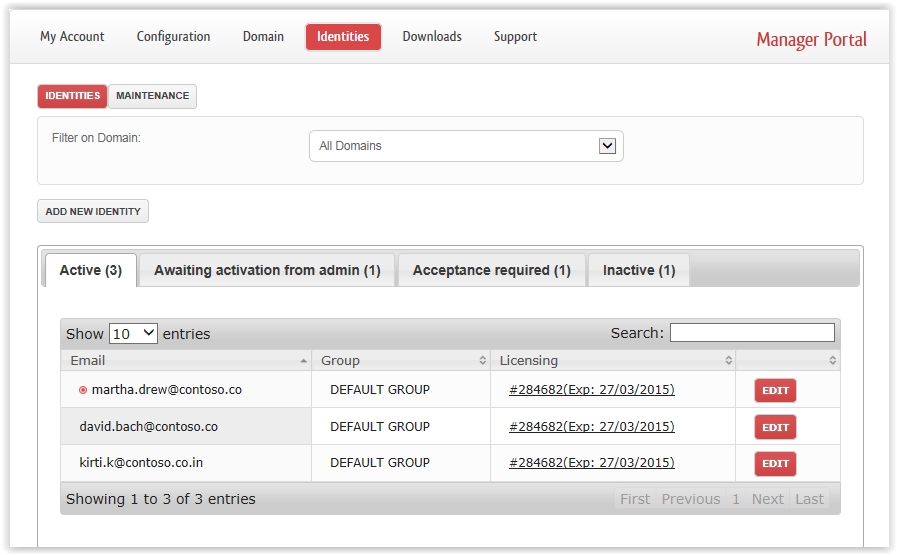
Please refer to the GADC Manual for more details

## 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. **Awaiting Activation From Admin:** Identities in this state has accepted their invitation but the admin has to assign them the license.
4. **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

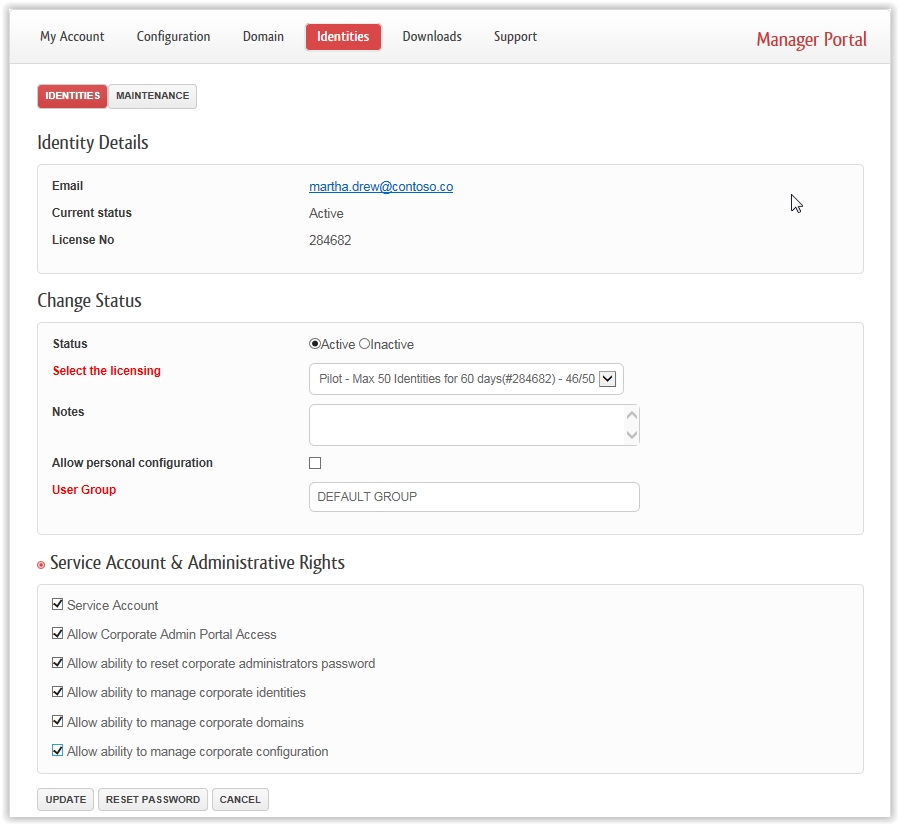
The listing of the identities in this tab displays the email address associated with the identity, the group in which the identity is currently present, licensing and the ability to edit the identity.

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.

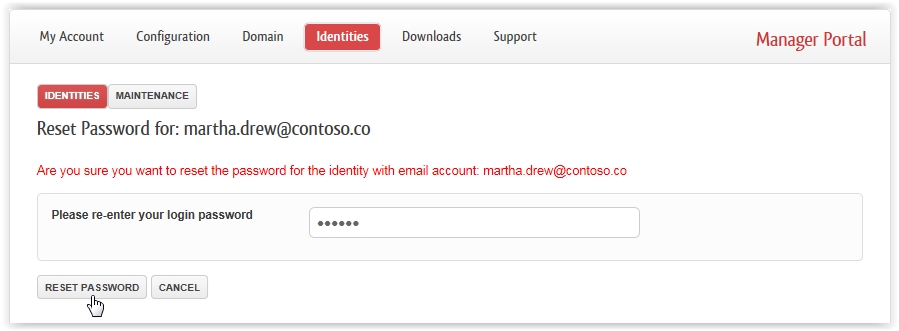
The edit button lets you edit the following identity details

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. **Define Groups**.
6. **Reset password** – explained in next paragraph.
7. **Enable Service Account & Administrative Rights**: With this you can delegate some of your Galaxkey management responsibilities to other user.

****

### Active – Reset Password

In the edit dialog there is an additional button called Reset Password. Using this button you can reset the users’ password in case the user has forgotten. Since Galaxkey does not store any password, the process of resetting the password is as follows



1. The Administrative user enters his own password
2. Using the admin password, the users’ key is extracted from the admins password store.
3. The extracted key is then secured using a temporary password which is emailed to the user.
4. The user has to first set the password once he logins to the portal.

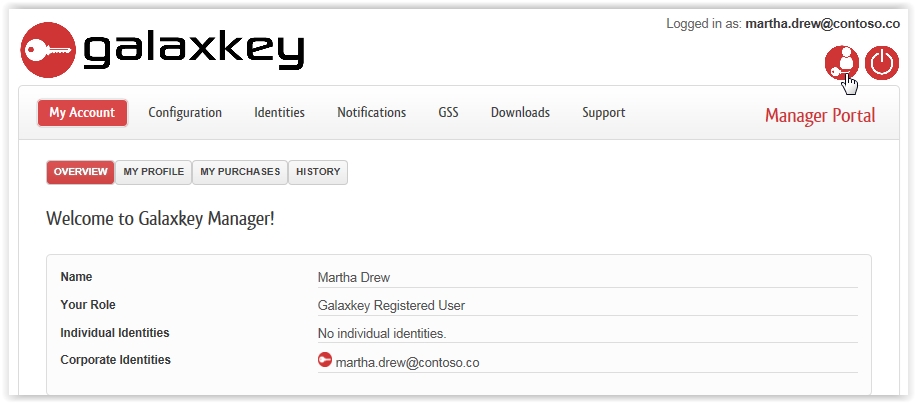
### Active – Service Account & Administrative Rights

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.



### Inactive

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

When the identities are in the inactive state, the license is release for that user.

Identities can be change from inactive to active state by editing the identity and assigning it a license.

The administrator cannot reset the password of the identity that is inactive state.

### Awaiting Activation from Admin

Identities will be listed in this tab if they have been registered by users but awaiting activation from the administrator. When an identity comes in this state, the administrator receives an email from Galaxkey informing that the identity has to be activated. The process of activating the identity is basically assigning the identity a valid license. The identities are listed in this tab only when they receive an invitation from external users.



In the above image when the identity completes stage 2 it is in the Awaiting Action From Admin

### Acceptance Required

When the corporate administrator add a new identity, it has to be accepted by the user.



So once the invitation is sent, the identity is in this state. When the identity is in this state, the administrator cannot make any changes to the identity. He can also resend the invitation to the user to remind him.

## 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 has to 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

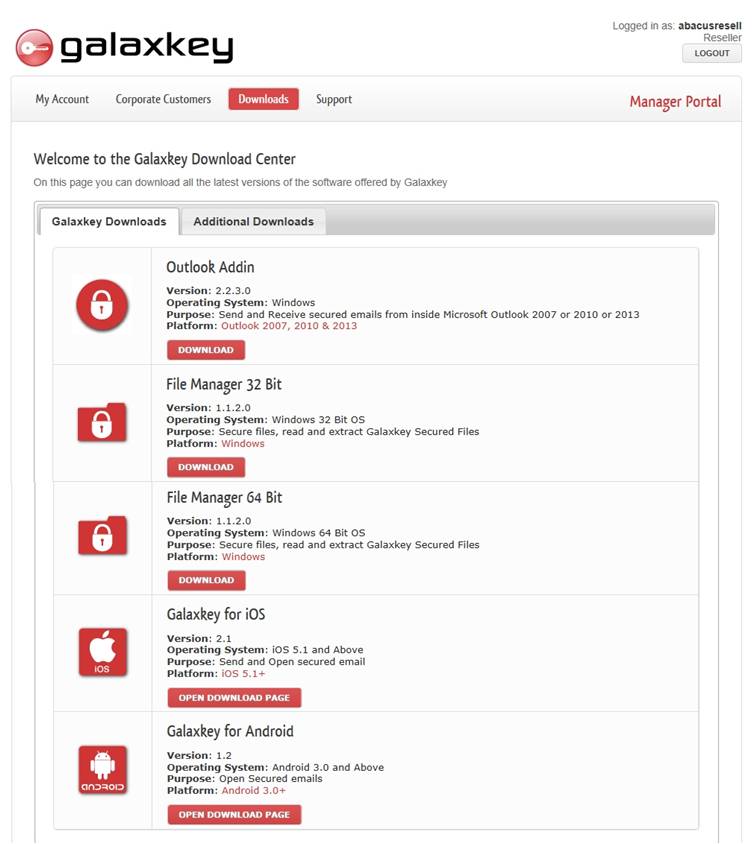
Since Galaxkey does not store any passwords, in case the administrator forgets his password, he will need the identities backup to regenerate new password. So it’s advised to do regular backups.

# 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.

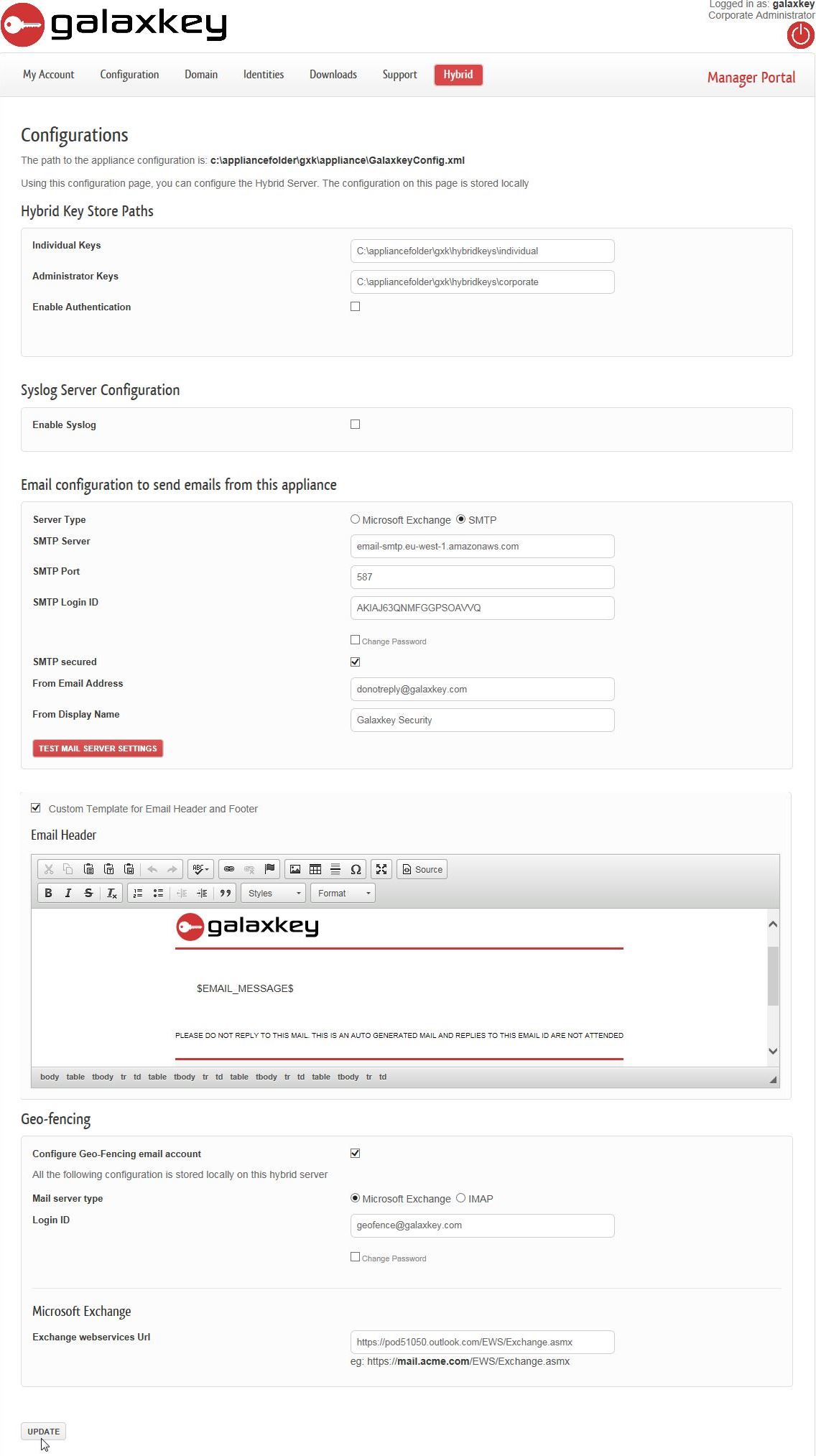
Apart from additional binaries, there are Power Point Presentations and Data Sheets. We suggest you to use these for evaluation purposes.



# 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.

**Allow users to self-reset their passwords** is the option for enabling corporate users to reset their own password. This is optional and unchecked by default. Thus, resetting passwords for the users is, primarily, the task assigned to the Corporate Administrator.

## 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

The email configuration lets the hybrid configurations to set a mail server that will be used to send out emails and Galaxkey Notifications

## Custom Template for Email Header and Footer

Using this option, you can configure the Email Headers for all the notification emails sent to users. The template should contain the place holder $EMAIL\_MESSAGE$. This place holder is replaced with the email message.

## Geo-Fencing

Geo-fencing in Galaxkey is the process of providing an option to the corporate whereby the secured mails will be received and stored in a central mailbox within your premises.

The mail sent to the recipient contains the link to the secured mail and can be accessed over the internet.

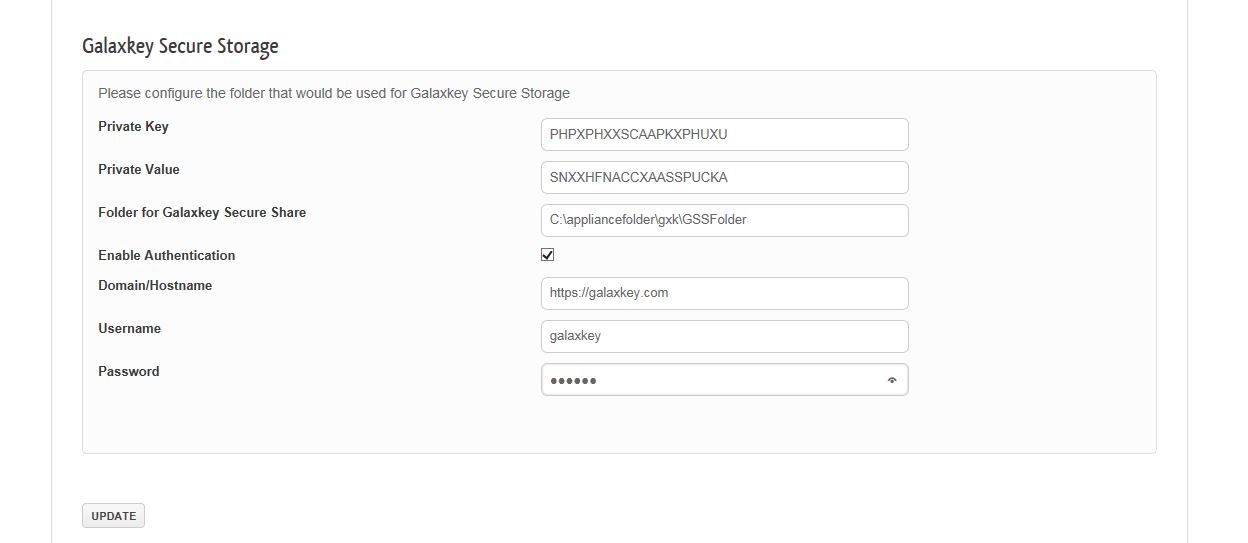
This option is available in the Hybrid set-up only.

When you select the ‘**Configure Geo-Fencing email account**’ checkbox, following settings will be enabled:

1. **Mail Server Type**: Select one of the two server type – **Microsoft Exchange** or **IMAP**. Based on this selection, you will have to 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 check the **SSL / TLS** checkbox to opt for a secure connection.
4. 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.

## 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