STAY PRIVATE

Administrator guide

v2.0

Table of Contents

STAY PRIVATE

1. StayPrivate Product Overview

1.1 Introduction

StayPrivate acts as a secure interface between the (secure) corporate network and the (unsecure) outside world, allowing companies to conveniently send and exchange information securely with external parties.

Each company is assigned its own independent, secure environment, including a company-specific URL, where all communications and information are safely stored. All information is protected using AES-256 encryption technology, held in EU-located, fully protected data centres, and subject to strict policy and security protocols.

StayPrivate is designed to be simple to set up and convenient to use. Company users can send and receive secure messages directly from within their current email client. All users can access StayPrivate from:

- their email via any web browser on any computer or device;
- directly in a web browser via the company URL;
- by downloading the white-labelled Secure Portal app, available free from iTunes, Google and Amazon app stores.

For companies which wish to integrate StayPrivate further, there is a well-documented API framework.

1.2 Functionality

StayPrivate is designed to automatically adapt to any business environment. The default set up works straight "out of the box". Nevertheless, StayPrivate includes a comprehensive range of settings, enabling companies to tailor the functionality available to their users and to improve upon pre-existing business processes. Companies can choose one of the four available subscription types.

StayPrivate Free	StayPrivate Business	StayPrivate Business Plus	StayPrivate Enterprise
1 Company User	3 Company Users*	5 Company Users*	Bespoke
Unlimited Client Users	Unlimited Client Users	Unlimited Client Users	Unlimited Client Users
Email (Including Attachments)	Email (Including Attachments)	Email (Including Attachments)	Email (Including Attachments)
Electronic Signatures	Electronic Signatures	Electronic Signatures	Electronic Signatures
File Sharing	File Sharing	File Sharing	File Sharing
Instant Messaging	Instant Messaging	Instant Messaging	Instant Messaging
Video Calling	Video Calling	Video Calling	Video Calling
Meeting Recordings	Meeting Recordings	Meeting Recordings	Meeting Recordings
Advanced Audit Functionality	Advanced Audit Functionality	Advanced Audit Functionality	Advanced Audit Functionality
Delegation Functionality	Delegation Functionality	Delegation Functionality	Delegation Functionality
Administrator Users	Administrator Users	Administrator Users	Administrator Users
Compliance Users	Compliance Users	Compliance Users	Compliance Users
Storage 1GB	Storage 150GB	Storage 250GB	Bespoke Storage
UK Server Location	UK Server Location	UK Server Location	Bespoke Server Location
UK Data Server Location	UK Data Server Location	UK Data Server Location	Bespoke Data Server Location
API Access	API Access	API Access	API Access
External Back-ups	External Back-ups	External Back-ups	External Back-ups
24/7 Support	24/7 Support	24/7 Support	24/7 Support
Bespoke Branding	Bespoke Branding	Bespoke Branding	Bespoke Branding
Bespoke Company URL	Bespoke Company URL	Bespoke Company URL	Bespoke Company URL
iOS & Android Apps	iOS & Android Apps	iOS & Android Apps	iOS & Android Apps
Outlook & Gmail Add-ins	Outlook & Gmail Add-ins	Outlook & Gmail Add-ins	Outlook & Gmail Add-ins

Besides, StayPrivate provides wide capabilities to adjust the system settings and functions. For instance, there is a comprehensive range of settings allowing companies to specify whether and under what circumstances users are able to delete items. Also, companies can choose whether to activate optional features: Vault (file sharing), Instant Messaging, and Electronic Signatures.

1.3 Company user's point of view

Company users can send secure emails (plus attachments) via StayPrivate directly from within their current email client. They follow a simple protocol to send the email to the StayPrivate secure server, rather than sending it directly to the end recipient. This is not difficult to do manually, but it is typically automated by using one of the StayPrivate 'SecureMail' add-ins. Add-ins are available for Outlook, Gmail and Office 365.

Replies and other notifications (copies of files uploaded, instant messages and notifications of electronic signature activity) are sent directly to the user's existing corporate email account. This means that for day-to-day use, the typical company user has no need to access the StayPrivate secure portal directly.

1.4 External user's point of view

External users receive StayPrivate emails directly into their current email accounts. The difference is that, depending on the level of security selected by the sender, either the attachments or the entire message can only be accessed by clicking a secure 'smart link' embedded in the email.

The smart link is designed so that when the external user clicks on it they are taken directly to their account's PIN authentication screen in the company portal. The user enters their four-digit PIN to gain access to their information. (The first time a user logs in they are asked to set their own PIN – unless an Administrator has set it for them already.)

1.5 Security

Private by design

One of the benefits of using StayPrivate is that it is "private by design". All communications and information are organised into distinct private channels. The first time a new recipient is sent a secure email, their StayPrivate user account is set up automatically and a private channel is created within StayPrivate for the sender and recipient(s). Only users who are members of a private channel can access the private channel. All members of a private channel can see all communication within the private channel. StayPrivate, therefore, not only ensures the security and privacy of all communications it carries, but it also provides clear, transparent evidence of this privacy.

Stability

StayPrivate runs on fully managed, dedicated servers, located in secure Tier 3+ data centres within the UK. Our data centres operate fully redundant subsystems (such as air conditioning, network access, power supply, fire protection) and have separate security zones controlled by biometric access. To further ensure durability, we have full geographic redundancy plus we back up encrypted versions of all our systems and data daily to the cloud and, periodically, in physical format too.

File Storage

All files shared or stored using StayPrivate are individually encrypted (using a different key for each document) before being stored in the Amazon S3 Cloud in Ireland, which is designed to provide 99.999999999% durability over a twelve-month period. Amazon S3 is designed to sustain the concurrent loss of data in two facilities.

Deletion and Versioning

We use versioning, which means that we preserve every version of every le stored, so that users cannot accidentally delete or overwrite important data. All old versions of files are stored fully encrypted in a restricted access area and are deleted after an appropriate period of time.

Encryption

All communications and information are encrypted both in transit and in storage. We use one of the most secure encryption algorithms available (AES 256) and all files are further encrypted before being stored in the Amazon S3 cloud in the UK, meaning that Amazon does not have access to any of your information. Encryption keys are not shared, but are derived dynamically for each document, meaning that even in the unlikely event of a catastrophic breach of data security, all information should remain fully encrypted. Emails between StayPrivate and the company email server are encrypted using TLS. It is important that the company email server is properly configured and TLS certification is kept up to date.

Password, PIN Access, Controls

Access is secured by password and PIN (two-step authentication). Users can log out from other devices remotely and there is a range of other security settings, including, for example, the option to automatically receive email notifications each time their account is accessed.

Users can reset their password via email. They can also reset their PIN. However, to maintain the security of the platform, there is a 24-hour quarantine period before a user PIN reset is processed. Administrators can override this on a user's behalf.

If there is no activity in the StayPrivate web portal or app for more than five minutes, the user is returned to the PIN authentication screen, and asked to log back in again. In the web portal, if there is still no response, the user is completely logged out of StayPrivate. Users can also log out themselves and can also 'log out elsewhere', which enables them to cancel all other current sessions on any other devices. It is also possible to disable all existing smart links for a user – simply by changing the user password.

Confidentiality

All communications and information are shared only between the sender and the recipient(s). In other words, users only have access to their own information. The StayPrivate user interface is built around the concept of private channels, and therefore reduces the risk of accidentally sharing information inappropriately by, for example, sending an email to the wrong recipient.

Location

All data reside in the European Union and are protected by European Union Data Protection laws. StayPrivate Ltd is registered under UK Data Protection laws with the Information Commissioner's Oce. StayPrivate and StayPrivate Ltd are GDPR-compliant.

Legal

We have been awarded ISO 27001 accreditation, the international standard for best practice for information security management systems.

Failure Protection

All company files are individually encrypted before being stored in a unique secure space within the Amazon S3 Cloud and all information remains the legal property of your company at all times. In the unlikely event of StayPrivate Ltd defaulting or otherwise failing to deliver the StayPrivate service, we will create a single account granting you direct access to your company's secure area.

We also offer an additional back up service, whereby we can send a copy of all information to a company's own entirely independent back up area, encrypted using a key provided by the company.

2. Access Points

StayPrivate is designed to offer maximum flexibility to users, so that companies and their contacts can reap all the benefits without changing the way they work. Users can access StayPrivate from within their existing email client (either directly, or by using the 'SecureMail' add-in), from the web portal (using either a smart link, or by logging in directly with their username and password), or via the Secure Portal mobile app. Whichever route they choose, users are provided with a professional, modern interface, all branded to match the company theme.

2.1 Email

Company users can send and receive secure communications directly from within their existing email account. Note that for communications to remain secure it is important that the company email server is properly configured with a valid, up-to-date TLS certificate.

StayPrivate add-ins are available for Outlook, Gmail and Microsoft Office 365 (Outlook Web). The add-ins make the process of sending a secure email as easy as clicking a button. Nevertheless, company users using an email client where the add-in is not available can easily send secure emails by changing the recipient email address to its secure equivalent: for example, for a company user with secure email address *'employee@exampleco.secure-comm.com'* sending to *'recipient@company.com'*, the user sends to the secure email address: *'recipient.at.company.com @exampleco.secure-comm.com'*.

Note that the above functionality is only available to company users, but that all users can access the web portal from within their email, by clicking on a smart link.

Company users can also request an electronic signature ('esign') for any attachments they send. If an electronic signature is requested for a document, once each recipient downloads or reads the document they are prompted to either 'confirm that they accept and agree with contents' or to 'decline' the document contents.

2.2 Web Portal

Each company is provided with its own unique secure StayPrivate domain which both acts as a host for the company and client secure email addresses and also provides the URL for the company web portal. The company URL is simply the company's unique ID plus the suffix *'.secure-comm.com'*. For example, the web portal for a company with ID '*exampleco*' would be accessed at the URL: *'https://exampleco.secure-comm.com'*.

Users log into the web portal using their username (or email address), password plus PIN. Alternatively, users can follow the smart link from a secure email which will take them straight to the portal and to the PIN screen, without needing to enter their username or password.

The web portal provides users with a secure, private and convenient way of viewing all their conversations, accessing attachments, organising their information, sharing files and, of course, communicating. It is fully responsive, and can be used equally well on phones and tablets as well as larger screens.

2.3 Mobile Apps

The 'Secure Portal' app is available free on iTunes, Google Play and Amazon app stores. It offers a convenient way for mobile users to access their secure environment. It works along very similar lines to the web portal, but as an installed app it has access to more functionality than a browser, and so can provide an even richer experience to the user.

2.4 Branding

Emails, the web portal, and the mobile apps are branded throughout (with the sole exception of the Secure Portal app icon, which cannot be changed) with the company name, logo, colours, and disclaimer. The result is that users not only receive a professional experience, but also have the confidence that 'they are in the right place'.

3. User Types

StayPrivate provides companies with control as well as security over their information. A key element of this is ensuring that users, both internal and external, only have access to the information they should. StayPrivate achieves this simply and effectively via its five user types: Agent, Client, Controller, Administrator and System Administrator.

3.1 Agents

The typical company user is an 'Agent'. Agent user rights are designed so that the user has everything they need to do business, but not so much that they can do anything potentially destructive.

Agents can communicate with other users, create new users (users are created automatically when they send an email to a new recipient) and set up new secure channels.

Agents can leave a channel to which they have access. However, they are not allowed to delete other users or channels. Furthermore, they are unable to see other channels and users to which they do not have access.

3.2 Clients

Client users are users external to the company. They have more restricted rights. They can access and communicate via existing channels to which they have access, but they cannot create new channels or users.

3.3 Controllers

The controller user is designed to enable compliance: for example, where a company needs to be able to gain access, see activity or get an overview of other accounts.

Controllers have all the rights of Agents plus the significant extra power that they can access (on a read-only basis) the account of any other user with whom they have a 'one-to-one' private channel. If they have access, they can see everything that user can see.

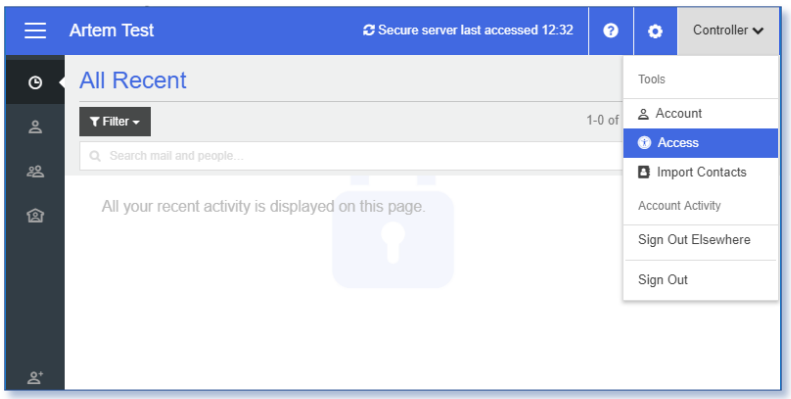
In the first instance, since StayPrivate ensures that there is already a full audit trail of all communication in the existing corporate email account, there is typically no immediate need for a company to introduce Controllers. Companies usually add controller users as usage increases and as the need arises, operating separate, extra Controller accounts alongside their normal user (Agent) accounts. This means that a compliance department can use Agent accounts for their individual business communications, whilst still having the Controller functionality to provide oversight.

3.3.1 How to access user accounts

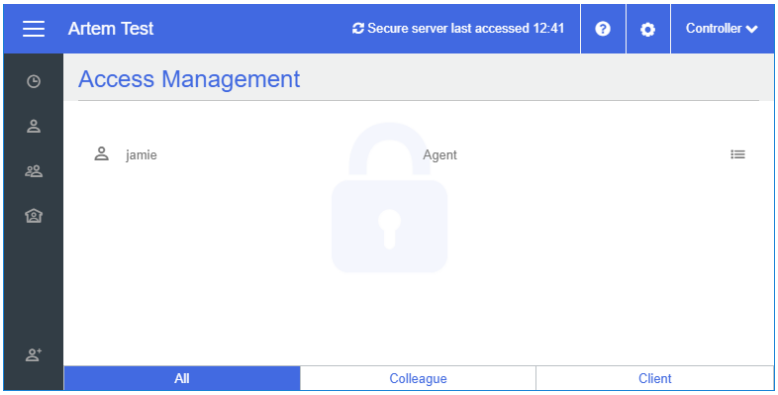
The Controller user is designed to make it simple for a company to implement effective compliance or control procedures. Controller users can access and see activity in other users' accounts.

Controller users have all the usual rights of Agents plus the significant extra power that they can access (on a read-only basis) the account of any other user who is a contact of theirs on a 'one-to-one' basis (it is not enough to be members of the same group).

To access another user account, select Access from the drop-down menu in the top right-hand corner of the secure web portal.



Select the ☰ icon corresponding to the user whose account you wish to view.



A new tab opens in the browser providing full read-only access to that user's account. The controller can see everything that the user can see.

3.4 Administrators

Administrators have enhanced user rights (although note that they do not have the oversight rights of Controllers; to ensure privacy and transparency, Administrators are not allowed to be Controllers).

Administrators can set up new Agent, Client, Administrator and Controller users, edit and delete users under their administration, and add, edit and delete channels.

Each company environment has one System Administrator (SA). The SA can amend the company's branding and colours, change system settings and transfer their SA rights to another Administrator.

Administrators can only make changes that affect only users under their administration (this includes both users directly under their administration and users under the administration of Administrators under their administration). This allows the company environment to be segmented into separate areas, with different Administrators taking responsibility for different sections. Every user (other than the System Administrator) is administered by an Administrator, and the Administrators form a strictly cascading hierarchy with the System Administrator at the top.

3.5 Delegating Access

Agents can grant access to their account to one or more other users. This allows another user to do work on behalf of the Agent. This can be useful if, for example, a user has a PA, or if they are on holiday. To preserve the integrity of the audit history, StayPrivate records the name of the user who actually performed the activity as well as the person it was performed on behalf of. (This information is hidden from CLIENT users.)

3.6 New Users

New users are automatically added to StayPrivate environment as they are required. Each time a secure email is sent to a new recipient, the recipient is set up as a new user. If the recipient email address matches the corporate domain, the user is set up as an AGENT; otherwise they are set up as a CLIENT.

All company users can also set up new users directly from within the web portal or the app. As well as being able to set up users, Administrators can edit users, including changing their user type, password and PIN from within the web portal.

4. Security

4.1 Stability

StayPrivate runs on fully managed, dedicated servers, located in secure Tier 3+ data centres within the UK. Our data centres operate fully redundant subsystems (such as air conditioning, network access, power supply, fire protection) and have separate security zones controlled by biometric access. To further ensure durability, we have full geographic redundancy plus we back up encrypted versions of all our systems and data daily to the cloud and, periodically, in physical format too..

4.2 File Storage

All files shared or stored using StayPrivate are individually encrypted (using a different key for each document) before being in the UK, which is designed to provide 99.999999999% durability over a twelve-month period. Amazon S3 is designed to sustain the concurrent loss of data in two facilities.

4.3 Deletion and Versioning

We use versioning, which means that we preserve every version of every file stored, so that users cannot accidentally delete or overwrite important data. All old versions of files are stored fully encrypted in a restricted access area and are deleted after an appropriate period of time.

4.4 Encryption

All communications and information are encrypted both in transit and in storage. We use one of the most secure encryption algorithms available (AES 256) and all files are further encrypted before being stored in the Amazon cloud, meaning that Amazon does not have access to any of your information. Encryption keys are not shared, but are derived dynamically for each document, meaning that even in the unlikely event of a catastrophic breach of data security, all information should remain fully encrypted.

Emails between StayPrivate and the company email server are encrypted using TLS. It is important that the company email server is properly configured, and TLS certification is kept up to date.

4.5 Password, PIN Access, Controls

Access is secured by password and PIN (two-step authentication). Users can log out from other devices remotely and there is a range of other security settings, including, for example, the option to automatically receive email notifications each time their account is accessed.

Users can reset their password via email. They can also reset their PIN. However, to maintain the security of the platform, there is a 24-hour quarantine period before a user PIN reset is processed. Administrators can override this on a user's behalf.

If there is a period of no activity in the StayPrivate web portal or app the user is returned to the PIN authentication screen, and asked to log back in again. In the web portal, if there is still no response, the user is completely logged out of StayPrivate. Users can also log out themselves and can also 'log out elsewhere', which enables them to cancel all other current sessions on any other devices.

It is also possible to disable all existing smart links for a user – simply by changing the user password.

4.6 Confidentiality

All communications and information are shared only between the sender and the recipient(s). In other words, users only have access to their own information. The StayPrivate user interface is built around the concept of private channels, and therefore reduces the risk of accidentally sharing information inappropriately by, for example, sending an email to the wrong recipient.

4.7 Location

All data reside in the European Union and are protected by European Union Data Protection laws. StayPrivate Ltd is registered under UK Data Protection laws with the Information Commissioner's Office. StayPrivate and StayPrivate Ltd are GDPR-compliant.

4.8 Legal, Default and Failure Protection

We have been awarded ISO 27001 accreditation, the international standard for best practice for information security management systems.

All company files are individually encrypted before being stored in a unique secure space within the Amazon S3 Cloud and all information remains the legal property of your company at all times. In the unlikely event of StayPrivate Ltd defaulting or otherwise failing to deliver the StayPrivate service, we will create a single account granting you direct access to your company's secure area.

We also offer an additional back up service, whereby we can send a copy of all information to a company's own entirely independent back up area, encrypted using a key provided by the company.

4.9 Private Channels

All communications are associated with a private channel. All participants in a channel can see (with a few minor exceptions) all activity associated with that channel, including the identity of other members of the channel. This is what we call transparent privacy. It means that information is not only private, but that users can see that it is private.

Company users also have their own individual private channel, for their eyes only, called 'My Area', where they can store information and send emails to themselves. This channel also carries certain system emails and notifications.

4.10 Primary Channels for Clients

StayPrivate automatically creates a primary communication channel between the company and each client (or group of clients) the first time a secure email is sent to the client. This ensures that all communications stay in one place and are available to all the necessary users.

In the standard StayPrivate configuration, additional company users can be added to the primary channel by a company user who is already a member copying in the new user on a secure client communication.

If a company user who is not a member of the primary channel attempts to contact the client securely, they receive an error message explaining that a primary channel already exists with this client. To send a secure email to the client they need to either get themselves added to the primary channel or to create a separate private channel with the same client – which they can do by including *'#private'* in the subject field of the secure email.

This set up works well for most businesses, as it provides a single channel to carry most communications between the client and the company, whilst also providing the flexibility to allow private communications as required. (this is not the case for strict primary channel configurations where additional members can only be set by the administrator).

4.11 Strict Primary Client Channels

For companies which wish an extra level of control, it is also possible to enforce 'strict' primary channels. In this case, only an administrator can change the members of a primary channel.

Additional private channels can still be established by including '#private' in the subject field as above.

4.12 No Primary Client Channel

Companies can also choose to switch off the primary channel behaviour entirely, so that a separate private channel is created every time a new company user contacts a client.

5. Settings

5.1 Company level settings

The StayPrivate default configuration is designed to work with any corporate set up. However, it is possible to tailor the way StayPrivate works to t the exact business need. As well as various branding, naming, content and technical options such as deletion rules, there are several system behaviour settings available to System Administrators:

- Functionality. Companies can choose whether to activate Vault (file sharing), Instant Messaging, and Electronic Signatures.
- Primary channel behaviour. As described above, in its standard configuration, StayPrivate creates a primary channel the first time a client user receives a secure email from the company. Company users are automatically added to this channel when they are copied in on subsequent client communications. It is also possible to add further channels for the same client, either from within the portal, or by sending an email with the phrase *'#private'* in the subject field. There are two alternative settings available. Companies can either switch off the default channel behaviour (so that all channels are private) or they can make the default channel behaviour 'strict' so that only Administrators can add users to default relationships.
- Deletion. There is a comprehensive range of settings allowing companies to specify whether and under what circumstances users are able to delete items.
- Reply-to email address. The default setting is for the 'reply-to' email address to be the original sender's email address, rather than the email address for their StayPrivate secure company domain. This enables external contacts to reply directly outside the secure environment as an alternative to sending a secure reply.

This setting can be changed so that the 'reply-to' address is the secure email address, meaning that all subsequent communication should go through StayPrivate. Note that any emails that are sent into the secure domain directly from the external user's email account are not necessarily secure and are automatically marked as originating from outside the secure system.

The setting can also be changed so that emails are sent directly from the corporate email account. To enable this, the company simply needs to add a one-line MX record to their email server.

5.2 User Settings

Company users have a range of settings available to them, such as what notifications they receive and when.

All users have a range of 'preferences' which enable them to tweak the behaviour of the web portal and app to suit their requirements.

STAY PRIVATE

SETUP GUIDE

1. Get Started

To get started quickly we recommend the System Administrator follow these simple steps:

1. Set up company users.
2. Deliver the add-ins, user guides and support to the company users.
3. (Optional) Customise the company environment by adding company logos and colours.

1.1 Setting up company users

There are four ways new users are added to the secure company environment:

	BEST FOR SPEED	BEST FOR CONTROL	CONVENIENCE	ULTIMATE CONVENIENCE
	In bulk	**Account management**	**Via the portal**	**Send an email**
From:	Web Portal, Email	Web Portal	Web Portal, Secure Portal App	Simple Secure Send, SecureMail Add-ins
Available to:	System Administrator	System Administrator, Administrator	System Administrator, Controller, Administrator, Agent	System Administrator, Controller, Administrator, Agent
Name:	Required	Required	Optional	Automatically generated
Username:	Optional	Required	Automatically generated from email prefix	Automatically generated from email prefix
Email/phone:	Optional	Optional	One required	Email required
Password:	Optional	Required	Automatically generated	Automatically generated
User type options:	Administrator, Controller, Agent, Client	Administrator, Controller, Agent, Client	Agent, Client	Agent, Client - automatically generated depending on email domain
Introductory email:	No	No	Yes - sent when new user receives first email	Yes - sent with email
	Send your list to the QUORUM Support client user. Alternatively send via email to support@stayprivate.com.	Click on your name top right of the Web Portal, then select 'Account'. Select the 'Users' tab and click on 'Create New User'.	Click on 'New' bottom left of the Web Portal (or the '+' button in the Secure Portal App), then follow the onscreen instructions.	Send an email. The user or users are created automatically.

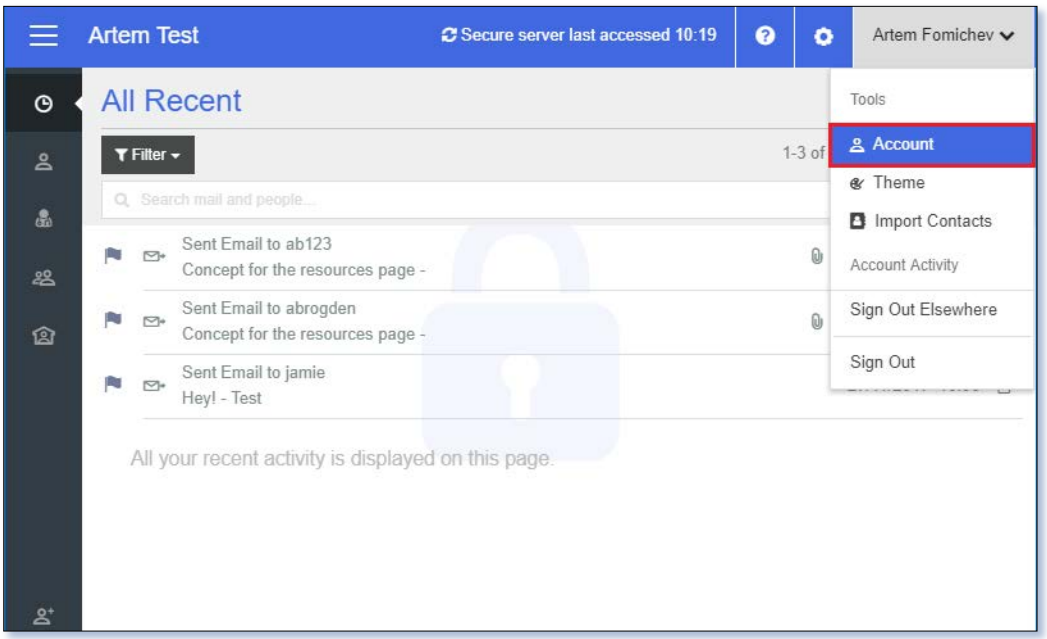
When a user is automatically added, their username is generated using the prefix to their email address. For example, 'johndoe@example.com' would be given the username 'johndoe'. If this user already exists, they would be assigned the username 'johndoe1'. Furthermore, all usernames are subject to a minimum of 5 characters – additional digits are added to usernames if they would be too short.

1.1.1 Setting up users in bulk

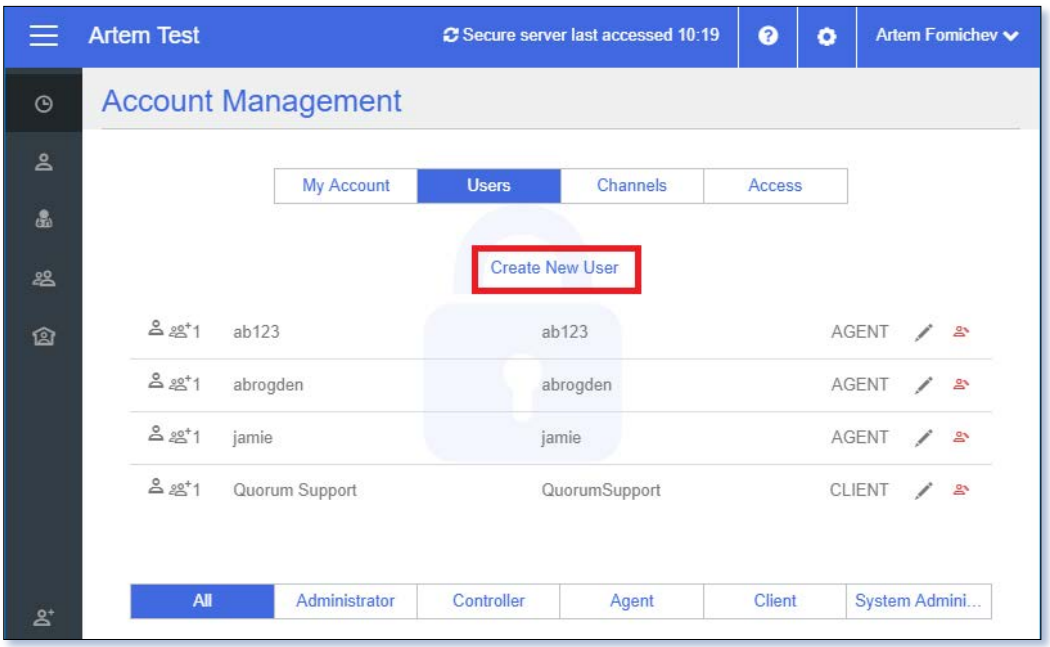
To set up users in bulk, please send the StayPrivate support team (support@stayprivate.com) a list of names, proposed usernames and corporate email addresses. The System Administrator can send this list securely using their company system - StayPrivate Support is automatically added as a client of the System Administrator in all new company environment.

1.1.2 Adding a User via Account Management

By using Account Management to set up users themselves, Administrators can keep close control on passwords, usernames and when users gain access to the system.

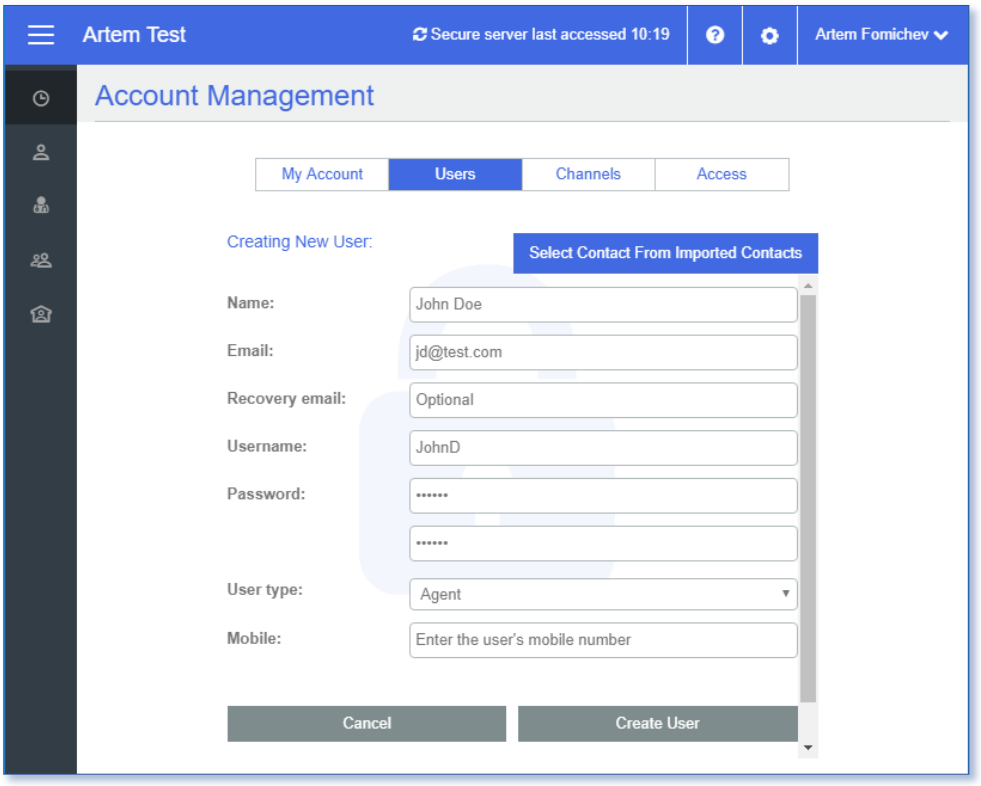


To create a new user using Account Management, go to the **Users** section and click **Create New User**.



Provide the user's details and select **Create User**.

You will be required to set a username and password.

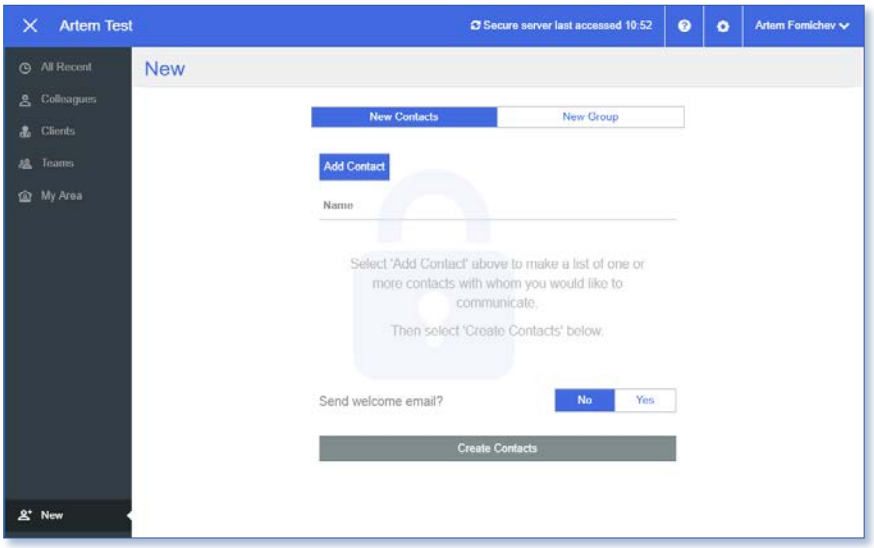


1.1.3 Setting Up Users via the Secure Portal

All company users can add new users and groups from within Secure Web Portal by selecting the **New** button in the bottom left-hand corner. Similar functionality is available in the Secure Portal apps.

1.1.4 Users Added Automatically by Receiving a Secure Email

Each time a new recipient receives a secure email, they are automatically set up as a Client user (exception: if the recipient email address matches the corporate domain, by default, the user is set up as an Agent). Their username and password are generated automatically, and they are notified of these details via a separate email. The first time they access the secure communication, they set their own 4-digit PIN.



Example of a registration email containing username and password:

STAY PRIVATE

To send a private reply to this email or to see your previous correspondence with this sender, please access the Secure Portal at: https://stayprivate.secure-comm.com. You can also reply to this message using standard email, but remember that email is neither secure nor private.

Dear artfomichev,

You have received an email from Artem Fomichev. This email was classified as sensitive and may only be accessed from within the Secure Portal. To read this email click **here** and enter your 4-digit PIN.

Yours sincerely,
STAY PRIVATE

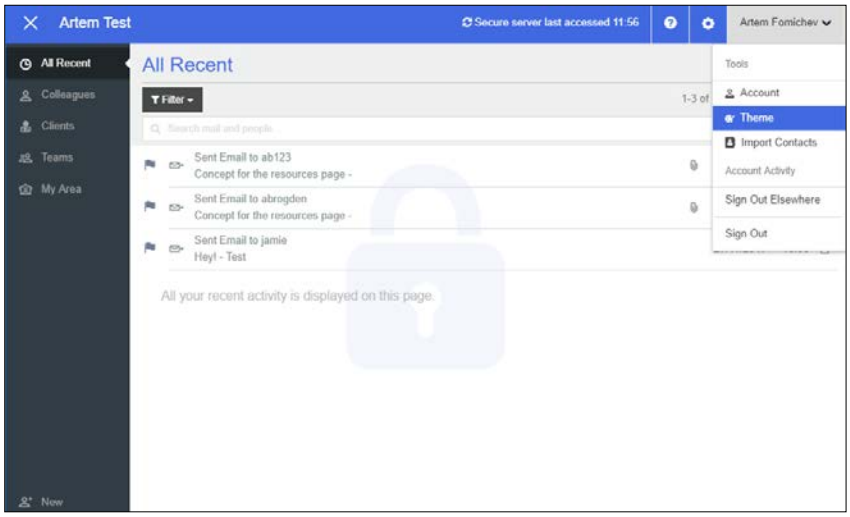
1.2 Delivering Add-ins and User Guides

Company users can send and receive secure communications directly from within their existing corporate email account using one of the StayPrivate add-ins – available for Outlook, Gmail and Microsoft 365. The add-ins make the process of sending a secure email as easy as clicking a button.

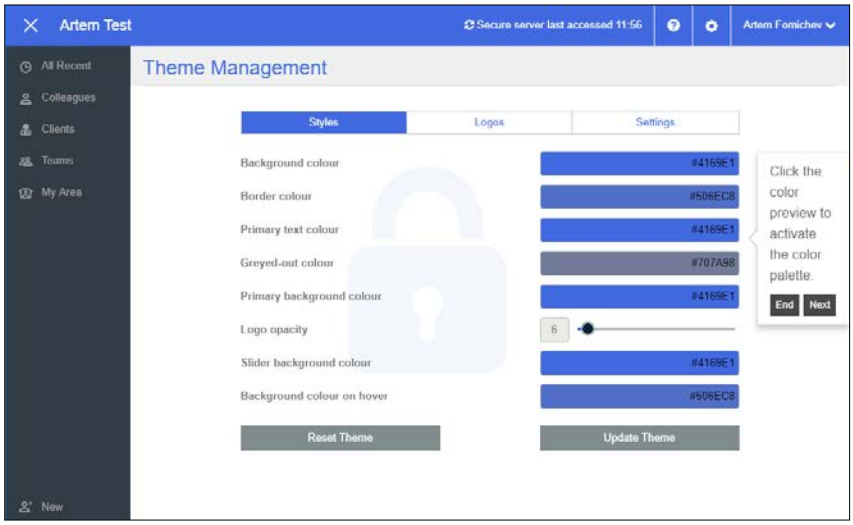
The add-ins and their accompanying installation guides can be downloaded from the Resources page at https://www.stayprivate.com/quorum/resources.html.

1.3 Customise and brand the environment

The System Administrator can personalise the entire environment, including emails, the Secure Web Portal, and the Secure Portal apps with their own branding, including company name, logo and colours. Correct branding not only ensures that users receive a professional experience, but also gives them the confidence that 'they are in the right place', and improves their chances of falling victim to 'phishing'.

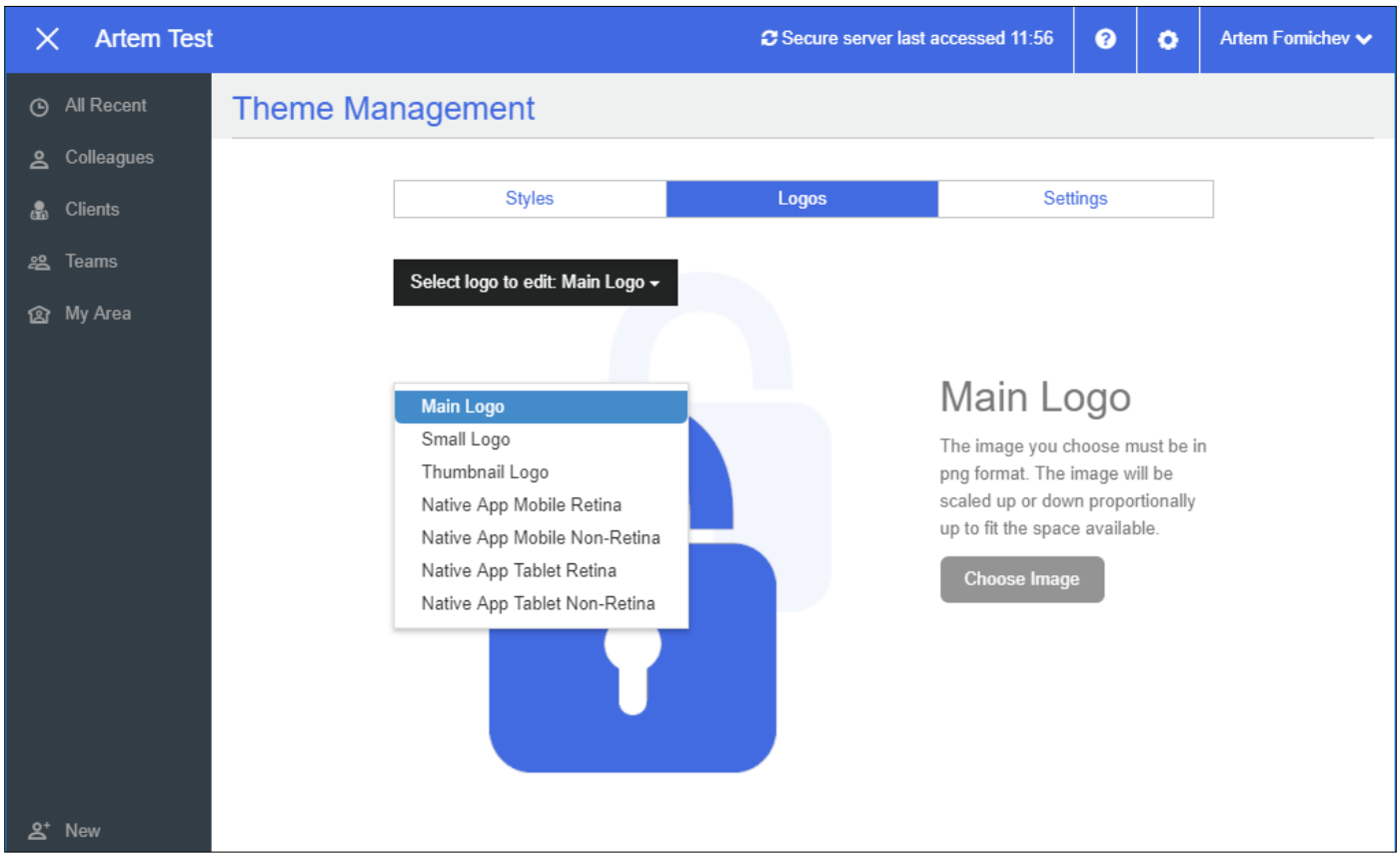


Access the theme settings in the **Theme** section by clicking the drop-down menu in the top right-hand corner of the Secure Web Portal.



Use the **Styles** section to set the colour scheme.

Upload company logos in the **Logos** section. Note that logos should be in **.PNG** format. There are six separate logos, covering all types of devices:



- Main Logo - the Main Logo appears in the background of the web environment at all times.
- Small Logo - the Small Logo appears on the login screen.
- Thumbnail Logo - the Thumbnail Logo appears in secure emails
- Native App Mobile Retina - the Native App Mobile Retina logo appears on the Secure Portal mobile app on mobile devices with retina display.
- Native App Mobile Non-Retina - the Native App Mobile Non-Retina appears on the Secure Portal mobile app on mobile devices without retina display.

- Native App Tablet Retina - the Native App Tablet Retina logo appears on the Secure Portal mobile app on tablet devices with retina display.
- Native App Tablet Non-Retina - the Native App Tablet Non-Retina logo appears on the Secure Portal mobile app on tablet devices without retina display

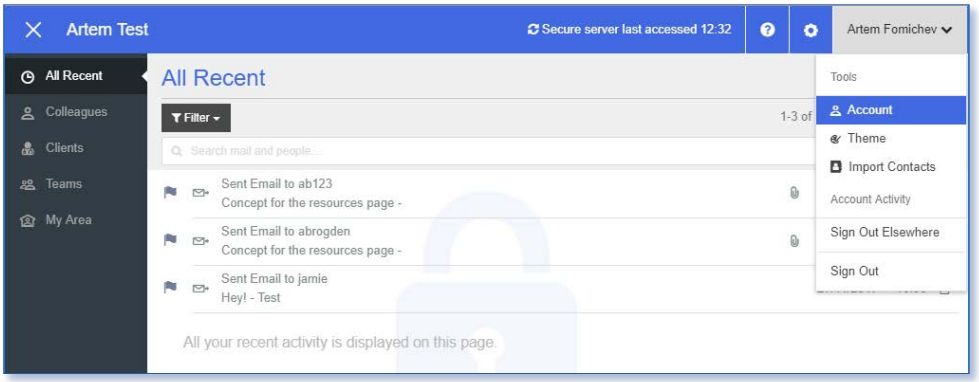
To add your **company disclaimer** to StayPrivate emails please supply your disclaimer, in HTML format, to support@stayprivate.com.

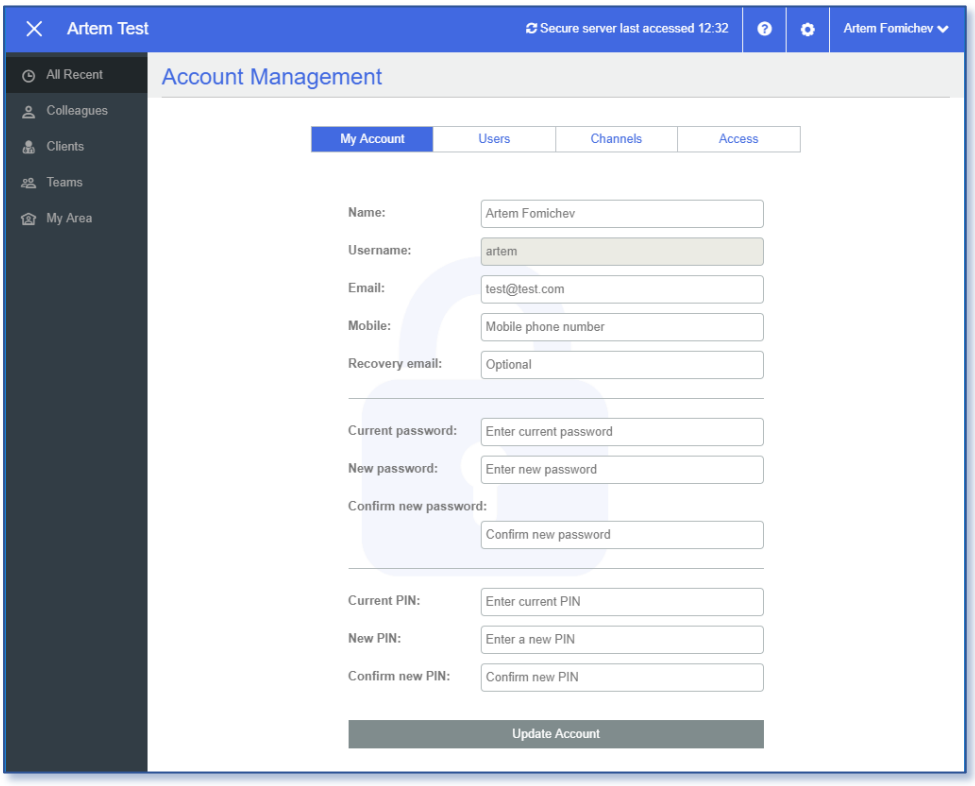
2. Managing Accounts, Users and Groups

Administrators can create, delete and edit user accounts, reset passwords and PINs and create, delete and edit private channels.

2.1 Account Management

Access the account management area section by selecting Account under the drop-down menu in the top right-hand corner of the secure web portal.

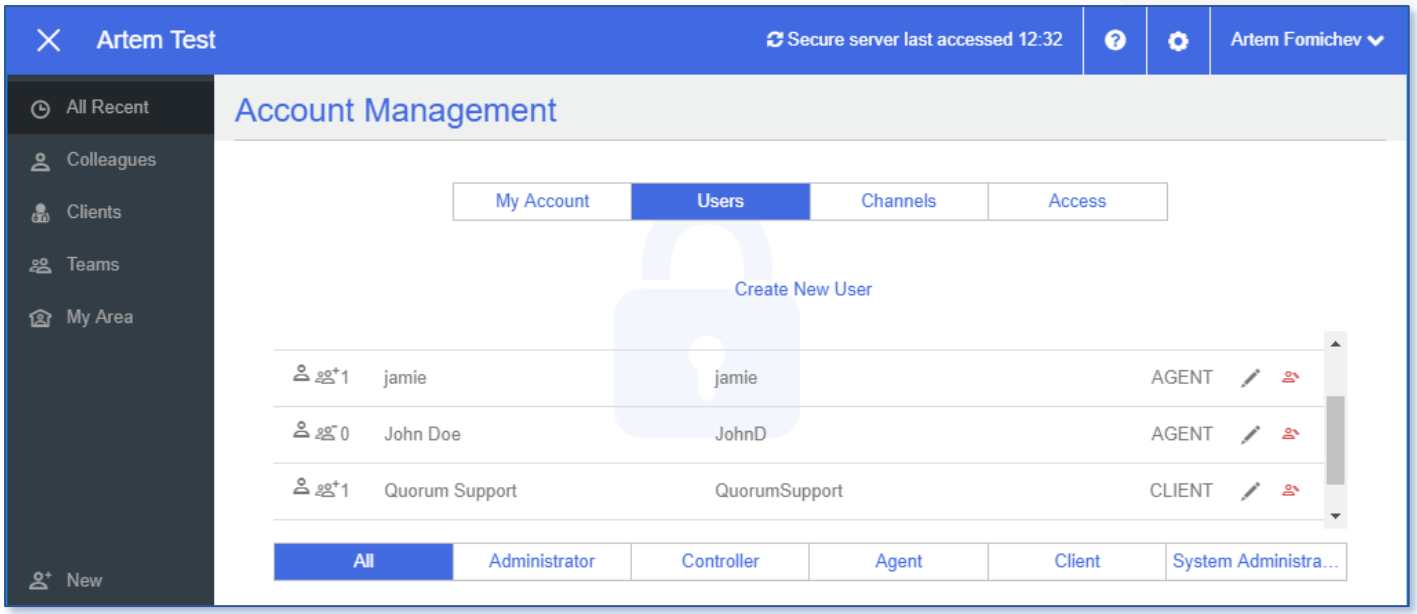




The My Account section allows users to update their own account details, including email, password and PIN.

2.2 Editing and Deleting Users

Administrators can see the list of users they administer in the Users section.



Edit users by clicking the symbol on the right-hand side of the user's details.

Administrators can edit a user's name, email address, password, PIN, user type and mobile number.

Administrators can also edit the private channels (groups) that a user is a part of: they can rename a channel, remove a user from any channel, add them to another existing channel or create a whole new channel.

To delete a user, click the symbol to the right-hand side of the user.

2.3 Private Channels

All communications are carried by a private channel. Similar as for users, new private channels are created in three ways:

- Automatically – by receiving a secure email.
- By being added by another user via the Secure Portal.
- By being added by an Administrator via Account Management.

All participants in a channel can see (with a few minor exceptions) all activity associated with that channel, including the identity of other members of the channel. This is what we call transparent privacy. It means that information is not only private, but that users can see that it is private.

2.3.1 Primary Channels for Clients

StayPrivate automatically creates a primary communication channel between the company and each client (or group of clients) the first time a secure email is sent to the client (or group of clients). This ensures that all communications stay in one place and are available to all the necessary users.

In the standard configuration, additional company users can be added to the primary channel by an existing (non-client) member copying in another (non-client) user on a secure email to the client. Additional company users can also be added by the administrator.

If a company user who is not a member of the primary channel attempts to contact the client securely, they receive an error message explaining that a primary channel already exists with this client and that to send a secure email to the client they need to either get themselves added to the primary channel or to create a separate private channel with the same client – which they can do by including '#private' in the subject field of the secure email.

2.3.2 Strict Primary Channels

For companies which wish an extra level of control, it is also possible to enforce 'strict' primary channels. In this case, only an administrator can change the members of a primary channel.

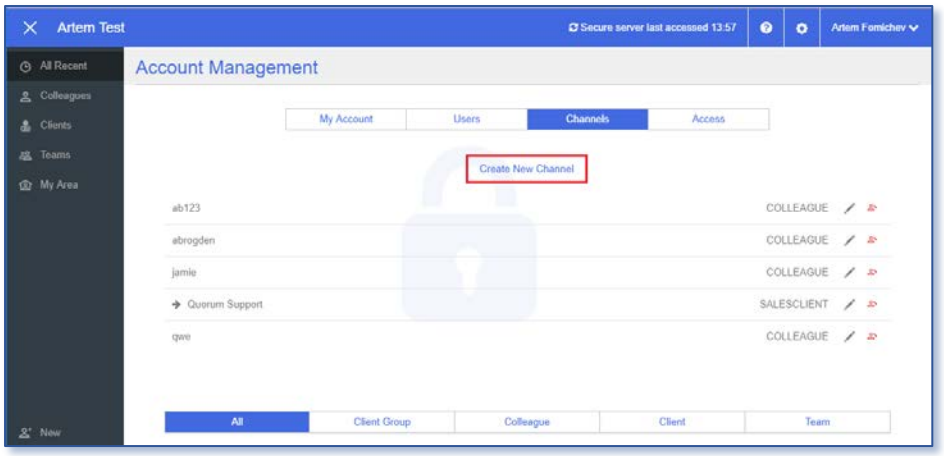
Additional private channels can still be created as required by users including '#private' in the subject field as above.

2.3.3 No Primary Client Channel

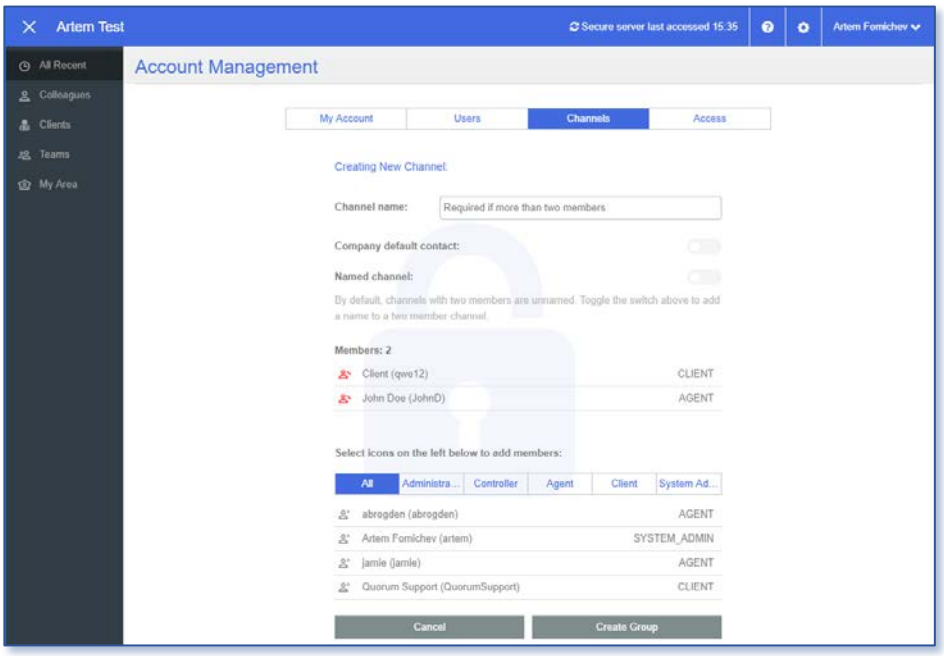
Companies can also choose to switch off the primary channel behaviour entirely, so that a separate private channel is created every time a new company user contacts a client.

2.3.4 Creating a One-to-One Channel or Group

The Channels section allows Administrators to create new private channels for users. Create a new channel by clicking **Create New Channel**.



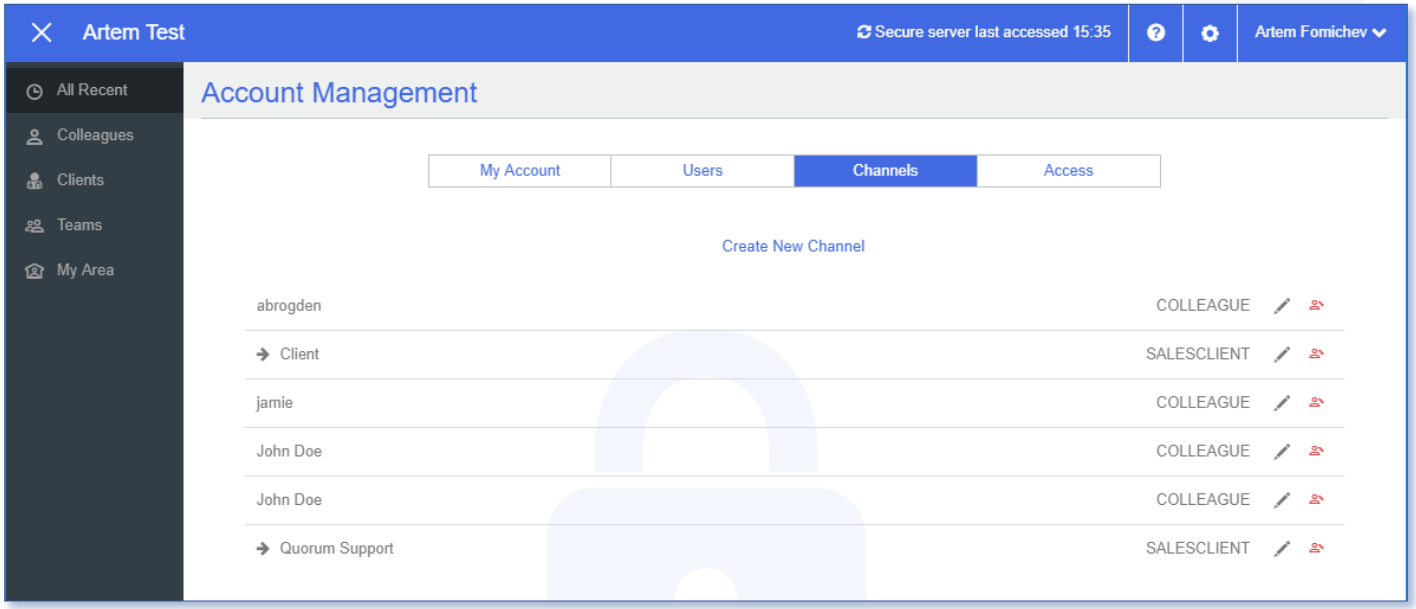
To create a one-to-one channel between two users, click the symbol next to the users that you would like to set up together. For a one-to-one channel you do not have to specify a **Channel Name.**



If creating a one-to-one channel between a company user and a client, you can choose whether to make this the primary channel for that client by checking **Company default contact**.

2.3.5 Editing and Deleting Channels

After creating channels, they can be viewed in the **Channels** section within Account Management. The number to the left-hand side of each channel represents the number of members of that channel. The symbol → indicates the client's primary channel.

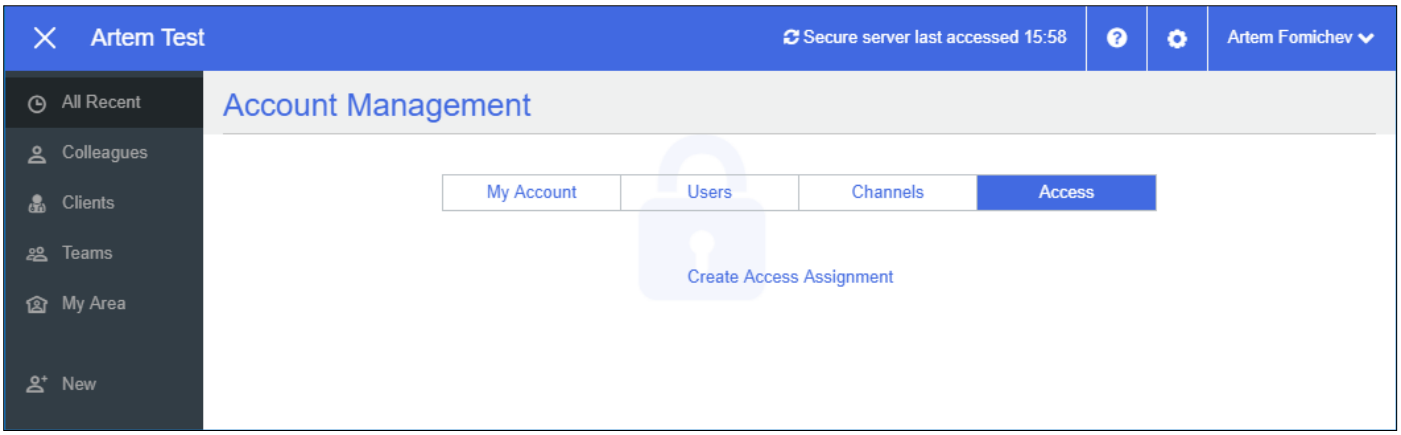


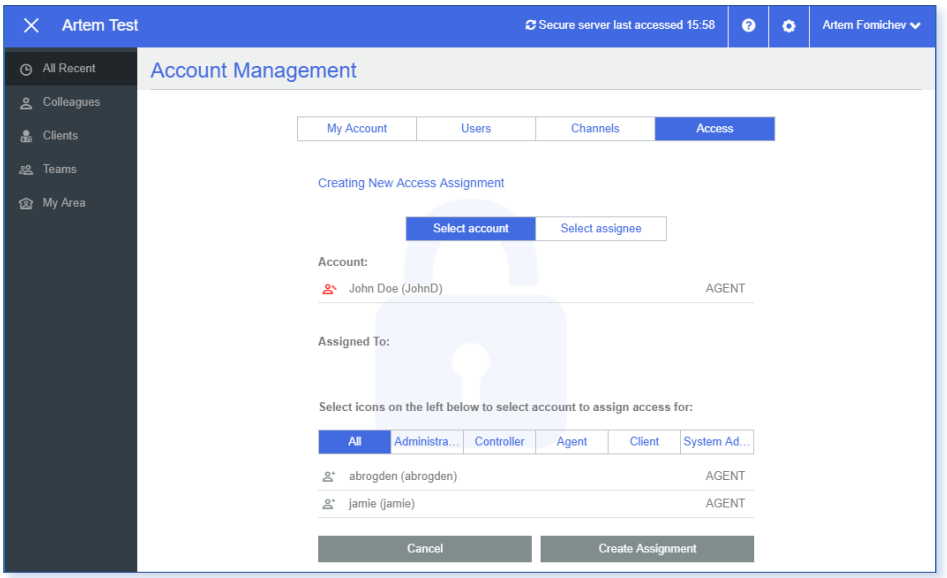
To edit channels, click the edit symbol to the right-hand side. You can add or remove users as necessary. For companies using Strict Primary Client Channels, this is the only way to add new users to the primary channels. To delete channels, click the  symbol on the right-hand side.

2.4 Managing Access

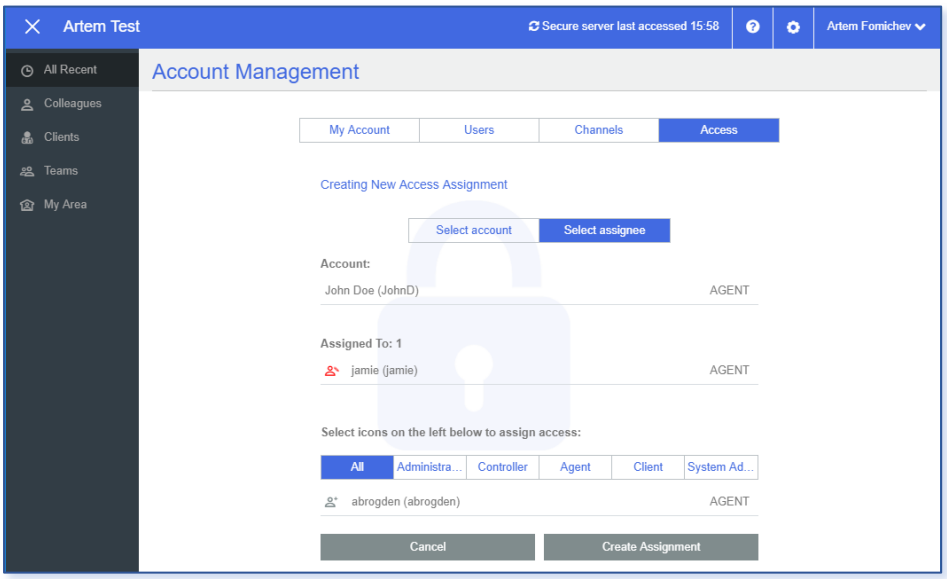
The system administrator can grant Agent users access to other Agent user accounts. This enables another user to do work on behalf of the Agent and can be useful if, for example, a user has a PA, or to provide holiday cover. To preserve the integrity of the audit history, StayPrivate records the name of the user who actually performed the activity as well as the person it was performed on behalf of. This information is not displayed to client users.

To grant access to user accounts go to the **Access** section and select **Create Access Assignment.**





Select the user whose account you would like to grant access to.



Select **Select Assignee** and choose the user who you wish to grant access to and then press **Create Assignment**.

3. Further Information

For more information and user guides (for the add-ins, portal etc.) please see the Resources page at: https://www.stayprivate.com/quorum/resources.html