STAY PRIVATE

Quick Setup Guide

Table of Contents

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 company users.
3. (Optional) Customise the company environment by adding company logos and colours

1.1 Setting up company users

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 a user with this username already exists, they are assigned the username 'johndoe1' etc. Furthermore, all usernames must be a minimum of 5 characters – additional digits are added to usernames in order that they are not too short.

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

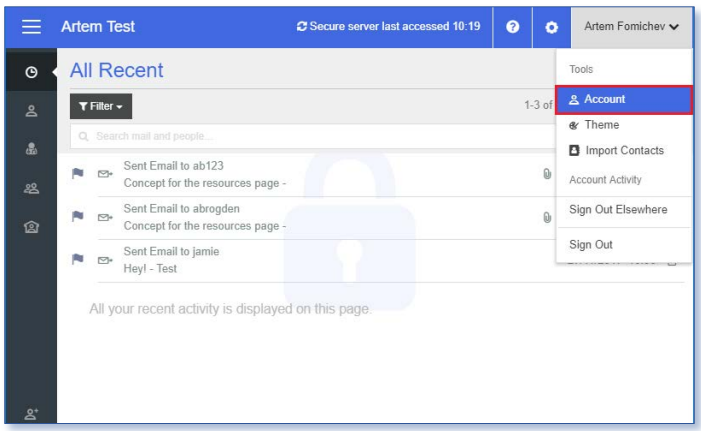
	BEST FOR SPEED	BEST FOR CONTROL	CONVENIENCE	ULTIMATE CONVENIENCE
	In bulk	**Account management**	**Via the portal**	**Send an email**
From:	Web Portal, Email	Web Portal	Web Portal, Secure Portal App	Simple Secure Send, SecureMail Add-ins
Available to:	System Administrator	System Administrator, Administrator	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 StayPrivate 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.

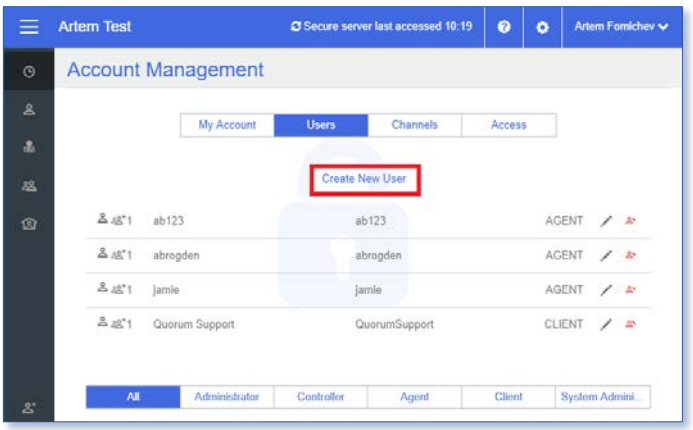
1.1.1 Setting up users in bulk

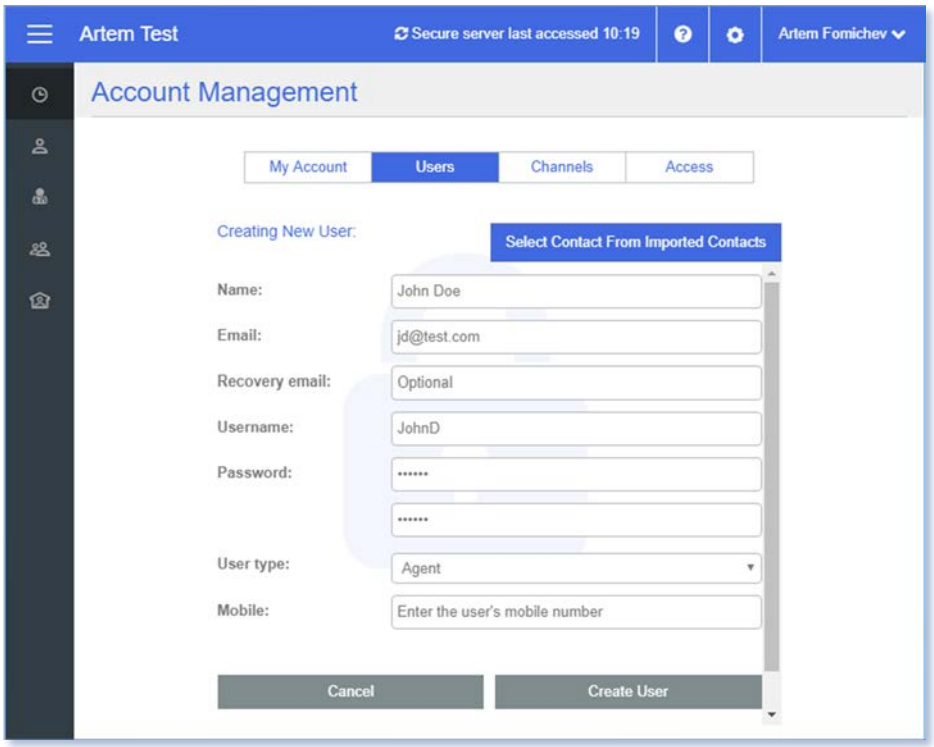
To set up users in bulk, please send the StayPrivate support team (support@stayprivate.com) a list of names, proposed usernames and corporate email addresses. The System Administrator can send this list securely using their company system – StayPrivate Support is automatically added as a client of the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



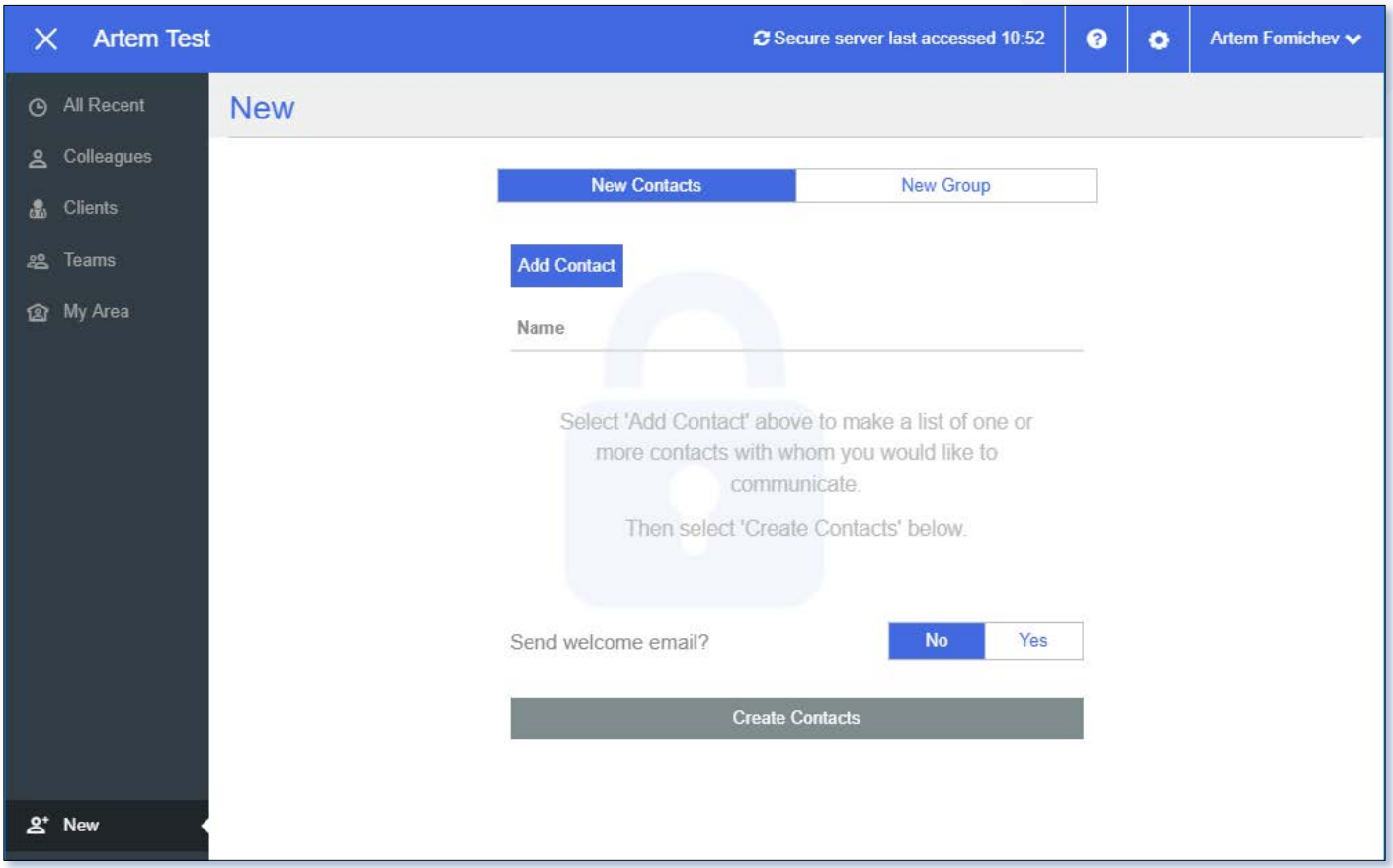




Provide the user's details and select **Create User**. You will be required to set a username and password.

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

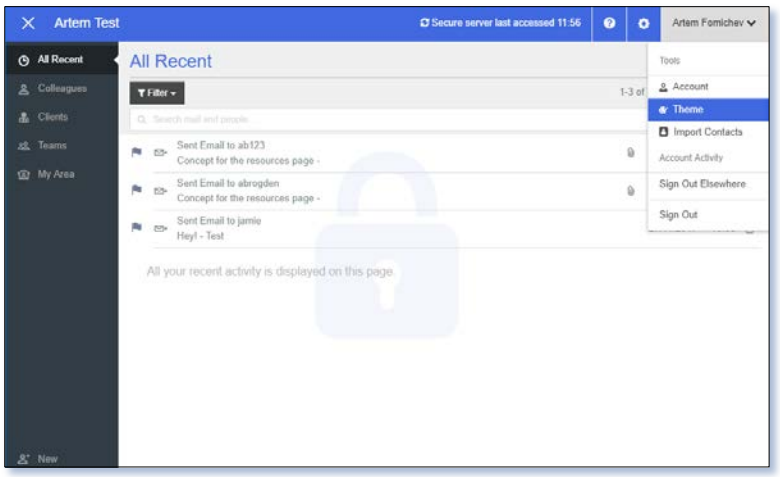
1.2 Delivering Add-ins, User Guides and Support

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.

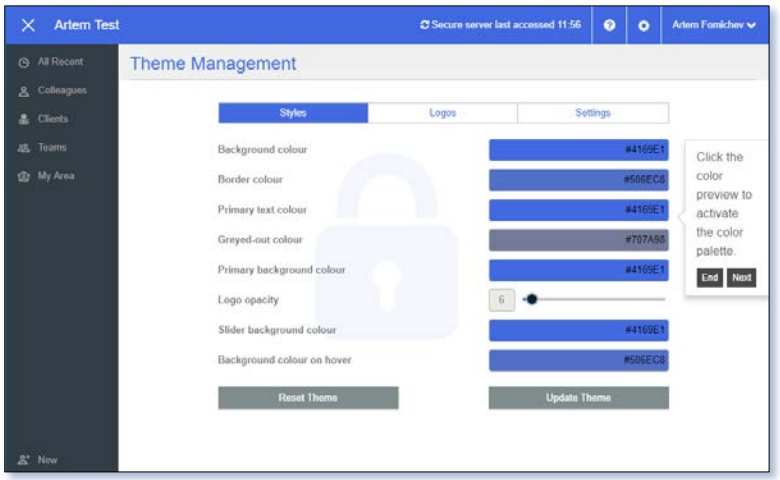
The add-ins and their accompanying installation guides can be downloaded from the Resources page at https://www.stayprivate.com/quorum/resources.html.

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 reduces their chances of falling victim to 'phishing'.

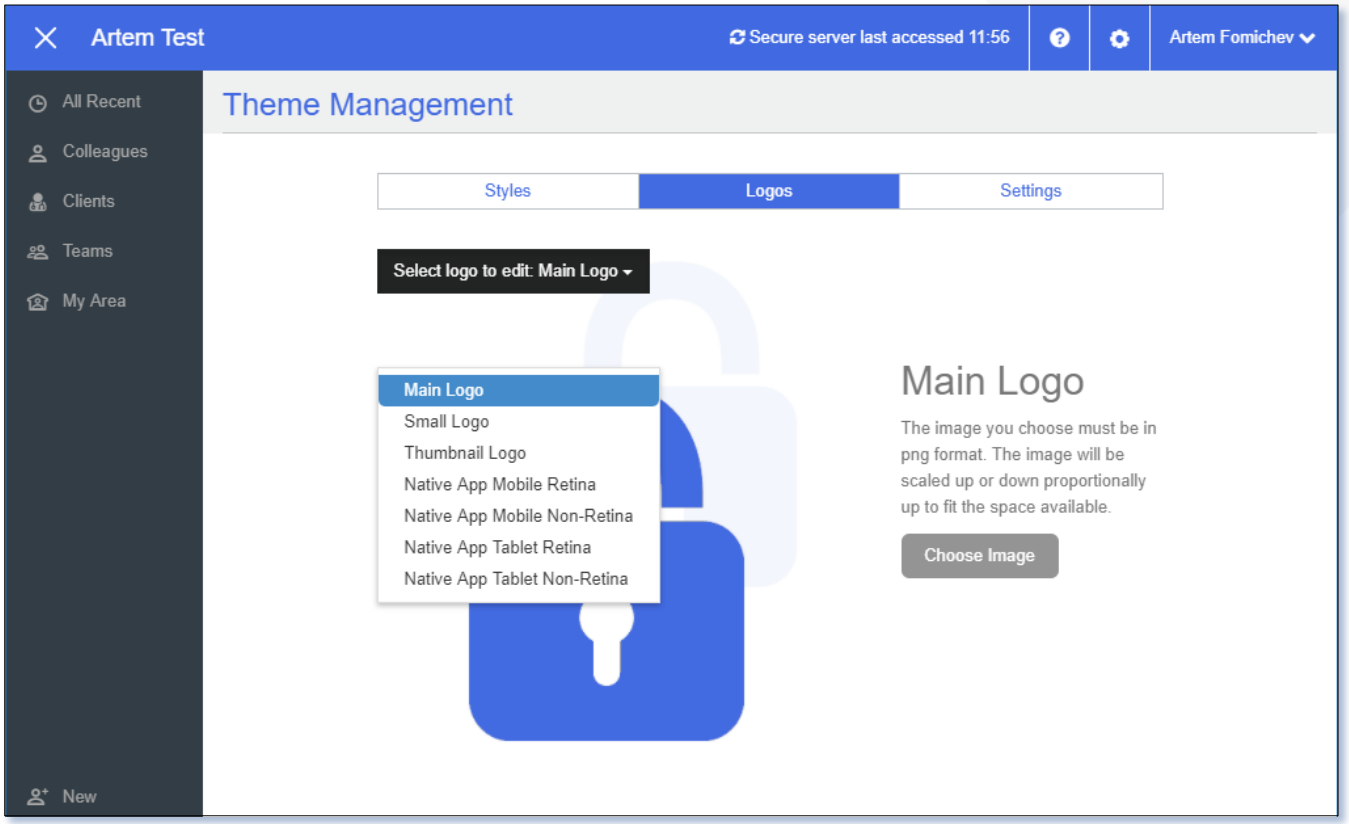


Access the theme settings in the **Theme** section by clicking the drop-down menu in the top right-hand corner of the Secure Web Portal.



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 log in 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

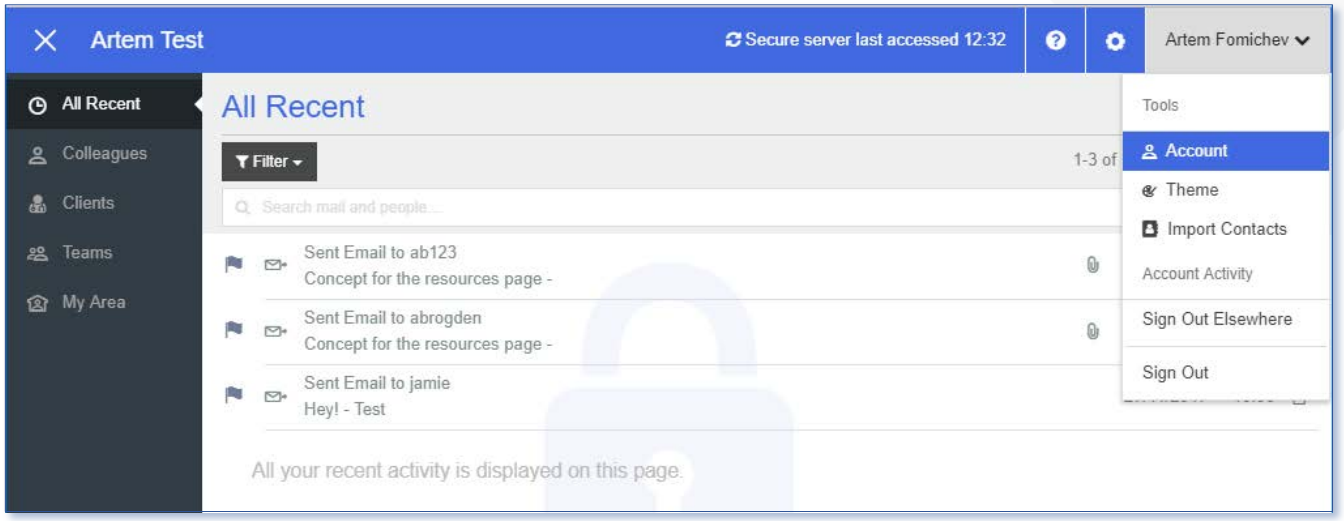
To add you **company disclaimer** to StayPrivate emails please supply your disclaimer, in HTML format, to support@stayprivate.com.

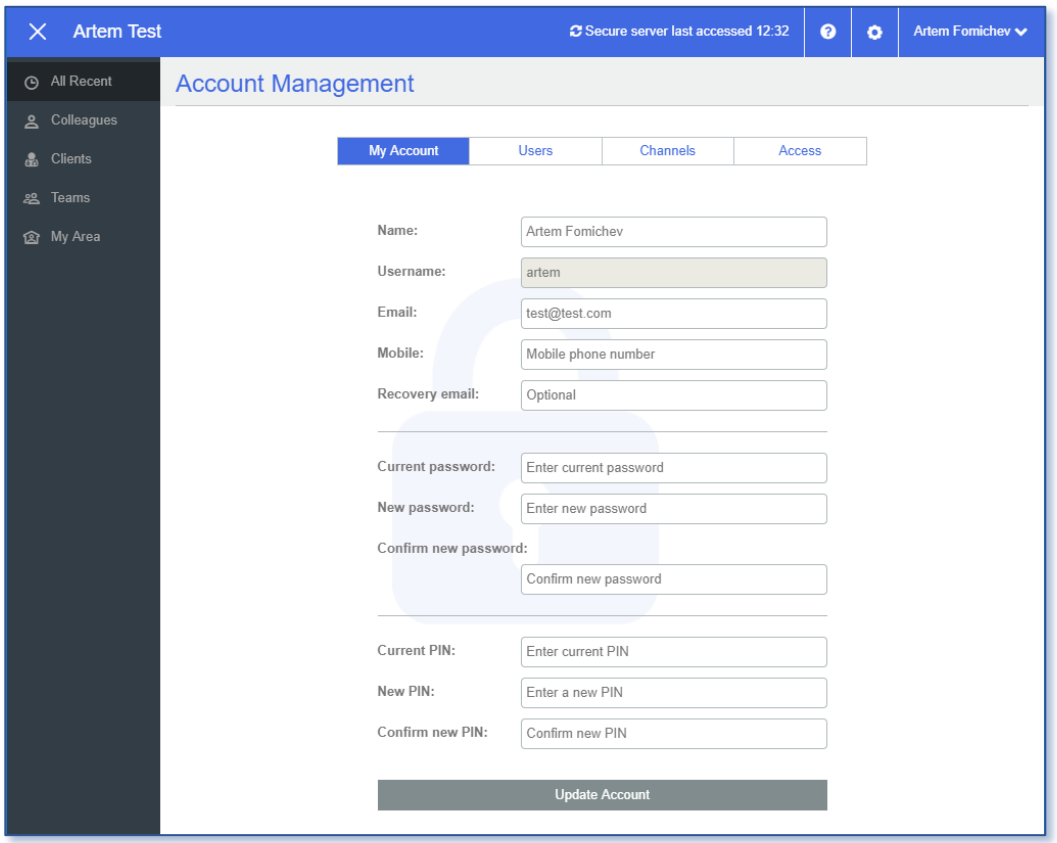
2. Managing Accounts, Users and Groups

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.

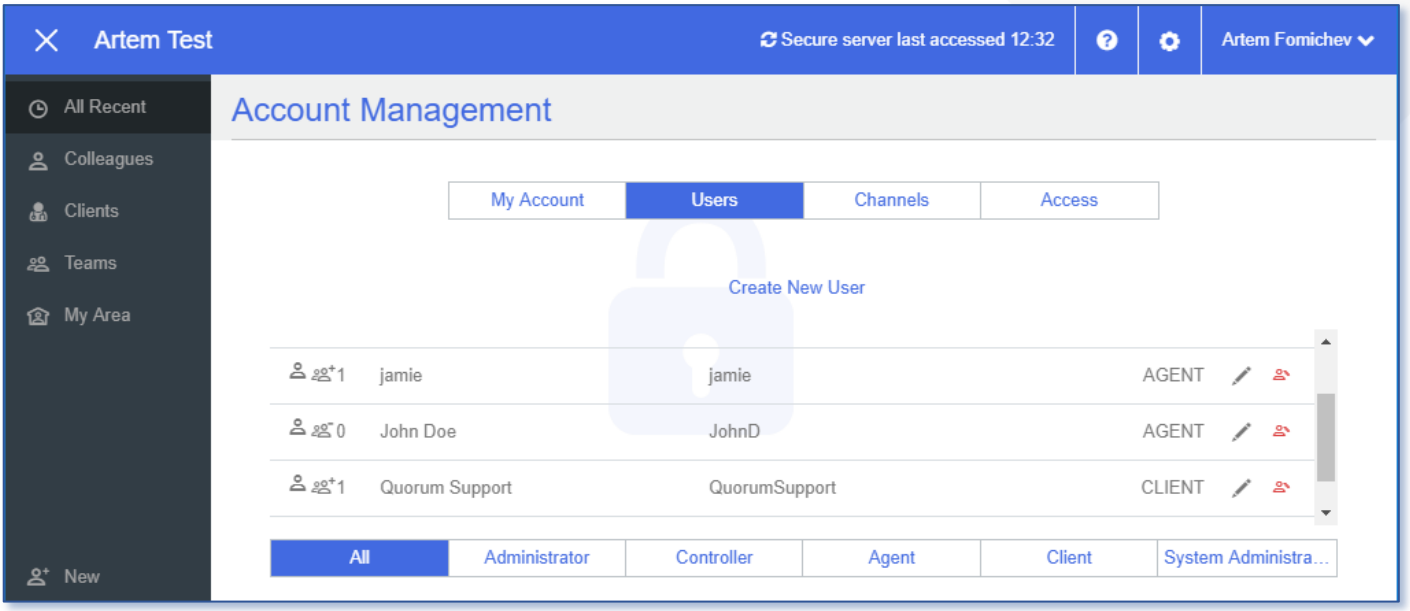




The My Account section allows users to update their own account details, including email, password and PIN.

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 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.

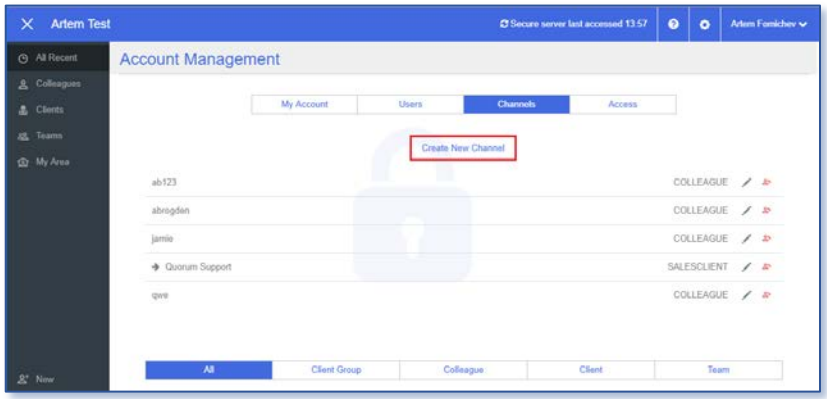
Additional private channels can still be created as required by users including '#private' in the subject field as above.

2.3.3 No Primary Client Channel

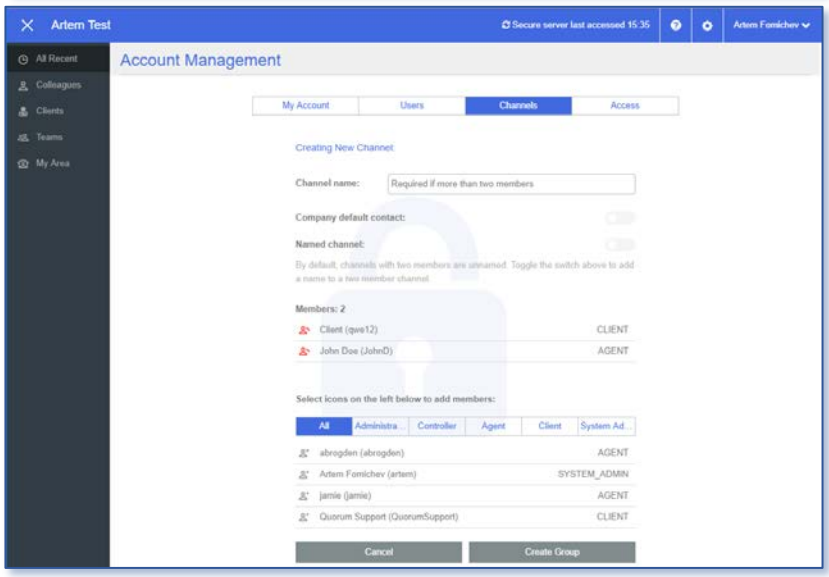
Companies can also choose to switch off the primary channel behaviour entirely, so that a separate private channel is created every time a new company user contacts a client.

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**.



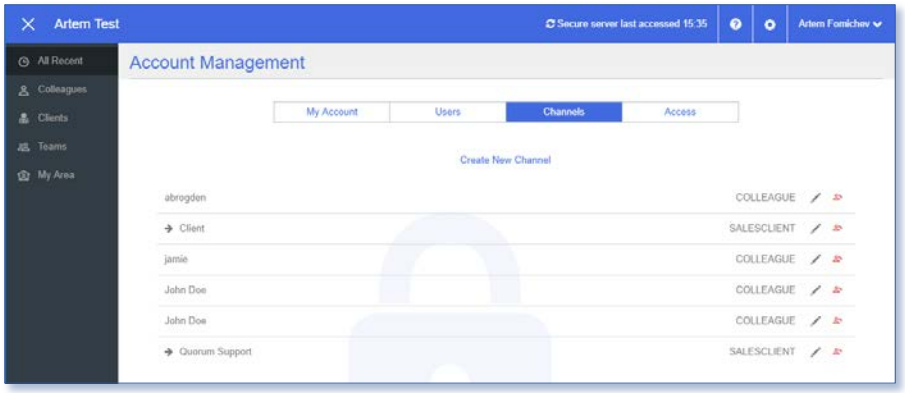
To create a one-to-one channel between two users, click the symbol next to the users that you would like to set up together. For a one-to-one channel you do not have to specify a **Channel Name.**



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

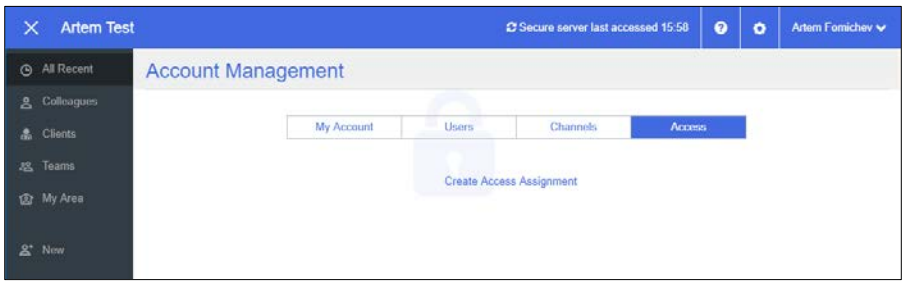
After creating channels, they can be viewed in the **Channels** section within Account Management. The number to the left-hand side of each channel represents the number of members of that channel. The symbol → indicates the client's primary channel.



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.

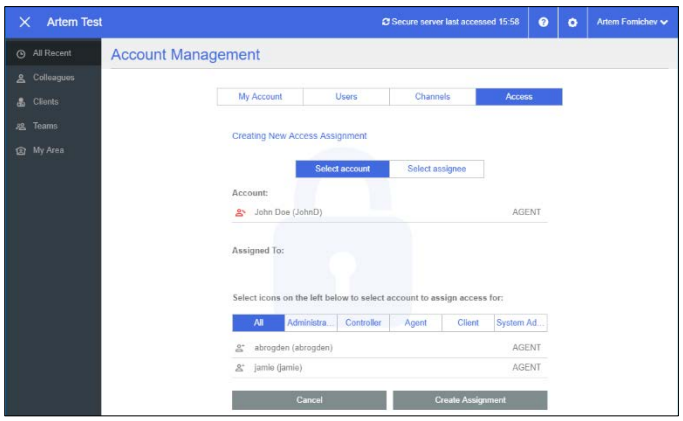
2.4 Managing Access

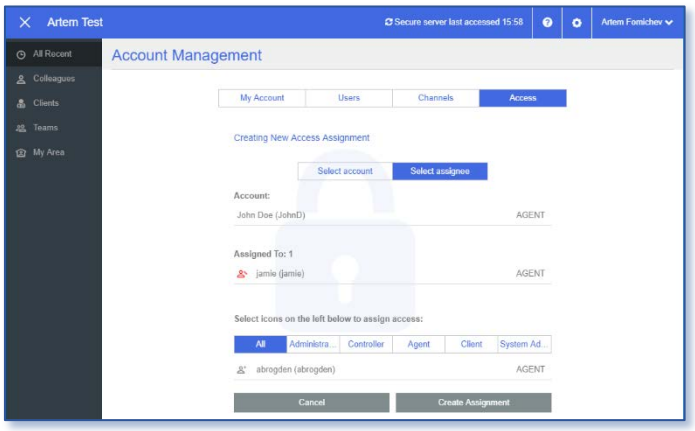
The system administrator can grant Agent users access to other Agent user accounts. This enables another user to do work on behalf of the Agent and can be useful if, for example, a user has a PA, or to provide holiday cover. To preserve the integrity of the audit history, StayPrivate records the name 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**.

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