CONTENT GURU
Engagement Made Easy®

storm®
FedRAMP™

Security Admin Guide

Document Revision 1.0.0

Version 5

Classification - Public

Contents

1 What's New in This Release

FedRAMP revision	Doc revision	Date	Change history
5	1.0.0	27 Feb 2026	Initial release.

Added in Previous Releases

FedRAMP revision	Doc revision	Date	Change history
N/A	N/A	N/A	N/A

2 About This Document

Welcome to the Recommended Secure Configuration (RSC) guide for **storm**®.

storm is a FedRAMP authorized cloud service.

This guide provides guidance for securely configuring and managing top-level administrative accounts in **storm**. It is designed to help FedRAMP customers understand administrative roles, account lifecycle processes, and security settings, while maintaining compliance with FedRAMP requirements.

storm offers a variety of configuration options. This guide focuses on topics of significant security implications and provides recommended best practices to help agencies make informed decisions. By following this guidance, organizations can reduce misconfiguration risks, maintain secure operations, and ensure proper administration of critical accounts throughout their lifecycle.

Guide revision 1.0.0

FedRAMP revision 5

Classification: Public

Copyright and Disclaimer

What's New in This Release

> **Note:** this is a customer-facing guide and does not cover internal Content Guru administration.

This guide is publicly available and versioned in accordance with FedRAMP guidance.

FedRAMP Alignment

This guide is intended to satisfy the following FedRAMP Rev. 5 RSC requirements:

FRR-RSC-01: Secure access, configuration, operation, and decommissioning of top-level admin accounts.

FRR-RSC-02: Explanation of security settings and their impact.

FRR-RSC-03: Guidance for privileged (non–top-level) accounts.

FRR-RSC-04: Secure defaults applied at provisioning.

System Requirements

storm products are accessed via your web browser.

The following browsers are supported:

- **Microsoft Edge**
- **Mozilla Firefox**
- **Google Chrome**

It is recommended that you use the latest available stable version of the relevant browser, with all critical security updates and patches installed. If you have a requirement to use an earlier version of a browser, contact your support representative for advice.

Licensing

All features of this software are licensed. Not all users will have access to every feature detailed in this help. Access to certain features depends upon your installation settings, user rights and licensing agreements. Contact your commercial representative for further details.

3 Administrative Account Roles

You cannot access, configure, operate, and decommission the top-level administrative account that controls enterprise access to the **storm** platform. This is handled internally at Content Guru.

Security-related settings that can be operated only by top-level administrative accounts are not customer facing and are handled internally at Content Guru.

Top-Level Administrative Roles

This describes all roles that meet the FedRAMP definition of top-level administrative access.

Role	Description	Permission Level/Impact	Security Recommendations
Content Guru Admin	Top level admin account only used by qualified Content Guru engineers.	Full access.	Only accessible by Content Guru.

Privileged (Non–Top-Level) Roles

Role	Description	Permission Level/Impact	Security Recommendations
Customer Administrator	Customer admin accounts are created by Content Guru.	This gives the Customer Admin access to features and products dependent on their licensing rights. within their partition on the **storm** platform and excludes global configuration options. **Note:** not all permissions are granted to customers by default.	This is to be held only by top level administrators within your organization.

4 Account Lifecycle

Top-Level Accounts for Customers

Customer administrator are created, edited and deleted by internal Content Guru engineers. It is the responsibility of the customer to ensure that only appropriate trust-worthy individuals from within their organization have access to these accounts.

Create **storm** Users in UC

You can create users singly or in bulk. Each user is assigned a user type, which can be one of the following:

User Type	Description	Number
PBX User (fixed seat)	The user can access standard UC functions. (This user type is provided to support a legacy licensing model).	0
Meeting Room	This user type is used to assign licenses to devices such as meeting room conference phones or fax devices that do not require advanced features such as voicemail or call forwarding.	1
PBX User	The user can access standard UC functions.	2
Inbound Agent	The user can access standard UC functions, and also work as a CONTACT agent handling inbound calls only.	3
Dialer Agent	The user can access standard UC functions, and also work as a CONTACT agent handling inbound and outbound calls.	4
Supervisor	The user can access standard UC functions, and work as an inbound and outbound CONTACT agent; and is able to monitor and control agent groups assigned to them.	5
CONTACT Switchboard Operator	Provides access to SWITCHBOARD functionality to allow the user to manage voice calls and non-voice communications.	6
PBX Switchboard Operator	Provides access to SWITCHBOARD functionality to allow the user to manage voice calls.	7

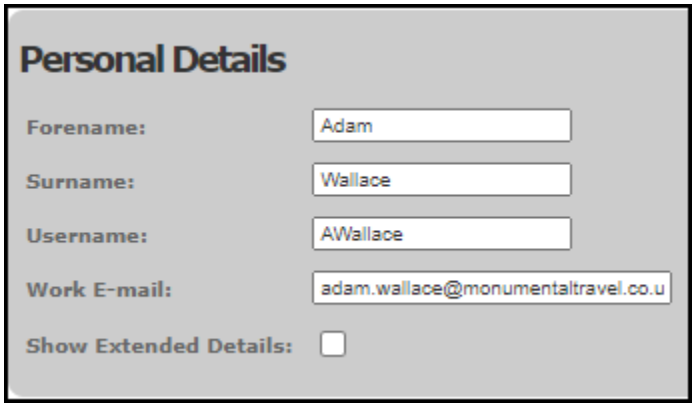
User Type	Description	Number
Supervisor Switchboard Operator	Provides access to SWITCHBOARD functionality and to Supervisor functionality (described above) to allow the user to supervise non-voice communications.	8
MS Teams User	The user can access standard UC functions, and can also use MS Teams (instead of **storm** DTA) to make and receive calls.	9

The user type assigned to a user governs what license they will need.

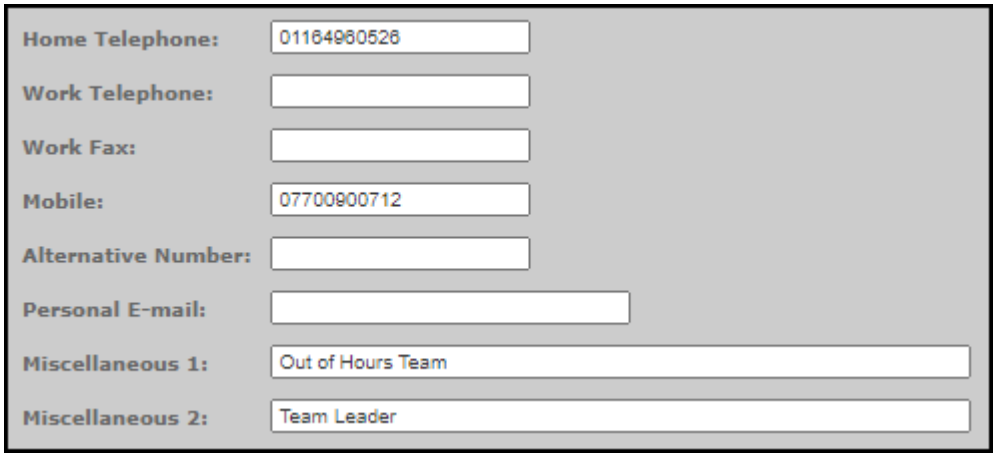
In addition to the user types described above, UC and CONTACT also has administrators, who are able to perform system configuration. Administrators are set up for you by Content Guru.

Add a Single User

1. Ensure that you have created at least one user group and one service type.
2. Select **Users** > **Add User**.
3. If the user is already known to the system, click the **Create UC Account for Existing** option. Otherwise, leave the **Create New User** option selected.
4. On the **Select User Role** panel, ensure that the **Standard User** option is selected. The other options are included for backwards compatibility.
5. On the **Personal Details** panel, enter the user's forename, surname, and your chosen username. The remaining fields are optional.

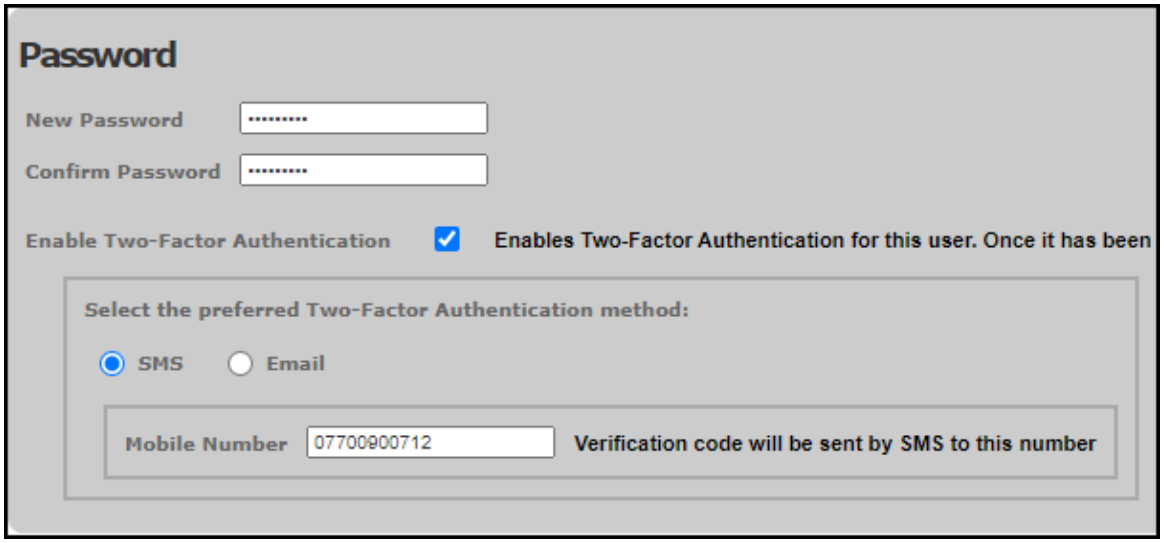


6. Select **Show Extended Details** to display further fields for recording additional details about the user.



> **Note:** if your organization has implemented Phonebook functionality, any custom user fields created by **storm** administrators in DTA are listed here, so that they can be populated with suitable values. See the *DTA User Guide* for information on creating custom user fields.

7. On the Password panel, enter the user's password for use with the DTA interface.



In addition to any rules imposed by your organization, the password must be at least nine characters long and must not contain the user's first name, last name, username or organization name.

8. On the **User Details** panel, select the user's user group, the site, and the user type as a minimum. Also change the **Initial Status** to 'Active' if the user is ready to start using the system.

General Settings	Notes
Roaming?	Select this check box if the site where the device is located may vary.

General Settings	Notes
	Note: this setting is important for emergency calls to services such as 913 and 911. If a device is set to Roaming, emergency calls will be presented to emergency operators with a code indicating that the caller may not be at the registered location for the device. Any devices which may be used at alternative locations must have this option selected.
Inherit Outgoing Domain Settings?	Select this check box if the user is to inherit the organization's outbound domain settings. To configure individual outbound domain settings for the user, clear this check box and use the fields that appear to define those settings.
ANI Presentation	The number presented as the calling party's number on outbound calls made by this user. Options are: **Use Service Type Default:** the value provided by the service type. **Organization**: the organization's number. **Destination Address:** deprecated, do not use. **Other ANI:** a custom ANI (for example the user's DID). **Note**: for calls to mobile networks, the ANI presented on the mobile device might not match what is entered here. This is because mobile networks choose to use either the presentation or network ANI. **Site ANI:** the ANI defined for the site where the user is currently logged in.
Network ANI	Provided for backward compatibility. Do not use.
User Type	The user type.
Initial Status	Set this to 'Pre-active' until you are ready for the user to start using the system. Setting it to 'Active' allocates the required licenses to the user. **Note**: changing a user's status from 'Pre-active' to 'Active' is not reversible (after saving the user details). Set a user to 'Pre-active' if the user is still required but is currently not needed to be 'Active'.
Ringback Tone	Select either a specific ringback tone or 'Use Service Type Default' to use the ringback tone set up for the service type assigned to this user.

General Settings	Notes
SIP Endpoint Device	Select this option when the user will be using a device connected to the organization's legacy PBX. Ensure the user is assigned an extension in a range/prefix mapped to a SIP endpoint.
PSTN Device	This option is used in conjunction with the DTA. If you select this option, the **Outbound telephone number** field is displayed. Enter the number that will be dialed when the system makes an outbound call to the user. **Note**: if you clear this feature for a user, their PSTN device is immediately logged out, meaning that they will no longer receive calls.
Padlock Username/ Padlock Password	These allow you to provide credentials to be used instead of the default PADLOCK merchant credentials that are sent to the organization's payment interface for transactions initiated by this user.
Speed Dial Profile	Select the speed dial profile to be assigned to this user. The profile you assign here overrides any speed dial profile assigned at user group or organization level.

9. On the **User Pairing Details** panel, either leave or overwrite the user code (starcode) that the user will use to log in to an IP phone. Enter the security code that is required for log in in both fields provided.
10. On the **Select Service** panel, select the service type (feature set) to assign to the user.
11. Click **Add User**.

Add Multiple Users (In Bulk)

1. Select **Users > Export Users** and then **Continue.**
2. Open the exported CSV file and add new user details under the existing column headings. You must provide a valid password in the **Password** column.
3. Save the edited file.
4. Select **Users > Import Users**.
5. Set **Reassign user extensions?** as required, then follow the on-screen instructions. (See the description of the **Extension** field for an explanation of what **Reassign user extensions?** controls.)

As the file is imported, **storm** calculates what licenses are needed and advises you of any shortfall.

The CSV file must contain a header row with the following fields:

Forename,Surname,Username,Password,Home Tel,Work Tel,Work E-mail,Work Fax,Mobile,Personal E-mail,User Group,ANI Presentation Type,User Type,Status,IP Address,Ringtone ID,Star Code,Security Code, Service Type,Extension,Destination Addresses,Billing Account,Alternative

Number,Whisper Prompt?,Forward Internal to Voicemail on Busy?,Forward External to Voicemail on Busy?,Disable Mailbox PIN?,Mailbox PIN,Mailbox Intro Type,Mailbox E-mail Address,E-mail Notification?,E-mail Attachment?,Max Mailbox Messages,Recording Service,Outbound Call Barring Profile,Site, Roaming?,storm Contact Agent?,Supervisor,PSTN Device?,Persistent Inbound Enabled?,Persistent Outbound Enabled?,Persistent Routing DID?,Network ANI Type,Restrict ANI?,Lync Agent?,Use Username as Lync Account?,Lync Account,Recording Mode,SAP User?,Use Username as SAP Account?,SAP Account,CRM User?,Use Username as CRM Account?,CRM Account,Require Agent Desktop Logon?,Domain,Inherit Outgoing Domain?,Outgoing Domain,Use Outgoing Domain in From Address,Specify Outgoing From Domain,Outgoing From Domain,Speed Dial Profile2,FA User?,2FA Method,2FA SMS Number,2FA Email Address,Use Outgoing Domain for PSTN Agent Calls,MS Teams DID,MS Teams Azure ID,Miscellaneous 1,Miscellaneous 2,storm WFM Contract Template

Note: if your organization has implemented Phonebook functionality, any custom user fields are included in the CSV file, using as their column headings the field names given to them when they were created. See the *DTA User Guide* for information on setting up custom user fields.

The on-screen field descriptions explain what these fields hold. The following table provides additional information, where necessary:

Column heading	Field on Add User Screen	Notes
Password	Password	Blank in the exported file. Provide passwords for new users. To overwrite an existing user's password, provide the new password in the field.
Home Tel	Home Telephone	Optional
Work Tel	Work Telephone	Optional
Work Email	Work E-mail	Optional
Work Fax	Work Fax	Optional
Mobile	Mobile	Optional
Personal Email	Personal E-mail	Optional
User Group	User Group	If the user group does not exist, one will be created with the type 'Department' and the parent 'Organization '. If left blank, the user will not be placed in a user group and the import log will show a warning.
ANI Presentation Type	ANI Presentation	-1: Service type default 1: Organization ANI 4: Site ANI

Column heading	Field on Add User Screen	Notes
		Or enter a full ANI. This must be a valid ANI for the organization.
User Type	User Type	
Status	Initial Status	0: Pre-Active 1: Active **Note**: a user's status cannot be set to 'Pre-Active' once the account has been active.
IP Address	N/A	Leave blank unless instructed otherwise.
Ringtone ID	Ringback tone	-1: Service type default Or enter the name of the ringtone.
User Code	Star Code	Enter specific digits (5 to 7 digits) or leave blank to auto-generate a 5-digit code.
Security Code	Security Code	
Service Type	Service	-1: Service type default Or enter the name of the service type.
Extension	N/A	The user's extension. If it does not exist, the system will create it. **storm** does not allow you to assign the same extension to more than one user. If the import file includes the same extension against more than one user, the import will fail. If you import user details that include an extension that is already assigned to another user: If **Reassign user extensions?** is not selected, the import will complete, but with an error message against the row that contained the duplicate extension. If **Reassign user extensions?** is selected, the extension is assigned to the user whose details are being imported, and removed from the user to whom it was previously assigned.

Column heading	Field on Add User Screen	Notes
Destination Addresses	N/A	Leave blank unless instructed otherwise.
Billing Account	Billing Account	-1: Service type default Or enter the user's account serial number.
Alternative Number	Alternative Number (in Extended Details)	
Whisper Prompt?	N/A	0: No whisper prompt 1: System speaks caller's ANI before call is answered
Forward Internal to Voicemail on Busy?	N/A	0: No forwarding rule to set 1: System will create a forwarding rule
Disable Mailbox PIN?	N/A	0: Enabled 1: Disabled
Mailbox Intro Type	N/A	0: Default greeting 1: Personal greeting 2: Mailbox number
Mailbox Email Address	N/A	The email address for the voicemail notification.
Email Notification?	N/A	0: Off 1: On
Email Attachment?	N/A	0: Voicemail message not attached with Email Notification 1: Voicemail message attached with Email Notification
Max Mailbox Messages	N/A	Leave blank for unlimited.
Recording Service	N/A	Relates to the drop-down menu in the Configure Recording section of Edit User Services. Enter the name of the required recording service type from this list (typically 'Default' or 'Record All Calls').

Column heading	Field on Add User Screen	Notes
		Note: see the *UC User Guide* for more information.
Outbound Call Barring Profile	Outbound Call Barring Profile	Leave blank if no profile configured.
Site	Site	
Roaming?	Roaming?	0: User will always log in from the same site 1: User may log in from multiple sites
storm Contact Agent?	N/A	Leave blank or do not change. Provided to support legacy systems.
Supervisor	N/A	Leave blank or do not change. Provided to support legacy systems.
PSTN Device?	PSTN Device	0: Disabled 1: Enabled
Network ANI Type	Network ANI	-1: Service type default 1: Organization ANI 4: Site ANI Or, enter a full ANI. This must be a valid ANI for the organization.
Restrict ANI?	Restrict ANI	0: ANI not withheld 1: ANI withheld
Use Username as Lync Account?	Use Username as Lync Account?	0: No 1: Yes
Recording Mode	N/A	Sets the recording mode for the user's recording account, if available. Enter one of: • On Demand (not supported if your organization uses **storm** integrated with Verint) • All Calls • All Internal Calls

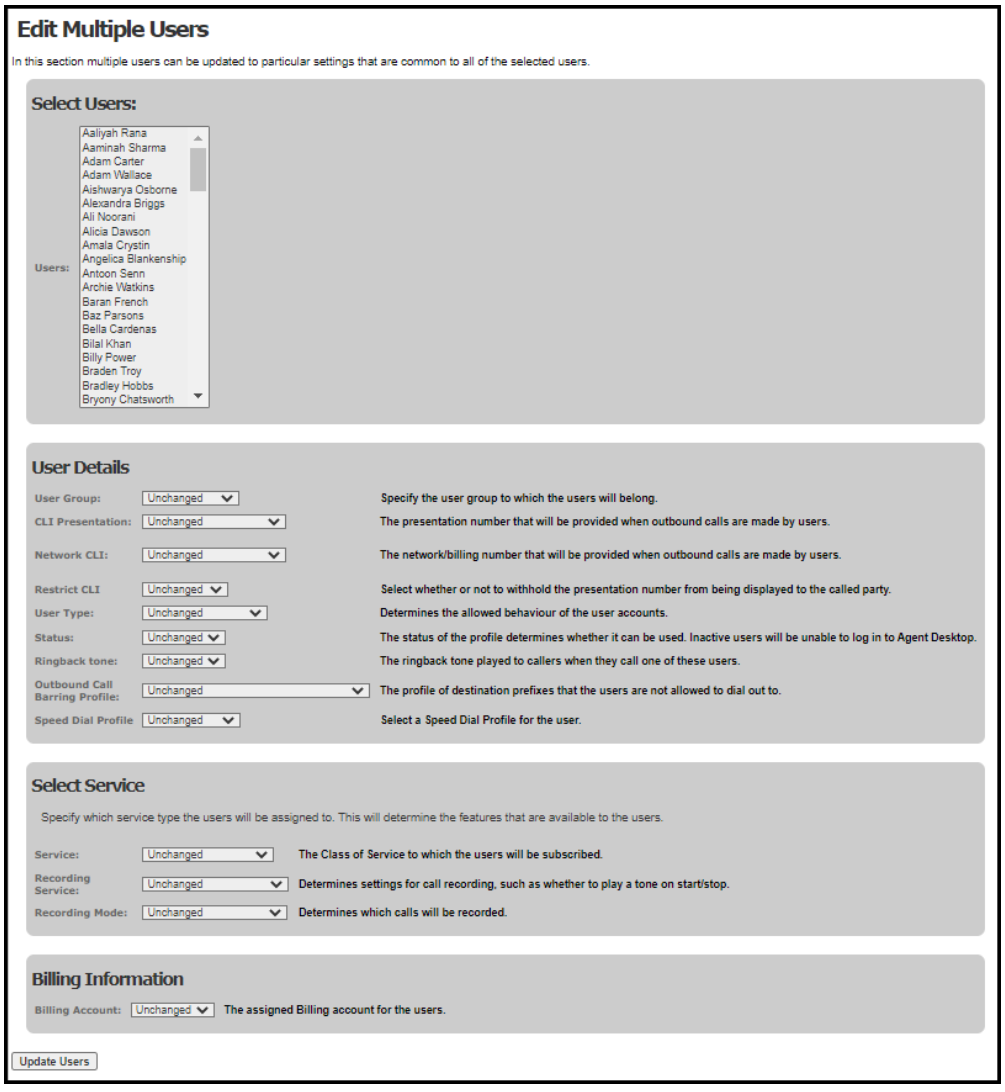
Column heading	Field on Add User Screen	Notes
		• All External Calls • Inbound External Calls • Outbound External Calls
SAP User?	SAP User?	0: No 1: Yes
Use Username as SAP Account?	Use Username as SAP Account?	0: No 1: Yes
SAP Account	SAP Account	(If field **SAP User?** and Use **Username as SAP Account?** = 0) Name of the user's SAP account
CRM User?	CRM User?	0: No 1: Yes
Use Username as CRM Account?	Use Username as CRM Account?	0: No 1: Yes
CRM Account	CRM Account	(If field **CRM User?** and **Use Username as CRM Account?** = 0) Name of the user's CRM account
Require Agent Desktop Logon?	Require Agent Desktop Logon?	0 = No 1 = Yes
Speed Dial Profile	Speed Dial Profile	0 = User has no speed dial profile. Or provide the name of the speed dial profile to be assigned to the user.
Method	SMS/Email	0 = SMS 1 = Email
Use Outgoing Domain for PSTN Agent Calls	N/A	Optional
MS Teams DID	MS Teams DID	Optional

Column heading	Field on Add User Screen	Notes
MS Teams Azure ID	MS Teams Azure ID	Optional
Miscellaneous 1	Miscellaneous 1	Optional
Miscellaneous 2	Miscellaneous 2	Optional

Edit Multiple Users at the Same Time

You are able to amend certain details of more than one user at once - for example, to move them all into the same user group, to set them all to have the same call barring profile, and to assign services.

1. Select the **Users > Edit Multiple Users** menu option.

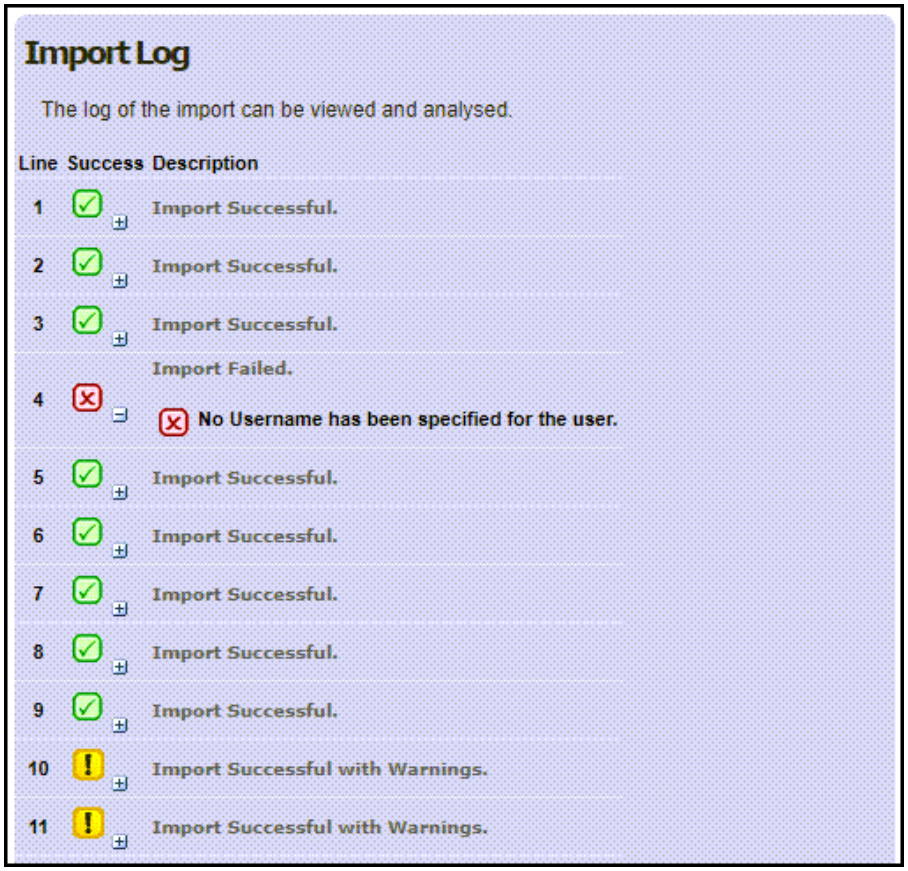


2. Highlight the users whose details you wish to change.
3. Use the fields provided to select each of the values that is to be applied to the selected users. If you leave a field set at 'Unchanged', then users will retain their existing settings for that option.
4. Click **Update Users** to apply your changes.

Import Error Log

Import logs contain useful troubleshooting information if problems occur when uploading CSV files.

1. Click the **View Detailed Import Log** link to open the error log.
2. The line number shown relates to the equivalent line in the CSV file, to help when correcting the error.



View User Summary

The user summary page allows administrators to view the configuration associated with the selected user.

To view a user summary:

1. Click **Users > User Summary.**
2. Select a user from the drop-down list.

The details shown will vary depending on the groups that the user is a member of, and the settings that have been applied to the user.

Click the + next to the queue name to expand the information shown, to include matching rule details.

5 View the **storm** User Audit Log in STUDIO

This shows you certain user operations performed through STUDIO on **storm.**

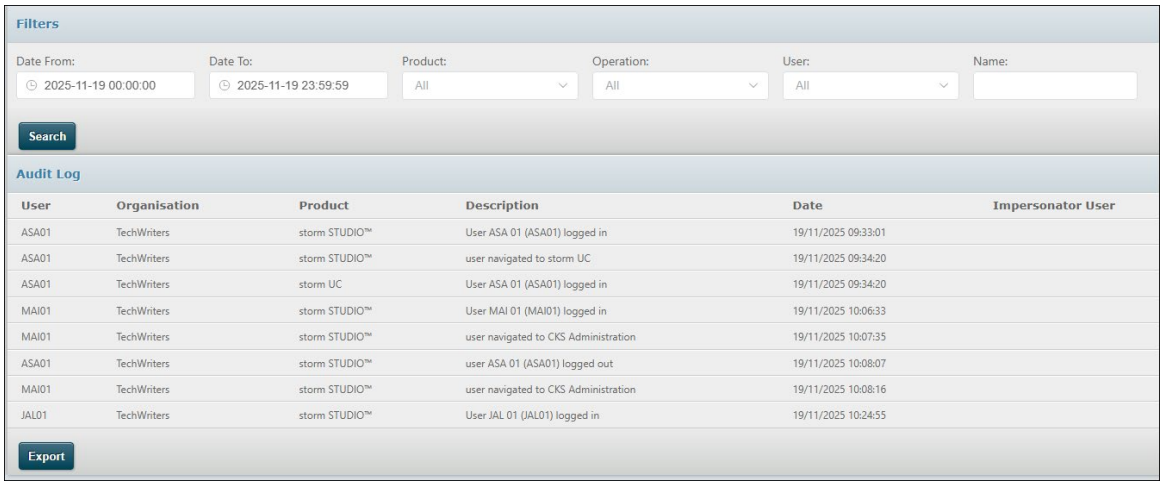
If the change was made by a user logging in to, and working within, an organization in the usual way, the **User** and **Organization** columns show their **storm** username and the name of the organization respectively.

If the change was made in a child organization by a user logged in to a parent organization using **Impersonate Users** functionality:

- The **Impersonator User** and **Impersonator Organization** columns show the **storm** username the person who made the change used to log in to the parent organization, and the name of the parent organization respectively.
- The **User** and **Organization** columns show the **storm** username used to carry out the change in the child organization (that is, the impersonated user's username), and the name of the child organization respectively.

1. Select **Reporting > Audit Log**.

This shows the audit log.

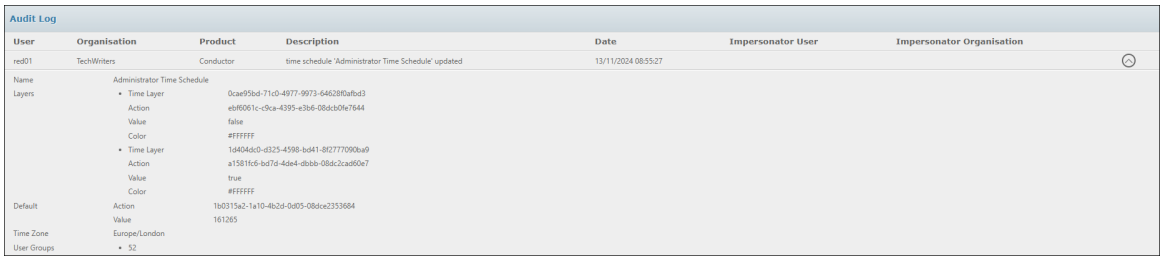


2. The Audit Log can be filtered using the following parameters:
    - A date range.
    - The product which you want to view the operations of.
    - Which operations you want to view.
    - The **storm** user whose activity you wish to view.
    - The name of a specific object. This needs to be the full and exact name of the object, but is not case sensitive**.**

> **Example:** the name of the route plan or user profile.

3. Click the **Search** button to apply the filters.
4. The **Export** button exports the current report, in CSV format.
5. Entries in the 'Audit Log' which feature parameter changes can be expanded by clicking on the corresponding **Arrow Button**  .

   The new values for changes made to parameters during user operation are now displayed.



6 Single Sign-On

Define Single Sign-On Identity Providers

storm provides a single sign-on service that allows users to sign on to their **storm** account automatically when they log in to a third-party product, without having to provide their **storm** username and password. Typical examples of single sign-on would be:

- To allow a user to sign into DTA using their company's own user authentication system (such as a standard Windows login)
- To allow a user to log in to a third-party product (such as Salesforce) and automatically be logged in to DTA.

You can only set up a single identify provider for single sign-on on **storm,** you must also add the details of each user that will use that system.

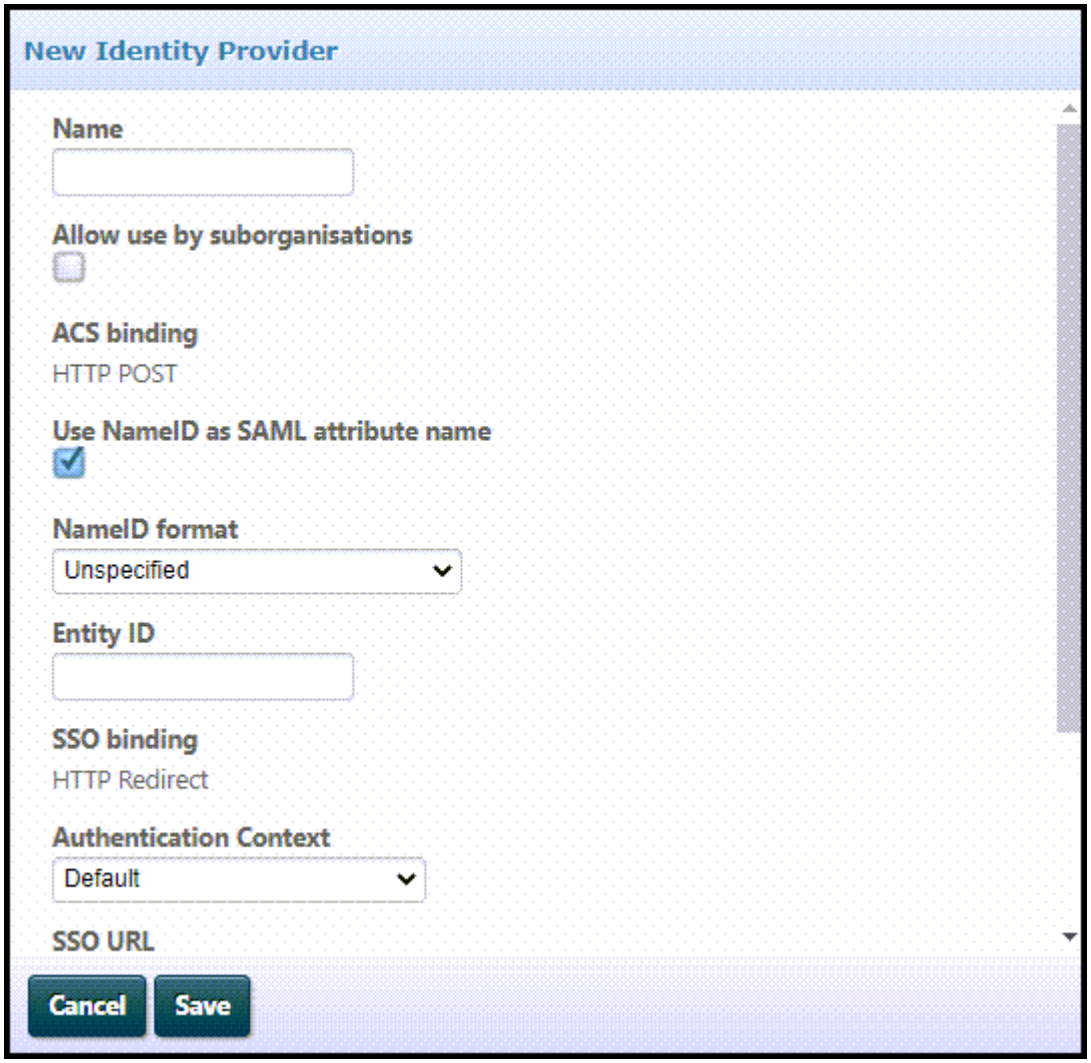
The identity provider performs the initial authentication when a user logs on, and passes the user's login details to **storm**'s single sign-on service provider.

Set Up the Identity Provider

1. To set up the identity providers used by the **storm** application, select the **System Admin > Identity Providers** menu option.

2. In the window that is displayed, click the **Add Identity Provider** button.

A window is displayed.



3. Fill in the fields as described in the following table.

Field	Description
Name	Enter a value that will help you identify the third-party product for which this identity provider has been set up.
Allow use by suborganizations	Select this check box if you wish to share the identity provider with sub-organizations.
ACS binding	The SAML protocol binding for the assertion consumer service endpoint to which authenticated user login credentials are transmitted. This is configured by Content Guru.
Use NameID as SAML attribute name	The name of the attribute in the SAML response that the name provided in the user's credentials must match

Field	Description
NameID format	Select the format in which the name must be provided to the service provider. If you do not want to enforce a single format, select 'Unspecified'.
Entity ID	The identity provider's URL.
SSO binding	The binding to use for single sign-on. This is configured by Content Guru.
Authentication Context	Select the authentication method to be used. If you do not want to enforce a single method, select 'Unspecified'.
SSO URL	The URL to be used for binding with the single sign-on service.
X.509 certificate	Upload the certificate to be used by the identity provider.
Allow identity provider initiated SSO	Select this check box to enable single sign-on for this identity provider and third-party product.

4. Click **Save** to close the window and save the identity provider.

Identify the Users

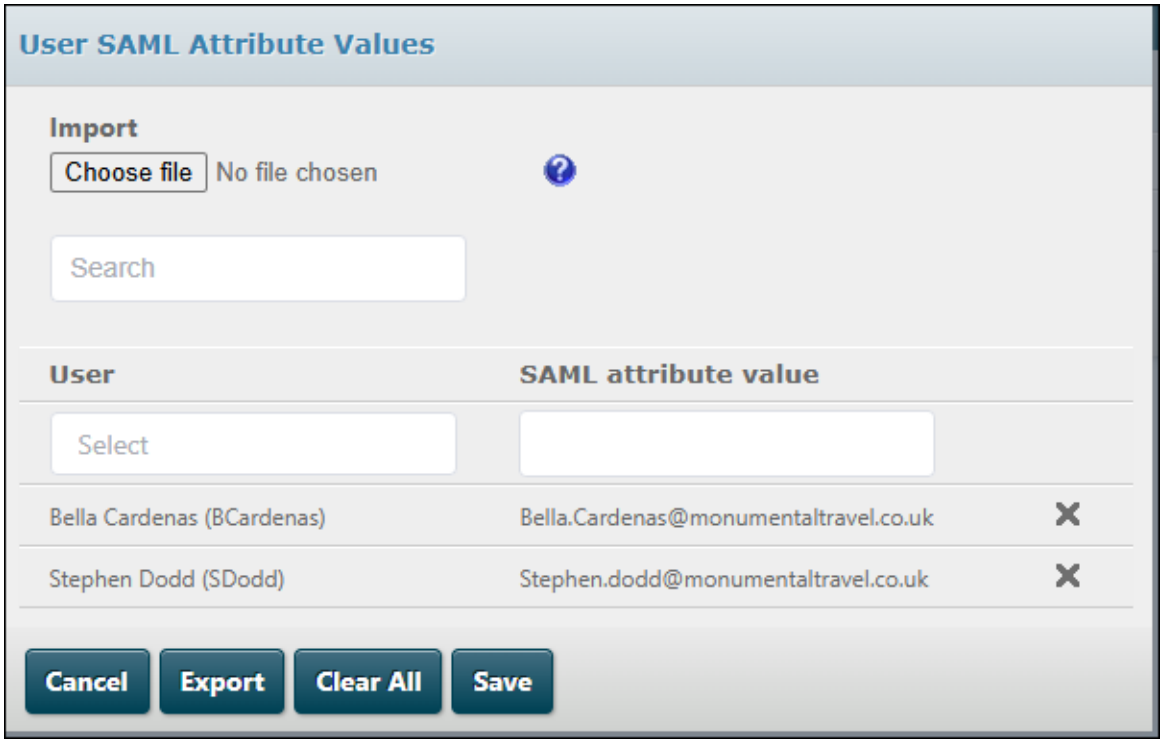
Once you have set up an identity provider, it is included in the window displayed when you select the **System Admin > Identity Providers menu option**.

The metadata URL is the unique identifier for the identity provider, and is generated automatically by the system.

You can identify the users that will log in to this third-party product using single sign-on either individually, or via a bulk update using a CSV file.

Identify Users Individually

1. Click the button.



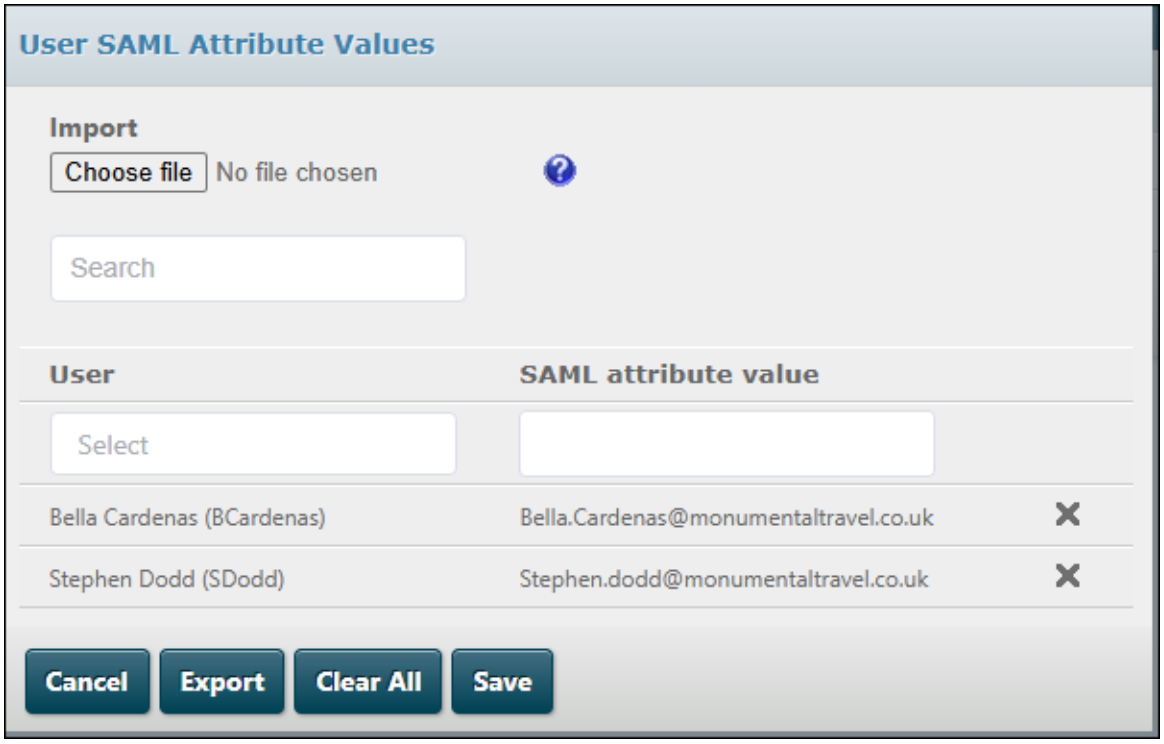
2. Use the **User** field to select a **storm** user.
3. Enter that user's login name in the third-party product into the **SAML attribute value** field.
4. Click the ✚ button.
5. Complete the line that appears with the next user's details.
6. Repeat the process for each user, then click **Save**.

Create a New List

1. Create a CSV file with the structure illustrated below.

   The columns must be in the order shown, and the file must include the header row, with the column titles shown. It must not have more than 400 lines.

2. In the Identity Providers screen, click the button against the relevant identity provider.



3. Click **Choose file** and browse to, and then open, the CSV file.
4. Click **OK** to close the warning message and proceed to import the file.

> **Note:** the **Clear All** button removes all SAML mappings for the selected identity provider.

Update an Existing List

1. In the Identity Providers screen, click the button against the relevant identity provider.
2. In the screen that appears, click the **Export** button. The system exports a CSV file containing the current values for the identity provider in your download folder.
3. Update this CSV file.
4. If you wish to replace the existing file completely, click the **Clear All** button.
5. Click **Choose file** and browse to, and then open, the amended CSV file.
6. Click **OK** to close the warning message and proceed to import the file.

Disable Single Sign-On

You may need to disable single sign-on for a third-party product in emergencies (for example, if the third-party product is unavailable) to allow users to sign on to **storm** directly temporarily.

1. In the Identity Providers screen, click the button against the relevant identity provider.
2. In the screen that appears, click the **Clear All** button. The system exports a CSV file containing the current values for the identity provider in your download folder.
3. Store this CSV file in a safe location.

Once the emergency situation has ended, you can re-import the saved CSV file to reactivate single sign-on functionality.

4. In the Identity Providers screen, click the  button against the relevant identity provider.
5. Select **Choose file** and browse to, and then open, the CSV file. This automatically uploads the CSV file - you do not need to click **Save**.

7 FedRAMP Compliant Recommended Security Settings

Setting	Function	Security impact	Recommended value
Role-Based Access Control	Determines what administrative actions a user is allowed to perform according to their assigned role and associated permissions.	Reduces the risk from compromised accounts by granting users only the permissions they need. Assigning overly broad roles can significantly increase the damage that a single compromised account may cause.	Apply the principle of least privilege when configuring access. Create custom roles that include only the permissions each administrator needs, and limit use of the Customer Administrator role to a small, trusted group of administrators.
Service account permissions	Restricts API access tokens to defined permission sets, determining which actions automated systems are allowed to perform.	If a service key is granted excessive permissions and becomes exposed, it can be misused to gain unauthorized access to user management, analytics, or other sensitive functions.	Limit service keys to the minimum permissions necessary. Create separate keys for each integration, granting only the access that specific integration requires, and rotate the keys on a regular basis.
Single Sign On (SSO) provider configuration	Sets up the identity provider for all user authentication, supporting OIDC and SAML 2.0 protocols. Email/password login is not supported. Configuring SSO requires coordination with the Content Guru FedRAMP team and is managed in the SSO section under Settings.	Consolidates authentication via the organization's identity provider (IdP), allowing enforcement of MFA, conditional access, and session policies. Incorrect configuration may result in user lockout or unintended access.	Set up authentication using your organization's approved identity provider. Confirm the configuration by testing login with a non-admin account before deploying it organization-wide.

8 Contact and Support

For FedRAMP related questions or incident reporting:

Point of Contact	Contact Information
Website	contentguru.com/en-us
Sales	PublicSectorSales@contentguru.com
Support	support@stormfedramp.com
Security	SecurityIncident@stormfedramp.com

9 Copyright and Disclaimer

Content Guru Inc., part of the Redwood Technologies Group Ltd., reserves the right to make changes to the information in this document at any time without notice. Information published in this document is believed to be reliable. However, Content Guru Inc. assumes no liabilities for inaccuracies or omissions in this document, or liability arising from the use of such information. Furthermore, Content Guru Inc. assumes no liability for the infringement of patents or other intellectual property rights owned by third parties which may result from the application of this information.

Content Guru Inc
900 E. Hamilton Avenue,
Suite 510,
Campbell,
CA 95008,
USA

t: +1 408-559-3988
e: info@contentguru.com
w: www.contentguru.com

storm®

CONTENT GURU

Engagement Made Easy®

contentguru.com

info@contentguru.com

+1-408-559-3988

bsi ISO/IEC 20000-1 IT Service Management CERTIFIED

bsi ISO 22301 Business Continuity Management CERTIFIED

bsi ISO/IEC 27001 Information Security Management CERTIFIED