



Software Release Security

Software Release Note

April 2010

Version 1(Published)

Contents

1. Document Purpose	4
2. Background	4
3. Release Contents	4
i. Password Strength and Password Remembered	5
ii. Unauthorised Access.....	6
iii. User Roles and Multiple Logins.....	7
4. Impact on System Functionality.....	8
5. Impact on Configured Items	9
6. Implementation	9
i. Promotion of Release to the Central Systems	9
ii. Environments included in this release.....	10
iii. Web Browser Compatibility	10
7. System changes – Technical Information	11
i. Changes to the GUI Messages Database	11
ii. Changes to LVI User Interface.....	12
Appendix 1: Password Strength	15
Appendix 2: Unauthorised Access	17
Appendix 3: User Roles and Multiple Logins	18

Revision History

Rev.	Date	Description	Author	Reviewer
Version 1	23/04/10	Draft	Gary Craig	

1. Document Purpose

This Release Note sets out the changes included in CMA Central System Software Release Security. These changes have been introduced through the Security Phase of the Security & Customer Names Project.

2. Background

The Security is being developed in response to the approved CMA change “CMACP074” – titled “CS Systems Security”. The changes pertaining to this are focused on enhanced security requirements. These requirements were raised following the last Market Audit. The development is being delivered by the Security and Customer Names (S & CN) Project and the Security Stage has undergone successful User Acceptance Testing (UAT) and Market Scenario Training (MST)¹.

3. Release Contents

The release covers four core areas:

- i. Password Strength and Password Remembered
- ii. Unauthorised Access
- iii. User Roles and Multiple Logins
- iv. Auditing (internal to the CMA so not covered in this document)

The following provides an overview of the user requirements in each of these areas. A more detailed presentation of the user requirements (URs) is given in the Appendices, with each individual requirement identified by an allocated UR number, taken from the relevant Impact Assessment (IA).

¹ A UAT and MST Requirements Document and Results Reports form part of the Project Documentation

i. Password Strength and Password Remembered

Current Arrangements

Currently the LVI has limited password strength constraints meaning weak passwords could exist within the system. Furthermore under certain circumstances the browser used to access the LVI will “remember” a user’s password at a given machine, meaning anyone on that machine could gain access to the LVI without knowing a username and password.

New Arrangements

The LVI has been modified to enforce stronger password constraints thus making it more difficult to infiltrate the system. New password strength constraints are enforced which passwords must conform to in order to exist within the system. Enforcing new password strength constraints does create a need to reset all password currently held in the system. This is because passwords currently held in the system do not conform to the requirements outlined in user requirements UR002 or UR003 (see Appendix 1). On the first working day following the Release all existing users will be emailed a new password and should log on and change this password immediately using the new password change functionality. Failure to log on and change the password within 30 days will lead to the user account being disabled.

The password criteria are set out in Appendix 1.

In addition, instead of the CMA admin users choosing passwords for new users, the system itself will generate passwords which conform to the new strength constraints. Furthermore users will also be forced to change their password every 90 days.

A new lock out feature has also been added to the system. If a user attempts to log in unsuccessfully three times their account will be locked. The system has also been modified to ensure a browser cannot “remember” a user’s password on any given machine.

Detailed User Requirements are included in Appendix 1.

ii. **Unauthorised Access**

Current Arrangements

In the current system there is no process on how to handle user accounts that have not been used for a long period of time. Presently the system relies on the Trading Parties to keep track of the states of their user accounts and notify the CMA of any change.

New Arrangements

An automated process has been put in place to handle the scenario of unused user accounts. A process is initiated when a user account has not been used for 30 days in which case the account will be disabled for a further period of up to 30 days and the user will be notified by email. A user will receive a warning email after 25 days that they need to log onto the system or their account will be disabled once the 30 day period has elapsed.

For a period of 30 days after an account has been disabled, the CMA administrator has the ability to either reactivate an account or delete it at the request of the main Trading Party contact. If this period passes with no requests for activation then the CMA administrator will delete the user account.

Reporting has been added to present the CMA Admin role with a list of all user accounts with details of whether accounts are active or disabled. The functionality for this is in the form of a web report which the CMA can filter and then export to file. A monthly email will be sent to the main contact at each Trading Party with the report file. The contact will then be able to inform the CMA administrator of which accounts can be safely deleted.

Detailed User Requirements are included in Appendix 2, identifying the individual user requirements specified in the IAs, with associated UR numbers.

iii. User Roles and Multiple Logins

Current Arrangements

Currently there are three Central System roles: CMA, LP and Wholesaler. Users can also currently have more than one LVI session open at once.

New Arrangements

New roles have been added to the LVI. A Read Only set of user roles have been introduced, and an additional role has been added as a result of Customer Names on the Database. The Customer Names roles will not be available until the Customer Names Software Release in June.

The new roles will be:

Name	Definition
CMAAdmin	CMA View + Filter + Update + Customer Name access
LPAdmin	LP View + Filter + Transact + Customer Name access
LP	LP View + Filter + Transact
SWW	SW View + Filter + Transact
CMAReadCN	CMA View + Filter ONLY + Customer Name access
LPReadCN	LP View + Filter ONLY + Customer Name access
LPReadOnly	LP View + Filter ONLY
SWReadOnly	SW View + Filter ONLY
CMAReadOnly	CMA View + Filter ONLY

Users will also only be able to have one LVI session open at once.

Detailed User Requirements can be found in Appendix 3.

4. Impact on System Functionality

Functional Area	Impact (Y/N)	Description
CMA User Interface (LVI)	Yes	<p>Passwords & Password Remembered: The create user page will be altered to no longer allow the CMA admin to create the password.</p> <p>Unauthorised Access: Additional web page with a grid has been added to show status of user accounts in the system. Changes to the edit user screen to activate/deactivate account</p> <p>User Roles & Multiple Logons: Removed current roles and addition of new roles. This will affect which pages are available for view/edit.</p> <p>User Roles & Multiple Logons: Automatic logout changed from 60 minutes to 20 minutes.</p>
Wholesaler User Interface (LVI)	Yes	<p>Passwords & Password Remembered: The login screen will now request only 3 characters of a password and the user will now be able to change their password.</p> <p>User Roles & Multiple Logons: Removed current roles and addition of new roles. This will affect which pages are available for view/edit.</p> <p>User Roles & Multiple Logons: Automatic logout changed from 60 minutes to 20 minutes.</p>
LP User Interface (LVI)	Yes	<p>Passwords & Password Remembered: The login screen will now request only 3 characters of a password and the user will now be able to change their password.</p> <p>User Roles & Multiple Logons: Removed current roles and addition of new roles. This will affect which pages are available for view/edit.</p> <p>User Roles & Multiple Logons: Automatic logout changed from 60 minutes to 20 minutes.</p>
Web Services (HVI)	No	
Aggregation and Settlements	No	
Registration	No	

Functional Area	Impact (Y/N)	Description
Work Flows	Yes	Unauthorised Access: New workflow to carry out checks on unused user accounts and deactivate when necessary.
Data Model	Yes	Unauthorised Access: Added IsApproved property to class UserInfo.
Reporting	Yes	Unauthorised Access: Administration will have access to live web report showing the status of user accounts

5. Impact on Configured Items

There are no changes to the Operational Code and the Market Code, including the CSDs.

Configured Item	Change Impact	See section
Market Code	No	
CSDs	No	
Schema (HVI) & CSD0301 Annex A	No	

6. Implementation

i. Promotion of Release to the Central Systems

The upgrade of the Central System to Version Security is scheduled across the various environments as set out below.

Activity	Expected date	Comments
CMA User Acceptance Testing	26 March 2010	Complete
Market Re-assurance	15-16 April 2010	Complete
Release code to production	26 April 2010	New passwords to be emailed for market opening on 26 April
Release code to Dundee 2 (test environment)	tbc	

ii. Environments included in this release

The following environments will be impacted by this release:

- Production Environment (Dundee One)
- Test Environment (Dundee Two)

iii. Web Browser Compatibility

The Low Volume Interface (LVI) is configured for operation with most available browsers. The browsers that are supported by our Service Provider are:

- a. Internet Explorer 6
- b. Internet Explorer 7
- c. Internet Explorer 8
- d. Mozilla Firefox Version 2
- e. Mozilla Firefox Version 3
- f. Google Chrome Version 4

7. System changes – Technical Information

i. Changes to the GUI Messages Database

Tables

The following changes have been made to tables

AllowedDomain

A new table called AllowedDomain has been created.

Column	Type	Nulls
AllowedDomainId	Int	No
DomainName	Varchar(255)	No

Primary Key: AllowedDomainId

PasswordHistory

A new table called PasswordHistory has been created.

Column	Type	Nulls
PasswordHistoryId	Int	No
Username	Varchar(256)	No
Password	Varchar(128)	No
CreatedDate	Datetime	No

Primary Key: PasswordHistoryId

PasswordHistoryId was set as an identity column

Stored Procedures

The following changes have been made to stored procedures

spr_insertPasswordHistoryRow

A new stored spr_insertPasswordHistoryRow was created

ii. Changes to LVI User Interface

Login

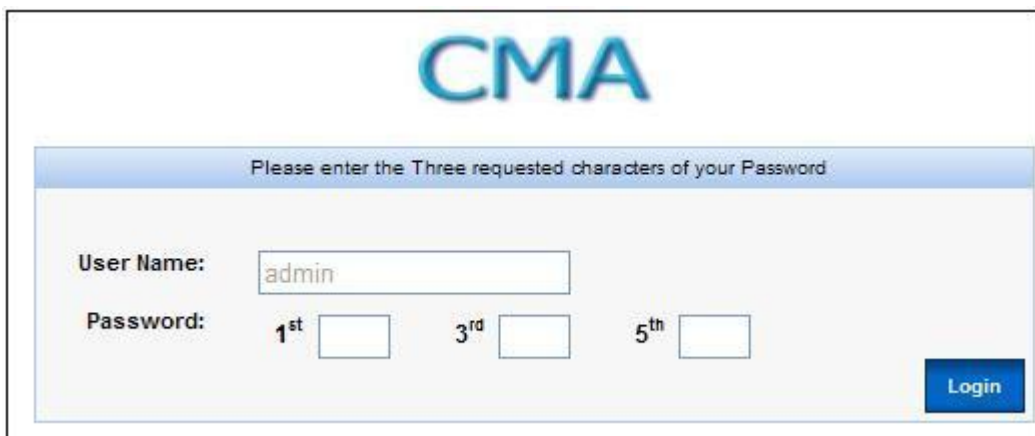
The login page has been modified to be a two step process with the password step asking for a three random characters from the user's password.

Step 1 – Enter User Name



The screenshot shows the CMA login interface for Step 1. At the top center is the 'CMA' logo. Below it is a blue header bar with the text 'Enter Your Username and press Proceed'. The main content area contains a 'User Name:' label followed by a text input field and a blue 'Proceed' button.

Step 2 – Enter Password



The screenshot shows the CMA login interface for Step 2. At the top center is the 'CMA' logo. Below it is a blue header bar with the text 'Please enter the Three requested characters of your Password'. The main content area contains a 'User Name:' label with a text input field containing 'admin'. Below that is a 'Password:' label followed by three text input fields labeled '1st', '3rd', and '5th'. A blue 'Login' button is located in the bottom right corner.

Create User

The create user page was modified to do the following:

- Allow a user to be linked to a role. This will be an additional step

Software Release Security

- Validate that the password conforms to the specified strength
- Validate the password against a history store of twelve passwords.

Select a Role Step

The screenshot displays the 'Create Users' interface within the CMA system. At the top right, it indicates the user is logged in as 'admin [CMA]' with a 'logout' link. The navigation bar includes links for 'My Account', 'Reports', 'Dashboards', 'Settlements', and 'Administration'. The breadcrumb trail shows the path: 'CMA Home > Administration > User Administration > Create Users'. A sidebar on the left lists navigation options under 'This Section': 'User Administration', 'Login', 'List Users', 'Create Users', and 'List User Statuses'. The main content area, titled 'Create Users', features a 'User Details' section with a dropdown menu for 'Please select a Role:' currently set to 'CMAAdmin'. Below the dropdown are 'Previous' and 'Next' buttons. The footer contains links for 'Contact the CMA' and 'About the CMA', along with logos for 'Genserv' and 'Logica'.

Edit User

The edit user page was modified to do the following:

- Allow a user to be linked to a role
- Allow a user to be activated/de-activated
- Validate that the password conforms to the specified strength
- Validate the password against a history store of twelve passwords

The screenshot shows the 'Edit User' interface in the CMA system. At the top right, it says 'You are logged in as admin [CMA] (logout)'. The navigation menu includes 'My Account', 'Reports', 'Dashboards', 'Settlements', and 'Administration'. The breadcrumb trail is 'CMA Home > Administration > User Administration > Edit User'. On the left, a 'This Section' dropdown menu is open, showing 'User Administration' with sub-links for 'Login', 'List Users', 'Create Users', and 'List User Statuses'. The main content area is titled 'User Details' and contains the following information: User Name: LP; Email: LP@bridgeall.com; Last Login: 23/03/2010; Role: LP (selected in a dropdown); Trading Party: Osprey Ltd; Active: Yes (selected) / No. At the bottom right of the form, there are two buttons: 'Reset and Email New Password To User' and 'Update'. At the bottom of the page, there are links for 'Contact the CMA' and 'About the CMA', and logos for 'Gemserve' and 'logica'.

My Account – Change password

The My Account page was modified to do the following:

- Allow a user to change their own password

The screenshot shows the 'Change Password' interface in the CMA system. At the top right, it says 'You are logged in as cmaadmin [CMA] (logout)'. The navigation menu includes 'My Account', 'Reports', 'Dashboards', 'Settlements', and 'Administration'. The breadcrumb trail is 'CMA Home > My Account > Change Password'. On the left, a 'This Section' dropdown menu is open, showing 'My Account' with sub-links for 'Change Password' and 'Manage Domains'. The main content area is titled 'Change Password' and contains the following information: 'Please Enter Your Old and New Passwords'; Password: [input field]; New Password: [input field]; Confirm New Password: [input field]; A note states: 'Your password must be between 8 and 16 characters.' At the bottom of the form, there are two buttons: 'Change Password' and 'Cancel'. At the bottom of the page, there are links for 'Contact the CMA' and 'About the CMA', and logos for 'bridgeall' and 'logica'.

Appendix 1: Password Strength

Specific User Requirements

Requirement Ref	
UR-001	Maintain password length at a minimum of 8 and a maximum of 16.
UR-002	Passwords must have at least 1 character from each of the following: a-z A-Z 0-9 32 punctuation characters
UR-003	Passwords may not contain a value preceding or following the '.' character in a user's userId.
UR-004	Users shall not be allowed to reuse any of their 12 most recent passwords.
UR-005	When a new username is being created by the CMA Admin User the system shall generate a default password and email both username and password to the user in separate emails. That password must adhere to the password strength rules above. When the user first logs on with the automatically generated password they should be forced to change the password. The user should be prompted for the old password and will be requested to enter the new password twice. The password must adhere to the password strength rules above.
UR-006	A new screen will be provided which will allow a user to alter his/her password. The user will be prompted for the old password and will be requested to enter the new password twice. The password must adhere to the password strength rules above. This feature will only be available to a user after they have successfully logged in.
UR-007	The system shall force the user to change his/her password every 90 days. The user will be prompted for the old password and will be requested to enter the new password twice. The password must adhere to the password strength rules above.

	The value of 90 days shall be parameterized.
UR-008	If a password is entered incorrectly three times consecutively within any time span the user should be disabled and prompted to contact the CS Administrator. After successfully logging in the retry attempts will be reset and the user will have three attempts once more. The CMA will have the facility to unlock a user by resetting their password and emailing this password to the user.
UR-009	Create logon functionality to allow the user to supply three characters from the password. The system should randomly decide which three characters must be supplied by the user at each logon.
UR-010	New user email addresses must be part of an allowed list of domains, managed by the administrator.

Appendix 2: Unauthorised Access

Specific User Requirements

Requirement Ref	
UR-001	User accounts should be automatically disabled if they haven't been used within a defined period of time (default 30 days).
UR-002	A User should be issued an email warning by the system 5 days prior and must contact the CMA. Failure to respond will result in deactivation of their account and a notification to the user of the deactivation.
UR-003	The CMA should within a 30 day period after deactivation, be issued with a request by the user to either manually reactivate the User Account, leave deactivated or permanently delete the account. If no request is received by the end of the period then the account will be permanently deleted.
UR-004	There should also be a live web report of all active and disabled usernames for each organization which can be exported for a monthly email to the main contact in the organisation. Filters should be developed.

Appendix 3: User Roles and Multiple Logins

The CMA admin will have the facility to re-assign users between roles.

Specific User Requirements

Requirement Ref	
UR-001	The system should allow for a user to have read only access to the LVI.
UR-002	<p>The following new roles should be created:</p> <p>LP View + Filter + Transact + Customer Name access CMA View + Filter + Update + Customer Name access</p> <p>LP View + Filter + Transact SW View + Filter + Transact</p> <p>LP View + Filter ONLY + Customer Name access CMA View + Filter ONLY + Customer Name access LP View + Filter ONLY SW View + Filter ONLY CMA View + Filter ONLY</p>
UR-003	The CMA should have the facility to re-assign users between roles.
UR-004	Users should only be able to have one active session open at any time.