CM apps Installation and EPSS Integration Guide

[December 2022]

Revision Record

|  |  |  |
| --- | --- | --- |
| Date | Page No. | Description of Change |
| December 2022 | ALL | Initial Version |
| March 2023 | ALL | Formatting Changes |
|  |  |  |

Contents

[1. CM 10.0.0 Installation from scratch 4](#_Toc131577151)

[1.1. Install EPSS 4](#_Toc131577152)

[1.2. SQL Server Schema Setup. 4](#_Toc131577153)

[1.3. Oracle Schema Setup. 4](#_Toc131577154)

[1.4. Application Setup. 4](#_Toc131577155)

[2. Opticash 10.0.0 Upgrade from 9.14. (Oracle) 6](#_Toc131577156)

[3. EPSS Integration with CM applications. 7](#_Toc131577157)

[3.1. Update EPSS Properties. 7](#_Toc131577158)

[3.2. Steps to encrypt the password. 8](#_Toc131577159)

[3.3. Add EPSS dashboard configuration (Portlet Registration part 1) 8](#_Toc131577160)

[3.4. Add URL links to the left menu (Portlet Registration part2) 8](#_Toc131577161)

[3.5. Add CM rights as roles in the Security Group 8](#_Toc131577162)

[3.6. Terminal Sync 9](#_Toc131577163)

[3.7. SAML 2.0 Authentication setup 10](#_Toc131577164)

[4. What’s changed in 10.x 11](#_Toc131577165)

[4.1. OptiCash 11](#_Toc131577166)

# 1. CM 10.0.0 Installation from scratch

## Install EPSS

1. Download the EPSS package of the stable version from https://ncr.jfrog.io/ui/native/fsg-ess-maven-releases/com/ncr/cxp/cxp-release-package.
2. Go through the document *epss-install.pdf* prior to installation.
3. After installation, the User should be able to login into EPSS with the default User credentials. (admin/Password-100)
4. After login into EPSS, the user should be able to see **Shared Services** e.g User Management, Terminal Management etc.

## SQL Server Schema Setup.

1. For SQL Server, Run the DB script **sqlserver-schema.sql**. which will result in the creation of an EMPTY\_OC DB and a user named **'EMPTY\_OC'** with the same password. As an alternative, it is possible to replace all instances of 'EMPTY\_OC' with a desired keyword to customize your schema, username, and password.
2. To change **'EMPTY\_OC'**, replace **'EMPTY\_OC'** with a user-defined name.
3. Run the DB script **sqlserver-data.sql**. Replace **'EMPTY\_OC'** in case it has been changed or modified.
4. For Oracle, run three parts of script files (Master\_Schema\_Creation\_Script\_build.part1.sql).

## Oracle Schema Setup.

1. Go through the installation guide of a particular CM app and create an empty schema and schema DB user.
2. Execute three ddl script files

Master\_Schema\_Creation\_Script\_build.part1.sql, Master\_Schema\_Creation\_Script\_build.part2.sql, and Master\_Schema\_Creation\_Script\_build.part3.sql.

## Application Setup.

1. Update database properties as below for SQL Server.

JdbcDriver=com.microsoft.sqlserver.jdbc.SQLServerDriver

JdbcUrl=jdbc:sqlserver://<host>;DatabaseName=<SCHEMA\_NAME>

JdbcParm1Value=<SCHEMA\_NAME>

JdbcParm2Value=<SCHEMA\_NAME>

1. For Oracle, use the Oracle diver details below

JdbcDriver= oracle.jdbc.driver.OracleDriver

JdbcUrl==jdbc\:oracle\:thin\:@<IP>\:<PORT>\:<SERVICEID>

JdbcParm1Value=<SCHEMA\_NAME>

JdbcParm2Value=<SCHEMA\_NAME>

1. Deploy WAR in any Tomcat. (Version 9.x + )
2. Add License. Kindly contact CASH Management for license creation.
3. Launch the application and attempt to log in. Users should be unable to access the application, as version 10.x requires login authentication through EPSS.

# 2. Opticash 10.0.0 Upgrade from 9.14. (Oracle)

To upgrade from 9.14 to 10.0 of OptiCash (Oracle), users can follow the instructions that are listed below.

1. Install EPSS. Refer to section 1.1 Install EPSS
2. Merge the old **properties** file with the new **properties** file in the new WAR.
3. kindly check all the properties mentioned in the 3.1 Update EPSS Integration Properties.
4. Ensure that the persistence.xml (for VLM Apps) contains the appropriate database driver.
5. Follow the instructions in Step [1.3 CXP Integration Setup](#CXP_Integration_Setup).

**Note**: The name of the deployed WAR should be consistent with the context name specified in the cmportlet.js file located in the WEB-INF folder.

# 3. EPSS Integration with CM applications.

The following instructions outline the step-by-step process for integrating the CM application with EPSS. It is recommended that users first complete sections 1 or 2 prior to beginning the integration steps. Additionally, both the EPSS and CM applications must be operational at this point, and direct login should not be functional in the CM application

## Update EPSS Properties.

1. To integrate with EPSS, CM apps need EPSS base URL, and default user credentials (admin/Password-100).
2. The EPSS base URL is utilized for the consumption of certain APIs.
3. Default credentials are used for synchronizing terminals.
4. Each application needs **MeshAuthorizer**, a component in the CM app which connects with EPSS for authentication and authorization.
5. Update the below properties in **opticash.**properties and **optivault**.properties for Opticash and Optivault applications.

AuthMethod=com.ncr.fe.cshmgmt.custom.mesh.auth.MeshAuthorizor

AuthClass=cxpPortalBaseUrl{EPSSRemoteBaseURL};

MeshEmbedded=true

DisableExUserCreation=false

cxpPortalBaseUrl=<point to cxp instance>

cxpPortalUsername=<cxp admin username>

cxpPortalPassword=<encrypted-pwd> (*Refer 3.2*)

cxp\_monitor\_session=false

LogsPath=C\:\\ncr\\logs\\

ImportPath=C\:\\ncr\\import

OutputPath=C\:\\ncr\\output

log4j.appender.ROL.File=C:/ncr/logs/cxp-<CMApp>.log in the WEB-INF/classes/log4j.properties

1. Update the below properties in the **optinet.**properties file in OptiNet App.

AuthMethod=com.ncr.fe.cshmgmt.custom.mesh.auth.MeshAuthorizor

AuthClass=cxpPortalBaseUrl{EPSSRemoteURL};

meshEnabled=true

cxp.portal\_base\_url=<EPSS Base URL>

cxp.monitor\_session=false

1. Update properties in **carrierweb**.properties, **invoicevalidation**.properties, **vaultbalance**.properties and **vaultbalanceagent**.properties in VML apps as shown below.

authentication.type=mesh opticore.auth.authorizer.class=com.ncr.fe.cshmgmt.custom.mesh.auth.MeshAuthorizor

opticore.auth.init.params=MeshAuthorizor

opticore.auth.app.name=CW/IV/VB/VBA

## Steps to encrypt the password.

1. In **encrypt**.cmd, set java path and Opticash installation folder.
2. Run **encrypt**.cmd with the actual password as an argument.

**Note**: Opticash must be deployed before encrypting a password.

## Add EPSS dashboard configuration (Portlet Registration part 1)

1. To view CM applications in the EPSS dashboard, all the left menus should be configured in the file default-dashboard.xml in the ‘**ncr’** folder. This folder contains all the required configurations, and certifications required for EPSS and this is set while installing EPSS.
2. All the CM apps are set up in a singular **‘CM’** product. Just copy the default-dashboard.xml file and place it in the ‘ncr’ folder.

## Add URL links to the left menu (Portlet Registration part2)

1. In the previous section, all the left menu items would be added to the EPSS dashboard under the CM product.
2. For each left menu item, a link should be set so that when the user clicks on a particular menu item, the respective app should be opened in a new tab.
3. Update CM app URLs in the script files and the same should be updated in cmportlet.js in the WEB-INF folder.
4. By running scripts in the CXP database, the registration of the portlet is completed.

## Add CM rights as roles in the Security Group

1. Users are granted privileges or rights in OptiCash and OptiVault which determine their authorization. These privileges must now be incorporated into EPSS, as authentication and authorization processes are exclusively carried out within EPSS.
2. In EPSS, roles can be grouped into Security groups.
3. For each application, the default Security group should be added to the EPSS.
4. Privileges/rights are considered as roles in EPSS and Business Unit as Security Group.
5. The business Unit contains the list of rights, list of users and list of assigned cashpoints.
6. Cashpoint assignment is done through Terminal Group in EPSS.
7. Execute scripts to add all default Security Groups, and roles.
8. Restart the EPSS application and log in with default credentials.
9. Default User should be able to see all CM apps under CM product.
10. Now CM app-specific users should be created and assigned with app-specific default security groups.//TODO new user in EPSS.
11. Login with opticash specific user and click on OptiCash and the Opticash main screen should be opened in a new tab without asking the user for credentials.
12. If the user of some security group logs into the CM application, the security group’s equivalent Business Unit is created.
13. In **CarrierWeb**, the default security groups are CW\_ADMIN and CW\_USER and these are mapped to Spring security ROLE\_ADMIN and ROLE\_USER respectively.
14. In **VaultBalance**, the default security groups are VB\_ADMIN and VB\_USER and these are mapped to Spring security ROLE\_ADMIN and ROLE\_USER respectively.
15. In **InvoiceValidation**, the default security groups are IV\_ADMIN and IV\_USER and these are mapped to Spring security ROLE\_ADMIN and ROLE\_USER respectively.

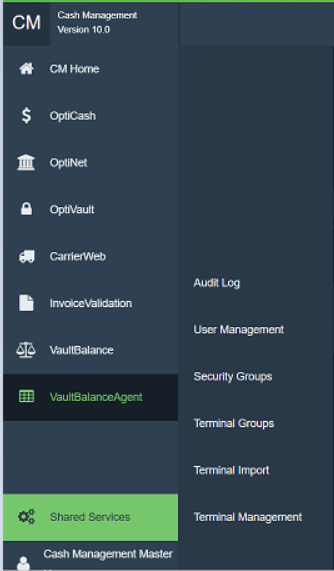
## Terminal Sync

1. Due to restrictions on ATM creation, this must be created through Terminal Management.
2. All the terminals created in EPSS should be synchronized in Opticash with default ATM parameters and should be listed in the list of Cashpoints.
3. Import//TODO

## SAML 2.0 Authentication setup

1. By default, EPSS uses database authentication for all EPSS users.
2. Go through the epss-ssoconfig.pdf in EPSS documentation and set SAML 2.0 authentication.

# 4. Navigation and UI Changes in 10.0

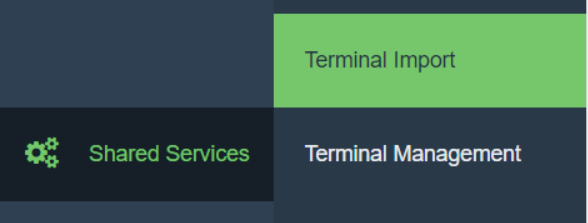


Now all applications of Cash Management along with Shared Services (with other NCR Applications catered by EPSS) can be accessed from the same page.

## OptiCash

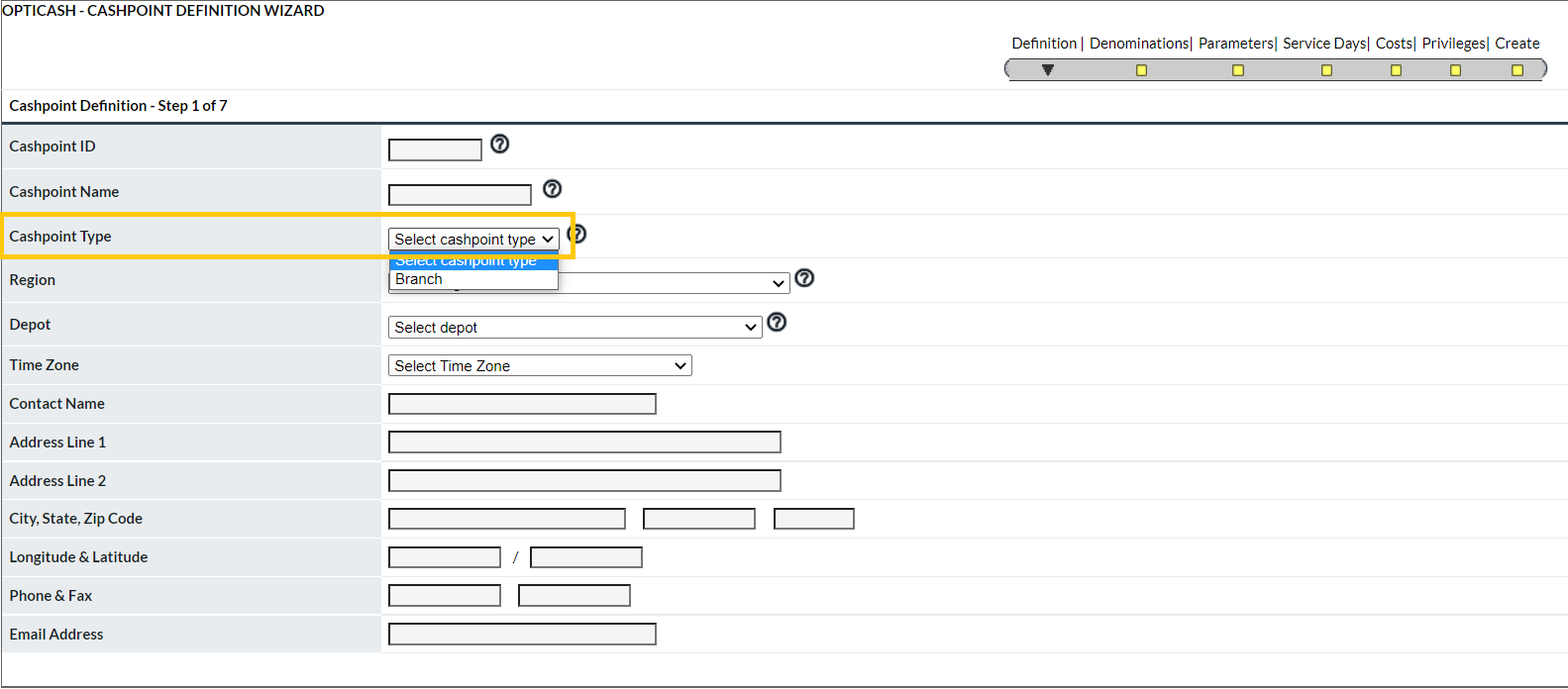
1. ATM creation is not allowed and only branched can be created.

ATM can be Created from Shared Services > Terminal Import

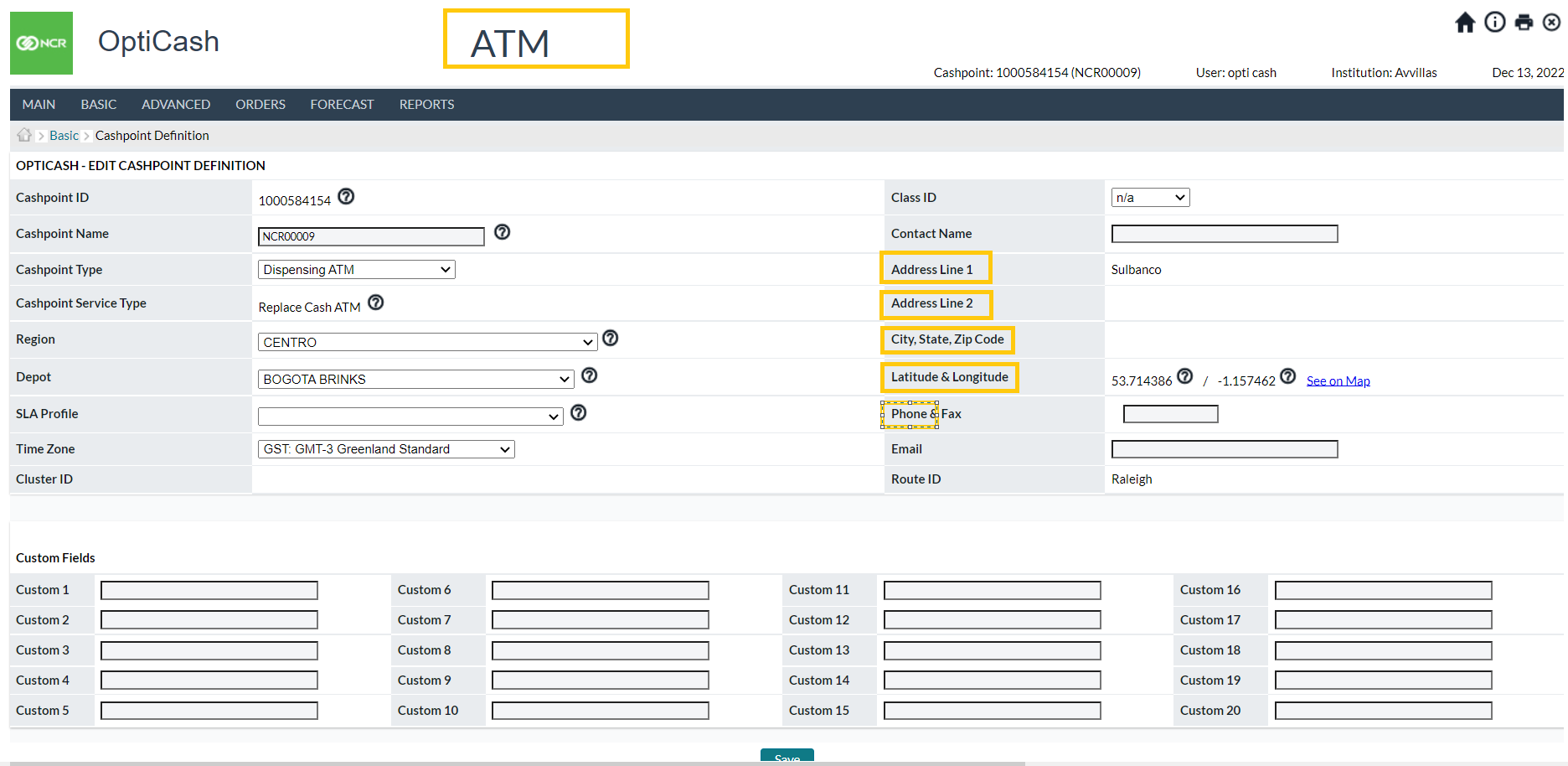


The import template is attached in this package as <terminal-import.csv>

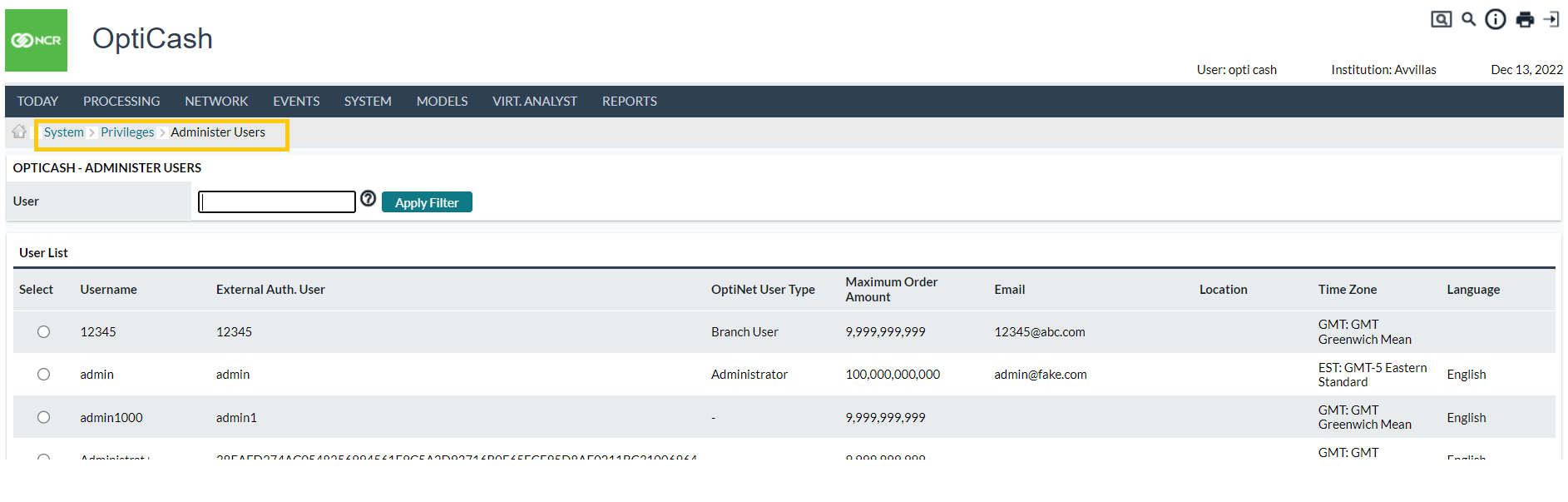
If there is integration with NCR Vision. It can also be created from the Vision terminal creation feature.



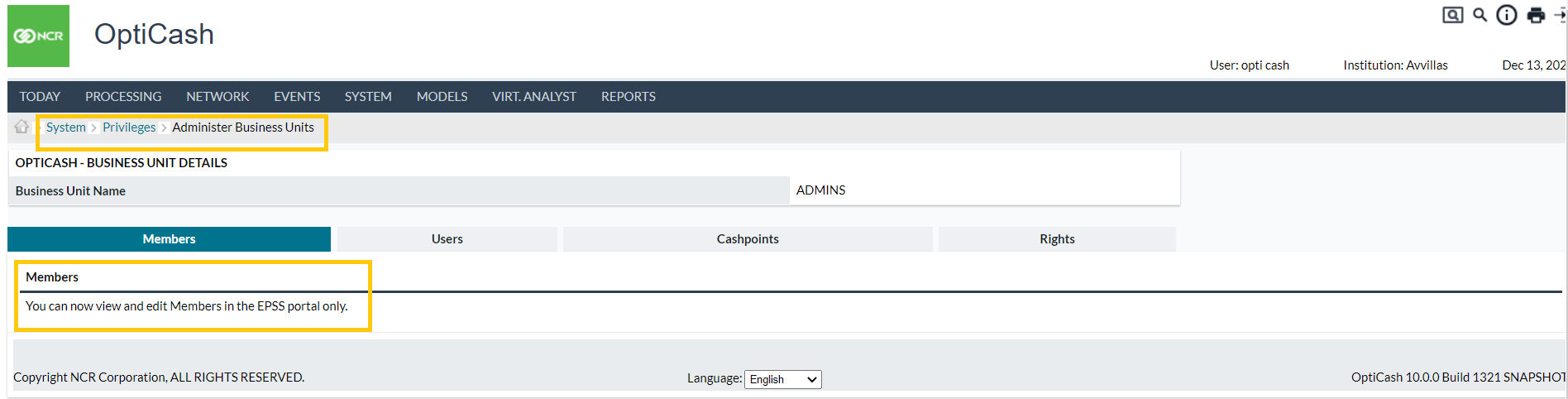
1. For ATM, in Cashpoint definition fields are not editable as shown below. This can again be updated via Terminal Import functionality.

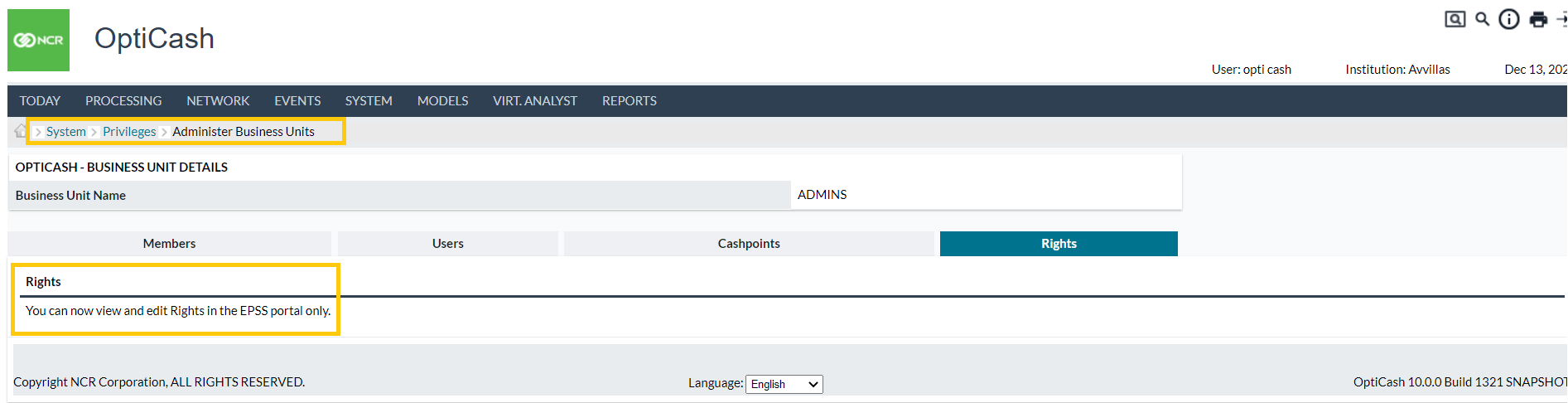


1. User creation in Opticash from *System>Privileges>Administer Users* is disabled. However, some of the Opticash-specific user attributes can be edited.



1. View and edit of **Members**, View and edit of **Rights** are moved from *System>Privileges>Administer Business Users* in Opticash to EPSS

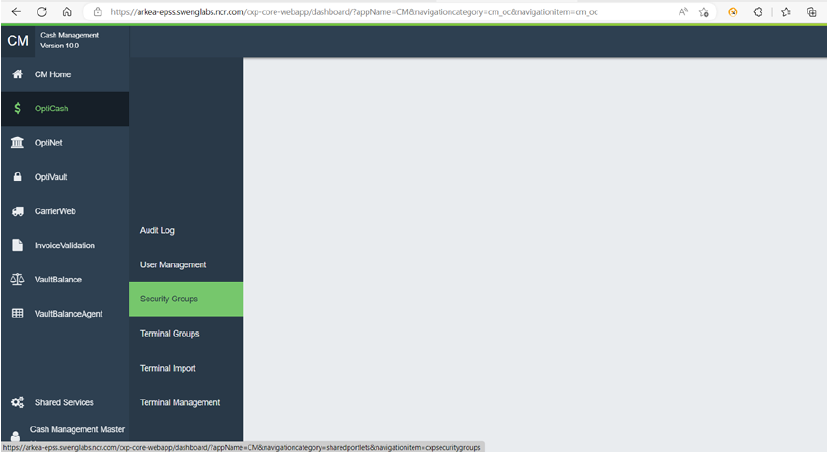




# EPSS UI for User Creation and Security Group

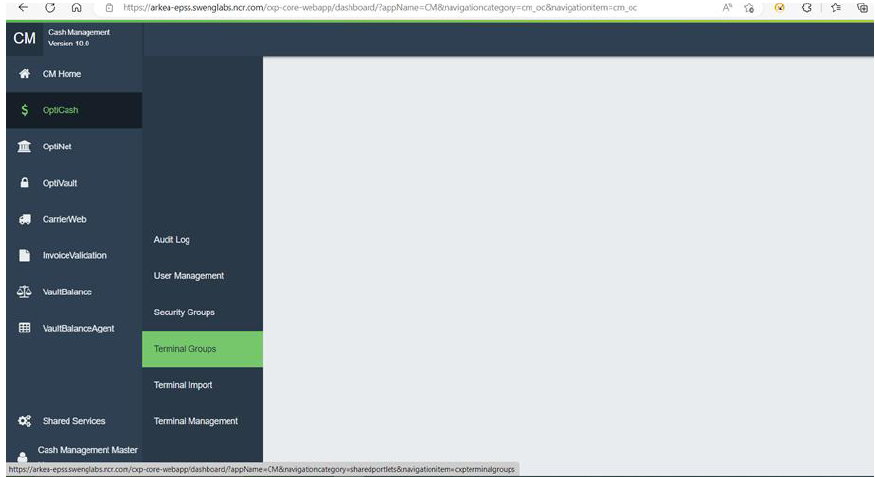
**Sync Business Units(OC, OV) and UserGroups(CW) to Security Groups**

* Since the Rights and Roles of Users can only be assigned from EPSS we have to migrate the existing Business Units and Usergroups to EPSS
* For OC/OV
  + Create a Security Group with the same name as the Business unit in OptiCash/OptiVault
  + Assign the Security Groups the same roles as the Rights were present in OptiCash/OptiVault
* For CW
  + Create a Security Group with the same name as UserGroup in CarrierWeb
  + Assign the Security Groups the same roles as the Rights were present in CarrierWeb



**Sync Business Units OC to Terminal Groups**

* Since ATM management has been moved to EPSS and new ATMs can only be created via EPSS we need to create and assign terminal groups to the ATMs synced between EPSS and OptiCash
* Create Terminal Groups with the same as Business Units in OptiCash and give all the ATMs of that Business unit to that Terminal Group

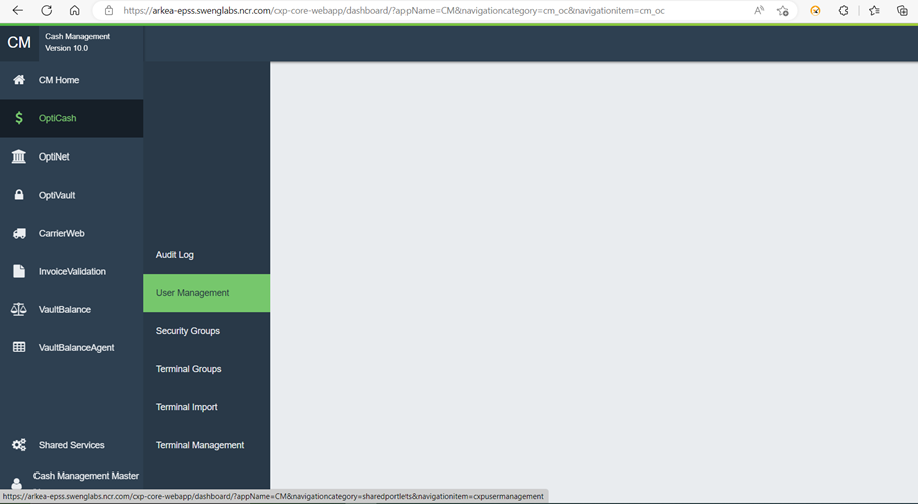


**User Creation**

Users can be created in User Management Screen, by providing their Username, First Name, Last name, Email ID and other required details.

Assign the user with all the Security Groups and Terminal Groups and map with the Business Units that the user has in OptiCash and OptiVault

For users accessing CarrierWeb provide the security groups that map to the CarrierWeb User groups that the user is a member of.

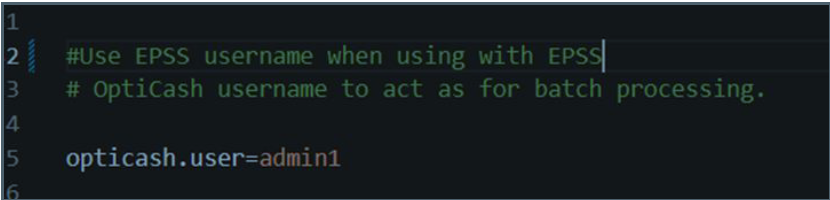


# For Batch Jobs IN OC and OV

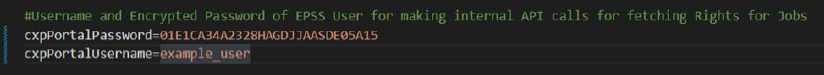
Have the username for carrying out the batch job in build.properties in

<opticash-directory>/Batch/ ant\_execution/build.properties

Make sure the provided user has all required rights



You need to configure cxpPortalBaseUrl, cxpPortalUsername and cxpPortalPassword in Opticash.properties and Optivault.properties



The cxpPortalPassword will be the encrypted password for the cxpPortalUsername encrypted using the encrypt.cmd

Note that the username in build.properties and Opticash/Optivault.properties can be different

Opticash Installation and CXP Integration Guide

Revised 2023

www.ncr.com