

Managing ViPR SRM Users and Roles

Author

Shashidhar Moji

Abstract

This article describes how to manage EMC ViPR SRM users and customize their access to different views in ViPR SRM.

June 2014

Copyright © 2014 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

VMware is a registered trademark of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number: Required for EMC.com, not needed for ECN

Table of Contents

Overview 4

Audience..... 4

Purpose 4

Prerequisites..... 4

Procedures..... 4

 View users..... 4

 Add or edit users 5

 Delete a user 7

 Test user settings 8

 View profiles 9

 Create, edit, and assign users to profiles..... 9

 View roles 11

 Create and assign users to roles 12

Overview

ViPR SRM supports multiple user accounts that have different purposes. It has predefined roles such as Datacenter Administrators, Storage Administrators, and Network Administrators etc. You can also create new custom roles and assign specific privileges to that role.

Audience

This article is for ViPR SRM appliance administrators or anyone who manages access to the ViPR SRM application.

Purpose

After reading this article, you will be able to manage the SRM user accounts, set roles and privileges to different user accounts, create/delete new user accounts and roles

Prerequisites

To perform this operation, you need SRM login credentials with global administrative privileges.

Procedures

View users

The APG Users page lists APG users, their status, profile, and whether their profile is enabled.

To view users:

On the top right of the web portal click **Administration > User Management > Users** or in the tree click **Users**. The APG Users page lists all of the ViPR SRM users.

Here are displayed all the users you can manage, either for the whole portal, either for a specific profile if one has been selected in the tree on the left.

A contextual menu (left click) is available on each user in the table.

Show entries

Search: [+ New User](#)

User Login	Title	First Name	Last Name	User Status	Email Address	Profile	User State
admin				admin		Default Profile	enabled
datacenter				user		Default Profile	enabled
network		Andy		user		Default Profile	enabled
noc-operator				user		Default Profile	enabled
storage-operator		Joe		user		Default Profile	enabled
vws-user				user		Default Profile	enabled

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

Add or edit users

1. Create a New User:

- Click **Administration > User Management > Users**. On the APG Users page click **New User**.
- Or in the left hand tree view, expand **Users** and click **New User**.

This section allows the creation and modification of users who can be given access to any parts of the application.

User Data | User Status | Other Options

i The user will have to provide this information when logging in. If using a customized authentication (LDAP for instance), then there is no need to specify a password.

User Login: ?

New Password:

Confirm Password:

i Some optional information about the user. They are not mandatory, but it is recommended to fill the email one in order to benefit some features.

Title: ▼

First Name:

Last Name:

Email Address: ?

[Save](#)

- On the User Data page enter the user login and password credentials. The new user will initially use these credentials to log on. Users can change their password after logging on with these credentials, in their own settings dialog. The user login and passwords are case-sensitive. Passwords do not need to be set if ViPR SRM is configured to use an external authentication system like LDAP.

3. Enter a title, first and last name, and email address of the user. The email address is used to send notifications of stored reports. These settings can also be entered by the user in their own settings dialog, which overrides anything set here.
4. Click the User Status tab and set the user's rights and access.

Administration >> Users >>

User Creation | Administration

This section allows the creation and modification of users who can be given access to any parts of the application.

User Data | **User Status** | Other Options

? The user status defines the rights and accesses in the whole application. Role assignment is an important step. Please note that a disabled user cannot login anymore.

User Status: Normal User ▼ Disabled? ☐ ?

Profile: Default Profile ▼ ?

User Roles: ?

Other Roles

- Datacenter Administrator Users
- Full Control Users
- Network Administrator Users
- NOC Operator Users
- Web Service Role

Add Role »

« Remove Role

Add All »»

«« Remove All

Assigned Roles

- Storage Administrator Users

Save

5. From the User Status list, select either **Normal User** or **Global Administrator**. Global Administrators have full rights to APG and all its components, cannot be disabled, and have no restrictions on templates. Normal User is the default status for other users.
6. If you want to disable the user so they cannot log on, select the **Disabled** check box. Users will not be able to log on until they are re-enabled. You can also toggle users to be enabled or disabled by clicking the user in the tree.
7. From the Profile list select the profile to apply to the new user. Profiles determine language, time zone, dynamic graph usage, and the logo used for the Web Portal.
8. From User Roles, add or remove assigned roles as necessary, using the **Add Role** and **Remove Role** buttons. Roles determine access and restrictions for the user.
9. Click the Other Options tab, and set the reports and metrics the user has access to.

User Creation | Administration

This section allows the creation and modification of users who can be given access to any parts of the application.

User Data

User Status

Other Options

i Those options regroup critical settings - such as the master filter - as well as other optional ones...

This filter is the combined filter from all the roles the user is in using an OR, combined with the user one using an AND. It is dynamically updated from the selected roles and the user master filter and thus cannot be edited.

devtype is Router
or devtype is Switch
or devtype is Probe
or devtype is Firewall
or devtype is LoadBalancer
or devtype is CallManager
or devtype is CallServer

(devtype=='Router' | devtype=='Switch' | devtype=='Probe' | devtype=='Firewall' | devtype=='LoadBalancer' | devtype=='CallManager' | devtype=='CallServer')

Master Filter



Everything



Custom Reports

allow custom reports ▼



Save

10. For the Master Filter, enter a filter that restricts the metrics the user can see. This filter is applied to the root node and cannot be modified by the user themselves. Filters can also be set for roles. Any role filters are combined with an OR, and the user filter, with an AND.
11. From the Custom Reports list, select whether custom reports are accessible for the user. The user custom tree is a specific per-user branch of the tree nested under My Reports, which can be modified by the user.
12. Click **Save** to save your changes.

Delete a user

1. Click **Administration > User Management > Users** or in the tree click **Users**.

Here are displayed all the users you can manage, either for the whole portal, either for a specific profile if one has been selected in the tree on the left.

A contextual menu (left click) is available on each user in the table.

Show entries

Search:

User Login	Title	First Name	Last Name	User Status	Email Address	Profile	User State
admin				admin		Default Profile	enabled ✓
datacenter		Andy		user		Default Profile	enabled ✓
network				user		Default Profile	enabled ✓
noc-operator				user		Default Profile	enabled ✓
storage-operator		Joe		user		Default Profile	enabled ✓
ws-user				user		Default Profile	enabled ✓

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

Contextual menu for 'datacenter':

- datacenter
- Edit
- Copy
- Test User
- Enable
- Disable
- Delete

Permanently removes an existing user.

- Click the user you want to delete and select **Delete**.

Test user settings

You can test user settings to check how their settings are applied, as if you were logging in as this user.

- Click **Administration > User Management > Users** or in the tree click **Users**.

Here are displayed all the users you can manage, either for the whole portal, either for a specific profile if one has been selected in the tree on the left.

A contextual menu (left click) is available on each user in the table.

Show entries

Search:

User Login	Title	First Name	Last Name	User Status	Email Address	Profile	User State
admin				admin		Default Profile	enabled ✓
datacenter		Andy		user		Default Profile	enabled ✓
network				user		Default Profile	enabled ✓
noc-operator				user		Default Profile	enabled ✓
storage-operator		Joe		user		Default Profile	enabled ✓
ws-user				user		Default Profile	enabled ✓

Showing 1 to 6 of 6 entries

First Previous 1 Next Last

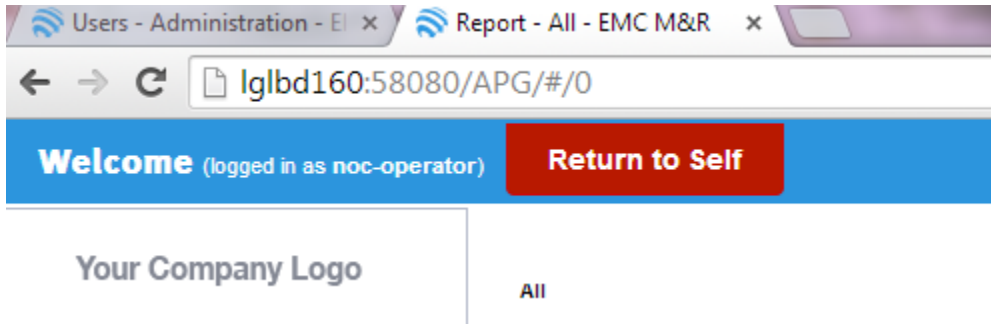
Contextual menu for 'datacenter':

- datacenter
- Edit
- Copy
- Test User
- Enable
- Disable
- Delete

Logs you as this user in order to test what he can see.

- Click the user you want to test and select **Test User**. You are launched into the APG User Interface, interacting with the Web Portal as if you had logged in as the user being tested.
- Browse reports and edit reports, and perform any other regular functions. Any changes you make, such as editing report settings, are saved with their new settings.

4. Simply click **Return to Self** to end user testing.



View profiles

The APG Profiles page gives you an at-a-glance view of the profiles on your system, their descriptions, and how many users are currently assigned to each profile.

On the top right of the web portal click **Administration > User Management > Profiles** or in the tree click Profiles. The APG Profiles page lists the profiles on your system.

Administration >> Profiles

Profiles Management | Administration

Those are the profiles that have been defined, along with the number of users that use them. Admin users are the only ones that can create or modify profiles before they can be assigned to users.

Click on a line to access the corresponding profile information.

Name	Description	User Count
Default Profile		4
Test		2

[+ New Profile](#)

Create, edit, and assign users to profiles

1. Click **Administration > User Management > Profiles** or in the tree expand Profiles and click **New Profile**.
2. In the Main Properties page, enter a name and description.

Administration >> Profiles >>

Profile Creation | Administration

This section allows the creation and modification of profiles for any user.

Main Properties | Customizable Settings | Members | External Members

Those properties are only here so that people who assign profiles will know what the profiles represent. It will help them decide whether the profile fits the user or not.

Name

Description

[Save](#)

- Click the Customizable Settings tab and set the language, time zone and logo. See Edit default display settings for information about these settings. A custom logo can be uploaded here which will show up in the login screen as well as in ViPR SRM user interface.

Administration >> Profiles >>

Profile Creation | Administration

This section allows the creation and modification of profiles for any user.

Main Properties Customizable Settings Members External Members

These settings will be applied for all users who have that profile.

Locale Default Language ?

Time Zone Default Time Zone ?

Logo to Display Default Logo (company-logo.png) ?

Your Company Logo

Delete Selected Logo

Upload New Logo

Login Report

Report Auto Refresh Rate seconds (0 or empty means no refresh)

Save

- Click the **Members** tab, and assign roles to this profile.

Administration >> Profiles >>

Profile Creation | Administration

This section allows the creation and modification of profiles for any user.

Main Properties Customizable Settings Members External Members

This section can be used to quickly switch users from another profile to this one.

Other Users

- admin [Default Profile]
- datacenter [Test]
- network [Test]
- noc-operator [Default Profile]
- storage-operator [Default Profile]
- ws-user [Default Profile]

Add to Profile »

« Remove from Profile

Add All »»

«« Remove All

Users with this Profile

Save

- Click the **External Members** tab, and bind an external group to the profile.

Profile Creation | Administration

This section allows the creation and modification of profiles for any user.

Main Properties Customizable Settings Members External Members

i This section can be used to assign profile to users coming from an external authentication mechanism.

External groups mapped to this profile

« Remove Selection from Profile

« Remove All

Bind an external group to this profile



Add to this profile

Save

6. Click **Save** to save your changes.

View roles

The APG Roles page gives you an at-a-glance view of the roles on your system, their descriptions, and how many users currently use each profile.

To view the roles on your system, click **Administration > User Management > Roles** or in the tree click **Roles**.

Roles Management | Administration

The roles define the rights and restrictions that will apply on users. They also define which templates are available to them, which makes them a great tool to manage accesses.

Standard Mode

Click on a line to access the corresponding role information.

+ New Role

Name	Description	User Count
Datcenter Administrator Users	This role allows its users to: * access datacenter oriented reports	1
Full Control Users	This role allows its users to access almost any module and tool in APG. It also gives them read-write access to all available tree templates.	0
NOC Operator Users	This role allows its users to: * access all reports	1
Network Administrator Users	This role allows its users to: * access network oriented reports * discovery devices (via Discovery Center & Device Discovery) * remove data & devices (via Management of Database Metrics) * modify groups and service levels (via Data Enrichment) * use snmp tools (Mib-Browser & Real-time grapher) * define alerts (via Alerting)	1
Storage Administrator Users	This role allows its users to: * access storage oriented reports * discovery devices (via Discovery Center & Device Discovery) * remove data & devices (via Management of Database Metrics) * modify groups and service levels (via Data Enrichment) * define alerts (via Alerting)	1
Web Service Role	This role aims to be used for web service calls only	1

Create and assign users to roles

1. Click **Administration** > **User Management** > **Roles** > **New Role** or in the tree expand **Roles** and click **New Role**.
2. Enter a name and description for the role.

[Administration](#) >> [Roles](#) >>

Role Creation | [Administration](#)

This section allows the creation and modification of roles for any user.

Main Properties Members External Members Template Access Actions Modules & Restrictions Access

i Name and description are only here for information purposes. The filter and disabled attributes are the only ones that will modify the role users behavior.

Name

Description

Master Filter

Disabled? ☐

3. Click **Members** tab and add users.

Role Creation | Administration

This section allows the creation and modification of roles for any user.

Main Properties Members External Members Template Access Actions Modules & Restrictions Access

i This section can be used to quickly manage the list of users who have this role.

Other Users

- admin [Default Profile]
- network [Default Profile]
- noc-operator [Default Profile]
- ws-user [Default Profile]

Users with this Role

- datacenter [Default Profile]
- storage-operator [Default Profile]

Add to Role »

« Remove from Role

Add All »»

«« Remove All

Save

- If you have configured LDAP authentication, Click **External Members** and bind an external group to the new role (LDAP Users)

Role Creation | Administration

This section allows the creation and modification of roles for any user.

Main Properties Members External Members Template Access Actions Modules & Restrictions Access

i This section can be used to assign roles to users coming from an external authentication mechanism.

External groups mapped to this role

« Remove Selection from Role

«« Remove All

Bind an external group to this role



Add to this role

Save

- Click the **Template Access** tab and set the templates this role has access to.
- Click **Actions** tab and add available actions

Role Creation | Administration

This section allows the creation and modification of roles for any user.

Main Properties Members External Members Template Access **Actions** Modules & Restrictions Access

i This section is used to manage the list of actions available to this role.

Inherit actions **Yes** ▼

Available actions

add-pool-expansion [add-reservation.xml]
add-reservation [add-reservation.xml]
remove-scenario [add-reservation.xml]

Add to Role »

« Remove from Role

Add All »»

«« Remove All

Selected actions

Save

- Click the **Module & Restrictions Access** tab. For each module, select whether users with this profile can access it.

Role Creation | Administration

This section allows the creation and modification of roles for any user.

Main Properties Members External Members Template Access Actions **Modules & Restrictions Access**

i For each module listed here, access has to be specifically granted before any user can use them. Inherited access means the value has not been enforced, and thus the default one will be applied. Once the access is granted, some modules offer specific accesses or restrictions of their own features.

▶ Watch4net Frontend	The Watch4net web interface displaying performances reports on collected values.	Yes ▼
▶ Alerting	The web interface that manages real-time alerts on collected values.	No ▼
▶ Centralized Management	The web interface allowing management of all Watch4net servers.	No ▼
● Formula Editor	Provides a graphical interface for formula edition and dynamic reloading.	No ▼
● IP SLA Configuration	A complete IP SLA Configuration suite.	No ▼
● Management of Database Metrics	This module currently allows metrics deletion.	No ▼
● MIB Browser	A complete MIB browsing suite that loads and parses MIBs, provides SNMP commands and dynamic polling.	No ▼
● Outage Editor	This module allows management of dynamic time filter settings.	No ▼
● Real Time Grapher	A grapher which can query the devices directly to get real-time performance data.	No ▼
● SNMP Collector	A graphical interface, linked to the MIB browser, which enables quick SNMP collection configuration.	No ▼
● SNMP Device Discovery	The interface used to discover SNMP devices and distribute them among SNMP collectors.	No ▼
● Transaction Collector	A collector which gathers statistics from generated transactions.	No ▼