APPLICATION NOTE

FOXMAN-UN

Role-based Access Control (RBAC)

Document ID	1MRC000110-FR18	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-06-03

Copyright and confidentiality

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.

All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.

Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.

The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.

This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Introduction

RBAC stands for Role Base Access Control.

This chapter describes the RBAC implementation in FOXMAN-UN based on IEC 62351-8:2020 Role-based access control for power system management [1].

With the definition of roles you can define the access rights to some functionality and/or elements in the system.

These roles can be then assigned to FOXMAN-UN users, and therefore the users will inherite the permissions of the roles they are assigned to. This will define the way a user can interact with the system.

RBAC is a primary method to meet the security principle of least privilege, which states that no subject should be authorized more permissions than necessary for performing that subject's task.

RBAC enables an organization to subdivide permissions and package them into special groups termed roles for assignment to specific individuals according to their associated duties.

The RBAC related UI can be opened by a FOXMAN-UN user with the appropriate permissions. From the NEM Desktop menu use **either of the** following applications to assign roles to users:

- **Application** > **NEM Configurator…**

  Change to the "Role Based Access Control" tab. Click on the "Users" node of the tree structure. In the right-hand side window click the "+ Add" button. Select a user and assign the role(s) and possible exceptions. Apply the assignment.

- **Application** > **Homepage…**

  From the application groups in the left panel select "Security", then start the "User and Role Management" application. In the "User" tab click on "+ Create" in the ribbon. Select a user and assign the role(s) and possible exceptions. In the summary, apply the assignment to create the user.

2 Roles

A FOXMAN-UN role is a group of permissions which are packaged together to expose the associated duties inside the system of specific persons.

There are 2 types of roles, namely system roles and user-defined roles.

System roles are based on the mandatory role definition present in IEC 62351-8, adapted to the FOXMAN-UN system: they define a basic set of functionalities associated with different duties a user can take inside the FOXMAN-UN. These roles can't be modified and are always exposed.

Yet, a user with proper permissions can create more roles: the so-called "User Created Roles". These roles, contrary to the system initial roles, can be created, modified, edited, and deleted. They can be adapted to specific needs of the operator.

The initial set of proposed roles are the following ones:

VIEWER	As a user with VIEWER role, you are able access FOXMAN-UN data and have a general overview of it. You are not permitted to modify FOXMAN-UN, Network Elements or system wide configuration.
OPERATOR	As an OPERATOR you can perform basic maintenance tasks on the network and inside the FOXMAN-UN, including basic access to the node and to network monitoring features.
ENGINEER	As network ENGINEER you can create and manage complex network services. The configuration and parametrization of advanced design tools are included. You will have a full access to the node (excluding security related features).
INSTALLER	As an INSTALLER user you are allowed to distribute software to the nodes and manage the installation process.
SECADM	The FOXMAN-UN security administrator - SECADM role, allows the user to configure the FOXMAN-UN itself and grants FOXMAN-UN admin rights to manage users and roles, and to manage DIRAC and FU credentials.
RBACMNT	The RBACMNT role represents a subset of Security Administrator permissions, allowing role configuration, definition and assignment.

The roles can be assigned to users. A user can have different roles at the same (i.e., it is possible to assign one or more roles to a user).

Assigning roles to a user will provide that user with the capability to access certain functionalities and resources in the network.

Please note:
Whenever a role is assigned to a user, the user will be granted permissions to see the nodes in FOXMAN-UN (old NEM Client).

3 Permissions

Each role is composed of a set of permissions.

These permissions are used to identify which parts and objects inside the FOXMAN-UN are subject to be operated/accessed by a user.

A user has roles assigned. Each role has a set of permissions. The sum of all permissions of all roles assigned to a user determines what a user can do inside the FOXMAN-UN.

Permissions are a fixed set of properties. The properties can be flags (enable/disable access to one functionality) or an access property determining if you have read access, full access, or no access (“none”) to specific elements in the system.

Permissions are responsible to give a user access to elements in the system

The definition of the permissions present in the system shown below will help clarifying the concept:

Network Engineering		**Linked Menu** (NEM Client)	**Authorization Filter, Restricted URLs** (not for admin or app token) (POST; PATCH, PUT)
Section Management	Enables the possibility to edit sections.	*Operation failure when writing section	sections
Network Design	Defines the capability to see or edit meaningful services on top of network infrastructure. Allows the management and configuration of MPLS-TP, Networking Package and advanced services.	Application → ENP Application → NP *operation failures on editing Application → CEM Application → ENP expert mode disabled for viewer	"/npnetworkmgr/", "/enp/" "\\/mib\\/mpls\\/", "\\/mib\\/cem\\/", "\\/mib\\/tdm\\/"
Traffic Engineering	Allows the creation and use of service profiles for MPLS-TP networks (only makes sense in combination with previous one).	*Authorization error	
Maps, Agents & Nodes	Exposes the permission to see the nodes in the system, or to be able to create and group nodes inside the FOXMAN-UN.	View/edit such items	symbols
	Provides the capability to access/edit the nodes, agents and maps defined in the FOXMAN-UN.	Execute commands in FO Agent Provides access to ALS Configurator (edit mode)	/agents /bpnodes
Ethernet Security Manager	Enables the possibility to access Ethernet Security Manager operations inside the client.	Application → ESM	
Network Monitoring			
Service Supervision	Exposes the possibility to supervise services and create such supervision services	Application → Service Supervision (No permission) *Authorization error	"service-supervision", "servicesupervision", "/bpservicemgr/services"
Performance Monitoring	Enables the access to performance monitoring	Network → PM System → Metrics Database	
Alarm Configuration	Configuration of alarm related settings (Alarm customization, forwarding and related global settings)	Fault management → Alarm Configuration	"/bpalarms/customisations", "/bpalarms/settings"
Alarm Management	Capability to see/manage system and node alarms and acknowledge them	Acknowledge/clear alarms in alarm list.	alarms

System Management			
Role Base Access Control	Allows the creation and edition of users, including the capability to assign/unassign roles to specific users.	Role Base Access Control tab in NEM Configurator	"/rbac", "/bp/security"
Credential Management	Exposes credential distribution functionality: the capability to distribute FOXMAN-UN keys or passwords to nodes. Management of SNMP security profiles.	SNMP Security Profiles Credentials distribution; Credentials distribution tasks	READ restricted also "/credentialdistribution"
Remote Administration	Exposes the capability to execute server related management operations, like starting or stopping services, creating private/public key pairs or main standby configuration.	System → RAT (Initial Screen → RAT)	"/mainstandby", "/nemcore/service", "/nemcore/inventory"
Remote Execution	Allows the access to a set of scripts executed on server side to perform various sets of functionalities.	System → Remote Executor	READ restricted also "/nemcore/scripts"
Node Management			
Node Restore Configuration	Enables the capability to restore one of the five previous NE configurations stored automatically by the system.	*Authorization	
Profile and CPS Management	Allows the access to legacy operations for administration of NE Passwords, Profile/CPS and ESW tasks.	Network → Profile & CPS Tasks	
Software Management	Exposes the possibility to access new software management tool.	Network → ESW Management	ESW
Node Access Information	Allows the possibility to access nodes as information user class.	ECST info Read-only other tools	
Node Access Maintenance	Allows the possibility to access nodes as maintenance user class.	ECST maintenance	
Node Access Manager	Allows the possibility to access nodes as manager user class, or to configure nodes in those which has no user class associated.	ECST Manager Other tools write access	
Node Access Session Manager	Allows the possibility to access nodes as session manager user class.	ECST Session Manager	

4 Restrictions

When assigning a role to a user, the role can be restricted:

- You can either restrict the set of nodes and elements the user will be able to manage (via selecting a domain) or
- set the expiration date for the assignment.

By default permissions are applied to all elements defined in the system (there is a domain called “NMS-All”).

By default roles assignments are not expiring.

5 Enhanced authorization filter

To strengthen security access to system items, some filtering can be defined based on the roles assigned to users and URLs they are trying to access.

The enhanced authorization security filter is exposed in the file

`/opt/nem/voyager/apigateway/etc/authorizationRules.json,`

and automatically used internally by the system. These filters can be extended, enhanced or disabled in case of necessity.

i

Please note:

- Enabling a new filter could end up in system malfunction if not carefully evaluated.
- Only a NEM administrator has the permission to edit the above-mentioned file.

6 Annex

6.1 Associated Documents

[1] IEC 62351-8:2020 Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control for power system management

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center
(Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks