NetIQ Privileged Access Manager 4.5 Security Target

Date: *July 30, 2024*
Version: *1.16*

Prepared By: *Michael Angelo*
Prepared For: *OpenText*
275 Frank Tompa Drive
Waterloo ON N2L 0A1
Canada

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Privileged Access Manager 4.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1. Introduction:

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1. Security Target Reference:

ST Title	NetIQ Privileged Access Manager 4.5 Security Target
ST Revision	1.16
ST Publication Date	July 30, 2024
Author	Michael F. Angelo

1.2. TOE Reference:

TOE Reference	NetIQ Privileged Access Manager 4.5

1.3. Document Organization:

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4. Document Terminology:

The following table describes the acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 3.1
DB	Database
EAL	Evaluation Assurance Level
EOE	Events Originating External to the TOE
ESX	Elastic Sky X
ESXI	ESX integrated
FIPS	Federal Information Processing System

TERM	DEFINITION
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
ISO	International Standards Organization.
LDAP	Lightweight Directory Access Protocol
NLA	Network Level Authentication
NTLM	NT Lan Manager
NTP	Network Time Protocol
OSP	Organizational Security Policy
OVF	Open Virtualization Format
PAM	Privileged Access Manager
PM	Password Management
RDP	Remote Desktop Protocol
SCP	Secure Copy
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Defined Protocol

Table 2 – Acronyms Used in Security Target

1.5. TOE Overview:

The TOE is Privileged Access Manager 4.5. The TOE is a privileged account management system which provides comprehensive privileged user management, advanced authentication for privileged accounts, risk-based privilege session control, and secure password vaulting.

This TOE features enable user data protection by enabling an administrator to:

- control account data and reduce administrative overhead
- provide visibility into privileged user activity
- enable administrators to detect unauthorized user access to sensitive information
- enable the control and monitoring of account (both privileged and non-privileged) access
- act as an aggregator / consolidator for multiple system accounts including applications, databases, servers, and the cloud
- allow for the delegation of privileges to users without exposing privileged account credentials
- enforce administrative access controls on system reports, components, audit logs, and configuration files for all users as well as users based on identity and roles

The TOE also enables user identification and authentication via:

- the ability to maintain a list of security attributes belonging to users such as identity passwords, and roles
- the ability to authenticate and identify users before performing any other actions

The TOE also provides for the protection of stored credentials and access to them as well as the ability to terminate interactive sessions after a configured timeframe or allow for users to terminate their own interactive sessions.

The TOE uses HTTPS/TLS to communicate with Users (Administrators, TOE Users, End point users. The TOE also uses HTTPS/TLS to communicate with TOE Elements. The TOE supports TLS v1.2. The operational environment must also support TLS v1.2 in order to interoperate with the TOE.

1.6. TOE Description:

1.6.1. Overview:

The TOE consists of the following components:

- Console[1] (Administrator, PAM User, EndPoint User)
- PAM Manager[2].
- PAM Agent[3] (AKA Server with Agent)

[1] The Console may also be referred to in documentation as the Framework Manager Console. Additional details of its functionality can be found in the Privileged Access Manager Administration Guide.

CE 24.3 (v4.5) Additional details of its functionality can be found in the Privileged Access Manager CE 24.3 (v4.5) Administration Guide.

[3] The PAM Agent may also be referred to in documentation as the Framework Agent. Additional details of its functionality can be found in the Privileged Access Manager CE 24.3 (v4.5) Administration Guide.

The evaluated configuration is depicted in the figure[4] below:

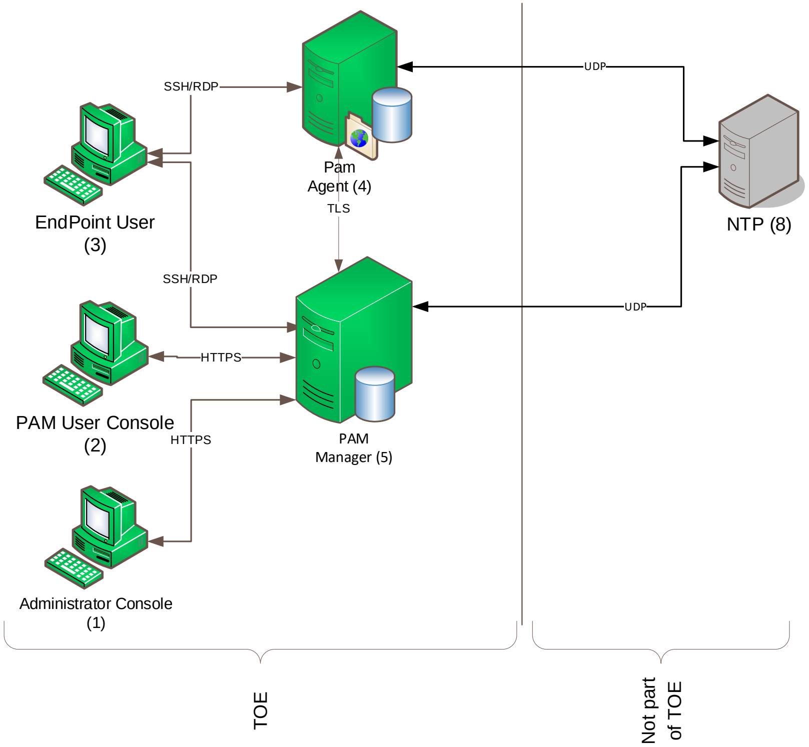


Figure 1 – PAM 4.5 Evaluated Configuration

1.6.2. TOE Environment:

The following TOE components can be installed in virtual machines (VM) or on explicit hardware. The TOE components are:

- Administrator Console / EndPoint User Console / PAM User Console
- PAM Manager
- PAM Agent

Note: The Pam Manager and the PAM Agent time needs to be synchronized.

The configuration requirements for the operational environment to support the TOE are listed in the table below:

Category	Administrator Console / EndPoint User Console / PAM User Console	PAM Manager	PAM Agent
Processor	2.5 GHZ or equivalent 2 CPU cores	2.5 GHZ or equivalent 2 CPU cores	2.5 GHZ or equivalent 2 CPU cores
Memory	8 GB	8 GB	4 GB
Storage	5 GB	5 GB	10 GB

Table 3 – Hardware Environment Requirements

The TOE requires the hardware as described in Table 3 and the Software environment in Table 4.

[4] Components that are not part of the TOE are to the

right of the line. These components are included in this diagram for completeness of documentation.

1.6.3. Software Supplied by the IT Environment:

The TOE consists of a set of software applications run on one or multiple distributed systems. The TOE requires the following software components:

TOE Component	Environment Requirements
Administrator Console / EndPoint User Console / PAM User Console	Microsoft Windows 10 (64-bit) Microsoft Edge (with latest updates)
PAM Manager	SUSE Linux Enterprise Server (with latest SP) (64-bit)
PAM Agent	Microsoft Windows Server 2019 (64-bit) SUSE Linux Enterprise Server 15 SP1(64-bit)

Table 4 – IT Environment Component Requirements

For the evaluation the IT environment also requires the following software components:

- NTP Server

1.6.4. TOE Usage:

The TOE allows for TOE Administrators to delegate roles to TOE users to provide general user access to systems. The product has a three-tier privilege concept. They are:

- TOE Administrators – TOE Administrators grant privileges to TOE ‘PAM’ Users, as well as defining roles and rules for the overall system.
- TOE ‘PAM’ Users – TOE ‘PAM’ Users enable endpoint users’ access to systems based on defined roles and rules.
- TOE Endpoint Users – TOE Endpoint Users use the TOE to access resources for which they are explicitly granted access.

1.6.5. TOE Component Descriptions:

This section has been winnowed down to include only the elements that are in the certification due to lack of consistency in the certifiers in the Canadian scheme and their requirements.

- Console[5]

The Console is a web-based interface accessed through supported web browsers. The Console provides access to Administrator or PAM Users to provide functions based on user associated roles and rules. The Console serves three functions. First, to enable the configuration of the system (Administrator). Second is to allow for the review and output from the product (EndPoint User). Outputs include alerts (indicating anomalies) and reports indicating status and events. Lastly, the console enables commands to be forwarded to systems or applications for which PAM is controlling access (PAM User).

- PAM Manager

The PAM Manager is responsible for validating access requests against the rules database to determine access and authorization. The PAM Manager is also responsible for generating audit records and enabling their review as well as storing them in the database.

- PAM Agent

The PAM Agent forwards requests to the PAM Manager and either allows or rejects request as appropriate to the response from the PAM Manager. The PAM Agent is also responsible for creating operational recordings.

1.6.6. Physical Boundary:

The TOE is a software TOE and includes the following components:

[5] The console is used for management and operational user functions and may be referred to as Framework Manager Console, User Console, Administrator Console depending on the functions it is performing.

- Console (EndPoint User[6], PAM User, and Administrator)
- PAM Manager
- Agents

The following figure presents the TOE diagram. The shaded elements are excluded from the TOE.

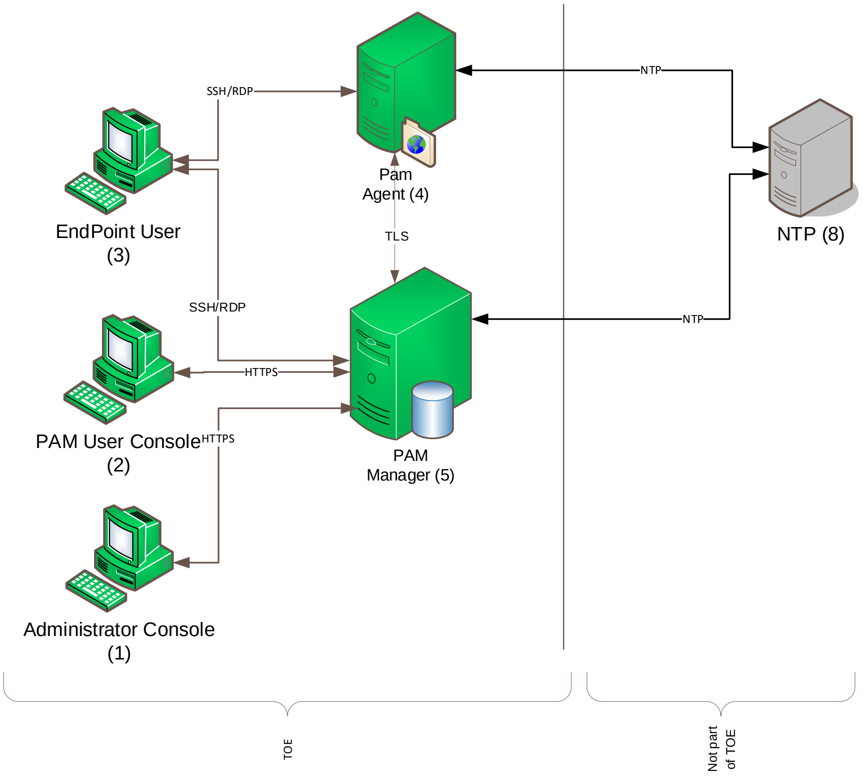


Figure 2 – TOE Boundary[7],

For the purpose of this evaluation the TOE will be configured as depicted in Figure 1. [8]

COMPONENT	VERSION NUMBER
Privileged Access Manager	4.5.0.0
Console (Consisting of PAM User Console, Administrator Console, and the EndPoint User)	4.5.0.0

[6] The endpoint user is another name for the user or non-system administrator non PAM administrator of the system.

[7] While PAM Manager / Agents can use a database package for storage of information, we do not own or provide the database package itself, and thus it is not part of the certification.

[8] SSH or RDP connections are based on the target system which can be Unix/Linux or Windows respectively.

COMPONENT	VERSION NUMBER
Agents	4.5.0.0

Table 5 – Evaluated Configurations for the TOE

Note the following constraints for the evaluated configuration:

- While the product may use a Database to store information, it is not included in the certification.
- The hardware, operating systems and third-party support software on each of the systems are excluded from the TOE boundary.
- The API and command line interfaces are excluded from evaluation.
- While PAM depends on encryption provided by the operating system in the form of the RDP protocol or Voltage Cryptographic Module v5.0, it does not implement its own.

1.6.7. Logical Boundary:

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

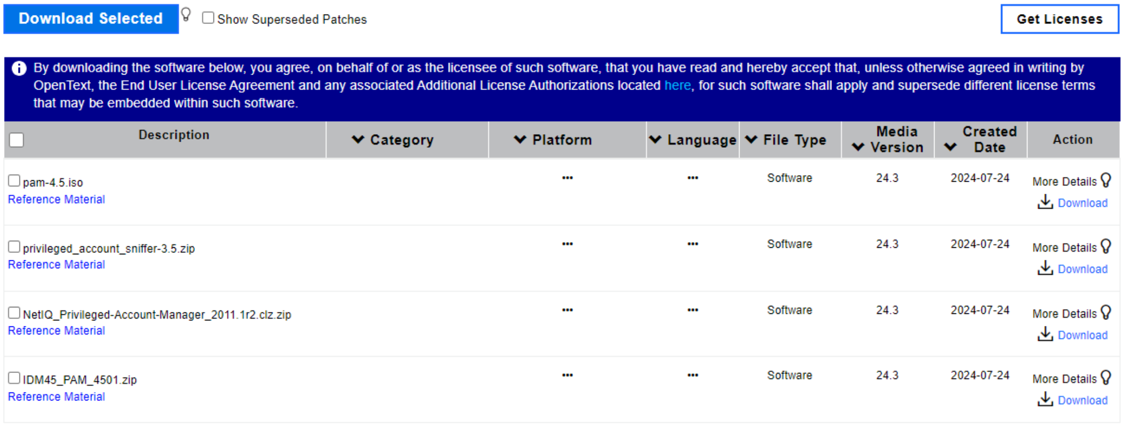
TSF	DESCRIPTION
Security Audit	The TOE generates audit records for all requested operations. The audit records include elements such as the requestor, requested access, status of request, conditions imposed on the request. For agent environments, the TOE supports the ability to authenticate the individual or rely on a third party for authentication, validate and enable roles and authorizations, and record all transactions that occur while the privilege is being used or the user is active. The TOE records events such as unauthorized access attempts, or privileges. Audit trails are stored for later review and analysis.
Cryptographic Support	Cryptography for TLS connections is supplied by the Voltage Cryptographic Module v.5.0, which is in the environment.
User Data Protection	The TOE provides two levels of access to the Credential Vault. These are PAM administrator and PAM User (also referred to as System User and User). The Credentials stored in the vault are protected via user account authorizations and permissions.
Identification and Authentication	The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. PAM Administrators, system administrators, and users must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.
Security Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of access control policies as well as control of roles associated with users. Administrators configure the TOE with the Console via a Web-based connection. The TOE provides an inactivity timeout mechanism which locks both the PAM Administrative console as well as for the End User Console. The TOE also provides a disconnect feature if a user attempts to execute unauthorized commands or facilities.
Protection of the TSF	The TOE protects the contents of the Credential Vault as well as the contents of the audit information from accidental disclosure.

TSF	DESCRIPTION
TOE Access	The TOE terminates interactive sessions after an administrator configurable time. It also allows the user to terminate their own interactive sessions.
Trusted Path / Channels	The TOE utilizes HTTPS/TLS to provide trusted paths and inter-TSF trusted channels.

Table 6 – Logical Boundary Descriptions

1.6.8. TOE Delivery:

The TOE software is provided to customers via secure download from the download portal (https://sld.microfocus.com/mysoftware/index)The software is available as an iso formatted optical disk (.iso). To install the TOE, you will need to download and expand PAM-4.5.iso. Once downloaded, the ISO files can be expanded to perform the installation.



By downloading the software below, you agree, on behalf of or as the licensee of such software, that you have read and hereby accept that, unless otherwise agreed in writing by OpenText, the End User License Agreement and any associated Additional License Authorizations located here, for such software shall apply and supersede different license terms that may be embedded within such software.

□ Description	Category	Platform	Language	File Type	Media Version	Created Date	Action
□ pam-4.5.iso Reference Material		•••	•••	Software	24.3	2024-07-24	More Details Download
□ privileged_account_sniffer-3.5.zip Reference Material		•••	•••	Software	24.3	2024-07-24	More Details Download
□ NetIQ_Privileged-Account-Manager_2011.1r2.clz.zip Reference Material		•••	•••	Software	24.3	2024-07-24	More Details Download
□ IDM45_PAM_4501.zip Reference Material		•••	•••	Software	24.3	2024-07-24	More Details Download

Figure 3 – Sample Download List

The documentation is available on the web in either html or pdf formats. For addition information please see the product guidance documents.

1.6.9. TOE Guidance:

The TOE includes the following guidance documentation:

- Privileged Access Manager 24.3 (v4.5) Release Notes July 2024
- Privileged Access Manager CE 24.2 (v4.5) Installation Guide July 2024
- Privileged Access Manager CE 24.3 (v4.5) Administration Guide July 2024
- Privileged Access Manager CE 24.2 (v4.5) User Guide July 2024
- Privileged Access Manager CE 24.2 (v4.5) Security Guide June 2024

For additional generic TOE Documentation, refer to Privileged Access Manager (Privileged Access Manager 4.5 (netiq.com)). Additional TOE operational guidance and installation procedures will be provided in the Privileged Access Manager 4.5 Operational Guidance and Installation Procedures (AGD-IGS.1) document.

1.7. Administrative Access Control SFP:

The TOE implements an access control SFP named *Administrative Access Control SFP*. This SFP determines and enforces the privileges associated with user roles. An authorized administrator can define specific privileges available to administrators and users via the Console.

The TOE implements user roles via defined collections of privileges, access entitlements, subjects, and times. These privileges are defined and assigned by the administrator.

- TOE Product Documentation

1.7.1. Supported Functionality Excluded from the Evaluated Configuration:

- While stored TOE data is encrypted, it is done by the environment database package.
- For some protocols, PAM depends on encryption provided by the operating environment.
- PAM is not evaluated with RDP and NLA enabled.
- RDP with NLA and FIPS mode enabled are excluded from the evaluated configuration.
- Agentless server.
- PAM CLI

2. Conformance Claims:

2.1. CC Conformance Claim:

The TOE is conformant to Common Criteria Version 3.1 Revision 5, April 2017 CC Part 2 extended and CC Part 3 conformant.

2.2. PP Claim:

The TOE does not claim conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017)). The TOE does not claim conformance to any functional package. The TOE EAL2 assurance package is augmented with ALC_FLR.3.

2.4. Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1. Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration. The asset is the configuration of the TOE.
T.NO_PRIV	An authorized user of the TOE exceeds their assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data. The assets are the: - audit data that is collected - configuration of the TOE - privileges / rights / roles assigned to users - stored credentials
T.SENSDATA	An unauthorized user may be able to view sensitive data passed between the TOE and its remote users, and between the TOE and external web servers, and exploit this data to gain unauthorized privileges on the TOE.

Table 7 – Threats Addressed by the TOE

3.2. Organizational Security Policies

The TOE meets the following organizational security policies:

ASSUMPTION	DESCRIPTION
P.EVENTS	All PAM administrator, System Administrators, and user activities involving the TOE shall be monitored.
P.INCIDENTS	Activities representing potential issues should be managed to resolution. This enables the detection and potential prevention of harm to the TOE or the infrastructure the TOE is used to monitor and or protect.

Table 8 – Organizational Security Policies

3.3. Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.AUDIT_PROTECT	The Audit Data (which is used to store transaction logs, and track other audit events) is located within a Database and facility that provides physical and logical controlled access.
A.CDB_PROTECT	The Configuration Database, which contains the Roles and Rules, is located within a facility that provides physical and logical controlled access.
A.HTTPS	Web browsers used to access the TOE shall support HTTPS using TLS.
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.LOST_CRED	The TOE environment protects against lost or stolen credentials from exposure or compromise.
A.MANAGE	Privileged users (Administrators and PAM Users) of the TOE are assumed to be appropriately trained (and competent) to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Privileged users (Administrators, PAM Users, and users) of the TOE, are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Privileged Users (Administrators and PAM Users, and users) will not leave their systems unattended and unlocked.
A.TIMESOURCE	The TOE has a trusted source for system time via NTP server
A.UPDATE	The TOE, and the TOE environment are regularly updated by an administrator to address potential and actual vulnerabilities.

Table 9 – Assumptions

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.AUDIT	The TOE shall collect data from all TOE activities including changes to permissions, privileges, roles, rules, and provisioning of access.
O.AUDIT_REVIEW	The TOE shall provide the capability to manage user activity and incidents. This enables the TOE to provide responses that an authorized PAM Administrator may execute to analyze and expedite resolutions to potential security events and issues.
O.CAPTURE_EVENT	The TOE shall collect transaction and audit data from PAM Administrators, PAM Users, and Users, and user activity employing the TOE with accurate timestamps. The collected data is critical to the analysis and tracking of user events in the environment which might indicate security issues.
O.PRIVILEGE	The TOE must protect stored credentials from disclosure.
O.SEC_ACCESS	The TOE shall ensure that only Administrators, PAM Users, and authorized applications are granted access to security functions, configuration, and associated data. This prevents unauthorized users from performing actions that may disable the TOE and result in undetected security events and issues.

Table 10 – TOE Security Objectives

4.2. Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.DATA_PROTECT	The facility surrounding the TOE data must provide physical and logical controlled access.
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
OE.COM_PROTECT	The TOE must make use of operating environment cryptographic functions for the protection of sensitive data in transit. The TOE must ensure the confidentiality of data passed between itself and remote users, and between the TOE and external web servers.
OE.HTTPS	Web browsers and web servers used to access the TOE shall support HTTPS using TLS.
OE.PERSONNEL	Authorized PAM administrators are non-hostile and follow all PAM administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any PAM administrator, user or operator of the TOE must be trusted to not disclose their authentication credentials. Authorized PAM administrators are also required to manage and administer the TOE in a secure manner. Authorized PAM administrators must be competent and security aware personnel in accordance with the administrator documentation.

OBJECTIVE	DESCRIPTION
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.
OE.PRO_STOREDCRED	The TOE operating environment shall protect stored credentials from disclosure.[9]
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.UPDATE	The TOE operational environment is updated by an administrator to address potential and actual vulnerabilities.

Table 11 – Operational Environment Security Objectives

4.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES ASSUMPTIONS / THREATS / POLICIES	O.AUDIT	O.AUDIT_REVIEW	O.CAPTURE_EVENT	OE.COM_PROTECT	O.PRIVILEGE	O.SEC_ACCESS	OE.DATA_PROTECT	OE.ENV_PROTECT	OE.HTTPS	OE.PERSONNEL	OE.PHYSEC	OE.PRO_STOREDCRED	OE.TIME	OE.UPDATE
A.AUDIT_PROTECT							✓				✓			
A.CDB_PROTECT							✓				✓			
A.HTTPS									✓					
A.LOCATE											✓			
A.LOST_CRED												✓		
A.MANAGE										✓				
A.NOEVIL										✓				
A.TIMESOURCE													✓	
A.UPDATE														✓
T.NO_AUTH	✓					✓	✓	✓		✓	✓			
T.NO_PRIV	✓				✓	✓								
T.SENSDATA				✓										
P.EVENTS			✓							✓			✓	
P.INCIDENTS		✓								✓			✓	

Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

[9] Records are encrypted in the DB. Also the entire DB may be configured to be encrypted with a capability to change the DB encryption keys.

4.3.1. Mapping of Objectives:

ASSUMPTION / THREAT / POLICY	RATIONALE
A.AUDIT_PROTECT	This assumption is addressed by • OE.DATA_PROTECT which ensures the facility surrounding the TOE data must provide physical and logical controlled access. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.
A.CDB_PROTECT	This assumption is addressed by • OE.DATA_PROTECT which ensures the facility surrounding the TOE data must provide physical and logical controlled access. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE
A.HTTPS	This assumption is addressed by • OE.HTTPS which ensures that Web browsers and web servers used to access the TOE shall support HTTPS using TLS.
A.LOCATE	This assumption is addressed by OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.LOST_CRED	This assumption is addressed by: • OE.PRO_STOREDCRED which ensure that the TOE environment protects against lost or stolen credentials.
A.MANAGE	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that the Authorized PAM administrators are non-hostile and follow all PAM administrator guidance.
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
A.UPDATE	This assumption is addressed by OE. UPDATE. OE.UPDATE which requires the TOE operational environment be updated regularly to address potential and actual operational security issues.

ASSUMPTION / THREAT / POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.AUDIT, which ensures that all TOE transactions and attempted transactions are auditable and • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • OE.DATA_PROTECT, which ensures the facility surrounding the TOE data must provide physical and logical controlled access. • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by competent and security aware personnel in accordance with the administrator documentation. As well as that any PAM administrator, user, or operator of the TOE must be trusted to not disclose their authentication credentials. • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by • O.AUDIT which ensures that all TOE transactions and attempted transactions are auditable • O.PRIVILEGE, which ensures that the TOE protects stored credentials from disclosure • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
T.SENSDATA	This threat is countered by: • OE.COM_PROTECT – which ensures the use of cryptographic functions provided by the operating environment to protect sensitive data in transit.
P.EVENTS	This organizational security policy is enforced by • O.CAPTURE_EVENT, which ensures that the TOE collects data from PAM Administrators, System Users, and user activity employing the TOE and • OE.TIME, which provides support for enforcement of this policy by ensuring the provision of an accurate time source and • OE.PERSONNEL, which ensures that authorized PAM administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any user or operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

ASSUMPTION / THREAT / POLICY	RATIONALE
P.INCIDENTS	This organizational security policy is enforced by • O.AUDIT_REVIEW, which ensures that the TOE will provide the capability to review audit logs and • OE.TIME, which ensures that the TOE operating environment shall provide an accurate timestamp (via reliable NTP server) and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any user or operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

Table 13 – Mapping of Threats, Policies, and Assumptions to Objectives

5. Extended Components Definition

5.1. Definition of Extended Components

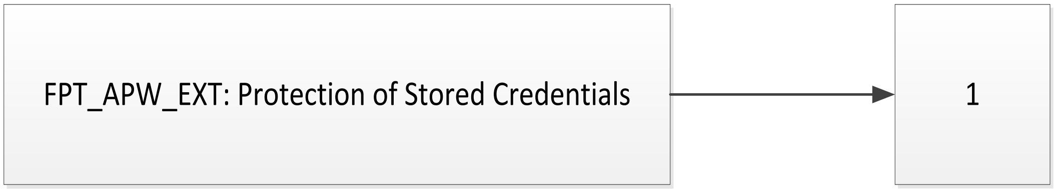
This section specifies the extended Security Functional Requirement (SFR) used in this ST. An extended family and an extended component have been created to address the protection of stored credentials. The family FPT_APW_EXT Protection of Stored Credentials is modeled after FPT_ITT Internal TOE TSF data transfer, and the SFR FPT_APW_EXT.1 Protection of Stored Credentials is modelled after FPT_ITT.1 Basic internal TSF data transfer protection.

5.1.1. FPT_APW_EXT Protection of Stored Credentials

Family Behavior

This family defines the requirements for protection of stored credentials from disclosure.

Component Leveling



FPT_APW_EXT describes the security and usage of stored credentials.

Management: FPT_APW_EXT.1

There are no management actions foreseen.

Audit: FPT_APW_EXT.1

There are no auditable events foreseen.

FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to:	No other components
Dependencies:	No dependencies

FPT_APW_EXT.1.1 The TSF shall prevent the disclosure of credentials by using access controls.

FPT_APW_EXT.1.2 The TSF shall present credentials to registered systems in response to a request from an authorized user.

6. Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1. Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by [*italicized text inside square brackets*].
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

6.2. Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit review
	FAU_STG.1	Protected Audit Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_APW_EXT.1 FPT_ITT.1	Protection of Stored Credentials Basic internal TSF data transfer protection
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TSE.1	TOE session establishment
Trusted Path/Channel	FTP_TRP.1	Trusted Path

Table 14 – TOE Security Functional Requirements

6.3. Security Audit (FAU)

6.3.1. FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the system;

b) All auditable events for the [*not specified*] level of audit; and

c) [User login/logout of the TOE, Login failures, All User access and activities performed while accessing systems]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information].

6.3.2. FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.3.3. FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator, and designated operators] with the capability to read [all audit data generated within the TOE] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.3.4. FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.3.5. FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.4. Cryptographic Support (FCS)

6.4.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [see table] and specified cryptographic key sizes [see table] that meet the following: [assignment: list of standards].

[

Algorithm	Mode (if applicable)	Key Size	Standard	Certificate #
AES	GCM	128, 192, 256 bits	SP 800-38D	3895
AES	CBC	128, 192, 256 bits	FIPS 197, SP 800-38A	3895
RSA		2048	FIPS 186-4	1985
ECDSA		Curves: P-224, P-256, P-384, P-521	FIPS 186-4	846
SHS	FIPS 180-4	1, 384, 256 bits	FIPS 180-4	3211

].

Application Note: This SFR corresponds to the correct invocation by the TOE, but not the implementation of cryptographic functionality.

6.4.2. FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwriting the RAM] that meets the following: [no standard].

Application Note: This SFR corresponds to the correct invocation by the TOE, but not the implementation of cryptographic functionality.

6.4.3. FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [establishment of TLS v1.2 channels] in accordance with a specified cryptographic algorithm [See Table] and cryptographic key sizes [See Table] that meet the following: [See Table].

[

Algorithm	Mode (if applicable)	Key Size	Standard	Certificate #
AES	GCM	128, 192, 256 bits	SP 800-38D	3895
AES	CBC	128, 192, 256 bits	FIPS 197, SP 800-38A	3895
RSA		2048	FIPS 186-4	1985
ECDSA		Curves: P-224, P-256, P-384, P-521	FIPS 186-4	846
SHS	FIPS 180-4	1, 384, 256 bits	FIPS 180-4	3211

].

Application Note: This SFR corresponds to the correct invocation by the TOE, but not the implementation of cryptographic functionality.

6.5. User Data Protection

6.5.1. FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [
Subjects: All Administrators and PAM users
Objects: System reports, components (i.e. credential vault, policies), audit logs, configuration files,
Operations: all Administrators and PAM users actions[10]]

6.5.2. FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [

Subjects: All Administrators and PAM users
Subject Attributes: User Identity, Roles
Objects: System reports, components, audit logs, configuration

[10] For example - Run report, schedule report, create role, create a user,

files[11],
Object Attributes: none.
Operations: View, Manage, Search, Run Reports
]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Authorized Administrators and PAM users are granted access to data if permitted by their role].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional rules].

6.6. Identification and Authentication (FIA)

6.6.1. FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Password, and Role].

6.6.2. FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.6.3. FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.7. Security Management (FMT)

6.7.1. FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to [*query, modify, delete*] the security attributes [User identity or Role] to [Administrator].

6.7.2. FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Administrative Access Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

[11] Configurations include the establishment and access to Correlation Engine/Rules, Reports, incidents, Event Actions

Application Note: All Roles must be explicitly granted by the Administrator. The default is to deny access to privileges not associated with Roles. <See Appendix A>

6.7.3. FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the functions listed in Table 15*] the [Role Data as listed in Table 15] to [Administrator]:

ROLE DATA	CHANGE_DEFAULT	QUERY	MODIFY	DELETE
User Role	✓	✓	✓	✓
User Account Attributes		✓	✓	✓

Table 15 – Management of TSF data

6.7.4. FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) Create accounts

b) Modify accounts

c) Define User Roles

d) Manage Reports

e) Change the user inactivity timeout interval].

6.7.5. FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, User, and Custom Roles[12]].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.8. Protection of the TSF (FPT_APW_EXT)

FPT_APW_EXT.1.1 The TSF shall prevent the disclosure of credentials by using access controls.

FPT_APW_EXT.1.2 The TSF shall present credentials to registered systems in response to a request from an authorized user.

6.9. Internal TOE TSF data transfer (FPT_ITT)

6.9.1. FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

Note: Cryptography is provided by the environment.

[12] A complete list of roles for reference can be found in Appendix A.

6.10. TOE Access (FTA)

6.10.1. FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a**n** [Administrator-configurable period of inactivity.]

6.10.2. FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session

6.10.3. FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [time].

6.11. Trusted Path / Channel

6.11.1. FTP_TRP Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [remote administration, PAM user access, and endpoint user access].

Note: The cryptography is provided by the environment.

6.12. Security Assurance Requirements

The assurance security requirements are summarized in the following table.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Part of TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.3	Systematic flaw remediation
ASE: ST evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Analysis of Coverage

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 16 – Security Assurance Requirements at EAL2+

6.13. Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access. The product was augmented to comply with ALC_FLR.3 in order to document and address requirements for remediation and reporting of faults that may be discovered in the product after release. The TOE invokes the Voltage Cryptographic Module v5.0 to establish TLS1.2 channels for secure communications.

6.14. Security Requirements Rationale

6.14.1. Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	YES	Although FIA_ UID.1 is not included, FIA_ UAU.2, which is hierarchical to FIA_ UID.1 is included. This satisfies this dependency.
FAU_SAR.1	FAU_GEN.1	YES	
FAU_SAR.2	FAU_SAR.1	YES	
FAU_STG.1	FAU_GEN.1	YES	
FCS_CKM.1	FCS_CKM.4	YES	Provided by the environment
FCS_CKM.4	FCS_CKM.1	YES	Provided by the environment
FCS_COP.1	FCS_CKM.4	YES	Provided by the environment
FDP_ACC.1	FDP_ACF.1	YES	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES	
FIA_ATD.1	N/A	N/A	
FIA_UAU.2	FIA_UID.1	YES	Although FIA_ UID.1 is not included, FIA_ UAU.2, which is hierarchical to FIA_ UID.1 is included. This satisfies this dependency.
FIA_UID.2	N/A	N/A	

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	YES	Satisfied by FDP_ACC.1, FMT_SMF.1, and FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_APW_EXT.1	N/A	N/A	
FTA_SSL.3	N/A	N/A	
FTA_SSL.4	N/A	N/A	
FTA_TSE.1	N/A	N/A	
FPT_ITT.1	N/A	N/A	
FTP_TRP.1	N/A	N/A	

Table 17 – Dependency Rationale

6.14.2. Security Functional Mappings

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE SFR	O.AUDIT	O.AUDIT_REVIEW	O.CAPTURE_EVENT	OE.COM_PROTECT	O.PRIVILEGE	O.SEC_ACCESS
FAU_GEN.1	✓	✓	✓			
FAU_GEN.2	✓	✓	✓			
FAU_SAR.1		✓	✓			
FAU_SAR.2		✓	✓			
FAU_STG.1			✓			✓
FCS_CKM.1				✓		
FCS_CKM.4				✓		
FCS_COP.1				✓		
FDP_ACC.1						✓
FDP_ACF.1						✓
FIA_ATD.1						✓
FIA_UAU.2						✓
FIA_UID.2						✓
FMT_MSA.1						✓
FMT_MSA.3						✓
FMT_MTD.1						✓
FMT_SMF.1						✓
FMT_SMR.1						✓
FPT_APW_EXT.1					✓	
FTA_SSL.3						✓
FTA_SSL.4						✓
FTA_TSE.1						✓
FPT_ITT.1				✓		
FTP_TRP.1				✓		

Table 18 – Mapping of TOE Security Functional Requirements and Objectives

6.14.3. Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.AUDIT	The objective to ensure that the TOE shall collect data from all TOE activities including changes to permissions or privileges and provisioning of access, and is met by the following security requirements: • FAU_GEN.1, FAU_GEN.2 define the auditing capability for events and administrative access control

Objective	RATIONALE
O.AUDIT_REVIEW	The objective to ensure that the TOE provides the capability to audit user activity and events is met by the following security requirements FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, and FAU_SAR.2 which define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs
O.CAPTURE_EVENT	The objective to ensure that the TOE shall collect data from PAM Administrators, System Users, and user activity employing the TOE with accurate timestamp. is met by the following security requirements: • FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, and FAU_SAR.2 define the auditing capability for events and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FAU_STG.1 defines the protection of the audit data.
OE.COM_PROTECT	This objective ensures that sensitive data in transit is protected[13]. The objective also ensures the confidentiality of data passed between itself and remote users, and between the TOE and external web servers. • FPT_ITT.1 specifies that a trusted communication channel is available to authorized TOE Components. • FTP_TRP.1 specifies that the TSF provides a distinct trusted communication path to/from TOE. • FCS_CKM.1 and FCS_COP.1 specify the keys that are generated and used. • FCS_CKM.4 specifies the destruction of the keys when no longer needed.
O.SEC_ACCESS	This objective ensures that the TOE shall ensure that only PAM Administrators, System Users, and authorized users and applications are granted access to security functions, configuration, and associated data only by authorized users and applications. • FAU_STG.1 defines the protection of the audit data. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user roles and their allowable actions • FIA_ATD.1 specifies security attributes for users of the TOE • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FMT_MSA.1 specifies that only privileged administrators can manage security attributes. • FMT_MSA.3 ensures that all default values of security attributes are restrictive in nature as to enforce the access control policy for the

[13] Note encryption is provided by the operating environment..

Objective	RATIONALE
	TOE. The Administrator can specify alternative initial values that will override default values. • FMT_MTD.1 restricts the ability to perform the functions listed in Table 15 on TSF data to the Administrator. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role. • FTA_SSL.3 requires the TSF terminate an interactive session after an administrator configured period. • FTA_SSL.4 requires the user be able to terminate their own session. • FTE_TSE.1 requires the TOE to deny access based on the time. •
O.PRIVILEGE	This objective ensures that the TOE shall protect stored credentials from exposure. • FPT_APW_EXT.1 specifies that the TOE shall protect credentials by using access controls and shall present credentials to registered systems in response to requests from authorized users.

Table 19 – Rationale for TOE SFRs to Objectives

7. TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path

7.2. Security Audit

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by start-up of the TOE)
- User login/logout, Login failures All User access and activities performed while accessing systems]

The TOE records the date, time and type of event as well as the subject identity and outcome of the event.

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console or via the external event sources. The Console provides a suitable means for an Administrator to interpret the information from either the audit log.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1
- FAU_SAR.2
- FAU_STG.1

7.3. Cryptographic Support

The Privileged Access Manager uses the Voltage Cryptographic Module v5.0 to establish TLS v1.2 connections for secure communications. This is not part of the TOE, but it is invoked by TOE.

The Cryptographic Support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1
- FCS_CKM.4
- FCS_COP.1

7.4. User Data Protection

The TOE implements a discretionary access control policy to define what roles can access particular functions of the TOE. All access and actions for system reports, component audit logs, TOE configuration, user account attributes (defined in FIA_ATD.1) are protected via access control lists. When a user attempts to perform an action on an object, the TOE verifies the role associated with the user. Access is granted if the user (or group of users) has the specific rights required for the type of operation requested on the object.

The User Data Protection is designed to satisfy the following security functional:

- FDP_ACC.1
- FDP_ACF.1

7.5. Identification and Authentication

The Console provides user interfaces that administrators may use to manage TOE functions. The Console provides web-based access to TOE functions through supported web browsers. The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Administrators and PAM Users with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Password
- Roles
- Rules

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

7.6. Security Management

Security Management is provided by enforcing roles and rules. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then assigned to individuals. In addition, rules can be specified controlling where and when the privileges may be used. Note a user may only have one role at a time.

The table below describes the TOE management functions along with their SFRs.

Functional Description	SFR
Only Administrators have the capability to change default values, query, modify, or delete users or roles.	FMT_MSA.1
The TOE provides restrictive default values for security attributes, as defined in Appendix A, by requiring the Administrator to explicitly allow access to Users. Only the Administrator may be able to change defaults.	FMT_MSA.3
Only the Administrator can control user privileges and user accounts attributes.	FMT_MTD.1

Functional Description	SFR
The TOE supports the following management functions: a) Create accounts b) Modify accounts c) Define User Roles d) Manage Reports e) Change the user inactivity timeout interval]	FMT_SMF.1
The TOE provides Administrator, PAM User, and user roles. For a complete list of default roles, refer to Appendix A. Administrator functions are defined in FMT_SMF.1. User privileges may be modified by the Administrator. By default, the User role allows limited viewing of events.	FMT_SMR.1

Table 20 – Security Management Functions and SFRs

7.7. Protection of the TSF

The TOE protects credentials from unauthorized access via access controls. The protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1

The TOE protects data transfers between TOE components using environmentally provided cryptography and HTTPS/TLS.

- FPT_ITT.1

The TOE OE supports TLS v1.2. The TOE OE supports the following TLS cipher suites, as defined in RFC 2246, RFC 4346 and RFC 5246:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_ CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

7.8. TOE Access

The TOE can terminate sessions either via a pre-configured inactivity timeout or via a user-initiated timeout. The TOE can also prevent TOE users (Administrators, PAM Users), from accessing the system outside of their authorized time.

Functional Description	SFR
The TOE provides the capability for TSF initiated termination of an interactive session after an administrator configurable period of inactivity.	FTA_SSL.3
The TOE provides the TSF with the ability to allow users to initiate termination of their interactive session.	FTA_SSL.4

Functional Description	SFR
The TOE provides the TSF with the ability to deny access at an unauthorized time.	FTA_TSE.1

7.9. Trusted Path

The Trusted Path function is designed to satisfy the following security functional requirements:

- FTP_TRP.1 – the TOE OE provides the trusted path for TOE Users, using **HTTPS/TLS.**

The Management and user Interfaces use operating system or environmentally supplied encryption and their associated protocols. All communications are provided by Voltage Cryptographic Module v5.0, and, in the test configuration, are performed using TLS 1.2).

8. Appendix A – Default Permissions[14]

8.1. Administration Permission

The following permissions can be assigned to any module if you want to delegate administrative rights.

Module	Descriptive Permission	Allows users to
Administration	Super Administrator	Have permission to access all modules and permissions.
	Administrator	Have permission to view and modify superusers, and view and modify groups with the super role defined. This role should also be able to add or delete users and groups and assign users to groups.

Administration Permission

8.2. Access Control Permission

The following permissions can be assigned to the command control module in order to control access to the Command Control and Access Control console. Select from the following permissions when you are creating a group that you want to manage and test the rules in the command control or access control database.

Module	Descriptive Permission	Allows users to
Access Control	All Permissions on Access Control and Command Control	Have permissions to perform all operations. This implies you have "*" permission to Access Control or Command Control console.
	View, Modify Objects and Transaction Permissions in Access Control and Command Control	Extract user credentials, including name and e-mail address, from the auth database into the account and user group definitions. Used in conjunction with the `cmdctrl` write (with read) and admin permissions. This implies you have read permission to `auth` module.
	View Access Control or Command Control Console	View the Access Control and Command Control console.
		This implies you have console permission to Access Control and Command Control console as applicable.
	View Access Control Objects	View the Access Control and Command Control objects.
	Manage Access Control and Command Control Objects	Configure the resources and credentials in the command control rules. This implies you have read permission to `prvcrdvlt` module.

[14] Section 4 Administrative Manual. Configuring Roles and Users, Overview

Module	Descriptive Permission	Allows users to
Access Control	All Permissions on Access Control and Command Control	Have permissions to perform all operations. This implies you have "*" permission to Access Control or Command Control console.
	View, Modify Objects and Transaction Permissions in Access Control and Command Control	Extract user credentials, including name and e-mail address, from the auth database into the account and user group definitions. Used in conjunction with the `cmdctrl` write (with read) and admin permissions. This implies you have read permission to `auth` module.
	View Access Control or Command Control Console	View the Access Control and Command Control console.
		This implies you have console permission to Access Control and Command Control console as applicable.
	View Access Control Objects	View the Access Control and Command Control objects.
	Manage Access Control and Command Control Objects	Configure the resources and credentials in the command control rules. This implies you have read permission to `prvcrdvlt` module.

Access Control Permission

8.3. Agent Management Permissions

The following permissions can be assigned to the agent management module.

Module	Descriptive Permission	Allows users to
Agent Management	All permissions on Agent Management	Have permissions to perform all operations. This implies you have "*" permission to Agent management.
	View the listed agents and perform administrative actions.	View the listed agents and perform administrative actions. This implies you have administrator permission to `unifi` module.
	View Host Console	View the Hosts console. This implies you have console permission to `unifi` module.
	Check agents status using command line utility	Check agents status using command line utility.
	Allow addition of Agents and Domains directly from the command line during registration	Allow addition of Agents and Domains directly from the command line during registration

Module	Descriptive Permission	Allows users to
	Allow creation of Agent records during registration	Allow creation of Agent records during registration.
	Allow creation of Domain records during registration	Allow creation of Domain records during registration

Agent Management Permission

8.4. Audit Reports Permission

The following permissions can be assigned to the auditing module to control access to the Reports console. For a group to manage auditing, the group also needs read permission to the auditing and authentication modules.

Module	Descriptive Permission	Allows users to
Audit Reports	All Permissions on audit reports	Have permissions to perform all operations. This implies you have "*" permission to audit reports.
	View audit sessions and manage settings	View the Compliance Auditor console. This implies you have console permission to `secaudit` module.
	View Reports Console	View the Reports console. This implies you have the console permission for `audit` module.
	View audit sessions	Read the audit database. You must use `console` along with read. This implies you have read permission for audit module.
	Create new audit reports and adjust filter settings in reports	Read and update the reports defined in the Reports console. This role is only useful when used in conjunction with the report permission.
	View command control reports	Read and update the reports defined in the Reports console. This role is only useful when used in conjunction with the report permission.
	View change log reports	View Account Logon reports. In conjunction you must use console and read permission. This implies you have logon permission for audit module.

Audit Reports Permission

You can use these Audit Report permissions to create the following types of audit managers:

- **Administrator:** To allow the group to update all aspects of the auditing module, including encryption and rollover, the group needs to be assigned the following permissions for the audit module:
    - admin
    - write
    - read
    - command
    - console

- **Manager:** To allow the group to update all aspects of the auditing module, except encryption and rollover, the group needs to be assigned the following permissions for the audit module:
    - write
    - read
    - command
    - console
- **User:** To allow the group to read and update a specific report, the group needs to be assigned the following permissions for the audit module:
    - command
    - console
    - report
    - <report defined read>
    - <report defined update>

    If you want the group to have read-only privileges to the report, do not assign the <report defined update> role. Users with read-only rights to a report can view the report from the console, view the keystroke sessions within the report, and select which audit databases to view (see the **Logfiles** tab). Users who also have the update right can update the report's filter, its name, and its description.

    Each report allows you to specify a read role and an update role. You need to remember those names and manually specify them here. The console does not provide any error checking, so you need to ensure to specify the valid name.

8.5. Compliance Audit Reports Permissions

The following permissions can be assigned to the compliance auditing module to control access to the Compliance Auditor console. For a group to manage compliance auditing, the group also needs read permission to the auditing and authentication modules.

Module	Descriptive Permission	Allows users to
Compliance Audit Report	All Permissions on compliance auditor	Have permissions to perform all operations. This implies you have "*" permission to audit reports.
	Add and modify audit rules in compliance auditor	Access reports with the report defined permissions.
		This implies you have report permissions to `audit` module.
	View compliance auditor console	View the Compliance Auditor console. This implies you have console permission to `secaudit` module.

Module	Descriptive Permission	Allows users to
	View and edit records in compliance auditor	View and edit records.

Compliance Audit Report Permission

8.6. Credential Vault Permissions

The following permissions can be assigned to the credential vault module in order to control access to the Credential Vault console. Select from the following permissions when you are creating a group to manage the Credential Vault.

Module	Descriptive Permission	Allows users to
Credential Vault	All Permissions on Credential vault	Have permissions to perform all operations. In conjunction you have to use `cmdctrl` module with admin permission. Must be used in conjunction with `userreqdashboard` module and admin role. This implies you have "*" permission to `prvcrdvlt` module.
	View, Add and Modify Resources and Credentials in Credential Vault	View, add, and modify the domains and credentials in Credential Vault. Must be used in conjunction with `userreqdashboard` module and admin role. To add, modify, delete scripts user requires module `taskmanager` in conjunction with the admin role. This implies you have admin permission to `prvcrdvlt` module.
	View Credential Vault Console	View the Credential Vault console. This implies you have console permission to `prvcrdvlt` module. View the resources and credentials in Credential Vault.
	View Resources and Credentials in Credential Vault	You must use `console` role along with `read` role to view the Credential Vault console and its content. This implies you have read permission to `prvcrdvlt` module. Add and modify the resources and credentials in Credential Vault.

Module	Descriptive Permission	Allows users to
	Add and Modify Resources and Credentials in Credential Vault	Must be used in conjunction with the prvcrdvlt read role. This implies you have write permission to `prvcrdvlt` module.
	Application SSO Administration	Add and modify the resources of Application SSO credentials in Credential Vault.

Credential Vault Permissions

8.7. Package Distribution Permissions

The following permissions can be assigned to the host module in order to control access to the Package Distribution console. Select from the following permissions when creating a group to manage the packages.

Module	Descriptive Permission	Allows users to
Package Distribution	Restricts Deployment of Packages to Specified Modules	Restricts deployment of packages to specified modules. This implies you have acl permission to distrib module.
	Install or patch the Command Control Agent (admin).	This implies you have install or patch permission to admin module.
	Install or patch the Command Control Agent (appsso).	This implies you have install or patch permission to appsso module.
	Install or Patch the Audit Manager (audit)	This implies you have install or patch permission to audit module.
	Install or patch the Command Control Agent (auth).	This implies you have install or patch permission to auth module.
	Install or patch the Command Control Agent (cmdctrl).	This implies you have install or patch permission to cmdctrl module.
	Install or patch the Command Control Agent (dbaudit).	This implies you have install or patch permission to dbaudit module.
	Install or patch the Command Control Agent (distrib).	This implies you have install or patch permission to distrib module.
	Install or patch the Command Control Agent (ldapagnt).	This implies you have install or patch permission to ldapagnt module.
	Install or patch the Command Control Agent (msgagnt).	This implies you have install or patch permission to msgagnt module.
	Install or patch the Command Control Agent (pkgman).	This implies you have install or patch permission to pkgman module.
	Install or patch the Command Control Agent (prvcrdvlt).	This implies you have install or patch permission to prvcrdvlt module.
	Install or patch the Command Control Agent (radiusagnt).	This implies you have install or patch permission to radiusagnt module.
	Install or patch the Command Control Agent (rdprelay).	This implies you have install or patch permission to rdprelay module.

Module	Descriptive Permission	Allows users to
	Install or patch the Command Control Agent (regclnt).	This implies you have install or patch permission to regclnt module.
	Install or patch the Command Control Agent (registry).	This implies you have install or patch permission to registry module.
	Install or patch the Command Control Agent (resreqagnt).	This implies you have install or patch permission to regreqagnt module.
	Install or patch the Command Control Agent (Command Control) Agent (rexec).	This implies you have install or patch permission to Command Control Agent rexec module.
	Install or patch the Command Control Agent (secaudit).	This implies you have install or patch permission to secaudit module.
	Install or Patch the SSH Agent (sshagnt)	This implies you have install or patch permission to sshagnt module.
	Install or patch the Command Control Agent (sshrelay).	This implies you have install or patch permission to sshrelay module.
	Install or patch the Command Control Agent (strfwd).	This implies you have install or patch permission to strfwd module.
	Install or patch the Command Control Agent (sysinfo).	This implies you have install or patch permission to sysinfo module.
	Install or patch the Command Control Agent (syslogemit).	This implies you have install or patch permission to syslogemit module.
	Install or patch the Command Control Agent (taskmanager).	This implies you have install or patch permission to taskmanager module.
	Install or patch the Command Control Agent (videoprocessor).	This implies you have install or patch permission to videoprocessor module.

Package Distribution Permissions

8.8. Package Management Permissions

The following role can be assigned to the package manager module in order to control access to the Package Manager console. When you are creating a group that you want to manage the distribution of updates to Privileged Access Manager, select the following:

Module	Descriptive Permission	Allows users to
Package Manager	All Permissions on Package Manager console	Have permissions to perform all operations. This implies you have “*” permission to audit reports.
	Manager Packages in Package repository	View the Package Manager console. This implies you have console permission to pkgman module.
	View Package Manager Console	View, add, update, or remove packages. This implies you have admin permission to pkgman module.

Package Management Permissions

8.9. Password Management Permissions

The following permissions can be assigned to the task manager module in order to view and modify scripts.

Module	Descriptive Permission	Allows users to
Password Management	View and Modify Scripts for Password Management.	Used for password management. This implies you have permission to taskmanager module

Password Management Permissions

8.10. User and Group Management Permissions

The following permissions can be assigned to the authentication module in order to control access to the User Manager console. Select from these permissions when you are setting up a group to manage users and groups.

Module	Descriptive Permission	Allows users to
User and Group Management	All Permissions on Framework user manager console	Have permissions to perform all operations. This implies you have "*" permission to `auth` module.
	Manage Users and Groups in Framework	Add or delete users and groups, and assign users to groups. This implies you have admin permission to `auth` module.
	View Users and Groups Management console	View the Users and Groups Management console. This implies you have console permission to `auth` module.
	Modify Attributes of Framework Users and Groups	Modify account settings. You must use `admin` role to view the Framework User Manager and its content. This implies you have act_settings permission to `auth` module.
	Add or Remove Permissions in Framework	Read the auth database. You must use `console` role along with `read` role to view the Framework User Manager and its content. This must be used with all other auth permissions. This implies you have read permission to `auth` module.
	View and Modify Super Users and Groups with Super Role in Framework	Add or remove permissions. You must use `console` role along with `read` and `admin` role to view the Framework User Manager and its content. This implies you have admin permission to `auth` module.

Module	Descriptive Permission	Allows users to
	Modify Account Settings in Framework	Modify superusers, and view and modify groups with the super role defined. This role should also be able to add or delete users and groups and assign users to groups. This implies you have super permission to `auth` module.
	View Framework Users and Groups	View superusers, and view groups with the super role defined.
	Generate API Tokens	Generate API tokens. This implies you have `api_token` permission to `auth` module.

User and group management permissions

8.11. User Access Requests Permissions

The following permissions can be assigned to control access to the Requests console. Select from the following permissions when you are creating a group to manage the Requests.

Module	Descriptive Permission	Allows users to
User Access Requests	All Permissions on Requests Console	Have permissions to perform all operations. This implies you have the "*" permission for the `userreqdashboard` module.
	View and Update Emergency Access and Credential Checkout requests	You will also require read and write permissions for `cmdctrl` and `prvcrdvlt` modules. View and update emergency access and credential checkout requests. This implies you have the admin permission for the `userreqdashboard` module. View the Requests console.
	View User Access Requests Console	This implies you have the console permission for the `userreqdashboard` module.

User Access Requests permissions

All modules can be allowed by following the above configuration of Module.