Oracle® Communications
Performance Intelligence Center

Security Guide

Release 10.2.1

E77483-01

June 2017

Oracle® Communications Performance Intelligence Center Security Guide, Release 10.2.1

⚠ **CAUTION: Use only the guide downloaded from Oracle Help Center.**

Refer to Appendix section for instructions on accessing My Oracle Support and Oracle Help Center.

Table of Contents

List of Figures

List of Tables

Part 1: Overview

This section gives an overview of the Oracle Communications Performance Intelligence Center and explains general principles of application security.

Audience and Scope

This document is provided for administrators who have to make arrangements and configure this product for secure operation.

To avoid replication and fragmentation of information, detailed instructions are only in the product's Installation Procedure. We suggest following usage of the documentation:

- Read this document for overview, key concepts and guidelines
- Perform installation steps following Installation Procedure
- Perform user management according to online manual of Security application
- Adjust PDU and field hiding according to online manual of Configuration application
- Review and apply relevant Security guides in case you add storage appliances (ODA, ZFS) or other Oracle Software (Database, Weblogic, Java, Oracle Linux)

Acronyms

Definition of terms frequently used in this document

Acronym	Definition
CLI	Command Line Interface through sh or bash Linux command interpreter. This can be reached either on a physical console or a virtual console (ILO/ILOM) or over ssh protocol.
ILO	Integrated Lights Out, electronic board inserted in HP servers allowing out of band access to the server even when it is powered off.
ILOM	Integrated Lights Out Management, electronic board inserted in Oracle servers allowing out of band access to the server even when it is powered off.
KPI	Key Performance Indicators, statistical counts aggregated by a rules-based engine. For Storage, KPI are considered as statistical xDR.
MOS	My Oracle Support, Oracle customer support web site where you can find additional information and resources about this product, see Appendix G for more information.
PIC	Oracle Communications Performance Intelligence Center
ODA	Oracle Database Appliance, engineered system, hardware and software, to run an Oracle Database for DR storage.
OS	Operating System, for PIC servers this is rpm based Linux 64 bits based on Oracle Enterprise Linux. Two flavors of OS are used for PIC servers, see Installation Overview.
PDU	Protocol Data Units are sequences of bytes captured on the telecommunications network, this is the main data input to PIC. During acquisition PIC adds a time stamp, link information and type code to later know what has been captured, when and where from.
TPD	Tekelec Platform Distribution, Linux distribution based on Oracle Linux 6.x with customization and tools dedicated to CGBU applications
xDR	eXtended Data Records is a generic term introduced by PIC to designate Call Detail Records (CDR), Transaction Detail Records (TDR), Session Detail Records (SDR), IP detail records (IPDR), …
ZFS	(formerly) Zettabyte File System, engineered system, hardware and software, storage appliance.

Glossary

Since Oracle Communications Performance Intelligence Center has had a significant rework of its licensing parts, new vocabulary has been introduced that is mostly aligned in user interface but not in all legacy features. Table below provides a mapping between licensing documentation and legacy user interfaces vocabulary.

Licensing Name	User Interface Old Name	Description
Acquisition Datafeed	TADAPT	Direct PDU feed from acquisition servers
Acquisition Server	xMF	Message Feeder, generic
DR Storage	DWS	Data Warehouse Server
Integrated Acquisition	IMF	Integrated Message Feeder
Management Server	NSP	Network Software Platform, host for configuration and applications
Mediation Datafeed	Datafeed	xDR feed from Mediation servers
Mediation Server	IXP	Integrated xDR Platform subsystem
Multiprotocol troubleshooting	ProTrace	xDR and call trace browser
Network and Service Alarm	ProAlarm	
Network and Service Dashboard	ProPerf	KPI graphing application
PDU Storage	PDU	Protocol Data Units storage
Performance Intelligence Center	PIC	Oracle Communications Performance Intelligence Center, the system as a whole
Probed Acquisition	PMF	Probed Message Feeder
SS7 Network Surveillance	ProDiag	Per Link activity counters

Table 1: Glossary

Product Overview

Oracle Communications Performance Intelligence Center is a Network and Service Performance Management system. It provides dashboard and alarming to monitor 2G/3G/LTE/IMS networks for network and service related criteria. It generates broad KPI to track events impacting the business and to analyze historical trends. It has near real-time call tracing capabilities to locate the source cause of network or service dysfunction. The system generates purpose built xDR used by various 3rd party applications like Business Intelligence, Revenue Assurance, Location Based Services, Machine to Machine (M2M) databases, or Fraud Management Systems. It can also deliver enriched signaling data and counters in near real-time mode to the service providers accounting system for interconnect billing and billing verification.

Oracle Communications Performance Intelligence Center is a distributed computing system over several Linux servers with dedicated roles: Management (and applications), Acquisition, Mediation and Storage.

General Security Principles

The following principles are fundamental to using any application securely.

Restrict physical Access to the System

Before considering IT security, consider first that all hardware (power, servers, disks, switches, cabling …) shall be installed in safe locations with restricted access in order prevent from unauthorized or accidental manipulation. Refer to the hardware documentation and make sure the installation is within normal operation range for temperature and electrical constraints.

Restrict Network Access to Critical Services

Management server front-end access shall be limited to your Intranet area. Only authorized workstations of your company and controlled remote access over VPN shall have access to the Management server. Servers and connections are not designed for use on public networks. Even on Intranet we recommend using secure https for Management server interaction with browsers.

Acquisition, Mediation and Storage servers shall be interconnected by an insulated back-end LAN or VLAN with firewalls filtering access. Management server has a second network access that is dedicated for interfacing with back-end servers. Only Administrators and Support teams need access to the back-end LAN. Standard end-users (other than administrators) interact only with Management server operating as a web application server.

Back-end VLAN makes use of non-ciphered protocols; detailed lists will be provided later in this document for firewall setup. Restrictive firewall and routing settings are recommended to avoid that those communications can be intercepted or tampered. This also extends to configurations where Acquisition or Mediation servers are relocated on a remote site. In such cases customer is requested to provide safe pipes from its own infrastructure to make sure machine to machine communication is safe.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities. Management server provides a security management application, with access restricted to Administrators that permits to configure roles, privilege and object ownership.

The system manages object ownership with the granularity of a "session" which collects a dedicated stream of xDR or statistics reconstituted from a subset of the network activity defined by protocol filters and link or SCTP association or logical flow in IP filters. This allows a segregation of access level considering different activities monitored. A session permanently gets new records and drops old records based on a lifetime configuration parameter.

Monitor System Activity

Audit log and System alarms are two applications provided to monitor system activity. Use these tools on a regular basis. Audit records normal action, including connections, configuration changes. System Alarms is a log of various incidents, when system encounters abnormal conditions.

Hardware related alarms are collected on Acquisition and Mediation servers and shown in System Alarms but not on standard servers (Management and Storage). To monitor hardware incidents on standard servers operating as Management server or Storage server, we recommend using of the shelf monitoring tools.

In addition it is possible to define threshold alarms on KPI, this product feature can also be used as a security feature if you set threshold values that would occur in case of abnormal action on the system. E.g. zero record per minute activity could be a security threshold alarm.

Virtualization Infrastructure

Some components of the system are compatible with an installation on a virtual server instead of a physical server.

Although security of the virtual infrastructure is out of the scope of this document, security in that area is not optional. Technical choices and security setup of the host, under local IT responsibility, shall follow best practices to protect the system against threats that could come from virtual infrastructure.

Oracle Communications Performance Intelligence Center behaves as expected from a guest system: it considers the virtual machine as a server. Adaptation to run in a VM consists of using drivers that match emulated hardware and being prepared for storage downsizing.

Other Software

Oracle Communications Performance Intelligence Center will deploy in combination with other Oracle products, depending on the configuration and role of each server, you will have to download latest revision of indicated version and install it according to instructions in installation guides. Recommended versions are:

Software	Acquisition or Mediation server	Generic server, Management or Storage	Comments
Linux	Special distribution TPD 7.4.x based on Oracle Linux 6.	Oracle Linux 7 latest update	Other versions may be in use on ODA and ZFS which have their own combination as an appliance.
Oracle Database	N/A	12c Enterprise edition with partitioning option ASMLIB 2.x	Other versions may be in use on ODA and ZFS which have their own combination as an appliance.
Java Development Kit (JDK)	8 latest update	8 latest update	PIC is not compatible with Java 9
Weblogic	N/A	12.2 WebLogic Server 12c	N/A

Table 2: Other Software

Release notes are provided to list compatible software for interoperation and links to update documents.

For each software make sure you download latest available update or minor version and apply required critical patches. For example Oracle Database 12.1.x.y.z: the product requires to use major version 12.1 but recommends using latest available x.y.z maintenance release or patch set to be in a safe situation versus possible known vulnerabilities or exposures.

Please refer to Oracle Help Center (http://docs.oracle.com/en/) for up to date information, each software has a dedicated Security Guide.

When using Linux, Java, Database, Weblogic assembled as an Oracle Database Appliance or a ZFS appliance, refer to the overall documentation dedicated to the engineered system.

For Acquisition and Mediation servers, OS distribution and application are bundled into a common ISO file, if needed, upgrades will be provided either as a maintenance release or as a patch set globally. MOS notes will inform you in case such updates are available.

Be careful, installation scripts and documented procedures provide predefined settings for these components, do not set parameters like for an independent use. Some changes in settings may show up incompatible with the product. Documenting all possible conflicts on settings goes beyond the scope of this document; generic recommendation is to follow installation guidelines provided with the product, in case you wish using different settings based on your internal policies, to be ready with reverting the changes in case of observed issues.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this note on MOS regularly for new patching notes or security related notes: Patches for Oracle Communications Performance Intelligence Center (Doc ID 1989320.2)

Part 2: Secure Installation and Configuration

Installation Overview

This section outlines the planning process for a secure installation and describes recommended deployment topologies for the system.

Understand Your Environment

Which resources am I protecting?

Oracle Communications Performance Intelligence Center is a distributed system over several standard servers and storage systems. Each server holds its own resources that require adapted level of protection:

Management server: is the central application and configuration server or group of servers. It holds system and session configuration and user information (login, credentials) as well as saved query results in an embedded database. It runs applications with an Apache http(s) front-end server and multiple Weblogic web container instances. The server acts as a web server but the type of application is meant for Intranet access level only. Security application in the Management server is the place where permissions are granted to users to browse all or parts of the data contained in sessions. Security application is restricted to administrators.

Storage servers: There are two types of storage servers. DWS store network reconstituted transactions (xDR) and statistics (KPI). PDU storage servers store PDU in flat files. Storage servers shall be connected to restricted back-end VLAN. They answer to queries from the Management server and work as high bandwidth data sink for meditation servers. Direct access to storage server would bypass the screening rules implemented in the Applications and therefore shall be protected. PDU storage servers share flat files on NFS shares.

Mediation servers: These servers perform real time correlation of PDU and generate xDR. They also aggregate xDR to generate KPI. Network tapped data transitions and is transformed on these servers. It is present from one minute to a few hours according to buffer management and aggregation level. Mediation servers get their configuration by replicating data from the Management server database.

Acquisition servers: They collect frames from the monitored network, or from associated network equipment in case of Integrated Acquisition, reassemble segments, split multiple chunks (in case of SCTP), timestamp each resulting PDU, and route it to Mediation servers according to filtering rules set on the Management server. Acquisition servers get their configuration by replicating data from the Management server database. Integrated Acquisition servers have dedicated interfaces to extract configuration information from the associated network equipment.

All servers are Linux based servers with their standard access protection (file system access protection for root and other users). By default all servers listen ssh, rmi and https ports in addition to dedicated ports that will be described later in this document. ssh access requires logging as per standard Linux account management, accounts are independent for each server. Oracle Communications Performance Intelligence Center does not use DHCP it connects configured IP addresses that are stored in the configuration database.. External servers can be addressed by names and need a DNS service: alarms forwarding, emailing passwords.

From whom am I protecting the resources?

All servers other than Management should be protected from any user access except administrators and support for maintenance.

Management server shall be accessible to identified Intranet users. They are asked for a personal login but this web server. Profile based permissions discriminate different levels of data access as configured by administrators. Access can be granted by users to sessions and this access can be full or with hidden fields according to user profile (more information in the online manual of Security application). Sessions containing call detail records can be restricted to Customer service troubleshooting teams, whereas sessions containing anonymized statistics (KPI) can be allowed for Network Planning or Marketing teams according to their nature. On sessions containing call detail records, a default field hiding mechanism applies to mask sensitive field content such as passwords or PIN codes or SMS content. Activate this mechanism (PDU hiding) from central configuration main page and make sure each user is associated with an appropriate profile.

What will happen if the protections on strategic resources fail?

Audit logs keep track over a few days of actions performed by users on the Management server. It is recommended to periodically browse these records to check if actions performed by each identified user are in the expected scope. Multiple condition filters allow looking at this from different perspectives. Excessive access permissions can be a result of misinterpreted application or privacy rules.

Failed login attempts are tracked as system alarms. An abnormal increase of such alarms could be a sign. System Alarms log is another part of the system that shall be watched at least daily because it also reports hardware failures.

OS level login attempts are tracked by standard Linux log services. Typically no such attempt is expected on any server for normal usage because all is managed by a web application portal. There is segregation on each server between system accounts (root) and application accounts (cfguser or tekelec) and Linux file permissions is a protection against unwanted access. OS account passwords shall be periodically changed and kept secret from end-users. Application users shall not get OS level login, if local infrastructure allows, ssh connection to servers shall be restricted to system administrator. However make sure management servers can open ssh connections on the backend VLAN with each managed server to perform backup operations.

The list of sessions with their timestamp of last insertion constitutes a valuable dashboard to watch because an intrusion as well as a hardware failure might interrupt the insertion of records to the sessions.

Recommended Deployment Topologies

This section describes recommended architectures for deploying Oracle Communication Performance Intelligence Center to secure access.

Intranet delimitation

Oracle Communications Performance Intelligence Center is an application designed to work inside an secured Intranet environment. It has not been specifically hardened to be exposed on The Internet. Computers able to reach product servers are expected to have passed a first level of authentication which is independent of this product and relies on local IT infrastructure (physical LAN connection, VPN connectors, MPLS, …)

Front-end and Back-end

The deployment recommendation is to use the well-known and generally accepted front-end back-end separation. Several variations of this architecture are possible depending on the number of locations for data collection and their distance from the Network operation Center (NOC):

Typical Deployment

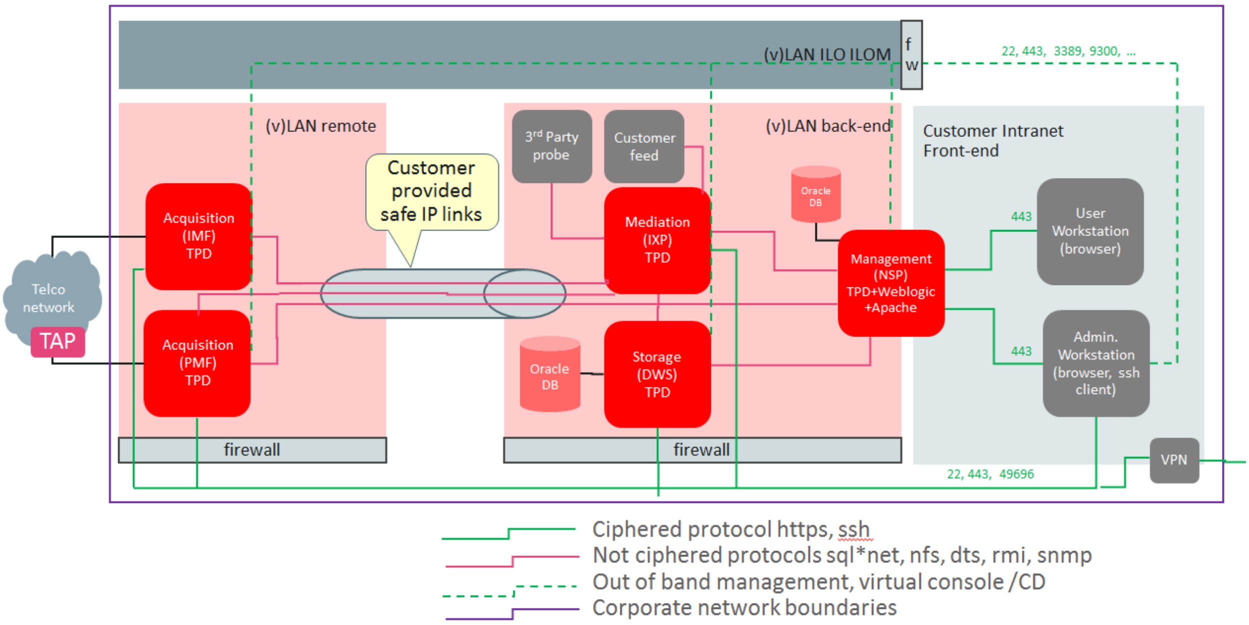
(v)LAN ILO ILOM
f
w
22, 443, 3389, 9300, ...
(v)LAN remote
Customer provided safe IP links
3rd Party probe
Customer feed
(v)LAN back-end
Customer Intranet
Front-end
Oracle DB
Acquisition (IMF) TPD
Mediation (IXP) TPD
Management (NSP) TPD+Weblogic +Apache
443
User Workstation (browser)
Telco network
TAP
Acquisition (PMF) TPD
Oracle DB
Storage (DWS) TPD
443
Admin. Workstation (browser, ssh client)
firewall
firewall
22, 443, 49696
VPN
Ciphered protocol https, ssh
Not ciphered protocols sql*net, nfs, dts, rmi, snmp
Out of band management, virtual console /CD
Corporate network boundaries

Figure 1: Traditional front-end back-end deployment

Alternatives are possible: Mediation and Storage can be on a remote site, multiple remote sites can exist, and Acquisition can exist on local back-end at NOC.

It is important to get this point for securing the system: Communication channels between Management, Mediation, Storage, and Acquisition are not on ciphered protocols and need a fence protection against unauthorized access. This extends to end-users who are only allowed to view parts of the contained information after screening has been performed by the application. Tapping internal links could lead to unwanted disclosure of information although this requires directed search and intrusion.

Out of Band management

Each server has an out of band management port (Integrated Lights Out – ILO/ILOM). These ports shall be connected to an independent LAN or VLAN, restricted to support and Maintenance. These ports allow access via a virtual console. Security of this maintenance access mode shall be enhanced for strong security, please refer to HP ILO documentation or Oracle/Sun ILOM documentation. Firewall filtering is recommended to protect access to the ILO/ILOM LAN or VLAN.

Note: Out of band connections are connected to the physical servers with a dedicated Ethernet port. It was not possible to make this obvious in figure 2-1 but these connections are not in contact with Back-end LAN or VLAN.

Server Types

This solution is using two types of operating system flavors which introduce differences in the way to manage security, especially critical patch updates:

- TPD servers run an adapted distribution of Oracle Linux with additional configuration and management procedures; on these servers application and operating system are closely bundled, changes to any of the two parts shall only be applied as maintenance releases, product patches or specific MOS notes. Changes update OS and application synchronously. The adapted distribution is restricted to an identified set of hardware configurations.
- Standard servers are installed with latest public release of Oracle Linux and applications are deployed in this environment in subsequent steps. Local administrators are in charge of applying needed critical patches when published for the Oracle Linux or for the applications.

Acquisition and Mediation servers are TPD servers. Management, Storage and other servers are standard servers with some exceptions when they are resulting as upgrades from older releases. As root CLI, it is possible to type getPlatRev, if this command is missing you are on a standard server, otherwise it will provide the TPD release and build numbers.

Installing Management

This section describes how to install and configure Management component securely. Please use Installation manual for step by step operation after security guidelines have been read in this document.

Management Key Concepts

Management server is a web server that is seen as the product façade by end-users. Except administrators for maintenance, no-one needs to connect on another server than the management server. This server runs administrative tools as well as applications in a web server mode.

Management has several sub-components that can collaborate physical server. Apache web server is serving https requests and load sharing over several Weblogic instances, by default there are 2 per physical server. Weblogic is in charge of the application logic in J2EE architecture. An Oracle Database Instance is used for persistence of user preferences, session configuration, application preferences, scheduled tasks, KPI parameters, temporary data queries and historical result sets.

Legacy Management servers are upgraded to run with the dedicated and pre-configured version of TPD. This version is adapted and tested for a given application version and shall not be changed or tuned. New Management servers are installed on top of a generic Oracle Linux.

Management Installation Security Steps

Once Management application is installed or upgraded on Management server according to installation manual, take care of these aspects:

- Deactivate http protocol (port 80) and configure http daemon for secure https protocol with a certificate. In-production systems shall use certificates purchased from a Certificate Authority (CA), lab and test systems can be configured with a self-signed certificate (this will trigger a warning message in the user's browsers). Appendix F provides additional information on http(s)
- Perform password handover with Consulting: change Application accounts with strong passwords in accordance to your local policy. Application accounts are listed in Appendix C (tagged with “PIC”).
- According to your local policies, set parameters for end user management. There is an option to send initial password by mail if you agree to connect Management server to a mail service (optional). As an alternative you can choose default initial passwords and communicate them without application support, flagged for change on first connection. Details can be found in the online guide of the Security application.
- Create or update end-user accounts in Security application. Each end-user shall have his personal identifier and password. We discourage from sharing team accounts…
- Define session boundaries and allocate ownership of sessions to end-users. This definition requires both security and telecom skills to define adequately the boundaries of each session. It can happen that because of important throughput a functional boundary may require several sessions in the configuration.

Management Ports

Oracle Communications Performance Intelligence Center does not include firewalls or configuration files for such equipment. Please use the list of ports that can connect to a Management server to create your firewall configurations. The product can be in various configurations and not all ports are needed, open only those that are active for your configuration and that come from outside the area delimited by your firewall.

Note: In tables to follow, lines with client type in blue represent additions made in latest release and applicable to site upgrades.

Front-end side (users LAN)

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Customer_Workstation	Management_FE	443	TCP/UDP	TLSV1+	https	N

Table 3: Management Ports Front-End

Back-End side (product services LAN, insulated from users LAN)

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Acquisition	Management_BE	0	ICMP	-	Ping	N
Acquisition	Management_BE	7	TCP/UDP	-	echo	N
Support_remote	Management_BE	22	TCP	SSHv2	ssh	N
Acquisition	Management_BE	22	TCP	SSHv2	ssh	N
Acquisition	Management_BE	123	UDP	-	ntp	N
Mediation	Management_BE	123	UDP	-	ntp	N
MicrotelInnovation	Management_BE	123	UDP	-	ntp	N
SWITCH	Management_BE	123	UDP	-	ntp	N
Customer_SNMP	Management_BE	161	UDP	-	snmp.a	N
MicrotelInnovation	Management_BE	162	UDP	-	snmp.b	Y
Support_remote	Management_FE	443	TCP/UDP	TLSV1+	https	N
Mediation	Management_BE	1099	TCP	-	RMI	N
Support_remote	Management_BE	1158	TCP	-	OracleDBEM.a	N
Acquisition	Management_BE	1521	TCP	-	OracleDBNet8	N
Support_remote	Management_BE	1521	TCP	-	OracleDBNet8	N
Mediation	Management_BE	1521	TCP	-	OracleDBNet8	N
Support_remote	Management_BE	5520	TCP	-	OracleDBEM.b	N
Support_remote	Management_BE	8001	TCP	-	nsp.admin.ldap	N
Mediation	Management_BE	41090	TCP	TLSV1+	NFM.b	N
Support_remote	Management_BE	49696	TCP	TLSV1+	JMX(https)	N
Acquisition	Management_BE	7001;7003	TCP	-	jms,t3	N
Support_remote	Management_BE	7001;7003	TCP	-	jms,t3	N
Mediation	Management_BE	7001;7003	TCP	-	jms,t3	N

Table 4: Management Ports Back-End

Installing Storage

Storage Key Concepts

Storage servers are used for large capacity data storage. There are two types of storage in the system:

xDR storage is based on an Oracle Database and provides structured tables for session data (call legs records, transaction records as well as statistics – KPI). Only Management server applications shall have access to xDR storage in a machine to machine paradigm. This server does not use accounts for end users. xDR storage servers can work together in a pool (up to 4 servers performing load sharing), this does not especially affect security, however be careful to apply security to each storage server independently this is not an integrated cluster.

PDU storage is based on shared directories with flat files. File sharing is based on NFS. Due to the huge size of PDU data, even with a few days lifetime only, it is difficult to find something specific in those large files. Applications use indexing through xDR to show right PDU content. Like for xDR no end user shall access directly to PDU storage; ProTrace application does this after checking individual permissions. PDU storage servers can work together in a pool (up to 4 servers performing load sharing), this does not especially affect security, however be careful to apply security to each storage server independently this is not an integrated cluster.

Both types of servers are Linux servers in a standard distribution. See paragraph "Other Software" in Part 1. about security updates.

Storage Installation Security Steps

Storage servers shall be installed from standard software, downloaded from Oracle. Each storage server has to be declared on the Management server. The connection is set on behalf of IPv4 addresses. The system does not use DNS.

These servers may require additional steps according to the security guides of the other software installed. In addition, ensure that the back-end delineation is effective: their IP should not be visible from computers of application users. This back-end separation is the duty of local network teams and firewalls settings that are out of scope of the product.

Storage Ports

Storage servers (DWS, PDU) are listening on a number of ports each dedicated for a special use:

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Mediation	Storage_PDU	0	ICMP	-	Ping	N
Mediation	Storage_PDU	111	TCP	-	portmap	N
Customer_Admin	Storage_PDU	215	TCP	TLSV1+	https	Y
Support_remote	Storage_PDU	215	TCP	TLSV1+	https	Y
Support_remote	Storage_DR	1158	TCP	-	OracleDBEM.a	N
Support_remote	Storage_DR	1521	TCP	-	OracleDBNet8	N
Management_BE	Storage_DR	1521	TCP	-	OracleDBNet8	N
Mediation	Storage_DR	1521	TCP	-	OracleDBNet8	N
Mediation	Storage_PDU	2049	UDP	-	NFS	N
Support_remote	Storage_DR	5520	TCP	-	OracleDBEM.b	N

Table 5: Storage Ports

Installing Mediation

Mediation Key Concepts

Mediation is performed on servers with specific and pre-configured Linux distribution. Linux modules come with Mediation ISO image. Mediation servers work in groups called subsystems in an operation mode similar to clusters. Servers belonging to the same subsystem shall be on a single site because inside the subsystem there are local communications that implement a middleware layer to make the subsystem working as a consistent entity. These communication shall not operate over long distance links (no WAN) due to both security and performance. PDU storage servers are also contributors to the subsystem because in addition to storing large files they can run mediation processes.

Mediation consists of several software operations based on a concept of data flows. A dataflow is a sequence of processes that get data from an acquisition or a mediation process. Some of them forward their result to another process, some forward data to storage servers. The connection between two processes is called a stream. It is based on a proprietary protocol on top of TCP/IP, not ciphered. A stream can get data from a distant server, from a server on the LAN or from the local loopback interface (process on the same server). Typical mediation processes are

- Build: input streams collect PDU from acquisition servers, several input streams can be involved. The process correlates PDU to generate xDR according to plug-in modules for various protocols (xDR builders). Output streams are made of xDR.
- Operate: operate takes one or several xDR streams as input and generates one or several xDR streams as output. The process works based on rules stored in scripts and provided by the Management server. Some scripts perform static enrichment (mapping values based on xDR field content), other scripts perform aggregation (counting records and summing variables based on rules) to generate KPI
- Store: input streams collect xDR either from Build or Operate and output is database insertion or CSV file generation. Note: this process is running on a mediation server as a client of the Storage server where records are actually preserved.

Each subsystem shares a virtual IP address (VIP) to designate its active master server which is the preferred interface to the Management server. In case of failure the VIP moves to the standby master, then becoming active. This VIP shall be reserved in the same range than other IP addresses for Mediation servers. Only Management server shall connect to the VIP and occasionally Administrators to physical server IP addresses for maintenance. End users shall not be allowed in this address space.

Management server shall be allowed to connect on any Mediation server because these mediation servers provide answers to PDU queries once the Management server has found xDR on a storage server.

Mediation Installation Security Steps

Mediation server installation ISO image comes with pre-configured settings that do not require special security actions on the server itself, except:

- Declare each Mediation server on the Management server by its IPv4 address. The product does not use DHCP, however IP setting and hostnames shall match naming convention.
- Setup firewalls between Intranet, Back-end and hardware support LAN.

- Make sure IP range for Mediation servers, including VIP are on a LAN or VLAN segregated from the end users and the visitors.

Mediation Ports

Firewall setup is proposed considering that usually mediation servers are connected to the same LAN than Storage servers and Management back-end.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Management_BE	Mediation	0	ICMP	-	Ping	N
Support_remote	Mediation	22	TCP	SSHv2	ssh	N
Management_BE	Mediation	22	TCP	SSHv2	ssh	N
Management_BE	Mediation	1099	TCP	-	RMI	N
Mediation	Mediation	2222	TCP	-	DTS	N
Management_BE	Mediation	5031	TCP	-	DSAPI.a	N
Management_BE	Mediation	5055	TCP	-	DSAPI.b	N
Mediation	Mediation	16810	TCP	-	inetsync	N
Mediation	Mediation	16878	TCP	-	inetmerge	N
Management_BE	Mediation	41000	TCP	-	RMI-JMX-sec	N
Management_BE	Mediation	41090	TCP	TLSV1+	NFM.b	N
Support_remote	Mediation	49696	TCP	TLSV1+	JMX(https)	N

Table 6: Mediation Ports

Installing Acquisition

Acquisition Key Concepts

Acquisition servers are frequently installed on remote sites to collect PDU from redundant points of the monitored network. When this is not needed they can be on the same LAN than Mediation servers. In case of installation on a remote site, IP connections flowing from site to site shall be protected by network provided encryption such as VPN or MPLS. This encryption is not provided by the product but is needed because those links forward PDU captured on the live network.

Acquisition servers have independent NIC. Standard Ethernet ports are connected to the LAN or a remote connection to Mediation LAN. Other ports, dedicated to acquisition are connected to devices that provide PDU data. In Integrated mode these ports are on a dedicated VLAN shared with Eagle™. In probed mode these ports are either connected to a switch capable of port mirroring or to a tapping device. This side of the connection shall get the same level of protection than the network links. The system does not encrypt captured data.

Acquisition Installation Security Steps

Acquisition servers installation ISO image comes with pre-configured settings that do not require extra security steps except to make sure connections with Acquisition servers are on a segregated LAN or VLAN protected by firewall settings.

Acquisition ports

Following list of ports have to be configured in firewalls or other network equipment surrounding acquisition servers:

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Management_BE	Acquisition	0	ICMP	-	Ping	N
Management_BE	Acquisition	7	TCP/UDP	-	echo	N
Support_remote	Acquisition	22	TCP	SSHv2	ssh	N
Management_BE	Acquisition	22	TCP	SSHv2	ssh	N
Management_BE	Acquisition	1099	TCP	-	RMI	N
Mediation	Acquisition	2222	TCP	-	DTS	N
Management_BE	Acquisition	3306	TCP	-	MySql	N
Management_BE	Acquisition	8060	TCP	-	http-s(ws)	Y
Management_BE	Acquisition	15616	TCP	-	JDBC	N
Acquisition	Acquisition	16810	TCP	-	inetsync	N
Management_BE	Acquisition	16810	TCP	-	inetsync	N
Acquisition	Acquisition	16878	TCP	-	inetmerge	N
Management_BE	Acquisition	16878	TCP	-	inetmerge	N
Management_BE	Acquisition	41000	TCP	-	RMI-JMX-sec	N
Support_remote	Acquisition	49696	TCP	TLSV1+	JMX(https)	N

Table 7: Acquisition Ports

Connecting other servers

Customer connection

Oracle Communications Performance Intelligence Center interacts with your local IT equipment to use standard IT services:

NTP

All servers have a constraint to have a redundant connection to a reliable Network Time Protocol source. The most frequent option to address this is to select Management primary server and one Mediation server as local NTP relays and connect only these two servers to an accurate NTP source. Then every server must be provided with a non-filtered NTP access to the Management server and to the first Mediation server.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Management_BE	Customer_NTP	123	UDP	-	ntp	N
Acquisition	Management_BE	123	UDP	-	ntp	N
Mediation	Management_BE	123	UDP	-	ntp	N
MicrotelInnovation	Management_BE	123	UDP	-	ntp	N
SWITCH	Management_BE	123	UDP	-	ntp	N

Table 8: NTP Ports

Mail

By default, passwords can be sent by a mail to application users. To achieve this you need to configure an access to a mail service and allow this destination in firewall settings.

Client type	Server type	Port	Transport	Secured layer	Protocol
Management_BE	Customer_MAIL	25	TCP	-	smtp

Table 9: Mail Ports

Feed targets

There are use cases where the data collected by the system is not only processed by Oracle Communications Performance Intelligence Center applications but also feeds local applications. There are two ways to feed data from the system, either by providing an Oracle Database server connection with a customized schema (Customer_DWH) or by providing NFS shared directories where the system can drop CSV files (Customer_NFS). These servers shall come with their own protection mechanisms and grant the system access as defined in next table.

NFS sharing to destinations out of back-end LAN shall not be used. Rather use a standard server and configure it as a file repository inside back-end LAN. Allow remote file access with secure standard services such as scp or sftp.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Management_BE	Customer_source	22	TCP	SSHv2	ssh	N
Mediation	Customer_feed	111	TCP	-	portmap	N
Management_BE	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Mediation	Customer_DWH	1521	TCP	-	OracleDBNet8	N
Mediation	Customer_feed	2049	UDP	-	NFS	N

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Acquisition	Customer_TADAPT	9090	TCP	-	MFP.a	TADAPT

Table 10: Feed Ports

Support and troubleshooting workstations

There are two ways to provide support access to servers: either with ssh protocol which is implemented in each of them or by ILO or ILOM access. ILO access is an out of band management board installed in each HP server used by the system. ILOM is an out of band management board installed in Oracle x86 servers as well as ODA and ZFS. This out of band access shall be segregated on maintenance VLAN with highly controlled access because with Web browsers it is possible to open a virtual console and gain full control of the servers. On the other hand this type of access permits to do most maintenance operations from a remote location, including OS fresh installation and server power off/on.

Rather than managing access of a large number of servers it is recommended to add one server to the LAN and use it as a jump-off server. With secure access to this single server, after authentication, it is then possible to open local connections to perform maintenance and investigation when support is needed.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Support_remote	ILO	22	TCP	SSHv2	ssh	HP HW
Support_remote	ILO	80	TCP	-	http (unsecure)	Prefer HTTPS
Support_remote	ILOM	80	TCP	-	http (unsecure)	Prefer HTTPS
Support_remote	TAP	80	TCP	-	http (unsecure)	Prefer HTTPS
Support_remote	ILO	443	TCP/UDP	TLSV1+	https	HP HW
Support_remote	SWITCH	443	TCP/UDP	TLSV1+	https	N
Support_remote	ILO	3389	TCP	TLSV1+	RDP	HP HW
Support_remote	ILO	9300	TCP	TLSV1+	iLO.a	HP HW
Support_remote	ILO	17988	TCP	-	iLO.b	HP HW
Support_remote	ILO	17990	TCP	-	iLO.c	HP HW

Table 11: Support Ports

If you have deployed Oracle Communications Performance Intelligence Center with Oracle x86 Servers, you need to open other ports to allow remote administration and troubleshooting from administrators' PC (for more detailed information

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Support_remote	ILOM	22	TCP	SSHv2	ssh	ORA HW
Support_remote	ILOM	443	TCP/UDP	TLSV1+	https	ORA HW
Support_remote	ILOM	5120	TCP	-	ilom.cd	ORA HW
Support_remote	ILOM	5121	TCP	-	ilom.km	ORA HW
Support_remote	ILOM	5555	TCP	-	ilom.encrypt	ORA HW
Support_remote	ILOM	5556	?	0	WeblogicNodeMgr	ORA

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
					/ilom	HW
Support_remote	ILOM	7578	TCP	-	ilom.video	ORA HW

Table 12: Remote Control Ports

If you use Engineered systems (ODA, ZFS), please refer to the dedicated documentation for each type of appliance and version for additional firewall rules.

Integrated Acquisition Devices

Integrated Acquisition working in promiscuous listen mode on port mirroring or with tapping devices this specific setup is out of scope of firewall rules. In case of Oracle Communications Diameter Signaling Router (DSR) Integrated Acquisition, some web services are accessed to grab configuration information. This connection requires specific ports depending on the interface option, http or https. Please note that connection with Oracle Communications Operations Monitor (OM) uses unciphered ftp, as a consequence this internal interface shall be restricted to a dedicated subnet surrounded by firewall protection and restricted user access.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Acquisition	DSR	443	TCP	TLSv1+	httpd	Y
Mediation	OM	20,21	TCP	no	ftp	Y

Table 13: Integrated Acquisition Ports

Third Party Acquisition Devices

Oracle Communications Performance Intelligence Center can collect data from third party devices. Follow secure setup guidelines provided with these products. Consider their criticality as similar to the network links from where they tap frames. When the device is connected to a probed acquisition server it can be on a dedicated acquisition LAN. When the device interacts directly with a mediation server, then we recommend connecting this device to the back-end LAN.

Client type	Server type	Port	Transport	Secured layer	Protocol	Optional
Support_remote	MicrotelInnovation	22	TCP	SSHv2	ssh	N
Support_remote	MicrotelInnovation	23	TCP	-	telnet	Y
Support_remote	TAP	80	TCP	-	http (unsecure)	Prefer HTTPS
Support_remote	MicrotelInnovation	161	UDP	-	snmp.a	N
Support_remote	NEPTUNE, NEPHUB	22222	TCP	SSHv2	Neptune.ssh	NEPTUNE
Mediation Server	NEPTUNE, NEPHUB	Many, see Astellia Documentation	TCP, UDP			

Table 14: Third Party Ports

Post Installation Configuration

Security configuration changes that must be considered after installation.

Lock root ssh access

It is a good security practice to disallow ssh connection to the super user account "root". Standard servers allow root ssh access by default. Please refer to Linux documentation or Security guide to change this setting.

TPD servers lock root ssh access by default but allow it to be changed with CLI (each parameter producing what is expected):

```
/usr/TKLC/plat/sbin/rootSshLogin --permit
```

```
/usr/TKLC/plat/sbin/rootSshLogin --revoke
```

```
/usr/TKLC/plat/sbin/rootSshLogin --status
```

Note: Be aware that after root ssh login has been revoked, remote access is only possible with other OS users on the server, followed by an **su –** command when need be. An alternative is the ILO access to a virtual console where root access is not locked.

For additional options, e.g. or restoring root access, please refer to

```
man rootSshLogin
```

To get an equivalent setting with Oracle Linux (non Acquisition or Mediation servers), please refer to Oracle Linux Security Guide where you can find instructions.

Change default OS user passwords

Security is most easily broken when a default database server user account still has a default password even after installation. Consider Appendix C with the list of all accounts and change their default passwords.

Install a signed certificate for the web server

By default after installation, Management server has a self-signed certificate for the https protocol. This mode of operation is mentioned as not safe by all modern web browsers and shall not be used in production. Consider acquiring a certificate signed by a third party authority and install this certificate according to detailed steps available in Installation Procedure (Configure Apache HTTPS Certificate).

Enforce password management.

Activate password enforcement verifications, such as password length, history, and complexity. This can be set in Management – Security Application. More information in online documentation of Security Application.

Activate and tune PDU hiding

PDU hiding is a mechanism that restricts access to certain fields of the xDR or of the PDU decoding (PIN codes, private identifiers, passwords) or even full PDU content, depending on each user profile. Administrators and users with "Business manager" role in their profile will be allowed to view values in such fields as well as fine-tune the list of these fields; keep such profiles restricted to people who have adapted level of permission in the company.

Configure session protection

The “session” is a basic object in the product, delimiting permissions. A smart way to keep control of data access is to define a session owner for each of them. Then the session owner can grant permission to another user to access his data

More information in the online guide of Management – Security.

Password handoff

In order to get safe control over passwords, it is strongly recommended to perform a password handoff procedure after consulting team has completed installation and acceptance procedures.

This procedure consists of:

1. Consulting team changes their usual or default passwords to a temporary password agreed with the permanent administrator team on location. Following rules apply:
    a. Use the account list provided in Appendix C to make sure all accesses have been processed. Read note in Appendix C about default values.
    b. UI passwords are centrally managed on the front end web application but Linux and hardware passwords are to be set server by server. However to not generate uncontrolled complexity we recommend using same password for Linux accounts across multiple servers (one for all ‘root’, one for all ‘admusr’, one for all ‘cfguser’, …).
    c. Passwords shall follow local policy for length and complexity (upper case, lower case, digits, symbols).
    d. Perform verification steps to ensure former passwords and default passwords are no more accepted.
2. Permanent administrator team updates temporary passwords to passwords known by their group only. Please follow these guidelines:
    a. Use the account list provided in Appendix C to make sure all accesses have been processed
    b. UI passwords are centrally managed on the front end web application but Linux and hardware passwords are to be server by server. However to not generate uncontrolled complexity we recommend using same password for Linux accounts across multiple servers (one for all ‘root’, one for all ‘admusr’, one for all ‘cfguser’, …).
    c. Be cautious with Linux root passwords as these represent the master key to super user accounts.
    d. Perform verification steps to ensure temporary passwords are no more accepted.

Part 3: Security Features

In this section outline the specific security mechanisms offered by the product.

The Security Model

The security Model based on roles and profiles with one user id and password for each identified application user. Detailed documentation of the security model is provided in the online manual of the Security Application. Only administrators of the Management server are allowed to run Security Application.

Security model of Management server implements all critical mechanisms:

Authentication: each user is prompted for an identifier and password to open a working session. An administrator can set a session timeout timer in Security – Actions – Manage tokens.

Authorization: an authenticated user can only access applications and objects as defined in his user profile by the administrator.

Audit: important steps of user interaction with the system are logged and can be browsed by an administrator in the Audit application.

Configuring and Using Authentication

Authentication is managed inside the web application by an embedded directory server. Security application is available to configure and manage user accounts. This application has an online user manual in PDF format that can be downloaded and printed.

Managing Authentication

Oracle Communications Performance Intelligence Center has a built-in super-user to create and manage other user's accounts. This user's login is TklcSrv. Users created with administrator privilege are granted to create additional users.

Password Policy

Only user TklcSrv in Security application is allowed to set password policy for all application users. There are two levels of password strength:

Default: only checks length

Strong: checks length and complexity (upper/lower case, digits, symbols) and history (not reusing one of last used passwords)

It is also possible to force maximum age, minimum age, grace period and expire warning periods for password changes.

More details are explained in the Security Application online documentation.

Locked accounts

After three failed login attempts, an account is locked. There is no self-service or timeout option, an administrator has to go into Security application and unlock the account. In case the user has lost his password it is possible to reset the password to a known value that will be changed on first login.

Intrusion attempts

Failed login attempts generate an alarm that needs to be cleared in the System Alarms application. This allows detection of intrusion attempts.

Configuring and Using Access Control

The cornerstone of access control in the system is the session. A session is determined by a set of PDU captured on selected links or associations and filtered with locally defined criteria. The system generates xDR based on PDU correlation and stores them in Sessions. The session is a configuration object that has an owner in the security model. So both technical and security criteria define how sessions shall be configured. Session setup will not be described in this document as it is too wide for this context. Usually training sessions are used to become familiar with session configuration.

User access works with profiles, each user gets a profile associated to his login. Before creating users, it is important to prepare the Profiles, each Profile defining an access level on two levels:

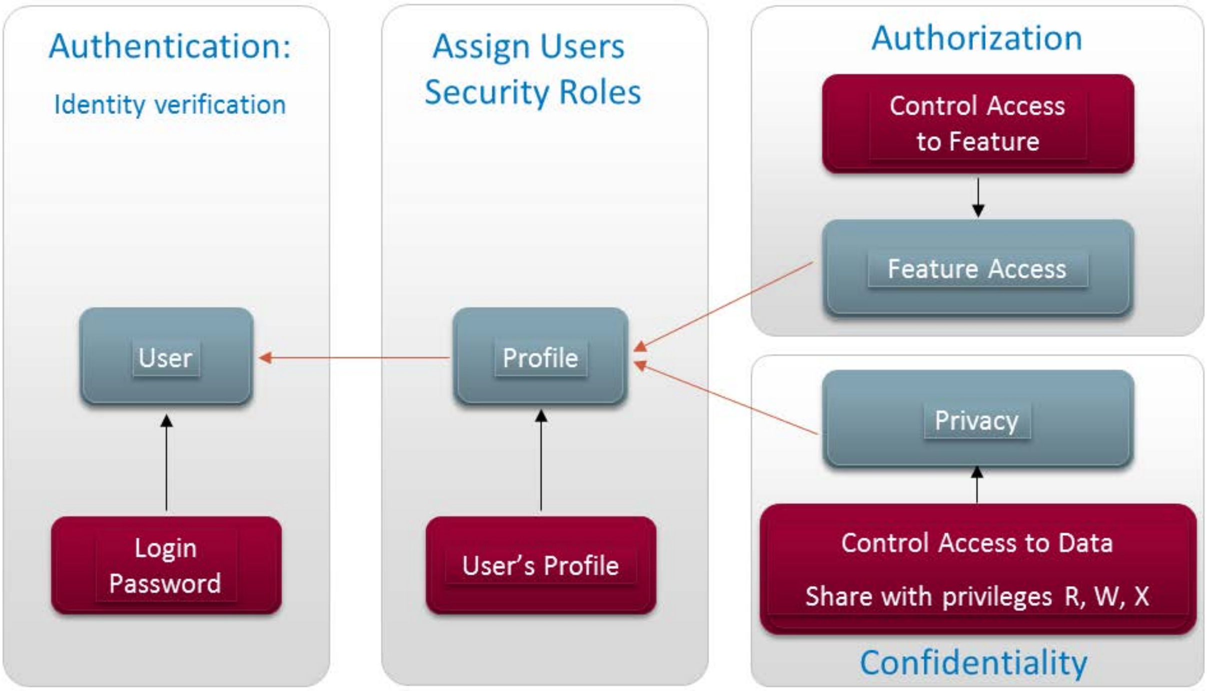

Figure 2: Security Roles Model

Authorization is a mapping towards product features (software modules) that are allowed or not according to the user profile.

Confidentiality is a mapping to user groups that are granted read, write or execute permissions on data objects. Most important data object is the session; but there are secondary data objects such as predefined queries or KPI configurations that follow the same data object permission model.

Part 5: Appendices

Appendix A: Secure Deployment Checklist

The following security checklist includes guidelines that help secure the system:

1. Install only what is required.
    i. On some configurations package bind is provided with the system image although the service named it is not configured and not needed. You can execute `rpm -e bind` to remove the software completely
2. Enforce password management and change all passwords from default values (procedure in Appendix C).
3. Enable session access protection.
4. Practice the principle of least privilege.
    i. Grant necessary privileges only.
5. Enforce access controls effectively and authenticate clients stringently.
6. Restrict network access.
    i. Use a firewall.
    ii. Never poke a hole through a firewall.
    iii. Monitor Audit logs (include who accesses the system)
    iv. Check network IP addresses.
7. Apply all security patches and workarounds.
8. Contact Oracle Security Products if you come across vulnerability in the system

Appendix B: Open Ports

Please check the list provided for each component, Management, Storage, Mediation, Acquisition and for external systems.

Appendix C: Accounts

Table below provides a list of used account names on different servers.

OS accounts with same name have independent passwords on each server of the system. No directory service is used to keep them aligned, however we recommend you, for ease of administration, to always use the same password for a given account name across servers.

Application accounts exist on Management server only.

ILO accounts are used for the out of band management of each server.

LANSwtch accounts apply to Cisco switches

This table does only document accounts used in a rack mount configuration which is hardware baseline for the product.

Area	Identifier	Description	Managmnt	Storage	Mediation	Acquisition	Other
Database	IXP	xDR storage schema owner		√			
Database	NSP	Configuration schema owner	√				
Database	Sys	Database administrator DBA user	√	√			
Database	System	Database administrator DBA user	√	√			
FC switch	admin	Brocade Fiber Channel switch admin					Switch
GRUB	grub	Linux boot configuration	√	√	√	√	
ILO	Administrator	Integrated Lights Out remote console login https, ssh	√	√	√	√	
ILO	tekelec	Integrated Lights Out remote console login https, ssh	√	√	√	√	
LANSwtch	enable	Internal software password to enable changes					Switch
LANSwtch	root	SSH remote access					Switch
LANSwtch	telnet	Telnet, port 23, configuration access					Switch
MRV	tklc	Terminal server for remote console				√	
OS	admusr	SSH connection account when root ssh is revoked	√	√	√	√	
OS	backup	SFTP access to backup files	√				
OS	cfguser	Application runtime owner and admin	√		√	√	
OS	grid	Automatic Storage Management admin		√			
OS	oracle	Database runtime owner and admin	√	√			
OS	platcfg	Platform (TPD) configuration utility dedicated	√	√	√	√	
OS	root	Linux server administrator	√	√	√	√	
OS	syscheck	Platform (TPD) system check utility dedicated	√	√	√	√	
OS	tekelec	Management (NSP) runtime owner and admin	√				
PIC	tekelec	Built-in Application administrator	√				
PIC	TklcSrv	Built-in Application administrator	√				
PIC	<user>	Accounts to be created by an administrator	√				
SNMP	Private	Network management MIB	√	√	√	√	
SNMP	Public	Network management MIB	√	√	√	√	
Weblogic	weblogic	Web server configuration console	√				

Table 15: General Accounts

Next table provides quick reminders for the password change process in each category of passwords. For more detailed instructions please refer to technical documentation of each component.

Area	Identifier(s)	Description
OS	root	To log as root, either use a console (physical or ILO/ILOM) or log with a ssh terminal on admusr and su -. Use command passwd to change active account, use command passwd <account> to force change another account.
Weblogic	weblogic	Log as root on the management server, enter configuration menu : **su – platcfg** > NSP configuration > NSP Password configuration > Weblogic Password Configuration > enter current and new weblogic password and confirm new password.
PIC	TklcSrv	Open Weblogic console > login as weblogic > Security Realms > myrealm > Users and Groups > TklcSrv > Passwords > Enter value New Password and Confirm New Password [Save]
PIC	ALL except TklcSrv	Open Management user interface with an account that has administrative permissions, open Security application, select user to change, click on icon with keys. Enter new password and confirm value for new password.
OS	ALL except root	Log to each server in CLI (either a console or an ssh terminal emulator), use **passwd** command.
Database	application user	NSP for Management server, IXP default for xDR storage serve, customer defined for data feeds. These passwords need to be changed with the wallet wrapping scripts. Refer to appendix E.

Table 16: Password Change Methods

Bold lines, OS root, Weblogic weblogic, PIC TklcSrv, are master accounts. It is mandatory to know actual password for root and weblogic to be able to change it. With master accounts you can force change on other related accounts (root for OS, weblogic for Weblogic, TklcSrv for the system). TklcSrv can have its password forced in the Weblogic console and it allows, in turn, forcing password change or unlocking other user accounts in Security application.

Note: when all administrator accounts of the Management server are locked after too many attempts with wrong password, you will also have to unlock TklcSrv in the weblogic console > Domain Structure > tekelec > Security > Unlock User > TklcSrv > [Save]

Note: As long as passwords remain at their default value at installation or upgrade, you can open a Service Request (SR) on MOS to get assistance on default values because this are not published via other communication sources. Please refer to appendix G for instruction on how to open an SR. Be careful and keep good track of the changed passwords once you apply changes from default values as recommended for a system in production, the SR procedure only works for default values.

Appendix D: root Account Special Care

root, as Linux super user account, is the master key to other access options and needs to be handled with great care. Please be aware that loss of root password will cause service interruption to recover credentials. Take good note of new passwords but store them in a safe place.

This security guide is not a convenient place to keep record of many technical details associated to this operation, therefore we recommend a search in regularly updated technical notes on MOS.

Appendix E: Database Account Special Care (wallets)

Oracle Communications Performance Intelligence Center as an application performs automatic connections to databases, configuration database, DR database, data feed database. To achieve this the system uses stored passwords in a ciphered container using Oracle Wallet.

Please note that for changing a database password you shall not use direct process with SQLPLUS and not standard wallet management procedures either. Instead, a set of scripts is provided with Management server to:

- Prompt for current credentials
- Prompt for new password
- Synchronize the password change process in databases
- Update ciphered passwords in wallets
- Synchronize wallets to other servers for application driven login.

The wallet does not store administrative account (SYS) credentials but only product specific database schema user credentials, which generally are 'NSP' for configuration database and 'IXP' for DR storage database. However there is a prompt for SYS credentials during the password change process, be ready to provide this information. Procedures are documented in Maintenance Guide, chapter 7.

The wallet file itself is protected by a passphrase which has a default initial value but Maintenance Guide provides instructions on how to change this password.

There is a master copy of the wallet on Management server, updated with specific scripts. This master copy is synchronized when needed to Acquisition and Mediation servers: change of password, addition or removal of a server. Storage servers do not need a copy of the wallet. Synchronize wallet files only with scripts installed on Management server to make sure wallet copies go to mandatory locations only based on configuration.

Appendix F: Configure secure https

Oracle Communications Performance Intelligence Center uses an Apache http server as the front-end system. In order to secure your front-end communication you need to deactivate http (port 80) and configure certificates and cipher suites for https (port 443). As a pre-requisite you need to acquire certificate files from a Certificate Authority (CA) that are adapted to your domain. (for testing see note 1)

For a detailed procedure check out Apache HTTP server documentation on the web. Below is a summary of the steps (we recommend keeping untouched copies of edited files):

1. Copy the certificate files "server.key" and "server.crt" in **`/etc/httpd/conf`**
2. Change permission of server.key to 400 using **`chmod 400 /etc/httpd/conf/server.key`**
3. Edit file **`/etc/httpd/conf.d/ssl.conf`**
   a. Uncomment following entry: **`SSLCACerttificateFile (…)`**
   b. Update following entry: **`SSLCipherSuite HIGH:!aNULL:!MD5`**
   c. Update following entry: **`SSLCertificateFile /etc/httpd/conf/server.crt`**
   d. Update following entry: **`SSLCertificateKeyFile /etc/httpd/conf/server.key`**
4. Edit file **`/etc/httpd/conf/httpd.conf`**
   a. Deactivate (# comment) line containing: **`Listen 80`** `(if present and not commented)`
5. Restart service: **`systemctl restart httpd.service`**
6. Check changes with a connection attempt to http://10.31.1.214/nsp expecting a connection timeout

Note1: for test purpose only, you can generate self-signed certificate files for step 1 with the command **openssl req -x509 -sha256 -newkey rsa:2048 -nodes -keyout server.key -out server.crt -days 365** but be prepared to get warnings on your browser.

Appendix G: My Oracle Support (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

7. Select 2 for New Service Request
8. Select 3 for Hardware, Networking and Solaris Operating System Support
9. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

MOS is available 24 hours a day, 7 days a week.