# Introduction

## Purpose

The purpose of this document is to describe the operation and maintenance procedures for BPLRT R160 Video Surveillance System in NSEWL. It provides the necessary knowledge and procedures for operator’s staff to operate and maintain the equipment in BPLRT R160 system.

The present Training Manual comprises of two items which as follow:

Trainees paper Document (Theory part as per O&M Manual, Practical, Demonstration, Hands-on).

Trainer part Presentation (objective of training, duration of lessons and some training aids, materials required e.g., Projector, location etc.). As in the form of slides and to be operated from a PC with Microsoft Power-point software.).   
Both items are to be considered for the related Training Manual and must be reviewed and commented simultaneously.   
The presentation for the training slide may be displayed on any convenient display equipment managed from a PC or laptop.

## Scope of Document

The scope of this document extends to the operations and maintenance staff of the operator (SMRT). This document provides them with sufficient information to have an in-depth understanding of the overall design of the CCTV Switching system and its interfaces with other sub-systems.

This O&M manual allows the operation and maintenance staff to:

Understand the functionalities of the BPLRT R160 system.

Understand the different BPLRT R160 system equipment used in NSEWL.

Identify the cable connections between the XXX system and interfacing systems.

Have the technical knowledge and practical skills to carry out Preventive Maintenance (PM) and Corrective Maintenance (CM).

## Abbreviation

**Description**

A&A

Addition and Alteration

BIOS

Basic Input/Output System

BOCC

Backup Operations Control Centre

BPLRT

Bukit Panjang Light Rapid Transit

CBN

Communications Backbone Network

CCTV

Closed Circuit Television

CER

Communication Equipment Room

FO

Fibre Optic

GUI

Graphical User Interface

iDRAC

Integrated Dell Remote Access Controller

IDS

Intrusion Detection System

IP

Internet Protocol

KVM

Keyboard, Video and Mouse

MSRA

Method Statement & Risk Assessment

MTBF

Mean-Time Between Failure

NMS

Network Management System

NTP

Network Time Protocol

OCC

Operations Control Centre

ODS

Overview Display System

SADP

Search Active Device Protocol

SAT

System Acceptance Test

SLD

Single Line Diagram

TCP/IP

Transmission Control Protocol / Internet Protocol

VDA

Video Distribution Amplifier

VMS

Video Management System

VSS

Video Surveillance System

## Reference Documents

R160 General Specification with Appendices.

R160 Particular Specification with Tables and Schedules.

R160 Design Criteria and Performance Specification with Appendices.

FCDD CCTV Switching System Design (DAR/R160/xxx/yyyyyy)

DAR/R160/BPLRT/3004 - BPLRT CCTV SINGLE LINE DIAGRAM

DAR/R160/BPLRT/2007 - RACK FACE LAYOUT - BPLRT CCTV SYSTEM

DAR/R160/BPLRT/2008 - INTERFACE CONTROL DOCUMENT -R160/C801B

DAR/R160/BPLRT/2009 - BPLRT CENTRAL EQUIPMENT ROOM LAYOUT PLAN

# Safety

All equipment should be installed and serviced ONLY by trained and competent service personnel who are familiar with its operation and hazards involved in the products. Proper attire, handling of wiring, mounting, fusing or other protection and grounding can reduce the chance of electric shocks, fires, or explosions.

All trained and competent service personnel must read all Warnings, Cautions and Notes contained in this document, and must follow all Safety Instructions and Hazard Warnings that are applicable to the area in which the equipment is installed. Do not attempt any maintenance or repairs of the unit until power has been switched off.

Any maintenance services that require height access must comply with MOM requirements. Voltage and current measurements present possibilities of exposure to hazardous voltages and should be performed only by competent service personnel.

Many troubleshooting techniques require measurements with input voltage applied requiring extra precautions to avoid electrical shocks. Use proper safety equipment such as eye protection and gloves when performing electrical measurements.

All competent service personnel must read all Warnings, Cautions and Notes contained in all attached Appendices, and must follow all Safety Instructions and Hazard Warnings that are applicable to the area in which the equipment is installed.

Electrical hazards can cause burns, shocks, and electrocution (death).

Never repair electrical cords or equipment unless qualified and authorized.

Never operate electrical equipment while you are in contact with water.

Have a competent service personnel to inspect electrical equipment that has gotten wet before energizing it.

Always exercise caution when working near electricity.

Assume that all wires are energized at lethal voltages. Never assume that a wire is safe to touch if it is down or appears to be insulated.

## Duties and Responsibilities of Competent Service Personnel

You should not endanger yourself or others working around you through unsafe working practices.

You must adhere to safe work procedures.

You should follow the instructions of your supervisor and ask questions if unsure.

You must report to your supervisor if you spot any unsafe acts or conditions, you are not well or are injured, or you witness any accident or incident.

Avoid sources of ignition such as sparks, flames, or cigarettes.

Avoid wearing open-covered shoes or sandals.

Always work in buddy system when working inside tunnels.

Always maintain good housekeeping.

## Handling of Equipment

Workers must be competent in operating or using machines and equipment.

Only those who are competent should be authorized to operate the equipment.

Techniques on lifting a load safely:

Make sure you are standing directly in front of the load.

Position your feet shoulder width apart.

Keep your back straight.

Squat to the floor by bending your knees.

Hold the load firmly and close to your body.

Stand up slowly using your leg muscles to straighten your legs.

Stand up slowly without jerking your body.

**Note**: General recommendations for lifting:

Maximum weight for men is 25kg

Maximum weight for women is 16kg

## Tools or Test Equipment Safety

Proper usage and storage for tools which are non-powered:

Screwdrivers and pliers.

Wrenches, spanners, multi-meter, and special tool.

Misuse and poor maintenance of hand tools pose many hazards and can cause injuries. Example: using a screwdriver as chisel may cause tip of screwdriver to break off and hit other workers.

# System Overview

The New CCTV Switching System is based on the latest network video technologies, making use of sophisticated computer-controlled systems and high sensitivity color and day/night of existing fixed cameras connected via existing Video Distribution Amplifiers and new Encoders. The video management system combines both latest IP technology and redundancy features to provide powerful performance without compromising on the stability of the system.

The New CCTV Switching System comprises of 16-Channel Encoders, 1-Channel Decoders, 48-ports Network Switches, Network Management Server, Video Management Servers, IO modules, workstations, and workstation monitors. The video output signals of the existing VDA will be connected to 20 new encoders with 20% spare encoder ports that convert 177 existing cameras’ analog video signals to digital video signal into the new CCTV Switching System via the 2x48-ports network switches in the CER.

The 177 camera’s connection to the encoders will be sorted by even and odd VDA ports. This will provide interleaving from the field end cameras to the new CCTV.

The encoders will be connected to the switches alternatingly, in the scenario whereby 1 switch were to fail, there will still be some camera’s stream available for every station.

There will be two sets of new workstations with 22” monitor (2 dedicated control consoles) loaded with Operator Client Software that enables the operators to select video images from cameras from the 13 stations to display on the new ODS in BPLRT OCC.

The new ODS in BPLRT OCC will be installed by C801B. R160-CCTV will interface with the C801B-ODS Datapath controller A & B to display the images from the new CCTV onto the ODS.

The new CCTV will be interfaced with IDS panel via 23 sets of new I/O modules connected to the IDS output cards to receive any IDS alarm activated by the devices from the stations such as Roller Shutters / Intercoms / Emergency Phones / Door contacts, etc. In the event of any triggering, the IDS triggered alarm will automatically display the associated video images to the specific monitors and the alarm texts will simultaneously displayed on monitor of the Operator Client workstation.

The New CCTV Switching System will be connected to new master clock system switch. This will allow the system to synchronize the time via the NTP signal provided.

Retrieval of recording will be done via existing DVR and the recorders are not upgraded by R160

## **System description**

### Video Management System

The solution is based on products from HikVision. The VMS Server is a powerful configuration and management tool that addresses virtually every aspect of the system configuration, management, and monitoring. Besides that, the VMS Server also manages system security for user and device authentication. VMS Servers are designed as a resilience group, which consist of two sets of servers, when one is active, another is on standby.

The VMS Server can be configured to log every event and alarm. It monitors cameras, video storage unit, decoders, and workstations. All network access is via VMS Server.

In summary, the VMS Server will perform the following functions:

Streaming Management

HikCentral Professional supports live view stream from camera. When an operator performs a live view function, it triggers a video stream command and send a streaming request to camera directly. The video stream will push to HikCentral professional and display on the Control Client.

Alarm management

HikCentral Professional supports to configure an alarm rule such as camera offline and generates notification to certain person through HikCentral control clients. When the alarm triggered and push to the operator, the operator can view the alarm related images or related video to check the details of alarm. If the operator acknowledged the alarm, the display color of alarm in alarm center will switch from red to green.

Management logbook

HikCentral Professional has many types of logs to record the activity during operating process and is easy-to-use for maintenance team. HikCentral Professional can also provide server logs file that stored in the VMS server. The log contains information logs, warning logs and error logs.

User management

HikCentral Professional adopts multiple permissions design through roles and user’s configuration. One role can be used by multiple users. For example, HikCentral Professional can be created a normal operator role with limited live view permission and the clients can create serval user account and assigned with normal operator roles. The roles can be assigned with different permissions including area display rule, resource access, and user permissions.

Device state management

HikCentral Professional supports the real-time historical operation and maintenance data statistics dashboard displaying resource online rate, device online rate and video integrity in a period.

Typical Real-time historical operation data statistics dashboard

The VMS server will require 2 LAN cables to be connected to both switches. One LAN port will serve as the management port, the other LAN port will serve as a data traffic port. Management port is used for remote management of Dell hardware server, while the data traffic port is used for VMS software network access.

#### Video Management System Software

VMS will have the following Software and Operating System:

HikCentral Professional Software 2.0

Rose vServer Cluster

Windows Server 2019

HikCentral Professional Web Client offers a graphical user-friendly interface for configuration and management of HikCentral Professional. It offers a user-friendly tool for configuring and managing system security, and user authentication. The storage for alarm log is 60,000,000 and the system log is another 60,000,000. Each log size is approximately 0.01KB per access and the storage period is configurable between 6 months to 3 years. The recommended storage period is 6 months. HikCentral Professional supports audit trail checking, for example user login, user logout, user login failed on web client and HikCentral Professional control client respectively.

The following logs are captured by the audit trails:

Logs are emitted by network devices, operating systems, and applications.

All text lines that include time and name of operations that occur in different environments.

Include messages of several types such as Server logs: informational, warning & error and Device logs: Alarm, Exception, Operation & information

Logs will be generated into files and stored on disk.

The two VMS servers are communicating directly in real-time through LAN and heart-beat detection. If the active VMS server with VMS Central has failed, the standby server will take over and will not affect any data transfer and data store. The VMS servers come with dual power supply unit for redundancy. The hard disks of VMS servers are configured in Raid 1.

VMS can be configured to back up on a periodic basis. The default back up interval is set to be monthly.

Encoders and decoders are backup individually through the web browser. This backup will be done manually. Back up will only be required when there are changes to the configuration.

HikCentral Professional has the same function of Network Management System (NMS) and equipped to provide at least the following functions:

Fault Management

Configuration Management

Performance Management

Security Management

All faults and alarms from the CCTV equipment will be reporting to VMS. The VMS will monitor all active components in the CCTV and provide status alarms of following:

Loss of video signals from encoders,

Failure of any management servers,

Power supply failure,

Loss of time and date synchronisation

Typical VMS Monitoring GUI

Each camera can be configured to display text blocks of up to 3 lines of 20 user-defined alphanumeric characters.

HikCentral Professional is a web-based software which consists of service module and client module. Service module consists of backend application services and database services. For the client module, HikCentral Professional has 2 kinds of clients, Web Client, and Control Client. Web Client can be accessed via browser (Chrome), it's focused on the system configuration and simple applications (Live View, Play Back, Alarm Search, etc.). Whereas Control Client is a desktop application, it's focused on daily operations (Live View, Play Back, Alarm Search, Live Alarm notification, Video Wall Control etc.) without the configuration features.

This VMS provisioned by R160 has the capability to scale upwards and it can manage up to 3000 cameras.

A total of 308 camera platform licenses are provided by R160. Only 177 will be utilized under R160 scope. For future addition of analogue cameras, user may connect it to the system by terminating it to the spare ports in encoders. For additional of IP cameras, it can also be linked to HiKCentral professional and utilize on the 308 cameras license provided. The additional of IP Camera capability will be demonstrated during the FAT.

#### Rose vServer

The VMS is running on two individual physical servers and one Rose vServer fault tolerance (FT) software.

Rose vServer FT software will merge the two physical servers into a single fault tolerant system using virtualization technology. To ensure that the system will not be disrupted due to the loss of data caused by hardware failure, redundant virtual machines will be implemented. Rose vServer Cluster will synchronize the status of redundant VM in real time and form the transparent protection for related applications.

Rose vServer FT Solution Architecture

Features of FT mode:

Prevent system downtime caused by single physical server failure.

Ensure system redundancy and seamless failover.

No manual intervention required; failover is automatic.

With the Rose vServer FT solution implemented, if one of the VMS server were to fail, a seamless failover will occur automatically. Upon the recovery of the faulty server, re-configuration for the Rose vServer software will be required to restore the failover system. The configuration required to set up Rose vServer software will be done on the server’s system BIOS, iDRAC and the Rose software itself.

Typically for a new VMS server replacement, the configuration to set up the Rose vServer software and the time required for synchronization of the two VMS server will take up to a maximum of 8 hours. During synchronization, VMS services on the active server will not be affected.

#### CCTV Client Workstation

The CCTV Client workstation will have the following software and operating system:

HikCentral Professional Control Client Software

Window 10 Pro

SADP software

The HikCentral Professional Control Client will allow operators simultaneously and independently control, select and view live images from any cameras located within BPLRT; and allow automatic sequential viewing of cameras from a multiple combination of selected cameras inputs.

SADP software is used to search for online devices in the same network. It supports viewing the device information, activating the device, editing network parameters, and resetting the device password.

All CCTV workstation facilities are equipped with the necessary hardware, software applications, licenses, and any ancillary and peripheral devices. The HikCentral Professional Control Client shall have at least the following features:

Camera’s selection in full screen format as well as multi-screen format (including quad format and 4 x 4 format),

Search functions based on alarms, camera IDs and date and time range,

Display the assigned camera images in sequence - at least 12 programmable sequence settings.

Typical live viewing format for full screen and multi-screen

All monitors provided for the CCTV workstations will be at least 22” LED illuminated LCD monitor with color graphics with the following features:

Horizontal and vertical viewing angle of more than 160°

Pixel pitch of less than 0.30mm

Resolution of 1920x1080 pixels

Contrast, colour, and brightness adjustment

The refresh rate will be such that flicker and annoying display aberrations are not perceivable to the operator.

#### Tabulation of Degraded Mode

**Event no**

**Event**

Degraded mode operation

**Operation**

[Fail A1]

VMS Server 1 fails

Alarm at VMS and NMS, viewable at Workstation.

VMS Server 2 takes over operation automatically.

No Impact

[Fail A2]

VMS Server 2 fails

Alarm at VMS and NMS,

viewable at Workstation

VMS Server 1 takes over operation automatically.

No Impact

[Fail A3]

Both VMS Servers fails

No alarm from VMS

Alarm at NMS

No CCTV functions available.

The last selected camera stream will remain on the CCTV workstation monitor and ODS.

[Fail B1]

Switch 1 fails

Alarm at NMS

There is impact on event triggering to I/O devices and workstation connected to switch 1.

There is impact on live viewing to cameras linked to encoders that are connected to switch 1.

VMS functions not affected.

[Fail B2]

Switch 2 fails

Alarm at NMS

There is impact on event triggering to I/O devices and workstation connected to switch 2.

There is impact on live viewing to cameras linked to encoders that are connected to switch 2.

VMS functions not affected.

[Fail B3]

Both switch 1 & 2 fails

Alarm at NMS

No CCTV functions available.

#### Tabulation of Operation Impact caused by equipment failure

**S/N**

**Event**

**Operation Impact**

Encoder Failure

No video stream will be available for cameras connected to the failed encoder.

Failure alarm will be reflected at Client Workstation and IDS summary alarm.

IO Module Failure

No event triggering will be available for the dry contacts connected to the failed IO Module.

Failure alarm will be reflected at Client Workstation and IDS summary alarm.

Decoder Failure

The ODS screen that is connected to the failed decoder will be blanked. Operator may re-assign the monitor for the remaining working decoder via the ODS workstation.

Failure alarm will be reflected at Client Workstation and IDS summary alarm.

NMS Server

Failure

No NMS function will be available.

Monitoring of the switches will not be available.

Functionality of the switches will not be affected.

Syslog Server Failure

No Syslog function will be available.

Failure alarm will be reflected onto NMS.

#### Future Storage System

This proposed design can expand its capability to include video recording for the 177 cameras connected to the encoders. To achieve this, another 2 sets of HiKVision Storage Management & Maintenance Server and Video Storage Unit will be required to be installed and linked to the switches provided. The playback and video extraction of recordings can then be completed through the workstation provided in BPLRT OCC.

#### Future External CCTV Streaming

For the streaming of CCTV images to other external areas like LTOC or Transcom. A lease line can be set up by the operator between the BPLRT OCC and the desired location to facilitate this function. The bandwidth of the lease line is dependent on the number of workstations that are put in place. The recommended bandwidth for a full HD IP system stream catered for 3 workstations (Max. of 16 image display for each workstation) is 300Mbps.

## Alarm management

VMS monitors the alarms of CCTV servers, Encoders, IO module & individual cameras connected to the encoders.

Health Monitoring module in built in Hikvision VMS software (HikCentral), it allows the network manager to access all the CCTV devices on the system for configuration and maintenance monitoring purposes. The operation is based on a client/web server architecture which is integrated in HikCentral. Operator would be able check all device online/offline status, alarm information.

Health monitoring provides both near-real-time and history information about the status of the HikCentral VMS software service and added hardware device. It is critical to multiple aspects of operating the servers or devices and is especially important for maintenance. When a device exception occurs, such as device offline, operator can enter this module to check the resource status and find out the abnormal device(s) and view the exception details.

The alarm information received by the HIKCENTRAL Control Client displays. Operator can check the detailed information of the event or alarm, and manage the related information, and so on.

After configuring the required settings on the Web Client and Control Client, the alarm window will open when the corresponding event/alarm is triggered. Operator can view the alarm time, the source device which trigger the alarm, the triggered event, and alarm status, etc.

The list for the different type of alarm provided by the HikCentral Alarm Centre are shown in the below table.

**No:**

**Type of Alarm**

Camera Offline (Individual)

Decoder Offline

Encoder Offline

VMS Server LAN Port Alarm

VMS Server HDD Alarm

VMS Server Offline

VMS Server Fan Alarm

VMS Server PSU Alarm

Clock Sync Loss Alarm

Rack Fan Failure Alarm

IO Module Failure Alarm (Individual)

## Users

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

User permissions can be granted/denied on a per user group basis. Every user belongs to exactly one user group. There is one predefined user group, the Administrator group. This group has full privileges and cannot be restricted. All newly created Operator Groups have no access to Configuration Client by default. But they can be granted this access with different permission levels from read only to nearly full access.

Every VMS user account can be protected with a separate password for identity verification with option to configure expiration time, access period. Identity verification means that the HIKVISION service will allocate a session ID to all request clients and verify the session validity of each request. For the inactive client within 15 minutes, the server will clear the session information. If the client wants to continue the request, it needs to log in to the service again by re-entering password.

The account password information allocated by the platform is required when the client wants to log in to the service. To ensure the system security, the input information is hidden during password input. After the server verified the password, it will allocate an effective session ID to the client.

All devices added to VMS will include with passwords. The passwords of the encoders will be centrally set and managed directly in VMS Web Configuration Client. Batch changing password option is available, providing a fast way of managing devices password.

**No:**

**Type of Users Account**

**Quantity**

Number of Users Created

3000

Number of Roles Created

3000

Concurrent Access of Users via Web/Control Client

100

### VMS User

#### Add Role

Role is a group of platform permissions. You can add roles and assign permissions to roles, so that users can be assigned with different roles to get different permissions.

Note: The platform has predefined two default roles: Administrator and Operator. You can click the role name to view details. The two default roles cannot be edited or deleted.

Administrator

Role that has all permissions of the platform.

Operator

Role that has all permissions for accessing resources and operating the Applications on the Web Client.

In the top left corner of Home page, select **All Modules**, then **General**, then **Account** and **Security**.

Click **Roles** on the left.

Click **Add** to enter Add Role page.

Set the basic information of the role, including role name, effective period, role status, permission schedule template, description, etc.

**Copy From**

Copy all settings from an existing role.

**Effective Period**

Set the time range within which the role takes effect. The role is inactive outside the effective period.

**Permission Schedule Template**

Set the authorized time period when the role's permission is valid. Select **All-day Template**/**Weekday Template**/**Weekend Template** as the permission schedule of the role, or click **Add New** to customize a new permission schedule template.

**Note:**

When role expires or the role's permission is invalid after editing the permission schedule, users assigned with the role will be forced to log out and not able to log in.

The permission schedule's time zone is consistent with that of the platform.

By default, the role will be linked with All-day Template after updating the platform.

The permission schedule also goes for RSM client and OpenSDK client.

Configure permission settings for the role.

**Area Display Rule**

Show or hide specific area(s) for the role. If an area is hidden, the user assigned with the role cannot see and access the area and its resources.

**Resource Access**

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

**Note:**

If you do not check the resources, the resource permission cannot be applied to the role.

**User Permission**

Assign resource permissions, configuration permissions, and operation permissions to the role.

Complete adding the role.

* Click **Add** to add the role and return to the role management page.
* Click **Add and Continue** to save the settings and continue to add another role.

**Optional:**Perform further operations on added roles.

**Edit Role**

Click role name to view and edit role settings.

**Delete Role**

Check a role and click **Delete** to delete the role.

**Inactivate Role**

Check a role and click **Inactivate** to set the role status to **Inactive**.

**Activate Role**

Check an inactive role and click **Activate** to set the role status to **Active**.

**Refresh Role**

Click **Refresh All** to get the latest status of the roles.

**Filter Role**

Click to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

#### Add Normal User

You can add normal users and assign roles to them for accessing the system and assign role to the normal user. Normal users refer to all users except the admin user.

On the top left corner of Home page, select **All Modules**, **General**, **Account and Security**.

Click **Users** on the left.

Click **Add**.

Set basic information for the user.

**User Name**

Can contain letters (a-z, A-Z), digits (0-9), and "-" only.

**Password**

Create an initial password for the user. The user will be asked to change the password when logging in for first time. See [First Time Login](http://enpinfo.hikvision.com/unzip/20220426164607_54506_doc/GUID-FBAD7272-823D-40BC-ADEC-C613EDB86195.html#GUID-FBAD7272-823D-40BC-ADEC-C613EDB86195) for Normal User for details.  
  
Note:  
We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

**Expiry Date**

The date when the user account becomes invalid.

**Email**

The system can notify user by sending an email to the email address. The user can also reset the password via email.

**Note:**

The email address of the admin user can be edited by the user assigned with the role of administrator.

**User Status**

If you select **Inactive**, the user account will be inactivated until you activate it.

**Restrict Concurrent Logins**

To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

Configure permission settings for the user.

**Assign Role**

Select the roles that you want to assign to the user.

**Note:**

If you want to add new roles, click **Add New Role**. See [Add Role](http://enpinfo.hikvision.com/unzip/20220426164607_54506_doc/GUID-6C43765F-0DD8-43CF-ADF0-5918B47787D1.html#GUID-6C43765F-0DD8-43CF-ADF0-5918B47787D1) for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

Do one of the following to complete adding the user.

Click **Add** to add the user and return to the user management page.

Click **Add and Continue** to save the settings and continue to add another user.

**Optional:**Perform further operations on the added normal users.

**Edit User**

Click user name to view and edit user settings.

**Reset Password**

Click user name and click **Reset** to set a new password for the user. Enter a new password and click **Reset**.

**Note:**

The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.

**Delete User**

Select a users and click **Delete** to delete the selected user.

**Force Logout**

Select an online user and click **Force Logout** to log out the online user.

**Inactivate/Activate User**

* + The admin user or user with administrator permission can inactivate or activate a user.
  + Select active users and click **Inactivate/Activate** to inactivate/activate the user.

**Refresh User**

Click **Refresh All** to get the latest status of all users.

**Filter User**

Click Filter button to set conditions and filter the users.

#### Import Domain User

You can batch import the users (including the user name, real name, and email) in the AD domain to the platform and assign roles to the domain users.

**Before you start**

Make sure you have configured active directory settings. See [Set Active Directory](http://enpinfo.hikvision.com/unzip/20220426164607_54506_doc/GUID-2DDD20AB-B910-4AE5-A0CF-9D9B97906B6A.html#GUID-2DDD20AB-B910-4AE5-A0CF-9D9B97906B6A) for details.

**Start**

Click **Users** on the left.

Click **Import Domain Users.**Select an importing mode.

**User**

Import individual users. Select an organization unit and select one or more domain users in this organization unit.

**Group**

Select an organization unit to import all the domain users in this organization unit.

**Security Group**

Import all the domain users in the security group(s). Select an organization unit and select one or more security groups in this organization unit.

Select the user status as **Active** or **Inactive**.

**Optional:**To limit the maximum IP addresses logged in to the platform using the user account, switch on **Restrict Concurrent Logins** and enter the maximum number of concurrent logins.

Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note:  
The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example  
When two users control the PTZ unit at the same time, the user who has the higher PTZ control permission level takes control of the PTZ.

Select the roles that you want to assign to the domain users.  
  
**Note:**

If no role has been added, two default roles are selectable: administrator and operator.

**Administrator**

The role that has all permissions of the HikCentral Professional.

**Operator**

The role that has all permissions of the HikCentral Professional Control Client.

If you want to add new roles, you can click **Add New Role**. See [Add Role](http://enpinfo.hikvision.com/unzip/20220426164607_54506_doc/GUID-6C43765F-0DD8-43CF-ADF0-5918B47787D1.html#GUID-6C43765F-0DD8-43CF-ADF0-5918B47787D1) for details. Click a role on the list and then **View Role Details** to view the Basic Information and Permission Settings of the role.

Complete importing the domain users.

Click **Add** to import the domain users and return to the user management page.

Click **Add and Continue** to save the settings and continue to import other domain users.

**Optional:**After importing the domain user information to the platform, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the platform. If the users are imported by group, it will synchronize the latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).

**Result**

After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client, Control Client, and Mobile Client with their domain accounts and passwords.

#### Change Password of Current User

You can change the password of your currently logged-in user account via Web Client.  
**Steps:**

Move the cursor to the username at the top-right corner of the Web Client.

In the drop-down list, click **Change Password** to open the Change Password panel.

Change Password Panel

Enter the old password and new password and confirm the new password.  
 **CAUTION:**The password strength of the device can be checked by the system. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.Click OK to save changes.

### NMS User

## Network management System

The NMS will be used to monitor the 2 switches newly installed for BPLRT – CCTV. The proposed NMS can be accessed through web browser and can be monitored from the KVM, as well as the CCTV workstation in OCC.

### Alcatel-Lucent OmniVista 2500 NMS

NMS will have the following Software and Operating System:

Omni vista 2500

Windows Server 2019

The NMS shall be equipped to provide at least the following functions:

Fault Management.

Configuration Management.

Performance Management; and

Security Management

The Alcatel-Lucent OmniVista 2500 NMS provides the necessary cohesive management and network-wide visibility increasing IT efficiency and business agility.

The NMS enables operators to easily provision, manage and maintain a Campus Mobile infrastructure with its network elements, alarms, unified access security policies, and virtualization. It also provides advanced network analytics for a full visibility into wired devices.

The key features of the NMS:

**Platform**

Enterprise class, web-based consolidated network management application for network provisioning, troubleshooting, performance analysis and configuration operations for AL-e

OmniSwitches. Unified workflow for network services, resources, and users for wired and wireless infrastructure

**Deployment**

Available as a virtual software appliance for full turnkey operation, supporting leading Hypervisors and operating systems.

High Availability mode for mission critical deployment with Master/Standby operations over Layer 2 and Layer 3 for Wired deployment.

**Dashboard**

Real-time monitoring and analysis of critical network performance indicators through visual widgets for LAN access points.

Full choice of displays, data and other important network and device for wired performances management information, with advanced reporting capabilities.

Typical Dashboard, Key indicators for Faults, Availability and Performance

**Network discovery**

Detailed discovery of Alcatel-Lucent Enterprise OmniSwitches and third-party devices over SNMP v2c/v3

**User interface**

Web-based client, allowing access through any browser, including mobile browsers

User interface follows Web 2.0 principles, responsive web design enabling easy navigation, consistent workflow, and user experience.

## Interface

### Clock

The new CCTV will interface with the existing sub-master clock system. The timing for CCTV equipment will synchronize via the NTP signal provided by the newly installed clock switch, hourly.

All CCTV equipment will be synchronized to the VMS Server. The VMS Servers in BPLRT will synchronize its system time with the Clock System. In the event of failure from the Clock System, the time of VMS Server will run on its own. Once time source is recovered, the VMS Server will try to automatically synchronize with the Clock System.

Connection from VMS server Clock Switch

## Overview Display System

The 22” LCD monitors will be interfaced with the new ODS (by C801B) to display the selected or triggered images. The new CCTV will interface with the new ODS (by C801B) to display the selected or triggered images.

R160 will provide 6 x HDMI output signals to datapath controller through the decoders. Datapath controller A and B will each receive 6 HDMI signals and the data transmitted to controller A and B will be the same. Operators will be able to select their desired image to display on the ODS through the workstation provided.

Video Stream request from Control Client to display onto Wall Monitor

The associated image for event triggering will automatically pop up onto the wall monitor. The alarm acknowledgement, resetting and the audits logs can be monitored through the workstation.

## Intrusion Detection System

The new CCTV shall interface with the IDS to display summary faults alarms. CCTV will trigger the summary alarm for IDS through dry contact at the existing spare ports on the security field panels. The IDS summary triggering will include the list stated in Table 4.

Upon the detection of any VMS alarm, the VMS will output a dry contact through the Adam 6050 Input / Output Module to IDS input card. The dry contact will be set as normally close as per the existing IDS configuration.

Connection from VMS server to IDS input card

## TCP/IP IO Module

The module offers multiple alarm inputs and auxiliary relay outputs. It is used to interface dry contact-based alarm triggers to the CCTV via TCP/IP protocol. When alarm is detected in the end device, the dry contact of the device will be closed to form a close loop between the dry contact and the IO module while triggering the TCP/IO device to send the alarm information to the VMS Server via TCP/IP.

## 1-Channel Video Decoder

The video decoder has equipped with HDMI and composite video output. To display camera video to the AFC 42” monitors in the existing station, the analogue video converted from the decoder will be output from the decoder composite video output via the existing RG6 cable to the existing 42” AFC monitor.   
For the 42” AFC monitors in CCL6 stations and OCC/BOCC, the digital video will be output from the HDMI of the decoder via the HDMI Extender and CAT5e cable to the 42” monitors.  
  
The Decoder will have the following functions:

Decode H.265 at full frame rate

Supports resolutions: CIF, 2CIF, 4CIF

View video from a single or up to four video streams in quad viewing mode

100BaseT Ethernet port

Support HDMI, VGA, and Composite video output

## 16-Channel Video Encoder

The 16-Ch video encoder deliver H.265 video up to 4CIF/25fps (PAL) on all ports. By incorporating H.265 video encoding technology, these devices provide excellent image clarity, with up to 50% reduction in use of network bandwidth and storage. The video encoder digitizes analogue video signals and sends digital video images directly over an IP network to the decoders or video storage unit. It encodes an analogue video into a digital video and enables users to view live and recorded on the CCTV monitor via decoder in stations, depot, OCC and LTOC while saving the video recording into the video storage unit. It also allows authorized viewers from different locations to simultaneously access video images from the same encoder.

The Encoder has equipped with the following functions:

To encode analogue video signal from cameras to the digital video streams,

Provide 16 composite video channels input for 16 unit of cameras.

Adopt H.265 video compression technique

Provide up to 25fps at 4CIF resolutions,

Ability to output dual video streams

Each channel could provide video frame rate up to PAL 25fps.

Bundle with 16 alarm inputs and 4 relay outputs,

1000BaseT Ethernet port

## Gigabit Ethernet Network Switch

The Gigabit Ethernet Network Switch will be in the CE/ISCS Room. The network switch will connect to all Station CCTV and Train borne CCTV network equipment. Inclusive of the VMS Server, VCC, VSU, Encoders, Decoders, IP Cameras, PSCC Switch, PoE Switches, TCCTV Switches, TCCTV Gateways, TCCTV Servers in OCC, Station, and Depot.

## Rack Mounted KVM

A KVM switch (Keyboard, Video Interface, and Mouse) is a hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse. A rack mounted switch with retractable keyboard, mouse and 17-inch LCD monitor will be in the CCTV cabinet in the CE/ISCS room. All the keyboards, mouse, and monitors outputs of all the CCTV servers and playback workstation in the CE/ISCS room will be connected to this KVM switch.

# Operation & Maintenance

## Operation

The New CCTV Switching System comprises of 16-Channel Encoders, 1-Channel Decoders, 48-ports Network Switch, Network Management Server, Video Management Servers, IO modules, workstations, and workstation monitors. The video output signals from the existing VDA will be connected to 20 new encoders with 20% spare encoder ports which convert 177 existing cameras’ analog video signals to digital video signals into the new CCTV System via the 2×48-ports network switches in the CER.   
  
There will be two sets of new workstations with a 22” monitor (2 dedicated control consoles) loaded with Operator Client Software that enables the operators to select video images from the analog cameras from the 13 stations to display on the new Overview Display System (ODS) in BPLRT OCC.  
  
The new Overview Display System (ODS) in BPLRT OCC will be installed by C801B. R160-CCTV will interface with the C801B-ODS Data path controller A & B to display the images from the new CCTV onto the ODS.

The new CCTV will be interfaced with IDS panel via 23 sets of new I/O modules connected to the IDS output cards to receive any IDS alarm activated by the devices from the stations such as Roller Shutters / Intercoms / Emergency Phones / Door contacts, etc. In the event of any triggering, the IDS triggered alarm will automatically display the respective video images to specific video displays and simultaneously, alarm texts will be shown on the monitors of the Operator Client workstation.

The new CCTV Switching System will be connected to the new master clock system switch. to synchronize the time via the NTP signal provided.

Logs are a critical part of any network security implementation and without the central collection and analysis of security and event logs security issues will only be detected after the fact (if at all). Central log collection will be accomplished using the Kiwi Syslog Server or similar. Syslog is a great solution because just about everything on your network uses it and the windows logs too can be forwarded using the forwarder available. All network access is via VMS server. Server log files are stores in VMS server. The first step in monitoring any type of logon attempts is to forward log entries to a central log aggregator.

## Preventive Maintenance

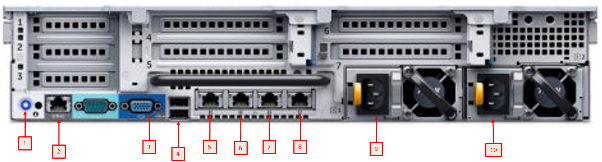
Preventive maintenance refers to regular, routine maintenance conducted to identify any potential faults or malfunction before it occurs. Preventive Maintenance will be conducted on a regular basis for all equipment, logs and file backup, clearance, and functional checks of all IP equipment.

### Hardware Ports Functions and LED Indicators

#### Station/Depot VMS Server (DS-VD22D-B/HW7) (Dell R730)



1



Indicator

Connection

System identification button

To locate the server inside the rack

iDRAC8 Enterprise port

Dedicated management port

Video connector

To connect the KVM cable to the server

USB port

To connect USB device to the server

Ethernet connector 1

To connect to the switch

Ethernet connector 2

To connect to the other server

Ethernet connector 3

To connect to the switch

Ethernet connector 4

Not used in the project

Power supply unit 1

To provide power for the server

Power supply unit 2

To provide power for the server

Diagnostic indicators on the front panel

NOTE: No diagnostic indicators are lit when the system is turned off. To start the system, plug it into a working power source and press the power button.

**ICON**

**DESCRIPTION**

**CONDITION**

**CORRECTIVE ACTION**

Health indicator

The indicator turns solid blue if the system is in good health.

None required.

The indicator flashes amber:

When the system is turned on.

When the system is in standby.

If any error condition exists. For example, a failed fan, PSU, or a hard drive.

Check the System Event Log or system messages for the specific issue.

The POST process is interrupted without any video output due to invalid memory configurations. See the Getting help section.

Hard drive indicator

The indicator flashes amber if there is a hard drive error.

Check the System Event Log to determine the hard drive that has an error. Run the appropriate Online Diagnostics test. Restart the system and run embedded diagnostics (ePSA). If the hard drives are configured in a RAID array, restart the system, and enter the host adapter configuration utility program.

Electrical indicator

The indicator flashes amber if the system experiences an electrical error (for example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator).

Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reseat the PSU. If the problem persists, see the Getting help section.

Temperature indicator

The indicator flashes amber if the system experiences a thermal error (for example, the ambient temperature is out of range or fan failure).

Ensure that none of the following conditions exist:

A cooling fan has been removed or has failed.

System cover, cooling shroud, EMI filler panel, memory module blank, or back filler bracket is removed.

Ambient temperature is too high.

External airflow is obstructed.

See the Getting help section.

Memory indicator

The indicator flashes amber if a memory error occurs.

Check the system event log or system messages for the location of the failed memory. Reseat the memory module. If the problem persists, see the Getting help section.

#### Video Encoder (Hikvision DS-6716HUHI-K)

Indicator

Description

Power

Lights green when the device is powered on.

Status

Lights green when data is being read from or written to HDD.

Tx/Rx

* 1. Does not light when the network is not connected
  2. Blinks in green when the data is transmitting / receiving

3. Blinks at a higher frequency when the data for transmitting /   
receiving is larger

#### Video Decoder (HikVision DS-6901UDI)

LED Indicator & Interface

Description

Power

Power indicator

Link

Network connection indicator

Tx/Rx

Data transmitting/receiving status indicator

HDMI Video Output

HDMI output for decoded video

VGA Video Output

VGA output for decoded video

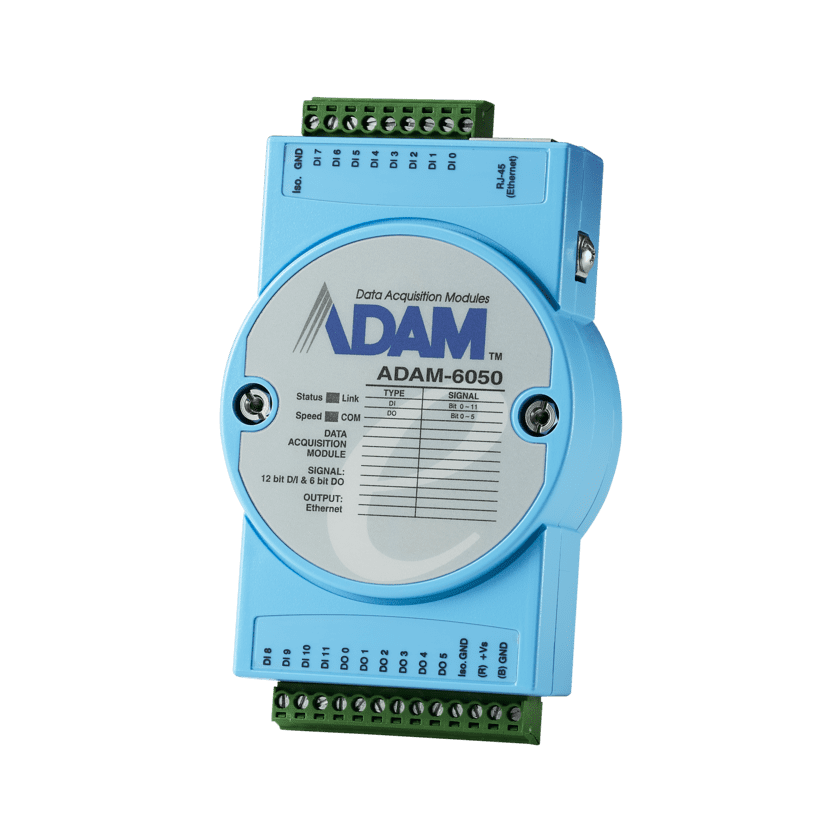
Audio Output

Audio output, 3.5mm connector

Video Output

Video output, BNC connector

#### TCP/IP IO Module (Advantech ADAM-6050)



LED Color Indication

Behavior

Status

Orange (when Status and Link are on at the same time)

Red

Blink

Module is normally running

ON for 30s

When user enable LOCATE function

Link

Green

ON

Ethernet is connected

Speed

Orange (when speed and COM are on at the same time)

Red

ON

Ethernet speed is 100Mbps

COM

Green

Blink

Module is transmitting or receiving data

#### ADAM 6050 TCP/IP I/O module PSD-A40W24

No.

LED Indicator & Interface

Description

DC ON

If green color, PSU is working well

Main Connector

Screw Terminal

Air Cooling

Conventional

Mounting Rail

TS35

Dimensions (W x H x D)

32 x 90.2 x 100 mm

Safety

Audio output, 3.5mm connector

Operating Temperature

-25 ~ 70°C

#### NMS Server (R450)

Corrective Action

Drive indicator

The indicator turns solid amber if there is a drive error.

Check the System Event Log to determine if the drive has an error.

Run the appropriate Online Diagnostics test. Restart the system and run embedded diagnostics (ePSA).

If the drives are configured in a RAID array, restart the system, and enter the host adapter configuration utility program.

Temperature indicator

The indicator turns solid amber if the system experiences a thermal error (for example, the ambient temperature is out of range or there is a fan failure).

Ensure that none of the following conditions exist:

A cooling fan has been removed or has failed.

System cover, air shroud, or back filler bracket has been removed.

Ambient temperature is too high.

External airflow is obstructed.

Electrical indicator

The indicator turns solid amber if the system experiences an electrical error (for example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator).

Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reset the Power Supply Unit.

If the problem persists, see the  
[Getting help](https://www.dell.com/support/manuals/en-sg/poweredge-r450/per450_ism_pub/getting-help?guid=guid-25fb1735-0447-492e-a026-1113ac63ef3f&lang=en-us) section.

Memory indicator

The indicator turns solid amber if a memory error occurs.

Check the System Event Log or system messages for the location of the failed memory. Reseat the memory module.

If the problem persists, see the  
[Getting help](https://www.dell.com/support/manuals/en-sg/poweredge-r450/per450_ism_pub/getting-help?guid=guid-25fb1735-0447-492e-a026-1113ac63ef3f&lang=en-us) section.

PCIe indicator

The indicator turns solid amber if a PCIe card experiences an error.

Restart the system.

Update any required drivers for the PCIe card. Reinstall the card.

If the problem persists, see the  
[Getting help](https://www.dell.com/support/manuals/en-sg/poweredge-r450/per450_ism_pub/getting-help?guid=guid-25fb1735-0447-492e-a026-1113ac63ef3f&lang=en-us) section.

#### CCTV Workstation (Dell Precision 3650 tower)

**POWER BUTTON   
LED STATE**

**DESCRIPTION**

Off

There is in Hibernate or Off state.

Solid White

Working state

Solid Amber

Various sleep states or No POST

Blinking Amber/White

Failure to POST

This platform relies on the Power button LED light blinking in an amber/white pattern to determine a failure as listed in the following table. Note: The blinking patterns consists of two numbers (representing First Group: Amber blinks, Second Group: White blinks).

First Group: The Power button LED light blinks Amber, 1 to 9 times followed by a short pause with LED off for a couple of seconds.

Second Group: The Power button LED light then blinks White, 1 to 9 times, followed by a longer pause before the next cycle starts again after a short interval.

Example: No Memory detected (2,3). Power button LED blinks 2-times in Amber followed by a pause, and then blinks 3-times in White. The Power button LED will pause for few seconds before the next cycle repeats itself again.

#### Alcatel Lucent Omni Switch 6560 -48X4

LED

State

Description

OK

Solid Green

System Diagnostics and AOS bootup OK

Blinking Green

System Diagnostics and AOS in progress (i.e., performing diagnostics or booting)

Solid Amber

System Diagnostics and/or AOS bootup failed.

VC

Solid Green

This unit is the master unit

Solid Amber

This unit is a slave unit

Off

This unit is in shutdown mode or is not part of

PWR

Solid Green

Two power supplies are installed in the chassis and both supplies are functioning normally.

Solid Green

One power supply is installed in the chassis and functioning normally (with the second power supply bay empty)

Solid Amber

Two power supplies are installed in the chassis and one or both supplies has experienced a failure.

Solid Amber

One power supply is installed in the chassis and has experienced a failure (with the second power supply bay empty).

Off

No power supply is present

10/100/100 Port LEDs

Solid Green

Valid port link (non-PoE)

Blinking Green

Valid port link with activity (non-PoE)

Solid Amber

Valid port link (PoE)

Blinking Amber

Valid port link with activity (PoE)

SFP+ Port LEDs

Solid Green

Valid port link

Blinking Green

Valid port link with activity

2.5G Port LEDs

Solid Green (Speed LED 1)

2.5G valid port link

Blinking Green (Speed LED 1)

2.5G valid port link with activity

Solid Amber (Speed LED 1)

100/1000 valid port link

Blinking Amber (Speed LED 1)

100/1000 valid port link with activity

Solid Amber (PoE LED 2)

PoE Enabled

Off (PoE LED 2)

PoE Disabled

## Corrective Maintenance

## Equipment Shutdown/Startup Procedures

#### Shutdown Procedures for VMS

Switch OFF the NMS server.

Switch OFF the secondary VMS server.

Switch OFF the primary VMS server.

Power OFF the Syslog server.

Switch OFF the encoders, decoders, and IO modules.

Finally, switch OFF the switches.

#### Start-up procedures for VMS

Switch ON the switches.

Switch ON the encoders, decoders, IO modules.

Power up the Syslog server.

Power up the primary VMS server.

After the primary VMS server is powered up, power up the secondary VMS server.  
7. Switch ON NMS server.

### Hardware Replacement Procedures

#### Replacing NMS Server

Perform Backup\Restore if an NMS server needs to be replaced. Backups can be used to restore configuration files to the network devices from which they were originally taken. You can also compare Configuration Backup Files on the same device or different devices and view a summary of all stored backups.

##### Performing a Backup

Click on the **Backup button** at the top of the screen to launch the Backup Wizard. Complete the screens as described below to backup one or more network devices. When you have completed all of the screens, click on the Backup button at the bottom of the screen to initiate the backup.

**Backup Method**

Select an option to choose a device selection method:

Backup by Devices - To select specific AOS Devices from a list of discovered devices.

Backup by Maps - To select a map(s) to backup all devices in the map(s). This option is used to backup all devices in the selected map(s). You cannot backup selected devices. To backup select devices, select the Backup by Devices option. Note that if some devices in a map are not on-line, a dialog box will pop up warning you of the condition. Click Yes to continue the backup. Click Cancel to cancel the backup. Also note that if a map contains AOS Devices and Stellar APs, the Stellar APs will not be backed up. Stellar APs can only be backed up by AP Group.

Backup by AP Groups - To backup Stellar AP Series Devices. Stellar AP Series Devices are backed up by AP Group. All of the APs in the group will be backed up. When the backup is complete, the backup files for each AP will appear in the Backup Files List on the Backup Screen.

Click on the **Next** button to go to the Device Selection Screen.

**Device Selection**

The options on this screen will depend on the Backup Method selected above.

Backup by Devices - Select the AOS Device(s) you want to backup and click on the Next button to go to the Configuration Screen.

Backup by Maps - Select the map(s) containing the devices you want to back up. Click on the Next button to go to the Configuration Screen.

Backup by AP Groups - Select the AP Group(s) you want to backup and click on the Next button to go to the Configuration Screen.

**Configuration**

This screen is used to configure the type of backup performed (e.g., Full, Configuration Only,

Images Only) and to schedule regular backups. Backup options (e.g., which directories to

include which files to include) vary according to the backup type. See the applicable section

below for details on each backup type.

**Full Backup**

A Full Backup backs up both configuration files and image files. For AOS Devices, all files in the Certified and Working directories are backed up. This includes all configuration-related files (user credentials, banner, time zone, etc.), and image files. If you are performing a Full Backup, select the folder(s) to be backed up (Certified or All).  
  
*Note: Image files will not be FTPed from a device. OmniVista will only record file*

*version(s). Therefore, before a Restore is to proceed, the required image file set must be*

*stored in the Upgrade Image Repository. If the required images are not in the Repository,*

*they will need to be imported using the Upgrade Image Screen in Resource Manager.*

*Also note that if the image file information retrieved from the device does not contain a file*

*version, the file will be physically copied from the device.*

**Directory**

If you are performing a Full Backup, select the directory(ies)/folders to be backed up.

Certified - Back up files in the Certified Directory.

All - Back up files from the Working, Certified, Switch, and Network Directories

**Include Diagnostic and Dump Files (AOS Devices Only)**

If you are performing a Full Back up on all files, you have the option to include/exclude

Diagnostic and Dump Files. By default, Diagnostic and Dump files are not included in the

backup. To include these files in the backup, set the Include Diagnostic and Dump Files slider to "On".

**Description**

Enter an optional description for the backup.

**Configuration Only Backup**

A Configuration Only Backup backs up all configuration-related files in all directories (including user credentials, banner, time zone, etc.). If are performing a Configuration Only backup, you will not have the option of selecting directories since all configuration-related files in all directories are backed up. However, on AOS Devices you will have the option to

include/exclude Security Files from the backup for security reasons.

**Include Security Files (AOS Devices Only)**

If you are performing a Configuration Only backup, you will not have the option of selecting

directories since all configuration-related files in all directories are backed up. However, on AOS devices you will have the option to exclude Security Files from the backup for security reasons. By default, Security Files are included in the backup. If you do not want to include Security Files in the backup, set the Include Security Files slider to "Off".

**Description**

Enter an optional description for the backup.

**Images Only Backup**

An Images Only Backup backs up image files only. Image files will not be FTPed from a device. OmniVista will only record file version(s). Therefore, before Restore is to proceed, the required image file set must be stored in the Upgrade Image Repository. If the required images are not in the Repository, they will need to be imported using the Upgrade Image Screen in Resource Manager. Note that if the image file information retrieved from the device does not contain a file version, the file will be physically copied from the device.

**Description**

Enter an optional description for the backup.

**Schedule Setting**

Enable the Schedule Setting option and complete the fields as described below to schedule a single or recurring backup. You can click on the View Scheduler button at the top of the

Backup/Restore Screen to view a list of Scheduled Jobs, and to edit a user-configured job.

* Start At - Select the time when you want to begin the scheduled backup (e.g.,

12:00 AM).

* Recurrence Pattern - Select the interval for a recurring backup.
* Daily - Backup will occur on the schedule day at the configured "Start At" time. By

default, the backup will occur every day ("Every 1 Day"). You can customize it by

clicking on the "Every 1 Day" field and entering a number (Range = 1 - 30 days). For

example, you could configure a Daily Backup to occur every 2 days if you want it to

occur every other day. **In our use case, set it to** **30 days.**

* Weekly - Backup will occur once a week on the selected day at the configured "Start

At" time. Select the day of the week on which you want the backup to occur. The

backup will occur every week on that day at the configured "Start At" time. You can

select more than one day to perform weekly backups on multiple days of the week.

* Monthly - Backup will occur monthly on the configured day at the configured "Start

At" time. Select the first radio button to schedule the backup for a specific day of the

month, and for a specific number of months. By default, the backup will occur on the

first day of every month ("Day 1 of every 1 Month"). However, you can customize it.

For example, you could schedule the backup for the 15th day every other month

("Day 15 of every 2 Months").

* End Date - Select "End by" to enter an end date for the backup. Select "No end

date" to continue the backup indefinitely.

**Review**

The Review Screen enables you to review your backup configuration before initiating/scheduling the backup. If necessary, click on the Back button to make changes to the configuration. When you have verified the backup configuration, click on the Backup button to initiate/schedule the backup.

*Note: If the CLI/FTP username and password for a device was not previously*

*defined to OmniVista, you will be prompted to enter them before the backup can*

*proceed.*

**Deleting a Backup**

Select the backup(s) you want to delete and click on the Delete icon. Click OK at the

confirmation prompt.

**Basic Information**

Device Name - The user-configured name of the device.

Device Address - The IP address of the device that was backed up.

Device Type - The device/model type (e.g., OS6860E-24).

Date - The date and time that the backup was initiated.

Backup Type - The type of backup performed. The Backup type can be Full Backup (both configuration files and image files were backed up), Configuration Only (only configuration files were backed up), or Image Only (only image files were backed up).

Version - The software version of the backup files (e.g., 8.4.1.193.R01).

Description - The user-configured description for the backup, if applicable.

**Detailed Information**

Name - The name of the individual file that was backed up and is currently stored on the OmniVista Server.

Directory - The directory where the file was stored on the device (e.g., /flash/certified).

Version - The firmware version of the file.

Description - Alcatel-Lucent Enterprise provided description of the file.

Date - The date the file was loaded into the device.

File Size - The size of the file, in bytes.

File Check Sum - The backup file checksum value.

##### Performing Restore

You can restore a configuration to the device from a previous backup. Note that you can

only restore the configuration to the original device from which the backup was taken.

(Backups cannot be restored to other devices, because doing so would cause

mismatched IP addresses and other network problems.) Select a Backup(s) in the

Backup List and click on the Restore button to bring up the Restore Wizard. Complete

the screens as described below.

**File Selection**

The selected Backup(s) are displayed. Click on a Backup to display a list of backup files

available for the restore. Select the files you want to restore to the device. Repeat for additional devices. Click Next.

**AOS 6x Device(s) Only**

If the selected device(s) is an AOS 6.x Switch, and you selected files only in the Certified

Directory, you have the option of restoring files to the Working Directory or restoring the files to both the Working and Certified Directories. Select the Restore to Working Directory or

Restore to Working & Certified Directory radio button to specify the directory(ies) to which

you want the backup restored. If you select files in only the Working Directory or in both the

Certified and Working Directories, you will not have this option. The files will be restored to their respective directories. Also note that this option is not available for AOS 7.x or 8.x Switches.

**Configuration**

For AOS Devices, select the options to be taken if the following changes are detected on the

device:

Continue to restore when chassis has changed - Select this option if you want

to continue the restore even if it is found that the chassis contents, or the chassis

type, has changed since the backup. If you do not enable this checkbox, the restore

will not take place if the chassis has changed.

Continue to restore when detecting new image files - Select this option if you

want to continue the restore even if it is found that a new image file resides on the

device (i.e., a file that was not previously backed up). If you do not enable this

checkbox, the restore will not take place if a new image file is found on the device.

Click on the Restore button then click Yes at the Confirmation Prompt to initiate the restore.

When the restore has successfully completed, click on the Go to Topology to Reboot Device

link. The Topology application will open with the device(s) highlighted. Click on Reboot in the

Device Actions area to reboot the device(s) to load the restored configuration into flash memory.

Note: You must reboot the device(s) to complete the restore operation.

**Compare**

The Resource Manager Compare Screen enables you to compare Configuration Backup Files on the same device or different devices using a "Diff" Utility to view any differences between the files on a line for line basis. You can compare files on different devices or compare files on the same device. You can also use the utility to compare text files on the local file system.

**Selecting Files**

The File Diff Screen is used to select the files you want to compare. To compare backup files

from different devices or backups from the same device, select "Backup File" from the Select

From File drop-down menu on the left side of the screen. Click on the Browse button to bring up a list of current backups. Select a backup to bring up a list of files contained in the backup. Select the file you want to compare and click OK. Repeat the steps to select a backup file on the right side of the screen. When you have selected both files, click on the Compare button. The file comparison is displayed in the File Diff Window.

Note: To compare text files on the local file system, select "Local" from the from the

Select From File drop-down menu. Click on the Browse button and browse to the

files on the local system.

**Comparing Files**

The File Diff Window displays the files side-by-side with all of the differences highlighted

(Changed, Inserted, Deleted). You can use the Arrow keys at the top of the screen on the right side of the window to jump to each change; or you can select a specific change from the Select to Jump drop-down menu. You can also use the scroll bars to scroll through the documents and view changes.

**Summary View**

The Resource Manager Summary View Screen displays a status summary of all

backup/restore/upgrade operations saved on the OmniVista Cirrus Server. By default, all

Backup/Restore/Upgrade operations are displayed. However, you can use the ""View Criteria" function to customize the display. Click on the "View Criteria" drop-down and select filters as described below. When you have selected all of your filters, click on the X in the upper-right corner of the window to close the window and view the filtered display.

Select Devices

All Devices - Displays information for all managed devices.

By Using Switch Picker - Click on the EDIT button to bring up a switch picker to

select devices. Click OK to return to the Summary View Screen.

By Using Topology - Click on the EDIT button to bring up the Topology application

to select devices. Click OK to return to the Summary View Screen.

By Using Quick Select - Click on the EDIT button and select a device(s) from the

drop down.

Type - Select the type of operation(s) you want to view (Backup/Restore/Upgrade)

Status - Select the status of the operation(s) you want to view (Success/Fail/All)

At any time, you can return to the default view by clicking on the Reset button next to the View Criteria to remove all filters.

**Summary View Table**

**Summary Type** - The type of operation (Backup/Restore/Upgrade).

**Device Address** - The IP address of the device.

**Last Attempt Date** - The date and time that the operation was initiated.

**Last Successful Date** - The date and time that the operation completed.

**Attempt Type** - The type of operation performed (e.g., Full Backup).

**Last Attempt Status** - The operation status (e.g., Success/Fail).

**Description** - The user-configured description for the operation, if applicable.

**Message** - Indicates whether or not the operation was successful (Back up Successfully/Finished Restore Configuration) or failed. If “failed” additional

information is provided.

#### Replacing VMS Server

##### Backup and Restore HikCentral

1. Run the installation file of HikCentral.
2. Click Next.

Select Custom and click Next.

Select “HikCentral Video Surveillance Management Server and click Next.

Click Next.

Click Next.

Select “Mirror Hot Spare” mode and click Install.

Once installation is successfully done, uncheck the box to run web client and click Finish.

Open Services.

Find HikCentral WDS Service and start the service.

At desktop, right click HikCentral Service Manager.

Wait for all the servers to start.

After all the services started, close HikCentral Service Manager.

Open Services and stop HikCentral WDS Service manually.

###### **Backup System Data**

For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, face comparison data, card swiping data, maintenance data, etc.

**Note:**

The backups are stored in the SYS server. You can edit the saving path only on the Web Client running on the SYS server.

In the top right of the client, click **Maintenance and Management** > **Back Up and Restore System Data**.

Select the **Back Up** tab.

In **Type**, select the system data that you want to back up.

**Configured Data**

Data configured via the Web Client, including resources, user permissions, etc. It is selected by default.

**Configured Pictures**

Pictures uploaded when configuring maps, persons, vehicles, etc.

**Maintenance Data**

Maintenance data includes received events/alarms, attendance records, visitor data, etc.

**Note:**

* + Person access records are the access records on the card readers of doors with credentials.
  + Device recorded data includes the data recorded by the access control devices, elevator control devices, video intercom devices and alarm inputs of these devices, and other records except access records on the doors.

Set a backup schedule to run backup regularly.

In **How Often**, select the frequency to back up the system data.

In **Which Day** and **When**, specify which time to back up.

Save the settings.

Click **Save** to save the backup schedule.

Click **Save and Back Up Now** if you need to back up the system data immediately.

###### **Restore System Data**

When an exception occurs, you can restore the system data if you have backed up system data before.

Make sure you have backed up system data. Refer to [Set System Data Backup](http://enpinfo.hikvision.com/unzip/20220426164607_54506_doc/GUID-1AF31681-DD4C-4819-B85A-74A0178F87E8.html#GUID-1AF31681-DD4C-4819-B85A-74A0178F87E8) for details.

**Note:**

System data recovery will restore the system to an earlier state, and thus the data added after backup date will be lost.

**Steps:**

In the top right of the client, click **Maintenance and Management** > **Back Up and Restore System Data**.

Select the **Restore** tab.

Select a backup file to be restored.

Click **Restore** to confirm the system data recovery.

You can export and save configuration data to local disk, including remote site configurations, recording settings and resource configurations.

In the top right of the client, click **Maintenance and Management** > **Export Configuration Data**.

Select the configuration data types that you want to export.

Click **Export** to download the data to the local PC.

**Note:** The configuration data file is in CSV format.

##### Installing Rose vServer

Select NETWORK and open  
  
The configuration parameters are as shown in the figure below. After the configuration is complete, click Return.  
Configure user information, root is used to log in to the server management interface.

**Enable Hyper-Threading**

After completing the above operations, return to save and return to the system.  
  
**Raid reconstruction**  
After completing the above operations, return to save and return to the system settings interface, enter device settings.  
Enter the disk configuration management, clear the original disk data and information.

After clearing, create a virtual disk and create at least two logical disks, one for installing the system (100GB is recommended) and one for storing data (the size can be adjusted according to the actual application)  
  
Select physical disks. At least two identical disks are required to create Raid1. One disk for Raid0 can also be created. Raid1 and Raid0 are created in the same way, but the number of physical disks are different. The following steps create **Raid1** as an example.  
  
Click to create virtual machine.   
  
After the system disk is created, select the remaining capacity to create a data disk.

**Select Boot Device**

The above section completes the Raid construction, select the OS disk just created as the boot device, and return to the disk configuration main menu interface.  
  
**Rose vServer system deployment**

Use the server management address configured above to log in and enter the virtual console  
  
Upload the CD image file to complete the installation of the system. The installation method of the two servers is the same.  
  
Select the local Rose vServer CD image file.  
  
Choose to boot from a virtual imaage file.

Check the information of the two virtual disks created before, enter to go to the next step.  
  
  
After entering the password, TAB to select OK to go to the next step. After naming, TAB select OK, press Enter.  
  
Select the gigabit port as the management address of the system, the 10 Gigabit port below is used for data synchronization, do not select it, TAB select OK to next step.

After the installation is complete, the system will restart automatically. You can log in as root user. The password is filled in by the installation system.  
  
Deploy the vServer OS as shown in previous steps on the second server. After the vServer OS is successfully installed on both servers, the vServer Cluster solution can be deployed on each vServer host, but the vServer host is still running as a single node. The two independent vServer hosts need to be created as one through the vServer Cluster Client vServer cluster.  
  
**Rose vServer Cluster Virtualization Cluster Creation**After the vServer OS and the vServer Cluster solution are deployed on two servers, the vServer hosts do not automatically form a cluster, and the two vServer hosts need to be formed into a virtualized cluster through the vServer Cluster Client.  
  
**Log in to the vServer host using the vServer Cluster Client**  
  
After the system is installed, log in to any rose platform, such as 10.41.8.92, the initial login information is admin/admin after logging in, you will be prompted to update the password and log in again.

**Licensing of vServer Hosts**Before running virtual machines on a vServer, the vServer host must be licensed. The vServer hosts in the vServer Cluster use independent licensing, and each vServer host must apply for and assign a license separately.  
  
The vServer Cluster Client navigates to the licensing page via the left navigation bar, Settings, then Product Licensing. After applying for authorization through the application ID, assign licenses to the corresponding hosts respectively.

To set up License key, go to Settings, then Product Authorization. Enter the path of the file and click Open.

The below image shows the successful result of assigning the license key.

**Creating a Cluster Using the vServer Cluster Client**

ClickCreate Cluster (VMS1) in the Dashboard.  
  
Create a Network for cluster nodes

Select the previous Gigabit Ethernet port for the network card and keep the same IP address.  
  
Then add a disaster recovery network to the node and use the previous 10G network card.

Add a cluster node, that is, we will add the second host. Configure the node network similar to the first host configuration.

After the node network configuration is complete, click Next.  
  
Select the heartbeat network for the cluster, click Next.  
Configure management network for the cluster, ping an address that cannot be reached on the same network segment, then select the previously configured service network, and click Next.

The management network is a highly available resource. After the cluster is successfully created, the vServer Cluster Service will manage the network to failover. After the cluster is created, the vServer cluster client can log into the vServer through the management network cluster to manage the cluster.  
  
**Create a highly available virtual machine**

In a vServer cluster, a virtual machine can be created as a high-availability resource. The high-availability virtual machine has a consistent static instance on all vServer hosts and is aggregated into a single instance on the virtual server formed by the vServer cluster. High-availability virtual machines implement real-time data replication between vServer hosts through vServer Replication Service to ensure data consistency and integrity. The high-availability virtual machine dynamically selects the master node according to the configured first node or load policy.

When the master node has a hardware and software failure that causes the virtual machine to run abnormally, the vServer Cluster Service will fail over the virtual machine to another available vServer host through the policy. Nodes to reduce business downtime caused by virtual machine failures to achieve maximum availability of virtual machines.  
  
Log in to the cluster management address **192.168.16.13** configured before and create a virtual machine. The login information is consistent with the single machine vServer Cluster Client that created the cluster.  
  
After logging in, upload the local virtual machine image file (Look for file extensions with .iso), and select any node server to upload.  
  
Click to create a virtual machine and follow the steps below to complete the creation. **Windows System Installation**Followthe steps to complete the creation of the virtual machine. The following are the installation steps for the Windows System. Firstly, find the Virtual Machine you had just created and start it.   
  
After the system is installed, install the guest tool. Send the key value to log in to the system to install the guest tool. After the system is installed, install the guest tool.

**System Configuration**

Complete the basic system configuration such as network and remote configuration and close firewall.  
  
At present there is only C drive in the system. Before installing the HCP platform, it is recommended to separate the disk of the installation platform from the C drive. Open the CMD and enter diskmgmt.msc and press enter.

After entering Disk management, select C drive, right click the following area and compress.  
After the platform is installed and activated, you can check which server node the service is running on the Rose vServer management platform.  
Click transfer as shown below to achieve manual switching.  
  
After the simulated downtime is recovered, you can view the data verification synchronization progress on the interface shown in the figure below.

The platform function is normal during the switching process. The effect of logging in to

the platform is as follows, and the preview playback has no obvious lag.  
  
**Setting Date and Time**To set date and time, go to settings, click Date and Time. Click Edit settings.  
  
Enter as shown in the screen below.  
  
The NTP server IP address is 192.168.10.5, ffee::123

##### Changing out of faulty VMS Server

Switch off the power of the faulty VMS Server.

Remove the cables, dongle from the faulty VMS Server and remove the VMS Server.

Install the new VMS Server and connect back the cables and dongle.

Power on the new VMS Server.

In rose Vserver, select the faulty server and right click Replace.

Click Next.

Key in the IP address. Click Next.

Key in the username and password as per below.

Username: admin

Password: admin

Click Confirm.

Select all and click Delete.

Click Add to add the IP address of the 2 servers.

Click Next.

Click Finish.

Select the existing server, in the right column, right click on the NIC card and select Properties.

To check the NIC card for the new server.

Click on Confirm, the error in the new server icon will disappear.

Select the old server and right click and select Delete to remove the server.

Click on Confirm.

Add back the 2 servers. On left side, right click and select connect. Key in either of the IP address.

Click Connect.

Click Confirm.

Log in to the servers.

#### Configuring of Hikvision equipment (Encoders and Decoders)

For new decoders and encoders, it is required to activate the device first by setting a strong password before the usage. There is 2 ways to configure, i.e., by SADP software and web browser.

For the decoder, the default user name is *admin,* and the default IP address is 192.0.0.64.

SADP software is used for detecting and activating the online device and resetting the password.  
  
**Installing SADP**   
  
Click the checkbox agreeing to the license agreements.  
  
Select English language.  
  
Enter the path of the installation folder.  
Installation completed successfully.

Power up the device.

Connect the laptop to the device with LAN cable.

Open the SADP Tool to search the online device.

Select the inactive device from the device list once it appears. Click on refresh or try to close on open the program to detect the device.

Used the password used in the faulty device and input it in the New Password box and Confirm Password box.

Click **Activate** to activate the device.

Change the device IP address to the same IP address as the faulty device.

Input the password and click **Modify** button to activate the IP address modification.

To activate the device via web browser:

Power up the device.

Connect the laptop to the device with LAN cable.

Open Internet Explorer.

Input the default IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Create the password and input it into the password field.

Confirm the password.

Click OK to save the password and enter the page.

Click **Configuration > Network > TCP/IP** to enter the general network settings interface.

Set the network as per the faulty device.

Click Power up the device.

Connect the laptop to the device with LAN cable.

Click **Save** to save the settings.

#### Replacing Decoder

Configure the new decoder with the same IP address used for the faulty decoder as per Appendix G.

Open Internet Explorer.

Input the decoder IP address into the address bar of the web browser.

Key in username and password.

In the web page, click **Configuration>Maintenance>Upgrade & Maintenance** to import the configuration file.

Under the heading of Import Config. File, click “Browse” to select the configuration file.

Click “Import”.

A pop-up box will appear. Click “Ok”.

Wait for 2 to 3 minutes for the decoder to reboot.

In the web page, click **Configuration > System Settings > Time Settings** to enter the following interface:

Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore

Check NTP.

Server Address: **192.168.10.3**

NTP Port: **123**

Switch off the power of the faulty decoder.

Remove the cables from the faulty decoder and removed the decoder.

Install the new decoder and connect back the cables.

Power on the new decoder.

Check that image can be pulled to the monitor and the alarm at Alarm Center turns green. If successfully done, it means the decoder is working in the system.

##### Importing Configuration Files

The configuration files of the device can be imported from the local device, which maintains

convenient parameters configuration.

Step 1: Enter the parameters import interface.

Import Configuration File

Step 2: Click **Browse** to select the file from the local directory and then click the **Import** button to import a configuration file. Click **Device Parameters** to export parameters.

##### Exporting Configuration File

The configuration files of the device can be exported to the local device, which maintains

convenient parameters configuration.

Step 1: Enter the parameters export interface.

Export Configuration File

Step 2: Click **Device Parameters** to export parameters.

##### Adding decoder device

#### Replacing Encoder

Configure the new encoder with the same IP address used for the faulty encoder as per Appendix G.

Open Internet Explorer or Chrome.

Input the encoder IP address into the address bar of the web browser.

Key in the username and password.

In the web page, click **Configuration>Maintenance>Upgrade & Maintenance**.

At the below of the webpage will have a pop up. Click “Allow”.

Under the heading of Import Config. File, click “Browse” to select the configuration file.

Click “Import”.

A pop-up box appears to input the password of configuration file.

Switch off the power of the faulty encoder.

Remove the cables from the faulty encoder and remove the encoder.

Install the new encoder and connect back the cables.

Power on the new encoder.

Log into the VMS Server.

Open Internet Explorer.

Input the encoder IP address into the address bar of the web browser.

Key in the user name and password.

Go to **Configuration>System>System Settings>Basic** Information and copy the serial number of the encoder.

Input the VMS Server IP address into the address bar of the web browser.

Key in the user name and password.

Click **Physical View > Encoding Device**.

Select the offline Encoder with a red “!”.

Edit the Serial No. to the new serial number of the new encoder.

Click **Save**.

Check that cameras connecting to the encoder can be viewed in Control Client, the alarm at Alarm Center turns green. If successfully done, it means the encoder is working in the system.

##### Importing/Exporting Configuration File

**Import configuration files**

The device configuration files can be exported to a local device for backup; and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

**Before You Start**

Connect a storage device to your device. To import the configuration file, the storage device must contain the file.

Go to **Maintenance** then, Import**/Export**.

Export or import the device configuration files.

Click export to export configuration files to the selected local backup device.

To import a configuration file, select the file from the selected backup device and click

Import.

Note: After having finished importing configuration files, the device will reboot automatically.

Under the heading of Import Config. File, click “Browse” to select the configuration file.

Graphical user interface, application

Description automatically generated

Click “Import”.

A pop-up box will appear. Click “Ok”.

Wait for 2 to 3 minutes for the decoder to reboot.

In the web page, click **Configuration > System Settings > Time Settings** to enter the following interface:

Time Zone: (GMT+08:00) Beijing, Urumqi, Singapore

Check NTP.

Server Address: 176.xx.56.115

NTP Port: 123

Switch off the power of the faulty decoder.

Remove the cables from the faulty decoder and removed the decoder.

Install the new decoder and connect back the cables.

Power on the new decoder.

Check that image can be pulled to the monitor and the alarm at Alarm Center turns green. If successfully done, it means the decoder is working in the system.

**Export configuration files**

Configure the new decoder with the same IP address used for the faulty decoder as per Appendix G.

Open Internet Explorer.

Input the decoder IP address into the address bar of the web browser.

Key in username and password.

In the web page, click **Configuration>Maintenance>Upgrade & Maintenance** to export the configuration file.

##### Adding an Encoding device

The following images provides a quick summary of how to add an encoding device.

#### Replacing TCP/IP IO Module

Once an ADAM-6000 module has been connected to the host PC and you have

searched for it, you will find it listed in the Module Tree Display Area under the Ether-

net category. Select the Ethernet category on the Module Tree Display Area and click

the Search Modules icon on the Toolbar. Adam/Apax .NET Utility will then

search for all ADAM-6000 modules on the Ethernet network. If this is the first time

you have connected the module; its IP will be 10.0.0.1 by default and it will appear

under Others in the Module Tree Display Area.

**Exporting ADAM module configuration file**

Under the Firmware tab, you may find the **File Export Panel** where you can export an ADAM module configuration file. Click **Save As…** and choose the destination file path. Then, click **Upload** to save the configuration file.

Switch off the power of the faulty IO Module at the Rack.

Remove the two connectors and LAN cable from the faulty IO Module and removed the module.

Install the new IO Module and connect back the two connectors.

Power on the IO Module at the Rack.

Connect the Laptop to the IO Module with LAN cable.

Open Adam/Apax .NET Utility.

The Application window will open.

Select the Ethernet category on the Module Tree Display Area, right click and click the Search Device.

Select the newly discovered device and go to network Tab. Select Static for IP Mode. Key in IP address, Subnet and Default Gateway then click Apply.  
  
Note:

You need to change the IP address of the ADAM-6000 module so that it is the same

subnet as the host PC. Enter the correct IP address, subnet address, and default

gateway on the Status Display Area and then click **Apply Change**. A dialog box will

appear asking you to enter the password. The default password of ADAM-6000 mod-

ules is "00000000" (without quotation marks). After you have entered the correct

password, the ADAM-6000 module will be under IP of your host PC. Note that you

can change the password later.

A dialog box will appear to enter the password. The default password of is "00000000" (without quotation marks). The IO module will be updated with the IP after the correct password is keyed.

Disconnect the maintenance laptop and connect the LAN cable from Ethernet switch to the IO Module.

Trigger one of the Event that belongs to the IO Module and verify the Event can be triggered.

If the event is triggered, the new IO module is working and connected to system.

Under the Firmware tab, you may find the **File Import Panel** where you can import an ADAM module configuration file. Click **Browse…** and choose the file path. Then, click **Download** to import the configuration file. The below images show the steps as mentioned.

#### Replacing TCP/IP IO Module PSU

Switch off the power of the faulty PSU at the Rack.

Remove the incoming power cables and outgoing power cables

Pull down the latch located below and lift the PSU.

To install new PSU, Tilt the unit slightly rearwards (1). Fit the unit over top hat rail (2). Slide it downward until it hits the stop (3). Press against the bottom for locking (4).

Reconnect back the cables.

Switch on the power at the rack.

#### Replacing CCTV Workstation

Switch off the power of the faulty Playback Workstation.

Remove the incoming cables.

Install the new Playback Workstation.

Plug back the cables.

Power on the new Playback Workstation.

#### Replacing Alcatel Switch 6560

##### Performing Backup

Copy **vcboot.cfg (**configuration file) and **vcsetup.cfg** (virtual chassis configuration file) from the switch to USB or FTP/SCP, under directory /flash/working.

If you have customized banner in the switch, you can also copy the **pre\_banner.txt** to USB or FTP/SCP under director /flash/switch.

##### Performing Restore

Similar to backing up the configuration file, you just must copy in the vcboot.cfg & vcsetup.cfg to the same folder /flash/working.

If you have pre\_banner.txt, copy back into the switch under the folder /flash/switch.

Once it’s done, reboot the switch by typing the below command:

**reload from working no rollback-timeout**

After reboot, check the configuration is there and save and sync the configuration by typing the below command:

**write memory flash-synchro**

#### Replacing Rack Fan

Procedure for replacement of Rack Fan

The fan tray should be always in the proper locking position.

Switch off the fan power before taking out the fan tray.

To lift the latches

Turn the latches to anti-clockwise for unlocking.

Unlock the two latches and hold the fan tray

Pull out the fan tray and hold tight

Lift up and disengaged the fan tray from the rear door

Insert the new fan tray, the slot hole at the bottom of the fan tray must seat properly on the fan tray chassis.

Now, push in the fan tray.

The latches lock to the keeper then turn the latch clockwise for locking.

Flip down the latches.

\*Warning Please **DO NOT** leave the fan tray in unlock position without people holding it. This is unjustified and dangerous action.

## Operation

### How to use HikCentral Control Client

This is the welcome screen when you login for the first time.

#### First Time Login

When normal user (except admin user) logs in to the system for the first time, he/she should change the initial password and set a new password for login.

Steps:

Double-click the icon as shown in the above desktop to run the Control Client.

Select Normal Login tab on the bottom.

Enter the username and password set by the administrator and click Login to continue.

If the above error shows in your screen, set a new password and confirm the password. Click Login to change the password.   
Note: The password strength of the device is checked by the system. Use a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters.

For subsequential logins, follow steps 1 to 4.

#### Control Client GUI

Monitoring

To show live and recorded images

Alarm Centre

To display the alarms

Alarm & Event Search

To search for alarm history

Health Monitoring

To get the status of all the equipment

Audit Trail

To search for logs

User

To change password or switch user

Smart Wall

To display the decoders output, drag and drop images to the monitors

Download Centre

To view the files downloaded

VSPlayer

To open VSPlayer to play the downloaded videos

Synchronisation

To synchronise VMS configuration. Whenever there are changes inside the web client with the control client open, there will be a red dot. Click for synchronisation.

#### Monitoring page

The monitoring page shows a list of cameras connected to encoders and decoders. Double click the items as highlighted inside of the red rectangle or click the right arrow to list down the cameras.

##### Window Division

Windows division can be selected by clicking at the top right of the screen.

Our recommendation will be to select 1, 4, 9 and 16. Higher numbers might cause the images to display at a slower frame rate.

The user can select the given options for window divisions and the control client will allocate them accordingly.

##### Live View

Select “Live View” located in the top center bar.

To view the live view of the camera, the user can either double click on the camera name or drag the camera label to the display window.

The user can select to “Play in Batch” or “Single-Screen Auto-switch”. To view all images at one go, select “Play in Batch”. To display one by one in sequence, select “Single-Screen Auto-switch”.

##### Save custom configuration

In the View mode, user can easily go to their previous view if the view was saved earlier.

Once the images are displayed in the window, click on the save icon on the top toolbar.  
Save the view group and select either *public view* or *private view*. Click OK.

Once the view is saved, go to the Smart Wall and the user will be able to find the view saved from the previous steps. Here *SSH* is the name given for the view saved earlier

##### Capture Pictures

Click Monitoring. The live view or playback page will display according to previous operations shown earlier. Move the cursor to one of live view display windows to show the toolbar. Click on the camera icon in the toolbar of the display window to capture the picture. The captured picture will be saved automatically and a dialog with the option of saving will open.

#### Alarm Centre

Operators will use this function to monitor the alarms generated. Green represents the alarm normalised. Red represents the active alarms. The start and stop time will inform operator when did the alarm start and when was it resolved. The following 2 screenshots will demonstrate the functions.

#### User

Operator can switch user account located in the top right corner

#### Smart Wall

The smart wall will be used to display live camera feed to the monitor. For AFC monitors, operator will need to use this to display.

Select Smart Wall in the GUI.

Select the sequencing that is for the monitor and drag to the monitor.

The below image shows Smart Wall in operation.

#### Download Centre

User can view the ongoing or completed tasks and manage all the tasks such as starting, stopping, deleting and so on in the Download Centre.

Click Download Center.

Click All to check all the downloading tasks.

User can perform the following operation(s).

Pause Downloading: Select an ongoing downloading task and click Pause.

Resume: Click Start to resume the downloading or click Start All to resume all the paused tasks.

Delete Downloading Task: Click to remove the downloading task or click Delete All to delete all the records currently downloading. For completed tasks, user can also select to delete the downloaded video files.

View Downloaded Video: For completed downloads, click Open File in Operation column to view the downloaded video files.

Click Downloading to check the ongoing downloading tasks.

Click Done tab to check the completed downloading tasks.

#### Synchronisation

When the icon is displayed with a red dot, it means there is new information updated to the system. Operator will have to click on it to synchronise the information for the control client.

#### Audit Trail

An audit trail (also called audit log) is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of camera activities. Hikvision provides audit data visualizations to provide a bird’s eye view of the duration of the devices such as encoders, decoders, and camera devices.

### How to use NMS server

The user will use only 3 main functions to monitor the 2 switches installed for R160 BPLRT – CCTV. They are **Analytics**, **Discovery**, and **Notifications**.

Once the user has entered the correct necessary credentials, the welcome screen will be shown as below.

The Analytics dashboard includes reports, statistics and provides a summary of the network in the switches. It provides insight in the network health with advanced graphical analytics on most problematic devices based on device state (CPU, memory, temperature)

• Wireless performances insights and KPIs for Stellar APs (Health, SSID, throughput, band utilization)

• Monitors network bandwidth and traffic patterns down to the device port level through sflow sampling collection and reporting

• Provides valuable insights into the applications (Top N apps) that are consuming the most network bandwidth, monitors application traffic arriving from users (Top N talkers), and stores and displays flow data with up to one- minute granularity

• Provides insight in the network health with advanced graphical analytics on most problematic switches based on device state (CPU, memory, temperature) and on PoE (Power over Ethernet) for power utilization at Port or switch level for trending analysis

• Enables automatic generation of business centric, CIO-oriented graphical analytics reports for network

The discovery dashboard enables the user to register new devices to the NMS server under the Managed Devices section.   
  
*Note: Choose SNMPv3 when doing device registration.*  
  
The Notification manager,  
Monitors and analyzes alerts, notifications and network performance from Alcatel-Lucent Portfolio and thirdparty devices in real time

Advanced alert capabilities through customizable filters and sorting capabilities

Remediation and notification actions based on predefined conditions with a single click

# IT Security

## IT Security Configuration

The principal network security defenses are firewalls, intrusion detection and prevention systems (IPS/IDS), Encryptions and content inspection systems like anti-virus, anti-malware, anti-spam, and Access Control Lists (ACL).

### Operating System Hardening

Hardening of the Operating System is identified as the initial step in securing the systems architecture. Operating Systems will be hardened based on the benchmarks available from CIS or other Network services include offerings such as file sharing, print services, email, web sites, and file transfer protocols (FTP), most of which can have compromised security. At the front line of security are hardware devices known as firewalls or intrusion detection/prevention systems. At the operating system level, there are several software firewalls available, as well as intrusion detection/prevention systems. Operating System used will be configured to disable unwanted service and program, and harden to protect against attacked.

### Anti-virus

Centrally managed Anti-virus solution is required where the virus definitions are manually downloaded periodically to update the main server. Central server has a connection to the test systems and the updates are applied to the test servers before applying into the production systems.