CONTENTS

1. Introduction ........................................................................................................ 3
   1.1. What is "hardening?" .................................................................................. 3
   1.2. Cyber threats and cyber risks .................................................................... 5
   1.3. Hardening system components .................................................................. 11

2. General setup ..................................................................................................... 13

3. Servers, Workstations, Clients and Applications ........................................ 15
   3.1. Basic steps .................................................................................................. 15
   3.2. Advanced steps ......................................................................................... 33

4. Devices and network ........................................................................................ 37
   4.1. Devices - basic steps ................................................................................ 37
   4.2. Network - basic steps .............................................................................. 39
   4.3. Devices - advanced steps ......................................................................... 41
   4.4. Network - advanced steps ....................................................................... 41

5. Sony Servers .................................................................................................. 43
   5.1. Basic steps .................................................................................................. 43
   5.2. Advanced steps ......................................................................................... 44
   5.3. SQL Server ................................................................................................ 46
   5.4. Management Server ................................................................................ 46
   5.5. Recording Server ...................................................................................... 48
   5.6. Sony Mobile server component ............................................................... 48
   5.7. Log Server ................................................................................................ 49

6. Client programs ................................................................................................ 51
   6.1. Basic steps (all client programs) .............................................................. 51
   6.2. Network Video Management System Smart Client - advanced steps...... 53
   6.3. Sony Mobile client - advanced steps ....................................................... 59
   6.4. Network Video Management System Web Client - advanced steps ...... 61

7. Appendix 1 - Resources ............................................................................... 63

8. Appendix 2 - Acronyms ............................................................................... 65

Revision History .................................................................................................. 66
1. Introduction

This guide describes security and physical security measures and best practices that can help secure your Network Video Management System video management software (VMS) against cyber-attacks. This includes security considerations for the hardware and software of servers, clients and network device components of a video surveillance system. This guide adopts standard security and privacy controls and maps them to each of the recommendations. That makes this guide a resource for compliance across industry and government security, and network security requirements.

1.1. What is "hardening?"

Developing and implementing security measures and best practices is known as "hardening." Hardening is a continuous process of identifying and understanding security risks, and taking appropriate steps to counter them. The process is dynamic because threats, and the systems they target, are continuously evolving.

Most of the information in this guide focuses on IT settings and techniques, but it's important to remember that physical security is also a vital part of hardening. For example, use physical barriers to servers and client computers, and make sure that things like camera enclosures, locks, tamper alarms, and access controls are secure.

The following are the actionable steps for hardening a VMS:

1. Understand the components to protect
2. Harden the surveillance system components:
   a. Harden the servers (physical and virtual) and client computers and devices
   b. Harden the network
   c. Harden the cameras
3. Document and maintain security settings on each system
4. Train and invest in people and skills, including your supply chain
1.1.1. Target audience

Everyone in an organization must understand at least the basics about network and software security. Attempts to compromise critical IT infrastructure are becoming more frequent, so everyone must take hardening and security seriously.

This guide provides basic and advanced information for end users, system integrators, consultants, and component manufacturers.

- Basic descriptions give general insight into security
- Advanced descriptions give IT-specific guidance for hardening Network Video Management System Enterprise Edition products. In addition to software, it also describes security considerations for the hardware and device components of the system.

1.1.2. Resources and references

The following organizations provide resources and information about best practices for security:

- International Standards Organization (ISO),
- United States (US) National Institute of Standards and Technology (NIST)
- Security Technical Implementation Guidelines (STIGs) from the US Defense Information Systems Administration (DISA)
- Center for Internet Security
- SANS Institute
- Cloud Security Alliance (CSA)
- Internet Engineering Task Force (IETF)
- British Standards

Additionally, camera manufacturers provide guidance for their hardware devices.

See Appendix 1 - Resources (on page 63) for a list of references and Appendix 2 - Acronyms (on page 65) for a list of acronyms.

The NIST document is written for the US Federal government; however, it is generally accepted in the security industry as the current set of best practices.

This guide refers and links to additional information about security controls. The guidance can be cross-referenced to industry-specific requirements and other international security and risk management standard and frameworks. For example, the current NIST Cybersecurity Framework uses SP 800-53 Rev4 as a basis for the controls and guidance. Another example is Appendix H in SP 800-53 Rev 4, which contains a reference to ISO/IEC 15408 requirements, such as Common Criteria.

1.1.3. Hardware and device components

In addition to software, the components of an Network Video Management System Enterprise Edition installation typically include hardware devices, such as:

- Cameras
- Encoders
- Networking products
- Storage systems
- Servers and client computers (physical or virtual machines)
- Mobile devices, such as smartphones

It is important to include hardware devices in your efforts to harden your Network Video Management System Enterprise Edition installation. For example, cameras often have default passwords. Some manufacturers publish these passwords online so that they’re easy for customers to find. Unfortunately, that means the passwords are also available to attackers.

This document provides recommendations for hardware devices.

1.2. Cyber threats and cyber risks

There are many sources of threats to a VMS, including business, technology, process and human attacks or failures. Threats take place over a lifecycle. The threat lifecycle, sometimes called the "cyber kill" or "cyber threat chain," was developed to describe the stages of advanced cyber threats.
Each stage in the threat lifecycle takes time. The amount of time for each stage is particular to the threat, or combination of threats, and its actors and targets.

The threat lifecycle is important for risk assessment because it shows where you can mitigate threats. The goal is to reduce the number of vulnerabilities, and to address them as early as possible. For example, discouraging an attacker who is probing a system for vulnerabilities can eliminate a threat.

Hardening puts in place actions that mitigate threats for each phase in the threat lifecycle. For example, during the reconnaissance phase an attacker scans to find open ports and determine the status of services that are related to the network and the VMS. To mitigate this, hardening guidance is to close unnecessary system ports in Network Video Management System Enterprise Edition and Windows configurations.

The risk and threat assessment process includes the following steps:

- Identify information and security risks
- Assess and prioritize risks
- Implement policy, procedures, and technical solutions to mitigate these risks

The overall process of risk and threat assessment, and the implementation of security
controls, is referred to as a risk management framework. This document refers to NIST security and privacy controls and other publications about risk management frameworks.

1.2.1. Cyber Risk Management Framework


The figures here show:

- An overview of the risk management process. It shows a high-level, overall approach.
- Risk management at a business level, taking strategic and tactical considerations into account.
- The lifecycle of a risk management framework, and the NIST documents that provides details for each of the steps in the lifecycle.
Security and privacy controls represent specific actions and recommendations to implement as part of a risk management process. It's important that the process includes the assessment of the organization, the particular requirements of a given deployment, and the aggregation of these activities into a security plan. SP 800-18 Revision 1 provides references for detailed security plans.

High-level view of risk management (SP 800-39, page 8

The process is interactive, and responses and their outcomes are iterative. Security threats, risks, responses and results are dynamic and adapt, and as a result so must a security plan.
This diagram shows how a risk management framework considers IT systems, business processes, and the organization as a whole to find a balance for the security plan.

**Balancing security and business goals (SP 800-39, page 9**

When hardening a system, you balance the impact on business productivity and usability for the sake of security, and vice versa, in the context of the services you deliver. Security guidance is not isolated from other business and IT activities.
For example, when a user enters their password incorrectly on three consecutive attempts, the password is blocked and they cannot access the system. The system is secure from brute-force attacks, but the unlucky user cannot use the device to do their work. A strong password policy that requires 30 character passwords, and changing passwords every 30 days is a best practice, but it’s also difficult to use.


To document its risk management framework, NIST produced multiple special publications. It includes the following components:

1. Categorization (identification of risk level)
2. Selection of security and privacy controls
3. Implementation
4. Assessment of the effectiveness of security controls
5. Creating an improved system security profile, and what’s called an Authority to Operate (ATO)

6. Monitoring and evaluating through iterations

The risk management framework helps put a security plan and guidance in a security context.

1.3. Hardening system components

To harden system components, you change configurations to reduce the risk of a successful attack. Attackers look for a way in, and look for vulnerabilities in exposed parts of the system. Surveillance systems can involve 100s or even 1000s of components. Failure to secure any one component can compromise the system.

The need to maintain configuration information is sometimes overlooked. Network Video Management System Enterprise Edition provides features for managing configurations, but organizations must have a policy and process in place, and commit to doing the work. Hardening requires that you keep your knowledge about security up-to-date:

- Be aware of issues that affect software and hardware, including operating systems, mobile devices, cameras, storage devices, and network devices. Establish a point-of-contact for all of the components in the system. Ideally, use reporting procedures to track bugs and vulnerabilities for all components.

- Keep current on Common Vulnerabilities and Exposures (CVEs) (described in Common Vulnerabilities and Exposures) for all system components. These can relate to the operating systems, devices that have hard-coded maintenance passwords, and so on. Address vulnerabilities for each component, and alert manufacturers to vulnerabilities.

- Maintain up-to-date configuration and system documentation for the system. Use change-control procedures for the work you perform, and follow best practices for configuration management, as described in SP 800-128.

The following sections provide basic and advanced hardening and security recommendations for each system component. The sections also contain examples of how these relate to specific security controls described in the NIST Special Publication 800-53 Revision 4, titled Security and Privacy Controls for Federal Information Systems and Organizations.

In addition to the NIST document, the following sources are referenced:
- Center for Internet Security
- SP 800-53
- ISO 27001

Appendix 1 - Resources (on page 63) in this document provides recommendations from camera manufacturers. This is a relatively new effort from manufacturers, so limited resources are available. For the most part, the recommendations can be generalized across camera manufacturers.
2. General setup

To help secure your surveillance system, Sony recommends the following:

- Restrict access to servers. Keep servers in locked rooms, and make it difficult for intruders to access network and power cables.
  
  (PE2 and PE3 in Appendices D and F in NIST SP 800-53 Rev4

- Design a network infrastructure that uses physical network or VLAN segmentation as much as possible.
  
  (SC3 in Appendices D and F in NIST SP 800-53 Rev4

- Separate the camera network from the server network by having two network interfaces in each recording server: one for the camera network, and one for the server network.

- Put the mobile server in a "demilitarized zone" (DMZ) with one network interface for public access, and one for private communication to other servers.
  
  (SC7 in Appendices D and F NIST SP 800-53 Rev4
  http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf.)

- Many precautions can be taken when it comes to general set up. In addition to firewalls, these include techniques to segment the network and control access to the servers, clients and applications.
  
  (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 in Appendices D and F in NIST SP 800-53 Rev4
  http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf (AC Access Controls), (CM Configuration Management) (IR Incident Response) (SA System and Service Acquisition) (SI Systems and Information Integrity).)

- Configure the VMS with roles that control access to the system, and designate tasks and responsibilities.
(AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, in Appendices D and F in NIST SP 800-53 Rev4)


The figure shows an example of a general setup.
3. Servers, Workstations, Clients and Applications

This section provides hardening guidance based on Microsoft Windows and the services that Network Video Management System Enterprise Edition uses. This includes:

- The Network Video Management System Enterprise Edition product running on Windows Servers
- The device pack installed on the recording servers
- The server hardware or virtual platforms, and operating systems and services
- The client computers for Network Video Management System Smart Client and Network Video Management System Web Client
- Mobile devices and their operating systems and applications

3.1. Basic steps

3.1.1. Establish surveillance and security objectives

Before implementing the VMS, Sony recommends that you establish surveillance objectives. Define goals and expectations related to capturing and using video data and related metadata. All stakeholders should understand the surveillance objectives.

Specifics of surveillance objectives can be found in other documents, for example BS EN 62676-1-1: Video surveillance systems for use in security applications. System requirements. General.

When surveillance objectives are in place, you can establish the security objectives. Security objectives support the surveillance objectives by addressing what to protect in the VMS. A shared understanding of security objectives makes it easier to secure the VMS and maintain data integrity.

With the surveillance and security objectives in place, you can more easily address the operational aspects of securing the VMS, such as how to:

- Prevent data from being compromised
- Respond to threats and incidents when they occur, including roles and responsibilities.

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 PL-2 *System Security Plan*
- NIST SP 800-53 SA-4 *Acquisition Process*

### 3.1.2. Establish a formal security policy and response plan

In compliance with NIST SP 800-100 Information Security Handbook: A Guide for Managers [http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100-mar07-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-100/sp800-100-mar07-2007.pdf), Sony recommends that you establish a formal security policy and a response plan that describe how your organization addresses security issues, in terms of practical procedures and guidelines. For example, a security policy can include:

- A password policy defined by the internal IT department
- Access control with ID badges
- Restrictions for smartphones from connecting to the network

Adopt existing IT policies and plans if they adhere to security best practices.

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 IR-1 *Incident Response Policy and Procedures*
- NIST SP 800-53 PM-1 *Information Security Program Plan*

### 3.1.3. Use Windows users with Active Directory

There are two types of users in Network Video Management System Enterprise Edition:

- Basic user: a dedicated VMS user account authenticated by a combination of username and password using a password policy. Basic users connect to the VMS using a secure socket layer (SSL) with current Transport Layer (TLS) security protocol session for login, encrypting the traffic contents and username and password.
- Windows user: the user account is specific to a machine or a domain, and it is authenticated based on the Windows login. Windows users connecting to the VMS can use Microsoft Windows Challenge/Response (NTML) for login, Kerberos (see "About Kerberos authentication" on page 19), or other SSP options from Microsoft.

Sony recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to authorize access to the VMS. This allows you to enforce:

- A password policy that requires users to change their password regularly
- Brute force protection, so that the Windows AD account is blocked after a number of failed authentication attempts, again in line with the organization password policy
- Multi-factor authentication in the VMS, particularly for administrators
- Role-based permissions, so you can apply access controls across your domain

If your organization does not use AD, you can add Windows users to workgroups on the management server instead. Workgroups give you some of the same advantages as Windows users with AD. You can enforce a password policy, which helps protect against brute force attacks, but Sony recommends that you use a Windows Domain because this gives you central control over user accounts.

Windows users have the advantage of being authenticated via the directory as a single authoritative source and enterprise service for the network and not ad hoc for their local machine. This lets you use role based access controls to assign permissions to users and groups consistently across the domain and the computers on the network.

If you use local Windows users, the user must create a local user name and password on each machine, which is problematic from security and usability perspectives.

To add Windows users or groups to roles in Management Client, follow these steps:

1. Open Management Client
2. Expand the **Security** node.
3. Select the role to which you want to add the Windows users.

4. On the **Users** and **Groups** tab, click **Add**, and select **Windows user**. A pop-up window appears.

5. If the domain name does not appear in the **From this location** field, click **Locations**.

6. Specify the Windows user, and then click **OK**.

To verify that the Windows user is an AD user, the domain name must appear as a prefix, for example "Domain\John".

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 CM-6 *Configuration Settings*
- NIST SP 800-53 SA-5 *Information System Documentation*
- NIST SP 800-53 SA-13 *Trustworthiness*
3.1.4. About Kerberos authentication

Kerberos is a ticket-based network authentication protocol. It is designed to provide strong
authentication for client/server or server/server applications.

Use Kerberos authentication as an alternative to the older Microsoft NT LAN (NTLM)
authentication protocol.

Kerberos authentication requires mutual authentication, where the client authenticates to
the service and the service authenticates to the client. This way you can authenticate more
securely from Network Video Management System clients to Network Video Management
System servers without exposing your password.

To make mutual authentication possible in your Network Video Management Software you
must register Service Principal Names (SPN) in the active directory. An SPN is an alias
that uniquely identifies an entity such as a Network Video Management System server
service. Every service that uses mutual authentication must have an SPN registered so
that clients can identify the service on the network. Without correctly registered SPNs,
mutable authentication is not possible.

The table below lists the different Sony services with corresponding port numbers you
need to register:

<table>
<thead>
<tr>
<th>Service</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management server - IIS</td>
<td>80 - Configurable</td>
</tr>
<tr>
<td>Management server - Internal</td>
<td>8080</td>
</tr>
<tr>
<td>Recording server - Data Collector</td>
<td>7609</td>
</tr>
<tr>
<td>Event Server</td>
<td>22331</td>
</tr>
</tbody>
</table>

The number of services you need to register in the active directory depends on your
current installation. Data Collector is installed automatically when installing Management
Server, Recording Server, Event Server.

You must register two SPNs for the user running the service: one with the hostname and
one with the fully qualified domain name.

If you are running the service under a network user service account, you must register the
two SPNs for each computer running this service.

This is the Sony SPN naming scheme:

```
VideoOS/[DNS Host Name]:[Port]
```
**VideoOS/[Fully qualified domain name]:[Port]**

The following is an example of SPNs for the recording server service running on a computer with the following details:

**Hostname:** Record-Server1  
**Domain:** Surveillance.com  

SPNs to register:  
**VideoOS/Record-Server1:7609**  
**VideoOS/Record-Server1.Surveillance.com:7609**

### 3.1.5. Use Windows update

Sony recommends that you use Windows Update to protect your VMS against vulnerabilities in the operating system by making sure that the latest updates are installed. Network Video Management System Enterprise Edition is Windows-based, so security updates from Windows Update are important.  
Updates can require a connection to the Internet, so Sony recommends that this connection is open only as required, and that it is monitored for unusual traffic patterns.  
Windows Updates often require a restart. This can be a problem if high-availability is required, because the server cannot receive data from devices while it restarts.  
There are several ways to avoid this, or minimize the impact. For example, you can download updates to the server, and then apply them at a time when a restart will disrupt surveillance as little as possible.  
If high availability is a concern, Sony recommends that you run management server and event servers in clusters. Do not include recording servers in the cluster.

Before implementing Windows updates across the organization, Sony recommends that you verify the updates in a test environment. See NIST 800-53 CM-8 Information system component inventory and sandboxing and SC-44 Detonation Chambers.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 *Flaw Remediation*

### 3.1.6. Keep software and device firmware updated

Sony recommends that you use the latest version of Network Video Management System
Enterprise Edition and firmware for the hardware devices, for example the cameras. This will ensure that your system includes the latest security fixes. For hardware, network components, and operating systems, check the CVE database as well as any updates pushed out by manufacturers. Before you upgrade the device firmware, verify that Network Video Management System Enterprise Edition supports it. Also, make sure that the device pack installed on the recording servers supports the device firmware. Do this in a test environment for configuration, integration and testing before putting it into the production environment. To verify that the VMS supports a device, please read NVMS Supported Device List that can be founded on our website (https://www.sony.net/CameraSystem/NVMS/Technical-Documents).

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 Flaw Remediation

3.1.7. Use secure and trusted networks connection

Network communications must be secure, whether or not you are on a closed network. By default, secure communications should be used when accessing the VMS. For example:

- VPN tunnels or HTTPS by default
- Latest version of the Transport Layer Security (TLS, currently 1.2) with valid certificates that meet industry best practices, such as from Public-Key Infrastructure (X.509) and CA/Browser Forum.

Otherwise, credentials may be compromised and intruders might use them to access the VMS. Configure the network to allow client computers to establish secure HTTPS sessions or VPN tunnels between the client devices and the VMS servers.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 SI-2 Flaw remediation
- NIST SP 800-53 CM-6 Configuration Settings
- NIST SP 800-53 SC-23 Session Authenticity

3.1.8. Use firewalls to limit IP access to servers and computers

Sony recommends that you use secure connections, and the following additional steps:

- Use secure device authentication
- Use TLS
- Use device whitelisting to authenticate devices
- Use firewalls to limit network communication between servers and client computers and programs.

All Network Video Management System components and the ports needed by them are listed in individual sections below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the Network Video Management System Enterprise Edition uses. You should only enable these ports. The lists also include the ports used for local processes. They are arranged in two groups:

- **Server components** (services) offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound connections.
- **Client components** (clients) initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall.

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections. Do keep in mind that server components can act as clients to other server components as well.

The port numbers are the default numbers, but this can be changed. Contact Sony Support, if you need to change ports that are not configurable through the Management Client.
Server components (inbound connections)

Each of the following sections list the ports which need to be opened for a particular service. In order to figure out which ports need to be opened on a particular computer, you need to consider all services running on this computer.

Management Server service and related processes

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>HTTP</td>
<td>IIS</td>
<td>All Network Video Management System components</td>
<td>Main communication, for example, authentication and configurations.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>IIS</td>
<td>Network Video Management System Smart Client and the Management Client</td>
<td>Authentication of basic users.</td>
</tr>
<tr>
<td>6473</td>
<td>TCP</td>
<td>Management Server service tray controller, local connection only.</td>
<td>Showing status and managing the service.</td>
<td></td>
</tr>
<tr>
<td>7475</td>
<td>TCP</td>
<td>Management Server service</td>
<td>Windows SNMP Service</td>
<td>Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. The port number was 6475.</td>
</tr>
<tr>
<td>8080</td>
<td>TCP</td>
<td>Management server</td>
<td>Local connection only.</td>
<td>Communication between internal processes on the server.</td>
</tr>
<tr>
<td>9993</td>
<td>TCP</td>
<td>Management Server service Recording Server services</td>
<td>Authentication, configuration, token exchange.</td>
<td></td>
</tr>
</tbody>
</table>
### Port number

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>12345</td>
<td>TCP</td>
<td>Management Server service</td>
<td>Network Video Management System Smart Client</td>
<td>Communication between the system and Matrix recipients. You can change the port number in the Management Client.</td>
</tr>
</tbody>
</table>

### SQL Server service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SQL Server service</td>
<td>Management Server service</td>
<td>Storing and retrieving configurations.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SQL Server</td>
<td>Event Server service</td>
<td>Storing and retrieving events.</td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>SQL Server</td>
<td>Log Server service</td>
<td>Storing and retrieving log entries.</td>
</tr>
</tbody>
</table>
## Data Collector service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7609</td>
<td>HTTP</td>
<td>IIS</td>
<td>On the Management Server computer: Data Collector services on all other servers. On other computers: Data Collector service on the Management Server.</td>
<td>System Monitor.</td>
</tr>
</tbody>
</table>

## Event Server service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>TCP/UDP</td>
<td>Event Server Service</td>
<td>Any server sending generic events to your Network Video Management System.</td>
<td>Listening for generic events from external systems or devices. Only if the relevant data source is enabled.</td>
</tr>
<tr>
<td>1235</td>
<td>TCP</td>
<td>Event Server service</td>
<td>Any server sending generic events to your Network Video Management System.</td>
<td>Listening for generic events from external systems or devices. Only if the relevant data source is enabled.</td>
</tr>
<tr>
<td>9090</td>
<td>TCP</td>
<td>Event Server service</td>
<td>Any system or device that sends analytics events to your Network Video Management System.</td>
<td>Listening for analytics events from external systems or devices. Only relevant if the Analytics Events feature is enabled.</td>
</tr>
</tbody>
</table>
### Event Server service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22331</td>
<td>TCP</td>
<td>Event Server service</td>
<td>Network Video Management System Smart Client and the Management Client</td>
<td>Configuration, events, alarms, and map data.</td>
</tr>
<tr>
<td>22333</td>
<td>TCP</td>
<td>Event Server service</td>
<td>MIP Plug-ins and applications.</td>
<td>MIP messaging.</td>
</tr>
</tbody>
</table>

### Recording Server service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Recording Server Service</td>
<td>Cameras, encoders, and I/O devices.</td>
<td>Listening for event messages from devices. The port is disabled per default.</td>
</tr>
<tr>
<td>5432</td>
<td>TCP</td>
<td>Recording Server Service</td>
<td>Cameras, encoders, and I/O devices.</td>
<td>Listening for event messages from devices.</td>
</tr>
<tr>
<td>7474</td>
<td>TCP</td>
<td>Recording Server Service</td>
<td>Windows SNMP service</td>
<td>Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. The port number was 6474.</td>
</tr>
<tr>
<td>7563</td>
<td>TCP</td>
<td>Recording Server Service</td>
<td>Network Video Management System Smart Client , Management Client</td>
<td>Retrieving video and audio streams, PTZ commands.</td>
</tr>
<tr>
<td>Port number</td>
<td>Protocol</td>
<td>Process</td>
<td>Connections from...</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>8966</td>
<td>TCP</td>
<td>Recording Server Service</td>
<td>Recording Server tray controller, local connection only.</td>
<td>Showing status and managing the service.</td>
</tr>
<tr>
<td>65101</td>
<td>UDP</td>
<td>Recording Server service</td>
<td>Local connection only</td>
<td>Listening for event notifications from the drivers.</td>
</tr>
</tbody>
</table>

Note that in addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

**Mobile Server service**

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8000</td>
<td>TCP</td>
<td>Mobile Server service</td>
<td>Mobil Server management (tray icon), local connection only.</td>
<td>SysTray application.</td>
</tr>
<tr>
<td>8081</td>
<td>HTTP</td>
<td>Mobile Server service</td>
<td>Mobile clients, Web clients, and Management Client.</td>
<td>Sending data streams; video and audio.</td>
</tr>
<tr>
<td>8082</td>
<td>HTTPS</td>
<td>Mobile Server service</td>
<td>Mobile clients and Web clients.</td>
<td>Sending data streams; video and audio.</td>
</tr>
</tbody>
</table>
### Screen Recorder service

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Process</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>52111</td>
<td>TCP</td>
<td>Network Video Management System Screen Recorder</td>
<td>Recording Server Service</td>
<td>Provides video from a monitor. It appears and acts in the same way as a camera on the recording server. You can change the port number in the Management Client.</td>
</tr>
</tbody>
</table>

### Cameras, encoders, and I/O devices

#### Inbound connections

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Connections from...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>Recording servers</td>
<td>Authentication, configuration, and data streams; video and audio.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Recording servers</td>
<td>Authentication, configuration, and data streams; video and audio.</td>
</tr>
<tr>
<td>554</td>
<td>RTSP</td>
<td>Recording servers</td>
<td>Data streams; video and audio.</td>
</tr>
</tbody>
</table>
# Outbound connections

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Connections to...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Recording servers</td>
<td>Sending event notifications (deprecated).</td>
</tr>
<tr>
<td>5432</td>
<td>TCP</td>
<td>Recording servers</td>
<td>Sending event notifications.</td>
</tr>
</tbody>
</table>

Note that only a few camera models are able to establish outbound connections.

## Client components (outbound connections)

**Network Video Management System Smart Client, Network Video Management System Management Client, Sony Mobile server**

<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Connections to...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Management server service</td>
<td>Authentication</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Management server service</td>
<td>Authentication of basic users.</td>
</tr>
<tr>
<td>7563</td>
<td>TCP</td>
<td>Recording server service</td>
<td>Retrieving video and audio streams, PTZ commands.</td>
</tr>
<tr>
<td>22331</td>
<td>TCP</td>
<td>Event Server service</td>
<td>Alarms.</td>
</tr>
</tbody>
</table>

**Web Client, Sony Mobile client**
<table>
<thead>
<tr>
<th>Port number</th>
<th>Protocol</th>
<th>Connections to...</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8081</td>
<td>HTTP</td>
<td>Sony Mobile server</td>
<td>Retrieving video and audio streams.</td>
</tr>
<tr>
<td>8082</td>
<td>HTTPS</td>
<td>Sony Mobile server</td>
<td>Retrieving video and audio streams.</td>
</tr>
</tbody>
</table>

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 **System Interconnections**
- NIST SP 800-53 CM-6 **Configuration Settings**
- NIST SP 800-53 SC-7 **Boundary Protection**

### 3.1.9. Use antivirus on all servers and computers

Sony recommends that you deploy anti-virus software on all servers and computers that connect to the VMS. Malware that gets inside your system can lock, encrypt, or otherwise compromise data on the servers and other devices on the network.

If mobile devices connect to the VMS, this includes ensuring that the devices have the latest operating systems and patches (though not directly anti-virus) installed.

When you do virus scanning, do not scan recording server directories and subdirectories that contain recording databases. In addition, do not scan for viruses on archive storage directories. Scanning for viruses on these directories can impact system performance.

For information about the ports, directories, and subdirectories to exclude from the virus scan, see the section "About virus scanning" in the Network Video Management System Enterprise Edition Administrator Guide.

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 PL-8 **Information Security Architecture**
- NIST SP 800-53 SI-2 **Flaw remediation**
- NIST SP 800-53 SI-3 **Malicious Code Protection**
- NIST SP 800-53 SI **Information Systems Monitoring**
3.1.10. Monitor logs in the VMS for signs of suspicious activity

Network Video Management System Enterprise Edition provides features for generating and viewing logs that provide information about patterns of use, system performance, and other issues. Sony recommends that you monitor the logs for signs of suspicious activities. There are tools that leverage logs for operational and security purposes. Many businesses use syslog servers to consolidate logs. You can use syslog to note activities at a Windows level, however, Network Video Management System Enterprise Edition does not support syslog.

Sony recommends that you use the Audit Log in Network Video Management System Enterprise Edition, and enable user access logging in Management Client. By default, the Audit Log notes only user logins. However, you can turn on user access logging so that the Audit Log notes all user activities in all of the client components of Network Video Management System Enterprise Edition products. This includes the times of the activities and the source IP addresses.

The client components are Network Video Management System Smart Client, Web Client, the Sony Management Client component, and integrations made by using the MIP SDK. Examples of activities are exports, activating outputs, viewing cameras live or in playback, and so on.

The Audit log does not note unsuccessful login attempts, or when the user logs out.

Logging all user activities in all clients increases the load on the system, and can affect performance.

You can adjust the load by specifying the following criteria that controls when the system will generate a log entry:

- The number of seconds that comprise one sequence. The VMS generates one log entry when a user plays video within the sequence.
- The number of frames that a user must view when playing back video before the VMS generates a log entry.

To turn on and configure extended user access logging, follow these steps:

1. In Management Client, click **Tools**, and select **Options**.
2. On the **Server Logs** tab, under **Log settings**, select **Audit Log**.
3. Under **Settings**, select the **Enable user access logging** check box.
4. Optional: To specify limitations for the information that is noted, and reduce impact on performance, make selections in the **Playback sequence logging length** and **Records seen before logging** fields.

To view the Audit Log in Network Video Management System Enterprise Edition, follow these steps:

1. Open Management Client.
2. Expand the **Server Logs** node.
3. Click **Audit Log**.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 AU-3 **Content of Audit Records**
- NIST SP 800-53 RA-5 **Vulnerability Scanning**
• NIST SP 800-53 AU-6 Audit Review, Analysis and Reporting

3.2. Advanced steps

3.2.1. Adopt standards for secure network and VMS implementations

Sony recommends that you adopt standards for secure networking and Network Video Management System Enterprise Edition implementations. The use of standards is a basic component of Internet and network engineering, and the basis of interoperability and system conformance. This also applies to the use of cryptographic solutions, where standards-based cryptography is the most commonly accepted approach.

3.2.2. Establish an incident response plan

Sony recommends you start with a set of policies and procedures and establish an incident response plan. Designate staff to monitor the status of the system and respond to suspicious events. For example, activities that happen at unusual times. Establish a security Point of Contact (POC) with each of your vendors, including Sony.
The following image is adapted from the NIST Cybersecurity Framework http://www.nist.gov/cyberframework/. It shows the lifecycle that needs to be considered when creating a plan. The supporting material in the framework provide details about the lifecycle and security controls for incident response plans.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 IR 1-13 Incident Response

### 3.2.3. Protect sensitive VMS components

Sony recommends that you use physical access control, and use the VMS to monitor and protect its sensitive VMS components. Physical restriction and role-based physical access control are countermeasures that keep servers and workstations secure. Administrators and users should only have access to the information they need in order to fulfill their responsibilities. If all internal users have the same access level to critical data, it’s easier for attackers to access the network.

Learn more
The following control(s) provide additional guidance:
3.2.4. Follow Microsoft OS Security best practices

Sony recommends that you follow the security best practices for Microsoft operating systems (OS) to mitigate OS risks and maintain security. This will help you keep the Microsoft servers and client computers secure. For more information, see Microsoft Security Update Guide https://technet.microsoft.com/en-us/security/dn550891.aspx.

3.2.5. Use tools to automate or implement the security policy

Sony recommends that you find one or more tools to help you automate and implement the security policy. Automation reduces the risk of human error and makes it easier to manage the policy. For example, you can automate the installation of security patches and updates on servers and client computers.

One way to implement this recommendation is to combine the Microsoft Security Configuration Manager (SCCM) with the Security Content Automation Protocol (SCAP). (See for example, Geek of All Trades: Automate Baseline Security Settings and Security Content Automation Protocol (SCAP) Validation Program.) This gives you a framework to create, distribute, and validate security settings on computers across your network.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 CM-1 Configuration Management Policy and Procedures
- NIST SP 800-53 CM-2 Baseline Configuration
- NIST SP 800-53 CM-3 Configuration Change Control

3.2.6. Follow established network security best practices

Sony recommends that you follow IT and vendor best practices to ensure that devices on your network are securely configured. Ask your vendors to provide this information. It is important to open and maintain a security dialogue, and a discussion of best practices is a
It is important to deny access to the VMS by not using vulnerable network settings. For more information, see SP 800-128, SP 800-41-rev1 (specific to firewalls), and ICS-CERT Standards and References (general list).

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 CM-6 Configuration Settings
- NIST 800-53 MA-3 Maintenance Tools
4. Devices and network

This section provides guidance for hardening the devices and network components related to Network Video Management System Enterprise Edition. This includes key parts of the system such as the cameras, storage, and the network. Surveillance systems often include cameras at the edge of the network. Cameras and their network connections, if left unprotected, represent a significant risk of compromise, potentially giving intruders further access to the system.

4.1. Devices - basic steps

4.1.1. Use strong passwords instead of default passwords

Sony recommends that you change the default passwords on devices, for example, on a camera. Do not use default passwords because they are often published to the Internet and are readily available.

Instead, use strong passwords for devices. Strong passwords include eight or more alpha-numeric characters, use upper and lower cases, and special characters.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 IA-4 Authenticator Management
- NIST 800-53 IA-8 Authenticator Feedback
- NIST 800-53 SI-11 Error Handling

4.1.2. Stop unused services and protocols

To help avoid unauthorized access or information disclosure, Sony recommends that you stop unused services and protocols on devices. For example, Telnet, SSH, FTP, UPnP, IPv6, and Bonjour.

It is also important to use strong authentication on any services that access the VMS, network, or devices. For example, use SSH keys instead of user names and passwords, and use certificates from a Certificate Authority for HTTPS. For more information, see the hardening guides and other guidance from the device manufacturer.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-17 Remote Access (Disable Unused Protocols)
- NIST SP 800-53 CM-6 Configuration Settings
- NIST SP 800-53 CM-7 Least Functionality
- NIST SP 800-53 IA-2 Identification and Authentication
- NIST SP 800-53 SA-9 External Information Services

4.1.3. Create dedicated user accounts on each device

All cameras have a default user account with a user name and password that the VMS uses to access the device. For auditing purposes, Sony recommends that you change the default user name and password.

Create a user account specifically for use by the VMS, and use this user account and password when you add the camera to the VMS. When a recording server connects to the camera, it uses the user name and password you have created. If the camera has a log, this log shows that the recording server has connected to the camera.

With a dedicated user name and password, the device logs can help you determine whether a recording server or a person accessed the camera. This is relevant when investigating potential security issues affecting devices.

You can change the user name and password for a device before or after you add it in Management Client.

To change the user name and password before you add the device, follow these steps:

1. Go to the device’s web interface, and change the default user name and password.
2. In Management Client, add the device, and specify the user name and password.

To change the user name and passwords of devices that are already added, follow these steps:

1. In Management Client, in the Site Navigation pane, expand the Servers node and select Recording Servers.
2. In the Recording Server pane, expand the recording server that contains the device, and then right-click the device and select **Edit hardware**.

![Edit Hardware](image)

3. Under **Authentication**, enter the new user name and password.

**Learn more**

The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 **Account Management**
- NIST SP 800-53 AC-4 **Least Privilege**

### 4.2. Network - basic steps

#### 4.2.1. Use a firewall between the VMS and the Internet

The VMS should not connect directly to the Internet. If you expose parts of the VMS to the Internet, Sony recommends that you use an appropriately configured firewall between the VMS and the Internet.
If possible, expose only the Sony Mobile server component to the Internet, and locate it in a demilitarize zone (DMZ) with firewalls on both sides. This is illustrated in the following figure.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 *System Interconnections*

### 4.2.2. Connect the camera subnet to the recording server subnet only

Sony recommends that you connect the camera subnet only to the recording server subnet. The cameras and other devices need to communicate only with the recording servers. For more information, see Recording Server (on page 48).

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 SC-7 *Boundary Protection*
4.3. Devices - advanced steps

4.3.1. Use Simple Network Management Protocol to monitor events

Sony recommends that you use Simple Network Management Protocol (SNMP) to monitor events on the devices on the network. You can use SNMP as a supplement for syslog. SNMP works in real-time with many types of events that can trigger alerts, for example if a device is restarted.

For this to work, the devices must support logging via SNMP.

There are multiple versions of SNMP protocols available. Versions 2c and 3 are the most current. Implementation involves a suite of standards. A good overview can be found on the SNMP reference site.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 SI-4 Event Monitoring

4.4. Network - advanced steps

4.4.1. Use secure wireless protocols

If you use wireless networks, Sony recommends that you use a secure wireless protocol to prevent unauthorized access to devices and computers. For example, use standardized configurations. The NIST guidance on wireless local area networks provides specific details on network management and configuration. For more information, see SP 800-48 revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks.

Additionally, Sony recommends that you do not use wireless cameras in mission-critical locations. Wireless cameras are easy to jam, which can lead to loss of video.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-18 Wireless Access
- NIST SP 800-53 SC-40 Wireless Link Protection
4.4.2. Use port-based access control

Use port-based access control to prevent unauthorized access to the camera network. If an unauthorized device connects to a switch or router port, the port should become blocked. Information about how to configure switches and routers is available from the manufacturers. See SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, for information about configuration management of information systems.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 CM-1 Configuration Management Policy and Procedures
- NIST 800-53 CM-2 Baseline Configuration
- NIST 800-53 AC-4 Least Privilege
- NIST 800-53 CM-6 Configuration Settings
- NIST 800-53 CM-7 Least Functionality

4.4.3. Run the VMS on a dedicated network

Sony recommends that, whenever possible, you separate the network where the VMS is running from networks with other purposes. For example, a shared network such as the printer network should be isolated from the VMS network. In addition, Network Video Management System Enterprise Edition deployments should follow a general set of best practices for system interconnections.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 CA-3 System Interconnections
5. Sony Servers

This section contains guidance on how to protect the Sony servers.

5.1. Basic steps

5.1.1. Use physical access controls and monitor the server room

Sony recommends that you place the hardware with the servers installed in a designated server room, and that you use physical access controls. In addition, you should maintain access logs to document who has had physical access to the servers. Surveillance of the server room is also a preventive precaution.

Sony supports integration of access control systems and their information. For example, you can view access logs in Network Video Management System Smart Client.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 PE-3 Physical Access Control

5.1.2. Use encrypted communication channels

Sony recommends that you use a VPN for communication channels for installations where servers are distributed across untrusted networks. This is to prevent attackers from intercepting communications between the servers. Even for trusted networks, Sony recommends that you use HTTPS for configuration of cameras and other system components.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 AC-4 Information Flow Enforcement
- NIST 800-53 AC-17 Remote Access
5.2. Advanced steps

5.2.1. Run services with service accounts

Sony recommends that you create service accounts for services related to Network Video Management System Enterprise Edition, instead of using a regular user account. Set up the service accounts as domain users, and only give them the permissions required to run the relevant services. See About Kerberos authentication (on page 19). For example, the service account should not be able to log on to the Windows desktop.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 AC-5 Separation of Duties
- NIST 800-53 AC-6 Least Privilege

5.2.2. Run components on dedicated virtual or physical servers

Sony recommends that you run the components of Network Video Management System Enterprise Edition only on dedicated virtual or physical servers without any other software or services installed.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 CM-9 Configuration Management Plan

5.2.3. Restrict the use of removable media on computers and servers

Sony recommends that you restrict the use of removable media, for example USB keys, SD cards, and smartphones on computers and servers where components of Network Video Management System Enterprise Edition are installed. This helps prevent malware from entering the network. For example, allow only authorized users to connect removable media when you need to transfer video evidence.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 MP-7 Media Use
5.2.4. Use individual administrator accounts for better auditing

As opposed to shared administrator accounts, Sony recommends using individual accounts for administrators. This lets you track who does what in Network Video Management System Enterprise Edition. This helps prevent malware from entering the network. You can then use an authoritative directory such as Active Directory to manage the administrator accounts.

You assign administrator accounts to roles in Management Client under Roles.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 AC-5 Separation of Duties
- NIST 800-53 CM-9 Configuration Management Plan

5.2.5. Use subnets or VLANs to limit server access

Sony recommends that you logically group different types of hosts and users into separate subnets. This can have benefits in managing privileges for these hosts and users as members of a group with a given function or role. Design the network so that there is a subnet or VLAN for each function. For example, one subnet or VLAN for surveillance operators and one for administrators. This allows you to define firewall rules by group instead of for individual hosts.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- NIST SP 800-53 SC-7 Boundary Protection

5.2.6. Enable only the ports used by Event Server

Sony recommends that you enable only the ports used by event server, and block all other ports, including the default Windows ports.

The event server ports used in Network Video Management System Enterprise Edition are: 22331, 22333, 9090, 1234, and 1235.

The ports used depend on the deployment. If in doubt, contact Sony Support.
Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

5.3. SQL Server

5.3.1. Run the SQL Server database on a separate server

Sony recommends that you make the SQL Server redundant. This reduces the risk of real or perceived downtime.

To support Windows Server Failover Clustering (WSFC), Sony recommends that you run the SQL Server database on a separate server, and not on the management server. SQL must run in WSFC setup, and the management and event servers must run in a Microsoft Cluster setup (or similar technology). For more information about WSFC, see Windows Server Failover Clustering (WSFC) with SQL Server https://msdn.microsoft.com/en-us/library/hh270278.aspx.

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 SC-7 Boundary Protection
- NIST 800-53 CM-9 Configuration Management Plan

5.4. Management Server

5.4.1. Adjust the token time-out

Network Video Management System Enterprise Edition uses session tokens when it logs in to the management server using SSL (basic users) or NTLM (Windows users) protocols. A token is retrieved from the management server and used on the secondary servers, for example the recording server and sometimes also the event server. This is to avoid that NTLM and AD lookup is performed on every server component.

By default, a token is valid for 240 minutes. You can adjust this down to 1 minute intervals. This value can also be adjusted over time. Short intervals increase security, however, the system generates additional communication when it renews the token.
The best interval to use depends on the deployment. This communication increases the system load and can impact performance.

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 IA-5 **Authenticator Management**

### 5.4.2. Enable only the ports used by the management server

Sony recommends that you enable only the ports used by the management server, and that you block all other ports, including the default Windows ports. This guidance is consistent for the server components of Network Video Management System Enterprise Edition.

The management server ports used in Network Video Management System Enterprise Edition are: 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

The ports used depend on the deployment. If in doubt, contact Sony Support.

**Learn more**
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 **Account Management**
- NIST SP 800-53 SC-7 **Boundary Protection**

### 5.4.3. Disable non-secure protocols

When a basic user logs in to the management server through IIS, the Management Client will use any protocol available. Sony recommends that you always implement the latest version of the Transport Layer Security (TLS, currently 1.2), and disable all improper cipher suites and obsolete versions of SSL/TLS protocols. Perform actions to block non-secure protocols at the OS level. This prevents the Management Client from using protocols that are not secure. The OS determines the protocol to use.

The protocols used depend on the deployment. If in doubt, contact Sony Support.

**Learn more**
The following control(s) provide additional guidance:
• NIST 800-53 AC-17 Remote Access (Disable Unused Protocols)
• NIST 800-53 CM-6 Configuration Settings
• NIST 800-53 CM-7 Least Functionality

5.5. Recording Server

5.5.1. Use separate network interface cards

Sony recommends that you use multiple network interface cards (NICs) to separate the communication between recording servers and devices from the communication between recording servers and client programs. Client programs do not need to communicate directly with devices.

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 SC-7 Boundary Protection

5.6. Sony Mobile server component

5.6.1. Only enable ports that Sony Mobile server uses

Sony recommends that you enable only the ports that Sony Mobile server uses, and block all other ports, including the default Windows ports.

By default, mobile server uses ports 8081 and 8082.

The ports used depend on the deployment. If in doubt, contact Sony Support.

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 AC-2 Account Management
• NIST SP 800-53 SC-7 Boundary Protection

5.6.2. Use a "demilitarized zone" (DMZ) to provide external access

Sony recommends that you install Sony Mobile server in a DMZ, and on a computer with two network interfaces:

• One for internal communication
• One for public Internet access

This allows mobile client users to connect to Sony Mobile server with a public IP address, without compromising the security or availability of the VMS network.

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 SC-7 Boundary Protection

5.6.3. Disable non-secure protocols

Sony recommends that you use only the necessary protocols, and only the latest versions. For example, implement the latest version of the Transport Layer Security (TLS, currently 1.2) and disable all other cipher suites and obsolete versions of SSL/TLS protocols. This requires configuration of Windows and other system components, and the proper use of digital certificates and keys.

The same recommendation is given for the management server. For more information, see the section in this document titled Disable non-secure protocols (on page 47).

Learn more
The following control(s) provide additional guidance:

• NIST 800-53 AC-17 Remote Access (Disable Unused Protocols)
• NIST 800-53 CM-6 Configuration Settings
• NIST 800-53 CM-7 Least Functionality

5.7. Log Server

5.7.1. Install Log Server on a separate SQL Server

Sony recommends that you install the Log Server on a separate SQL Server. If the Log Server is affected by a performance issue, for example, due to flooding or other reasons, and uses the same database as the management server, both can be affected.

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 SC-7 Boundary Protection
• NIST SP 800-53 CM-9 Configuration Management Plan

5.7.2. Limit the IP access to Log Server

Sony recommends that only VMS components can contact the Log Server. Log Server uses port 80.

Learn more
The following control(s) provide additional guidance:

• NIST 800-53 CM-6 Configuration Settings
• NIST 800-53 CM-7 Least Functionality
6. Client programs

This section provides guidance about how to protect the Sony client programs. The client programs are:

- Network Video Management System Smart Client
- Network Video Management System Web Client
- Network Video Management System Management Client
- Network Video Management System Mobile client

6.1. Basic steps (all client programs)

6.1.1. Use Windows users with AD

Sony recommends that, whenever possible, you use Windows users in combination with Active Directory (AD) to log in to the VMS with the client programs. This enables you to enforce a password policy, and apply user settings consistently across the domain and network. It also provides protection against brute force attacks. For more information, see Use Windows users with Active Directory (AD) (see "Use Windows users with Active Directory" on page 16).

Learn more
The following control(s) provide additional guidance:

- NIST 800-53 CM-6 Configuration Settings
- NIST 800-53 SA-5 Information System Documentation
- NIST 800-53 SA-13 Trustworthiness

6.1.2. Restrict permissions for client users

Sony recommends that administrators specify what users can do in Management Client or Network Video Management System Smart Client. The following instructions describe how to do this. To restrict client user permissions, follow these steps:
1. Open Management Client.

2. Expand the Security node, select Roles, and then select the role that the user is associated with.

3. On the tabs at the bottom, you can set permissions and restrictions for the role.

By default, all users associated with the Administrator role have unrestricted access to the system. This includes users who are associated with the Administrator role in AD as well as those with the role of administrator on the management server.

**Learn more**

The following documents provide additional information:

- NIST 800-53 AC-4 *Least Privilege*
- NIST 800-53 CM-6 *Configuration Settings*
6.1.3. Always run clients on trusted hardware on trusted networks

Sony recommends that you always run Network Video Management System clients on hardware devices with the proper security settings. Specific guidance for mobile devices is available in SP 800-124. These settings are specific to the device.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 Boundary Protection
- NIST SP800-53 CM-6 Configuration Settings

6.2. Network Video Management System Smart Client - advanced steps

6.2.1. Restrict physical access to any computer running Network Video Management System Smart Client

Sony recommends that you restrict physical access to computers running Network Video Management System Smart Client. Allow only authorized personnel to access the computers. For example, keep the door locked, and use access controls and surveillance.

Learn more

The following control(s) provide additional guidance:

- NIST SP 800-53 PE-1 Physical and Environmental Protection Policy and Procedures
- NIST SP 800-53 PE-2 Physical Access Authorizations
- NIST SP 800-53 PE-3 Physical Access Control
- NIST SP 800-53 PE-6 Monitoring Physical Access

6.2.2. Always use a secure connection by default, particularly over public networks

If you need to access the VMS with Network Video Management System Smart Client over a public or untrusted network, Sony recommends that you use a secure connection through VPN. This helps ensure that communication between Network Video Management System Smart Client and the VMS server is protected.
Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 AC-17 Remote Access
- NIST SP 800-53 CM-6 Configuration Settings

6.2.3. Activate login authorization

Login authorization requires a user to log in on Network Video Management System Smart Client or Management Client, and another user who has an elevated status, such as a supervisor, to provide approval.

You set up login authorization on the roles. Users associated with the role are prompted for a second user (a supervisor) to authorize their access to the system.

Login authorization is currently not supported by mobile client, Network Video Management System Web Client, and any MIP SDK integrations.

To turn on login authorization for a role, follow these steps:

1. Open Management Client.
2. Expand the Security node, select Roles, and then select the relevant role.

   Select the Login authorization required check box.
To configure the roles that authorize and grant access, follow these steps:

1. To create a new role, for example "Security supervisor", expand the Security node, right-click Roles and create a new role.

2. Click the Overall Security tab, and select the Management Server node. Select the Allow check box next to the Authorize users check box.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 AC-6 Least Privilege
- NIST SP 800-53 AC-17 Remote Access
• NIST SP 800-53 CM-6 *Configuration Settings*
6.2.4. Do not store passwords

Network Video Management System Smart Client provides the option to remember passwords for users. To reduce the risk of unauthorized access, Sony recommends that you do not use this feature.

To turn off the remember password feature, follow these steps:

1. Open Management Client.
2. Expand the Client node, select Smart Client Profiles, and then select the relevant Smart Client profile.
3. In the Remember password list, select Unavailable.

The Remember password option is not available the next time a user with this profile logs into Network Video Management System Smart Client.

Learn more

The following control(s) provide additional guidance:
• NIST SP 800-53 AC-2 **Account Management**
• NIST SP 800-53 CM-6 **Configuration Settings**
• NIST SP 800-53 IA-1 **Identification and Authentication Policy and Procedures**

### 6.2.5. Turn on only required client features

Turn on only required features, and turn off features that a surveillance operator does not need. The point is to limit opportunities for misuse or mistakes.

You can turn on and turn off features in Network Video Management System Smart Client and in Network Video Management System Management Client.

In Management Client, configure Smart Client profiles to specify sets of permissions for users who are assigned to the profile.

To configure a Smart Client profile, follow these steps:

1. Open Management Client.
2. Expand the **Client** node, select **Smart Client Profiles**, and then select the relevant Smart Client profile.
3. Use the tabs to specify settings for features in Smart Client. For example, use the settings on the Playback tab to control features used to investigate recorded video.

Before you assign a user to a Smart Client profile, ensure that the permissions for the user’s role are appropriate for the profile. For example, if you want a user to be able to investigate video, make sure that the role allows the user to play back video from cameras, and that Sequence Explorer tab is available on the Smart Client profile.

**Learn more**
The following control(s) provide additional guidance:

• NIST SP 800-53 AC-2 **Account Management**
• NIST SP 800-53 AC-6 **Least Privilege**
• NIST SP 800-53 CM-6 **Configuration Settings**

### 6.2.6. Use separate names for user accounts

Sony recommends that you create a user account for each user, and use a naming convention that makes it easy to identify the user personally, such as their name or initials. This is a best practice for limiting access to only what is necessary, and it also reduces confusion when auditing.

**Learn more**
The following control(s) provide additional guidance:

- NIST 800-53 AC-4 **Least Privilege**
- NIST 800-53 CM-1 **Configuration Management Policy and Procedures**
- NIST 800-53 CM-2 **Baseline Configuration**
- NIST 800-53 CM-6 **Configuration Settings**
- NIST 800-53 CM-7 **Least Functionality**

### 6.2.7. Prohibit the use of removable media

For video exports, establish a chain of procedures that are specific to evidence. Sony recommends that the security policy allows only authorized Network Video Management System Smart Client operators to connect removable storage devices such as USB flash drives, SD cards, and smartphones to the computer where Network Video Management System Smart Client is installed.

Removable media can transfer malware to the network, and subject video to unauthorized distribution.

Alternatively, the security policy can specify that users can export evidence only to a specific location on the network, or to a media burner only. You can control this through the Smart Client profile.

**Learn more**

The following control(s) provide additional guidance:

- NIST SO 800-53 MP-7 **Media Use**
- NIST SP 800-53 SI-3 **Malicious Code Protection**

### 6.3. Sony Mobile client - advanced steps

SP 800-124 revision 1 provides guidance that is specifically for mobile devices. The information it contains applies to all topics in this section.

#### 6.3.1. Always use the Sony Mobile client on secure devices

Sony recommends that you always use the Sony Mobile client on secure devices that are configured and maintained according to a security policy. For example, ensure that mobile devices do not allow users to install software from unauthorized sources. An enterprise app store is one example of a way to constrain device applications as part of overall mobile device management.
Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 Boundary Protection
- NIST SP 800-53 CM-6 Configuration Settings

6.3.2. Download the Sony Mobile client from authorized sources

Sony recommends that you download the Sony Mobile client from one of these sources:

- Google Play Store
- Apple App Store

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 SC-7 Boundary Protection
- NIST SP 800-53 CM-6 Configuration Settings

6.3.3. Mobile devices should be secured

If you want to access the VMS with a mobile device over a public or untrusted network, Sony recommends that you do so with a secure connection, use proper authentication and Transport Layer Security (TLS) (or connect through VPN) and HTTPS. This helps protect communications between the mobile device and the VMS.

Sony recommends that mobile devices use screen-lock. This helps prevent unauthorized access to the VMS, for example, if the smart phone is lost. For maximum security, implement a security policy to prohibit the Sony Mobile client from remembering the user name and password.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 AC-17 Remote Access
- NIST SP 800-53 CM-6 Configuration Settings
6.4. Network Video Management System Web Client - advanced steps

6.4.1. Always run Network Video Management System Web Client on trusted client computers

Always securely connect all components of the VMS. Server-to-server and client-to-server connections should use HTTPS and the latest TLS. Always run Network Video Management System Web Client on trusted computers, for example, do not use a client computer in a public space. Sony recommends that you educate users about the security measures to remember when using browser-based applications, such as Network Video Management System Web Client. For example, make sure they know to disallow the browser from remembering their password.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 CM-6 Configuration Settings
- NIST SP 800-53 IA-2 Identification and Authentication

6.4.2. Use certificates to confirm the identity of a Sony Mobile server

This document emphasizes the use of the latest TLS. With that comes the need for the proper use of certificates and the implementation of the TLS cipher suite. Sony recommends that you install a certificate on the Sony Mobile server to confirm the identity of the server when a user tries to connect through Network Video Management System Web Client.

For more information, see the Edit certificates section in the Sony Mobile Server 2016 - Administrator Guide.

Learn more
The following control(s) provide additional guidance:

- NIST SP 800-53 AC-2 Account Management
- NIST SP 800-53 CM-6 Configuration Settings
- NIST SP 800-53 IA-2 Identification and Authentication

6.4.3. Use only supported browsers with the latest security updates

Sony recommends that you install only one of the following browsers on client computers. Make sure to include the latest security updates.
• Apple Safari
• Google Chrome
• Microsoft Internet Explorer
• Mozilla Firefox

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 CM-1 Configuration Management Policy and Procedures
• NIST SP 800-53 CM-2 Baseline Configuration
• NIST SP 800-53 CM-6 Configuration Settings
• NIST SP 800-53 PL-8 Information Security Architecture
• NIST SP 800-53 SI-3 Malicious Code Protection

6.4.4. Run the Management Client on trusted and secure networks

If you access the Management Server with Management Client over HTTP, the plain text communication can contain unencrypted system details. Sony recommends that you run the Management Client only on trusted and known networks. Use a VPN to provide remote access.

Learn more
The following control(s) provide additional guidance:

• NIST SP 800-53 AC-2 Account Management
• NIST SP 800-53 CM-6 Configuration Settings
• NIST SP 800-53 IA-2 Identification and Authentication
7. Appendix 1 - Resources

1. Axis Communications: Hardening Guide  

2. Bosch Security Systems: Bosch IP Video and Data Security Guidebook  

   Standards/  
   Describes the minimum requirements for a video surveillance system. See also related standards.


5. Cloud Security Alliance (CSA) and the Cloud Controls Matrix


7. Internet Engineering Task Force (IETF), multiple references


9. ISO/IEC 31000, Risk management – Principles and guidelines  
   http://www.iso.org/iso/home/standards/iso31000.htm

10. ISO/IEC 31010, Risk management – Risk assessment techniques  
    http://www.iso.org/iso/catalogue_detail?csnumber=51073

11. ISO 27001: A standard and framework for managing threats in an information security management system (ISMS) http://www.iso.org/iso/iso27001


   See also Why We’re Not Recommending "FIPS Mode" Anymore


15. National Institute of Standards and Technology: Cybersecurity Framework
    http://www.nist.gov/cyberframework/


17. National Institute of Standards and Technology: Managing Information Security Risk

    http://dx.doi.org/10.6028/nist.sp.800-53r4 and Pre-Draft Revision 5
    http://csrc.nist.gov/groups/sma/fisma/sp800-53r5_pre-draft.html


20. NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise

21. SANS institute website and the SANS Critical Security Controls
8. Appendix 2 - Acronyms

AD – Active Directory
CSA – Cloud Security Alliance
CVE – Common Vulnerabilities and Exposures
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Secure
IEC – International Electrotechnical Commission
IETF – Internet Engineering Task Force
IP – Internet Protocol
ISO – International Standards Organization
IT – Information Technology
KB – Knowledge Base
NIST – National Institute of Standards and Technology
RSTP – Rapid Spanning Tree Protocol
SMTP – Simple Mail Transfer Protocol
SSL – Secure Socket Layer
STIG – Security Technical Information Guide
TCP – Transmission Control Protocol
TLS - Transport Layer Security
UDP – User Datagram Protocol
VMS – Video Management Software
VPN – Virtual Private Network
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018/03/02</td>
<td>1.0.0</td>
<td>First edition.</td>
</tr>
</tbody>
</table>
Disclaimer
This document, in whole or in part, may not be reproduced or transferred for any purpose without prior written approval from Sony Corporation. Sony Corporation reserves the right to make any modification to this document or the information contained herein at any time without notice. Sony Corporation shall not bear any responsibility or liability for any damage, lost earning, and third party claim, resulting from the products and related documents.

Copyright
This document contains registered trademarks and trademarks that are owned by their respective companies.