



# DELL PowerFlex Rack Security Configuration with PowerFlex 4.x User Guide

[Home](#) » [Dell](#) » DELL PowerFlex Rack Security Configuration with PowerFlex 4.x User Guide 

## Contents

- [1 DELL PowerFlex Rack Security Configuration with PowerFlex 4.x](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Notes, cautions, and warnings](#)
- [5 Introduction](#)
- [6 Security considerations](#)
- [7 Authentication and authorization](#)
- [8 PowerFlex Manager local user access](#)
- [9 Dell PowerSwitch switches](#)
- [10 Auditing and logging](#)
- [11 Documents / Resources](#)
  - [11.1 References](#)
- [12 Related Posts](#)



**DELL PowerFlex Rack Security Configuration with PowerFlex 4.x**



## Product Information

The Dell PowerFlex Rack with PowerFlex 4.x is a security-focused product designed to provide users with a secure and reliable deployment model. The product includes features such as administrative control, network security, and management stack protection to ensure the safety of data and resources. It also integrates common security technologies and provides guidance related to specific compliance frameworks and advanced cloud solutions.

## Notes, Cautions, and Warnings

- **Note:** Important information to help you make better use of your product
- **Caution:** Indicates potential damage to hardware or loss of data and tells you how to avoid the problem
- **Warning:** Indicates a potential for property damage, personal injury, or death

## Contents

- Chapter 1: Introduction
- Chapter 2: Revision history
- Chapter 3: Disclaimer
- Chapter 4: Deployment model
- Chapter 5: Security considerations
- Chapter 6: Cloud Link Center server logs
- Chapter 7: Data security

## Product Usage Instructions

### Deployment Model

The deployment model chapter provides information on how to deploy the Dell PowerFlex Rack with PowerFlex 4.x product. It includes details on the different components and how to administer them. It also provides guidance on how to use separation of duties and minimize the use of shared credentials.

## Security Considerations

The security considerations chapter provides information on how to ensure the security of the product. It includes details on administrative control, network security, and management stack protection. It also provides guidance on how to capture event logs with a security information and event management (SIEM) system and audit all privilege and role change activity.

## Data Security

The data security chapter provides information on encryption keys and how to ensure data security. It includes guidance on how to manage encryption keys and protect them from unauthorized access. Overall, it is important to follow the instructions provided in the Dell PowerFlex Rack with PowerFlex 4.x Security Configuration Guide to ensure the safety and security of your data and resources.

## Notes, cautions, and warnings

- **NOTE:** A NOTE indicates important information that helps you make better use of your product.
- **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.
- **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

## Introduction

This guide provides a set of security best practices to enhance security for the PowerFlex rack environment. The intended audience for this guide includes those who are planning, implementing, administering, or auditing security controls in a PowerFlex rack environment. The primary audience is technical, but the document addresses the needs of a range of security program professionals. You should have a reasonable understanding of the PowerFlex rack architecture, particularly the management infrastructure. See the Dell PowerFlex Rack with PowerFlex 4.x Architecture Overview for more information. Dell Technologies provides other assistance that might be useful in assisting with security or compliance-related issues, such as

- PowerFlex rack guidance for addressing multi-tenant concerns
- Protection of management interfaces with enhanced separation of duties, identification, authorization, auditing, and access control
- Integrating common security technologies with PowerFlex rack
- Guidance related to specific compliance frameworks and outcomes (for example, PCI, HIPAA, FISMA, and so forth)
- Guidance related to advanced cloud solutions

## Revision history

Date	Document revision	Description of changes
March 2023	1.2	Editorial updates
January 2023	1.1	Editorial updates
August 2022	1.0	Initial release

## Disclaimer

- The information in this publication is provided “as is.” Dell Technologies makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties or merchantability or fitness for a particular purpose.
- Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by Dell Technologies, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
- Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding by laws or rules of governmental agencies.

## **Deployment model**

- This guide provides a set of security best practices to enhance security for the PowerFlex rack environment.
- The Dell PowerFlex Rack with PowerFlex 4.x Architecture Overview describes the default deployment model and other deployment scenarios. These deployment options affect the security posture for PowerFlex rack and in particular the management security zone, where many security controls come into scope for deployment in your data center environment.
- For the default deployment model for PowerFlex rack, the system design assumes you will provide the network security services for protecting the management security zone. Consider deploying firewalls at the edge of the PowerFlex rack management network to provide these controls.
- This guide provides references to helpful information regarding network management interfaces, ports, and protocols required for management and administrative operations. Use this information to create a baseline firewall ruleset that can be deployed to provide required network access control for the management zone.

## **Security considerations**

### **Administrative control**

Dell Technologies takes the precaution of changing all default administrator passwords and follows a policy of creating complex passwords for all accounts controlling the management interfaces. Dell Technologies uses a more secure password storage option whenever possible. In addition to changing administrative access control default settings, Dell Technologies recommends using the following security counter measures, provided they do not conflict with your organization’s security policy

- Use LDAP server or Windows AD authentication for all PowerFlex rack components. These counter measures mitigate password-related threats with password policies and facilitate entitlements audit.
- Use low-level privilege roles for all PowerFlex rack components.
- Use separation of duties to the greatest extent feasible when administering components.
- Minimize the use of shared credentials. In particular, minimize the use of the default superuser accounts.
- Capture all event logs with a security information and event management (SIEM) system. Audit all privilege and role change activity, and set up alerts for this activity.

### **Network security**

- As with other network environments, PowerFlex rack needs to be protected from network attacks such as spoofing, traffic sniffing, and traffic tampering. All PowerFlex rack components are configured to use secure

administrative interfaces that are authenticated and encrypted. PowerFlex rack authenticates, encrypts, and segregates traffic on the management, control, and data planes.

- The default PowerFlex rack architecture separates traffic by creating distinct, dedicated network zones for control, data, VMware vSphere vMotion, backup, and other purposes. PowerFlex rack network design incorporates security best practices from the component manufacturers for both physical and virtual network components.
- If you require network segmentation beyond VLANs, you can configure PowerFlex rack to provide enhanced physical or logical separation of network zones. The standard product can support some configuration options, such as network access control lists (ACLs) on Cisco Nexus switches or VMware ESXi host firewall rule configuration. Other deployment options might require additional hardware, software, or entitlements (such as partner ecosystem solutions). For example, although not part of the standard product architecture, compatible physical or virtual firewall technology can be introduced at critical network boundaries where required, to achieve the required level of security and access control.
- Consult with your Dell Technologies account team to learn more about options for network segmentation and security.

### **Management stack protection**

Management system security is vital to the protection of PowerFlex rack and its managed components and resource pools. In addition to the authentication, authorization and accounting (AAA) controls, the following are important considerations:

- Management interfaces should have banner messages officially notifying users of monitoring, lack of privacy expectations, and civil and criminal responsibilities for malicious or damaging behavior, regardless of intent.
- Remove or disable default or well-known accounts.
- Configure management interfaces to require strong passwords.
- Configure management interfaces with a relatively short connection timeout period.
- Apply standard operations hygiene on the systems hosting management applications. For example, deploy anti-virus applications, backup procedures, and patching management.

### **Authentication and authorization**

VMware vSphere environment VMware vCenter uses single sign-on to authenticate a user based on the user's group membership. A user's role on an object or the user's global permission determines whether the user can perform other VMware vSphere tasks. For more information, see the following topics:

- vSphere Permissions and User Management tasks
- Understanding Authorization in vSphere

You can integrate VMware vCenter with Microsoft Active Directory for centralized identity and access management.

### **PowerFlex Manager local user access**

#### **User roles**

- User roles control the activities that can be performed by different types of users, depending on the activities that they perform when using PowerFlex Manager.
- The roles that can be assigned to local users and LDAP users are identical. Each user can only be assigned one role. If an LDAP user is assigned directly to a user role and also to a group role, the LDAP user will have the permissions of both roles.
  - **NOTE:** User definitions are not imported from earlier versions of PowerFlex and must be configured again.

The following table summarizes the activities that can be performed for each user role

Role	Activities
Super User	<ul style="list-style-type: none"> <li>• Manage storage resources</li> </ul>
	<ul style="list-style-type: none"> <li>• Manage lifecycle operations, resource groups, templates, deployment, backend operations</li> </ul>
A Super User can perform all system operations.	<ul style="list-style-type: none"> <li>• Manage replication operations, peer systems, RCGs</li> <li>• Manage snapshots, snapshot policies</li> </ul>
	<ul style="list-style-type: none"> <li>• Manage users, certificates</li> </ul>
	<ul style="list-style-type: none"> <li>• Replace drives</li> </ul>
	<ul style="list-style-type: none"> <li>• Hardware operations</li> </ul>
	<ul style="list-style-type: none"> <li>• View storage configurations, resource details</li> </ul>
	<ul style="list-style-type: none"> <li>• View platform configuration, resource details</li> </ul>
	<ul style="list-style-type: none"> <li>• System monitoring (events, alerts)</li> </ul>
	<ul style="list-style-type: none"> <li>• Perform serviceability operations</li> </ul>
	<ul style="list-style-type: none"> <li>• Update system settings</li> </ul>

System Admin	<ul style="list-style-type: none"> <li>• Manage storage resources</li> </ul>
	<ul style="list-style-type: none"> <li>• Manage lifecycle operations, resource groups, templates, deployment, backend operations</li> </ul>
A System Admin can perform all operations, except for user management and security ones.	<ul style="list-style-type: none"> <li>• Manage replication operations, peer systems, RCGs</li> <li>• Manage snapshots, snapshot policies</li> <li>• Replace drives</li> </ul>
	<ul style="list-style-type: none"> <li>• Hardware operations</li> </ul>
	<ul style="list-style-type: none"> <li>• View storage configurations, resource details</li> </ul>
	<ul style="list-style-type: none"> <li>• View platform configuration, resource details</li> </ul>
	<ul style="list-style-type: none"> <li>• System monitoring (events, alerts)</li> </ul>

Role	Activities
	<ul style="list-style-type: none"> <li>• Perform serviceability operations</li> <li>• Update system settings</li> </ul>
<b>Storage Admin</b> A Storage Admin can perform all storage-related front-end operations including element management of already setup NAS and block systems. For <b>example:</b> create volume, create file system, manage file-server user quotas. <b>NOTE:</b> Operations such as create storage pool, create file-server, and add NAS node cannot be performed by Storage Admin, but can be performed by the Lifecycle Admin role.	<ul style="list-style-type: none"> <li>• Manage storage resources</li> <li>• Manage replication operations, peer systems, RCGs</li> <li>• Manage snapshots, snapshot policies</li> <li>• Replace drives</li> <li>• Hardware operations</li> <li>• View storage configurations, resource details</li> <li>• View platform configuration, resource details</li> <li>• System monitoring (events, alerts)</li> </ul>

<p><b>Lifecycle Admin</b> A Lifecycle Admin can manage the life cycle of hardware and systems.</p>	<ul style="list-style-type: none"> <li>• Manage lifecycle operations, resource groups, templates, deployment, backend operations</li> <li>• Replace drives</li> <li>• Hardware operations</li> <li>• View resource groups and templates</li> <li>• System monitoring (events, alerts)</li> </ul>
<p><b>Replication Manager</b> The Replication Manager is a subset of the Storage Admin role, for work on existing systems for setup and management of replication and snapshots.</p>	<ul style="list-style-type: none"> <li>• Manage replication operations, peer systems, RCGs</li> <li>• Manage snapshots, snapshot policies</li> <li>• View storage configurations, resource details (volume, snapshot, replication views)</li> <li>• System monitoring (events, alerts)</li> </ul>
<p><b>Snapshot Manager</b> Snapshot Manager is a subset of Storage Admin, working only on existing systems. This role includes all operations required to setup and manage snapshots.</p>	<ul style="list-style-type: none"> <li>• Manage snapshots, snapshot policies</li> <li>• View storage configurations, resource details</li> <li>• System monitoring (events, alerts)</li> </ul>
<p><b>Security Admin</b> The Security Admin manages role-based access control (RBAC), and LDAP user federation. It includes all security aspects of the system.</p>	<ul style="list-style-type: none"> <li>• Manage users, certificates</li> <li>• System monitoring (events, alerts)</li> </ul>
<p><b>Technician</b> This user is allowed to do all HW FRU operations on the system. He can also perform the relevant commands for proper maintenance, such</p>	<ul style="list-style-type: none"> <li>• Replace drives</li> <li>• Hardware operations</li> <li>• System monitoring (events, alerts)</li> <li>• Perform serviceability operations</li> </ul>



Role	Activities
as entering a node into maintenance mode.	
<b>Drive Replacer</b> This is a subset of the Technician role. The Drive Replacer is a user who is only allowed to do operations required for drive replacement. For example: life cycle operations on the node, and evacuating a block system device.	<ul style="list-style-type: none"> <li>• Replace drives</li> <li>• System monitoring (events, alerts)</li> </ul>
<b>Monitor</b> The Monitor role has read-only access to the system, including topology, alerts, events, and metrics.	<ul style="list-style-type: none"> <li>• View storage configurations, resource details</li> <li>• View platform configuration, resource details</li> <li>• System monitoring (events, alerts)</li> </ul>
<b>Support</b> The Support role is a special kind of System Admin (all activities except for user/security management operations) to be used only by support staff (CX) and developers. This user role has access to undocumented, special operations and options for common operations, required only for support purposes. <b>NOTE:</b> This special role should be used only by support. It opens special, often dangerous, commands for advanced troubleshooting.	<ul style="list-style-type: none"> <li>• Manage storage resources</li> <li>• Manage lifecycle operations, resource groups, templates, deployment, backend operations</li> <li>• Manage replication operations, peer systems, RCGs</li> <li>• Manage snapshots, snapshot policies</li> <li>• Replace drives</li> <li>• Hardware operations</li> <li>• View storage configurations, resource details</li> <li>• View platform configuration, resource details</li> <li>• System monitoring (events, alerts)</li> <li>• Perform serviceability operations</li> <li>• Special Dell Technologies Support operations</li> </ul>

## Secure remote dial-in support

- PowerFlex rack uses Secure Connect Gateway to provide secure remote dial-in support from Dell Technologies Support.
- The remote service credential feature provides a mechanism to securely generate session-based authentication tokens, using a service account defined on a managed device for remote device dial-in support.

## PowerFlex default account

PowerFlex Manager has the following default account.

User account	Description
<b>Admin</b>	<ul style="list-style-type: none"> <li>PowerFlex Manager has one default account (“admin”) with default password Admin123!. Use the Web UI when you are logging in for the first time. You must replace the password after the initial deployment is complete.</li> <li>This account is a Super User, and provides full administrator privileges to all configuration and monitoring activities.</li> </ul>

User accounts are kept local or through LDAP. For information on user role mapping, see the Dell PowerFlex 4.0.x Security Configuration Guide.

## PowerFlex nodes

- You can set up user accounts with specific privileges (role-based authority) to manage your PowerFlex nodes using Integrated Dell Remote Access Controller (iDRAC).
- Set up local users or use directory services such as Microsoft Active Directory or LDAP to set up user accounts.
- iDRAC supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read-only, or none. The role defines the maximum privileges available.
- For more information, see the Integrated Dell Remote Access Controller User’s Guide.

## Embedded operating system-based jump server default accounts

The embedded operating system-based management jump server uses the following default accounts:

User account	Description
admin	Account used for remote login through SSH or VNC
root	Root SSH is disabled by default

SSH and GUI (VNC) access is enabled by default for the embedded operating system-based jump server.

## Dell PowerSwitch switches

PowerSwitch switches use OS10 as the operating system. OS10 supports two default users

- admin – used to sign in to the CLI
- linuxadmin – used to access the Linux shell

To disable the linuxadmin user

- Enter CONFIGURATION mode.
- Enter this command: OS10(config)# system-user linuxadmin disable

## Role-based access for PowerSwitch switches

- PowerSwitch switches support role-based access control.
- The following table summarizes the roles to which a user can be assigned

User account	Description
sysadmin	System administrator

User account	Description
	<ul style="list-style-type: none"><li>• Full access to all system commands and the system shell</li><li>• Exclusive access to commands that manipulate the file system</li><li>• Can create user IDs and user roles</li></ul>
<b>secadmin</b>	<b>Security administrator</b> <ul style="list-style-type: none"><li>• Full access to configuration commands that set security policy and system access, such as password strength, AAA authorization, and cryptographic keys</li><li>• Can display security information, such as cryptographic keys, login statistics, and log information</li></ul>
<b>netadmin</b>	<b>Network administrator</b> <ul style="list-style-type: none"><li>• Full access to configuration commands that manage traffic flowing through the switch, such as routes, interfaces, and ACLs</li><li>• Cannot access configuration commands for security features</li><li>• Cannot view security information</li></ul>
<b>netoperator</b>	<b>Network operator</b> <ul style="list-style-type: none"><li>• Access to EXEC mode to view the current configuration</li><li>• Cannot modify any configuration setting on a switch</li></ul>

## Privilege levels for PowerSwitch switches

Use privilege levels to limit user access to a subset of commands. The following table describes the supported privilege levels:

Level	Description
0	Provides users the least privilege, restricting access to basic commands
1	Provides access to a set of show commands and certain operations, such as ping, traceroute, and so on
15	Provides access to all available commands for a particular user role
0, 1, and 15	System-configured privilege levels with a predefined command set
2 to 14	Not configured; you can customize these levels for different users and access rights.

For additional information, see the OS10 Enterprise Edition User Guide.

### Dell CloudLink

Each CloudLink user is assigned a role that determines their permissions in CloudLink Center. The following table lists the default CloudLink Center user accounts:

User account	Description	Default password
root	Operating system root account	None
secadmin	Used for the CloudLink Center administrator through the web user interface	None; user must set the password at initial login

CloudLink supports different types of authentication methods through

- Local user accounts on CloudLink Center server
  - Windows Active Directory LDAP or LDAPs service
  - Multi-factor authentication using either Google Authenticator or RSA SecurID for local or Windows domain users
- CloudLink support role-based access for user accounts. For more information, see the Dell CloudLink Administration Guide

### Microsoft Windows Server 2019-based PowerFlex compute-only nodes configuration

This section contains authentication and authorization configuration details for Windows Server 2019-based PowerFlex compute-only nodes.

#### Disable the built-in guest account

Use this procedure to disable the built-in guest account.

##### Steps

1. In the Run window, enter gpedit.msc and click OK. The Local Group Policy Editor is displayed.
2. In the left pane, click Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
3. In the Policy pane, double-click Accounts: Guest account status and select Disabled.
4. Click OK.

#### Enable the password complexity policy

Use this procedure to enable the password complexity policy.

## Steps

1. In the Run window, enter gpedit.msc and click OK. The Local Group Policy Editor is displayed.
2. In the left pane, click Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.
3. In the Policy pane, double-click Password must meet complexity requirements and select Enabled.
4. Click OK.

### Configure the minimum password length

Use this procedure to configure the Windows Server 2019 minimum password length.

#### Steps

1. In the Run window, enter gpedit.msc and click OK. The Local Group Policy Editor is displayed.
2. In the left pane, click Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.
3. In the Policy pane, double-click Minimum password length and change Password must be at least: to 14 characters.
4. Click OK.

### Disable the Server Message Block

Use this procedure to disable the Server Message Block (SMB) v1.

#### Steps

1. Open the Server Manager, and select the server with the feature.
2. On the header, click Manager. Select Remove Roles and Features from the drop-down list.
3. In the Select destination server window, select the appropriate server from the Server Selection section and click Next.
4. Click Next.
  1. The Features page is displayed.
5. Search for SMB 1.0/CIFS File Sharing Support and do one of the following
  1. If the SMB 1.0/CIFS File Sharing Support check box is clear, click Cancel.
  2. If the SMB 1.0/CIFS File Sharing Support check box is selected, clear the check box and click Next > Remove.

### Set inactivity limit and screen saver

Use this procedure to set the inactivity limit to 15 minutes or less. This locks the system with a screen saver.

#### Steps

1. In the Run window, enter gpedit.msc and click OK.
  1. The Local Group Policy Editor is displayed.
2. In the left pane, click Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. The Policy is displayed on the right pane.
3. In the Policy pane, double-click Interactive logon: Machine inactivity limit and set Machine will be locked after to 900 seconds or less (excluding 0).
4. Click OK.

## Restrict access

Use this procedure to restrict access from the network to only administrators, authenticated users, and enterprise domain controllers groups on domain controllers.

### Steps

1. In the Run window, enter gpedit.msc and click OK.
  1. The Local Group Policy Editor is displayed.
2. In the left pane, click Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.
3. In the Policy pane, double-click Access this computer from the network and select Administrators, Authenticated Users, and Enterprise Domain Controllers only.

**NOTE:** To select multiple accounts or groups, press Ctrl and click the accounts or groups you want to select.
4. Click OK.

## Auditing and logging

### System alerts

- PowerFlex Manager displays all alerts generated by the system components such as block, file services, nodes, and switches. You can view the system alerts by using PowerFlex Manager, API, or CLI.
- Set the notification policies to send the alerts to email, SNMP traps, and external syslog. For more information, see Add a notification policy.
- You can modify the severity level of the system alerts. Factory-defined alerts are sent to Dell Technologies, along with the original factory-defined severity data for root cause analysis. For other purposes, user-defined severity levels are used.

### Add a notification policy

When you add a notification policy, you define the rules for processing events or alerts from sources, and to which destinations that information should be sent.

### Steps

1. Go to Settings > Events and Alerts > Notification Policies.
2. Click Create New Policy.
3. Enter a name and a description for the notification policy.
4. From the Resource Domain menu, select the resource domain that you want to add a notification policy to. The resource domain options are:
  - All
  - Management
  - Block (Storage)
  - File (Storage)
  - Compute (Servers, Operating Systems, virtualization)
  - Network (Switches, connectivity etc.)
  - Security (RBAC, certificates, CloudLink etc.)
5. From the Source Type menu, select how you want events and alerts to be received. The source type options are:
  - Snmpv2c

- Snmpv3
- Syslog
- Powerflex

6. Select the check box beside the severity levels that you want to associate with this policy. The severity indicates the risk (if any) to the system, in relation to the changes that generated the event message.
7. Select the required destination and click Submit.

### **Modify a notification policy**

You can modify certain settings that are associated with a notification policy.

#### **About this task**

You cannot modify the source type or destination once it is assigned to a notification policy.

#### **Steps**

1. Go to Settings > Events and Alerts > Notification Policies.
2. Select the notification policy that you want to modify.
3. You can choose to modify the notification policy in the following ways:
  - To activate or deactivate the policy, click Active.
  - To modify the policy, click Modify. The Edit Notification Policy window opens.
4. Click Submit.

### **Delete a notification policy**

Once a notification policy is deleted, it cannot be recovered.

#### **About this task**

To delete a notification policy

#### **Steps**

1. Go to Settings > Events and Alerts > Notification Policies.
2. Select the notification policy that you want to delete.
3. Click Delete. You receive an information message asking if you are sure that you want to delete the policy.
4. Click Submit and click Dismiss.

### **System event logs**

- PowerFlex Manager displays the system event logs generated by system components, hardware, and software stacks. You can view the system events log using PowerFlex Manager, REST API, or CLI.
- The retention policy for system events logs is 13 months or 3 million events. You can set the notification policies to send the system events log to email or redirect to syslog. For more information, see Add a notification policy.

### **Application logs**

Application logs are low-level logs of system components. These are mostly useful for root cause analysis. Secure connect gateway enables secure, high-speed, 24×7, remote connection between Dell Technologies and customer installations, including:

- Remote monitoring

- Remote diagnosis and repair
- Daily sending of system events (syslog output), alerts, and PowerFlex topology.

PowerFlex sends data to CloudIQ through Secure connect gateway. To enable the data transfer to CloudIQ, configure Support Assist and make sure that Connect to CloudIQ option is enabled. For information, see Enabling SupportAssist in the Dell PowerFlex 4.0.x Administration Guide.

The following table describes various logs collected by different components

Component	Location
<b>MDM log</b> <ul style="list-style-type: none"> <li>• The logs do not contain any user data (as the user data does not pass through the MDM)</li> <li>• The logs may contain the MDM user names (but never passwords)</li> </ul>	Linux: /opt/emc/scaleio/mdm/logs

Component	Location
IP addresses, MDM configuration commands, events, and so forth.	
LIA logs	Linux: /opt/emc/scaleio/lia/logs

### Log management and retrieval

You can manage and retrieve logs in various ways:

- Viewing MDM application logs locally—Use the `showevents.py` command, using filter switches to control the severity of alerts.
- Get Info—Get Info allows you to assemble a ZIP file of system logs for troubleshooting. You can run this function from a local node for its own logs, or by using PowerFlex Manager to assemble logs from all system components.

### VMware vSphere environment

For more information on VMware vSphere ESXi and vCenter Server log management, see the appropriate VMware vSphere Security audit logging section.

### Dell iDRAC server logs

For information on iDRAC server logs, see the Integrated Dell Remote Access Controller User's Guide.

### PowerSwitch switch logs

PowerSwitch switches support audit and security logs.



Log type	Description
Audit	<p>Contains configuration events and information, including</p> <ul style="list-style-type: none"> <li>• User logins to the switch</li> <li>• System events for network or system issues</li> <li>• User configuration changes, including who made the change and the change date and time</li> <li>• Uncontrolled shutdown</li> </ul>
Security	<p>Contains security events and information, including</p> <ul style="list-style-type: none"> <li>• Establishment of secure traffic flows, such as SSH</li> <li>• Violations on secure flows or certificate issues</li> <li>• Adding and deleting of users</li> <li>• User access and configuration changes to security and crypto parameters</li> </ul>

Role-based access control (RBAC) restricts access to audit and security logs, based on the CLI session user role. Enabling RBAC is recommended when enabling audit and security logs. When RBAC is enabled:

- Only the system administrator user role can run the command to enable logging.
- The system administrator and system security administrator user roles can view security events and system events.
- The system administrator user role can view audit, security, and system events.
- Only the system administrator and security administrator user roles can view security logs.
- The network administrator and network operator roles can view system events.

You can configure a remote syslog server to receive system messages from PowerSwitch switches. See the Dell Configuration Guide for the particular switch for detailed information.

### CloudLink Center server logs

Events are logged and can be accessed through the CloudLink Center management interface. The CloudLink Center server logs security events including:

- User logins
- Failed attempts to unlock the CloudLink Vault using a passcode
- Machine registrations
- Changes to the CloudLink Vault mode
- Successful or failed attempts to perform a secure user action
- Key activities, such as requests, updates, or moves

Use a web browser to view these events in the CloudLink Center management interface. These events can also be sent to a defined syslog server.

### Data security

CloudLink provides policy-based key management and data-at-rest-encryption for both virtual machines and PowerFlex devices. CloudLink has two data security components:

Component	Description
CloudLink Center	<p>Web-based interface that manages the CloudLink environment</p> <ul style="list-style-type: none"><li>• Manages the encryption keys used to secure the devices for the protected machines</li><li>• Configures security policies</li><li>• Monitors security and operations events</li><li>• Collects logs</li></ul>
CloudLink SecureVM agent	<ul style="list-style-type: none"><li>• Agent software deployed on storage data server (SDS), VMware ESXi SVM, or physical Linux machine.</li><li>• It communicates to the CloudLink Center for pre-startup authorization and decryption of dm-crypt encryption keys.</li></ul>

### Encryption keys

CloudLink uses two types of encryption keys to secure machines that use software-based storage encryption

Key	Description
Device/volume key encryption key (VKEK)	CloudLink generates a VKEK pair for each device.
Device encryption key	CloudLink generates a unique device encryption key for each encrypted device. Native technologies in the machine's operating system use the encryption key.

CloudLink Center manages self-encrypting drives (SED). A CloudLink-managed SED is locked. CloudLink Center must release the encryption key to unlock the SED.

- **Ports and authentication protocols**

For the list of PowerFlex Manager ports and protocols, see the Dell PowerFlex 4.0.x Security Configuration Guide.

- **VMware vSphere ports and protocols**

This section contains information for VMware vSphere ports and protocols.

- **VMware vSphere 7.0**

For information about ports and protocols for VMware vCenter Server and VMware ESXi hosts, see VMware Ports and Protocols.

- **CloudLink Center ports and protocols**

CloudLink Center uses the following ports and protocols for data communication

Port	Protocol	Port type	Direction	Use
80	HTTP	TCP	Inbound/outbound	CloudLink agent download and cluster communication
443	HTTPS	TCP	Inbound/outbound	CloudLink Center web access and cluster communication
1194	Proprietary over TLS 1.2	TCP, UDP	Inbound	CloudLink agent communication
5696	KMIP	TCP	Inbound	KMIP service
123	NTP	UDP	Outbound	NTP traffic
162	SNMP	UDP	Outbound	SNMP traffic
514	syslog	UDP	Outbound	Remote syslog server communication

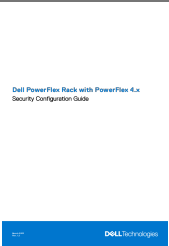
### Embedded operating system-based management jump server ports and protocols

The embedded operating system-based jump server uses the following ports and protocols for data communication:

Port	Protocol	Port type	Direction	Use
22	SSH	TCP	Inbound	Management access
5901	VNC	TCP	Inbound	Remote desktop access
5902	VNC	TCP	Inbound	Remote desktop access


© 2022- 2023 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

## Documents / Resources

	<a href="#">DELL PowerFlex Rack Security Configuration with PowerFlex 4.x</a> [pdf] User Guide PowerFlex 4.x, PowerFlex Rack with PowerFlex 4.x, PowerFlex Rack, PowerFlex Rack Security Configuration with PowerFlex 4.x, PowerFlex Rack Security Configuration
---	---

## References

-  [vSphere Permissions and User Management Tasks](#)
-  [Understanding Authorization in vSphere](#)
-  [Audit Logging](#)
-  [VMware Ports and Protocols](#)
-  [Manuals | Dell Canada](#)

-  [Support | Dell US](#)
-  [SmartFabric OS10 Info Hub | Dell Canada](#)

Manuals+.