Dell EMC PowerProtect Cyber Recovery

Version 19.3

Security Configuration Guide

REV 02

February 2020

Copyright © 2019-2020 Dell Inc. or its subsidiaries. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of the software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function correctly or does not function as described in this document.

ⓘ Note: This document was accurate at publication time. To find the latest version of this document, go to Dell EMC Online Support.

Purpose

This guide provides an overview of Dell EMC PowerProtect Cyber Recovery settings for access control, logfiles, communication, and data security. It also includes useful information about Cyber Recovery licensing and code integrity, security patches, malware protection, and manual vault security.

Audience

The information in this guide is primarily intended for Cyber Recovery administrators, users, and recovery managers.

Revision history

The following table presents the revision history of this document:

Revision	Date	Description
01	December 17, 2019	First release of Dell EMC PowerProtect Cyber Recovery 19.3
02	February 7, 2020	Added ports to the Network ports table in the Communication security settings topic.

Product Documentation

The Cyber Recovery product documentation set includes:

- Dell EMC PowerProtect Cyber Recovery Release Notes
- Dell EMC PowerProtect Cyber Recovery Installation Guide
- Dell EMC PowerProtect Cyber Recovery Product Guide
- Dell EMC PowerProtect Cyber Recovery Solutions Guide
- Dell EMC PowerProtect Cyber Recovery Security Configuration Guide
- Dell EMC PowerProtect Cyber Recovery Open Source License and Copyright Information

ⓘ Note: Also, see the documentation for the products that are integrated with Cyber Recovery, such as Dell EMC Data Domain Series Appliances, Dell EMC Avamar, Dell EMC NetWorker, and Dell EMC PowerProtect Data Manager applications.

ⓘ Note: Also, see the documentation for the products that are integrated with Cyber Recovery, such as Dell EMC Data Domain Series Appliances and Dell EMC PowerProtect Data Manager applications.

Where to get help

Go to Dell EMC Online Support to obtain Dell EMC support, and product and licensing information. You can also find documentation, release notes, software updates, or information about other Dell EMC products.

You see several options for contacting Dell EMC Technical Support. To open a service request, you must have a valid support agreement. Contact your Dell EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Comments and suggestions

Comments and suggestions help us to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision
- Page numbers
- Other details to help address documentation issues

CHAPTER 1

Introduction

This chapter includes the following topics:

About this guide

This guide provides an overview of Dell EMC PowerProtect Cyber Recovery settings for access control, log files, communication, and data security.

This guide also includes useful information about Cyber Recovery licensing and code integrity, security patches, malware protection, and manual vault security.

Cyber Recovery software

The Cyber Recovery solution minimizes the impact of a cyber-attack and provides a higher likelihood of success in the recovery of business-critical systems.

The Cyber Recovery software runs in a secure, air-gapped 'vault' environment. The Cyber Recovery Vault (CR Vault) is physically isolated from an unsecure system or network. It provides management tools and technology to automate the creation of restore points that are used for recovery or security analytics. The software is built on a secure microservices architecture.

A primary storage system replicates its data over an air-gapped link to the Cyber Recovery environment. The data that is in the CR Vault can be analyzed and checked for signs of tampering. If the copied data is deemed to be good, it is saved as an independent full backup copy that can be restored if needed. If this data must be restored, data can be sent out of the Cyber Recovery environment and back to the production environment.

With the Cyber Recovery software, you can create, run, and monitor policies that protect your data.

CHAPTER 2

Security Quick Reference

This chapter includes the following topic:

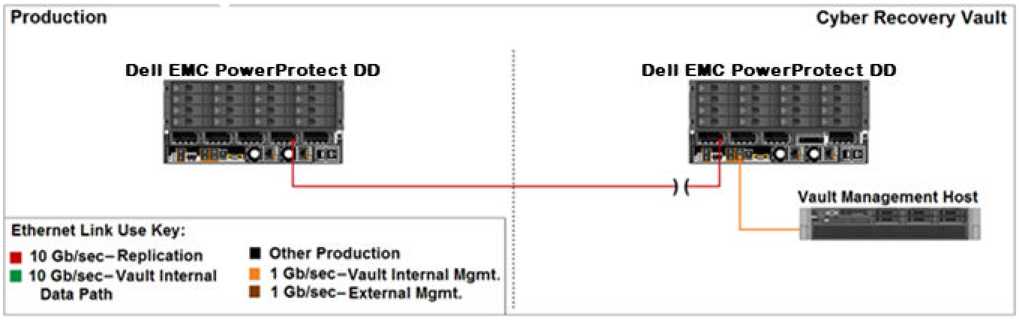
Deployment model

The Cyber Recovery Vault (CR Vault) is a highly secure part of the data center that hosts infrastructure on a dedicated and separate network. By default, the only connection between the production-side Data Domain system and the vault-side Data Domain system is the MTree replication link that is used for synchronization of data during specified intervals. By taking the target-side Data Domain replication port offline, the data link is "air gapped," which reduces the attack surface. The CR Vault infrastructure is hardened as part of the service delivery.

> **Note:** Any references to Data Domain systems in the documentation covers existing Data Domain systems as well as newer PowerProtect DD systems moving forward.

The following figure illustrates the deployment model:

Figure 1 Cyber Recovery reference architecture base



CHAPTER 3

Product and Subsystem Security

This chapter includes the following topics:

Authentication

Authentication for the Cyber Recovery deployment is based on the credentials of the user account and is implemented by using the Cyber Recovery UI, CRCLI, and REST API.

Security components

The Cyber Recovery software includes the following security components.

Users

User accounts refer to Cyber Recovery users in the CR Vault. A username, password, role, first name, last name, email address, and telephone number define each user.

Create user accounts by using the Cyber Recovery UI, CLI, or REST API. Then, define user information and roles.

Privileges

Privileges define the tasks that users can perform in the Cyber Recovery environment. Privileges are assigned to roles and are granted to users depending on their role assignment.

Privileges are assigned to user roles. They cannot be assigned directly to a user.

Roles

Roles are containers of access privileges that you assign to users. In being assigned a role, the users receive the privileges that are assigned to that role. RBAC privileges on page 21 describes the roles that are available.

Authentication

The Cyber Recovery REST API is used to provide authentication and authorization services in the CR Vault. The Cyber Recovery software uses HTTPS to secure communications between the Cyber Recovery REST API and end-user components or client applications.

Token-based authentication

Authentication in the CR Vault is performed by using tokens. This approach ensures that users can connect securely to the CR Vault and perform authorized and secure operations.

Key-based authentication

SSH enables communication with Cyber Recovery assets. When you add an asset to your Cyber Recovery environment, provide a password to establish the initial SSH connection to add the Cyber Recovery software's public key to the asset. All subsequent SSH connections use the private and public keys for authentication with the password as a backup.

Login security settings

This section describes login security settings and how these settings are configured.

Failed login behavior

To mitigate brute-force attacks on Cyber Recovery user accounts, the Cyber Recovery software applies a timeout period to an account after several incorrect login attempts.

During a timeout period, the Cyber Recovery software ignores all login attempts. The login prompt instructs you to log in again later. After 12 timeout occurrences, the account is locked unless the user is the Security Officer. This same timeout behavior occurs when the login attempt is made using the Cyber Recovery UI, CLI, or REST API.

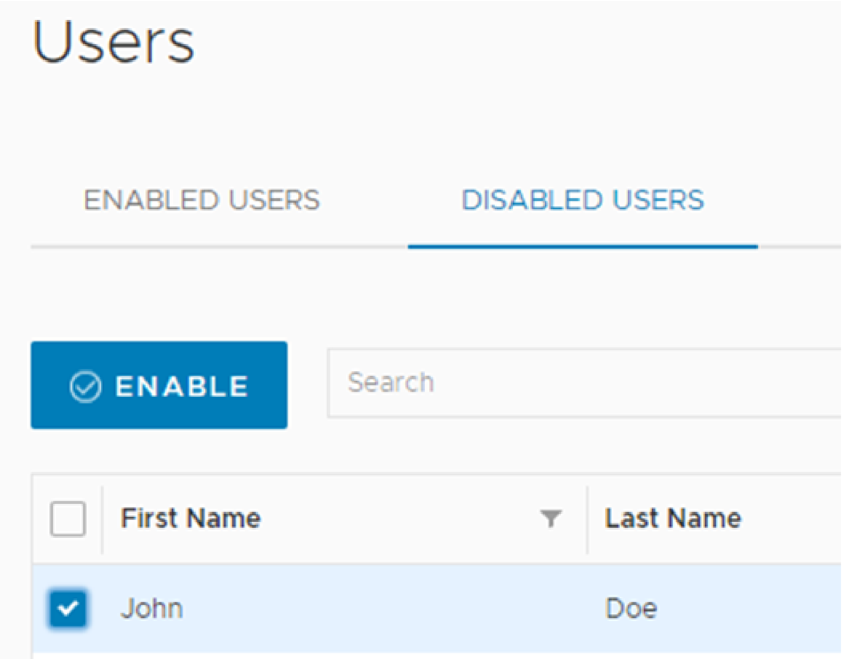
Emergency user lockout

If a Cyber Recovery user account is locked and the user requires immediate access, the Security Officer can use the Cyber Recovery UI, CLI, or REST API to grant a new password and unlock that account.

Procedure

1. Log in to the Cyber Recovery UI.
2. From the Main Menu, click **Administration** > **Users**.
3. At the top of the content pane, click **Disabled Users**.
4. Select the check box next to the user who requires access.
5. Click **Enable** to unlock the user account.

Figure 2 Users content pane: Enable a disabled user



☐	First Name	Last Name
☑	John	Doe

Configuring login count

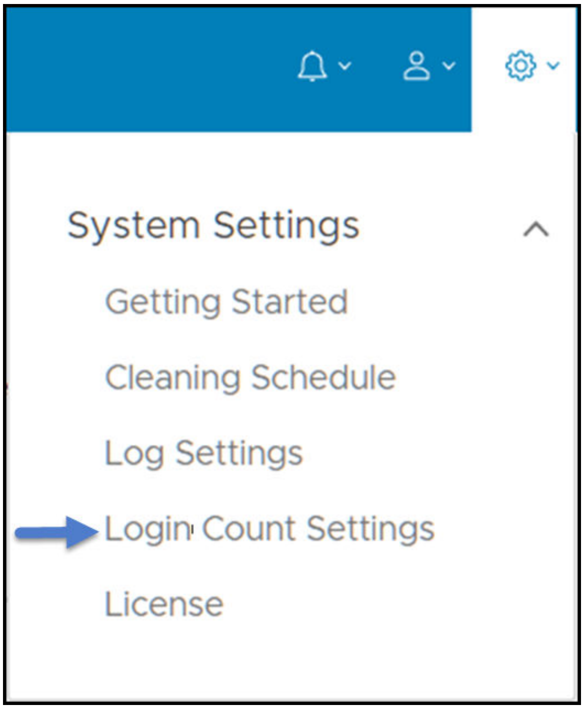
The Security Officer manages the number of simultaneous login sessions to the Cyber Recovery software.

By default, the values are:

- Security Officer—One session
- Admin user—Three sessions
- Dashboard user—Three sessions

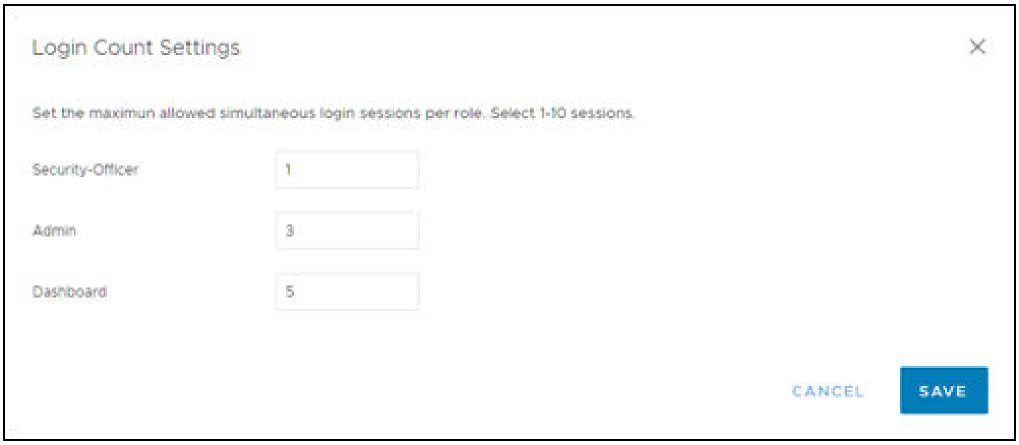
To modify the login count settings, log in as the Security Officer to the crso account. From the Masthead Navigation, select the gear icon to access the **System Settings** menu, and then click **Login Count Settings**, as shown in the following figure:

Figure 3 Login Count Settings option in the System Settings menu



The Login Count Settings window opens, as shown in the following figure:

Figure 4 Login Count Settings dialog box



Login Count Settings

Set the maximun allowed simultaneous login sessions per role. Select 1-10 sessions.

Security-Officer 1

Admin 3

Dashboard 5

The login count uses a first in, first out priority. If a specific user and role exceeds the number of simultaneous logins, that user's earliest session is no longer a valid Cyber Recovery session. When that specific session's access token for the user expires, that session's refresh token will no longer be valid to generate additional access tokens.

Configuring session timeout

Each interface has an automatic timeout setting.

The following table lists the default timeout values for the specified interfaces.

Table 1 Default timeout values

Interface	Default timeout
Access token	1 minute
Refresh token	8 hours
UI session	10 minutes
CLI session	10 minutes

You cannot modify the access and refresh token timeout values. However, you can modify the UI and CLI session timeout values. The following sections describe how to perform these tasks.

Modifying the UI session timeout value

To modify a user's UI session timeout value, complete the following steps.

Procedure

1. Log in to the Cyber Recovery UI.
2. From the Main Menu on the left, click **Administration**, and then click **Users**.
3. On the **Users** content pane, select the user.
4. Click **Edit**.
5. In the **Edit User** dialog box, select the session timeout value from the **Session Timeout** list menu.

Modifying the CLI session timeout value

To modify a user's CLI timeout value, complete the following steps:

Procedure

1. Log in to the management host.
2. Type the following command:

   ```
   export CRSESSIONTIMEOUT=<minutes>
   ```
   where *<minutes>* is a value 3 through 20.

   If there is no CLI activity for the specified period, authenticated CLI users are logged out of the Cyber Recovery environment.

User and credential management

Learn how to manage Cyber Recovery users and credentials.

Preloaded accounts

The following accounts are initialized at Cyber Recovery installation:

- Cyber Recovery accounts—The Cyber Recovery installation procedure creates the Security Officer (crso) user account that uses a password that the user provides. This user is assigned the Security Officer role and must perform the initial Cyber Recovery login and configuration. After successfully logging in, the Security Officer can create and manage Admin users.
- Operating system accounts—The Cyber Recovery installation procedure creates a system user on the management host system. The installation procedure assigns this management host system user account (cyber-recovery-admin) User ID 14999 and Group ID 14999. The management host system user owns certain Cyber Recovery files, folders, and processes within the application.

  If User ID 14999 and Group ID 14999 are allocated to another system user, the installation procedure prompts whether to continue the installation with that other system user or cancel the installation.

Default credentials

A Cyber Recovery virtual appliance deployment requires you to set a password for the root user and admin user during the Cyber Recovery installation.

The Cyber Recovery virtual appliance system uses the following default user accounts and default passwords:

User account	Default password	Description
root	**changeme**	Linux OS root account ⓘ Note: You cannot use SSH to access the root user account.
Admin	**changeme**	Linux OS administrative account ⓘ Note: You can use SSH with the Admin user account to log in to the appliance.

Disabling local accounts

The Security Officer can disable and enable users by using the Cyber Recovery UI, CLI, or REST API.

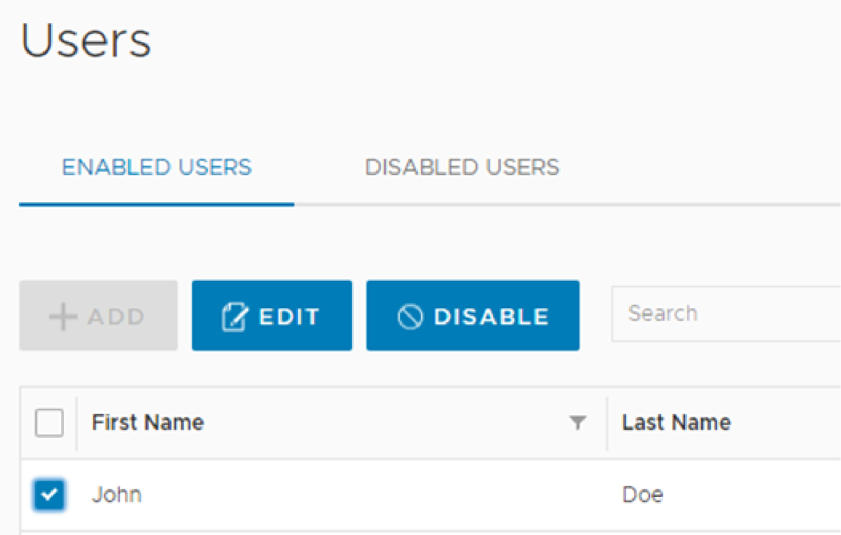
About this task

Disabled users are unable to log in to the Cyber Recovery system and cannot perform any Cyber Recovery functions.

Procedure

1. Log in to the Cyber Recovery UI.
2. From the Main Menu, click **Administration** > **Users**.
3. On the **Users** content pane, select the check box next to the user whose account you want to disable.
4. Click **Disable**.

Figure 5 Users content pane: Disable a user


Users

ENABLED USERS DISABLED USERS

□	First Name	Last Name
☑	John	Doe

Managing credentials

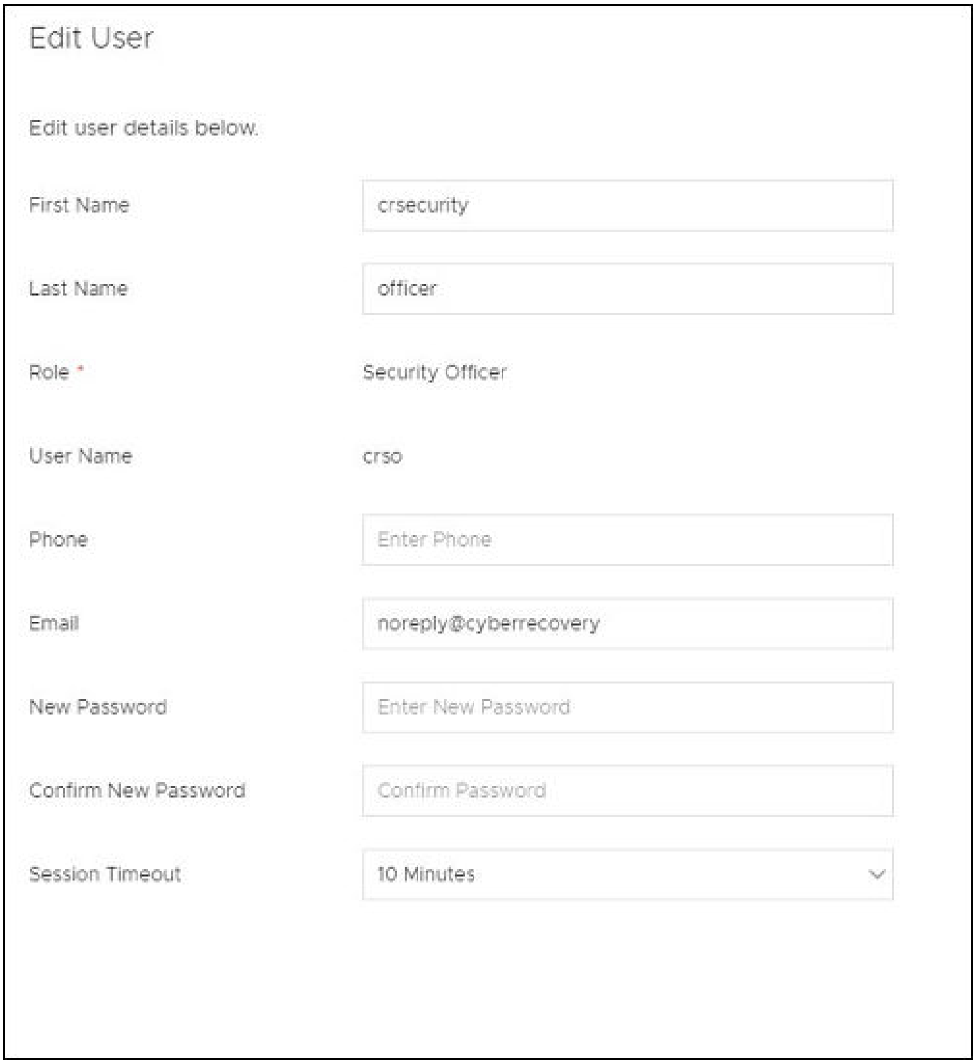
Admin users and Security Officers can change their own passwords by using the Cyber Recovery UI, CLI, or REST API. Security Officers can change their own passwords and the passwords of Admin and dashboard users.

Procedure

1. Log in to the Cyber Recovery UI.

   When the Security Officer first logs in to the Cyber Recovery UI, the **Getting Started** wizard is displayed. After the initial configuration, the Cyber Recovery dashboard is displayed.
2. From the Main Menu, click **Administration** > **Users**.
3. On the **Users** content pane, select the check box next to the user whose password you want to change.
4. Click **Edit**.
5. In the **Edit User** dialog box, enter the new password, and then confirm the password, as shown in the following figure:

Figure 6 Modifying user passwords



Edit User

Edit user details below.

First Name	crsecurity
Last Name	officer
Role *	Security Officer
User Name	crso
Phone	Enter Phone
Email	noreply@cyberrecovery
New Password	Enter New Password
Confirm New Password	Confirm Password
Session Timeout	10 Minutes

6. Click **Save**.

Password complexity

Ensure that the password meets the following requirements:

- Minimum of nine characters
- At least one numeric character (0-9)
- At least one uppercase character (A-Z)
- At least one lowercase character (a-z)
- At least one of the following special characters: (~!@#$%^&*()+={}|:";<>?[]-_.,^')

Authentication to external systems

The following sections describes how to configure authentication of supported Cyber Recovery components, also referred to as Cyber Recovery assets. Examples of these components include the Avamar, NetWorker, and PowerProtect Data Manager applications, Index Engines' CyberSense data-analysis software, and a Data Domain system.

Configuring remote connections

You can configure the Cyber Recovery deployment with remote systems to manage and audit the data flow in the CR Vault.

With the Cyber Recovery UI, CLI, and REST API, Admin users can define these supported CR Vault assets so that they are represented in the Cyber Recovery environment:

- The Storage asset is used to define the storage systems, which are Data Domain systems.
- The Application asset is used to define the:
  - Applications that are installed in the CR Vault environment, such as the Avamar, NetWorker, and PowerProtect Data Manager applications.
  - Recovery host to which the backup and application and data are recovered by using applications that are installed in the CR Vault environment.
  - Validation host on which scanning and validation is performed by using software that is installed in the CR Vault environment, such as Index Engines' CyberSense software.

See the Dell EMC PowerProtect Cyber Recovery Product Guide for more information about managing supported components.

Remote component authentication

During Cyber Recovery remote configuration with other systems in the CR Vault, information such as credentials for the remote hosts is required to perform successful authentication and configuration. By using the Cyber Recovery UI, CLI, or REST API, you can make changes.

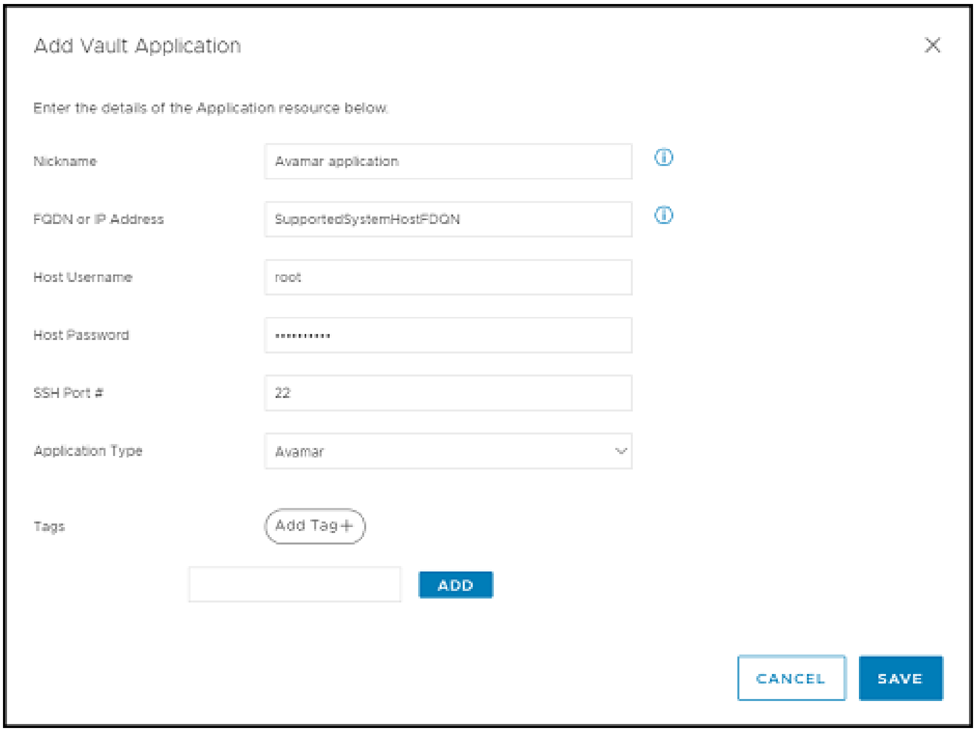
Adding a supported component

Learn how to add a supported component to the CR Vault.

Procedure

1. Log in to the Cyber Recovery UI.
2. From the Main Menu, click **Assets**.
3. On the **Assets** page, click **Applications**.
4. Click **Add**.
5. In the **Add Vault Application** window, enter information about the system, as shown in the following figure.

Figure 7 Adding a supported component



Add Vault Application

Enter the details of the Application resource below.

Nickname	Avamar application
FQDN or IP Address	SupportedSystemHostFDQN
Host Username	root
Host Password	••••••••••
SSH Port #	22
Application Type	Avamar
Tags	Add Tag+

Removing a supported component

You can remove an online and available asset from the **Assets** page in the Cyber Recovery UI. To remove an offline and unavailable asset, use the Cyber Recovery CLI.

About this task

To remove an added component in the CR Vault by using the CLI:

Procedure

1. Log in to the Cyber Recovery CLI:

   ```
   crcli login --username <admin_user>
   ```

2. To view the list of assets, type the following commands:

   ```
   crcli dd
   ```

   ```
   crcli apps list
   ```

3. Obtain the asset's nickname from the second column in the output.
4. Type either one of the following commands:

   ```
   crcli dd delete --nickname <asset_nickname>
   ```

   ```
   crcli apps delete --nickname <asset_nickname>
   ```

Authorization

The Cyber Recovery software prohibits access by unauthorized users. A user must be authenticated as either Dashboard, Admin, or Security Officer to be functional according to the role association of those users.

RBAC privileges

Role-based access control (RBAC) assigns privileges to users through roles. The default roles that the Cyber Recovery software uses are described in the following topic.

Default roles

The following table shows the default RBAC roles.

Table 2 Default roles

Role	Description
Dashboard	The dashboard user enables users to view the Cyber Recovery dashboard but not perform tasks. The dashboard does not time out.
Admin	The Admin role manages all Cyber Recovery operations. The Security Officer (crso) account adds users and assigns them to the Admin role. Admin users can change their own passwords, but not the passwords that belong to other Admin users.
Security Officer	The Security Officer is recognized as the superuser account and can perform all Admin role functions. The Security Officer can also create additional Admin accounts and change passwords for any user. The Security Officer role is the default role at installation. The username is crso and uses a password that is set during the Cyber Recovery installation.

Network security

Cyber Recovery includes the security of networked subsystems and interfaces.

Communication security settings

The following table provides the required and optional network ports for the Cyber Recovery deployment. Internal ports are only used and accessed in the Cyber Recovery environment. External ports enable remote connections.

Table 3 Network ports

Port	Required	Service	Direction	Description
14777	Yes	Nginx	Inbound	Provides web browsers with HTTPS access to the Cyber Recovery UI.
14778	Yes	REST API	Inbound	Provides the HTTPS connection for the user and UI REST interface.

Table 3 Network ports (continued)

Port	Required	Service	Direction	Description
14779	Yes	Cyber Recovery Docker Registry	Inbound	Used to upload or download the Docker container images. The installation and upgrade scripts retrieve the images from the registry, if needed.
14780	No	Swagger	Inbound	Provides access to the Cyber Recovery REST API documentation.
27017	Yes	MongoDB	Inbound	Provides access to the database that holds Cyber Recovery configurations
22	Yes	SSH	Outbound	Provides bi-directional communication between the SSH client and the remote systems in the CR Vault.
25	No	Notifications	Outbound	Used for SMTP email notifications about alerts and events.
111	Yes	NFS Client	Inbound/ Outbound	Used to perform NFS mounts between the Data Domain system and the Cyber Recovery management host.
2049	Yes	NFS Client	Inbound/ Outbound	Used to perform NFS mounts between the Data Domain system and the Cyber Recovery management host.
2052	Yes	NFS Client	Outbound	Used to mount to the Data Domain system.
5000	Yes	Cyber Recovery Docker Registry	Inbound	Used to upload or download the Docker container images. The installation and upgrade scripts retrieve the images from the registry, if needed.

Disable all network ports and interfaces that are not required for your environment.

Data security settings

Cyber Recovery microservices communicate with the MongoDB database to access policies and other persisted data. The database is password-protected and only accessible by the microservices that run in the environment.

Data-at-rest encryption

The Cyber Recovery software uses a lockbox resource to securely store sensitive information, such as credentials for application resources and databases. The lockbox securely manages sensitive information by storing the information in an encrypted format. The lockbox operates in Federal Information Processing Standards (FIPS) mode. As a result, only FIPS-approved algorithms are available for use.

Data integrity

Data Domain replication encrypts data in flight, which securely encapsulates its replication payload during transmission. For more information about the Data Domain replication security configuration, see the *Dell EMC DD OS, PowerProtect DD Virtual Edition, and PowerProtect DD Management Center Security Configuration Guide*.

You can also create a sandbox environment in the Cyber Recovery UI to inspect any replicated data, as described in Authentication to external systems on page 18. For more information about the sandbox functionality, see the Dell EMC PowerProtect Cyber Recovery Product Guide.

Cryptography

The Cyber Recovery software initiates and accepts connections by using the TLS 1.2 cryptographic protocol. Older versions of TLS and SSL have been disabled to prevent known vulnerabilities and downgrade attacks. This configuration provides a higher level of security and is compatible with modern browsers and clients.

Auditing and logging

This section describes how Cyber Recovery logs events and protects against tampering. The Cyber Recovery software has auditing, events, and logging capabilities.

The Cyber Recovery dashboard provides a high-level status of the CR Vault. It enables you to access more comprehensive details in the form of alerts, CR Vault status, and jobs that are related to point-in-time copies.

Log management

Use the Cyber Recovery UI, CLI, or REST API to change between INFO and DEBUG log levels. The default configuration is INFO.

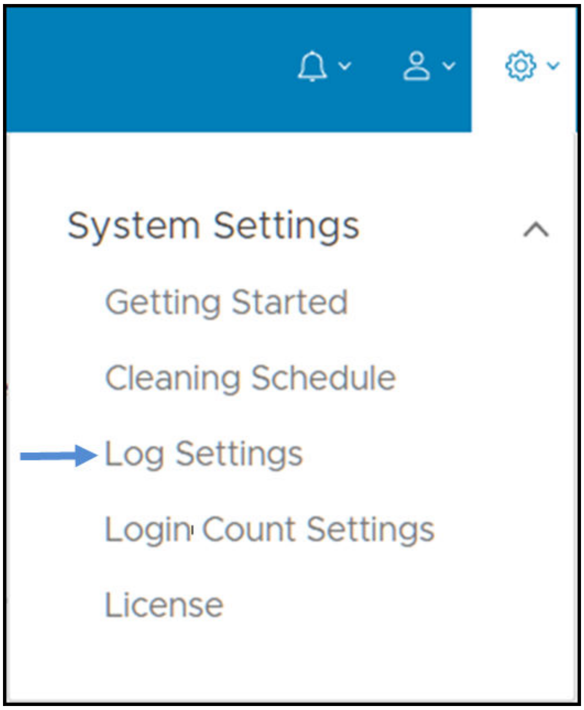
On the Cyber Recovery virtual appliance, log files reside in the `/var/log/dellemc/cr/var/log` directory.

If installed on a virtual machine with a supported operating system, the log files reside in the `/opt/dellemc/cr/var/log` directory.

Generating a log bundle

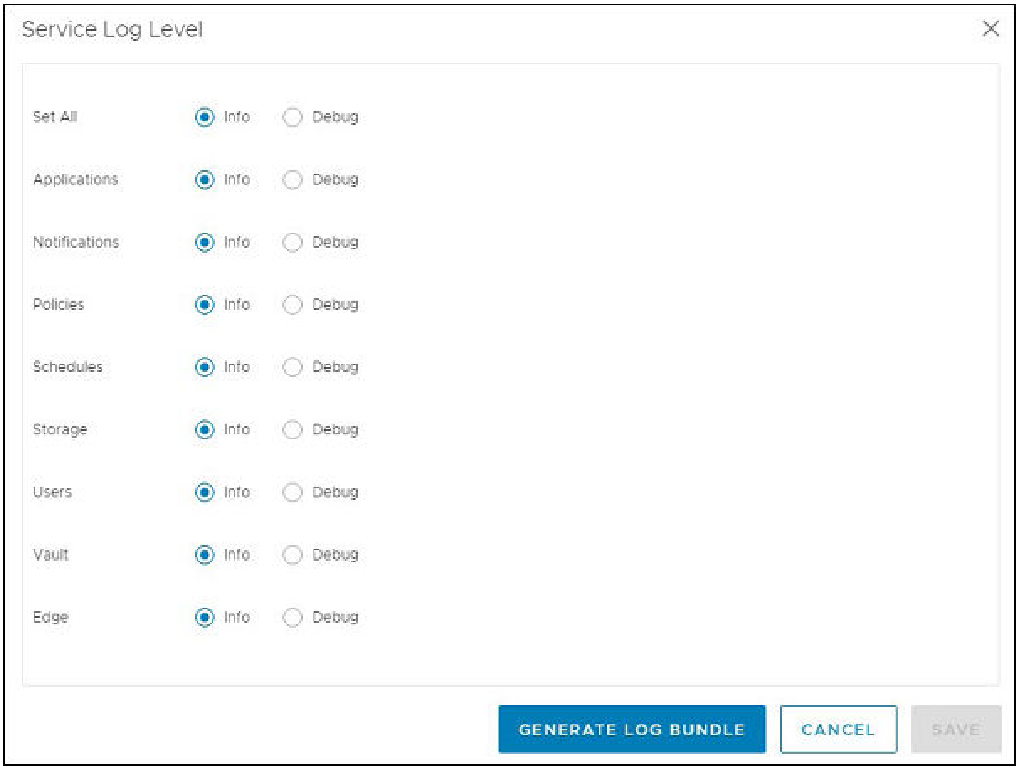
Generate a log bundle by clicking the **System Settings** icon on the Masthead Navigation and selecting **Log Settings** from the drop-down list, as shown in the following figure:

Figure 8 Log Settings option in the System Settings menu



The **Service Log Level** dialog box is displayed, as shown in the following figure:

Figure 9 Service Log Level dialog box



Service Log Level

Set All ● Info ○ Debug

Applications ● Info ○ Debug

Notifications ● Info ○ Debug

Policies ● Info ○ Debug

Schedules ● Info ○ Debug

Storage ● Info ○ Debug

Users ● Info ○ Debug

Vault ● Info ○ Debug

Edge ● Info ○ Debug

Log format

All Cyber Recovery log files use the following log message format:

```
[<date/time>] [<error type>] <microservice name> [<source file name>:
<line number>] : message
```

For example:

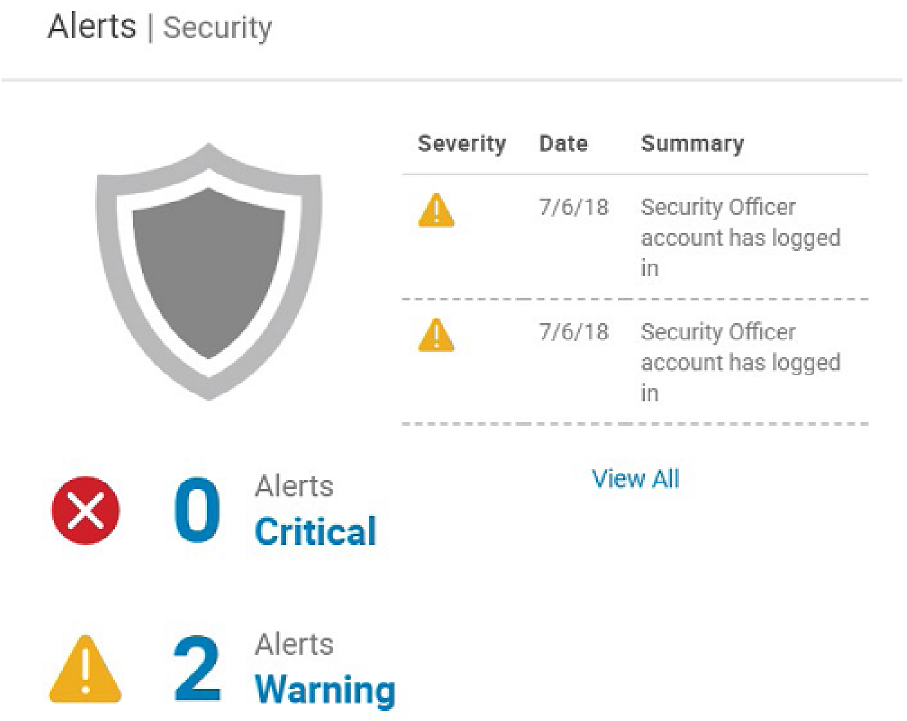
```
[2018-05-22 09:12:20] [DEBUG] [mgmtdds] [restapi_client.go:268
CallRESTAPIHeader()] : status = 200 OK
```

Alerting

Alerts enable you to identify anomalies in CR Vault activity. These anomalies can be a result of replication and analysis jobs.

The **Alerts** panel in the Cyber Recovery dashboard provides alert information, as shown in the following illustration. To view additional alert details, click any of the hyperlinks on the **Alerts and Events** panel.

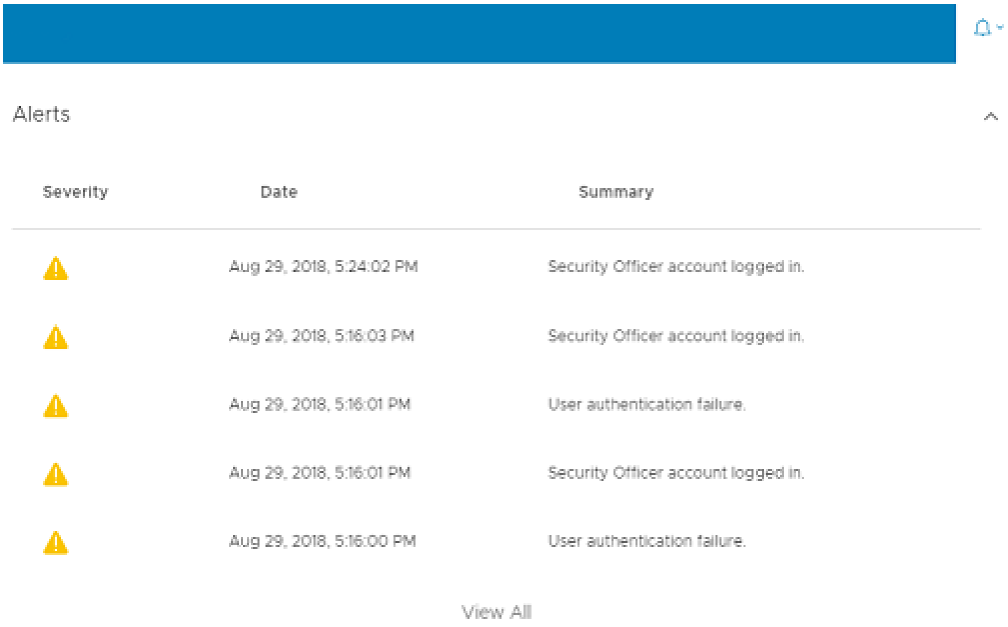
Figure 10 Alerts that are displayed on the dashboard



Severity	Date	Summary
⚠	7/6/18	Security Officer account has logged in
⚠	7/6/18	Security Officer account has logged in

Alternatively, click **Alerts and Events** in the Main Menu to view alert details. You can also click the bell icon on the Masthead Navigation to access the alerts shortcut, as shown in the following illustration.

Figure 11 Accessing alerts through the Alerts and Events shortcut



Alerts

Severity	Date	Summary
⚠	Aug 29, 2018, 5:24:02 PM	Security Officer account logged in.
⚠	Aug 29, 2018, 5:16:03 PM	Security Officer account logged in.
⚠	Aug 29, 2018, 5:16:01 PM	User authentication failure.
⚠	Aug 29, 2018, 5:16:01 PM	Security Officer account logged in.
⚠	Aug 29, 2018, 5:16:00 PM	User authentication failure.

Serviceability

The CR Vault has no remote access capabilities and, therefore, does not support the current implementation of Dell EMC Secure Remote Services (formerly EMC Secure Remote Services, or ESRS).

Security patches

Dell EMC periodically provides cumulative Cyber Recovery security updates. A security advisory announces each periodic update and provides details and installation instructions.

To view these advisories or to register for email notifications, go to Dell EMC Online Support.

Prevent malware

The Cyber Recovery software enables the administrator to add any number of validation hosts that scan replicated copies for any traces of malware. The Admin user can configure a validation host through the Cyber Recovery UI, CLI, or REST API.

Manual CR Vault security

The Data Domain system's Ethernet interface enables data to be replicated from the production system to the CR Vault when a synchronization job is run.

Policies can be run manually or scheduled to synchronize regularly. Each synchronization job triggers the opening and closing of the CR Vault through the Data Domain replication Ethernet interface, as needed. On completion of the replication, the CR Vault Data Domain system's replication Ethernet interface returns to a closed state.

The following table describes the connection states:

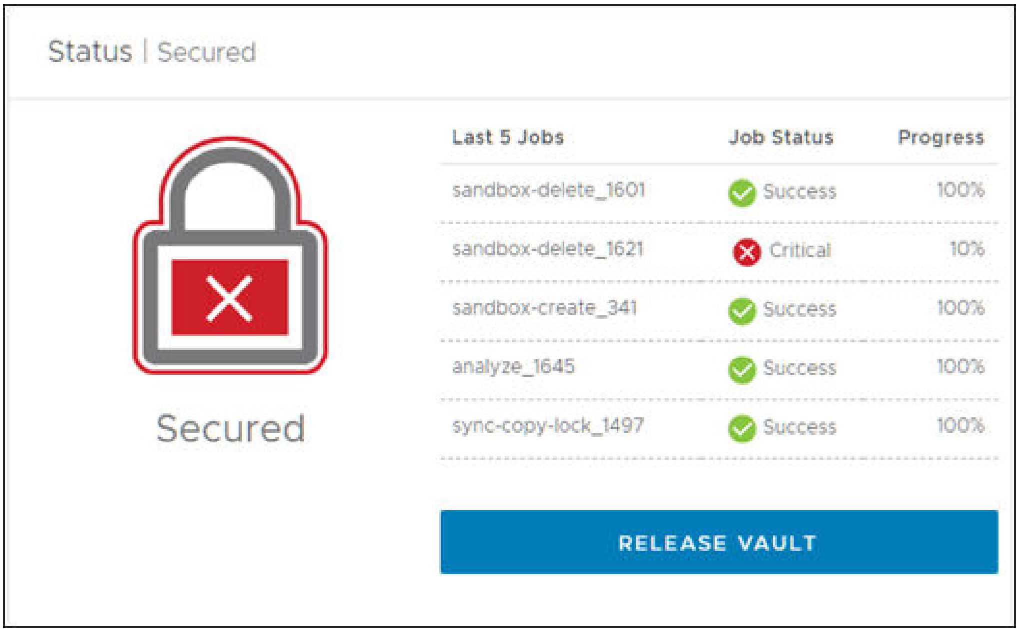
Table 4 Cyber Recovery connection states

Status	Icon	Description
Locked	✓	All configured replication connections are closed because no replication is being performed. If a replication policy is run, the Cyber Recovery software opens the connection and changes the vault state to Unlocked.
Unlocked	⇄	One or more replication network connections are open because a replication is being performed. The state returns to Locked when the replication completes.
Secured	✕	All replication network connections are secured because the Security Officer or an Admin user manually locked the connection due to a security breach. You cannot initiate any replication policy actions. When the CR Vault is released and returns to the Locked state, you can then run replication policies.
Degraded	⦸	If there are multiple Data Domain systems in the CR Vault and one Data Domain system is unable to communicate with the Cyber Recovery software, the vault status is Degraded. This scenario can occur if you change either the FQDN or the IP address of the Data Domain system. An alert notifies you about the CR Vault status.
Unknown	?	If there are multiple Data Domain systems in the CR Vault and all the Data Domain systems are unable to communicate with the Cyber Recovery software, the vault status is Unknown. This scenario can occur when you first install the Cyber Recovery software or if you change either the FQDNs or IP addresses of the Data Domain systems. An alert notifies you about the CR Vault status.

Manually securing and releasing the CR Vault

Usually, Dell EMC recommends that you open and close the CR Vault by running jobs for the policies. However, if a network event occurs when the CR Vault is open, the Security Officer and Admin users can secure the CR Vault manually to secure the environment. The secure CR Vault action runs immediately to switch the CR Vault to a secured state. The closed lock icon with an X indicates that the CR Vault has been manually secured and locked, as shown in the following figure:

Figure 12 Manually secured and locked CR Vault



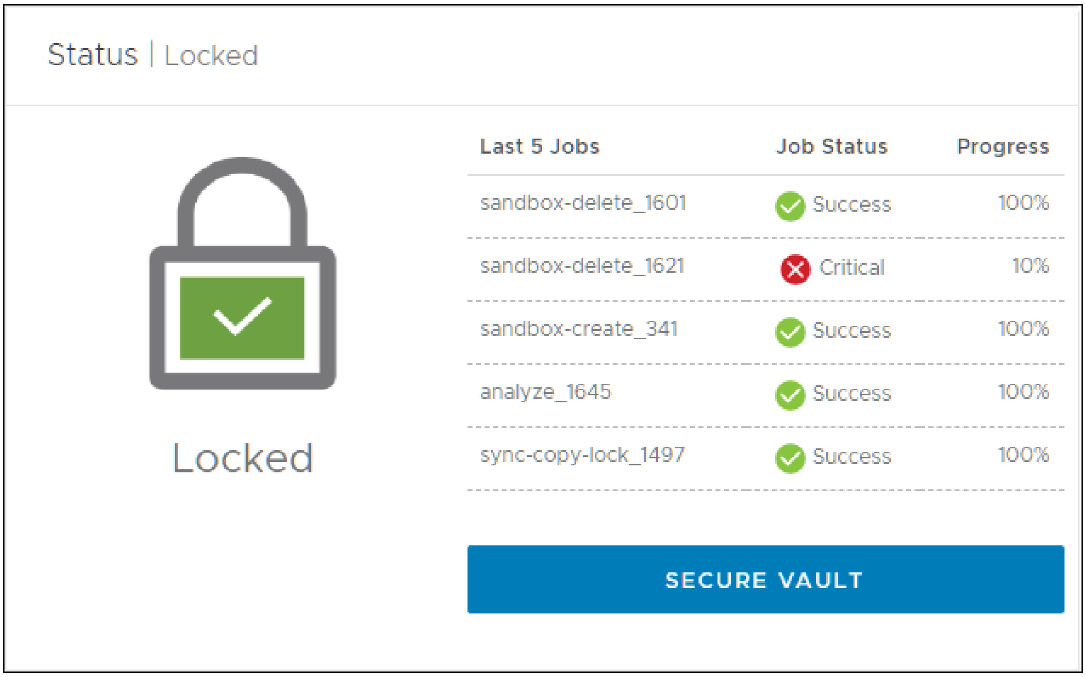
Status | Secured

Secured

Last 5 Jobs	Job Status	Progress
sandbox-delete_1601	✓ Success	100%
sandbox-delete_1621	☒ Critical	10%
sandbox-create_341	✓ Success	100%
analyze_1645	✓ Success	100%
sync-copy-lock_1497	✓ Success	100%

After you secure the CR Vault manually and complete the inspection of the network, release the CR Vault to resume normal operations. The closed lock icon with a check mark indicates that the CR Vault is operating normally and is locked, as shown in the following figure:

Figure 13 Normally operating and locked CR Vault



Status | Locked

Locked

Last 5 Jobs	Job Status	Progress
sandbox-delete_1601	✓ Success	100%
sandbox-delete_1621	☒ Critical	10%
sandbox-create_341	✓ Success	100%
analyze_1645	✓ Success	100%
sync-copy-lock_1497	✓ Success	100%

CHAPTER 4

Miscellaneous Configuration and Management

This chapter includes the following topics:

Firewall configuration

If you use an Cyber Recovery virtual appliance file to deploy the Cyber Recovery software in a VMware ESXi environment, the SuSEfirewall2 service is used as the default firewall. The rules are located in the `/opt/dellemc/firewall/scripts/SuSEfirewall2-dellemc-custom` file.

ⓘ **Note:** If the firewall rules change due to a SuSEfirewall2 service stop or restart, restart the Docker service so that the Docker network rules are reapplied.

Cyber Recovery licensing

Cyber Recovery license activation is performed through Electronic Licensing Management System (ELMS) during fulfillment of the software.

You can activate the license from the Cyber Recovery UI or the CLI as described in the following sections.

Activate the license from the Cyber Recovery UI

Learn how to activate the license from the Cyber Recovery UI.

Before you begin

To acquire a license, first install the Cyber Recovery software and retrieve the Software Instance ID by clicking either the information icon or the **System Settings** drop-down list on the Masthead Navigation. Provide the Software Instance ID to Dell EMC so that ELMS can generate a license file. Then, using the license file, activate your license through the Cyber Recovery UI, CLI, or REST API.

Procedure

1. Log in to the Cyber Recovery UI as the Security Officer (crso).
2. From the Masthead Navigation, click the gear icon to access the **System Settings** list.
3. Choose **License** from the drop-down list.
4. Click **Choose File** to upload the license file.

Activate the license from CLI

Learn how to activate the license from the CLI.

Before you begin

To acquire a license, first install the Cyber Recovery software and retrieve the Software Instance ID by clicking either the information icon or the **System Settings** drop-down list on the Masthead Navigation. Provide the Software Instance ID to Dell EMC so that ELMS can generate a license file. Then, using the license file, activate your license through the Cyber Recovery UI, CLI, or REST API.

Procedure

1. Log in to the Cyber Recovery CLI (crcli).
2. Type the following commands:

   a. **`crcli login --username crso`**

b.

```
crcli license add --location <path to license file>
```

c.

```
crcli license show
```

Authenticity and integrity of Cyber Recovery code

Digital signing and cryptographic checksums ensure the authenticity and integrity of product modules.

The Cyber Recovery software uses code signing to guarantee the integrity and authenticity of binaries that Dell EMC provides. Code signing adds a digital signature to product artifacts such as drivers, binary files, or configuration files to authenticate the origin of the artifact and provide a claim of integrity by Dell EMC.