CONTENTS

Chapter 1  Security Quick Reference  9
High level architecture................................................................. 10
Deployment methods......................................................................... 11
Security profiles............................................................................... 11
Certificate management................................................................. 11
Generate a self-sign certificate.................................................... 11
Generate a Certificate Signing Request................................. 12

Chapter 2  Product and Subsystem Security  15
Authentication....................................................................................... 16
Login security settings................................................................. 16
Authentication types and setup considerations.......................... 17
Authentication to external systems.............................................. 18
Authorization......................................................................................... 18
Network security.................................................................................. 18
External ports that have SSL enabled......................................... 18
Internal ports that are listening only to the local interface......... 18
Data security....................................................................................... 19
Cryptography....................................................................................... 19
Auditing and logging........................................................................... 19
Security patches.................................................................................. 20

Chapter 3  Miscellaneous Configuration and Management  21
Licensing........................................................................................... 22
Protect authenticity and integrity .................................................. 22
Perform backups and restores of Data Protection Central................. 22
Embedded component usage ......................................................... 22
As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

**Note**

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website at https://support.emc.com.

**Purpose**

This document includes information about security features and capabilities of Data Protection Central.

**Audience**

This document is intended for individuals who are responsible for managing security for Data Protection Central.

**Revision history**

The following table presents the revision history of this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>July 9, 2018</td>
<td>This release includes the following revisions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the &quot;Reset the <a href="mailto:administrator@dpc.local">administrator@dpc.local</a> password&quot; procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated the Avamar to Data Protection Central data communication port number in &quot;External ports that have SSL enabled&quot;</td>
</tr>
<tr>
<td>01</td>
<td>March 9, 2018</td>
<td>Initial release of the Data Protection Central 1.0 Security Configuration Guide.</td>
</tr>
</tbody>
</table>

**Related Documentation**

For information about Data Protection Central compatibility, refer to the Data Protection Central Release Notes.

The Data Protection Central documentation set includes the following publications:

- *Data Protection Central Getting Started Guide*
- *Data Protection Central Security Configuration Guide*
- *Data Protection Central Release Notes*
- *Data Protection Central Administration Guide*

The documentation for the following products includes more information:
Special notice conventions that are used in this document
The following conventions are used for special notices:

**NOTICE**

Identifies content that warns of potential business or data loss.

---

**Note**

Contains information that is incidental, but not essential, to the topic.

Typographical conventions
The following type style conventions are used in this document:

**Table 2 Style conventions**

<table>
<thead>
<tr>
<th>Style</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Used for full titles of publications that are referenced in text.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Used for:</td>
</tr>
<tr>
<td></td>
<td>- System code</td>
</tr>
<tr>
<td></td>
<td>- System output, such as an error message or script</td>
</tr>
<tr>
<td></td>
<td>- Pathnames, file names, file name extensions, prompts, and syntax</td>
</tr>
<tr>
<td></td>
<td>- Commands and options</td>
</tr>
<tr>
<td><strong>Monospace italic</strong></td>
<td>Used for variables.</td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
<td>Used for user input.</td>
</tr>
<tr>
<td><strong>[]</strong></td>
<td>Square brackets enclose optional values.</td>
</tr>
<tr>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td><strong>{}</strong></td>
<td>Braces enclose content that the user must specify, such as x, y, or z.</td>
</tr>
<tr>
<td><strong>...</strong></td>
<td>Ellipses indicate non-essential information that is omitted from the example.</td>
</tr>
</tbody>
</table>

You can use the following resources to find more information about this product, obtain support, and provide feedback.

**Where to find product documentation**

- [https://support.emc.com](https://support.emc.com)
- [https://community.emc.com](https://community.emc.com)
Where to get support
The Support website at https://support.emc.com provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact Support.

To access a product specific Support page:

1. Go to https://support.emc.com/products.
2. In the Find a Product by Name box, type a product name, and then select the product from the list that appears.
3. Click the following button:

4. (Optional) To add the product to My Saved Products, in the product specific page, click Add to My Saved Products.

Knowledgebase
The Knowledgebase contains applicable solutions that you can search for by solution number, for example, 123456, or by keyword.

To search the Knowledgebase:

2. Click Advanced Search.
   The screen refreshes and filter options appear.
3. In the Search Support or Find Service Request by Number box, type a solution number or keywords.
4. (Optional) To limit the search to specific products, type a product name in the Scope by product box, and then select the product from the list that appears.
5. In the Scope by resource list box, select Knowledgebase.
   The Knowledgebase Advanced Search panel appears.
6. (Optional) Specify other filters or advanced options.
7. Click the following button:

Live chat
To participate in a live interactive chat with a support agent:

2. Click Chat with Support.

Service requests
To obtain in-depth help from Support, submit a service request. To submit a service request:

2. Click Create a Service Request.

Note
To create a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request:
2. Click Manage service requests.

Online communities
Go to the Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all products.

How to provide feedback
Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.
CHAPTER 1

Security Quick Reference

Topics include:

- High level architecture ................................................................. 10
- Deployment methods ................................................................. 11
- Security profiles ........................................................................ 11
High level architecture

Data Protection Central runs on virtual servers, supporting Avamar servers and Data Domain backup targets.

Each Avamar uses a Data Protection Central DPC adapter to send alerts and events to RabbitMQ, which is the message queue system.

The Data Protection Central monitoring service saves the alert and event data from RabbitMQ to the MongoDB database.

The Data Protection Central UI provides a centralized location for monitoring of alerts and events as well as providing management capabilities.

All system credentials are stored within the Data Protection Central lockbox.

The following figure displays the Data Protection Central high level architecture.
Deployment methods

Data Protection Central is deployed with the Data Protection Central OVA.

Security profiles

The Data Protection Central default security profile is secure. Certificates may be replaced.

Certificate management

Consider the following when managing certificates:

- Certificates are used for secure http access (https).
- By default, Data Protection Central generates a default SSL self-signed certificate in the following location:
  `/var/lib/dpc/webcerts`
- The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server.
- The self-signed certificate cannot be used for authentication.
- Consider company policies when creating certificates.
- You can create a self-signed certificate.
- You can create a certificate that is signed by a trusted certificate authority (CA) vendor.

Generate a self-sign certificate

To enable a secure browser connection, create a private key and a self-sign certificate.

Procedure

1. To connect to the Data Protection Central server as an admin user, run the following command:

   ```
   ssh admin@SERVER
   ```

2. To change to the root user, run the following command:

   ```
   su -
   ```

3. To change the directory to `/var/lib/dpc/webcerts`, run the following command:

   ```
   cd /var/lib/dpc/webcerts
   ```
4. To generate a new certificate, run the following command:

```bash
openssl req -newkey rsa:2048 -sha256 -x509 -keyout private-key.pem -out cert.pem -nodes -days 3650
```

5. Set the owner and group of the new certificate files to the following:

```bash
chown admin *.pem
```

6. Restart NGINX.

```bash
systemctl restart nginx
```

7. To verify the new self-sign certificate, browse Data Protection Central.

**Generate a Certificate Signing Request**

To enable a secure browser connection, generate a Certificate Signing Request (CSR).

**Procedure**

1. To connect to the Data Protection Central server as an admin user, type the following command:

```bash
ssh admin@SERVER
```

2. To change to the root user, type the following command:

```bash
su -
```

3. To change the directory to `/var/lib/dpc/webcerts`, type the following command:

```bash
cd /var/lib/dpc/webcerts
```

4. To generate a new certificate using the private key at the self-sign step, type the following command:

```bash
openssl req -newkey rsa:2048 -sha256 -key private-key.pem -out cert.csr
```

5. Send the `cert.csr` to a certificate authority (CA) vendor.

6. Replace the current `cert.pem` file to the certificate received from the CA vendor.
7. Restart NGINX.

```
systemctl restart nginx
```

8. To verify the new certificate, browse Data Protection Central.
CHAPTER 2

Product and Subsystem Security

Topics include:

- Authentication ................................................................. 16
- Authorization ........................................................................ 18
- Network security ................................................................. 18
- Data security ........................................................................ 19
- Cryptography ....................................................................... 19
- Auditing and logging .......................................................... 19
- Security patches ............................................................... 20
Authentication

Learn about authentication in Data Protection Central.

Login security settings

Data Protection Central includes login security settings.

Access control

Access control settings provide protection of resources against unauthorized access.

Data Protection Central includes a single account, for logging in to the user interface.

The username of this internal account is:

administrator@dpc.local

The administrator@dpc.local account has all rights within the Data Protection Central application.

On initial log in to Data Protection Central, the user is prompted to change the password.

Default accounts

The following table includes the Data Protection Central default accounts and passwords.

<table>
<thead>
<tr>
<th>User account</th>
<th>Password</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web and browser admin</td>
<td>The admin password is set when Data Protection Central is deployed. The account is <a href="mailto:administrator@dpc.local">administrator@dpc.local</a> and the default password is secret.</td>
<td>The default user for Data Protection Central web application administration.</td>
</tr>
<tr>
<td>Linux OS admin</td>
<td>The admin password is set when Data Protection Central is deployed. The account is admin and the default password is changeme. This user account is for an OVA/VM deployment only.</td>
<td>The default user for Data Protection Central OS-level administration. Only admin can log in using secure shell. After 5 failed login tries, the admin account is locked out.</td>
</tr>
<tr>
<td>Linux OS root</td>
<td>The default password is changeme.</td>
<td>Root operation system account. This account is for an OVA deployment only.</td>
</tr>
</tbody>
</table>

NOTICE

After completing the Data Protection Central deployment, it is recommended that you change the default passwords.

To change the password for the admin and root accounts, use the UNIX passwd command.
Only the admin account can log in using a secure shell (ssh).

**Failed login behavior**

Data Protection Central includes security settings for when there are multiple unsuccessful authentication occurrences.

After five failed SSH login tries, the username is locked out on the OVA.

The web account cannot be locked out.

**Reset the administrator@dpc.local password**

If required, you can reset the administrator@dpc.local password to the default password. The default password is *secret*.

**Procedure**

1. To stop the msm-elg.service, type the following command:

   ```bash
   systemctl stop msm-elg.service
   ```

2. To change the directory, type the following command:

   ```bash
   cd /usr/local/dpc/lib/elg
   ```

3. To delete the account, type the following command:

   ```bash
   bin/elgcli --deleteUserAccount
   ```

4. To start the msm-elg.service, type the following command:

   ```bash
   systemctl start msm-elg.service
   ```

**Authentication types and setup considerations**

Learn about authentication types and setup considerations in Data Protection Central.

Consider the following:

- **Http Basic AUTH (RFC 2617)** is used for authentication.
- The default provider root password is stored in a configuration file.
- To reset the local and default account, edit the configuration file, and then restart the server.
- Data Protection Central can be configured to authenticate through a specified LDAP server. The *Data Protection Central Getting Started Guide* provides LDAP configuration details.
- The password that is entered during the OVA deployment is stored in a configuration file. On the first start up, the password is stored in an encrypted
format in the Data Protection Central lockbox, and then the configuration file is deleted.

Authentication to external systems

Data Protection Central includes features to monitor and manage external data protection resources, such as Avamar. To access these data protection resources, Data Protection Central requires credentials for the external system. Data Protection Central stores these credentials securely.

Authorization

Data Protection Central supports a single administrative role. When the Data Protection Central administrator logs in, they have access to all Data Protection Central features and functions.

The administrator also has access to the configured external data protection resources.

Membership in the dp_admin group is required for a Data Protection Central administrator. Add any users that require access to Data Protection Central to the dp_admin group.

Network security

Learn about network security in Data Protection Central.

External ports that have SSL enabled

Learn about the Data Protection Central external ports that have SSL enabled.

The ports that are listed in the following table are the Data Protection Central external ports that have SSL enabled.

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>User web access</td>
<td>443, 80</td>
</tr>
<tr>
<td>Avamar to Data Protection Central data communication</td>
<td>5671</td>
</tr>
</tbody>
</table>

Internal ports that are listening only to the local interface

Learn about the Data Protection Central internal ports that are listening only to the local interface.

The ports that are listed in the following table are the Data Protection Central internal ports that are listening only to the local interface.

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal nodejs web access</td>
<td>8080</td>
</tr>
<tr>
<td>internal REST API access</td>
<td>9002</td>
</tr>
</tbody>
</table>
Table 5 Internal ports (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal RabbitMQ access</td>
<td>5672</td>
</tr>
<tr>
<td>internal MongoDB database access</td>
<td>27017</td>
</tr>
</tbody>
</table>

Data security

The data that are held, managed, used, or operated on by Data Protection Central is stored and secured.

Data Protection Central does not encrypt event, or application data within MongoDB.

Data Protection Central prevents unauthorized access to the Data Protection Central system.

Cryptography

Learn about cryptography in Data Protection Central.

Data Protection Central includes cryptography for the following:

- Access control
- Authentication
- Digital signatures

Auditing and logging

Learn about auditing and logging in Data Protection Central.

The following list includes information about the Data Protection Central directory structure and log information:

- The `/var/lib/dpc` directory hosts all Data Protection Central generated data which consists of MongoDB and RabbitMQ.
- The `/var/log/dpc` directory hosts all Data Protection Central related logs including NGINX, MongoDB, and RabbitMQ.
- All Data Protection Central related logs are under:
  `/var/log/dpc/[module name]`
  - `[module name].out` files contain console logging from starting and running the module process.
  - `[module name].log` files contain logging from the module.
- All Elemental Gateway (ELG) logs are under:
  `/var/log/dpc/elg/`
- The Data Protection Central user interface (msm-ui-main service) log is under:
  `/var/log/dpc/msm-ui-main`
  This log file is small and contains information from starting the Node.js server.
- The Data Protection Central Monitoring (dpc-monitor service) logs are under:
  `/var/log/dpc/monitor`
This directory contains the rolling log files from the monitoring process.

**Security patches**

A security update for Data Protection Central may be periodically provided.

The periodic updates are cumulative.

Each periodic update is announced through a security advisory. The security advisory provides details about the contents of the periodic update and installation instructions. To view these advisories or to register for email notifications, go to the Support website at:

https://support.emc.com
CHAPTER 3

Miscellaneous Configuration and Management

Topics include:

- Licensing ............................................................................................................. 22
- Protect authenticity and integrity .................................................................... 22
- Perform backups and restores of Data Protection Central ............................ 22
- Embedded component usage ......................................................................... 22
Licensing

Data Protection Central does not require any special or additional product licensing.

Protect authenticity and integrity

To ensure product integrity, the Data Protection Central installation components are signed.
Enable external web access with SSL using a trusted certificate authority (CA).

Perform backups and restores of Data Protection Central

To protect Data Protection Central from a disaster scenario, it is recommended that you perform backups of Data Protection Central. If required, you can restore Data Protection Central from these backups.

To perform backups and restores of Data Protection Central, it is recommended that you use vCenter. Refer to the vCenter documentation for more information.

If you are not using vCenter to perform backup and restore operations, you can also perform the following steps to backup and restore Data Protection Central.

**Procedure**

1. **Backup the** `/var/lib/dpc` **directory.**
2. **To shutdown the Data Protection Central software,** type the following command:
   ```bash
   sudo /usr/local/dpc/bin/dpc stop
   ```
3. **Restore the** `/var/lib/dpc` **directory.**
4. **To start Data Protection Central,** type the following command:
   ```bash
   sudo /usr/local/dpc/bin/dpc start
   ```

Embedded component usage

Learn about Data Protection Central embedded component usage.

To locate Data Protection Central OSS third party software, use the `/usr/local/dpc/licenses` folder. In this folder, three HTML files with the latest release candidate build are found.