This document describes how to configure Gemalto KeySecure on Data Domain Operating System (DD OS) version 6.1. Topics include:

- Overview................................................................................................................ 2
- Accessing the KeySecure server............................................................................. 2
- Installing a KeySecure license................................................................................. 4
- Enabling FIPS compliance....................................................................................... 6
- Creating a certificate authority (CA)...................................................................... 6
- Configuring a trusted CA on KeySecure............................................................... 12
- Creating and installing a KeySecure KMIP server certificate................................. 17
- Importing the signed server certificate................................................................. 29
- Configuring KMIP service on KeySecure............................................................... 30
- Creating a local user............................................................................................. 32
- Creating and installing the host certificate............................................................ 33
- Importing the CA certificate to a Data Domain system......................................... 36
- Creating the KeySecure encryption key................................................................ 37
- Configuring KMIP on the Data Domain system..................................................... 39
Overview

This document describes how to create keys in Gemalto KeySecure and use them on a Data Domain system.

Note
Pay attention to the order in which steps are completed in this guide. The order of execution is extremely important.

Terminology
This document uses the following terminology:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMIP</td>
<td>Key Management Interoperability Protocol</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
</tbody>
</table>

Accessing the KeySecure server

Complete the following steps to access the KeySecure server.

Procedure

1. In a browser window, access the KeySecure web interface using the default port 9443.

   Note
   The web admin server port listens for requests from port 9443.

   The Gemalto KeySecure login screen appears.

   ![SafeNet KeySecure Management Console]

   **Administrator Authentication**

   Username:  
   Password:  
   Log In

2. Log in with the following username, and create the default password during initial configuration.
   - Username: admin
The system creates a default administrative account with this name.

- Password: `<password>`

Use the password that is configured during KeySecure setup, or as provided by the customer.

After login, the **System Summary** screen appears if a KeySecure license is installed.

If a KeySecure license is not installed, the system displays a warning.

If the KeySecure license is already installed, go to **Enabling FIPS compliance** on page 6.
If the KeySecure license is not already installed, go to Installing a KeySecure license on page 4.

## Installing a KeySecure license

Complete the following steps to install a KeySecure license.

**Procedure**

1. Get a permanent license from Gemalto KeySecure.
2. In the left-most pane, select Device > Maintenance > System Information & Upgrade.
Device Information

<table>
<thead>
<tr>
<th>Product:</th>
<th>KeySecure 150v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box ID:</td>
<td>7IFG-X6RP-5M6T-H</td>
</tr>
<tr>
<td>Software Version:</td>
<td>8.4.3</td>
</tr>
<tr>
<td>Software Install Date:</td>
<td>Wed Aug 17 15:26:05 EDT 2016</td>
</tr>
</tbody>
</table>

License Information

| Application Server Licenses: | None |
| Database Licenses:           | None |
| Transform Utility Licenses:  | None |
| Licenses in Use:             | 0    |

Feature Activation List

| Description | Activation Date |

Software & License Upgrade/Install

- **Source:**
  - Upload from browser
  - File: [Browse...]
  - FTP
  - SCP
  - Host: [Field]
  - Filename: [Field]
  - Username: [Field]
  - Password: [Field]
  - Machine will reboot after upgrade/install

3. Under **Software & License Upgrade/Install**, select **Upload from browser** to upload the license through the web browser.
4. Click **Browse** to locate the file on a local or network drive.
5. Click **Upgrade/Install**.
6. Click **Confirm**.
   If the license uploads successfully, the system displays a success message and reboots.
Enabling FIPS compliance

Complete the following steps to enable FIPS compliance.

Procedure

1. From the left-most pane, select Security > Advanced Security > High Security

The High Security Configuration screen appears.

2. In the FIPS Compliance section, click Set FIPS Compliance.

The system displays Is FIPS Compliance: Yes.

Creating a certificate authority (CA)

There are three ways to handle/create the CA in KeySecure.

- Create a local CA.
- Import a CA.
• Import a hierarchical CA.

Note
Setup with a hierarchical CA is beyond the scope of this document and requires Gemalto support.

Creating a local CA

Complete the following steps to create a local CA.

Procedure
1. From the left-most pane, select Security > Local CAs.
2. Click Local CAs.

Certificate and CA Configuration

Local Certificate Authority List

<table>
<thead>
<tr>
<th>CA Name</th>
<th>CA Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Local Certificate Authorities.</td>
<td></td>
</tr>
</tbody>
</table>

Create Local Certificate Authority

Certificate Authority Name: [Input field]
Common Name: [Input field]
Organization Name: [Input field]
Organizational Unit Name: [Input field]
Locality Name: [Input field]
State or Province Name: [Input field]
Country Name: US
Email Address: [Input field]
Key Size: 2048

Certificate Authority Type:
- Self-signed Root CA
- CA Certificate Duration (days): [Input field]
- Maximum User Certificate Duration (days): [Input field]

Create

(Image shows "No Local Certificate Authorities" and the dialog boxes for creating a new CA.)

3. Specify the following information:
- Certificate Authority Name: <Local CA Name>
- Common Name: <Local CA Name>

**Note**
Match the Common Name to the Certificate Authority Name.

- Organization Name: <Your Organization>
- Organizational Unit Name: <Your Organizational Unit>
- Locality Name: <City>
- State: <State>
- Country Name
- Email Address: <Email Address>
- Key Size: 2048

**Note**
Recommended minimum size to create a 256-bit encryption.

4. Click **Create** to create the KeySecure local CA.
Importing a CA

Complete the following steps to import a CA.

Procedure

1. From the left-most pane, select Security > Known CAs.
2. In the Install CA Certificate pane, specify the certificate name in the Certificate Name field.

3. In the Certificate field, paste the CA certificate text.
Security > Known CAs

Certificate and CA Configuration

CA Certificate List

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Certificate Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca_certificate</td>
<td>Issuer: Dell Technologies Expires: Dell Technologies Oct 16 15:52:27 2026 GMT</td>
</tr>
</tbody>
</table>

4. Click Install.

Security > Known CAs

Certificate and CA Configuration

CA Certificate List

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Certificate Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca_certificate</td>
<td>Issuer: Dell Technologies Expires: Dell Technologies Oct 16 15:52:27 2026 GMT</td>
</tr>
</tbody>
</table>

Warning: CA certificates must be added to a trusted CA list in order to be recognized by the NAE Server
Configuring a trusted CA on KeySecure

Complete the following steps to configure the trusted CA.

Procedure

1. In the left-most pane, select Security > Trusted CA Lists.

2. Select Default.

3. Click Properties.
4. Click **Edit**.

The next screen provides the ability to select which CAs to trust.
5. Use the arrow buttons to move Local CA to the Trusted CAs list.
6. Click **Add**.
7. Click **Save**.
Creating and installing a KeySecure KMIP server certificate

Complete the following steps to create the server SSL certificate.

Procedure

1. In the left-most pane, select Security > SSL Certificates.
2. Specify the following information:

- Certificate Name: <SSL Certificate Name>
- Common Name: <SSL Certificate Name>
- Organization Name: <Your Organization>
- Organizational Unit Name: <Your Organizational Unit>
- Locality Name: <City>
- State: <State>
- Country Name
- Email Address: <Email Address>
- Key Size: 2048
**Security** » SSL Certificates

**Certificate and CA Configuration**

### Certificate List

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Certificate Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Certificates.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Create Certificate Request**

| Certificate Name: KMIP-Server-1 |
|-------------------|-----------------|
| Common Name: KMIP-Server-1 |
| Organization Name: EMC |
| Organizational Unit Name: DataDomain |
| Locality Name: SantaClar |
| State or Province Name: CA |
| Country Name: US |
| Email Address: josep.wonosaputra@emc.com |
| Key Size: 2048 |

[Create Certificate Request]

3. Click **Create Certificate Request**.
The SSL certificate is created, but is in a Request Pending state because it has yet to be signed by the local CA.

4. Click the newly created certificate to open it.
5. Copy the CSR text.

**Note**

The first and last lines of the CSR text, that say **BEGIN CERTIFICATE REQUEST** and **END CERTIFICATE REQUEST** must be included when the CSR text is copied. Do not include any extra white space when copying the CSR text.

The CSR text should look like:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAgAwEQQBEB7z4vXjAQBE6fXjABJHEB9mFv-powered-by-DD-OS
....
MIIEAWECCAgAwEQQBEB7z4vXjAQBE6fXjABJHEB9mFv-powered-by-DD-OS
-----END CERTIFICATE REQUEST-----
```
6. From the left-most pane, select **Security > Local CAs**.
7. Click Local CAs.
8. Select the local CA, and click Sign Request.

10. Paste the CSR text into the Certificate Request field.
11. Click **Sign Certificate**.

12. Copy the signed certificate.

**Note**

The first and last lines of the CSR text, that say `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST` must be included when the CSR text is copied. Do not include any extra white space when copying the CSR text.

The signed certificate text should look like:

```
-----BEGIN CERTIFICATE-----
MIIDyzCCArOgAwIBAgICKlYwDQYJKoZIhvcNAQELBQAwgZQxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJDQTEUMBIGA1UEBxMLU2FudGEgQ2xhcmExDDAKBgNVBAoTA0VN
QzEUMBIGA1UECxMKRGF0YSBEb21haW4xFDASBgNVBAMTC0pXLUtNSVAtQ0EyMSgw
JgYJKoZIhvcNAQcLBgAwgggAEMCAQAwEAoordBQg6YXNzZXRzMCsGA1UdEwQCMAAw
EQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBCwUAA4IBAwggEKAoIBAQDC
-----END CERTIFICATE-----
```
13. From the stop of the screen, select Security > SSL Certificate
14. Select the radio button for the new certificate. The certificate displays as Pending CSR.

15. Click **Install Certificate**.
16. Paste the signed certificate text in the **Certificate Response** field.
17. Click **Save**.

**Note**

Verify that the Certificate Status displays as **Active**.
**Importing the signed server certificate**

Complete the following steps to import the signed server certificate.

**Procedure**

1. In the left-most pane, select **Security > SSL Certificates**.

---

### Certificate List

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Certificate Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMIP_Server-1</td>
<td>Common: KMIP-Server-1</td>
</tr>
<tr>
<td></td>
<td>Issuer: EMC</td>
</tr>
<tr>
<td></td>
<td>Expires: Apr 23 2018</td>
</tr>
</tbody>
</table>

**Edit**  **Delete**  **Properties**

---

### Create Certificate Request

- **Certificate Name:**
- **Common Name:**
- **Organization Name:**
- **Organizational Unit Name:**
- **Locality Name:**
- **State or Province Name:**
- **Country Name:** **US**
- **Email Address:**
- **Key Size:** **2048**

Create Certificate Request

---

### Import Certificate

- **Source:**
  - Upload from browser
  - SCP
    - Host:
    - Filename:
    - Username:
    - Password:
- **Certificate Name:**
- **Private Key Password:**

Import Certificate
2. In Import Certificate, select Upload from browser to upload the server certificate through the web browser.

3. Click Browse to locate the file on a local or network drive.

4. In the Certificate Name field, specify the certificate name.

5. In the Private Key Password field, specify the certificate password.

6. Click Import to import the certificate into KeySecure.

**Configuring KMIP service on KeySecure**

Complete the following steps to create the client certificate.

**Procedure**

1. Click the Device tab.

2. In the Cryptographic Server Key Settings pane, click Add. On the Protocol drop-down list, select KMIP.

3. Select Edit, and specify the following information:
   - IP Address: `<KMIP-server-IP-address>`
- Port: 5696
- Use SSL: Select the checkbox (SSL is required for KMIP)
- Server Certificate: `<Previously-created-server-certificate>`

4. Click **Save**.

5. Select the **KMIP** radio button, and click **Properties**.

6. At the bottom of the **Authentication Settings** pane, click **Edit**.

7. Specify the following information:
   - Password Authentication: Optional
   - Client Certificate Authentication: Used for SSL session and username (most secure)
   - Trusted CA List Profile: Default
   - Username Filed in Client Certificate: CN (Common Name)
   - Require Client Certificate to Contain Source IP: Leave this field blank

8. Click **Save**.
Creating a local user

Complete the following steps to create a local user.

Procedure

1. In the left-most pane, browse to Security > Users & Groups > Local Authentication. Click Add.
2. Type in values for:

- Username: `<local-username>`
- Password: `<passwd-mgmt-setting>` Password must be at least 8 characters
- User Administration Permission: `<check-mark-to-enable>`
- Change Password Permission: `<check-mark-to-enable>`

3. Click Save.

Creating and installing the host certificate

A host certificate can be generated on either the Data Domain system or on a Linux system and imported to a Data Domain system.

Generating a host certificate

Procedure

1. To generate a host certificate signing request (CSR), type the following command: `adminaccess certificate cert-signing-request generate [key-strength {1024bit | 2048bit | 3072bit | 4096bit}] [country <country-code>] [state <state>] [city <city>] [org-name <organization-name>] [org-unit <organization unit>] [common-name <common-name>]`
Note

<common-name> should be the KeySecure admin username. See Create a new user topic in this document.

dsysadmin@dd4500-90# adminaccess certificate cert-signing-request generate key-strength 2048bit country US state CA city Santa Clara org-name Dell org-unit DD common-name user1
Certificate signing request (CSR) already exists at /ddvar/certificates/CertificateSigningRequest.csr
With following parameters:
  Key Strength        : 2048
  Country            : US
  State              : California
  City               : Santa Clara
  Organization Name  : My Company Ltd
  Organization Unit  :
  Common Name        : dd4500-90.datadomain.com
Do you want to regenerate? (yes|no) [no]: yes
Certificate signing request (CSR) successfully generated at /ddvar/certificates/CertificateSigningRequest.csr with the following parameters:
  Key Strength        : 2048
  Country            : US
  State              : CA
  City               : Santa Clara
  Organization Name  : Dell
  Organization Unit  : DD
  Common Name        : user1

2. Copy CSR from /ddvar/certificates/ CertificateSigningRequest.csr

3. Obtain the host certificate signing request (CSR) signed by KeySecure certificate authority (CA).
   a. In KeySecure, browse to Security > Local CAs, and select the radio button for the newly created CA.
b. Click **Sign Request**.

c. Paste CSR on certificate request, and select **Client** for Certificate Purpose. Click **Sign Request**.
4. Download signed certificate.

Certificate and CA Configuration

CA Certificate Information

Key Sizes: 2048
Start Date: Apr 27 03:31:27 2017 GMT
Expiration: Oct 16 03:31:27 2026 GMT

- US
- CA
- Santa Clara
- Dell
- DD
- user1

-----BEGIN CERTIFICATE-----
MIIDOTCCAqAgAwIBAgIBADBGA5gMEQwDOTAwDQYJKoZIhvcNAQcCoAAo3YXQz
MA0GCSqGSIb3DQEBCwUA油脂授 destabilize
-----END CERTIFICATE-----

5. Install the signed host certificate on the Data Domain system.
   a. Copy the signed certificate to /ddvar/certificates folder.
   b. Import host certificate to the Data Domain system. Import host certificate to the Data Domain system.

adminaccess certificate import host application keysecure file <Certificate in PEM>

Importing the CA certificate to a Data Domain system

In order for KeySecure to transmit and manage key management requests from KMIP clients (a Data Domain system), it is essential that the Data Domain system have both a CA certificate and Host certificate. Hence, both certificates (CA and Host) are required to be imported to a Data Domain system. This step is about importing CA certificate.

Here are the steps for importing the CA certificate.

Procedure

1. In KeySecure, select Security > Local CAs.
2. Click the CA used to sign the server certificate.
3. Copy the certificate text, and paste it into the file named cacert.pem in the /ddvar/certificates directory on the Data Domain system.
Creating the KeySecure encryption key

Complete the following steps to create the KeySecure encryption key.

Procedure

1. In KeySecure, select **Security > Managed Objects > Keys**.
2. Click **Create Key**.
3. Specify the following information:
   - **Key Name**: `<Key-name>`
   - **Template**: None
   - **Owner Username**: `<KMIP-admin-username>`

---

**Note**

Download the CA certificate on the Data Domain system as `cacert.pem` and copy it to the `/ddvar/certificates/` directory.
- Algorithm: AES-256
- Deletable: Leave blank
- Exportable: Yes
- Versioned Key Bytes: Leave blank
- Template: Leave blank
- Activation Date: Immediately
- Process Start Date: Immediately

4. Click **Create**.
5. Select **Keys** (Security > Managed Objects > Keys), and select the radio button for the new key.
6. Click the **Attributes** tab.
7. Under the Application Specific Information pane, click **Add**.
   - Specify the following information:
     - Application Namespace: DD_DARE_KEYS
     - Application Data: `<Key Class Name>`

   **Note**
   This `<Key Class>` acts as a group identifier for all of this particular Data Domain system's keys. Note this value, and use the exact text to later configure the Data Domain system. The chosen value has to be alphanumeric value.
Complete the following steps to configure KMIP on the Data Domain system.

Procedure

1. Set the "system passphrase."
   A strong passphrase is required in order for the KMIP feature to work and must contain:
   - A minimum of nine characters,
   - A minimum of one lowercase character,
   - A minimum of one uppercase character,
   - A minimum of one digit, and
   - A minimum of one special character.
   a. In DDSH, run `system passphrase set`.
   b. Type passphrase: *********
   c. Re-enter passphrase: *********

   **Note**
   A weak passphrase that does not comply with the guidelines will cause the KMIP feature to fail. If a weak passphrase was previously set, update the system passphrase according to the guidelines previously listed.

2. Import the CA certificate to the Data Domain system.
   `sysadmin@ddxxxx-xx# adminaccess certificate import ca application keysecure file <CA certificate>`
The SHA1 fingerprint for the imported CA certificate is CB:3F:B6:7D:00:7C:5D:B3:1B:CD:27:63:32:2F:4F:CF:E9:F1:1B:E4

Do you want to import this certificate? (yes|no) [yes]: yes
CA certificate imported for application(s) : "keysecure".
sysadmin@ddxxxx-xx#

3. Verify both host and CA certificates are imported by running the command #
adminaccess certificate show.

4. On the Data Domain system, run filesystem encryption enable.

sysadmin@ddxxxx-xx# filesystem encryption enable
Enter new passphrase: *********
Re-enter new passphrase: *********
Passphrases matched.
The passphrase is set.
Encryption feature is enabled on the system.
The filesystem must be restarted to effect this change.
sysadmin@ddxxxx-xx#
sysadmin@ddxxxx-xx# filesystem restart

This action will restart the file system.
Applications may experience interruptions while the file system is restarted.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Disabling filesystem:
Please wait...........
The filesystem is now disabled.
Enabling filesystem:
Please wait................
The filesystem is now enabled.
sysadmin@ddxxxx-xx#

Note

<key-class> should be set to same value as the Application Data of Application Specific Information in the KeySecure.

sysadmin@ddxxxx-xx# filesystem encryption key-manager set server
<KeySecure-IP-Address> port 5696 fips-mode enabled key-class <key-class-name>
server-type keysecure kmip-user <KeySecure-username>
The current key-manager configuration is:

Key Manager:            Disabled
Server Type:            KeySecure
Server:                 <KeySecure-IP-Address>
Port:                   5696
Fips-mode:              enabled
Status:                 Online
Key-class:              <key-class>
KMIP-user:              <KeySecure-username>
sysadmin@ddxxxx-xx#
sysadmin@ddxxxx-xx# filesystem encryption key-manager enable

Key manager is enabled.
The filesystem must be restarted to effect this change.
sysadmin@ddxxxx-xx#
sysadmin@ddxxxx-xx# filesystem restart

This action will restart the file system.
Applications may experience interruptions while the file system is restarted.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Disabling filesystem:
Please wait............

The filesystem is now disabled.
Enabling filesystem:
Please wait...................
The filesystem is now enabled.
sysadmin@ddxxxx-xx#

5. Verify that the key manager is set to KeySecure.

sysadmin@ddxxxx-xx# filesys encryption key-manager show
The current key-manager configuration is:
Key Manager:                           Enabled
Server Type:                           KeySecure
Server:                                 <KeySecure-IP-Address>
Port:                                   5696
Fips-mode:                              Enabled
Status:                                 Online
Key-class:                              <key-class>
KMIP-user:                              <KeySecure-username>
sysadmin@ddxxxx-xx#

sysadmin@ddxxxx-xx# filesys encryption keys show
Active Tier:
Key   Key                                                                State
 Size
Id    MUID                                                               ------------
--------
-------
0.1  817                                                                Deactivated
-
0.2  38D41BCEB0D2FEBD3676A54960E6C3074A0699DA1CE7603CFE2BEE286160E6B2  Activated-RW
-
--------
* Post-comp size will be updated after next cleaning cycle.
sysadmin@ddxxxx-xx#

6. Restart the Data Domain file system.

Run the following command:
filesys restart
# filesys restart
This action will restart the file system.
Applications may experience interruptions
while the file system is restarted.
Are you sure? (yes|no) [no]: yes
ok, proceeding.
Disabling filesystem:
Please wait....... The filesystem is now disabled.
Enabling filesystem:
Please wait.................
The filesystem is now enabled.

7. Verify that the key manager is set to KeySecure.

Run the following command:
filesys encryption key-manager show
# filesys encryption key-manager show
The current key-manager configuration is:
Key Manager:                           Enabled
Server Type:                           KeySecure
Server:                                 10.110.140.151
Port:                                   5696
Fips-mode:                              enabled
Status:                                 Online
<table>
<thead>
<tr>
<th>Key-class:</th>
<th>ddve6.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>KMIP-user:</td>
<td>ddve</td>
</tr>
</tbody>
</table>