Certificate Hub 4.3

EDM Deployment Guide

Document issue: 1.3
Issue date: May 15, 2026

Contents

1 About this guide

This document describes how to deploy the 4.3.x Certificate Hub releases in Entrust Deployment Manager.

Revision information

See the following table for the issued versions of this document.

Issue	Date	Section	Changes
1.4	May 2026	Fixed bugs for 4.3.1	Fix the list of fixed bugs
1.3	Dec 2025	Upgrading	Update the warning note about the required version for upgrading
1.2	Nov 2025	Release Notes for 4.3.1	New section
1.1	Nov 2025	Known issues for 4.3.0	Add the ATEAM-18848 issue
1.0	Oct 2025	All sections	The first release of this document

Related documentation

See the following table for the documentation related to this guide.

Document	Contents
Entrust Deployment Manager 2.0.2 - Installation and Administration Guide	Installation and administration of the Entrust Deployment Manager 2.0.2 platform running Certificate Hub.
https://api.managed.entrust.com/csp/1.2/Using-Certificate-Manager.html	User options of the Certificate Manager console.

Documentation feedback

You can rate and provide feedback about product documentation by completing the online feedback form:

https://go.entrust.com/documentation-feedback

Any information you provide goes directly to the documentation team and is used to improve and correct the information in our guides.

2 Overview

Certificate Hub has three sets of capabilities:

- The **find capabilities** inventory certificates across your organization (through network discovery) and automated certificate import (from CA databases and cloud services).
- The **control capabilities** centrally manage policy, issuance & access to public and private certificates regardless of vendor. Perform manual operations as necessary to issue, renew, and revoke certificates.
- The **automation capabilities** push keys and certificates to endpoints, with fully managed rotation and certificate profile management.
- The **report capabilities** provide organizational, issue notifications, and reports to remind certificate owners of actions they need to take.

Administrators can customize Certificate Hub to meet enterprise needs like access permissions, system metadata, notifications, or report branding.

Licensing model

Certificate Hub is licensed by capability tier. The find and report tier provides functionalities like the following.

- Certificate discovery with centralized management through the CertHub console
- Automated and customized reporting
- Expiry notifications
- Fixed, per-year subscription
- Plugin management

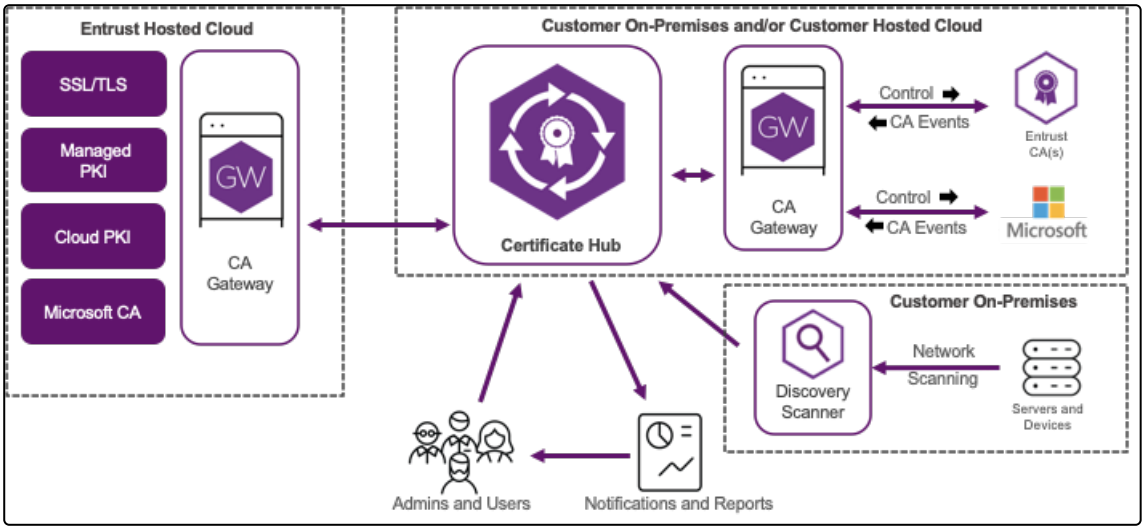
The control and automate tier provides functionalities like the following.

- Find features
- Single Pane of Glass Authority management
- Certificate manual issuance and renewal
- Automated certificate renewal.
- Certificate lifecycle management
- Push certs to defined Destinations
- Open Plugin Interfaces

When we refer to "you", we mean the customer who has purchased one or more PKIaaS licenses, or one of that customer's internal users, i.e., personnel. In general, the software is licensed for your internal use only. However, you are permitted to assign identities (uniquely identified endpoints) and digital certificates to Users outside your organization solely to enable communications between you and those Users concerning your business.

High-level architecture

The high-level architecture integrates the following main components.



Discovery Scanners

Certificate Hub Discovery Scanners:

- Search your enterprise's networks or portions of networks for the most recent information about deployed certificates.
- Record each certificate's location, type, algorithms, and expiry, regardless of the certificate issuer.

Discovery Scanners are typically deployed on your premises, inside corporate firewalls, to access the internal private servers. However, only Discovery Scanners require this kind of deployment; you can deploy the other Certificate Hub components in a less restrictive environment.

When started, a Discovery Scanner:

1. Contacts Certificate Hub to get the policy and scan configuration.
2. Launches the Certificate Hub scheduling process for scanning.
3. Executes one or more configured scans according to the calendar schedule and priority.
4. Periodically polls Certificate Hub for any policy and or configuration updates.

Discovery Scanners run a custom-built version of Nmap to scan ports, capture the returned SSL certificate chain, and transmit scan results to Certificate Hub for processing.

Entrust CA Gateway

Through Entrust CA Gateway, Certificate Hub obtains a direct feed of issued certificates from each supported Certificate Authority (CA).

1. Entrust Authority Security Manager (on-prem and Entrust-managed).
2. Entrust Public Certificate Services (ECS).
3. Microsoft CAs.
4. Entrust PKIaaS.

Thus, Certificate Hub can request certificates from all the CAs managed by a CA Gateway instance.

Certificate Hub

Certificate Hub is a container-based set of services amenable to either customer premises or commercial cloud hosting. Certificate Hub provides:

- An API interface to the companion Certificate Hub browser UI.
- The underlying certificate database.
- The necessary background processes.

3 Release notes

See below the release notes for Certificate Hub from 4.2.0 to 4.3.1.

Release Notes for 4.2.0

See below for the Certificate Hub 4.2.0 release notes.

New features for 4.2.0

Certificate Hub 4.2.0 adds the following features.

Fingerprint of the destination keys displayed on creation (ATEAM-3217)

When you click the **Verify** button, the destination creation form displays the fingerprint of the destination SSH key, allowing you to verify it before adding the destination.

Header row added to empty reports (ATEAM-17510)

Certificate reports without records include a row header to ensure they are not confused with failed reports.

Key Manager selection separated from Destinations (ATEAM-18208)

Key Management Systems are no longer included in the **Destinations** list. They are now included in an independent list, allowing users to select both a Key Management System and a destination.

High availability support (ATEAM-18346)

On multinode installations, each pod runs with two replicas to ensure high availability.

Profile ID column added to the certificates grid (ATEAM-18472)

The new **Profile ID** column on the **Certificates** page displays the name of each certificate profile and supports filtering and sorting.

New option to close all messages (ATEAM-18474)

A new **Close all messages** button allows closing all the toasts in the breadcrumb area.

Column sorting improved usability (ATEAM-18475)

The headers of console grids (for certificates, sources, destinations, etc.) better indicate which columns support sorting. Specifically, sortable headers display a "This column is sortable" message when the mouse hovers over them.

Fixed bugs for 4.2.0

Certificate Hub 4.2.0 fixes the following bugs.

- Matching tags not sorted (ATEAM-18116)
- Missing keyboard accessibility options (ATEAM-18302)
- Mandatory fields not validated (ATEAM-18315)
- No charts dislayed on widgets (ATEAM-18328)
- Shared partitions not supported on path (ATEAM-18348)
- Certificate autorenewal cannot be disabled (ATEAM-18470)
- Multiple DNS in SAN not supported (ATEAM-18674)

Matching tags not sorted (ATEAM-18116)

When typing a tag name, the **Authorized Tag** field does not display a sorted list of the matching tags.

Missing keyboard accessibility options (ATEAM-18302)

The user cannot select a **Destination** using the keyboard accessibility options instead of the mouse.

Mandatory fields not validated (ATEAM-18315)

The generated public enrollment forms do not validate the mandatory fields.

No charts dislayed on widgets (ATEAM-18328)

The widgets of the **Certificates** page display the "NaN%" string instead of a chart.

> Click **>> Show Insights** on the **Certificates** page to display the widgets.

Shared partitions not supported on path (ATEAM-18348)

Destinations of the **F5-BIG-IP-Destination-Plugin** type do not support shared partitions on the path.

Certificate autorenewal cannot be disabled (ATEAM-18470)

When creating a certificate, the wizard does not display the renewal options if `key_client_generated` is set to `true` in the selected profile.

Multiple DNS in SAN not supported (ATEAM-18674)

When requesting a certificate using a public enrollment form, the SAN (Subject Alternative Names) field only supports one DNS value.

Known issues for 4.2.0

Certificate Hub 4.2.0 has the following known issues.

Error when taking certificates off hold (ATEAM-1445)

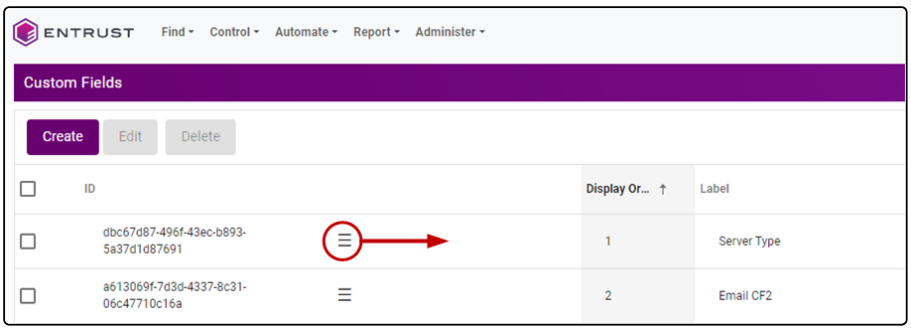
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, administrators can change the display order of the custom fields. However:

- Reordering a custom field does not change the **Display Order** column value.
- Refreshing the **Custom Field** page reverts all changes.

Workaround: After dragging a custom field to a different position, move the ☰ drag icon within its row to make the changes persistent.



Some endpoint filters display invalid results on report files (ATEAM-15933)

The following endpoint filters do not display correct results on the downloaded report files.

- is empty
- is not empty

Certificates without names not synced from source (ATEAM-16039)

Certificates without a name are not successfully synced from Sources.

Wildcard certificates not recorded (ATEAM-16436)

The application does not record wildcard certificates successfully scanned by the Discovery Scanner.

> Wildcard certificates are certificates containing the wildcard asterisk in the issuer and subject.

Buttons language not affected when switching language (ATEAM-16920)

Switching the language before logging in does not affect the language of the **Delete** and **Cancel** buttons in the **Confirm Delete** popup on the **Destinations** page.

Owner grid column not populated when accessing reports (ATEAM-16923)

The **Owner** grid column is not populated when accessing the **Report Schedules** from the **Report Designer** grid.

Workaround: Access the **Report Schedules** grid from the navigation bar.

The Verify button does not trigger a verification without additional changes (ATEAM-16950)

After the failed verification of a Destination, clicking **Verify** again does not trigger a new verification.

Workaround: Make any change in the create form – for example, change the **Description**.

The public key ID can refer to the private key ID (ATEAM-16982)

When issuing a certificate using the **Key Manager (KMIP)** destination, the **public key ID** is also referring to the **private key ID**

Error when selecting the Domains widget (ATEAM-16986)

When using a FIND license, selecting the **Domains** widget on the **Dashboard** displays the following error.

```
Unable to show information: Forbidden. This request is not allowed.
```

Archive certificates option missing with FIND licenses (ATEAM-16988)

When using a FIND license, the option to **Archive** certificates is missing in the **Actions** dropdown on the **Certificates** grid.

Incomplete CA certificate chain (ATEAM-16997)

When creating a new certificate, the downloaded chain only includes the certificate of the CA that issued the new certificate instead of including the entire chain.

Verification fails for IIS destinations (ATEAM-17030)

Verification fails for IIS destinations if the username includes a domain name – for example:

```
.\user
```

```
domain\user
```

Not found error messages during deployment (ATEAM-17230)

When deploying, you can safely ignore the not found error messages like this one:

```
Error from server (NotFound): configmaps "postgres-config" not found
```

502 status code when selecting Preview CSV for a report (ATEAM-18121)

Certificate Hub can return a 502 status code when exporting a report to CSV. That is, when:

1. Navigating to **Report / Designer**.
2. Selecting the **Design** action for a report.
3. Selecting **Preview CSV** in the menu bar.

Workaround:

1. Log in to the machine hosting the appliance or the Kubernetes deployment.
2. Run the following command to edit the `acm-api` configuration file.

   ```
   sudo kubectl edit deployment/acm-api -n certhub
   ```

3. Add `-Xmx4g` to the `JAVA_OPTS` setting.

   ```
   env:
     - name: JAVA_OPTS
       value: -Xmx4g
   ```

4. Run the following command to make the changes effective.

   ```
   sudo kubectl rollout restart deployment/acm-api -n certhub
   ```

5. Run the following command to edit the `scheduler` configuration file.

```
run ssudo kubectl edit deployment/scheduler -n certhub
```

6. Add `-Xmx4g` to the `JAVA_OPTS` setting.

```
env:
  - name: JAVA_OPTS
    value: -Xmx4g
```

7. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/scheduler-n certhub
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Sectigo CA not supported (ATEAM-18790)

This Certificate Hub release does not support requesting certificates from a CA Gateway instance integrated with a Sectigo CA.

> Certificate Hub 4.2.1 will support requesting certificates from a CA Gateway 3.2.1 instance integrated with a Sectigo CA.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

Release Notes for 4.2.1

See below for the Certificate Hub 4.2.1 release notes.

Fixed bugs for 4.2.1

Certificate Hub 4.2.1 fixes the following bug.

502 status code when selecting Preview CSV for a report (ATEAM-18121)

Certificate Hub can return a 502 status code when exporting a report to CSV. That is, when:

1. Navigating to **Report / Designer**.
2. Selecting the **Design** action for a report.
3. Selecting **Preview CSV** in the menu bar.

Workaround:

1. Log in to the machine hosting the appliance or the Kubernetes deployment.
2. Run the following command to edit the `acm-api` configuration file.

```
sudo kubectl edit deployment/acm-api -n certhub
```

3. Add `-Xmx4g` to the `JAVA_OPTS` setting.

```
env:
  - name: JAVA_OPTS
    value: -Xmx4g
```

4. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/acm-api -n certhub
```

5. Run the following command to edit the `scheduler` configuration file.

```
run ssudo kubectl edit deployment/scheduler -n certhub
```

6. Add `-Xmx4g` to the `JAVA_OPTS` setting.

```
env:
  - name: JAVA_OPTS
    value: -Xmx4g
```

7. Run the following command to make the changes effective.

```
sudo kubectl rollout restart deployment/scheduler-n certhub
```

Sectigo CA not supported (ATEAM-18790)

Certificate Hub 4.2.0 does not support requesting certificates from a CA Gateway 3.2.0 instance integrated with a Sectigo CA.

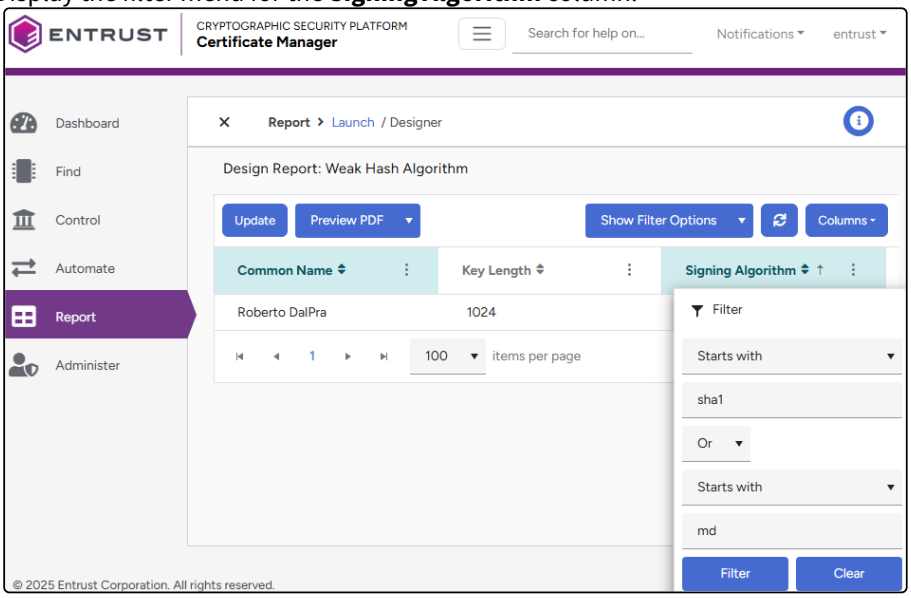
> ⚠ To fix this bug, you must install Certificate Hub 4.2.1 and CA Gateway 3.2.1.

"Weak Hash Algorithm" filter requires resetting before generating a report (ATEAM-18804)

When using the **Preview** button to export the contents of the **Weak Hash Algorithm** system report, the generated report file includes more certificates than just those with a weak hash algorithm.

Workaround:

1. Log in to the user console of Certificate Manager.
2. Navigate to **Report > Designer**.
3. On the report grid, click on **Weak Hash Algorithm**.
4. Display the filter menu for the **Signing Algorithm** column.



5. Click **Clear** to remove all the filter settings.
6. Click the **Update** button.
7. Set again the initial filter configuration:

   Starts with

   sha1

   Or

   Starts with

   md

8. Click the **Update** button.
9. Click **Preview** to confirm the generated report only includes certificates matching the filter.

Known issues for 4.2.1

Certificate Hub 4.2.1 has the following known issues.

Error when taking certificates off hold (ATEAM-1445)

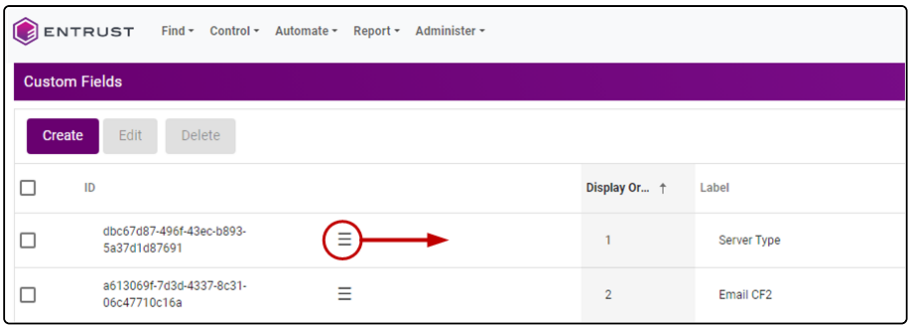
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, administrators can change the display order of the custom fields. However:

- Reordering a custom field does not change the **Display Order** column value.
- Refreshing the **Custom Field** page reverts all changes.

Workaround: After dragging a custom field to a different position, move the ☰ drag icon within its row to make the changes persistent.



Some endpoint filters display invalid results on report files (ATEAM-15933)

The following endpoint filters do not display correct results on the downloaded report files.

- is empty
- is not empty

Certificates without names not synced from source (ATEAM-16039)

Certificates without a name are not successfully synced from Sources.

Wildcard certificates not recorded (ATEAM-16436)

The application does not record wildcard certificates successfully scanned by the Discovery Scanner.

> Wildcard certificates are certificates containing the wildcard asterisk in the issuer and subject.

Buttons language not affected when switching language (ATEAM-16920)

Switching the language before logging in does not affect the language of the **Delete** and **Cancel** buttons in the **Confirm Delete** popup on the **Destinations** page.

Owner grid column not populated when accessing reports (ATEAM-16923)

The **Owner** grid column is not populated when accessing the **Report Schedules** from the **Report Designer** grid.

Workaround: Access the **Report Schedules** grid from the navigation bar.

The Verify button does not trigger a verification without additional changes (ATEAM-16950)

After the failed verification of a Destination, clicking **Verify** again does not trigger a new verification.

Workaround: Make any change in the create form – for example, change the **Description**.

The public key ID can refer to the private key ID (ATEAM-16982)

When issuing a certificate using the **Key Manager (KMIP)** destination, the **public key ID** is also referring to the **private key ID**

Error when selecting the Domains widget (ATEAM-16986)

When using a FIND license, selecting the **Domains** widget on the **Dashboard** displays the following error.

```
Unable to show information: Forbidden. This request is not allowed.
```

Archive certificates option missing with FIND licenses (ATEAM-16988)

When using a FIND license, the option to **Archive** certificates is missing in the **Actions** dropdown on the **Certificates** grid.

Incomplete CA certificate chain (ATEAM-16997)

When creating a new certificate, the downloaded chain only includes the certificate of the CA that issued the new certificate instead of including the entire chain.

Verification fails for IIS destinations (ATEAM-17030)

Verification fails for IIS destinations if the username includes a domain name – for example:

```
.\user
```

```
domain\user
```

Not found error messages during deployment (ATEAM-17230)

When deploying, you can safely ignore the not found error messages like this one:

```
Error from server (NotFound): configmaps "postgres-config" not found
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Release Notes for 4.3.0

See below for the Certificate Hub 4.3.0 release notes.

- New features for 4.3.0
- Fixed bugs for 4.3.0
- Known issues for 4.3.0

New features for 4.3.0

Certificate Hub 4.3.0 adds the following features.

- Custom layout for email notification (ATEAM-17499)
- JWT security enhanced with cookies (ATEAM-18693)
- Apache restart without sudo permissions (ATEAM-18827)

Custom layout for email notification (ATEAM-17499)

The new **Email** configuration setting allows for the definition of a custom header and footer for the notification emails.

JWT security enhanced with cookies (ATEAM-18693)

The security of the JSON Web Tokens (JWTs) granted to console users has been enhanced by using browser cookies.

Apache restart without sudo permissions (ATEAM-18827)

The Apache web server destinations add support for restarting the Apache server without sudo permissions.

Fixed bugs for 4.3.0

This release fixes the following bug.

Filters do not support custom rules (ATEAM-18762)

The automation rules do not support custom rules.

Known issues for 4.3.0

This release has the following known issues.

- Error when taking certificates off hold (ATEAM-1445)
- Issues when changing the display order of custom fields (ATEAM-15463)
- Some endpoint filters display invalid results on report files (ATEAM-15933)
- Certificates without names not synced from source (ATEAM-16039)
- Wildcard certificates not recorded (ATEAM-16436)
- Buttons language not affected when switching language (ATEAM-16920)
- Owner grid column not populated when accessing reports (ATEAM-16923)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)
- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Not found error messages during deployment (ATEAM-17230)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)
- STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

Error when taking certificates off hold (ATEAM-1445)

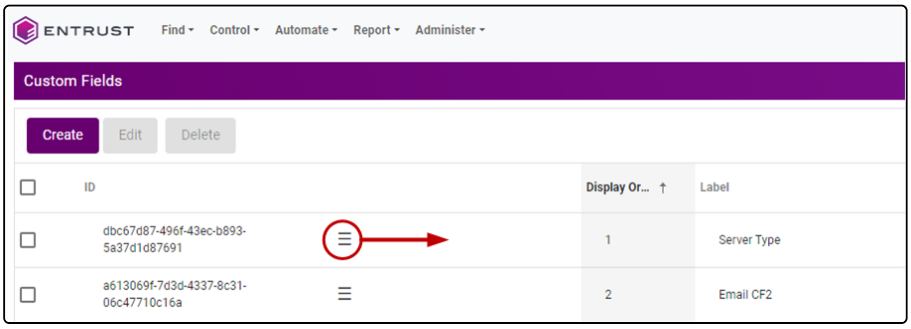
For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, administrators can change the display order of the custom fields. However:

- Reordering a custom field does not change the **Display Order** column value.
- Refreshing the **Custom Field** page reverts all changes.

Workaround: After dragging a custom field to a different position, move the Ξ drag icon within its row to make the changes persistent.



Some endpoint filters display invalid results on report files (ATEAM-15933)

The following endpoint filters do not display correct results on the downloaded report files.

- is empty
- is not empty

Certificates without names not synced from source (ATEAM-16039)

Certificates without a name are not successfully synced from Sources.

Wildcard certificates not recorded (ATEAM-16436)

The application does not record wildcard certificates successfully scanned by the Discovery Scanner.

> Wildcard certificates are certificates containing the wildcard asterisk in the issuer and subject.

Buttons language not affected when switching language (ATEAM-16920)

Switching the language before logging in does not affect the language of the **Delete** and **Cancel** buttons in the **Confirm Delete** popup on the **Destinations** page.

Owner grid column not populated when accessing reports (ATEAM-16923)

The **Owner** grid column is not populated when accessing the **Report Schedules** from the **Report Designer** grid.

Workaround: Access the **Report Schedules** grid from the navigation bar.

The Verify button does not trigger a verification without additional changes (ATEAM-16950)

After the failed verification of a Destination, clicking **Verify** again does not trigger a new verification.

Workaround: Make any change in the create form – for example, change the **Description**.

The public key ID can refer to the private key ID (ATEAM-16982)

When issuing a certificate using the **Key Manager (KMIP)** destination, the **public key ID** is also referring to the **private key ID**

Archive certificates option missing with FIND licenses (ATEAM-16988)

When using a FIND license, the option to **Archive** certificates is missing in the **Actions** dropdown on the **Certificates** grid.

Incomplete CA certificate chain (ATEAM-16997)

When creating a new certificate, the downloaded chain only includes the certificate of the CA that issued the new certificate instead of including the entire chain.

Verification fails for IIS destinations (ATEAM-17030)

Verification fails for IIS destinations if the username includes a domain name – for example:

```
.\user
```

```
domain\user
```

Not found error messages during deployment (ATEAM-17230)

When deploying, you can safely ignore the not found error messages like this one:

```
Error from server (NotFound): configmaps "postgres-config" not found
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

The **Use TLS** option of the SMTP plugin configuration does not enable STARTTLS.

> ⚠ The STARTTLS command upgrades an SMTP communication channel to a secure, encrypted connection using TLS (Transport Layer Security).

Workaround:

1. Log in to the Certificate Manager user console.
2. Navigate to **Administer > Settings > PLUGINS**.
3. Edit the **smtp-notification-plugin** configuration.
4. Activate the following options:
    - Use TLS
    - Use SSL
5. Click **Save**.
6. Edit the plugin configuration again.
7. Disable the **Use SSL** option.
8. Click **Save**.

Release Notes for 4.3.1

See below for the Certificate Hub 4.3.1 release notes.

New features for 4.3.1

Certificate Hub 4.3.1 adds the following feature.

New renewalSerialNumber enrollment value (ATEAM-18902)

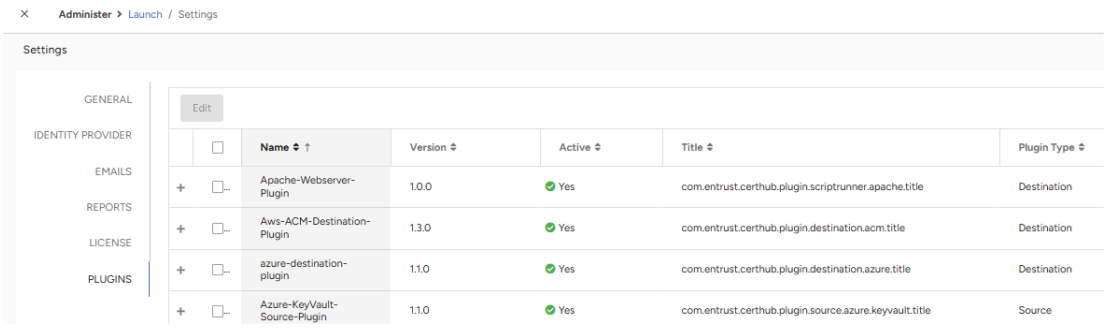
When requesting a certificate renewal from certificate authorities like Sectigo, the enrollment API will include the new `renewalSerialNumber` value.

Fixed bugs for 4.3.1

Certificate Hub 4.3.1 fixes the following bugs.

Plugin titles not properly displayed (ATEAM-18894)

The **Title** column of the plugins grid shows the keys of the plugin titles instead of the real titles.



Error when issuing a certificate for an Apache or IIS destination (ATEAM-18895)

Certificate Manager returns an error when issuing a certificate for an Apache or IIS web server destination.

Error when verifying access and credentials for an Apache or IIS destination (ATEAM-18904)

Certificate Manager may return an error when verifying access and credentials for an Apache or Microsoft IIS web server destination.

Known issues for 4.3.1

Certificate Hub 4.3.1 has the following known issues.

- Error when taking certificates off hold (ATEAM-1445)
- Issues when changing the display order of custom fields (ATEAM-15463)
- Some endpoint filters display invalid results on report files (ATEAM-15933)
- Certificates without names not synced from source (ATEAM-16039)
- Wildcard certificates not recorded (ATEAM-16436)
- Buttons language not affected when switching language (ATEAM-16920)
- Owner grid column not populated when accessing reports (ATEAM-16923)
- The Verify button does not trigger a verification without additional changes (ATEAM-16950)
- The public key ID can refer to the private key ID (ATEAM-16982)
- Archive certificates option missing with FIND licenses (ATEAM-16988)
- Incomplete CA certificate chain (ATEAM-16997)
- Verification fails for IIS destinations (ATEAM-17030)
- Not found error messages during deployment (ATEAM-17230)
- Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)
- Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)
- STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

Error when taking certificates off hold (ATEAM-1445)

For certificates with **Revocation Reason**: **On Hold**, attempting to unhold the certificate may fail, or the **Unhold** option may be absent from the **Actions** dropdown.

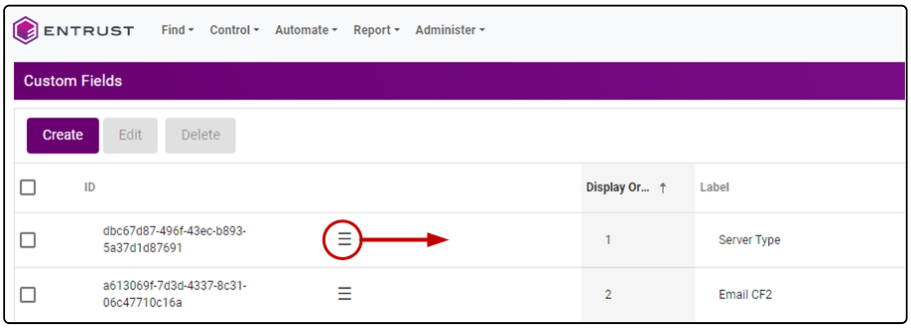
Issues when changing the display order of custom fields (ATEAM-15463)

In the **Custom Fields** page of the web console, administrators can change the display order of the custom fields. However:

- Reordering a custom field does not change the **Display Order** column value.

- Refreshing the **Custom Field** page reverts all changes.

Workaround: After dragging a custom field to a different position, move the ☰ drag icon within its row to make the changes persistent.



Some endpoint filters display invalid results on report files (ATEAM-15933)

The following endpoint filters do not display correct results on the downloaded report files.

- is empty
- is not empty

Certificates without names not synced from source (ATEAM-16039)

Certificates without a name are not successfully synced from Sources.

Wildcard certificates not recorded (ATEAM-16436)

The application does not record wildcard certificates successfully scanned by the Discovery Scanner.

> Wildcard certificates are certificates containing the wildcard asterisk in the issuer and subject.

Buttons language not affected when switching language (ATEAM-16920)

Switching the language before logging in does not affect the language of the **Delete** and **Cancel** buttons in the **Confirm Delete** popup on the **Destinations** page.

Owner grid column not populated when accessing reports (ATEAM-16923)

The **Owner** grid column is not populated when accessing the **Report Schedules** from the **Report Designer** grid.

Workaround: Access the **Report Schedules** grid from the navigation bar.

The Verify button does not trigger a verification without additional changes (ATEAM-16950)

After the failed verification of a Destination, clicking **Verify** again does not trigger a new verification.

Workaround: Make any change in the create form – for example, change the **Description**.

The public key ID can refer to the private key ID (ATEAM-16982)

When issuing a certificate using the **Key Manager (KMIP)** destination, the **public key ID** is also referring to the **private key ID**

Archive certificates option missing with FIND licenses (ATEAM-16988)

When using a FIND license, the option to **Archive** certificates is missing in the **Actions** dropdown on the **Certificates** grid.

Incomplete CA certificate chain (ATEAM-16997)

When creating a new certificate, the downloaded chain only includes the certificate of the CA that issued the new certificate instead of including the entire chain.

Verification fails for IIS destinations (ATEAM-17030)

Verification fails for IIS destinations if the username includes a domain name – for example:

```
.\user
```

```
domain\user
```

Not found error messages during deployment (ATEAM-17230)

When deploying, you can safely ignore the not found error messages like this one:

```
Error from server (NotFound): configmaps "postgres-config" not found
```

Unexpected Error When Pushing Certificate to SFTP (ATEAM-18788)

Pushing a certificate to an SFTP destination may fail with an error message that includes the following:

```
Caused by: java.lang.UnsupportedOperationException
```

Workaround: This error may occur if the plugin manages an outdated hash of the destination SSH key. To resolve this issue, please follow these steps:

1. Edit the SFTP destination as explained in Editing a destination.
2. In the **Edit** dialog, click **Verify** to force an update of the destination SSH key hash.
3. Ensure the hash displayed by the confirmation message matches the hash of the destination public SSH key.
4. Click **Save** to confirm the changes.

Occasional blank page when renewing a Sectigo CA certificate (ATEAM-18799)

The Certificate Manager console may display a blank page when manually renewing a certificate issued by a Sectigo CA

Workaround:

1. Reload the page.
2. Repeat the renewal operation.

STARTTLS not enabled when "Use TLS" option is checked (ATEAM-18848)

The **Use TLS** option of the SMTP plugin configuration does not enable STARTTLS.

> ⚠ The STARTTLS command upgrades an SMTP communication channel to a secure, encrypted connection using TLS (Transport Layer Security).

Workaround:

1. Log in to the Certificate Manager user console.
2. Navigate to **Administer > Settings > PLUGINS**.
3. Edit the **smtp-notification-plugin** configuration.
4. Activate the following options:
    - Use TLS
    - Use SSL
5. Click **Save**.
6. Edit the plugin configuration again.
7. Disable the **Use SSL** option.
8. Click **Save**.

4 Certificate Hub requirements

To deploy Certificate Hub 4.3, you must meet the following requirements.

- Database requirements
- Entrust Deployment Manager requirements

> See the Entrust Deployment Manager installation guide for additional requirements, such as network or machine requirements.

Database requirements

When configuring Certificate Hub, you must provide an external, empty database that meets the following requirements.

- DBMS
- Packages
- Database storage
- Database permissions
- Database SSL connection
- Database names

DBMS

The external Certificate Hub database must be hosted on the following Database Management System (DBMS).

DBMS	Version
PostgreSQL	15 or higher

Packages

Pre-packaged PostgreSQL packages typically include the `postgresql-contrib` subpackage. If not included, install this subpackage to obtain some of the required extensions.

https://www.postgresql.org/docs/current/contrib.html

Database storage

Calculate the required database storage based on the expected certificates and reports. For example, 1G storage is enough for 25,000 certificates and a few weeks of reports.

Data	Quantity	Bytes/Item	Total
Certificates	25,000 certificates	20 KB/certificate	500 MB
Reports	200 reports	1 MB/report	200 MB

Data	Quantity	Bytes/Item	Total
			700 MB

Database permissions

To create an external database user with sufficient permissions, connect to PSQL using the default PostgreSQL user and execute the following commands.

```
CREATE USER ${POSTGRES_USER} WITH NOSUPERUSER CREATEDB ENCRYPTED PASSWORD '$
{POSTGRES_PWD}';
\c postgres ${POSTGRES_USER}
CREATE DATABASE certhub;
\c certhub ${POSTGRES_USER}
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Where:

- `${POSTGRES_USER}` is the database user name.
- `${POSTGRES_PWD}` is the database user password.

Database SSL connection

Certificate Hub only supports SSL-protected connections with the PostgreSQL database.

Database names

Database names should not use uppercase letters to avoid case sensitivity problems. Unquoted identifiers in SQL syntax are converted to lowercase, which can lead to problems when mapping to a name with uppercase letters.

Entrust Deployment Manager requirements

Certificate Hub 4.3.x runs on Entrust Deployment Manager 2.0.x. See the Entrust Deployment Manager guide for how to:

- Install Entrust Deployment Manager.
- Upgrade Entrust Deployment Manager to the latest 2.0.x version.

5 Preparing the deployment

Prepare the Certificate Hub deployment as explained in the following sections.

Getting the Certificate Hub license

After making the order for Certficate Hub, you will get an email from licensing@pki.entrust.com with a signed license file.

Downloading the installation files

You need to download the following installation files from TrustedCare.

File	Description
Certificate Hub for EDM	The `.sln` installation file for deploying Certificate Hub on Entrust Deployment Manager.
Database Management Scripts	The package containing the `dbctl.sh` script for Backing up and restoring the database.

To download the installation files

1. Log in to https://trustedcare.entrust.com
2. Go to **PRODUCTS > PKI > Certificate Hub.**
3. Click on the Certificate Hub version you want to download.
4. Select the **SOFTWARE DOWNLOADS** tab to download the installation files.
5. Select the **DOCUMENTS** tab to download the product documentation.

Verifying the downloaded files

Generate a digest to verify the integrity of each downloaded installation and documentation file. On a Windows machine, you can run the following command line to generate the digest of the `<file>` file.

```
certutil -hashfile <file> SHA256
```

For example:

```
>certutil -hashfile c:\Users\john\Downloads\edm-2.0.2.iso SHA256
SHA256 hash of c:\Users\john\Downloads\edm-2.0.2.iso:
d841d57c7e1433622d219a7dea405935ff593a6831c1c94ba1c9dbde763b5baa
CertUtil: -hashfile command completed successfully.
```

On the **SOFTWARE DOWNLOADS** and **DOCUMENTATION** tabs, click the **Digest** column for each downloaded file and verify the displayed SHA-256 digest matches the generated one.

> ⚠ Although TrustedCare also displays the MD5 and SHA-1 digests, we recommend using only the SHA-256 algorithm, which is more secure. Further versions of TrustedCare will remove the MD5 and SHA-1 algorithms from the digest list.

6 Starting up and deploying Certificate Hub

Start up and deploy Certificate Hub with the Management Console as explained in the "Starting up and deploying solutions" section of *Entrust Deployment Manager - Installation and Administration Guide*.

- When uploading the license file, do not change the name of the license file.
- When configuring the solution, set the Certificate Hub-specific settings described in: https://api.managed.entrust.com/csp/1.2/Configuring-and-deploying-Certificate-Manager.html

If you already have a Certificate Hub installation, upgrade to 4.1.0 as explained in Upgrading.

7 Using the Certificate Manager console

After deploying Certificate Hub, you can use the Certificate Manager to manage certificate issuance and lifecycle.

Logging in to the Certificate Manager console

See below for opening a session in the Certificate Manager console of Certificate Hub.

To log in to the Certificate Manager console

1. Open a web browser at the following URL.

   ```
   https://<host>/certhub
   ```

   Where `<host>` is the value of the hostname or IP address assigned to the **Certificate Hub Hostname** configuration parameter.
2. Authenticate using the credentials assigned to the Initial **Administrator Username** and **Initial Administrator Password** configuration parameters.

Browsing the Certificate Manager console guide

The Certificate Manager console user guide is published as part of the Cryptographic Security Platform documentation at:

https://api.managed.entrust.com/csp/1.2/Using-Certificate-Manager.html

8 Backing up and restoring the database

See below for backing up and restoring the Certificate Hub database.

Installing the dbctl.sh script

Install the `dbctl.sh` script in a folder containing the configuration of the original installation.

To install the dbctl.sh script

1. Run the following command to export the Certificate Hub configuration in the `<dir_path>` directory.

```
sudo clusterctl solution config export -n certhub --path <dir_path>
```

2. Download the Database Management Scripts compressed file as explained in Downloading the installation files.
3. Extract the `dbctl.sh` script in the `<dir_path>` directory.

Backing up the database

See below for backing up the Certificate Hub database.

⚠ Back up the databases regularly to restore your data in case of disaster recovery.

Vacuuming the database

Run this command once before any backup to release orphaned pages from the database and decrease its size.

```
sudo dbctl.sh vacuum -n certhub
```

Backing up the database contents

Back up the Certificate Hub database using the tools provided by the DBMS.

Backing up the database encryption key

Run the following command to back up the database encryption key.

```
sudo dbctl.sh backup -n certhub
```

Restoring the database

To restore the Certificate Hub database, follow the steps below in the same Certificate Hub version used when Backing up the database.

- Restoring the configuration
- Restoring the database contents
- Restoring the database encryption key
- Completing the database restoration

Restoring the configuration

Reapply the following configurations.

- Name of the PostgreSQL Database
- Database User Name
- Database User Password
- Host of the PostgreSQL database
- External database port
- SSLMode for the PostgreSQL external database
- CA Certificate(s)

See https://api.managed.entrust.com/csp/1.2/Configuring-and-deploying-Certificate-Manager.html for a description of each setting.

Restoring the database contents

Restore the Certificate Hub database using the Database Management System (DBMS) tools.

Restoring the database encryption key

Run the following command to restore the database encryption key.

```
sudo dbctl.sh restore -n certhub --backup-file <backup-file>
```

Where `<backup-file>` is the path of the backup file.

> Before running this command, you can ignore or delete the `user-creation` and `role-update` jobs in ERROR state.

Completing the database restoration

Redeploy Certificate Hub to make effective the restoration of the database encryption key.

9 Error reference

When executed, Certificate Hub can print the following errors.

Authentication and authorization errors

The application throws the following authentication and authorization errors.

Code	Message
ERR_1006	Failed to hash the password for user: `<Username>`
ERR_1010	`hasPermission` unexpectedly invoked for `<Permission>`
ERR_1011	The util command must have a `--cmd` argument.
ERR_1012	Unknown command `<Command>`
ERR_1013	`--username`, `--password`, and `--email` must be supplied to the `createUser` command.
ERR_1014	Unexpected crypto error:
ERR_1015	Error creating default cert expiry rule for initial user:
ERR_1016	`--username` and `--role` must be provided.
ERR_1017	Unexpected crypto exception:
ERR_1040	Unexpected parsing error while loading auth request:
ERR_1041	Unexpected parsing error while saving auth request:

Code	Message
ERR_1042	Unexpected parsing error while removing auth request:
ERR_1046	Could not find password auth provider entry.
ERR_1047	Failed to hash the password for user: `<Username>`
ERR_1048	Cannot update non-existent user. User must have existing id.
ERR_1049	Login denied. Tenant id not found for user `<Username>`.
ERR_1056	More than one LDAP auth provider registration found (`<Number of registrations>`). Unexpected behavior may result!
ERR_1057	More than one PASSWORD auth provider registration found (`<Number of registrations>`). Unexpected behavior may result!
ERR_1076	Unable to create keystore: `<CA>`
ERR_1077	Cryptography issue when creating user.
ERR_1078	Cryptographic error processing password.
ERR_1079	Unable to initialize SSLContext for LDAPS
ERR_1080	More that one LDAP auth provider registration present. Unexpected results may occur.
ERR_1081	LDAP authentication error.

Code	Message
ERR_1082	Unexpected exception during LDAP lookup.
ERR_1083	Error closing LDAP context.
ERR_1084	Could not find Active Directory user.
ERR_1085	Error creating the daemon user:
ERR_1086	Error creating the initial user:

Administration errors

The application throws the following administration errors.

Code	Message
ERR_1100	Internal error occurred
ERR_1101	Error parsing license : `<Error message>`
ERR_1102	Error parsing license: Epm client could not parse license
ERR_1103	Error parsing license : `<Error message>`
ERR_1104	Error parsing license: Epm client could not parse license
ERR_1105	Order Number of `<Order number>` uploaded license doesn't match the existing license `<Customer contact reference>`

Code	Message
ERR_11106	License revision `<Revision>` already uploaded.
ERR_11107	Uploaded license revision `<Uploaded revision>` is outdated. Current license revision : `<Current revision>`.
ERR_11108	Failed to create the license expiry schedule
ERR_11109	Failed to send email for license consumption
ERR_11110	Failed to send email for license expiry
ERR_11111	Failed to check the license expiry schedule
ERR_11112	Failed to delete existing license expiry schedule
ERR_11113	Failed to create the license expiry schedule
ERR_11114	Invalid plugin name: `<Plugin name>`
ERR_11115	Error executing plugin options for plugin: `<Plugin name>`
ERR_11116	Error loading plugin jar `<JAR file name>`. Plugin will not be loaded!
ERR_11117	Error loading plugin classloader.
ERR_11118	Plugin `<Canonical name>` is missing a language bundle. Plugin will not be loaded!

Code	Message
ERR_11919	Plugin `<Canonical name>` has invalid language bundle. No messages section found. Plugin will not be loaded!
ERR_11920	Plugin `<Canonical name>` has invalid language bundle. No languages found. Plugin will not be loaded!
ERR_11921	Plugin `<Canonical name>` has an invalid language bundle. Language `<Key>` is an invalid map. Plugin will not be loaded!
ERR_11922	Plugin `<Canonical name>` has an invalid language bundle. Language `<Name>`, key `<Key>` is invalid (`<Value>`). Plugin will not be loaded!
ERR_11923	Error initializing plugins! No `<Plugin class name>` plugins will be loaded until invalid plugin is removed!
ERR_11924	updatePlugin: Error converting global options to Json string from list
ERR_11925	validatePluginStateUpdate : cannot deactivate plugins that don't require license
ERR_11926	validatePluginStateUpdate : cannot deactivate plugin `<Name>` as its in use by destination : `<Label>`
ERR_11927	validatePluginStateUpdate : cannot deactivate plugin `<Name>` as its in use by source : `<Label>`
ERR_11928	addPlugin: Error converting global options to Json string from list
ERR_11929	Error converting global options to list from `Json byte[]`
ERR_11930	addPlugin: Error converting global options to list from `Json byte[]`
ERR_11931	Error fetching language bundle, Plugin `<Plugin name>` not found

Code	Message
ERR_1132	Failed to add an entry to the keystore: `<TBU>`
ERR_1133	Plugin update failed, plugin ID `<Plugin ID>`
ERR_1149	Failed importing multiple addresses.
ERR_1150	Failed importing single addresses.
ERR_1153	Failed to check the events retention schedule: `<Error>`
ERR_1154	Failed to create the events retention schedule: `<Error>`
ERR_1199	Unhandled exception caught

Automation errors

The application throws the following automation errors.

Code	Message
ERR_1207	Failed to mapping existing source plugin options.
ERR_1208	Failed to process existing source plugin options.
ERR_1209	Failed to migrate existing source plugin options.
ERR_1214	Failed to send email for report `<Report name>`, schedule id: `<Schedule ID>`. Error:
ERR_1215	Failed to generate missing report: `<Report ID>`

Code	Message
ERR_12016	Failed to generate missing schedule: `<Schedule ID>`
ERR_12017	Failed to return report: `<Report ID>` . Error: `<Error>`
ERR_12018	Error while retrieving report data:
ERR_12019	Error while generating report:
ERR_12020	User `<Username>` does not have permission to edit or delete report `<Report name>`
ERR_12021	Error while generating report: `<Error>`
ERR_12022	User `<Username>` does not have permission to access artifact `<Artifact ID>`
ERR_12023	User `<Username>` does not have permission to access execution `<Execution ID>`
ERR_12024	Failed to check the reports retention schedule: `<Error>`
ERR_12025	Failed to create the reports retention schedule: `<Error>`
ERR_12030	Field ' `<Name>` ' value ' `<Value>` ' cannot be parsed as `<Type>` . Field will be treated as a String.
ERR_12031	Unexpected exception while processing rule. RULE WILL BE SKIPPED!
ERR_12032	Expiry notification is dropped for certificate `<Certificate name>` . The address field `<Address field>` is empty.

Code	Message
ERR_1233	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is not referring to a text custom field.
ERR_1234	Action plugins not currently supported. THIS ACTION WILL BE SKIPPED!
ERR_1235	Exception while executing rule. RULE WILL BE SKIPPED!
ERR_1236	Error running rules engine for certificate renewal rule.
ERR_1237	Execution of action failed.
ERR_1238	FAILED processing conditions. RULE WILL BE SKIPPED!
ERR_1239	I/O issue while parsing conditions. RULE WILL BE SKIPPED!
ERR_1240	Error running rules engine for event.
ERR_1241	Could not parse plugin config, ACTION WILL BE SKIPPED: `<Plugin config>`
ERR_1242	FAILED to create the expiration rules schedule! Expiry notifications will not be sent!
ERR_1243	Error while processing event rule conditions. RULE WILL BE SKIPPED!
ERR_1244	Only NOTIFICATION actions are supported! ACTION WILL BE SKIPPED!
ERR_1254	Unexpected IOException while formatting the certificate. Error:

Code	Message
ERR_1255	Unexpected IOException while formatting the certificate chain. Error:
ERR_1256	Unexpected IOException while formatting the certificate. Error:
ERR_1260	FAILED to create the key manager scan schedule! Key managers will not be scanned!
ERR_1261	Error encountered while scanning key manager.
ERR_1262	Error encountered while scanning source.
ERR_1271	User `<User ID>` does not have permission to view, edit or delete destination `<Label>`
ERR_1272	Error verifying destination config `<Label>`
ERR_1273	Error verifying destination config for plugin `<Plugin name>`
ERR_1274	Error while generating report.
ERR_1275	Failed to retrieve schedule runtimes for `<Schedule name>`
ERR_1276	Failed to parse schedule runtimes for `<Schedule name>`
ERR_1280	Failed processing conditions for renewal success. RULE WILL BE SKIPPED!
ERR_1281	I/O issue while parsing conditions for renewal success. RULE WILL BE SKIPPED!
ERR_1282	Failed processing conditions for renewal failure. RULE WILL BE SKIPPED!

Code	Message
ERR_1283	I/O issue while parsing conditions for renewal failure. RULE WILL BE SKIPPED!
ERR_1289	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is empty.
ERR_1290	Error running rules engine for certificate renewal rule.
ERR_1291	Failed processing rule. RULE WILL BE SKIPPED!
ERR_1292	I/O issue while running rule. RULE WILL BE SKIPPED!
ERR_1293	Expiry notification is dropped for certificate `<Certificate name>`. The custom field `<Custom field>` is empty.
ERR_1294	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is not referring to a text custom field.
ERR_1295	Expiry notification is dropped for certificate `<Certificate name>`. The address field `<Address field>` is empty.
ERR_1296	Error running rules engine for certificate renewal rule.
ERR_1299	Execution of rule action failed.

Control errors

The application throws the following control errors.

Code	Message
ERR_1302	Error getting authority capabilities from CAGW

Code	Message
ERR_1303	Failed to check the domain sync trigger
ERR_1304	Unable to add domain sync for authority
ERR_1305	Internal error contacting CAGW.
ERR_1306	Error while reading XML stream from upload.
ERR_1307	Unexpected exception while pushing certificate:
ERR_1308	HTTP Error while uploading certificate: `<Error>` : \n `<Response body>`
ERR_1309	Error while uploading certificate: `<Error>`
ERR_1310	Unable to parse properties for domain: `<Domain name>`
ERR_1311	User `<User ID>` doesn't have access to authority `<Authority ID>`
ERR_1312	Internal error contacting CAGW.
ERR_1313	Unable to get profiles for authority
ERR_1314	Unable to get the subject DN for authority
ERR_1315	Unable to get the Capabilities for authority
ERR_1316	Unexpected error contacting CAGW: `<Error>`
ERR_1330	User `<User ID>` does not have permission to view, edit or delete key manager `<Key manager>`
ERR_1331	Error verifying key manager config `<Key manager label>`
ERR_1332	saveOrUpdateKeyManager: Error converting plugin options to Json string from list
ERR_1333	Error converting plugin options to list from Json byte[]

Code	Message
ERR_1334	Error verifying key manager config for plugin `<Plugin name>`
ERR_1349	Failed to sync domains, Error from CAGW: `<Error>`
ERR_1350	Unexpected response received from CAGW
ERR_1351	Internal error contacting CAGW
ERR_1352	Unexpected response received from CAGW: `<Error>`
ERR_1353	Unexpected response received from CAGW: `<Error>`
ERR_1354	Unexpected response received from CAGW: `<Error>`
ERR_1355	Error configuring the SSL client connection to the CAGW APIs.
ERR_1356	Error configuring the SSL client connection to the CAGW APIs.
ERR_1357	Error configuring the SSL client connection to the CAGW APIs
ERR_1358	Error configuring the SSL client connection to the CAGW APIs.
ERR_1359	Error configuring the SSL client connection to the CAGW APIs.
ERR_1362	Error parsing authority certificate validity period: `<Certificate validity period>`
ERR_1363	Error parsing authority certificate validity period: `<Certificate validity period>`
ERR_1374	Error response from CAGW: `<Error>`
ERR_1375	Unable to parse properties for domain: `<Domain name>`
ERR_1376	Internal error contacting CAGW: `<Error>`
ERR_1377	Internal error contacting CAGW.

Code	Message
ERR_1378	Internal error contacting CAGW.
ERR_1379	Internal error contacting CAGW while responding to an authority request.
ERR_1380	Failed to create the authority domain sync schedule for authority `<Authority ID>`
ERR_1381	Failed to delete the authority domain sync schedule for authority `<Authority ID>`
ERR_1382	Certificate Authority `<Authority ID>` not found
ERR_1383	Unable to parse plugin options for authority `<Authority ID>` :
ERR_1384	Error response from CAGW while getting domain: `<Domain name>`
ERR_1385	Failed to get domain. Error from CAGW: `<Error>`
ERR_1386	Failed to submit domain, Error from CAGW: `<Error>`
ERR_1387	Unable to fetch whois record from server `<Server name>` . Error:
ERR_1388	Unable to close whois client connection with server `<Server name>` . Error:
ERR_1389	Unable to fetch whois record from default host. Error:
ERR_1390	Unable to close whois client connection with default server. Error:
ERR_1392	Error on DNS lookup : `<Error>`
ERR_1394	Failed to submit domain, Error from CAGW: `<Error>`
ERR_1397	Certificate Authority `<Authority ID>` not found
ERR_1398	Unable to parse plugin options for authority `<Authority ID>`

Code	Message
ERR_1399	Unable to import/update domain id `<Domain ID>` due to Json parsing error from authority `<Authority ID>`

Certificate errors

The application throws the following certificate errors.

Code	Message
ERR_1426	Renewal failed. Missing certificate id.
ERR_1427	Failed auto renewal for certificate `<Certificate ID>`.
ERR_1428	Automated renewal failed for certificate `<Certificate ID>` due to certificate processing error
ERR_1430	Automated renewal failed for certificate `<Certificate ID>` due to destination errors: `<List of errors>`
ERR_1431	Failed to find the renewal daemon user for auto renewal
ERR_1432	Failed to create the renewal schedule for cert `<Certificate serial>` : `<Error>`
ERR_1433	Failed to check the renewal schedule `<Error>`
ERR_1434	Failed to create the renewal schedule `<Error>`
ERR_1435	Adding definition for custom field with duplicate display order : `<Label>` of type `<Type>` at position `<Display order>`
ERR_1436	Deleting definition for custom field with Id : `<Metadata ID>` failed as it is in use by `<Certificates using metadata>` certificates

Code	Message
ERR_1437	Updating definition for custom field with duplicate display order : `<Label>` of type `<Type>` at position `<Display order>`
ERR_1438	Updating definition for custom field with Id : `<Metadata ID>` failed as it is in use by `<Certificates using metadata>` certificates
ERR_1439	Updating definition for custom field with duplicate display order : `<Metadata values>`
ERR_1440	Other certificate custom field definitions exists with same display order `<List>`
ERR_1441	Updating definition for custom field with Id : `<Metadata ID>` failed as one of its value `<List>` is in use by `<Certificates>` certificates
ERR_1442	Error parsing the value `<Value>` for custom field `<Metadata ID>`
ERR_1443	Unsupported Operator `<Operator>` for custom field Id: `<Metadata ID>`
ERR_1450	Could not unarchive certificate because entitlement limit reached.
ERR_1452	Error response from CAGW `<Error>`
ERR_1453	Error exporting a certificate: `<Error>`
ERR_1454	Failed to parse certificate `<Certificate name>` stored in DB. Error: `<Error>`
ERR_1455	Certificate Chain is not available for export
ERR_1456	Error while exporting certificate: `<Error>`

Code	Message
ERR_1457	Error saving chain to keystore for export of : `<Certificate name>`
ERR_1458	Error adding P12 to response stream
ERR_1459	Unable to parse response from CAGW to export certificate for : `<Certificate name>`. Error: `<Error>`
ERR_1460	Certificate can not be exported since the issuing Authority is not known
ERR_1461	Certificate Authority not found
ERR_1462	Error adding P12 to response stream
ERR_1463	Unexpected response received from CAGW when exporting a certificate
ERR_1464	Internal error contacting CAGW
ERR_1465	Failed to export certificate for `<Certificate name>`. Error from CAGW: `<Error>`
ERR_1466	Failed to export certificate for `<Certificate name>` with serial number `<Certificate serial number>`. Certificate key is not backed up.
ERR_1467	Unable to parse response from CAGW to export certificate for : `<Certificate name>`. Error: `<Error>`
ERR_1468	Export private key is not supported for export type `<Type>` You can uncheck \\\"Include Private Key\\\" and try again, however, your exported certificate will not have the private key
ERR_1469	Export certificate chain is not supported for export type `<Type>` You can uncheck \\\"Include Certificate Chain\\\" and try again, however, your exported certificate will not have certificate chain

Code	Message
ERR_1470	Public certificate must be requested for export type `<Type>`
ERR_1471	At least one of public certificate, certificate chain or private key must be requested for export type `<Type>`
ERR_1472	At least one of public certificate, certificate chain or private key must be requested for export type `<Type>`
ERR_1473	Unable to revoke the authority `<Authority name>`
ERR_1474	Unable to unhold the authority `<Authority name>`
ERR_1477	Error building certificate query with filter : `<Filter>` . Error `<Error>`
ERR_1478	Error fetching certificates with predicate : `<Predicate>` . Error `<Error>`
ERR_1479	Certificate Bulk Edit Error: 'certificatesFilter' missing from request body
ERR_1480	Certificate Bulk Edit Error: If 'clearOutAccessTags' is set, 'accessTags' must be empty.
ERR_1481	Certificate Bulk Edit Error: No updated values provided
ERR_1482	Certificate Bulk Edit Error building certificate query with filter : `<Filter>` , Error : `<Error>` .
ERR_1483	Certificate Bulk Edit Error building certificate query with filter : `<Filter>` , Error : `<Error>` .
ERR_1484	Certificate Bulk Edit Error updating certificates with filter : `<Filter>` , Error : `<Error>`

Code	Message
ERR_1486	Certificate unhold error : Could not find certificate with id: `<Certificate ID>` .
ERR_1487	Certificate unhold error : No Authority Id associated with this certificate: `<Certificate ID>` .
ERR_1488	Certificate unhold error : Cannot unhold certificate `<Certificate ID>` . Authority is not active : `<Authority ID>` .
ERR_1489	Certificate unhold error : Cannot unhold certificate `<Certificate ID>` . No external id found.
ERR_1490	Issue certificate error : Subject DN is required for CSR.
ERR_1491	Issue certificate error : CAGW failed to create certificate for authority `<Authority ID>`
ERR_1492	Issue certificate error : CAGW Failed to create certificate: `<Key manager ID>` .
ERR_1493	Issue certificate error : Subject DN is required for CSR.
ERR_1494	Issue certificate error : Subject DN is required for CSR.
ERR_1495	Issue certificate error : Subject DN is required for CSR.
ERR_1496	Issue certificate error : Subject DN is required for CSR.
ERR_1497	Failed to save certificate: `<Error>`
ERR_1498	Failed to upload certificate to the key manager `<Key manager ID>` . Error `<Error>`

Code	Message
ERR_1499	Certificate revoke error : No Authority Id associated with this certificate. `<Certificate ID>`
ERR_1500	Certificate revoke error : Cannot revoke certificate `<Certificate ID>`. Authority `<Authority ID>` is not active.
ERR_1501	Certificate revoke error : Cannot revoke certificate `<Certificate ID>`. No external id found.
ERR_1502	Failed to apply service-level filters on query `<Filter>`
ERR_1503	Failed to apply service-level filters on query `<Filter>`
ERR_1504	Failed to apply service-level filters on query `<Filter>`
ERR_1505	Could not find certificate with id `<Certificate ID>`
ERR_1506	Could not find certificate with id `<Certificate ID>`
ERR_1508	Failed to issue a certificate from authority `<Authority name>`. Error `<Error>`
ERR_1509	Failed to parse the X509 certificate `<Certificate body>` \n Message: `<Error>`
ERR_1510	Unable to find certificate `<Certificate ID>`
ERR_1511	Failed to process the certificate `<Certificate import request body>` \n Message: `<Error>`
ERR_1512	Failed to process the certificate `<Certificate body>` \n External ID: `<Certificate External ID>` \n Message: `<Error>`

Code	Message
ERR_1513	Failed to apply service-level filters on query `<Filter>`
ERR_1514	Failed to run the certificate count query: `<Error>`
ERR_1521	Error verifying source config `<Source Label>`
ERR_1522	Error verifying source config for plugin `<Plugin name>`
ERR_1523	addOrUpdateSource: Error converting plugin options to Json string from list
ERR_1524	Error scheduling source sync, sources will not ne scanned!
ERR_1525	Error creating certificate from certficate request
ERR_1526	Failed to send new external certificate request notification to approver(s). Error : `<Notification message>`
ERR_1527	Failed to send external certificate request cancellation notification to requestor. Error : `<Notification message>`
ERR_1528	Failed to send certificate request approval notification to requestor. Error : `<Notification message>`
ERR_1529	Failed to send certificate request rejection notification to requestor. Error : `<Notification message>`
ERR_1530	Failed to send new certificate request notification to internal requestor. Error : `<Notification message>`
ERR_1531	Failed to send new internal certificate request notification to approver(s). Error : `<Notification message>`

Code	Message
ERR_1533	Failed to send new certificate request notification to external requestor. Error: `<Notification message>`
ERR_1534	CSR key algorithm `<CSR key algorithm>` does not match the required key algorithm `<Allowed key algorithm>`
ERR_1536	CSR key algorithm keysize `<CSR key size>` does not meet minimum public key size required : `<Allowed key size>`
ERR_1537	Invalid certificate signing request provided
ERR_1540	Failed to send new certificate request notification to external requestor. SMTP Notification Plugin not found
ERR_1541	Failed to send certificate request cancellation notification to external requestor. SMTP Notification Plugin not found
ERR_1542	Failed to send new external certificate request notification to approver(s). SMTP Notification Plugin not found
ERR_1543	Failed to send new certificate request notification to admin. SMTP Notification Plugin not found
ERR_1544	Failed to send new internal certificate request notification to approver(s). SMTP Notification Plugin not found
ERR_1545	Failed to send notification for certificate request cancellation. SMTP Notification Plugin not found
ERR_1546	Failed to send notification for certificate request approval. SMTP Notification Plugin not found
ERR_2010	Found invalid certificate with name `<Certificate name>`.
ERR_2011	Unexpected exception while processing certificate.

Code	Message
ERR_2012	Error processing certificate.
ERR_2013	Error creating certificate factory.
ERR_2015	Failed to parse certificate `<Certificate name>` stored in DB. Error: `<Error message>`

10 Upgrading

See below for instructions on upgrading from Certificate Hub 3.3.0 or higher to version 4.3.

> ⚠ If you are using a version of Certificate Hub below 3.3.0, you must first upgrade to Certificate Hub 3.3.0, as explained in *Certificate Hub 3.3 - EDM Deployment Guide*.

To upgrade the Certificate Hub solution

1. Log in to the Management Console provided by Entrust Deployment Manager.
2. Upload the Certificate Hub 4.3.x solution file.
3. If required, update the Certificate Hub configuration.
4. Deploy the new Certificate Hub version.

11 Integration report

Certificate Hub allows you to view and manage certificates across your enterprise, regardless of the issuer.

> Certificate Hub Manager uses Entrust CA Gateway as the underlying CA interface.

Entrust products compatible with Certificate Hub

Product(s)	Version(s)	Support Notes
CA Gateway	3.x	
IDaaS	Not applicable	IDaaS (Identity as a Service) is supported as an Identity Provider for multi-factor login

Supported Deployment Platforms

Platform	Version	Support Notes
EDM	2.0.2	

Supported Web Browser

Certificate Hub administration console supports the following web browsers.

Browser	Windows	Mac OS
Apple Safari	5 or higher	5 or higher
Google Chrome	8 or higher	8 or higher
Microsoft Edge	The stable versions listed by Microsoft in https://learn.microsoft.com/en-us/deployedge/microsoft-edge-support-lifecycle	Not supported

Browser	Windows	Mac OS
Mozilla Firefox	9 or higher	9 or higher

Browser compatibility is quite high, so most versions operate without issue. If there is an issue, we will address it using the latest browser version available for the operating system.

Databases supported by Certificate Hub

The external Certificate Hub database must be hosted on PostgreSQL 15 or higher.

Plugins supported by Certificate Hub

Certificate Hub supports the following plugins.

Plugin	Version	Support Notes
KMIP KMS	2.0	Works for any KMS supported by a KMIP 2.0 protocol
F5 BIG IP	F5 iControl REST API version 15.1	Also compatible with newer F5 BIG-IP versions.

Standards supported by Certificate Hub

Certificate Hub supports the following standards.

Standard	Version	Supported for external IdP providers	Notes
OpenID Connect (OIDC)	1.0	✔	OIDC 1.0 is a layer on top of OAuth 2.0.
Lightweight Directory Access Protocol (LDAP)	v3	✔	Includes Active Directory.