

Managing Inbound Connection Endpoints

Date published: 2021-04-06

Date modified: 2024-01-09

CLOUDERA

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Deleting and reassigning Inbound Connection Endpoints.....	4
Renewing certificates for Outbound Connection Endpoints.....	4
Renew certificates manually for an Inbound Connection Endpoint.....	4

Deleting and reassigning Inbound Connection Endpoints

Learn about deleting and reassigning Inbound Connection Endpoints.



Note: Inbound Connection Endpoints exist within the environment where they were created. They cannot be moved between environments. If you delete an environment, endpoints get destroyed as well and they cannot be reused.

- To delete an Inbound Connection Endpoint, you need to terminate the flow deployment to which it is currently assigned, selecting the Delete assigned endpoint hostname option during termination.
- To reassign an existing Inbound Connection Endpoint, you need to delete the flow deployment to which it is currently assigned, making sure that the Delete assigned endpoint hostname option is not selected. You can reassign existing, unassigned endpoints during flow deployment.

Renewing certificates for Outbound Connection Endpoints

Learn about certificate renewal for Inbound Connection Endpoints.

For security reasons, the certificates generated for Inbound Connection Endpoints need to be renewed after a certain period:

- NiFi Inbound SSL Context Service - 90 days
- Client SSL Context - 1 year
- Client CA - 5 years

CDF polls certificate status, and they are automatically renewed 30 days before expiration. At this point you receive a notification on the Alerts tab, asking you to restart the deployment so that the new certificate takes effect.

If it becomes necessary, for example, because a certificate is compromised, you can also renew certificates manually.

Renew certificates manually for an Inbound Connection Endpoint

If you need to replace an X.509 certificate for an inbound connection endpoint before it expires, you can do so manually.

Before you begin

You need DFFlowAdmin privilege to perform this action.

Procedure

1. On the Dashboard select the DataFlow deployment for which you want to renew the certificate. The Deployment Details pane opens.
2. On the Deployment Details pane click Manage DataFlow.
3. On the Deployment Manager page from Deployment Settings pane select NiFi Configuration.

4. Click Renew Certificates.

- To renew the server certificate, select NiFi Inbound SSL Context Service.



Note: Each server certificate is limited to five renewals in a 7 day sliding window.

- To renew the client certificate, select Client SSL Context.
- If you leave Revoke previously issued client certificates unchecked, existing client certificates remain valid and existing clients can continue to connect to your deployment using it. By selecting the Revoke previously issued client certificates option, you invalidate all existing certificates and you will need to add the new certificate to existing clients so that they can keep connecting to your CDF deployment.

5. Click Renew & Restart.

The UI switches to the **KPIs and Alerts** pane where you can monitor as your deployment restarts and the new certificate or certificates become available.

What to do next**If you have renewed the NiFi Inbound SSL Context Service:**

You have take no further action.

If you have renewed the Client SSL Context:

After your CDP deployment has restarted, you switch to the NiFi Configuration pane to download the Client Certificate and the Client Private Key. You can then add these to your client.

Related Information

[Connecting applications to an endpoint](#)