



# Data Platform

## Certificate Authentication

# Legal Information

**Book Name:** Certificate Authentication

**Part Number:** FLEXERA- CAC5535

**Product Release Date:** June 2022

## Copyright Notice

Copyright © 2023 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

## Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/legal/intellectual-property.html>. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

## Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

## Table of Contents

<b>Legal Information.....</b>	<b>1</b>
<b>I. Overview .....</b>	<b>3</b>
<b>II. Prerequisites.....</b>	<b>3</b>
<b>III. How to Configure and Test .....</b>	<b>3</b>
<b>A. Pre-Configuration (for Data Platform and User Console Application Servers).....</b>	<b>3</b>
1. Install Client Certificate Mapping Authentication Feature .....	3
2. Enable "Active Directory Client Certificate Authentication" for IIS.....	4
3. Configure SSL Bindings for Default Website .....	6
<b>B. Data Platform Configuration.....</b>	<b>7</b>
1. Install Data Platform 5.5.35 or Patch Your Installation to At Least 5.5.35 .....	7
2. Run the Configuration Wizard for Data Platform .....	8
<b>C. User Console Configuration .....</b>	<b>15</b>
1. For New Installations of Data Platform .....	15
2. For Existing Data Platform Installations .....	15
<b>IV. Usage and Troubleshooting.....</b>	<b>18</b>
<b>A. Usage .....</b>	<b>18</b>
<b>Product Support Resources .....</b>	<b>21</b>

## I. Overview

Flexera is introducing a new authentication option into Data Platform: "Certificate Authentication". Certificate Authentication is an SSO implementation which leverages PKI to authenticate and authorize users via digital certificates that can be stored and secured on a computer or on a smartcard device. This means that instead of supplying a standard username and password to a PKI enabled application, you present a certificate which asserts your identity.

With Certificate Authentication, Enterprises that rely on PKI to authenticate users in a Windows environment where Active Directory is also deployed can now configure Data Platform to use the same PKI without the requirement of proxies or other intermediary devices.

## II. Prerequisites

This feature requires:

- Data Platform 5.5.35 or higher
- A fully functioning PKI Environment integrated with Microsoft Active Directory
- The "Client Certificate Mapping Authentication" feature for the Web Server Role
- PKI Certificates issued to the Data Platform and User Console application servers

## III. How to Configure and Test

### A. Pre-Configuration (for Data Platform and User Console Application Servers)

#### 1. Install Client Certificate Mapping Authentication Feature

To install this feature, use the "Add Roles and Features Wizard" and within the "Web Server (IIS)" Role, find and enable the "Client Certificate Mapping Authentication" feature within the "Security" option

## Select server roles

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

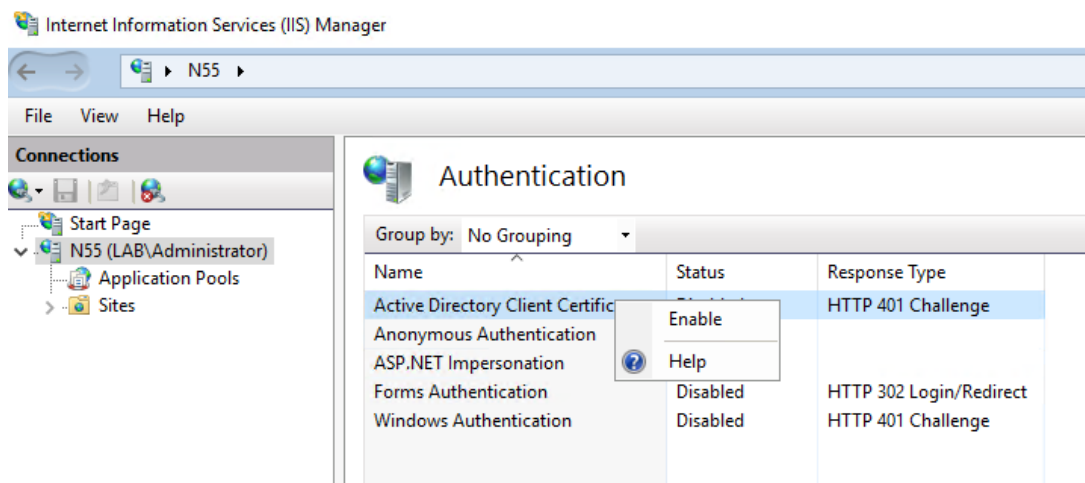
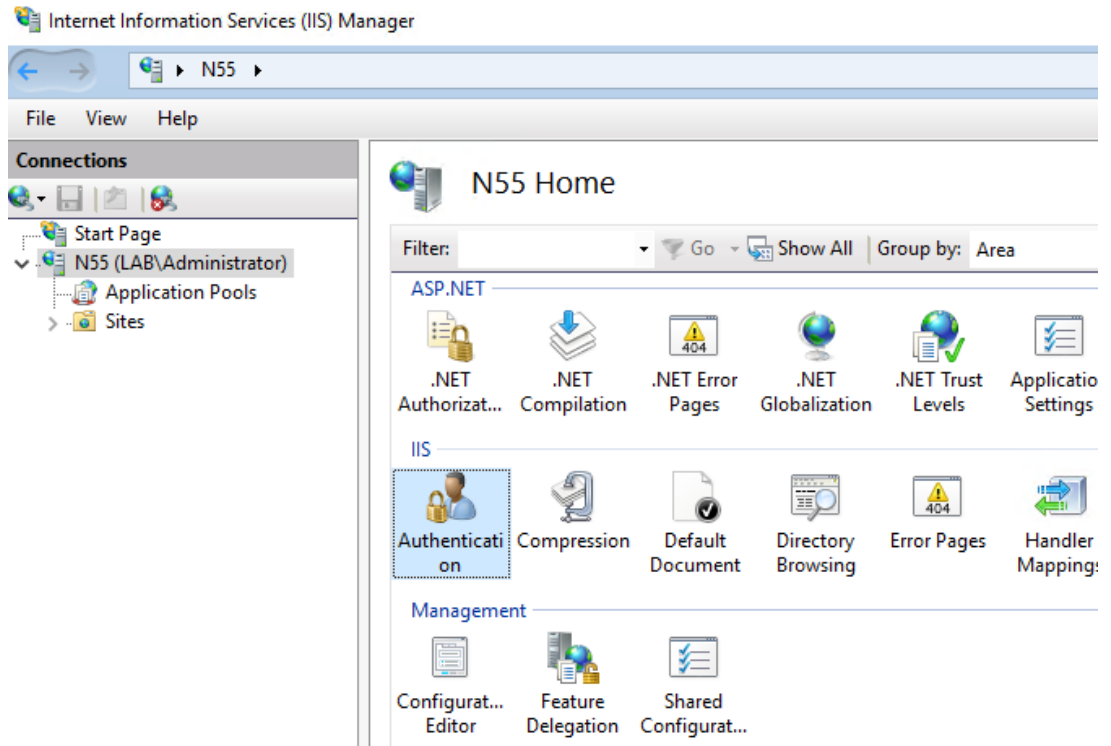
Select one or more roles to install on the selected server.

## Roles

- ☒ Active Directory Certificate Services (1 of 6 installed)
  - ☐ Active Directory Domain Services
  - ☐ Active Directory Federation Services
  - ☐ Active Directory Lightweight Directory Services
  - ☐ Active Directory Rights Management Services
  - ☐ Device Health Attestation
  - ☐ DHCP Server
  - ☐ DNS Server
  - ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
  - ☐ Host Guardian Service
  - ☐ Hyper-V
  - ☐ Network Policy and Access Services
  - ☐ Print and Document Services
  - ☐ Remote Access
  - ☐ Remote Desktop Services
  - ☐ Volume Activation Services
- ☒ Web Server (IIS) (13 of 43 installed)
  - ☒ Web Server (11 of 34 installed)
    - ☒ Common HTTP Features (5 of 6 installed)
    - ☒ Health and Diagnostics (4 of 6 installed)
    - ☒ Performance (1 of 2 installed)
    - ☐ Security
      - ☐ Request Filtering
      - ☐ Basic Authentication
      - ☐ Centralized SSL Certificate Support
      - ☐ Client Certificate Mapping Authentication
      - ☐ Digest Authentication
      - ☐ IIS Client Certificate Mapping Authentication
      - ☐ IP and Domain Restrictions
      - ☐ URL Authorization
      - ☐ Windows Authentication
  - ☒ Application Development (1 of 11 installed)
  - ☐ FTP Server
  - ☒ Management Tools (2 of 7 installed)
  - ☐ Windows Deployment Services
  - ☐ Windows Server Update Services

## 2. Enable "Active Directory Client Certificate Authentication" for IIS

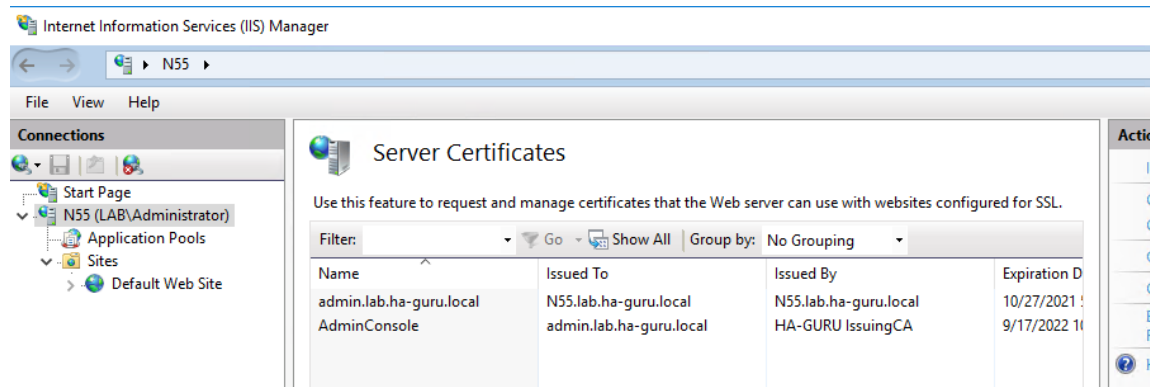
Open the IIS Manager on the application server that will be hosting either Data Platform or User Console. Select the server root node and Home pane double click "Authentication". Right click the "Active Directory Client Certificate Authentication" option and choose "Enable" to activate



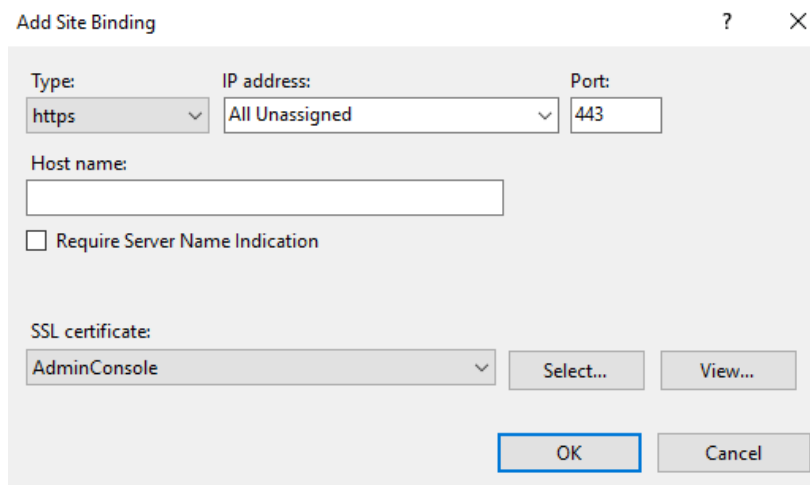
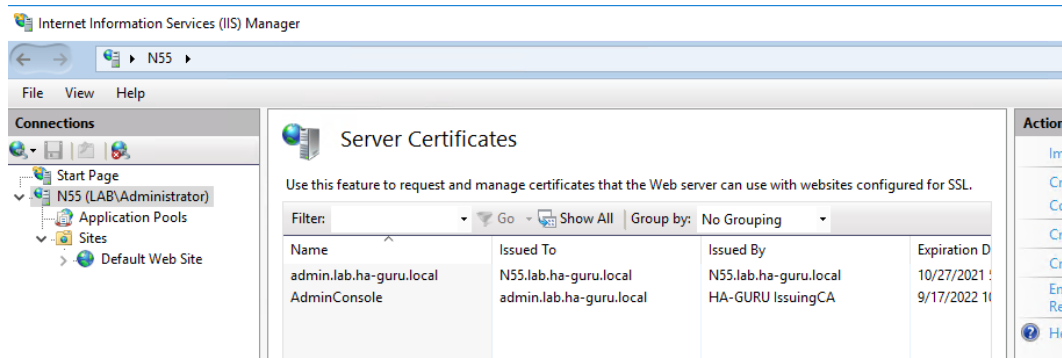
### 3. Configure SSL Bindings for Default Website

The Certificate authentication process can only occur over a secure channel between the client browser and the application server. To create the secure channel, the IIS Default Website must be configured to support the Secure Sockets Layer (SSL) protocol.

To enable SSL, open IIS Manager and select the root node. In the Home pane select "Server Certificates". If there are no certificates listed, it is recommended that you go through your organization's processes to obtain a Server certificate issued by your organization's authorities for your web server. If your organization's policies allow, you may also use the actions within IIS Manager to generate a "self-signed" certificate for use. Self-signed certificates are useful for testing, but it is highly recommended that you obtain a production certificate from your organization as self-signed certificates may generate warnings/errors and depending upon certain policies, you may even be prohibited from accessing the application.



Once a validate certificate has been installed, within the IIS Manager, select the Default Website and in the actions to the right select "Bindings". Click "Add" to add a new binding. Select "https" as the type and select the certificate that was added earlier from the dropdown. Lastly remove any non-https binding from the website.



## B. Data Platform Configuration

### 1. Install Data Platform 5.5.35 or Patch Your Installation to At Least 5.5.35

If you are applying patches to an existing installation of Data Platform and you also have deployed the Flexera User Console, then before doing so, validate that the Data Platform and User Console applications are able to communicate. Go to the "BDNA User Console" tab in the Preferences section of the Data Platform Admin Console. Verify that the "Activate BDNA User Console" checkbox is activated, and the page says "Connected" near/under the Test connection button. If this is not the case, resolve any issues such as resetting passwords, restarting services.



## Preferences

Registration **BDNA User Console** LAN Settings

Enable access to the BDNA User Console server. Enter the same credentials you used in the User Console Configuration Wizard.

☒ Activate BDNA User Console

**BDNA User Console Server:**

uc.lab.ha-guru.local

**User :**

svc\_flexera@lab.ha-guru.local

**Password:**

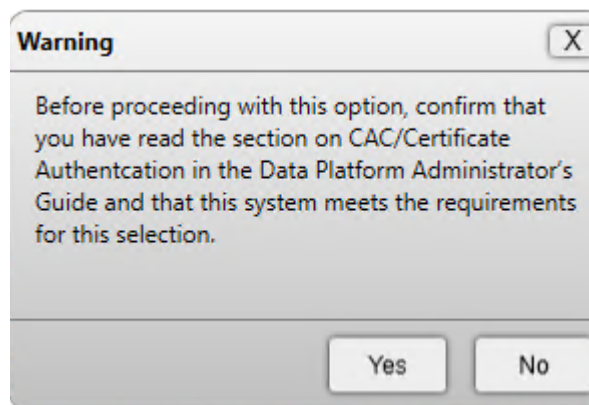
TEST CONNECTION

SAVE

Connected!

## 2. Run the Configuration Wizard for Data Platform

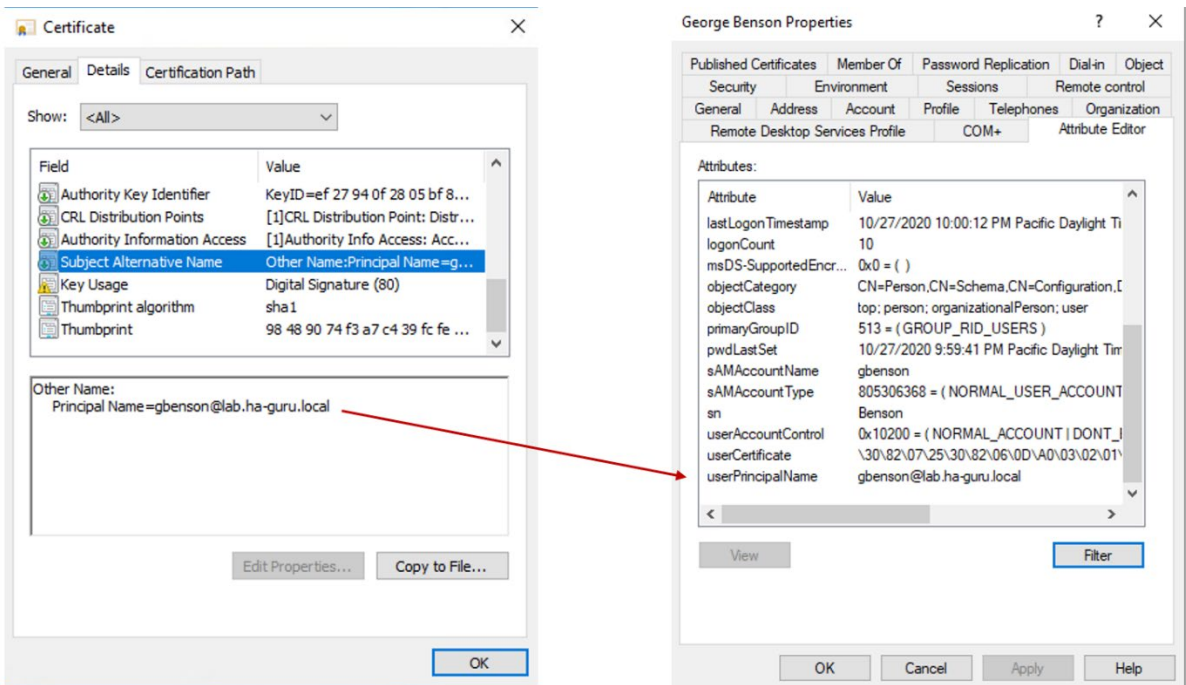
After installation/patching, run the Configuration Wizard for Data Platform and at the 4th step, select "Certificate Authentication..." and hit Next. You will receive a warning about ensuring your environment meets the necessary requirements. It is recommended that you revisit the sections above and validate that you have completed each item.



After validation, select Yes and continue with the configuration. Certificate authentication within Data Platform requires you to also configure a working Active Directory connection. Please refer to the section within the Data Platform Administrator’s guide for more detail.

When the user presents a certificate for authentication, Data Platform uses the subject data in the certificate to map to details found within Active Directory. In most PKI/Active Directory integrations this is accomplished through the Subject Alternative Name attribute in the digital certificate via the “OtherName” SAN extension. (See more about the SAN field here).

The values of the Other Name field are extracted for the “Principal Name” value. If present, this value is used to search for the user in Active Directory via the “userPrincipalName” value.



If a user is found, Data Platform validates that the user is assigned the applicable role for the application (either directly or indirectly via group membership).

The search attribute is controlled via the “User Attribute” value in the Active Directory configuration screen

Flexera Data Platform 5.5.35 Build20201028\_3018 Configuration

Authentication Settings

Active Directory ▼

Authentication

Server: DC1.lab.ha-guru.local:636

User DN: CN=svc\_flexera,OU=Service Accounts,OU=Testing,DC=lab,DC=ha-guru,DC=local

Password: \*\*\*\*\*

☒ SSL 

Certificate

 ✓

Advanced settings ▲

The information shown below has been auto-populated.

[Click here to automatically refresh the information.](#) Or, you can enter other values manually.

User Search

Search Base: DC=lab,DC=ha-guru,DC=local

Search Filter: (&(objectClass=Person)) User Attribute: userPrincipalName

Authorities Search

Search Base: DC=lab,DC=ha-guru,DC=local

Search Filter: (&(objectClass=group)) Group Attribute: cn

Populator

Search Base: DC=lab,DC=ha-guru,DC=local

Search Filter: (member={0}) Group Role Attribute: cn

Admin account: svc\_flexera@lab.ha-guru.local ☐ Convert to Upper Case ☒ Subtree

Test

Previous

Next

Cancel

Next you must configure and validate the certificate authentication settings. Data Platform will require that you supply the certificate thumbprint for at least one root certificate authority in the PKI and the certificate data (base64) for a standard, non-service account user that is expected to access the application(s).

**Certificate Authentication Setting**

## Root Certificates

Enter the thumbprint for up to 3 root certificates.

CA Thumbprint 1:  \*CA Thumbprint 2: CA Thumbprint 3: 

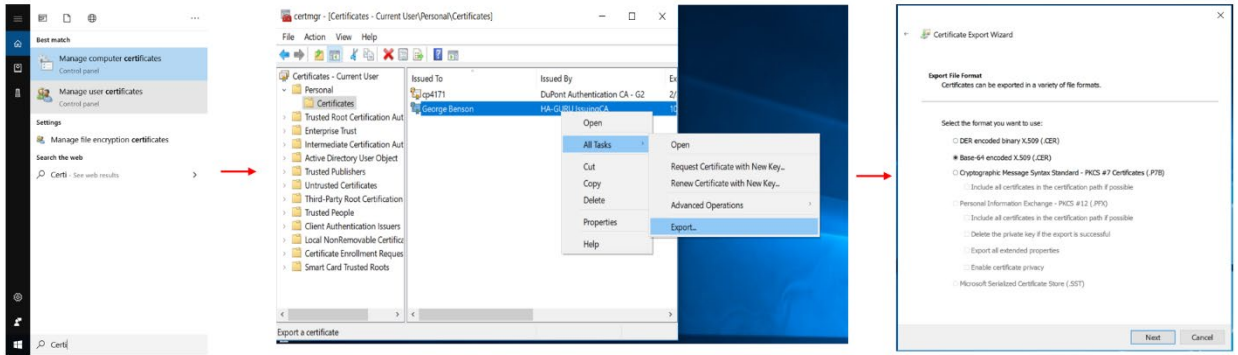
## User Certificate

Certificate Data:

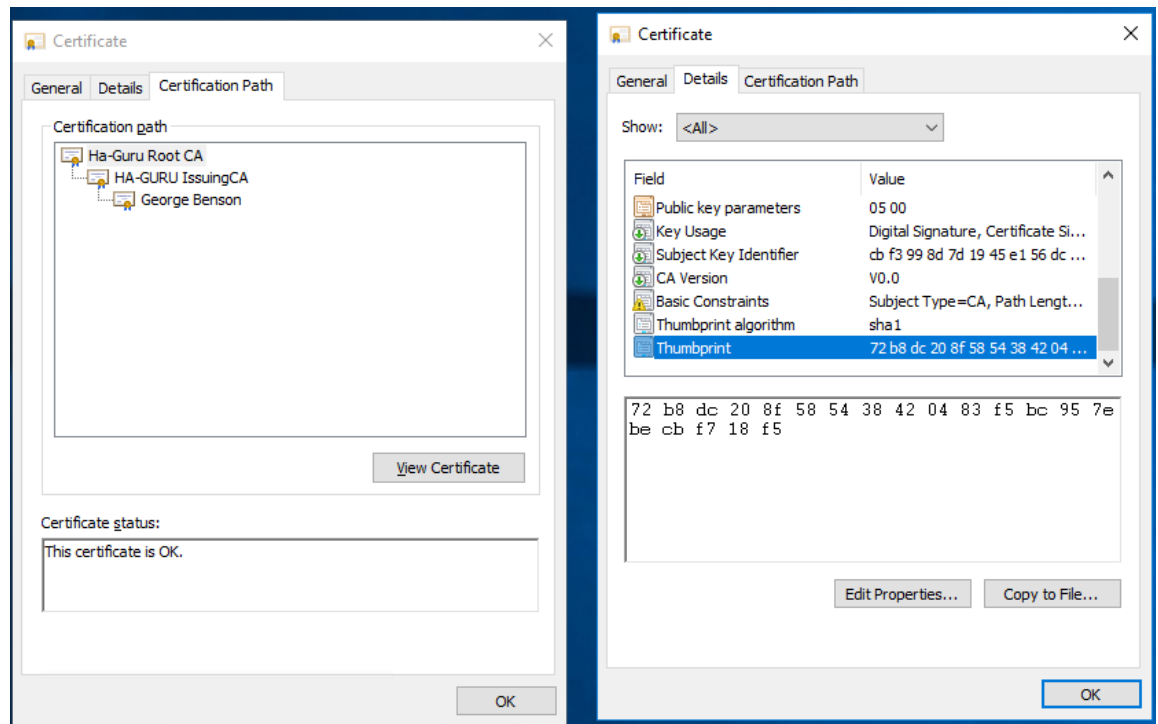
User Attribute: cn

To obtain the certificate data for a user, the administrator can open a valid personal certificate that can be used for Client authentication or Smart Card authentication that has been signed by the target Root Certificate Authority and export it to the Base-64 file format. Be sure to not export the Private Key as it is not needed.

Once exported, a standard text reader can be used to open the file and paste the contents into the configuration Wizard.



To obtain the certificate thumbprint, use the same certificate above. Select the "Certification Path" and select the root signer and select "View Certificate". In the details for the certificate of the root CA, select the "Thumbprint" field and copy the value into the Configuration Wizard.



Once the values are populated, hit Test to validate the settings.

**Certificate Authentication Setting**

## Root Certificates

Enter the thumbprint for up to 3 root certificates.

CA Thumbprint 1: 72 b8 dc 20 8f 58 54 38 42 04 83 f5 bc 95 7e be cb f7 18 f5

CA Thumbprint 2:

CA Thumbprint 3:

## Test Certificate

Certificate Data:

```
-----BEGIN CERTIFICATE-----
+ujxuQiBrbxswuWLnMki3fHTE/r7UAMnK
ynQ2wtmdUaOcwuxJVwuQO64ZuiV9s8Xya4l3lsiWdxCTW098mfwzehz
rw/RPt0Ew
89u7Jpu3jgc3XVdt5LPayKzIS+q4l1rO1EKDKqtHBGK
+RkaR3mdvhKbMffk/Kp7W
B
+PSAhqzAa5zrPyws77iNUNXt83vRca3Wf38LmknZYcDuxOXzhA1CXAIO
YI2+3gQ
ZCMK+AAuEelNujJbultsFd3xFxmL/1l8ftsDLLM2hFvKOy4evzZk/
VNjMXWbEdA6
BU7zBzpQnVyZ
-----END CERTIFICATE-----
```

User Attribute: userPrincipalName

Test

Previous

Next

Cancel








The CA thumbprint(s) ensures only authorized PKI can be used to access the application. Certificates presented for authentication that are not signed by authorities configured in Data Platform will fail the authentication process.

Hit Next to finish the setup and initialize Data Platform.

## Flexera Data Platform 5.5.35 Build20201028\_3018 Configuration

### Configuration Progress

The table below shows the progress of the installation. Click Execute to begin.

	Step	Description	Status
	1	Stop BDNA Data Platform Service.	
	2	Save database connection.	
	3	Remove BDNA IIS.	
	4	Deploy BDNA Admin Console IIS.	
	5	Configure Authority.	
	6	Backup configuration to Database.	
	7	Start BDNA Data Platform Service.	

Previous

Execute

Cancel

Once the configuration process has finished. You should now be able to access the Data Platform and authenticate with a personal certificate.

## C. User Console Configuration

### 1. For New Installations of Data Platform

(For new installations of Data Platform, you need to install User Console first. Please refer to the User Console installation guide and follow the pre-configuration steps as described above).

### 2. For Existing Data Platform Installations

For existing Data Platform installations, once the Data Platform has successfully patched the User Console, the Data Platform Configuration Wizard has been run and Certificate Authentication configured; the Configuration Wizard on the User Console should be re-run. Due to the nature of the new configuration, in most cases, only two options will require adjustment however, the configuration wizard must still be executed from start to completion for the User Console to retrieve the new security settings and apply them.

**Note:** before continuing with the configuration, be sure that you have executed the pre-configuration steps for the User Console as detailed above.

Launch the User Console Configuration Wizard and modify the second page so that the application is updated with the correct protocol and username settings. If using the "admin" account to retrieve settings, be sure that username matches the value used when configuring the Data Platform. If not using this account, then ensure that the username format is identical to the admin account.



## Flexera User Console 5.5.35 Build20201028\_3018 Configuration

### Connect to BDNA Data Platform

Enter connection settings and credentials to retrieve configuration information from the BDNA Data Platform server. The configuration wizard will use this information to set up the BDNA User Console service.

Data Platform server

Protocol Type:

https

Host:

admin.lab.ha-guru.local

Port:

443

BDNA Admin Console Login Credential

User Name:

svc\_flexera@lab.ha-guru.local

Password:

\*\*\*\*\*

[Previous](#)[Next](#)[Cancel](#)

In addition, the Management account must be adjusted. If the same account is used for both the Management and Admin functions, then be sure to update the username in this section. Otherwise, ensure that the format is identical to the format.

## Flexera User Console 5.5.35 Build20201028\_3018 Configuration

### IIS and Management Account Information

Select IIS website that will host the BDNA User Console. Additionally, enter Management Account information. If you are using AD/LDAP authentication, select a User group that the user name belongs to.

User Console Host

IIS WebSite:

Management Account

User name:

Password:

User Group:

**Note:** The Management Account role performs User Console administrative and system operations.

[Previous](#)[Next](#)[Cancel](#)

Once making the necessary changes, select Execute to allow the wizard to deploy the necessary changes

## Flexera User Console 5.5.35 Build20201028\_3018 Configuration

### Configuration Progress

The table below shows the progress of the configuration. Click Execute to begin.

	Step Name	Message
⌚	Stop BDNA User Console service.	
⌚	Create IIS proxy.	
⌚	Configure BDNA User Console.	
⌚	Start BDNA User Console service.	
⌚	Initialize the solution	

Previous

Execute

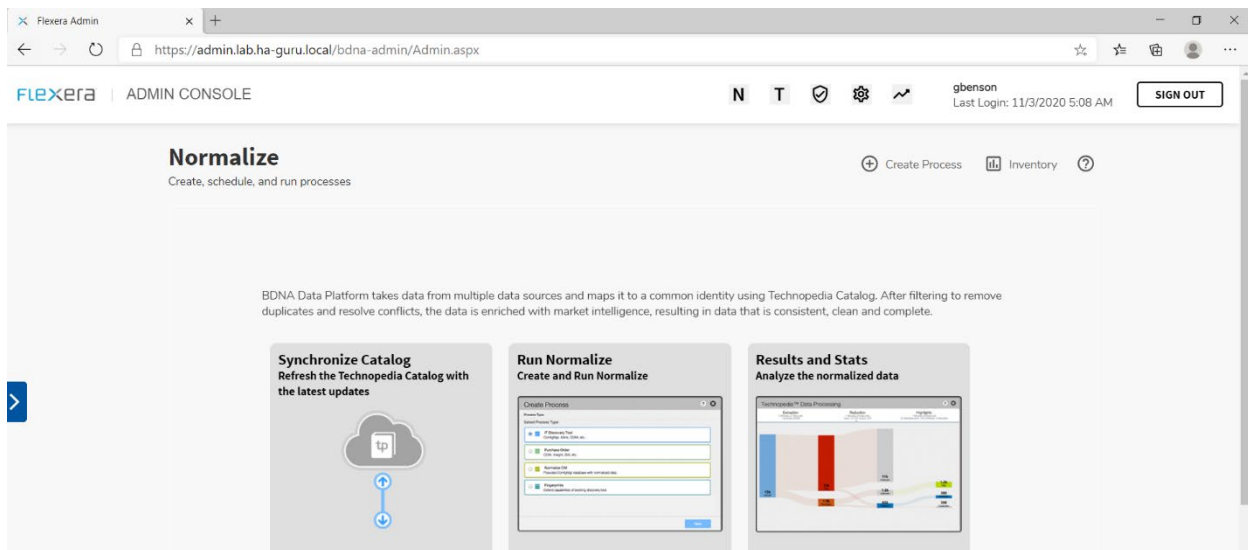
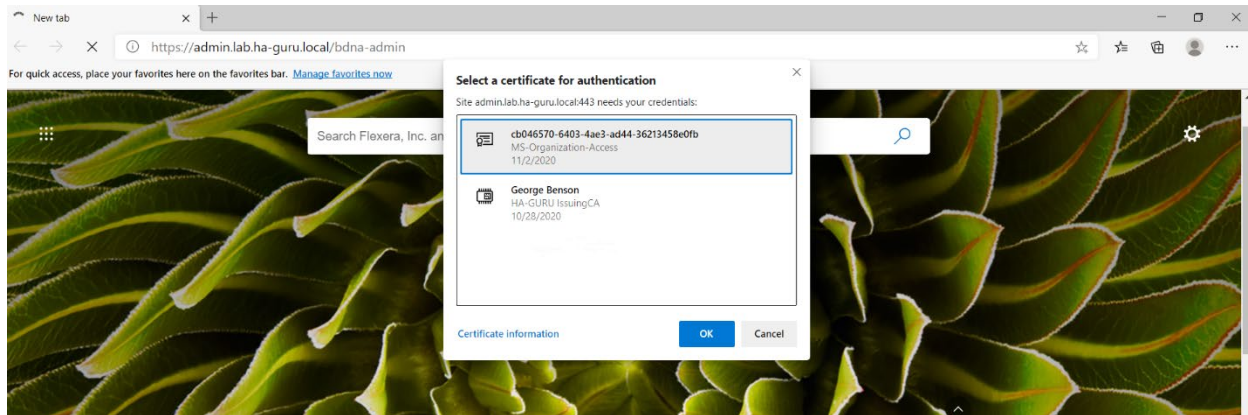
Cancel

## IV. Usage and Troubleshooting

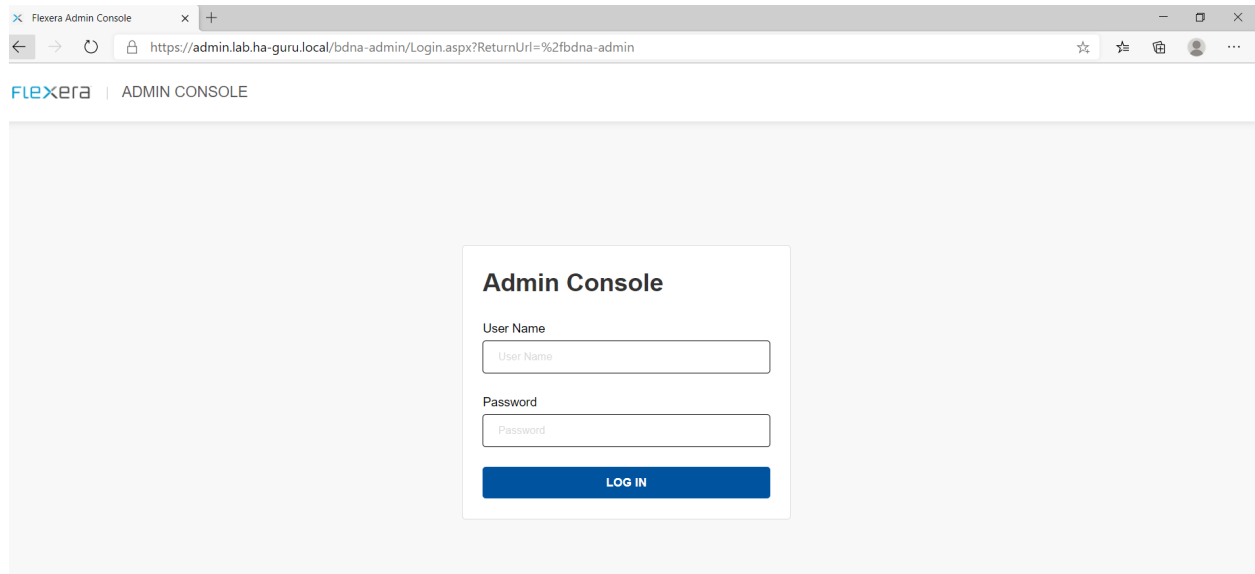
### A. Usage

The Certificate Authentication feature allows for signing into Data Platform Admin and User Consoles using x509 based Certificates. The Data Platform verifies any certificates presented for authentication. This is in addition to any revocation or validity checks that may be performed via Windows.

When logging onto the Admin Console via a new session, when prompted, choose any available certificate for authentication.



If you do not choose a certificate (e.g., hit cancel) or do not have an available certificate to choose from, the standard Logon form will load.



This allows Data Platform and User Console to support Certificate and non-Certificate users concurrently.

# Product Support Resources

The following resources are available to assist you with using this product:

- [Flexera Product Documentation](#)
- [Flexera Community](#)
- [Flexera Learning Center](#)
- [Flexera Support](#)

## Flexera Product Documentation

You can find documentation for all Flexera products on the [Flexera Product](#)

Documentation site: <https://docs.flexera.com>

## Flexera Community

On the [Flexera Community](#) site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Flexera's product solutions, you can access forums, blog posts, and knowledge base articles.

<https://community.flexera.com>

## Flexera Learning Center

Flexera offers a variety of training courses—both instructor-led and online—to help you understand how to quickly get the most out of your Flexera products. The Flexera Learning Center offers free, self-guided, online training classes. You can also choose to participate in structured classroom training delivered as public classes. You can find a complete list of both online content and public instructor-led training in the Learning Center.

<https://learn.flexera.com>

## Flexera Support

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the Flexera Community.

<https://community.flexera.com>

## Contact Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at: <http://www.flexera.com>

You can also follow us on social media: [Twitter](#), [Facebook](#), [LinkedIn](#), [YouTube](#), [Instagram](#)