UiPath Robotic Process Automation

nShield® Integration Guide

18 May 2023

Contents

1. Introduction

UiPath Robots log in to Windows machines to perform automated functions using username and passwords. Integrating the UiPath Robotic Process Automation (RPA) platform with the nShield Hardware Security Module (HSM) provides strong client authentication. When HSM-integrated Robots log in to domain systems, they are using certificate-based login.

1.1. Product configurations

Entrust has successfully tested nShield HSM integration in the following configurations:

Product	Version
UiPath Orchestrator (Local and Cloud)	2022.4
UiPath Studio (Robot)	2022.4
Operating system for the Robot machine	Windows Server 2022
nShield 5c	13.3.2
PowerShell	5.1 or later
.NET Framework	4.7.2 or later
IIS	8 or later

1.2. Supported nShield hardware and software versions

Entrust has successfully tested with the following nShield hardware and software versions:

1.2.1. Connect XC

Security World Software	Firmware	Image	OCS	Softcard	Module
12.80.4	12.72.1 (FIPS Certified)	12.80.5		✓	
13.3.2	12.72.1 (FIPS Certified)	12.80.5		✓	

Entrust has successfully tested with the following nShield hardware and software

versions:

1.2.2. nShield 5c

Security World Software	Firmware	Image	OCS	Softcard	Module
13.3.2	13.2.2 (FIPS Pending)	13.3.2		✓	

1.3. Supported nShield HSM functionality

Feature	Support
Module-Only key	No
OCS cards	No
Softcards	Yes
nSaaS	Yes
FIPS 140 Level 3	Yes [1]

[1] When using FIPS 140 Level 3, ECDSA credential is required for the Robot to force Windows PKINIT to use something other than SHA-1.

1.4. Requirements

An nShield Security World Software installation is required prior to using UiPath RPA. Instructions on how to set up an nShield Connect, a Remote File System (RFS) for the nShield Connect, a client computer, and installation instructions for the nShield Security World are included in the *nShield Installation Guide* and *nShield User Guide*.

To access and use cryptographic keys from within a Security World, you must:

- Load or create a Security World on the nShield Connect.
- Map the key management data folder (`kmdata`) from your container host machine into the running application containers.

Before installing these products, read the associated documentation:

- For the nShield HSM: *Installation Guide* and *User Guide*.

- If nShield Remote Administration is to be used: *nShield Remote Administration User Guide*.
- UiPath documentation (https://docs.uipath.com/).

In addition:

- The integration between nShield HSMs and UiPath RPA requires:
  - A correct quorum for the Administrator Card Set (ACS).
  - On the Firewall, configure 9004 for the HSM (hardserver).
- The following design decisions have an impact on how the HSM is installed and configured:
  - Whether your Security World must comply with FIPS 140 Level 3 standards.

    If using FIPS 140 Level 3, it is advisable to create an OCS for FIPS authorization. For information about limitations on FIPS authorization, see the *Installation Guide* of the nShield HSM.

    Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

  - Whether to instantiate the Security World as recoverable or not.

1.5. More information

For more information about OS support, contact your UiPath sales representative or Entrust nShield Support, https://nshieldsupport.entrust.com.

Access to the Entrust nShield Support Portal is available to customers under maintenance. To request an account, contact nshield.support@entrust.com.

2. Procedures

To integrate the UiPath Robotic Process Automation platform with the nShield HSM:

1. Deploy the backbone server
2. Deploy a Robot service

2.1. Deploy the backbone server

To deploy the backbone server:

1. Configure the backbone server, domain groups, and users
2. Configure ADCS
3. Set up UiPath Orchestrator

2.1.1. Configure the backbone server, domain groups, and users

To configure the backbone server, domain groups, and users:

1. For prerequisites, see https://docs.uipath.com/orchestrator/standalone/2022.4/installation-guide/orchestrator-prerequisites-for-installation.
2. Install and configure Microsoft Windows Server Operating System.
3. Install and configure the ADDS role.
4. Create a domain group. (i.e., **AutoEnrollGroup**)
5. Create the user accounts to be used by the Robots for authentication.
    a. Open **Active Directory Users and Computers** through the Windows Start menu or the Microsoft Management Console.
    b. Enable the advanced view so you can see the **Published Certificates** tab for user accounts.
    c. Right-click **Users** under your domain name and select **New**.
    d. Select **User**.
    e. Create users such as **RobotVM3** for the Robot user on system VM3. This helps distinguish that this particular Robot user has its Softcard or key on VM3.
6. Add group memberships to the Robot accounts so they can sign in to the Windows Server machines.
    a. In **AD Users and Computers**, select **Users** and find the users that were created.
    b. Right-click each user and select **Properties**.
    c. Select the **Member Of** tab.
    d. Add the following groups:

- Administrators
- Enterprise Admins
- Domain Admins
- Domain Users
- AutoEnrollGroup

7. Enable **Log On as a batch job** rights for the **Application Pool** user.
    a. Select **Windows > Run > mmc**.
    b. Select **File > Add/Remove Snap-in**.
    c. Add **Group Policy Object**.
    d. Select **Finish**.
    e. Select **OK**.

2.1.2. Configure ADCS

Microsoft ADCS does not have to be installed on the same "backbone" server as ADDS. For testing purposes, this document describes the specific steps for setting up all needed roles on the same machine.

To configure ADCS:

1. Install and configure the Active Directory Certificate Services role
2. Configure the ADCS certificate templates

2.1.2.1. Install and configure the Active Directory Certificate Services role

To install and configure the Active Directory Certificate Services role:

1. Open Server Manager and Install ADCS.
2. Configure as an enterprise root CA.
3. Optionally, if you want the CA to use the HSM for its signing key:
    a. Select the nShield CNG provider to write the CA key.
    b. Select **RSA2048/SHA256**.
    c. Select **module protected key** for simplicity.

2.1.2.2. Configure the ADCS certificate templates

To configure the ADCS certificate templates:

1. Open the **Certification Authority** Microsoft Management Console.
2. Expand the **CA** node.

3. Right-click **Certificate Templates** and select **Manage to create a new certificate template for the Robot**.
4. Right-click **Smartcard Logon** and select **Duplicate Template**.
5. Configure the following tabs:

Do not select **Apply** or **OK** until the end, else the template will be saved with the incorrect name.

Tab	Configuration option	Recommended setting or value
Compatibility	Show resulting changes	Clear the selection box.
	Certification Authority	**Windows Server 2012** or higher (required for CNG)
	Certificate recipient	**Windows 8 / Windows Server 2012** or higher (required for CNG)
General	Template Display Name	**UiPath Robot nShield KSP**
	Validity period	Select appropriate value
	Renewal period	Select appropriate value
	Publish certificate in Active Directory	Select this option
	Do not automatically reenroll if a duplicate certificate exists in Active Directory	Select this option

Tab	Configuration option	Recommended setting or value
Request handling	If an ECC key is to be used instead of RSA, the **Signature and smartcard logon** choice forces an ECDH key which will not work with the nShield. To force ADCS into issuing an ECDSA certificate for SCL: After previously selecting Signature and smartcard logon, change to **Signature**. ADCS will add the appropriate certificate extensions/attributes to the template for **Signature and smartcard** logon. When you afterwards switch to **Signature**, it retains those extensions/attributes but allows ECDSA keys.	**Signature and smartcard logon**, select **YES** in the dialog
	Do the following when the subject is enrolled and when the private key associated with this certificate is used	**Prompt the user during enrollment**
Cryptography	Provider Category	**Key Storage Provider** (which is CNG)
	Algorithm name	**RSA** or **ECDSA_P384**
	Minimum key size	**2048** (for RSA) **384** (for ECDSA_P384)
	Choose which cryptographic providers can be used for requests	**Requests must use one of the following providers**
	Providers	**nCipher Security World Key Storage Provider**
	Request Hash	**SHA256** (for RSA) **SHA-384** (for ECDSA_P384)

Tab	Configuration option	Recommended setting or value
Security	Select **Add**, enter **AutoEnrollGroup** and select **Check Names**. Then select **OK**. Select **AutoEnrollGroup** from the list and enable permissions **read enroll autoenroll**.	
Subject name	Build from this Active Directory Information	Select this option
	Subject name format	Fully distinguished name
	Include this information in alternate subject name	Ensure only **UPN** is selected

6. Select **OK**.

   The new certificate template is included in the list.

7. In the **Certification Authority** Microsoft Management Console, right-click **Certificate Templates** and select **New > Certificate Template to issue**.
8. Ctrl+click to select both **Web Server** and **UiPath Robot nShield KSP** and select **OK**.
9. Both templates are added to the **Certificate Templates** list and can now be issued.

2.1.3. Set up UiPath Orchestrator

The procedures described in this guide are an example test set-up for integration purposes. Your organization's needs may require alternate steps for set-up and deployment.

For information, see also https://docs.uipath.com/installation-and-upgrade/docs/orchestrator-about-installation.

Select one of the three following installation options:

- Set up a cloud Orchestrator.
- Set up a local Orchestrator through UiPath Platform.
- Set up a local Orchestrator with the installer.

2.1.3.1. Set up a cloud Orchestrator

To set up a cloud Orchestrator:

1. Go to https://cloud.uipath.com.
2. Create an account and sign in.
3. Select **Create new**.
4. Under **Services**, select the **Orchestrator** link.
5. Use a UI Path License to allocate one **Unattended Runtime** slot for each Robot you intend to use.
6. Create a machine:
   a. Go to **Tenant** and then select **Machines**.
   b. Select **Add machine**.
   c. Select **Standard machine**.
   d. Enter a name for the machine.

      The name must match exactly the name of the workstation on which the Robot is installed. To check it, run `hostname` on the Robot machine.

      Add one **Production (Unattended)** runtime.

      This is a type of license that allows the Robot to run triggered from Orchestrator.

   e. Select **Provision**.
   f. Make sure to copy the **Machine key**. You will need the key when you are connecting UiPath Assistant to the Orchestrator instance.
7. Create a Robot Account: Select **Admin** from the top left menu.
   a. Select **Manage**.
   b. Select **Accounts & Groups**.
   c. Select **Robot accounts**.
   d. Select **Add Robot Account**:
      i. Enter a name for the Robot Account.
      ii. Designate the Group Membership for the account.
      iii. Select **Add**.
8. On the Orchestrator, select **Tenant > Manage Access > Assign roles > Robot Account**, then set its properties:

Search for a Robot account	Select the Robot account that you created.

Roles	Designate roles for the Robot account.
Foreground automation settings	Select **Use a specific Windows user account. Add credentials below**.
Domain\Username	*<domain\username>*
Credential Store	Select **Orchestrator Database**.
Password	*<Softcard passphrase>*
Credential type	Select **nShield Key Storage Provider**.

The *<domain\username>* will be for the Robot machine account. To check the Robot username at the command prompt on the Robot machine, use `whoami`.

9. Under **Logging settings**, select **Login to console > YES**.
10. Select **Assign**.
11. Assign the Robot Account to your folder:
    a. Select the folder to be used and then **Settings**.
    b. Select **Assign Account/Group**.
    c. Enter and select the Robot Account previously created.
    d. Designate roles.
    e. Select **Assign**.
12. Upload a package:

    Select **Tenant > Packages > Upload**.

13. Browse to a package to upload:

    Select your **Folder > Automations > Add process**.

    Create the process from the package that you previously uploaded.

The Orchestrator has been created and configured.

2.1.3.2. Set up a local Orchestrator through UiPath Platform

To set up a local Orchestrator through UiPath Platform:

1. Read https://docs.uipath.com/installation-and-upgrade/docs/orchestrator-about-installation.

2. Ensure that your environment meets these requirements: https://docs.uipath.com/installation-and-upgrade/docs/orchestrator-prerequisites-for-installation.
3. Run **UI Path Platform**.
4. Accept the Agreement.
5. Select **Install Single Node**, and then select **Next**.
6. Enter **Computer Account Username and Password**.
7. Select **Next** until the **Host and Tenant passwords** menu appears.
8. Enter the **Host** and **Tenant** passwords. These will be used to log in to Orchestrator later.
9. Select **Enable Windows Authentication**.
10. Next to **Active Directory Domain**, enter the domain name, and then select **Next**.
11. Make a note of the URL. This will be used to access the Orchestrator interface through a web browser.
12. Select **Install**.

2.1.3.3. Set up a local Orchestrator with the installer

It is required to set up Microsoft IIS and SQL Server before proceeding with the on-premise local Orchestrator install.

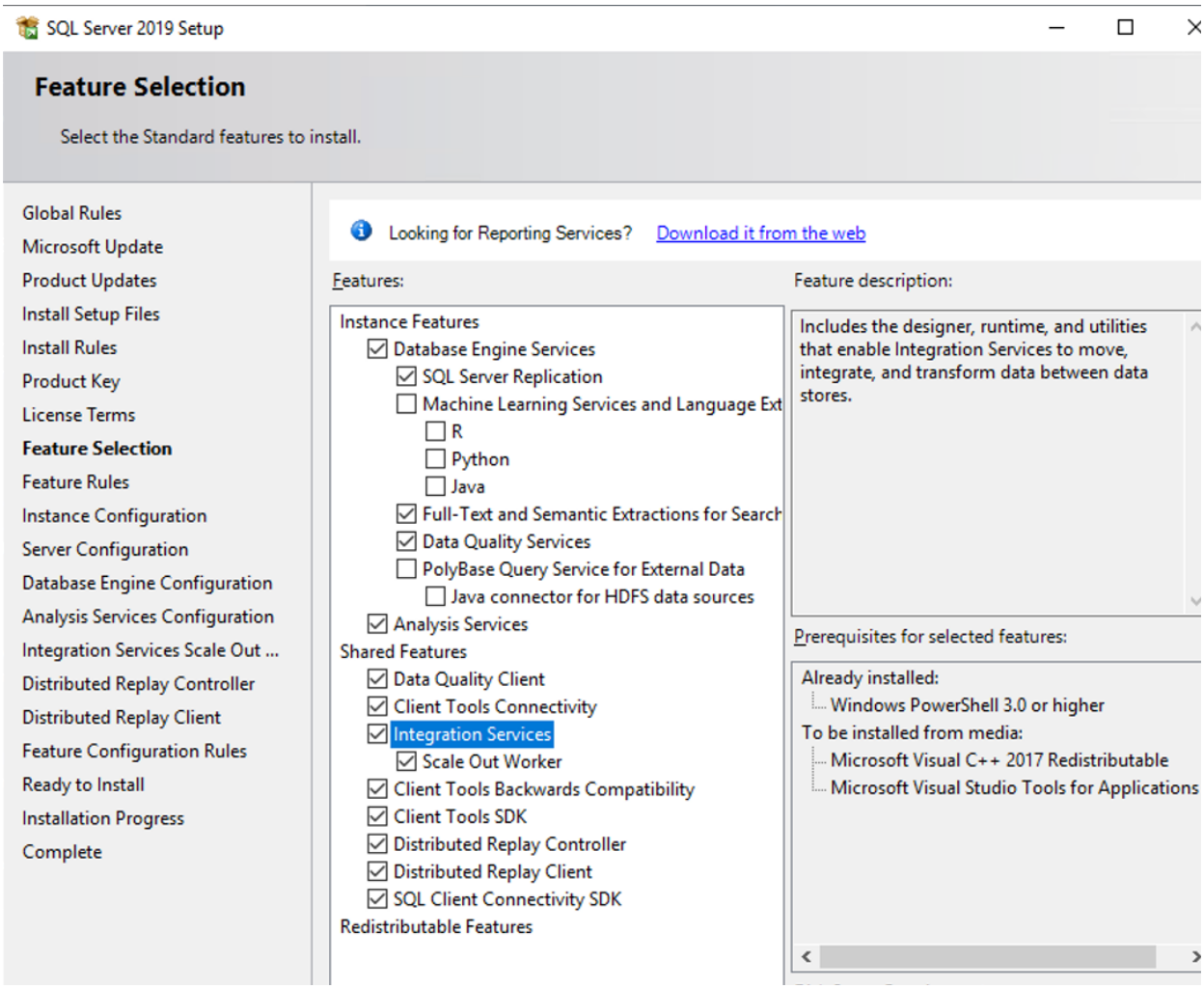
To configure Internet Information Services (IIS):

1. Request a Web Server certificate from ADCS using RSA2048/SHA256.
2. Open **IIS**.
3. Select **Server Certificates**.
4. Select **Create Domain Certificate**.
5. Fill in the required information and then select **Next**.
6. Specify the Certificate Authority that was created earlier.
7. Enter **Friendly Name**.
8. Select **Finish**.

To install Microsoft SQL Server:

1. Select **Custom Installation**.
2. Select **New SQL Server stand-alone installation or add features to an existing installation**.
3. Select the product license.
4. Accept the terms.
5. Select **Use Microsoft Update to check for updates (recommended)**, and then select **Next**.

6. Select the following features:



7. Select **Next**.
8. Select **Next**.
9. Select **Add Current User** and select **Next**.
10. Continue selecting **Next** until **Install**.
11. Close the installer.

To set up a local Orchestrator with the installer:

1. Right-click the `UiPathOrchestrator.msi` file, and select **Install**.
2. Select **Next** on the welcome screen.
3. Accept the terms and select **Install**.
4. On the **Product Features** menu, select **Next**.
5. The **Orchestrator IIS Settings** should be auto-filled.
6. If there is an error about SSL certificate, edit the box and paste in the thumbprint of the certificate requested in IIS.
7. Select **Next**.

8. On the **Orchestrator Application Pool Settings** screen, make sure **Custom Account** is selected.
9. Enter the username and password of the Orchestrator Computer Account, and then select **Next**.
10. On the **Orchestrator Database Settings** screen, select **Leave as is**.
11. Select **Next**.
12. On the **Identify Server Settings** screen, make a note of the Orchestrator public URL.
13. Paste in the Signing Certificate Thumbprint.
14. Select **Next**.
15. On the **Orchestrator Elasticsearch Log Settings** screen, select **Next**.
16. On the **Orchestrator Authentication Settings** screen, enter passwords for the **Host** and **Default Tenant**.
17. Select **Enable Windows Authentication**.
18. Enter the **Domain Name**.
19. Select **Next**.
20. Select **Install**.
21. Select **Finish**.

2.2. Deploy a Robot service

To deploy a Robot service:

1. Install the operating system on the machine that will host the Robot service.

   Windows Server 2022, Windows 10, Windows Server 2019, and Windows Server 2016 were tested as the host operating systems for the Robot service.

2. Join the server to the domain.

   For instructions, see https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain.

3. Install the nShield Security World client.
   a. Configure the existing Security World.
   b. Run the **CNG wizard** or the `cnginstall` command.
   c. Create an HSM Softcard.

      For example, at the command prompt run the following command:

      ```
      ppmk --new RobotVM1
      ```

4. Configure the custom CNG provider.

   The `SmartCardLogin` functionality is protected by a registry setting. Configure the following `SmartCardMode` registry settings to the recommended values in the table. This will enable the `SmartCardLogin` support on any machine where the revised CNG provider is installed:

Parameter	Value
`HKEY_LOCAL_MACHINE\SOFTWARE\nCipher\CryptoNG\SmartCardMode`	`1` [a]
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\nCipher\CryptoNG\SmartCardMode`	`1` [b]
`HKEY_LOCAL_MACHINE\SOFTWARE\nCipher\CryptoNG\UseModuleKeys`	`0` [c]
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\nCipher\CryptoNG\UseModuleKeys`	`0` [c]

   [a] It will be necessary to add the `DWORD` value for the 64-bit CNG provider.

   [b] It will be necessary to add the `DWORD` value for the 32-bit CNG provider.

   [c] This value is set to `0` so distinct protection tokens can be used for each user associated with a `SmartCardLogin` certificate.

5. Sign in to the Robot machine with the Robot user account that was created in Configure the backbone server, domain groups, and users.
6. Request the user certificate **UiPath Robot nShield KSP** using the HSM Softcard.
   a. Select **Control Panel > Manage User Certificates**.
   b. Right-click the **Personal** node, and select **All Tasks > Request New Certificate**.
   c. On the **Before You Begin** screen, select **Next**.
   d. On the **Select Certificate Enrollment Policy screen**, keep the default Active Directory Enrollment Policy selected and then select **Next**.
   e. On the **Request Certificates** screen:
      i. Select the UiPath Robot nShield KSP certificate template and Select **Enroll**.
      ii. On the **nCipher Key Storage Provider - Create Key** screen, select **Next**.
      iii. On the **Select a method to protect new key** screen, select **Softcard protection (unavailable in HSM Pool mode)**, and select **Next**.
      iv. Select the previously created Softcard and select **Finish**.
      v. On the password screen, enter the Softcard passphrase and select **Finish**.
   f. On the **Certificate Installation Results** screen, ensure that it shows successful enrollment and select **Finish**.
7. Install **UiPath Studio (Robot)**:

a. Double-click on the MSI installer to begin installation.
b. On the **Please read the UiPath Studio License Agreement** screen:
    i. (Optional) Select **Advanced** to configure any specific packages.
    ii. Select **I accept the terms in the License Agreement**.
    iii. Select **Install**.
c. On the **Completed the UiPath Studio Setup Wizard** screen, select **Finish**.

2.2.1. Configure UiPath for Robots

To configure UiPath for Robots:

1. Configure UiPath for nShield HSMs.
2. Configure UiPath for Robots if a local Orchestrator was used.

2.2.1.1. Configure UiPath for nShield HSMs

Configure the Robot to use only the 64-bit nShield CNG provider with the Microsoft CorFlags tool: https://docs.microsoft.com/en-us/dotnet/framework/tools/corflags-exe-corflags-conversion-tool.

Visual Studio 2019 is required to run the Visual Studio Command Line, which is needed to run the `corflags.exe` command.

1. Stop the `UiRobotSvc` service.
2. From the Administrator command prompt, run the `corflags.exe` command:

```
CorFlags.exe "C:\Program Files (x86)\UiPath\Studio\UiPath.Service.Host.exe" /32BITPREF-
```

3. Restart the `UiRobotSvc` service.

2.2.1.2. Configure UiPath for Robots if a local Orchestrator was used

Skip this section if the Robot was set up through a cloud Orchestrator. This is because these steps would already have been completed in Set up a cloud Orchestrator.

If a local Orchestrator was used, the Robot must be set up to get the machine key.

1. Sign in to the machine with Orchestrator.
2. Enter the Orchestrator URL into a browser.
3. Make sure the organization is set to **host**.

4. Enter **admin** as the **username** and use the password set for the **host** when the local Orchestrator was installed.
5. Select **License** and enter your license in whichever way works best: online or offline.
6. When the license has been activated, select **Tenants** and select the 3 vertical dots on the right side of the **Default Tenant**.
7. Select **Allocate Licenses**.
8. Allocate one **Production (Unattended) Runtime** slot for each Robot you intend to use.
9. Log out of the tenant host and login with the organization set to default. Use **admin** as the username and use the password set for **tenant** when the local Orchestrator was installed.
10. Select **Tenant**.
11. Select **Add machine**.
12. Select **Standard Machine**.
13. Enter the machine name.

The name must match exactly the name of the workstation on which the Robot is installed. To check it, run `hostname` on the Robot machine.

14. Under **License - Unattended Runtimes**, enter **1**.
15. Select **Provision**, then select **Copy** to copy the machine key.
16. Go to **Default > Robots > Add > Standard Robot**.
17. Under **Runtime license (execution slots) - Production (Unattended)**, enter **1**.
18. Select **Provision**, then select **Copy** to copy the machine key. You will need the key when you are connecting UiPath Assistant to the Orchestrator instance.
19. Select **Tenant > Folders > Your_Folder > Machines > Manage Machines in Folder**
20. Add the previously created machine.
21. Create a Robot Account:
    a. Select **Tenant**.
    b. Select **Manage Access**.
    c. Select **Manage Accounts & Groups**.
    d. Select **Robot accounts**.
    e. Select **Add Robot Account**.
        i. Enter a name for the Robot Account.
        ii. Designate the Group Membership for the account.
        iii. Select **Add**.

22. On the Orchestrator, select **Tenant > Manage Access > Assign roles > Robot Account**, then set its properties:

Search for a Robot account	Select the Robot account that you created.
Roles	Designate roles for the Robot account.
Settings	Select **Machine login credentials**.
Domain\Username	*<domain\username>*
Credential Store	Select **Orchestrator Database**.
Password	*<Softcard passphrase>*
Credential type	Select **nShield Key Storage Provider**.

The *<domain\username>* will be for the Robot machine account. To check the Robot username at the command prompt on the Robot machine, use `whoami`. If the **nShield Key Storage Provider** option does not exist, ensure the `Features.SmartCardAuthentication.Enabled` parameter is set to `True` in `C:\Program Files(x86)\UiPath\Orchestrator\UiPath.Orchestrator.dll.config`.

23. Under **Logging settings**, select **Login to console > YES**.
24. Select **Assign**.
25. Assign the Robot Account to your folder:
    a. Select the folder to be used and then **Settings**.
    b. Select **Assign Account/Group**.
    c. Enter and select the Robot Account previously created.
    d. Designate roles.
    e. Select **Assign**.
26. Upload a package:

    Select **Tenant > Packages > Upload**.

27. Browse to a package to upload:
    a. Select your **Folder > Automations > Add process**.
    b. Create the process from the package that you previously uploaded.

The Orchestrator has been created and configured.

2.2.2. Connect the Robot Machine to the Orchestrator

To connect the Robot Machine to the Orchestrator:

1. On the Robot Machine, start **UiPath Assistant** from the Windows Start menu.
2. Select **Preferences > Orchestrator Settings**, and add the Orchestrator URL and the machine key that you created.
3. Select **Connect**.

The Robot can now be connected. The processes should now be viewable.

2.2.3. Test the UiPath Studio Robot

To test the UiPath Studio Robot, run the process that you have added in Orchestrator.

To start a process from Orchestrator:

1. On the **Orchestrator** screen, select your **Folder > Automations > Start a job**.
2. Select the **Process Name, Account, and Machine**.
3. Select **Start**.