Azure Batch Azure Authentication Setup

Azure Batch is effectively a pool of virtual machines (VMs) that can run various compute tasks. Azure Batch can be configured in an Azure Data Factory Custom Activity to run PowerShell commands.

The following process sets up an Azure Batch account to authenticate to Azure. Specifically, this enables running Azure PowerShell Az cmdlets on the Azure Batch VMs after using a certificate to authenticate to Azure.

There are many methods to accomplish the following, but the instructions here are limited to the Azure Portal and PowerShell commands (vs. Terraform, Azure CLI, etc.).

Contents

[Prerequisites 2](#_Toc8988882)

[Create & Export Certificate 2](#_Toc8988883)

[Export Private Key (.pfx) 2](#_Toc8988884)

[Export Public Key (.cer) 4](#_Toc8988885)

[Set Up App Registration 5](#_Toc8988886)

[Get Tenant ID 5](#_Toc8988887)

[Create App Registration 5](#_Toc8988888)

[Get Application ID 6](#_Toc8988889)

[Upload Public Key 6](#_Toc8988890)

[Grant App Registration Access to Azure Active Directory 6](#_Toc8988891)

[Grant App Registration Access to Azure Batch 7](#_Toc8988892)

[Grant Azure Batch Account Access to App Registration 7](#_Toc8988893)

[Set up Certificate on Azure VMs 7](#_Toc8988894)

[Apply Certificate to Azure Batch Account 7](#_Toc8988895)

[Apply Certificate to Azure Batch Pool 7](#_Toc8988896)

[Reboot Azure Batch VMs 8](#_Toc8988897)

[Grant Access to MachineKeys Folder on Azure Batch VM(s) 8](#_Toc8988898)

[Create Start Task for Azure Batch VMs 8](#_Toc8988899)

[Test Connectivity 10](#_Toc8988900)

# Prerequisites

1. Set up an Azure Batch account in Azure.
2. On each Azure Batch VM:
   1. ~~Install~~ **~~.NET Framework 4.7.2~~** ~~if necessary (~~[~~details~~](https://docs.microsoft.com/en-us/dotnet/framework/install/)~~).~~
   2. Install **Azure PowerShell Az** by running the following in PowerShell as Administrator ([details](https://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-1.3.0)):

Install-Module -Name Az -AllowClobber

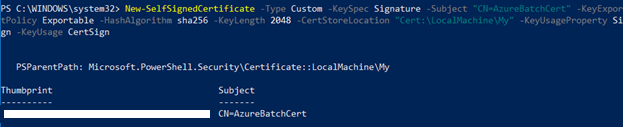
* 1. ~~Alternatively~~ **~~Azure PowerShell Az~~** ~~may be installed as part of installing~~ **~~Windows Management Framework 5.1~~** ~~(~~[~~details~~](https://www.microsoft.com/en-us/download/details.aspx?id=54616)~~).~~

# Create & Export Certificate

1. In PowerShell, run the following command, supplying a name, to create a new certificate on the local machine:

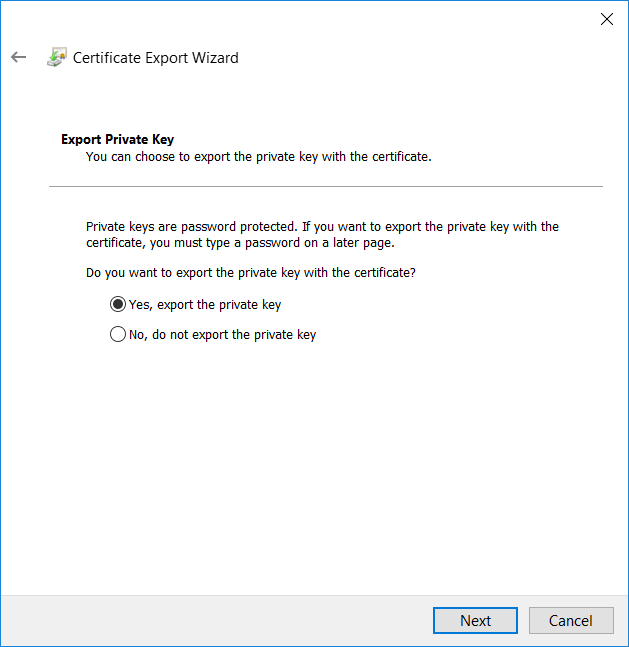
**New-SelfSignedCertificate** -Type Custom -KeySpec Signature -Subject "CN=AzureBatchCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\LocalMachine\My" -KeyUsageProperty Sign -KeyUsage CertSign

1. Copy and save-off the generated *Thumbprint* value:

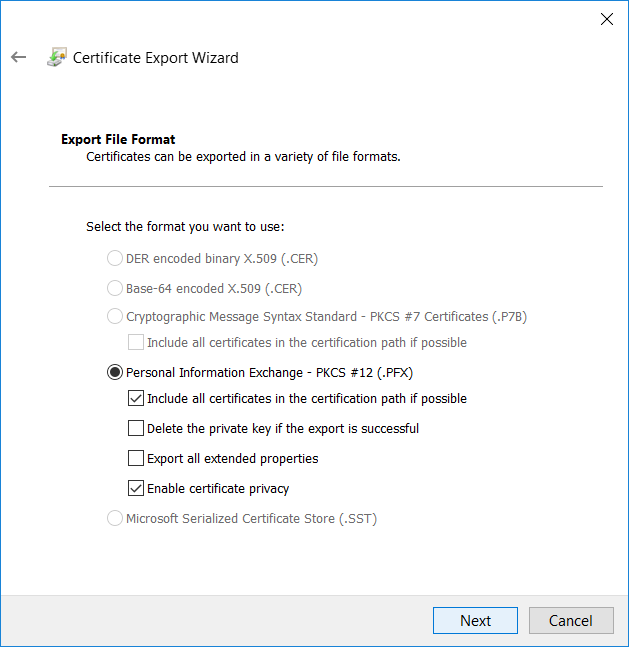


## Export Private Key (.pfx)

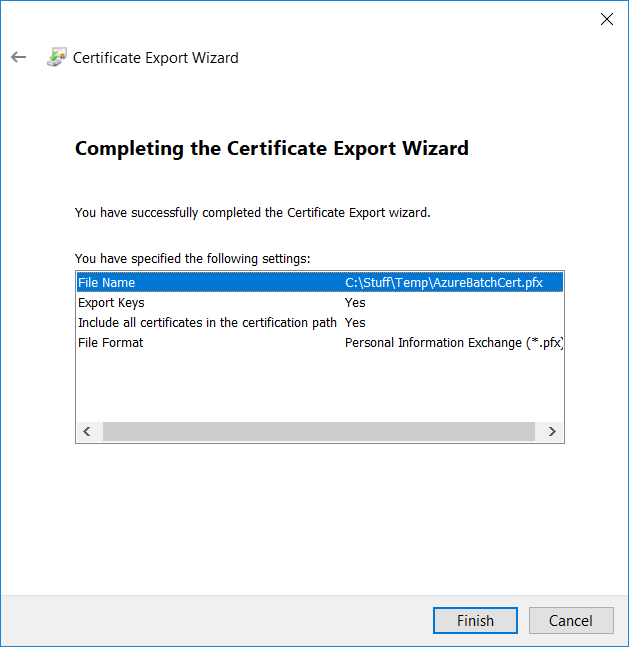
1. Go to Start, search for “Manage computer certificates”, and open it. (Do not confuse this with “Manage *user* certificates”.)
2. Navigate to Certificates - Local Computer | Personal | Certificates and select the certificate created above (e.g., AzureBatchCert).
3. Right-click the certificate, go to All Tasks | Export.
4. Select the “Yes, export private key” radio button:



1. Select the following options for File Format:

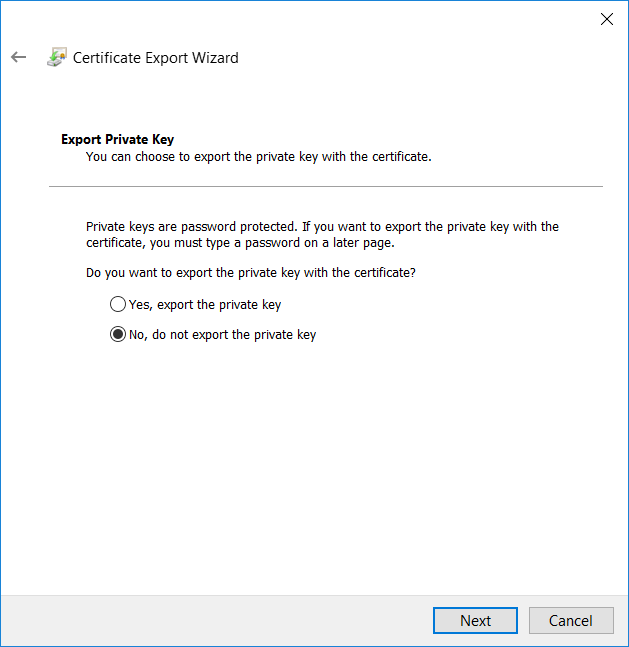


1. On the Security tab, enter a password and remember it.
2. Click Finish.

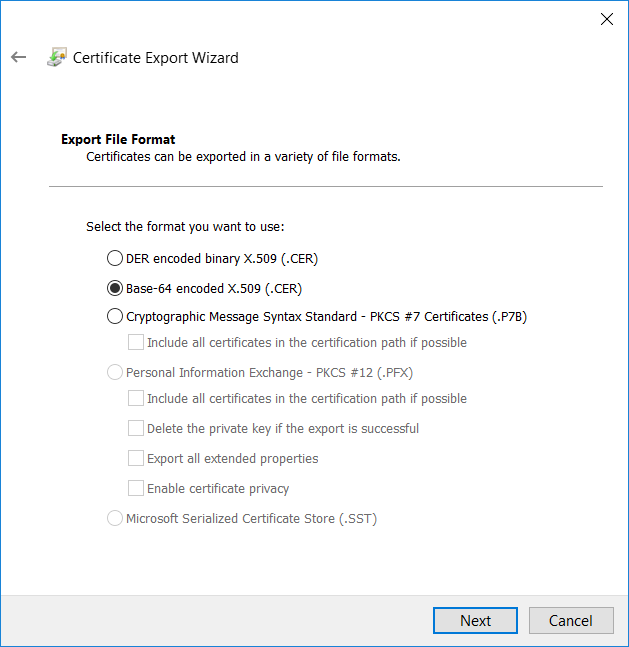


## Export Public Key (.cer)

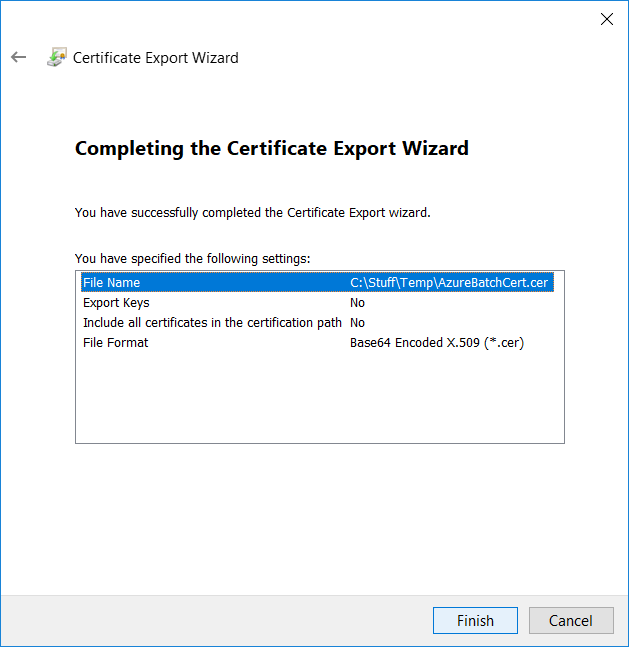
1. Right-click the same certificate, and again go to All Tasks | Export.
2. Select the “No, do not export the private key” radio button:



1. Select “Base-64 encoded X.509 (.CER)”:



1. Click Finish.



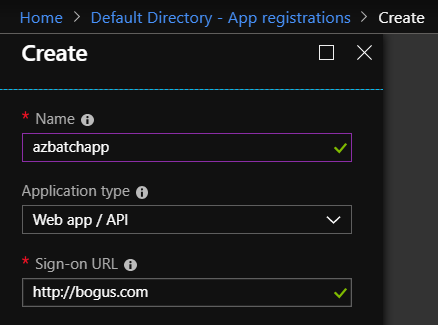
# Set Up App Registration

## Get Tenant ID

1. In the **Azure Portal**, go to **Azure Active Directory**.
2. Click **Properties**.
3. Copy and save-off the value for *Directory ID*. This is the *Tenant ID****.***

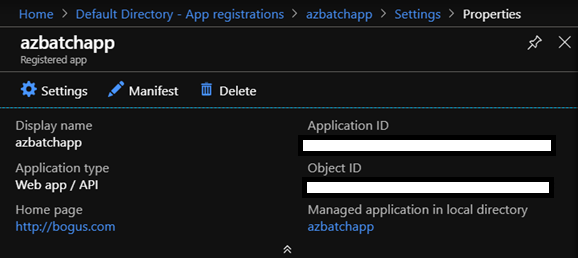
## Create App Registration

1. Click **App Registrations** (not to be confused with**App Registrations (Preview)**).
2. Click **New Application Registration**.
3. Assign a name (e.g. azbatchapp), the application type should be **Web app / API**, and set some URL (which will not be used):



## Get Application ID

1. Select the **App registration** created above in the Azure Portal and click **Settings**.
2. Click **Properties** and copy and save-off the *Application ID*:



## Upload Public Key

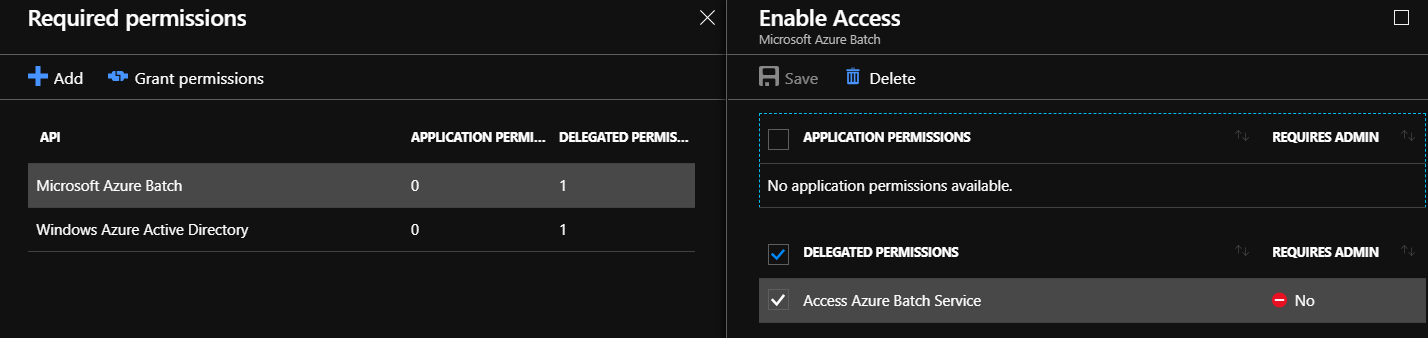
1. Select the **App registration** created above in the Azure Portal and click **Settings**.
2. Click **Keys**.
3. Click **Upload Public Key**.
4. Navigate to the .cer file created in the “Export Public Key (.cer)” section above and upload.

## Grant App Registration Access to Azure Active Directory

1. Navigate to the Application Registration in Azure Active Directory in the Azure Portal.
2. Click **Settings**.
3. Click **Required permissions**.
4. Click **Windows Azure Active Directory**.
5. Under **Application Permissions**, check “Read directory data”.
6. Click **Save**.
7. Click **Grant permissions**.

## Grant App Registration Access to Azure Batch

1. Select the **App registration** created above in the Azure Portal and click **Settings**.
2. Click **Required permissions**.
3. Click **Add**.
4. Click **Select an API** and search for “Microsoft Azure Batch”.
5. Check the checkbox next to “Access Azure Batch Service” and click **Save**.
6. Click **Grant permissions**.



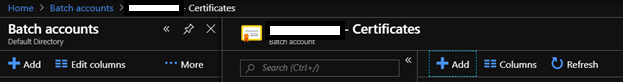
# Grant Azure Batch Account Access to App Registration

1. Navigate to the Azure Batch account in the Azure Portal.
2. Click **Access control (IAM)**, then **Role Assignments**, then **Add**, then **Add Role Assignment**.
3. Set **Role** to *Reader*.
4. Set **Select** to the Application Registration.
5. Click **Save**.

# Set up Certificate on Azure VMs

## Apply Certificate to Azure Batch Account

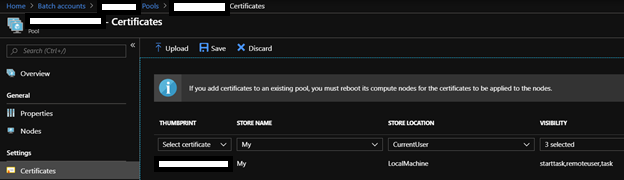
1. In the Azure Portal, navigate to the Azure Batch account and click **Certificates**.



1. Click **Add**, navigate to the exported .pfx file, and upload.
2. Verify *Thumbprint* value.

## Apply Certificate to Azure Batch Pool

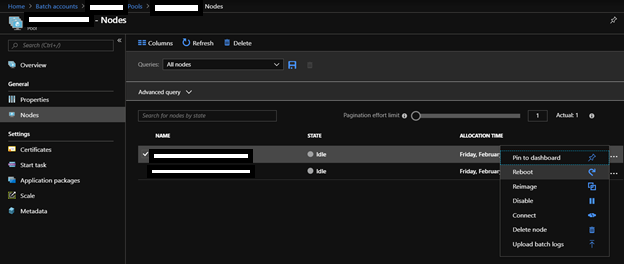
1. From the Azure Batch account, click **Pools** and then **Certificates**.
2. Select the correct *Thumbprint* in the dropdown, set Store Location to **LocalMachine**, and ensure that all Visibility options are selected:



1. Click **Save**.

## Reboot Azure Batch VMs

1. From the Azure Batch Pool, select **Nodes**.
2. Reboot each of the Azure Batch VMs so the Certificate is applied:



# Grant Access to MachineKeys Folder on Azure Batch VM(s)

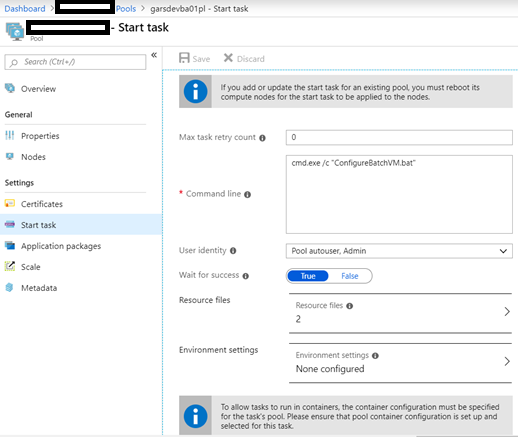
1. Unless the account running the PowerShell scripts on the Azure Batch VM(s) has access to the folder **C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys**, you will receive a “keyset does not exist”.
2. Sign onto each Azure Batch VM and grant **Read** access to **Everyone** on the **C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys** folder.

# Create Start Task for Azure Batch VMs

The MachineKeys folder permissions and certificate application can be undone by Azure during updates, causing the Azure Batch VMs to enter a bad state.

To mitigate this issue, create Start Tasks for the Azure Batch VMs to keep them in the desired state.

1. Navigate to the **Azure Batch Pool**.
2. Click on **Start Task**.



1. Enter the following:
   1. **Command line**: cmd.exe /c “ConfigureBatchVM.bat”
   2. **User identity**: Pool autouser, Admin
   3. **Wait for success**: True
2. The **ConfigureBatchVM.bat** file consists of:

:: REMOVE FOLDER PERMISSION : Everyone

icacls "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys" /remove "Everyone" /T /C

:: REMOVE FOLDER PERMISSION : WATASK\_COMMON\_GROUP

icacls "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys" /remove "WATASK\_COMMON\_GROUP" /T /C

:: SET DEFAULT FOLDER PERMISSION : Everyone

icacls "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys" /grant "Everyone":(NP)(RD,RA,REA,WD,AD,WA,WEA,RA,RC) /inheritance:r /T /C

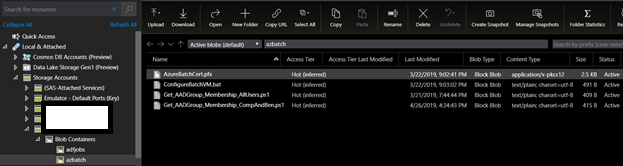
:: REAPPLY CERTIFICATE

CERTUTIL -f -p Password123! -importpfx "AzureBatchCert.pfx"

:: ADD FOLDER PERMISSION : WATASK\_COMMON\_GROUP

icacls "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys" /grant "WATASK\_COMMON\_GROUP":(OI)(CI)(R) /T /C

1. Click **Resource Files** and upload the following files to Azure Blob Storage under the folder **azbatch**:
   1. the Certificate .pfx file used above
   2. the ConfigureBatchVM.bat file (contents below)



1. Click **Save**.
2. Reboot the Batch VMs.

# Test Connectivity

1. Sign into one of the Azure Batch VMs.
2. Open PowerShell.
3. Run the following command, substituting the values saved-off above as appropriate:

**Connect-AzAccount** -CertificateThumbprint "ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ" -Appl

icationId "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX" -Tenant "YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY" -ServicePrincipal



1. If working correctly, no errors should appear.