To connect to **Azure** using **PowerShell** with a **client certificate** (typically for service principal authentication), you can use the Connect-AzAccount cmdlet along with the certificate thumbprint.

Here’s the PowerShell code to do this securely:

### **✅ Pre-requisites**

1. A **service principal** created with a certificate (either self-signed or issued by a CA).
2. The certificate installed in the **CurrentUser\My** store.
3. The **thumbprint** of the certificate.
4. The **Application (client) ID**, **Tenant ID**, and **Subscription ID**.

### **🔐 PowerShell Code: Login with Client Certificate**

powershell

CopyEdit

# Variables  
$tenantId = "<Your-Tenant-ID>"  
$appId = "<Your-Application-Client-ID>"  
$certThumbprint = "<Your-Certificate-Thumbprint>"  
$subscriptionId = "<Your-Subscription-ID>"  
  
# Connect using certificate  
Connect-AzAccount `  
 -ServicePrincipal `  
 -Tenant $tenantId `  
 -ApplicationId $appId `  
 -CertificateThumbprint $certThumbprint `  
 -SubscriptionId $subscriptionId

### **📌 Notes**

* The certificate must be located in the **Current User's Personal store** (Cert:\CurrentUser\My).
* You can check for your certificate with:

powershell

CopyEdit

Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object { $\_.Thumbprint -eq "<Your-Certificate-Thumbprint>" }

* If you are using a **PFX file**, you can import it first:

powershell

CopyEdit

$cert = Import-PfxCertificate -FilePath "C:\Path\To\Cert.pfx" -CertStoreLocation Cert:\CurrentUser\My

Let me know if you'd prefer to use the certificate from a file directly without importing it to the store, or if you're using a managed identity instead.

##### **You said:**

want to use the certificate from the file directly and it requires certificate password as well

###### **ChatGPT said:**

To authenticate to **Azure** using **PowerShell** with a **client certificate file (.pfx)** and a **password**, you can use the Connect-AzAccount cmdlet with the -Certificate parameter.

Here’s how you can do it:

### **✅ PowerShell Script: Connect Using Client Certificate File (.pfx)**

powershell

CopyEdit

# Variables  
$pfxPath = "C:\Path\To\YourCert.pfx"  
$certPassword = ConvertTo-SecureString -String "your-cert-password" -AsPlainText -Force  
$appId = "<Your-Application-Client-ID>"  
$tenantId = "<Your-Tenant-ID>"  
$subscriptionId = "<Your-Subscription-ID>"  
  
# Import the certificate from PFX file  
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2  
$cert.Import($pfxPath, $certPassword, [System.Security.Cryptography.X509Certificates.X509KeyStorageFlags]::Exportable)  
  
# Connect to Azure using the certificate  
Connect-AzAccount `  
 -ServicePrincipal `  
 -ApplicationId $appId `  
 -TenantId $tenantId `  
 -Certificate $cert `  
 -SubscriptionId $subscriptionId

### **📌 Notes**

* Exportable flag is used so the private key can be used for authentication.
* This does **not** require you to import the certificate into the store.
* If you want to **secure the password** better, use Read-Host -AsSecureString or a Key Vault reference instead of hardcoding it.

Example for secure password prompt:

powershell

CopyEdit

$certPassword = Read-Host -Prompt "Enter certificate password" -AsSecureString

Let me know if you’d like to automate this further with Azure Key Vault to retrieve the certificate and password securely.

##### **You said:**

get me the whole code whole code using venafi certificate along certificate password

###### **ChatGPT said:**

If you're using a **Venafi-issued certificate** stored as a **.pfx file**, and want to authenticate to **Azure using PowerShell** with the **certificate file and password**, here's a complete script that securely handles the connection.

This script does **not** require the certificate to be imported into the Windows certificate store.

### **✅ Complete PowerShell Script: Connect to Azure using Venafi PFX Certificate**

powershell

CopyEdit

# ---------------------------------------------  
# Configuration: Set these variables  
# ---------------------------------------------  
$pfxPath = "C:\Path\To\VenafiIssuedCertificate.pfx" # Path to your Venafi-issued PFX file  
$appId = "<Your-Azure-AD-App-Client-ID>" # Application (client) ID of the service principal  
$tenantId = "<Your-Azure-AD-Tenant-ID>" # Azure AD Tenant ID  
$subscriptionId = "<Your-Azure-Subscription-ID>" # Azure Subscription ID  
  
# Prompt user for the certificate password securely  
$certPassword = Read-Host -Prompt "Enter certificate password" -AsSecureString  
  
# ---------------------------------------------  
# Load the certificate from file  
# ---------------------------------------------  
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2  
$cert.Import(  
 $pfxPath,  
 $certPassword,  
 [System.Security.Cryptography.X509Certificates.X509KeyStorageFlags]::Exportable  
)  
  
# Optional: Print certificate info (for debug)  
Write-Host "Using Certificate Subject:" $cert.Subject  
Write-Host "Thumbprint:" $cert.Thumbprint  
  
# ---------------------------------------------  
# Connect to Azure with client certificate  
# ---------------------------------------------  
Connect-AzAccount `  
 -ServicePrincipal `  
 -ApplicationId $appId `  
 -TenantId $tenantId `  
 -Certificate $cert `  
 -SubscriptionId $subscriptionId  
  
# ---------------------------------------------  
# Validate Connection  
# ---------------------------------------------  
$context = Get-AzContext  
Write-Host "Connected to Azure subscription:" $context.Subscription.Name

### **🔒 Security Tips**

* Never hardcode the password in scripts.
* Use Read-Host -AsSecureString or pull it securely from **Azure Key Vault** if running in CI/CD or automation scenarios.
* Ensure the **service principal** in Azure AD has the correct **RBAC permissions** to access Azure resources.

Let me know if you want the same workflow using Azure Key Vault to retrieve the Venafi certificate and password at runtime (without storing on disk).

##### **You said:**

need the powershell code to upload folders/files to azure storage account using the same client certificate authentication. put all of these together in a single code file

###### **ChatGPT said:**

Here’s a **complete PowerShell script** that:

1. **Authenticates to Azure** using a **Venafi-issued .pfx certificate** (from file, with password).
2. **Connects to a specific Azure subscription.**
3. **Uploads folders/files** to an **Azure Blob Storage container** using Az.Storage module.

### **📄 Complete PowerShell Script: Authenticate with Certificate + Upload Files to Blob Storage**

powershell

CopyEdit

# ============================  
# Configuration Section  
# ============================  
  
# Certificate config  
$pfxPath = "C:\Path\To\VenafiIssuedCertificate.pfx" # Path to PFX certificate  
$appId = "<Your-Azure-AD-App-Client-ID>" # Azure AD App (client ID)  
$tenantId = "<Your-Azure-AD-Tenant-ID>" # Azure AD tenant  
$subscriptionId = "<Your-Azure-Subscription-ID>" # Azure subscription  
  
# Storage upload config  
$resourceGroupName = "<Your-Resource-Group-Name>"  
$storageAccountName = "<YourStorageAccountName>" # Must be globally unique  
$containerName = "<YourContainerName>" # Blob container name  
$localPathToUpload = "C:\Path\To\Local\FolderOrFile" # Folder or file to upload  
  
# ============================  
# Authentication  
# ============================  
  
# Prompt for certificate password securely  
$certPassword = Read-Host -Prompt "Enter certificate password" -AsSecureString  
  
# Load the certificate from the PFX file  
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2  
$cert.Import($pfxPath, $certPassword, [System.Security.Cryptography.X509Certificates.X509KeyStorageFlags]::Exportable)  
  
# Login to Azure using the certificate  
Connect-AzAccount `  
 -ServicePrincipal `  
 -ApplicationId $appId `  
 -TenantId $tenantId `  
 -Certificate $cert `  
 -SubscriptionId $subscriptionId  
  
# ============================  
# Get Storage Context  
# ============================  
  
# Get the storage account key  
$storageAccountKey = (Get-AzStorageAccountKey -ResourceGroupName $resourceGroupName -Name $storageAccountName)[0].Value  
  
# Create the storage context  
$ctx = New-AzStorageContext -StorageAccountName $storageAccountName -StorageAccountKey $storageAccountKey  
  
# ============================  
# Upload File(s)  
# ============================  
  
# Check if it's a directory or file  
if (Test-Path $localPathToUpload -PathType Container) {  
 # Upload folder (recursively)  
 Get-ChildItem -Path $localPathToUpload -Recurse | ForEach-Object {  
 if (-not $\_.PSIsContainer) {  
 $relativePath = $\_.FullName.Substring($localPathToUpload.Length).TrimStart('\')  
 Set-AzStorageBlobContent -File $\_.FullName -Container $containerName -Blob $relativePath -Context $ctx | Out-Null  
 Write-Host "Uploaded file: $relativePath"  
 }  
 }  
}  
elseif (Test-Path $localPathToUpload -PathType Leaf) {  
 # Upload single file  
 $fileName = Split-Path -Path $localPathToUpload -Leaf  
 Set-AzStorageBlobContent -File $localPathToUpload -Container $containerName -Blob $fileName -Context $ctx | Out-Null  
 Write-Host "Uploaded file: $fileName"  
}  
else {  
 Write-Error "Path not found: $localPathToUpload"  
}  
  
# ============================  
# Done  
# ============================  
Write-Host "`n✅ Upload complete."

### **✅ Requirements**

* PowerShell modules:
  + Az.Accounts
  + Az.Storage
* Venafi certificate in .pfx format accessible on disk.
* Role assignment: The service principal must have **Storage Blob Data Contributor** on the storage account.

Let me know if you want to **upload to Azure Data Lake (ADLS Gen2)** or **read the certificate and password from Azure Key Vault** instead.