

Palo Alto Global Protect VPN - Smart Card Client Authentication Workaround

These instructions are designed to resolve an issue which can occur if you have a VPN such as Palo Alto GlobalProtect which expects a Client Authentication certificate and automatically selects an incorrect certificate on a YubiKey. If Client Authentication is removed from the Application Policies on the template, RDP and Kerberos authentication no longer work.

This guide will assist you with creating a new certificate template based on the existing one, removing Client Authentication and adding back Kerberos and RDP authentication functionality. The existing template will not be deleted. The purpose of keeping the existing template is for maximum compatibility where Client Authentication is required but GlobalProtect is not required.

These instructions are provided as-is for guidance purposes only. Ensure you are familiar with ADCS and the implications of incorrect configurations.

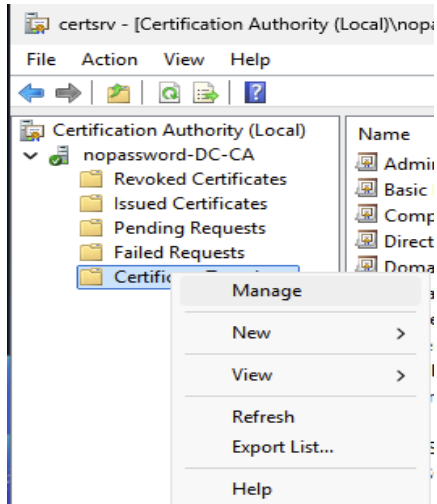
Requirements

Before starting, please ensure that you have the following available:

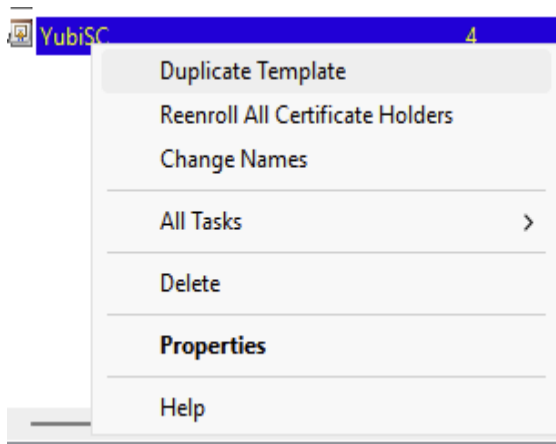
- A fully configured Active Directory Certificate Services installation with an appropriate YubiKey template already defined.
- Rights to edit the Certificate Services configuration including creation and configuration of templates
- Appropriate approved change controls in place.

Process

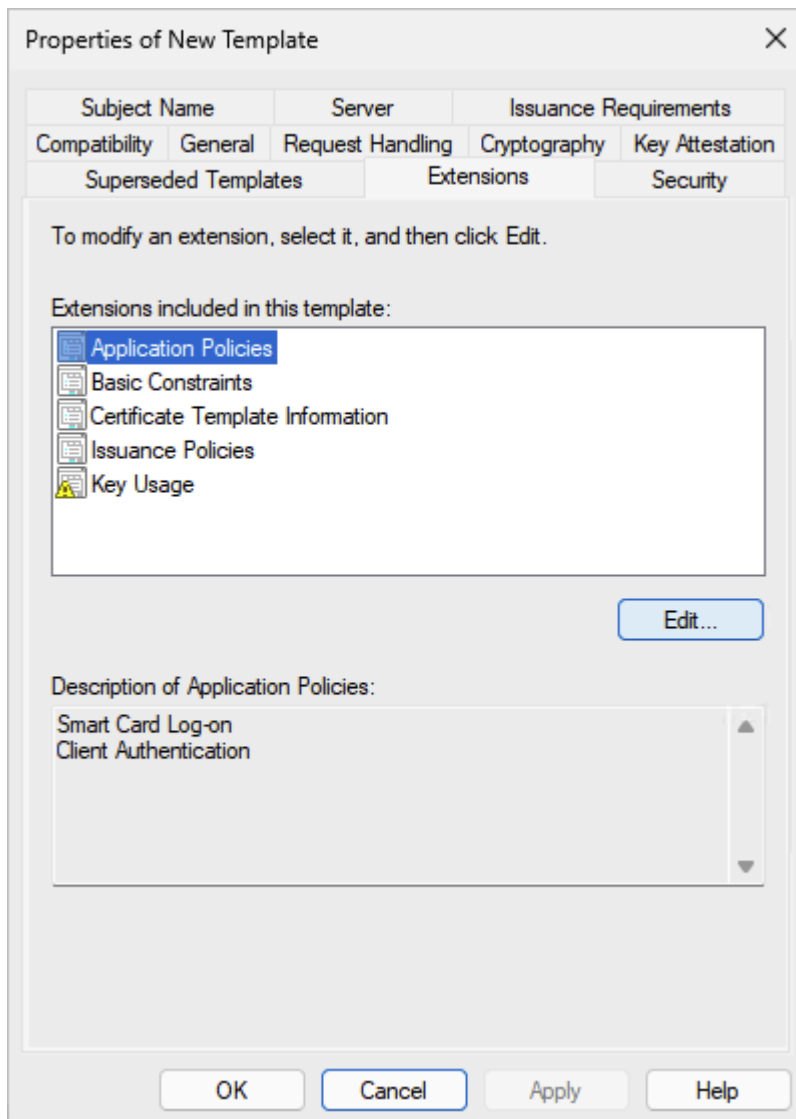
- 1) Open the Certification Authority mmc and expand out the CA. Right click on **Certificate Templates** and choose **Manage**.



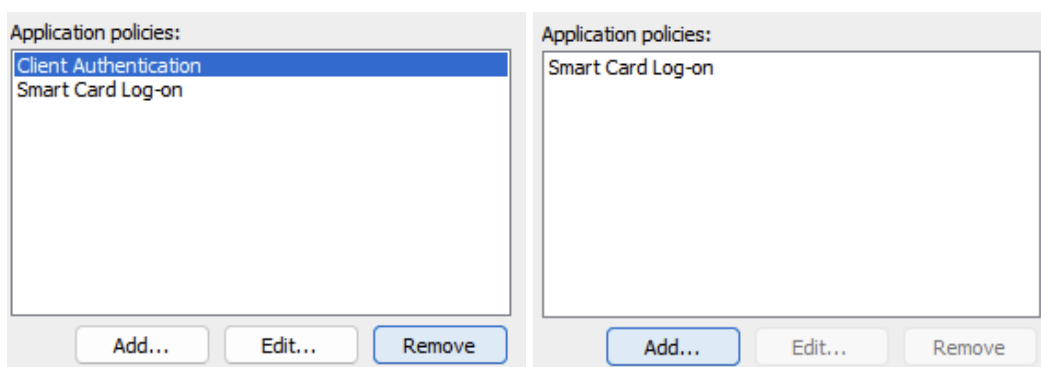
- 2) The certificate templates console will open. Right click your existing YubiKey template and choose **Duplicate Template**.



- 3) Click **Extensions**, make sure **Application Policies** is selected and click Edit.



4) Select **Client Authentication** and click Remove, then click Add.



- 5) Click on New. In the **New Application Policy** Window type the following in the fields.

Name: PKInit Kerberos

Object Identifier: 1.3.6.1.5.2.3.4 (Replace the existing contents with this)

The image shows two overlapping Windows dialog boxes. The top dialog, titled 'Add Application Policy', contains explanatory text about application policies. The bottom dialog, titled 'New Application Policy', is the active window for creating a new policy. It has two text input fields: 'Name' with the value 'PKInit Kerberos' and 'Object identifier' with the value '1.3.6.1.5.2.3.4'. At the bottom of this dialog are 'OK' and 'Cancel' buttons. Below the 'New Application Policy' dialog, there is a 'New...' button and another set of 'OK' and 'Cancel' buttons, which are part of the parent 'Add Application Policy' dialog.

Click OK to save the policy.

- 6) Add another policy by clicking New. In the **New Application Policy** Window type the following in the fields.

Name: Remote Desktop

Object Identifier: 1.3.6.1.4.311.54.1.2 (Replace the existing contents with this)

The image shows two overlapping Windows dialog boxes. The top dialog, titled 'Add Application Policy', contains explanatory text about application policies. The bottom dialog, titled 'New Application Policy', is active and contains two text input fields. The first field, labeled 'Name:', contains the text 'Remote Desktop'. The second field, labeled 'Object identifier:', contains the text '1.3.6.1.4.1.311.54.1.2'. At the bottom of the 'New Application Policy' dialog, there are two sets of buttons: 'OK' and 'Cancel' on the left, and 'New...' and 'OK' on the right.

Add Application Policy

An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

New Application Policy

Type a name for the new application policy, and if necessary change the object identifier.

Name:

Remote Desktop

Object identifier:

1.3.6.1.4.1.311.54.1.2

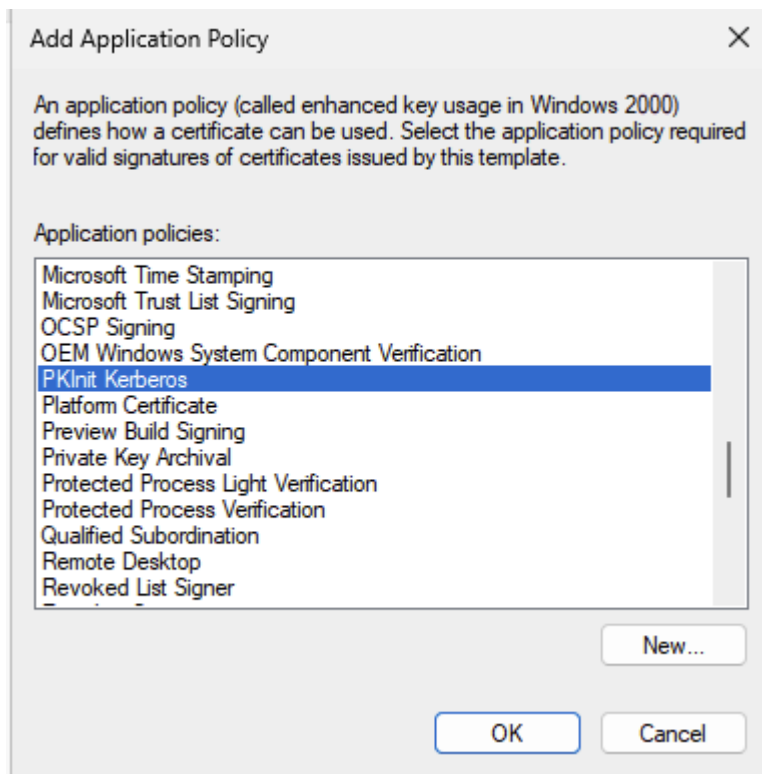
OK Cancel

New...

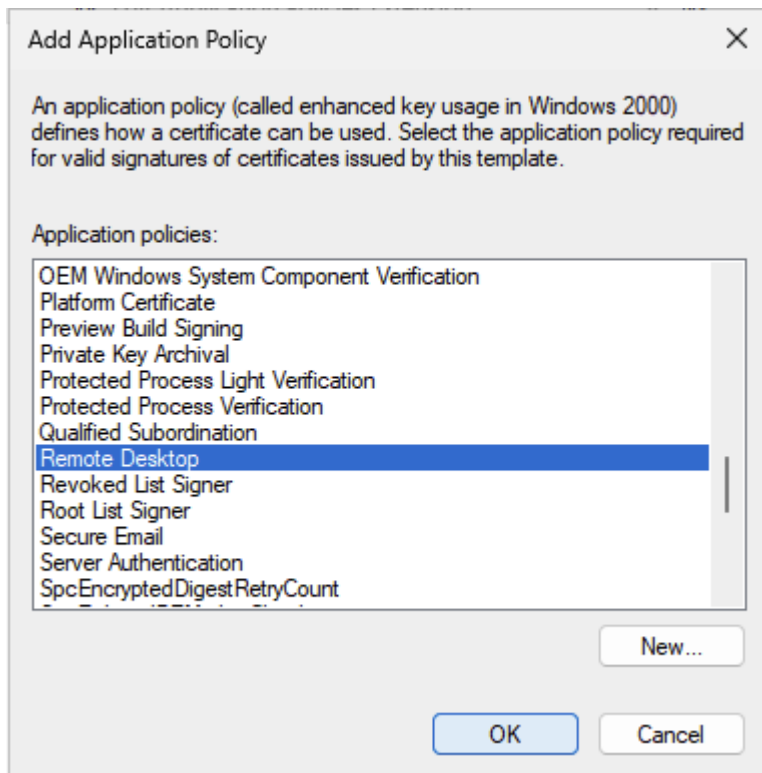
OK Cancel

Click OK to save the policy.

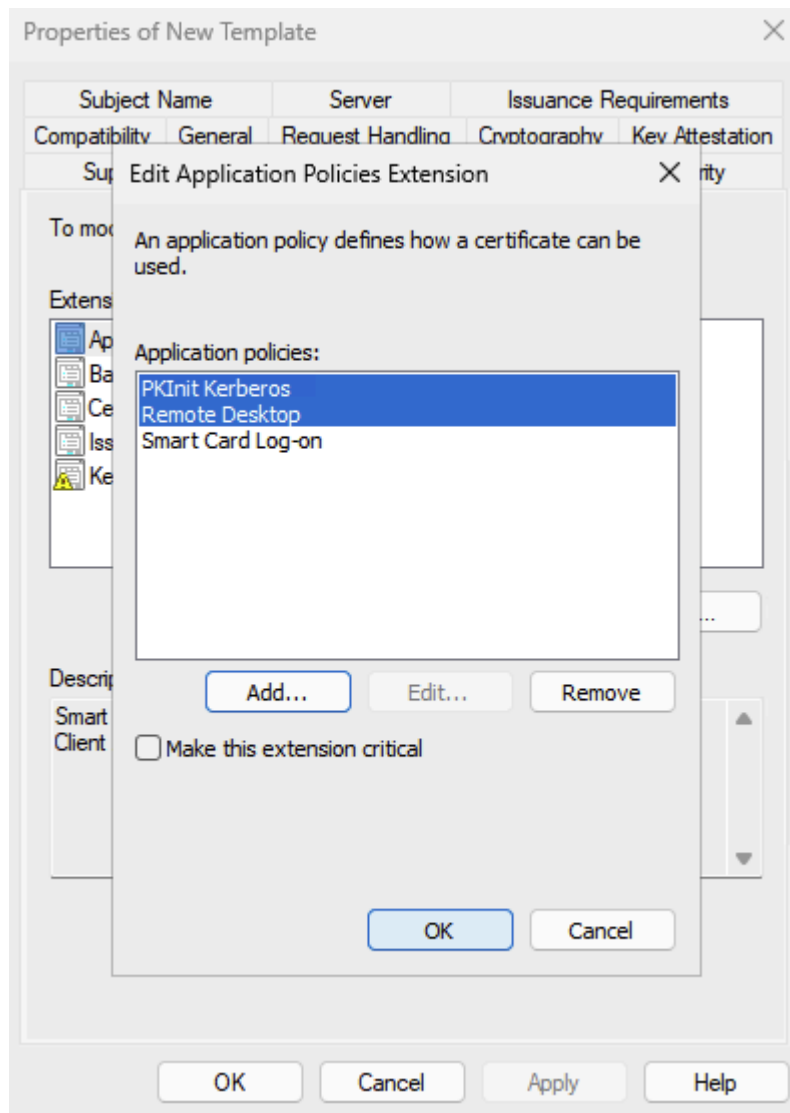
- 7) Add both of the new policies to the template. Find **PKInit Kerberos**, select it and then click **OK**.



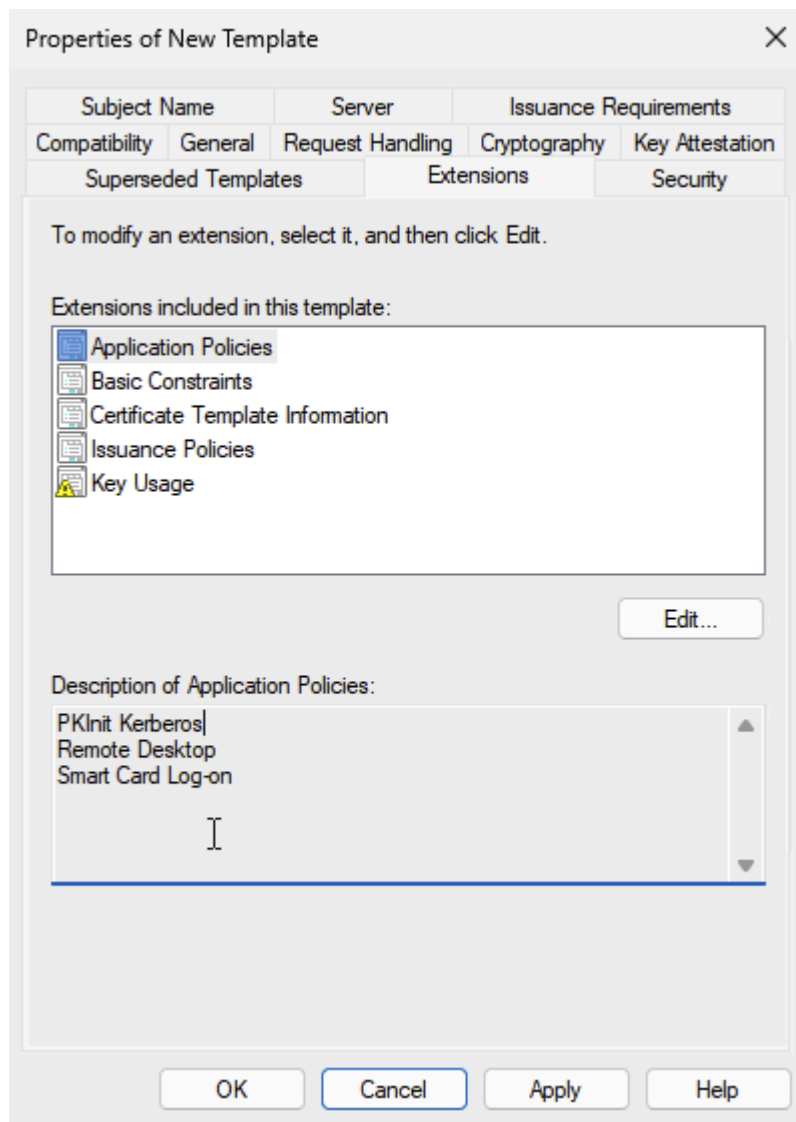
Do the same for Remote Desktop by clicking **Add** on the **Edit Application Policies Extension** window, then search for Remote Desktop and click OK.



8) Click OK to accept the new additions to the template.



- 9) Description of Application Policies should now contain the three items as shown in the image below.



- 10) Click on **General** and rename the template to a suitable name for your environment then click **OK**. **Important:** This template name **must** be fundamentally different from the existing template if you have Auto Enrollment enabled.

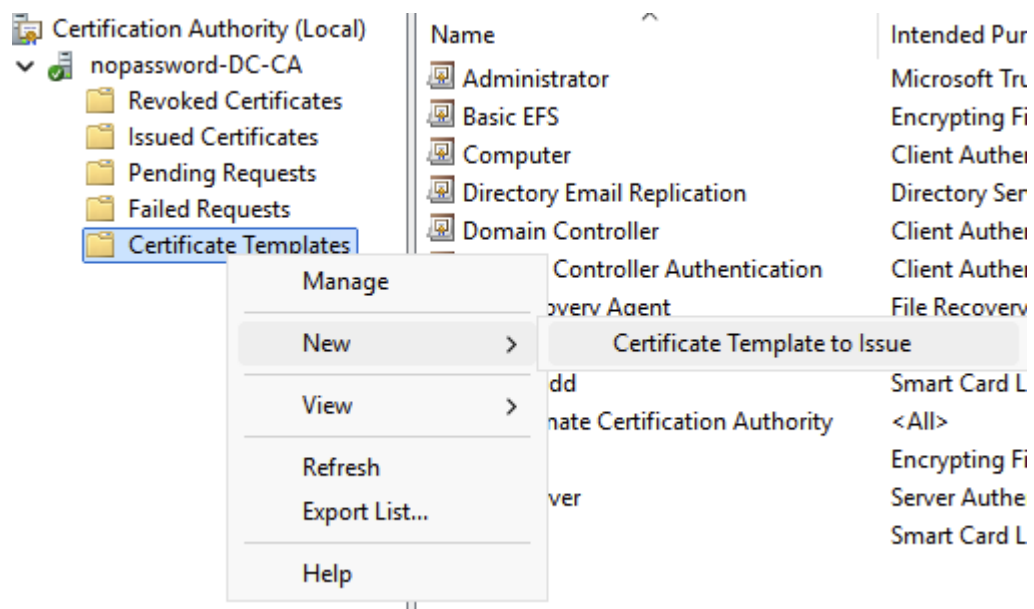
The screenshot shows the 'Properties of New Template' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Subject Name, Server, Issuance Requirements, Superseded Templates, Extensions, Security, Compatibility, General (selected), Request Handling, Cryptography, and Key Attestation. The 'General' tab contains the following fields and options:

- Template display name:** A text box containing 'YubiKey-NoClientAuth'.
- Template name:** A text box containing 'YubiKey-NoClientAuth'.
- Validity period:** A dropdown menu showing '2' and 'years'.
- Renewal period:** A dropdown menu showing '6' and 'weeks'.
- ☐ **Publish certificate in Active Directory**
 - ☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

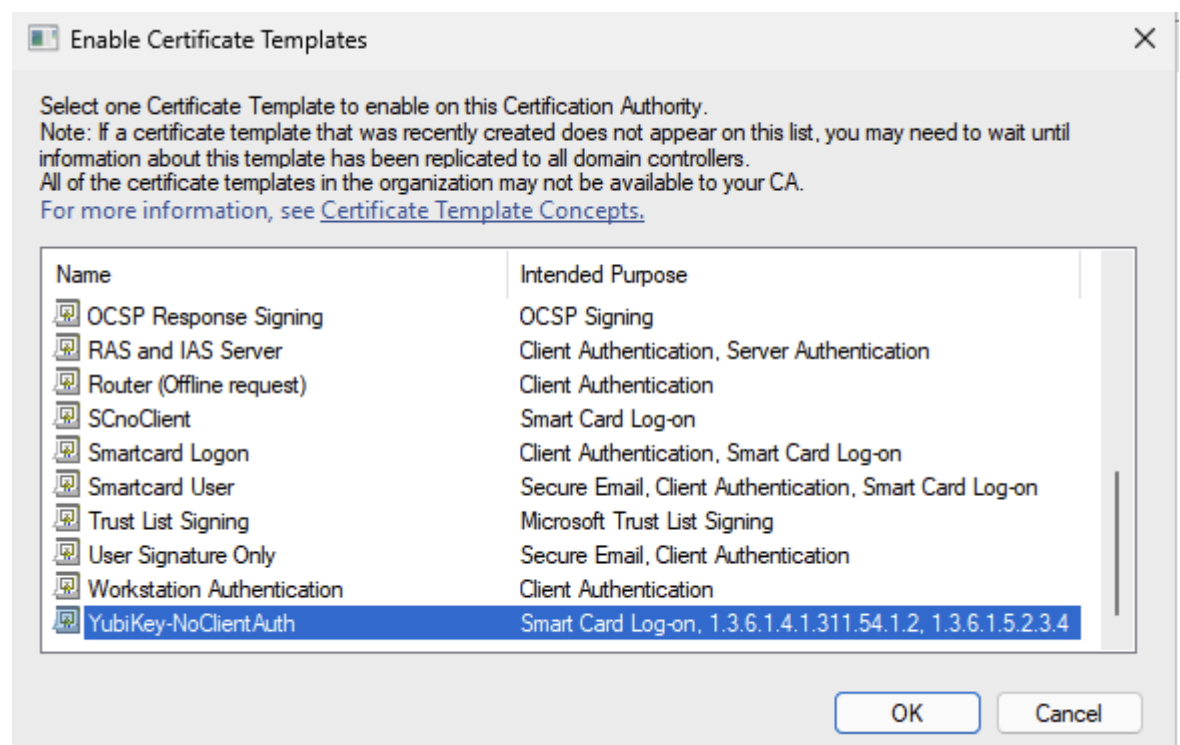
At the bottom of the dialog are four buttons: OK, Cancel, Apply, and Help.

11) No other template changes are required as this is a direct copy of your existing YubiKey template. Close the **Certificate Templates** window and return to the **Certification Authority** window.

12) Right click on **Certificate Templates**, choose **New > Certificate Template to Issue**.



Find your new template in the list, select it and click **OK**

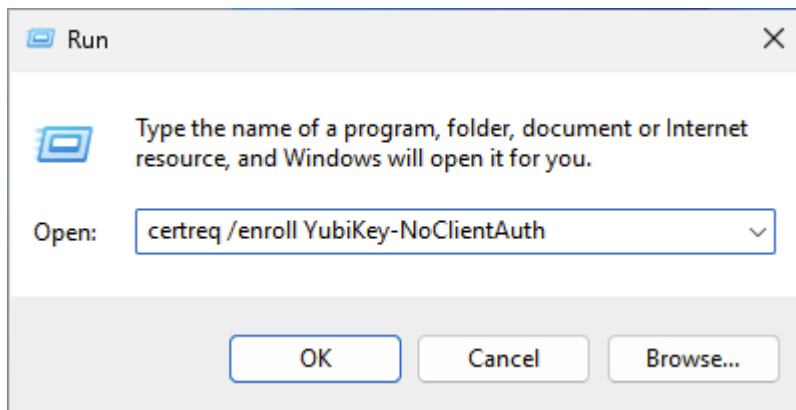


- 13) Allow for Certificate Services and Active Directory replication to propagate the template. This will vary depending on your individual domain setup.

After this has completed, use a new YubiKey to enroll using the new template. The easiest way to achieve this is to sign on as the target user and run certreq.exe as shown below.

Note: Replace the template name with your new template name.

certreq /enroll YubiKey-NoClientAuth



- 14) Click **Next** when prompted and then click **Enroll**. Type the YubiKey PIN when prompted and click **OK** to finish the provisioning process.
- 15) Perform testing to ensure the YubiKey is able to authenticate your Kerberos and RDP based sessions as well as Windows Logon.