Microsoft Direct Access Integration

Contents

Introduction

Microsoft Direct Access allows a VPN connection to be brought up when a user requires access to an organisations internal resources. PINsafe can authenticate a user accessing those internal resources using Dual channel authentication such as SMS, Mobile Phone Client and the Taskbar utility Taskbar How to Guide and Token.

Prerequisites

Microsoft Direct Access fully configured

Microsoft CA server for OTP authentication

PINsafe 3.x

Baseline

Microsoft UAG SP1 with Direct access configured

PINsafe 3.8

Architecture

When a Direct Access connection is made, a pop up appears for the user prompting them to enter their One Time Code. This is then checked by the UAG against PINsafe using RADIUS authentication.

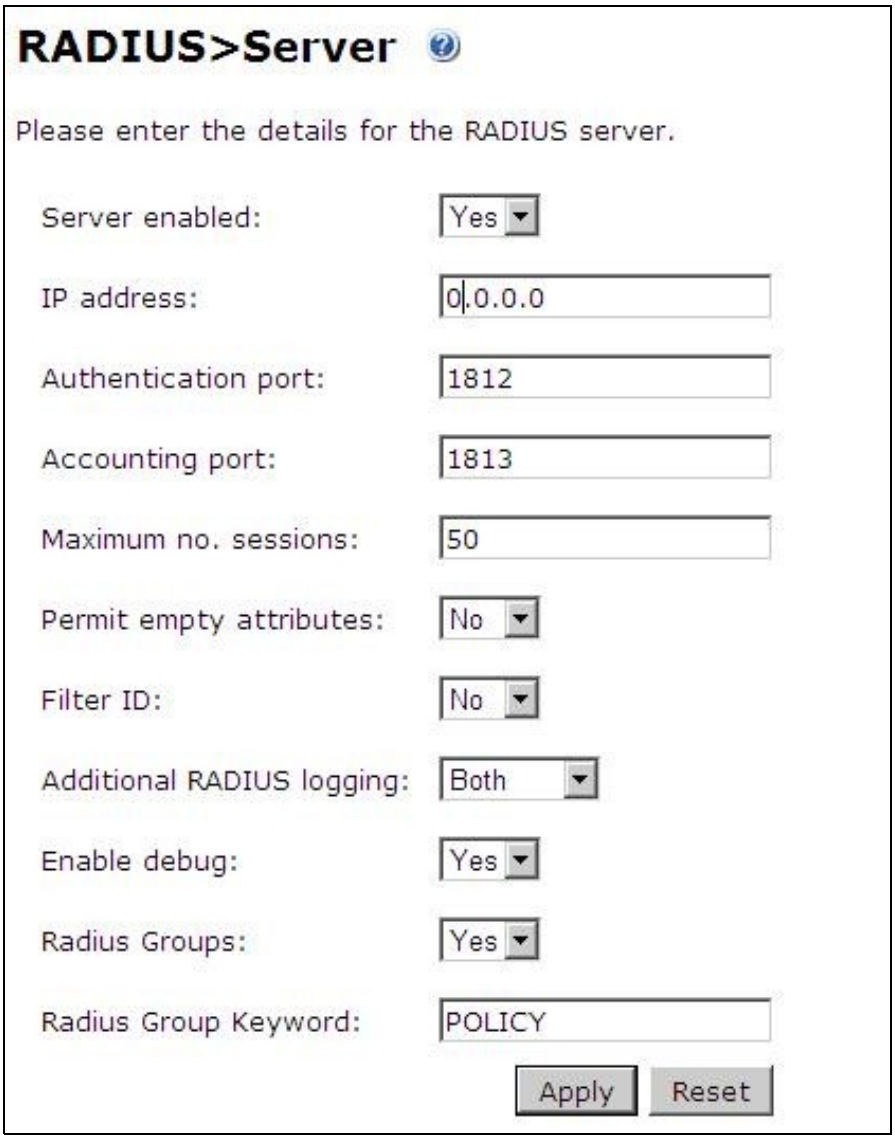
Installation

PINsafe Configuration

Configuring the RADIUS server

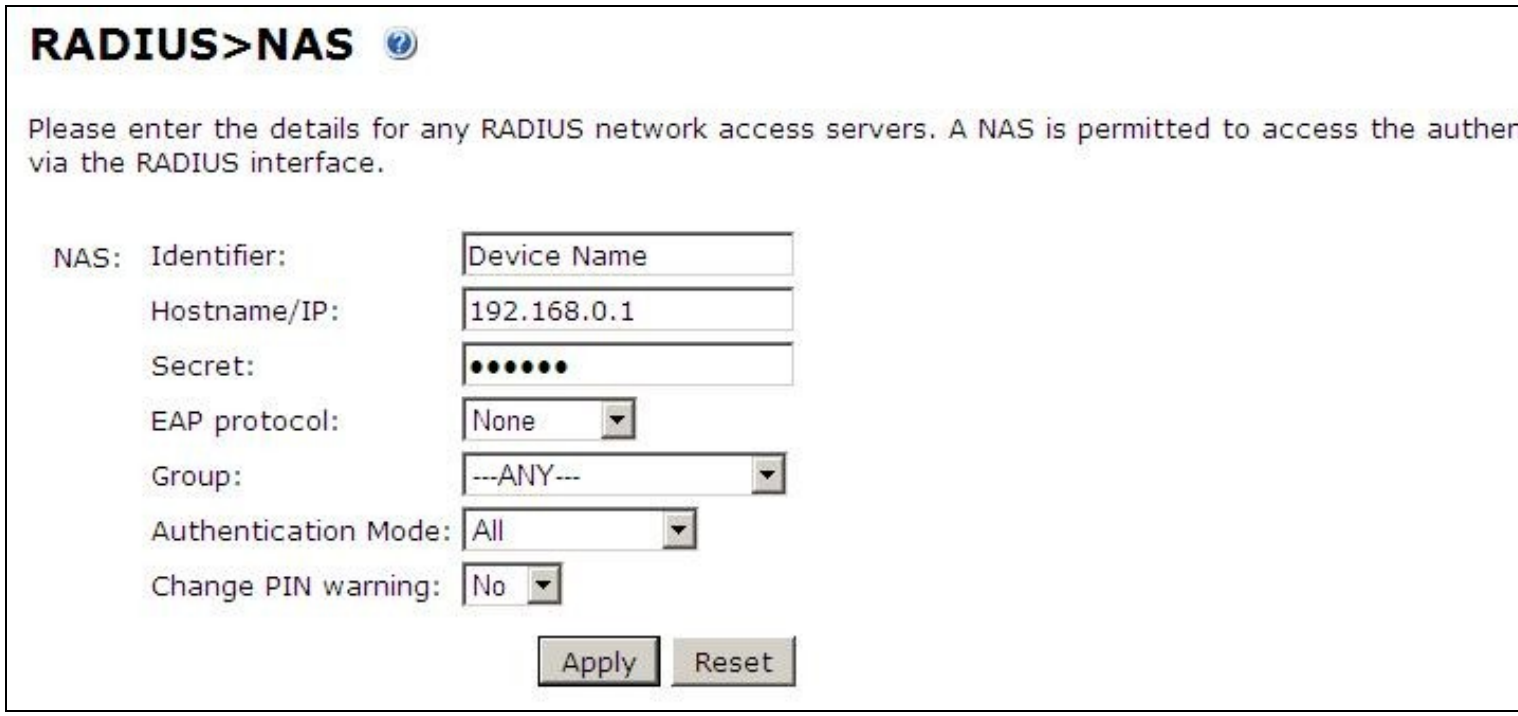
Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for appliances, the PINsafe VIP should not be used as the server IP address, see VIP on PINsafe Appliances



Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.



You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP will be supported. All users will be able to authenticate via this NAS unless to restrict authentication to a specific repository group.

Enabling Session creation with username

PINsafe can be configured to use the Taskbar to present a TURing image to users when prompted for authentication by Direct Access. See Taskbar How to Guide

To allow Single Channel authentication on PINsafe follow the below steps.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid PINsafe username:

Appliance

https://PINsafe_server_IP:8443/proxy/SCImage?username=testuser

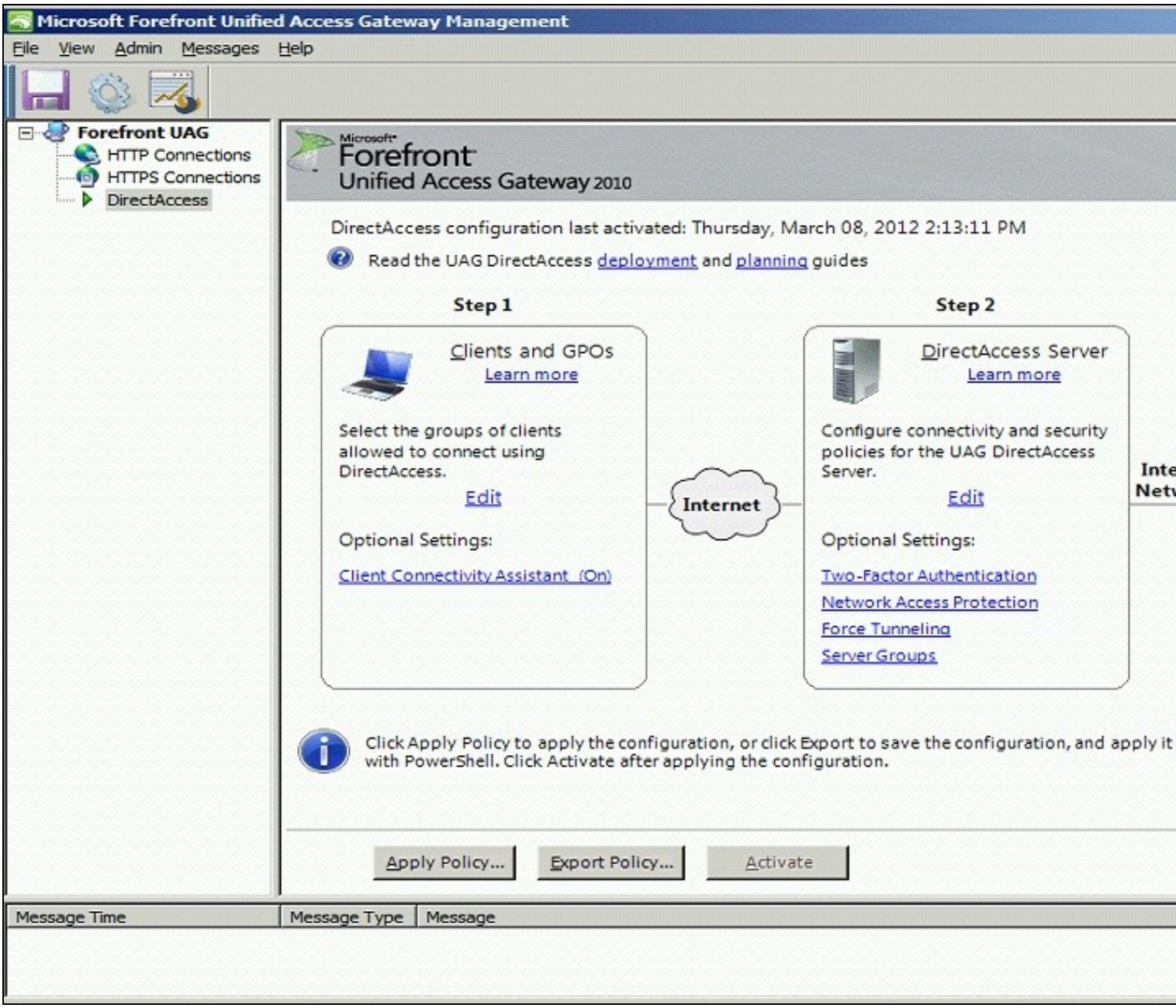
For a software only install see Software Only Installation

Microsoft Direct Access Integration

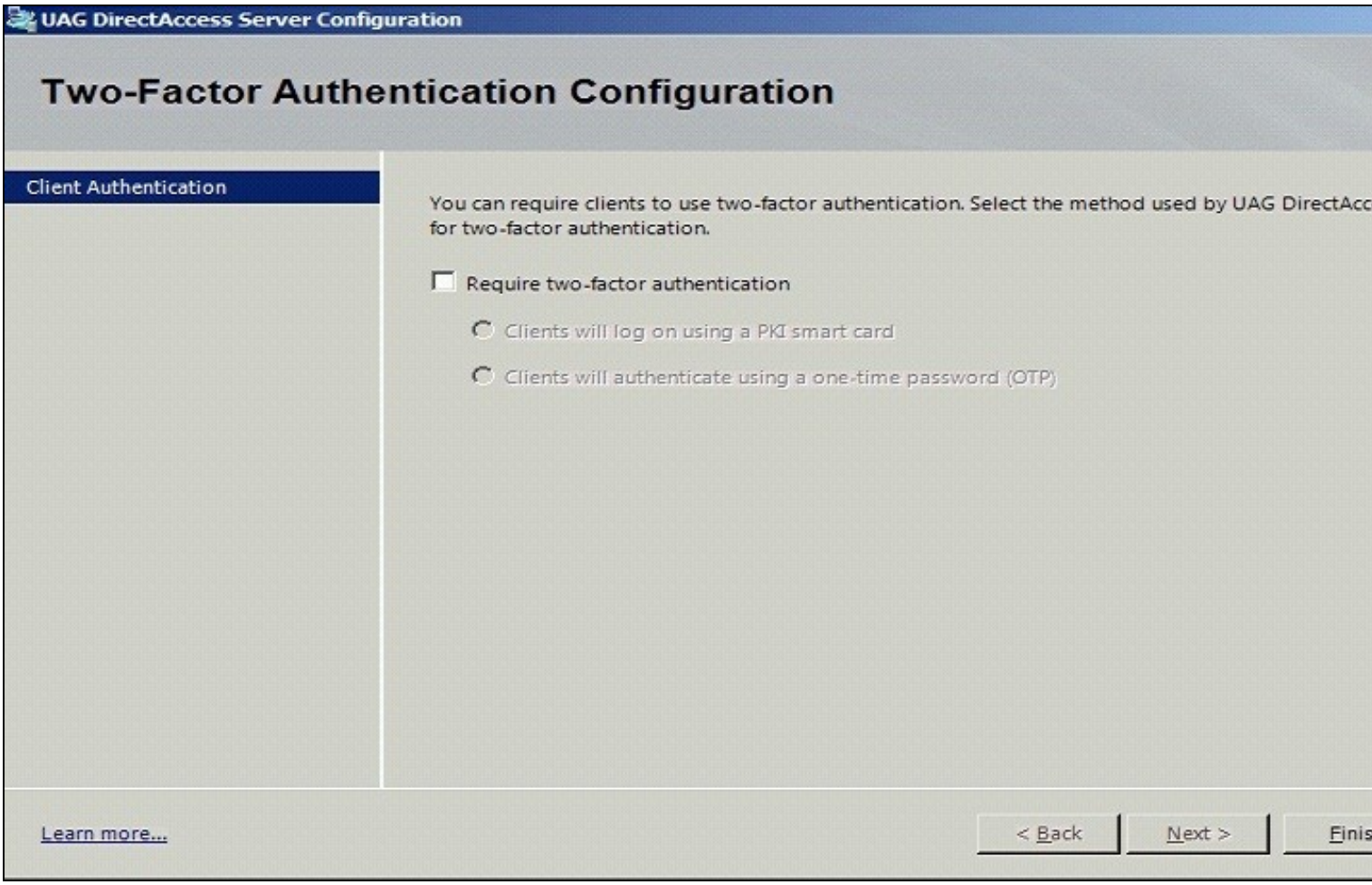
Ensure that the Microsoft Direct Access is fully working and tested before startigng the PINsafe integration.

Enable Two Factor Authentication

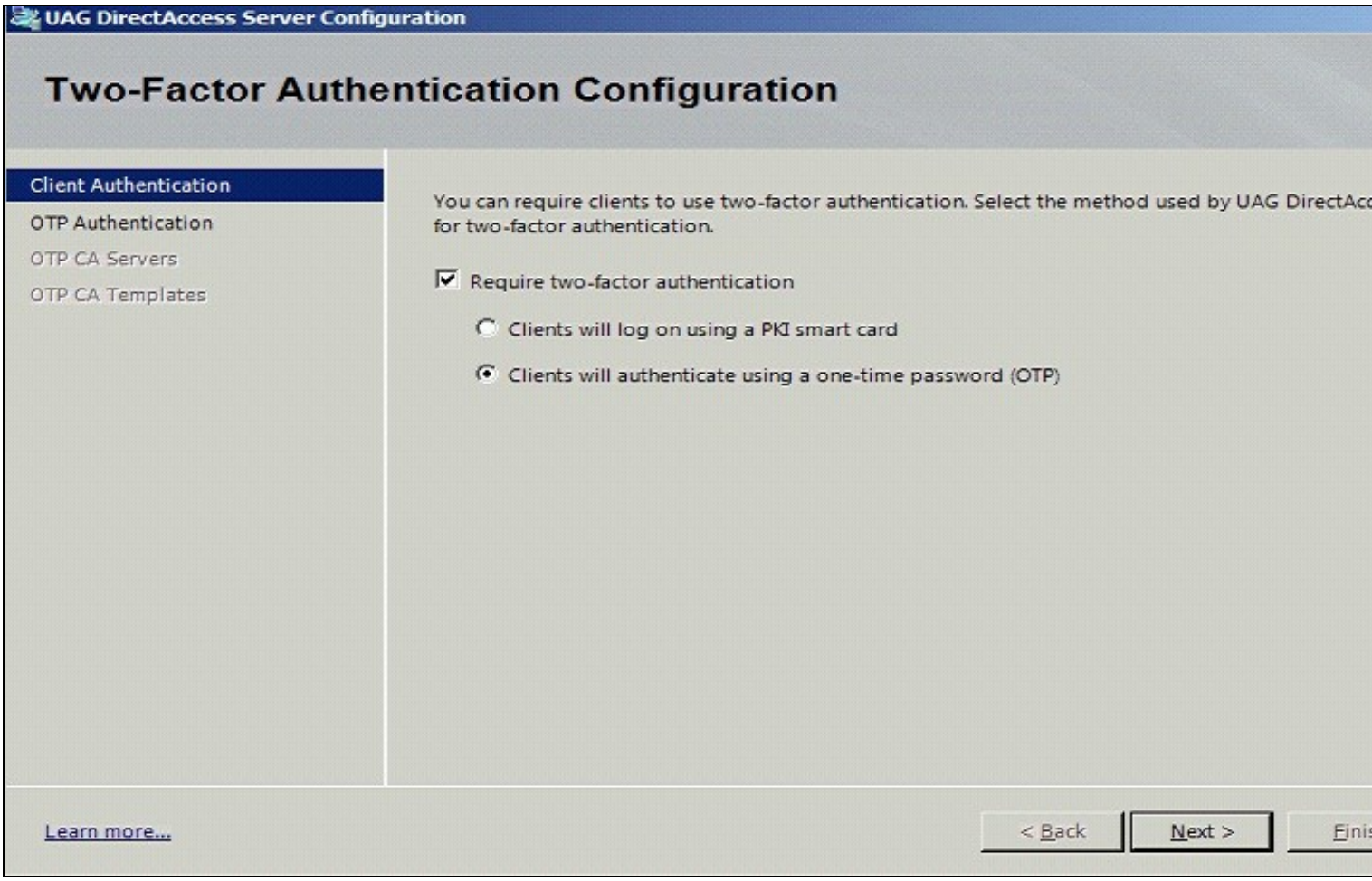
On the Forefront UAG Direct Access configuration page select under Step 2 Optional Settings the link for *Two-Factor Authentication*



Click on *Require two-factor authentication*

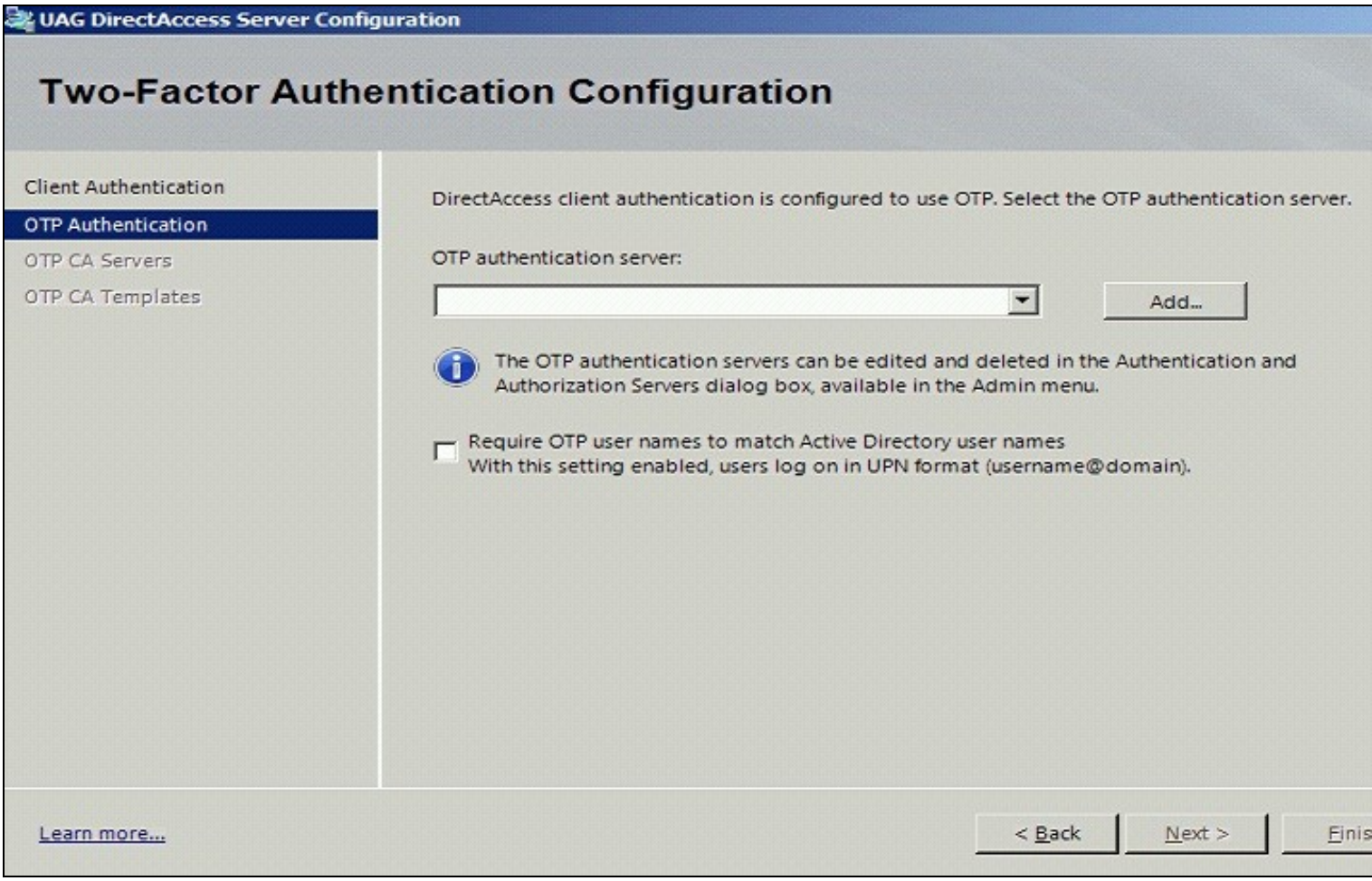


Click on *Clients will authenticate using a one-time password (OTP)*



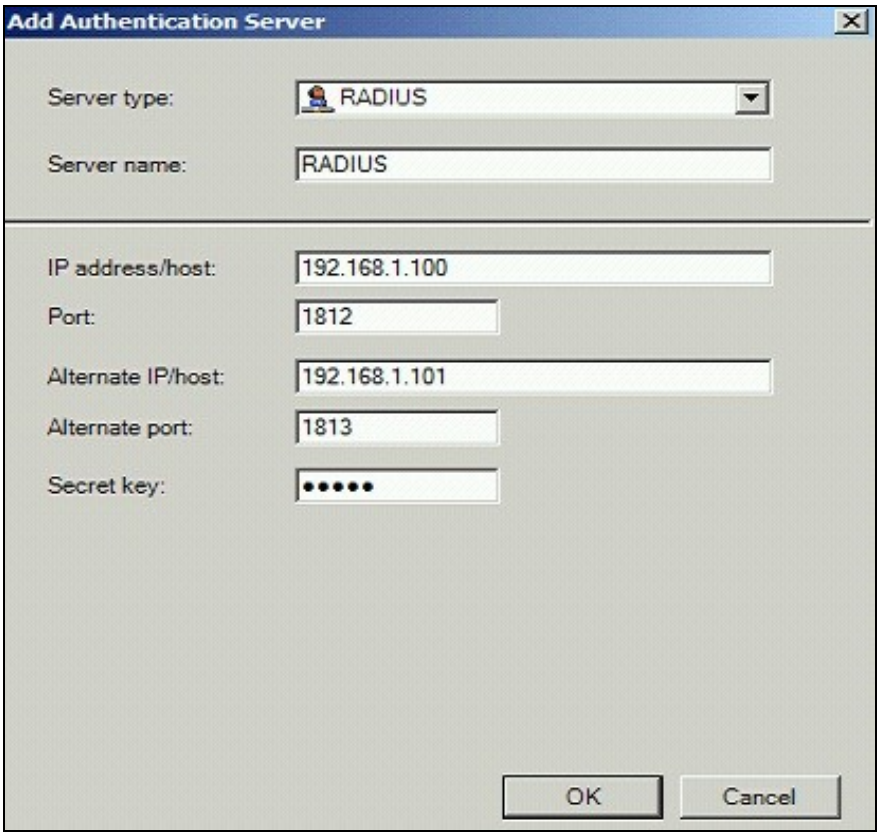
Configure OTP Authentication Server

On the OTP Authentication tab click Add

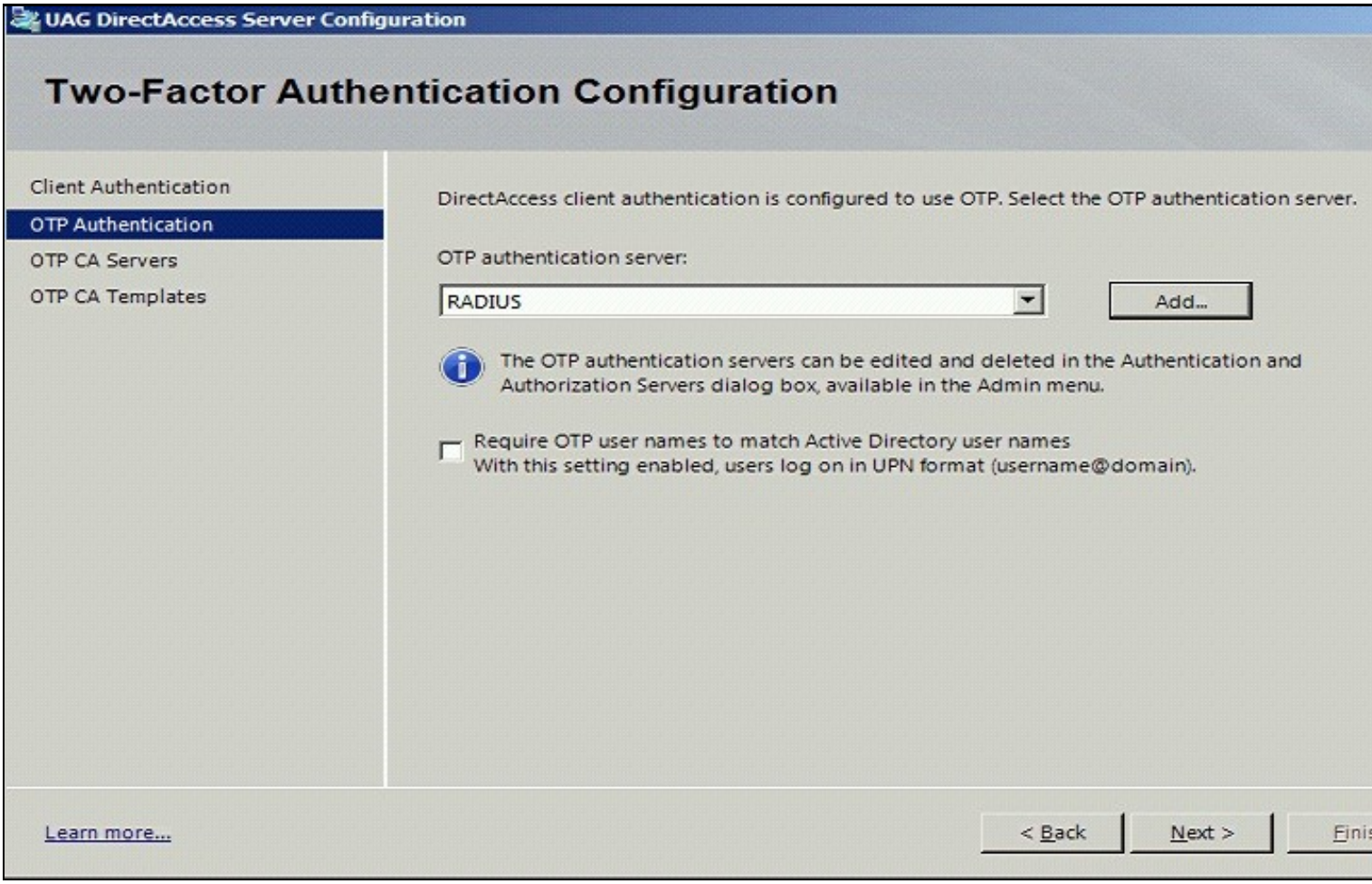


Select Server Type RADIUS and enter the following information:

- Server Name: A descriptive name for the RADIUS server
- Port: RADIUS port used by the Swivel server, usually 1812
- IP address/host: The Swivel RADIUS server
- Alternate IP/host: A secondary Swivel RADIUS server
- Alternate port: The port used by the secondary Swivel server, usually 1812
- Secret Key: A shared secret entered on the Swivel servers.

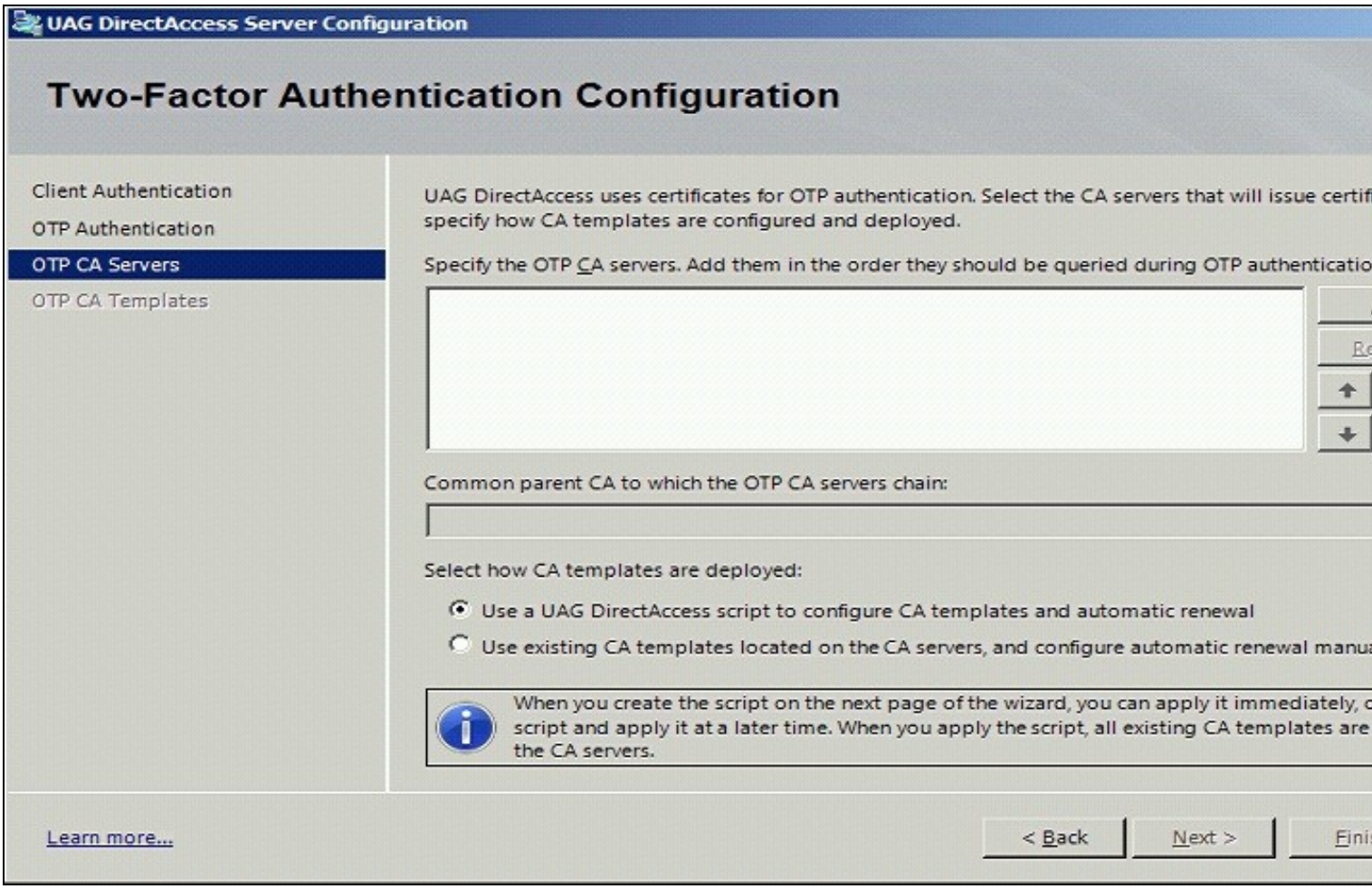


Ensure that the new Swivel server is selected. Optionally select *Require OTP user names to match Active Directory user names with this setting enabled, users log on in UPN format (username@domain).* then the user name will be automatically populated at the direct access login.

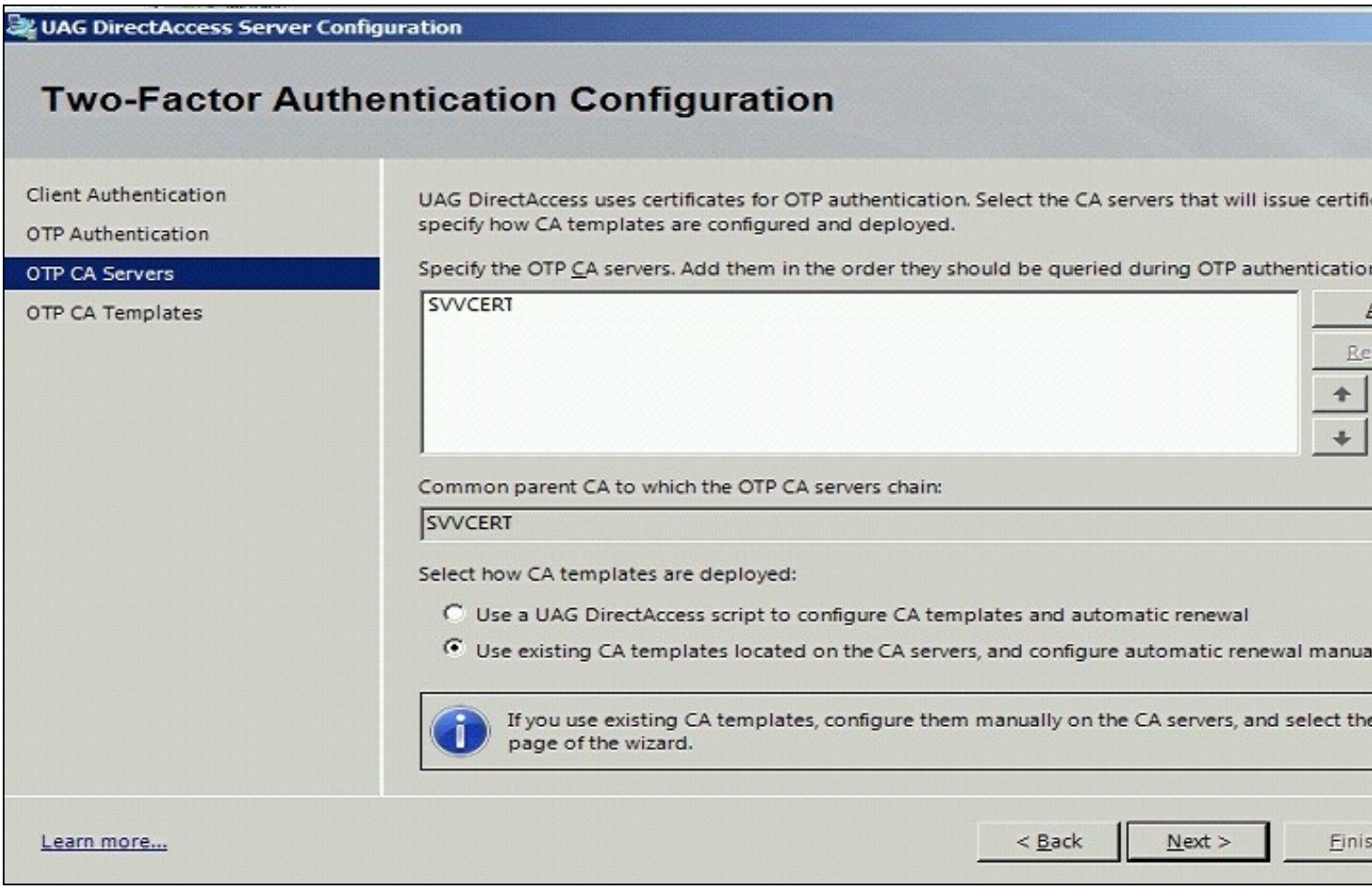


CA Server Configuration

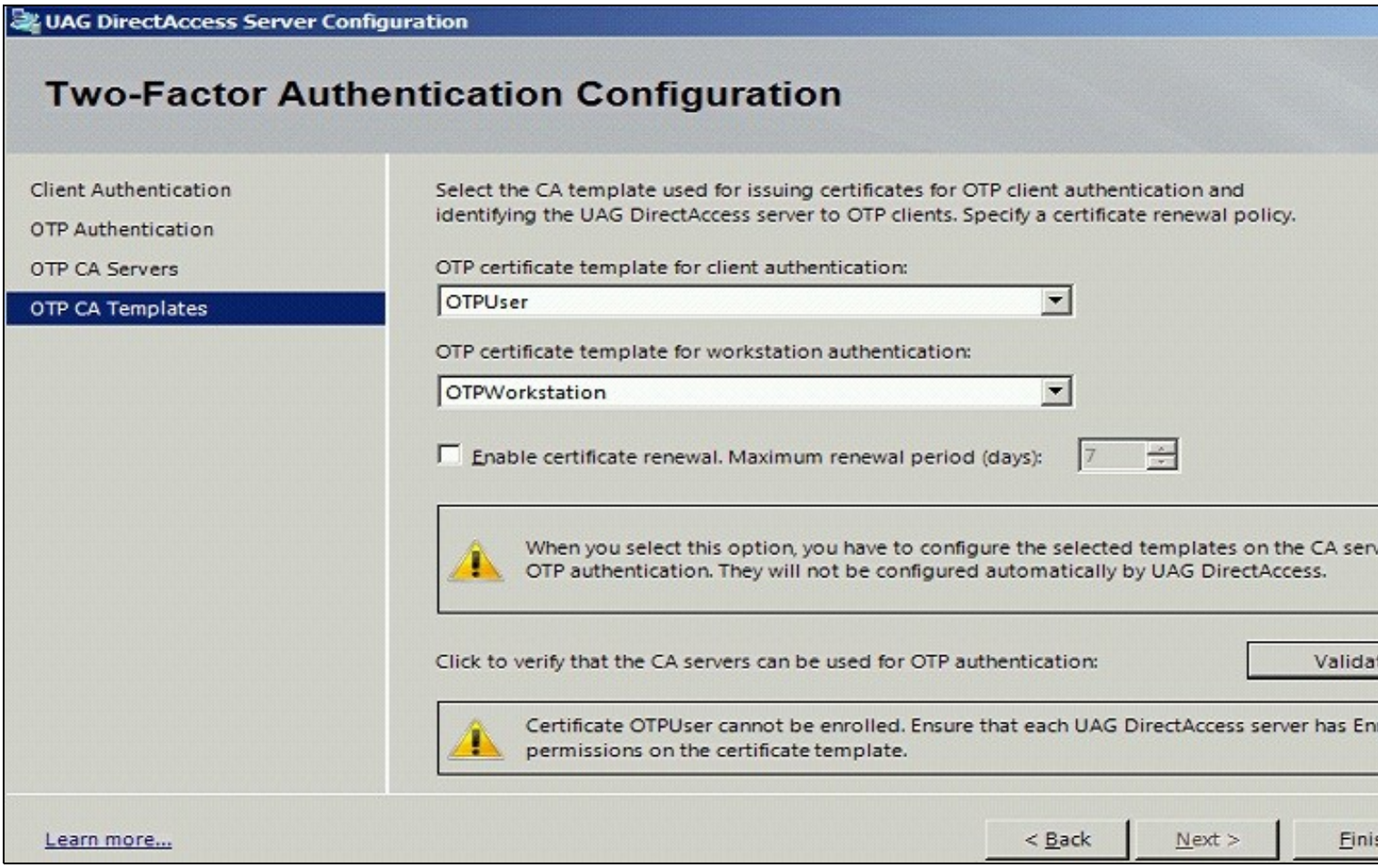
Under OTP CA Servers click on Add and select the OTP CA Server.



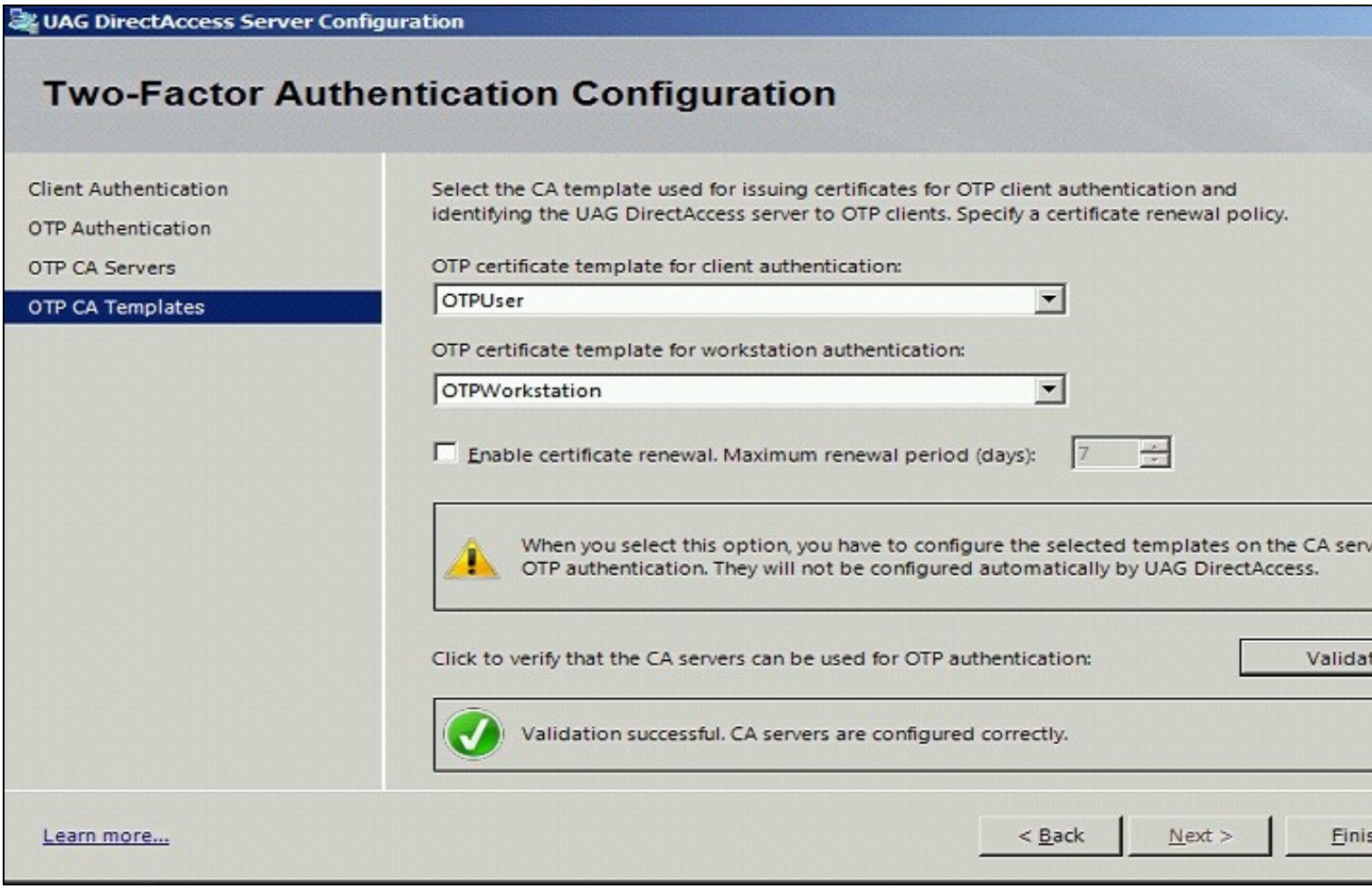
This example is configured to use existing CA templates.



Select the required templates



Validate the CA templates



Additional Installation Options

Verifying the Installation

Access with the Direct Access client entering username, AD password and One Time Code. If the option to *Require OTP user names to match Active Directory user names* then the user name will be automatically populated.

Check the UAG and PINsafe logs for authentication messages.

Uninstalling the PINsafe Integration

Troubleshooting

Known Issues and Limitations

Additional Information

Microsoft DirectAccess