Infoblox
NEXT LEVEL NETWORKING

Deployment Guide

Two-Factor Authentication Deployment Guide

Table of Contents

Introduction *3*

Prerequisites 3

Authentication data flow for 2-factor authentication on the Infoblox appliance: *3*

Setting up 2 factor authentication on NIOS appliances *4*

Introduction

Your enterprise has implemented two-factor authentication for all access to computer systems. In a nutshell, two-factor authentication is something you know and something you have. The ‘something you know’ can be a password. The ‘something you have’ can be a token card or a certificate. A cyber criminal would need both to gain access. Knowing the password is not enough.

You can configure NIOS to use the two-factor authentication method to authenticate users based on X.509 client certificates. In two-factor authentication, NIOS first negotiates SSL/TLS client authentication to validate client certificates. It then authenticates the admins based on the configured authentication policy. You must first configure an authentication policy, and then configure and enable the certificate authentication service for the two-factor authentication to take effect. NIOS uses certificate authentication service as the authentication policy.

Prerequisites

- OCSP (online certificate status protocol) responder.
- Microsoft Active Directory server with Certificate Authority.

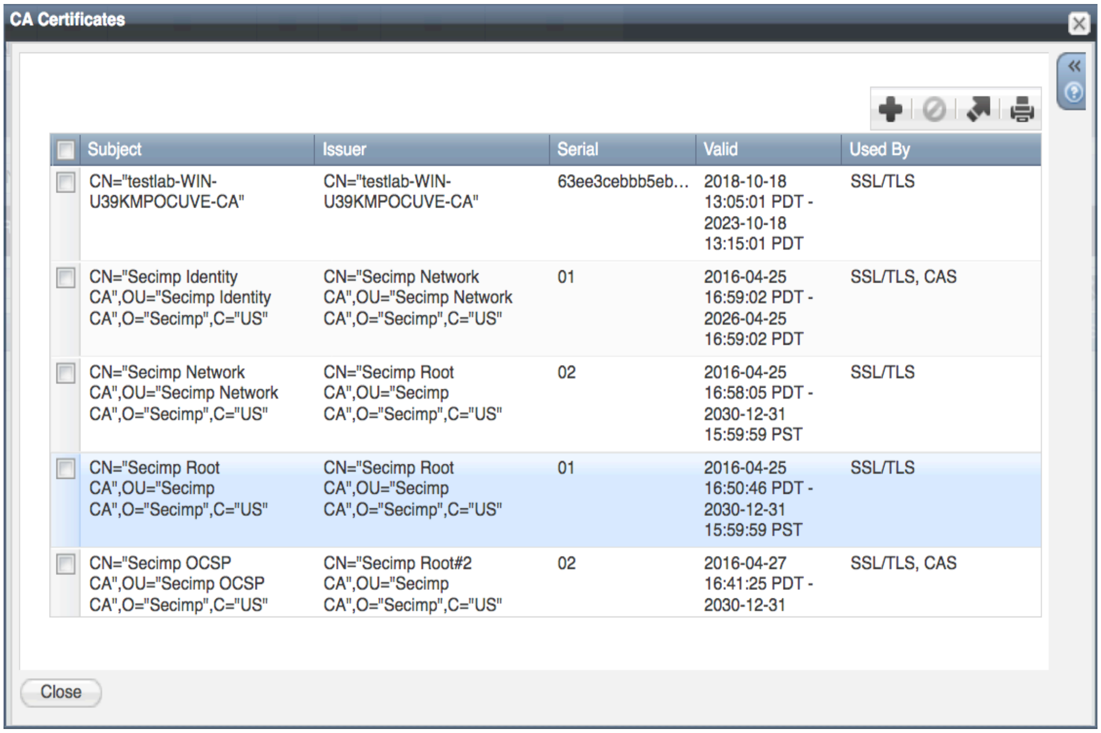
Please consult with your PKI (public key infrastructure) expert on the certificates.

Authentication data flow for 2-factor authentication on the Infoblox appliance:

1. The client workstation issues an HTTPS request to the FQDN or IP address of the Infoblox appliance.
2. The Infoblox appliance sends a certificate request to the client.
3. Optionally, the certificate on the client is sent to the Infoblox appliance.
4. Infoblox appliance then sends the public part of the certicate to the OCSP responder to determine certicate validity.
5. If successful, the Infoblox appliance will generate a nuance (ie random bits of characters) and encrypt that with the public part of the certificate.
6. The Infoblox appliance will send that nuance to the client to decrypt.
7. If the client decrypts the nuance and sends the decrypted nuance back to the Infoblox appliance and is matched up successfully, then that proves the client has the exact public and private key.
8. The Infoblox appliance will use a user group lookup against the Active Directory server.
9. Depending upon the attribute passed in the certificate (ie SAN (subject alternate name) account name or SAN UPN (user principle name) passed to the Active Directory server for authentication.
10. The Infoblox appliance talks with the Active Directory server via a service account.
11. Authentication successful.

Setting up 2 factor authentication on NIOS appliances

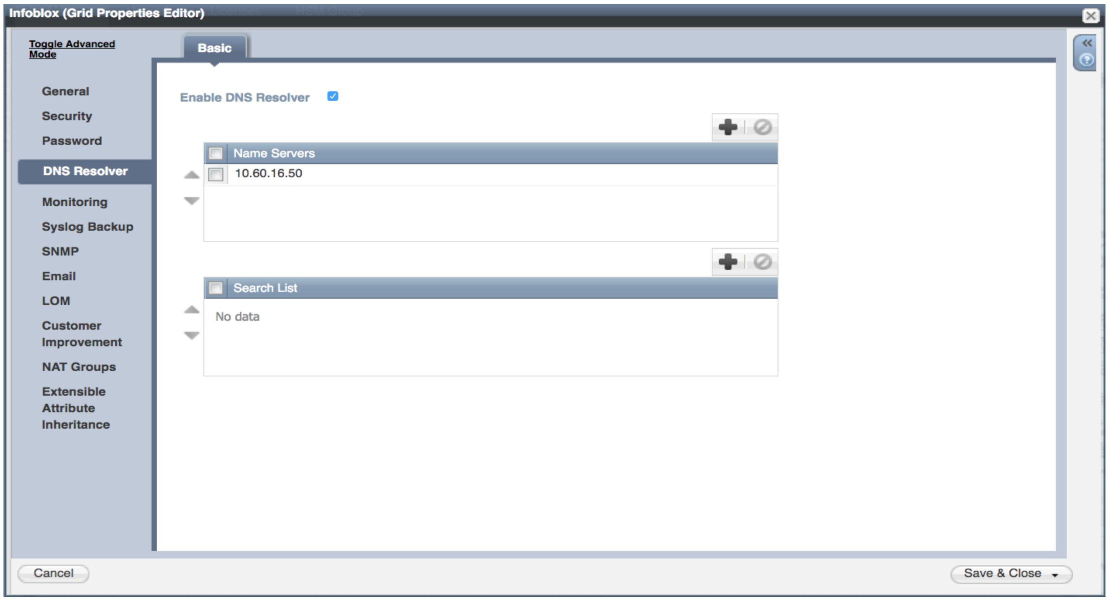
1. Log into the Infoblox GUI.
2. Navigate to Grid → Grid Manager → Toolbar → Certificates → Manage



☐	Subject	Issuer	Serial	Valid	Used By
☐	CN="testlab-WIN-U39KMPOCUVE-CA"	CN="testlab-WIN-U39KMPOCUVE-CA"	63ee3cebbb5eb...	2018-10-18 13:05:01 PDT - 2023-10-18 13:15:01 PDT	SSL/TLS
☐	CN="Secimp Identity CA",OU="Secimp Identity CA",O="Secimp",C="US"	CN="Secimp Network CA",OU="Secimp Network CA",O="Secimp",C="US"	01	2016-04-25 16:59:02 PDT - 2026-04-25 16:59:02 PDT	SSL/TLS, CAS
☐	CN="Secimp Network CA",OU="Secimp Network CA",O="Secimp",C="US"	CN="Secimp Root CA",OU="Secimp CA",O="Secimp",C="US"	02	2016-04-25 16:58:05 PDT - 2030-12-31 15:59:59 PST	SSL/TLS
☐	CN="Secimp Root CA",OU="Secimp CA",O="Secimp",C="US"	CN="Secimp Root CA",OU="Secimp CA",O="Secimp",C="US"	01	2016-04-25 16:50:46 PDT - 2030-12-31 15:59:59 PST	SSL/TLS
☐	CN="Secimp OCSP CA",OU="Secimp OCSP CA",O="Secimp",C="US"	CN="Secimp Root#2 CA",OU="Secimp CA",O="Secimp",C="US"	02	2016-04-27 16:41:25 PDT - 2030-12-31	SSL/TLS, CAS

Certificates.

3. Click on the '+' button to upload the certificates from the Certificate Authority chain.
4. If different from step 3, upload the OCSP CA chain from your OCSP responder.
5. Navigate to Toolbar → Grid Properties → Edit → DNS Resolver.
6. Click on the button to enable DNS resolver.

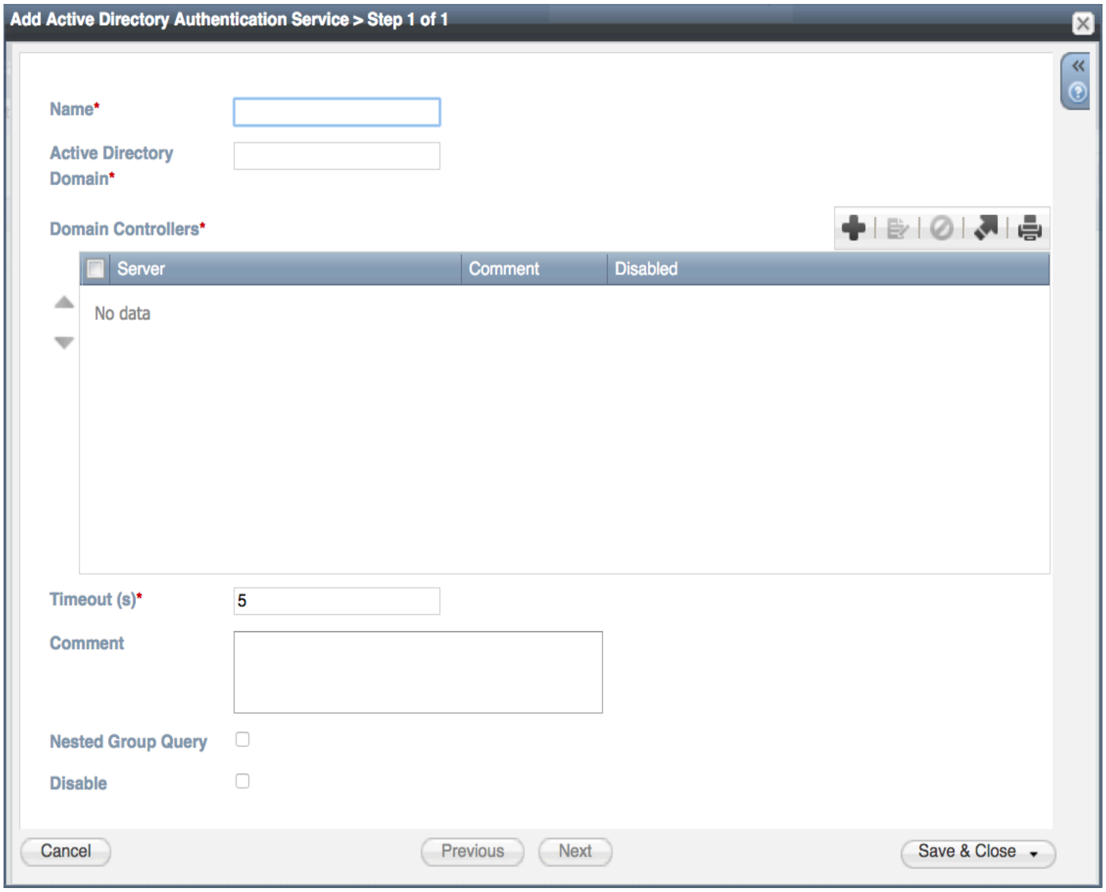


Enable DNS Resolver ☑

☐	Name Servers
☐	10.60.16.50

☐	Search List
	No data

7. Click on the ‘+’ button to add the IP address of the Active Directory server.



Add Active Directory Authentication Service > Step 1 of 1

Name*

Active Directory Domain*

Domain Controllers*

□ Server	Comment	Disabled
No data		

Timeout (s)* 5

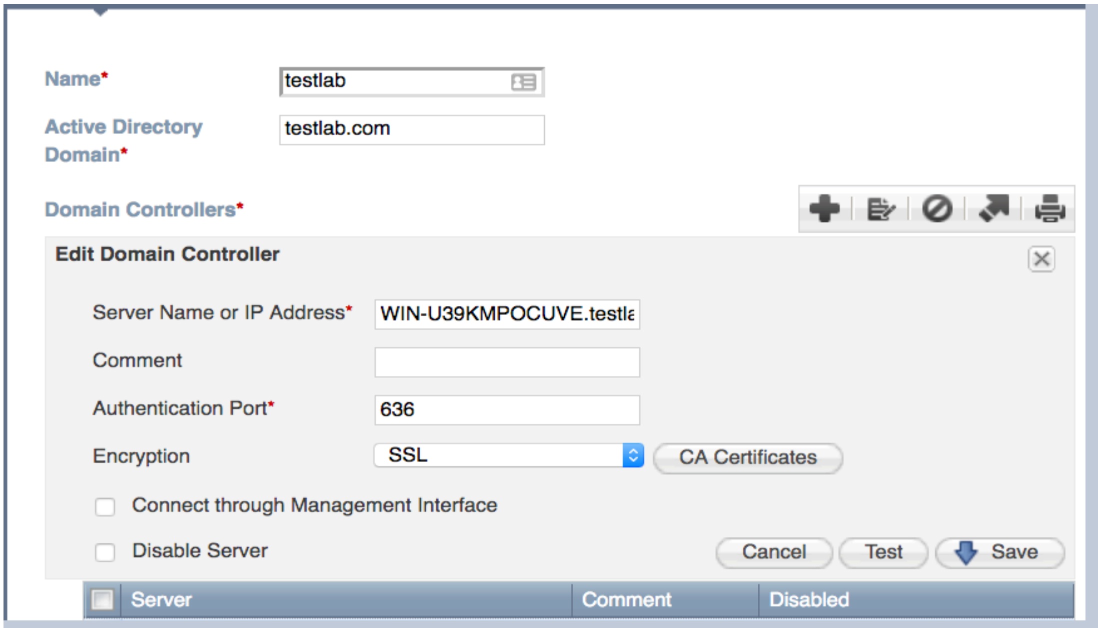
Comment

Nested Group Query □

Disable □

8. Click Save and Close.
9. Navigate Administration → Authentication Server Groups → Active Directory Services.
10. Hit the ‘+’ to add an entry.
11. Enter the name of the Active Directory Service.
12. Enter the name of the Active Directory Domain.

13. In the domain controllers section, click on the + button to add a server. Use the fully qualified domain name of the server.



Name* testlab

Active Directory Domain* testlab.com

Domain Controllers*

Edit Domain Controller

Server Name or IP Address* WIN-U39KMPOCUVE.testla

Comment

Authentication Port* 636

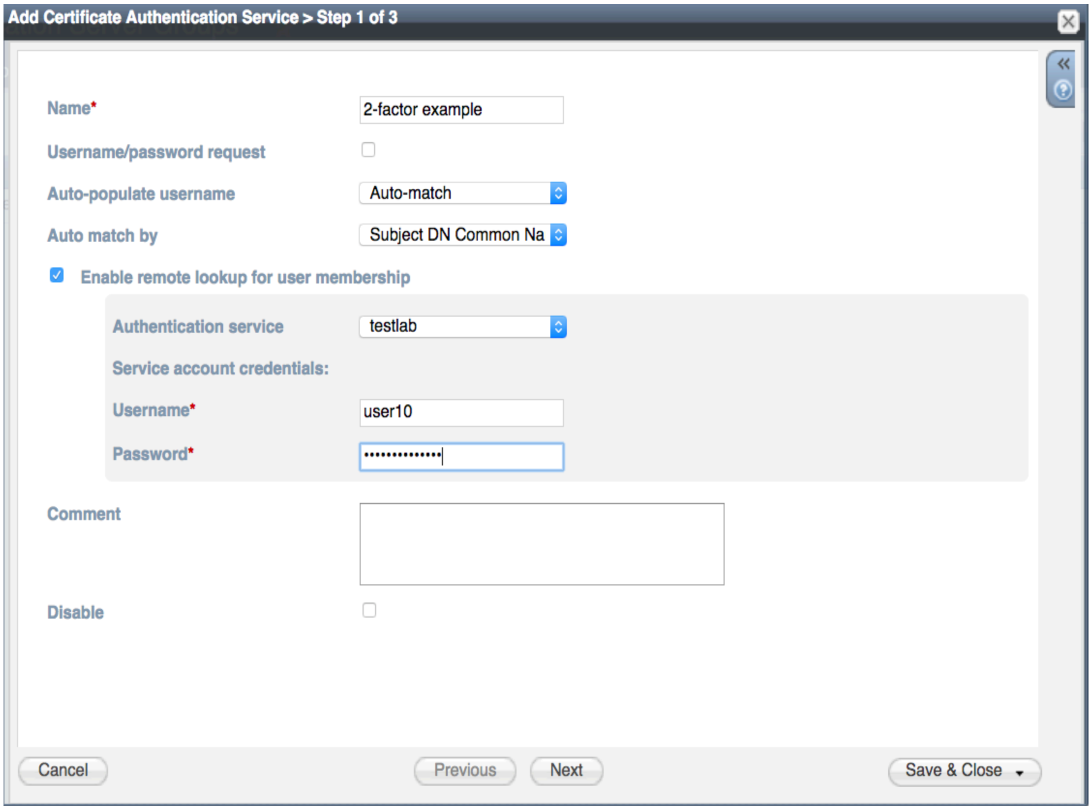
Encryption SSL

□ Connect through Management Interface

□ Disable Server

□ Server	Comment	Disabled

14. Change the encryption to SSL.
15. Click on the ‘test’ button. If it is successful, click on the ‘add’ button.
16. Click ‘Save and Close’.
17. Navigate to Certificate Authentication Services.
18. Click on the ‘+’ button to a Certificate Authentication Service.



Add Certificate Authentication Service > Step 1 of 3

Name* 2-factor example

Username/password request □

Auto-populate username Auto-match

Auto match by Subject DN Common Na

☑ Enable remote lookup for user membership

Authentication service testlab

Service account credentials:

Username* user10

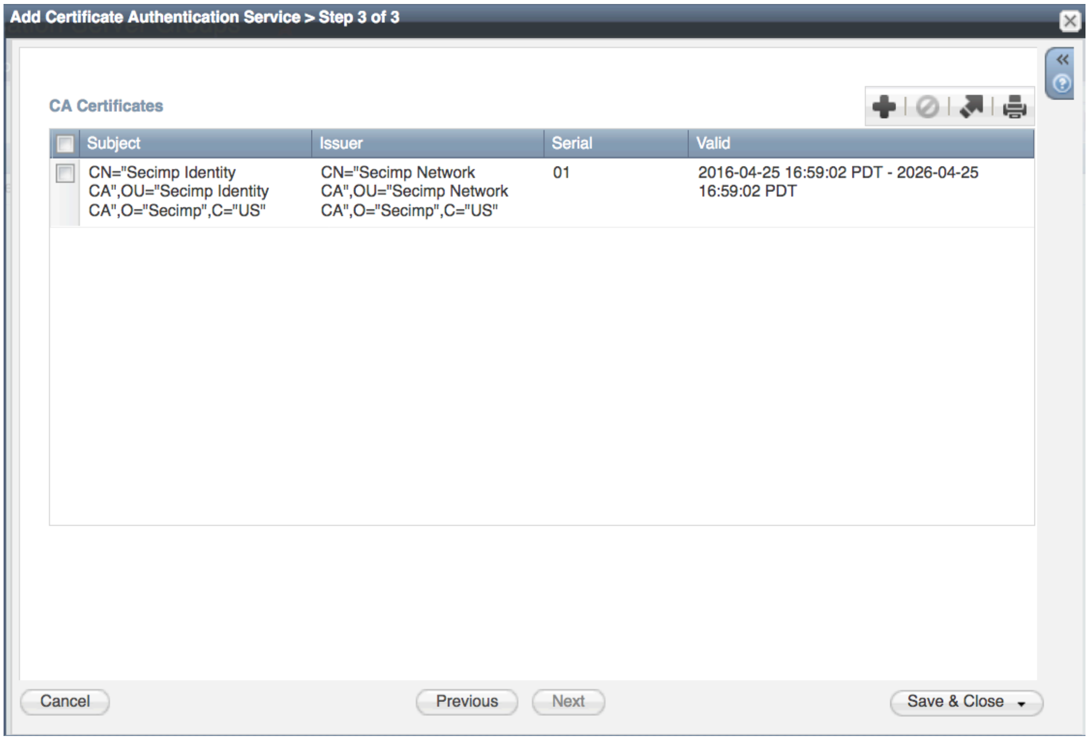
Password* ••••••••••••••

Comment

Disable □

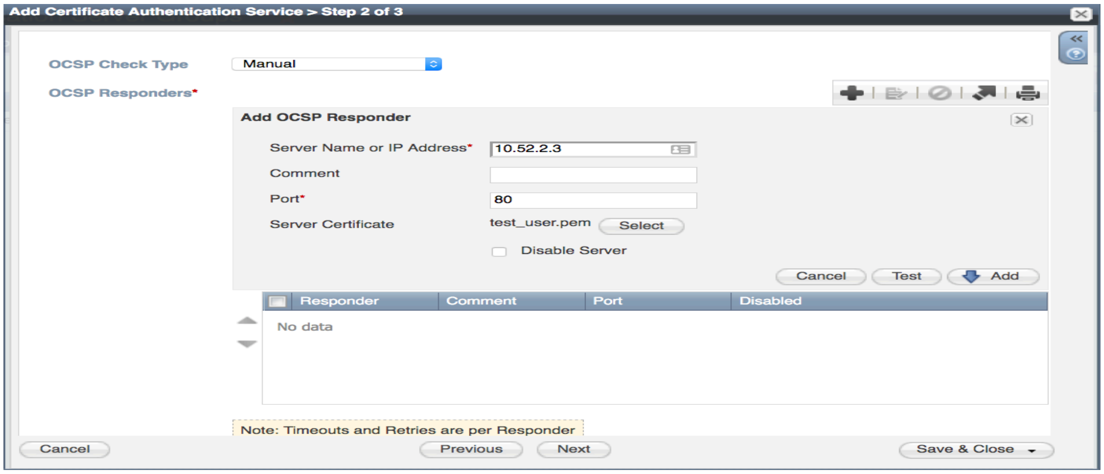
19. Add a name for the service.

20. Uncheck Username/password request.
21. Click on the button to Enable remote lookup for user membership.



☐	Subject	Issuer	Serial	Valid
☐	CN="Secimp Identity CA",OU="Secimp Identity CA",O="Secimp",C="US"	CN="Secimp Network CA",OU="Secimp Network CA",O="Secimp",C="US"	01	2016-04-25 16:59:02 PDT - 2026-04-25 16:59:02 PDT

22. In Authentication service, add the name of the active directory service.
23. Add the username that was created in AD server for the Infoblox appliance to log into the AD server.
24. Click on Next.
25. Click on the ‘+’ button to add and an OSCP responder ip address.



OCSP Check Type: Manual

OCSP Responders*

Server Name or IP Address*: 10.52.2.3

Comment:

Port*: 80

Server Certificate: test_user.pem

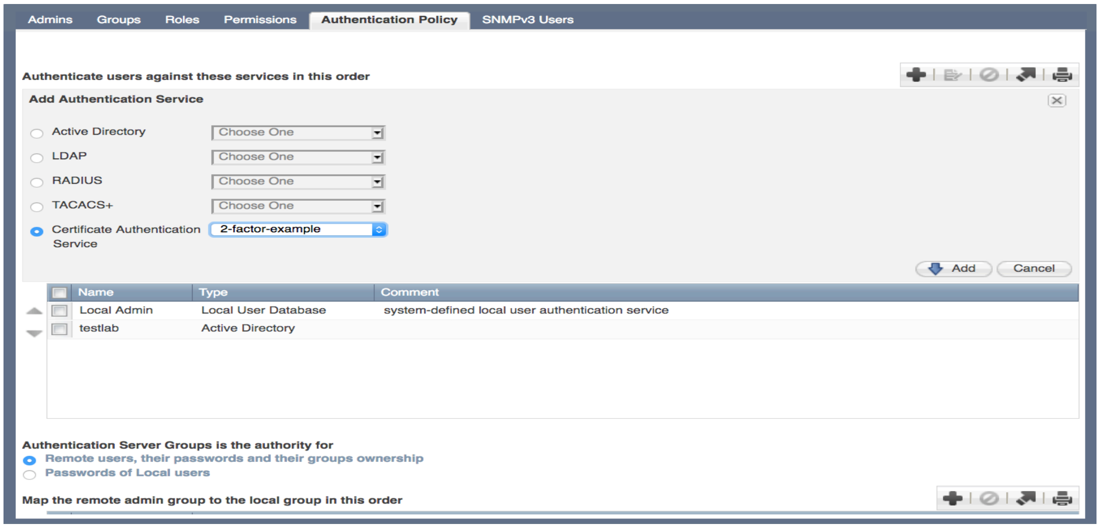
☐ Disable Server

☐	Responder	Comment	Port	Disabled

Note: Timeouts and Retries are per Responder

26. Enter the port number that was configured on the OCSP server. This port number would come from your PKI (public key infrastructure) expert.
27. Add the certificate for the OCSP server if you want to use the test button.
28. Click on the test button.
29. If successful, click Add.
30. Click Next.
31. Click on the ‘+’ button to add the CA certificates from the certificate store that will used to authenticate users.

32. Click save and close.
33. Navigate to Administration → Administrators → Authentication Policy.
34. Click on the '+' on Authenticate users section.



Authenticate users against these services in this order

Add Authentication Service

○ Active Directory — Choose One
○ LDAP — Choose One
○ RADIUS — Choose One
○ TACACS+ — Choose One
● Certificate Authentication Service — 2-factor-example

□	Name	Type	Comment
□	Local Admin	Local User Database	system-defined local user authentication service
□	testlab	Active Directory	

Authentication Server Groups is the authority for
● Remote users, their passwords and their groups ownership
○ Passwords of Local users

Map the remote admin group to the local group in this order

35. Click on the Certificate Authentication Service button.
36. Choose the Authentication Server Group that was created before.
37. Click the Add button.
38. You should get a message stating 2-factor authentication enabled.

Note: The last thing that needs to be done is to install your certificate onto your browser. Please consult your PKI expert to install certificates onto your browser.

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com