Infoblox

Deployment Guide

NetMRI Certificate Authentication with CAC/PIV

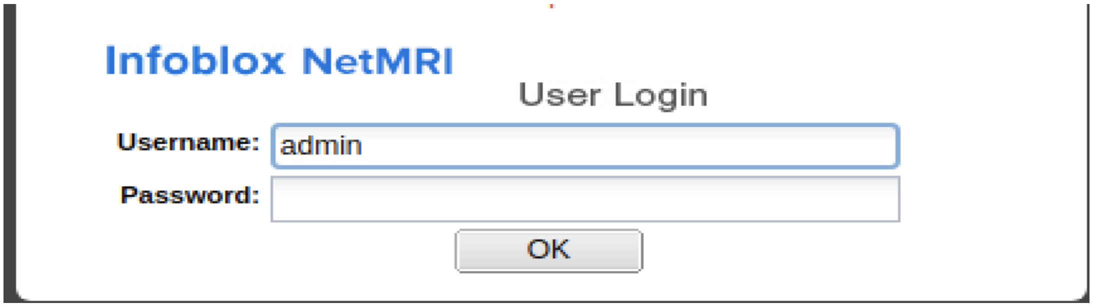
Table of Contents

Requirements

- Working CAC/PIV (common access card/personal identity verification) or Certificate Authority infrastructure.
- Client machine and browser already configured for your client certificate.
- Existing and functional NetMRI appliance.
- Your Certificate Authority chain's public certificates.
- OCSP(online certificate status protocol) Responder's operating at the web root.
- AIA (authority information access) Information does not need to be followed to obtain the OCSP response.
- A user created where the CN or common name is the username and assigned to the appropriate role.

Deployment Instructions

1. Log into the NetMRI GUI. Enter your default username of admin and password of infoblox.



Infoblox NetMRI

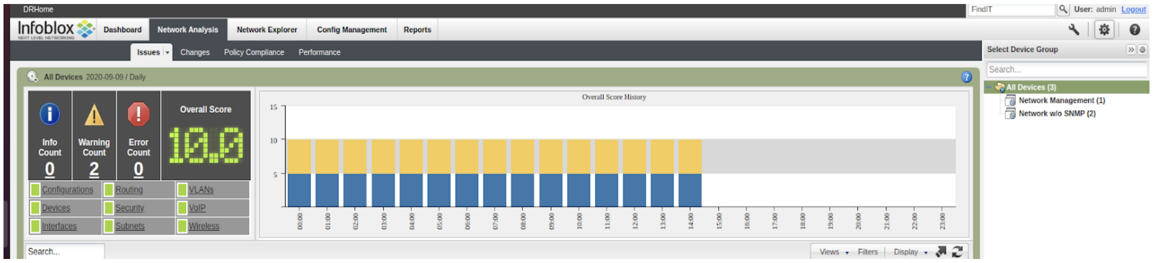
User Login

Username: admin

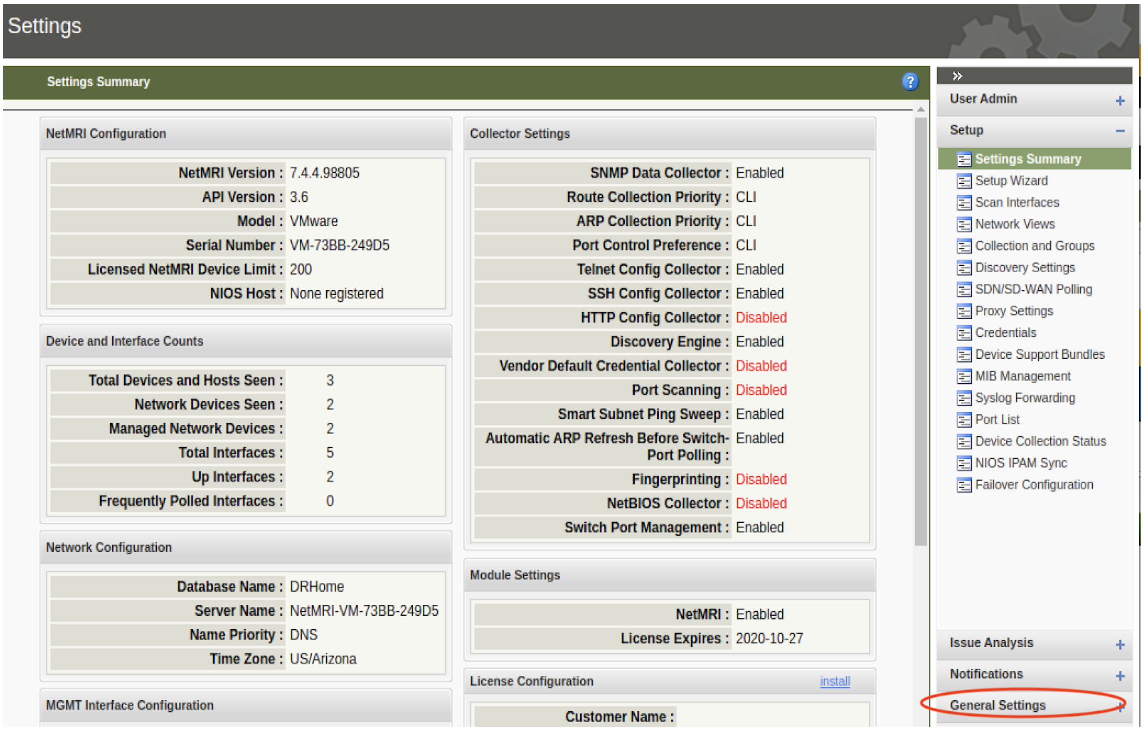
Password:

OK

2. The following screen will appear. To set up certificate authentication click on the wheel icon in the upper right corner of the screen.



3. Click on the ‘General Settings’ tab on the right.



Settings

Settings Summary

NetMRI Configuration

NetMRI Version :	7.4.4.98805
API Version :	3.6
Model :	VMware
Serial Number :	VM-73BB-249D5
Licensed NetMRI Device Limit :	200
NIOS Host :	None registered

Device and Interface Counts

Total Devices and Hosts Seen :	3
Network Devices Seen :	2
Managed Network Devices :	2
Total Interfaces :	5
Up Interfaces :	2
Frequently Polled Interfaces :	0

Network Configuration

Database Name :	DRHome
Server Name :	NetMRI-VM-73BB-249D5
Name Priority :	DNS
Time Zone :	US/Arizona

MGMT Interface Configuration

Collector Settings

SNMP Data Collector :	Enabled
Route Collection Priority :	CLI
ARP Collection Priority :	CLI
Port Control Preference :	CLI
Telnet Config Collector :	Enabled
SSH Config Collector :	Enabled
HTTP Config Collector :	Disabled
Discovery Engine :	Enabled
Vendor Default Credential Collector :	Disabled
Port Scanning :	Disabled
Smart Subnet Ping Sweep :	Enabled
Automatic ARP Refresh Before Switch-Port Polling :	Enabled
Fingerprinting :	Disabled
NetBIOS Collector :	Disabled
Switch Port Management :	Enabled

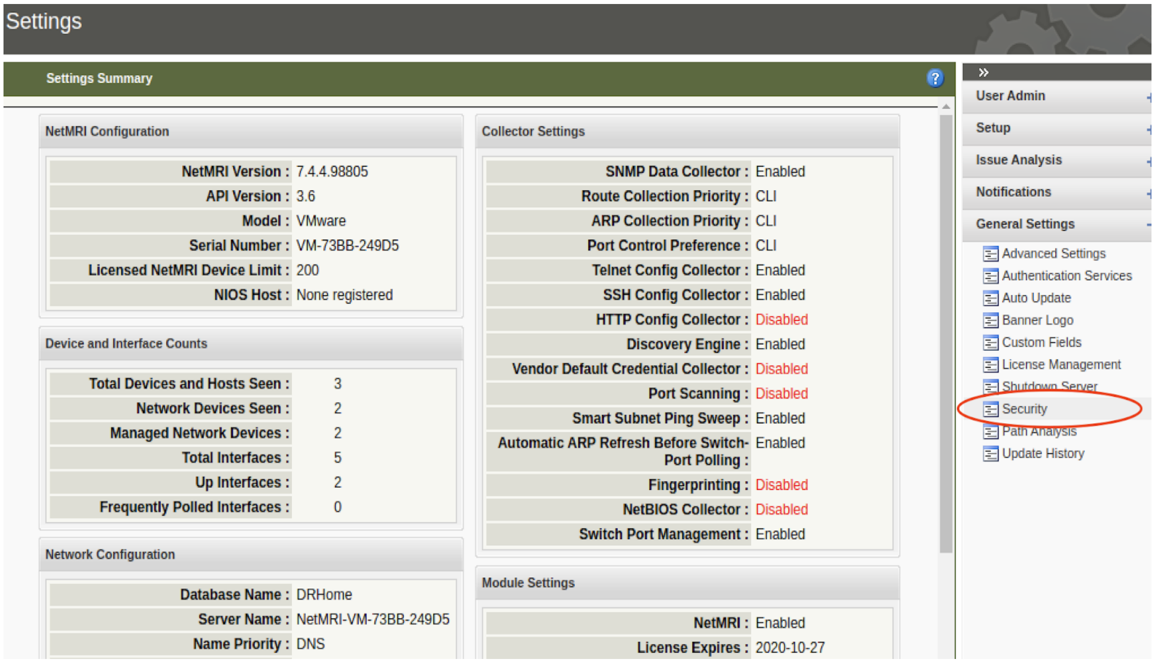
Module Settings

NetMRI :	Enabled
License Expires :	2020-10-27

License Configuration

Customer Name :	

4. Click on the ‘Security’ tab.



Settings

Settings Summary

NetMRI Configuration

NetMRI Version :	7.4.4.98805
API Version :	3.6
Model :	VMware
Serial Number :	VM-73BB-249D5
Licensed NetMRI Device Limit :	200
NIOS Host :	None registered

Device and Interface Counts

Total Devices and Hosts Seen :	3
Network Devices Seen :	2
Managed Network Devices :	2
Total Interfaces :	5
Up Interfaces :	2
Frequently Polled Interfaces :	0

Network Configuration

Database Name :	DRHome
Server Name :	NetMRI-VM-73BB-249D5
Name Priority :	DNS

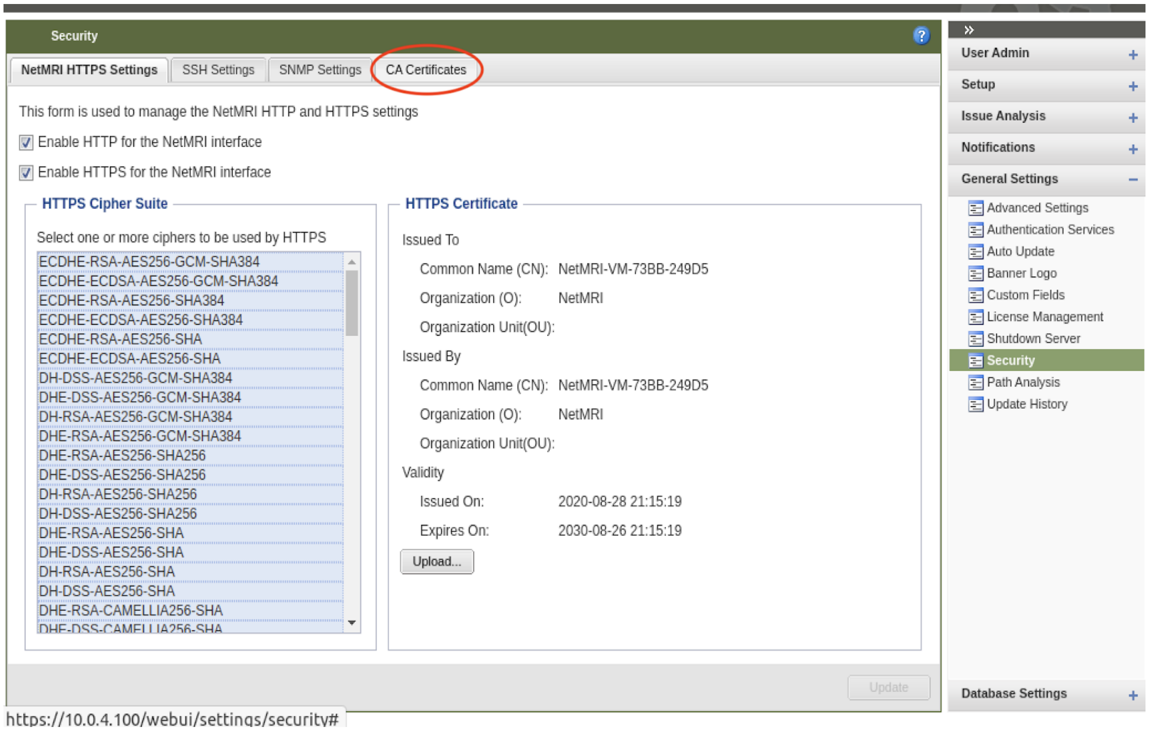
Collector Settings

SNMP Data Collector :	Enabled
Route Collection Priority :	CLI
ARP Collection Priority :	CLI
Port Control Preference :	CLI
Telnet Config Collector :	Enabled
SSH Config Collector :	Enabled
HTTP Config Collector :	Disabled
Discovery Engine :	Enabled
Vendor Default Credential Collector :	Disabled
Port Scanning :	Disabled
Smart Subnet Ping Sweep :	Enabled
Automatic ARP Refresh Before Switch-Port Polling :	Enabled
Fingerprinting :	Disabled
NetBIOS Collector :	Disabled
Switch Port Management :	Enabled

Module Settings

NetMRI :	Enabled
License Expires :	2020-10-27

5. Select the ‘CA Certificate’ tab.



This form is used to manage the NetMRI HTTP and HTTPS settings

☑ Enable HTTP for the NetMRI interface

☑ Enable HTTPS for the NetMRI interface

HTTPS Cipher Suite

Select one or more ciphers to be used by HTTPS

ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA
DH-DSS-AES256-GCM-SHA384
DHE-DSS-AES256-GCM-SHA384
DH-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
DHE-DSS-AES256-SHA256
DH-RSA-AES256-SHA256
DH-DSS-AES256-SHA256
DHE-RSA-AES256-SHA
DHE-DSS-AES256-SHA
DH-RSA-AES256-SHA
DH-DSS-AES256-SHA
DHE-RSA-CAMELLIA256-SHA
DHE-DSS-CAMELLIA256-SHA

HTTPS Certificate

Issued To

Common Name (CN):	NetMRI-VM-73BB-249D5
Organization (O):	NetMRI
Organization Unit(OU):	

Issued By

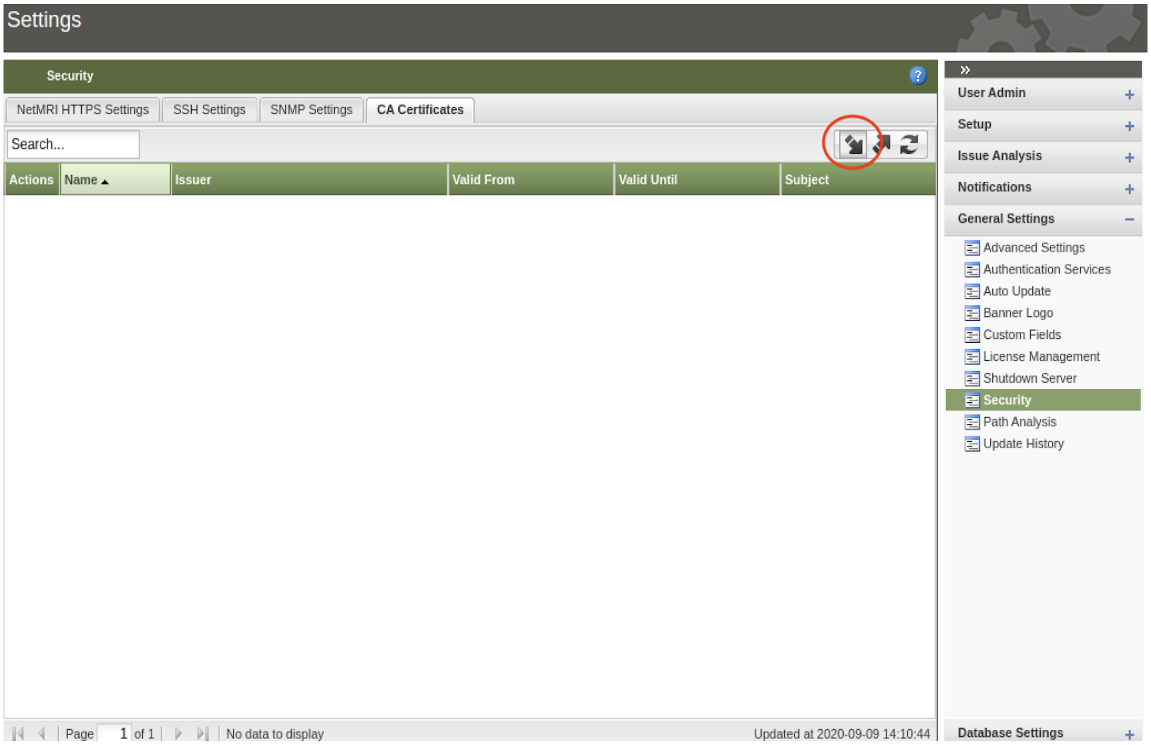
Common Name (CN):	NetMRI-VM-73BB-249D5
Organization (O):	NetMRI
Organization Unit(OU):	

Validity

Issued On:	2020-08-28 21:15:19
Expires On:	2030-08-26 21:15:19

https://10.0.4.100/webui/settings/security#

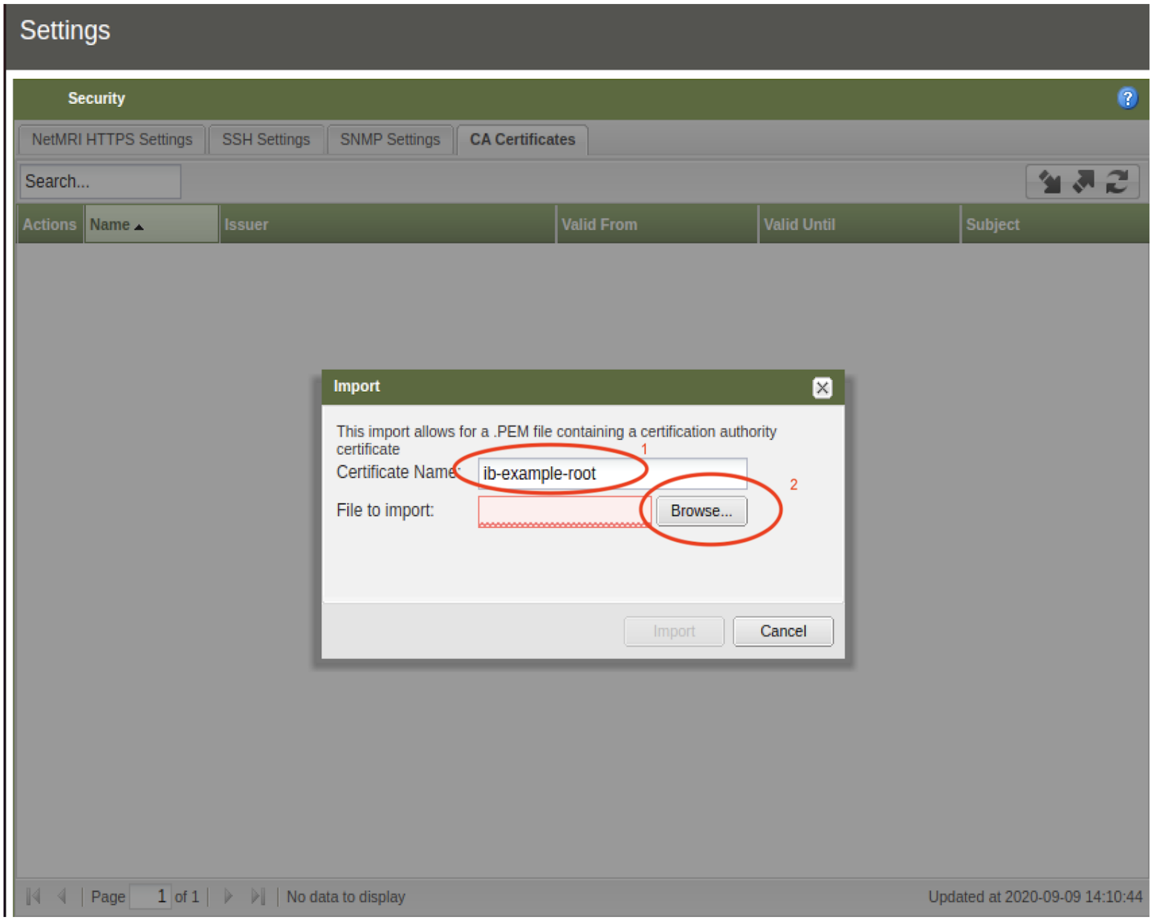
6. Select the ‘Import’ button to import the certificates.



Actions	Name ▲	Issuer	Valid From	Valid Until	Subject

Page 1 of 1 | No data to display | Updated at 2020-09-09 14:10:44

7. Input the root certificate. Type the certificate name and then browse for the file on your computer. The certificate name is only local to NetMRI. Click Import.



This import allows for a .PEM file containing a certification authority certificate

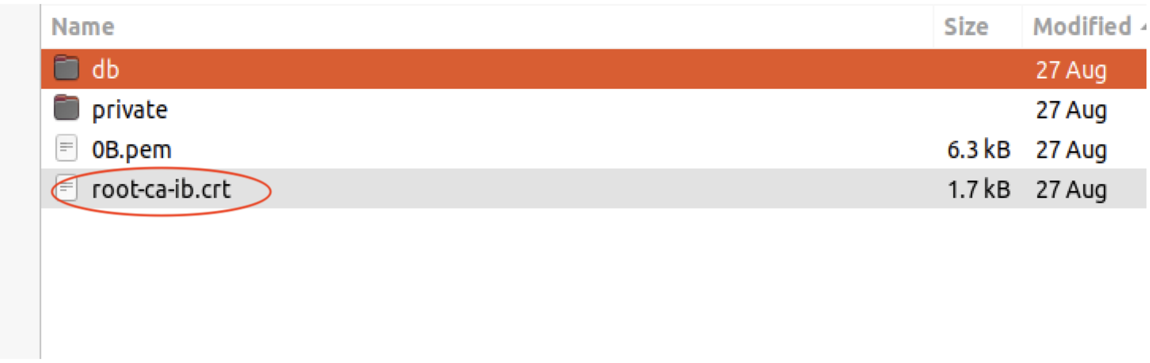
Certificate Name: ib-example-root

File to import:

Page 1 of 1 | No data to display

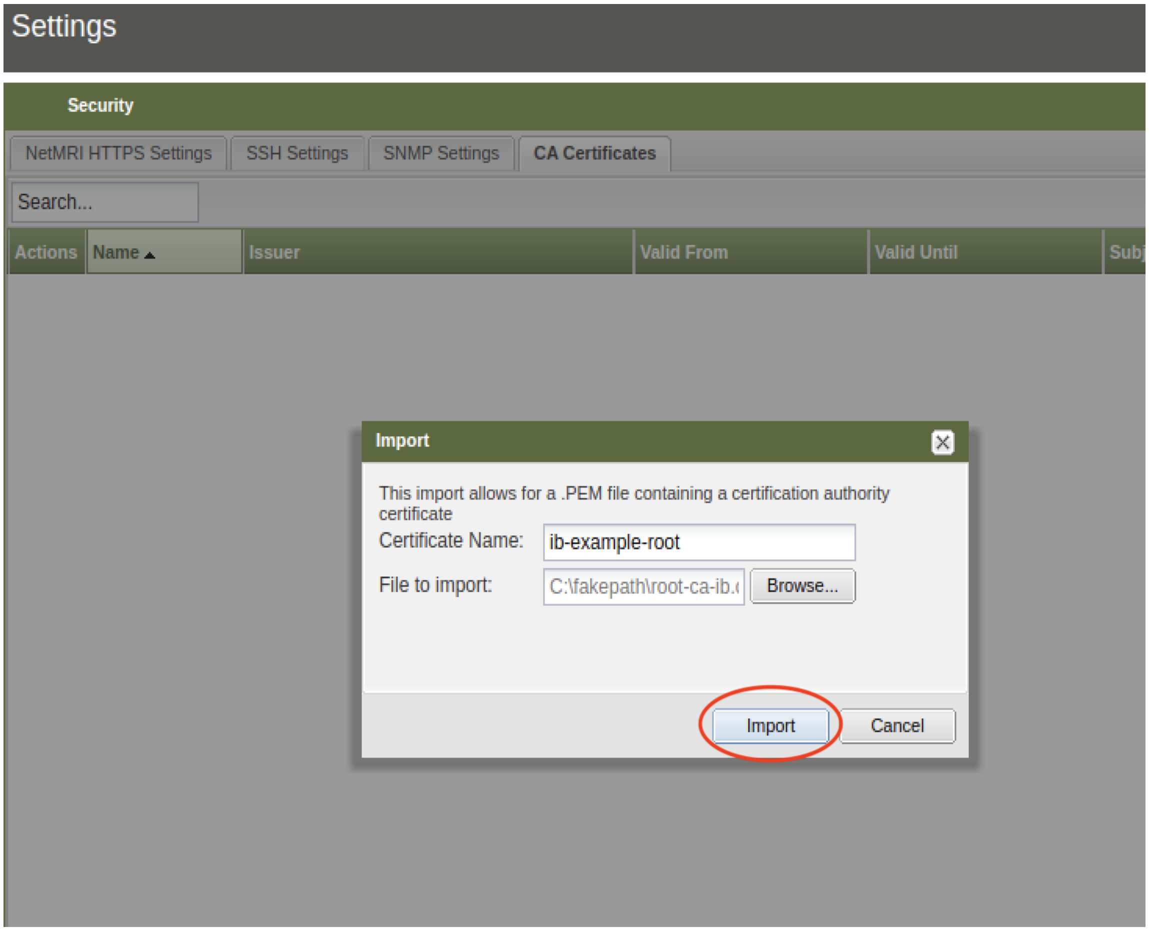
Updated at 2020-09-09 14:10:44

8. Here is an example of the root certificate.



Name	Size	Modified
db		27 Aug
private		27 Aug
0B.pem	6.3 kB	27 Aug
root-ca-ib.crt	1.7 kB	27 Aug

9. Once you have selected the proper certificate file from your hard drive, click import.

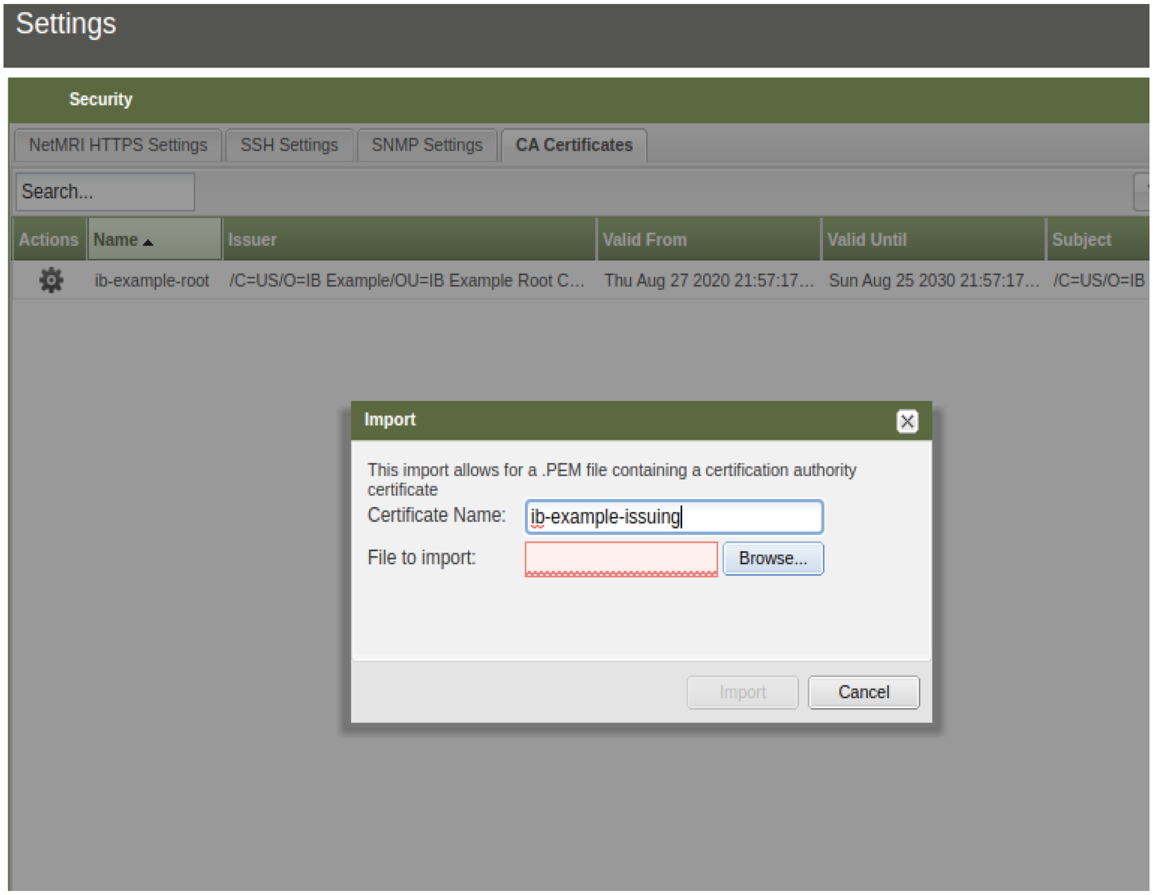


This import allows for a .PEM file containing a certification authority certificate

Certificate Name: ib-example-root

File to import: C:\fakepath\root-ca-ib.(

10. Add the issuing certificate.



Actions	Name ▲	Issuer	Valid From	Valid Until	Subject
⚙	ib-example-root	/C=US/O=IB Example/OU=IB Example Root C...	Thu Aug 27 2020 21:57:17...	Sun Aug 25 2030 21:57:17...	/C=US/O=IB

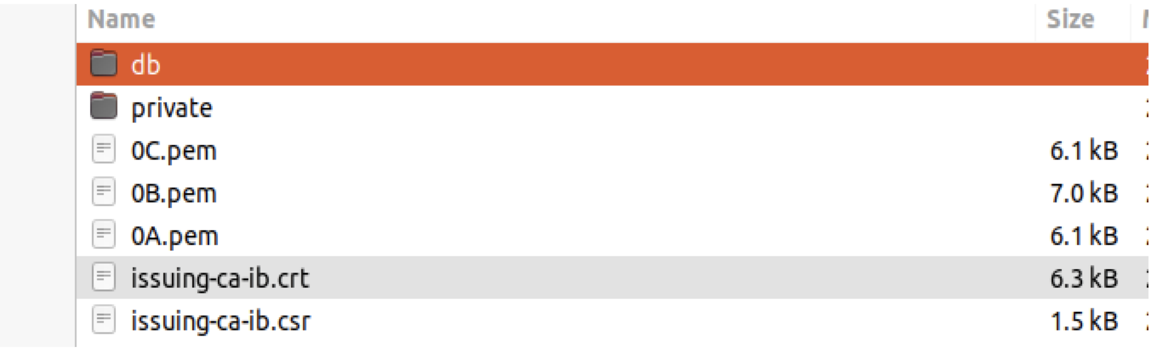
Import

This import allows for a .PEM file containing a certification authority certificate

Certificate Name: ib-example-issuing

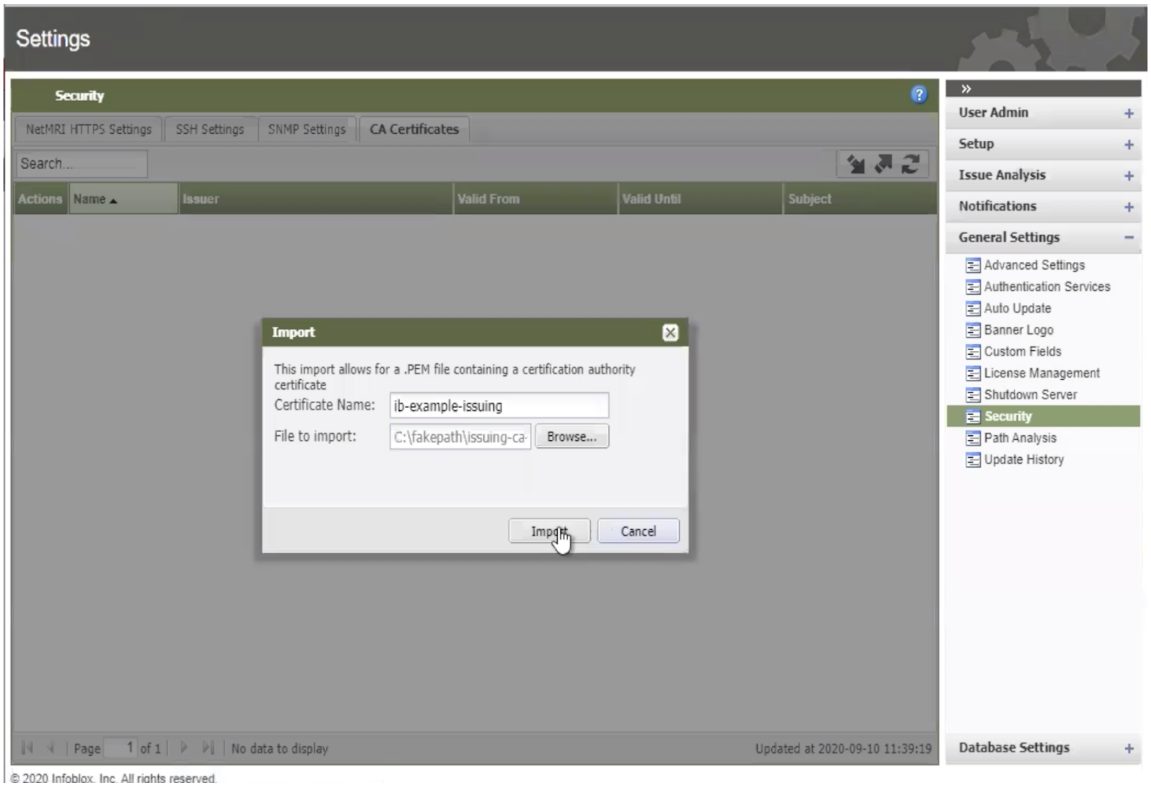
File to import:

11. Select the certificate.



Name	Size
db	
private	
0C.pem	6.1 kB
0B.pem	7.0 kB
0A.pem	6.1 kB
issuing-ca-ib.crt	6.3 kB
issuing-ca-ib.csr	1.5 kB

12. Once you have selected the proper certificate file from your hard drive, click import.



This import allows for a .PEM file containing a certification authority certificate

Certificate Name: ib-example-issuing

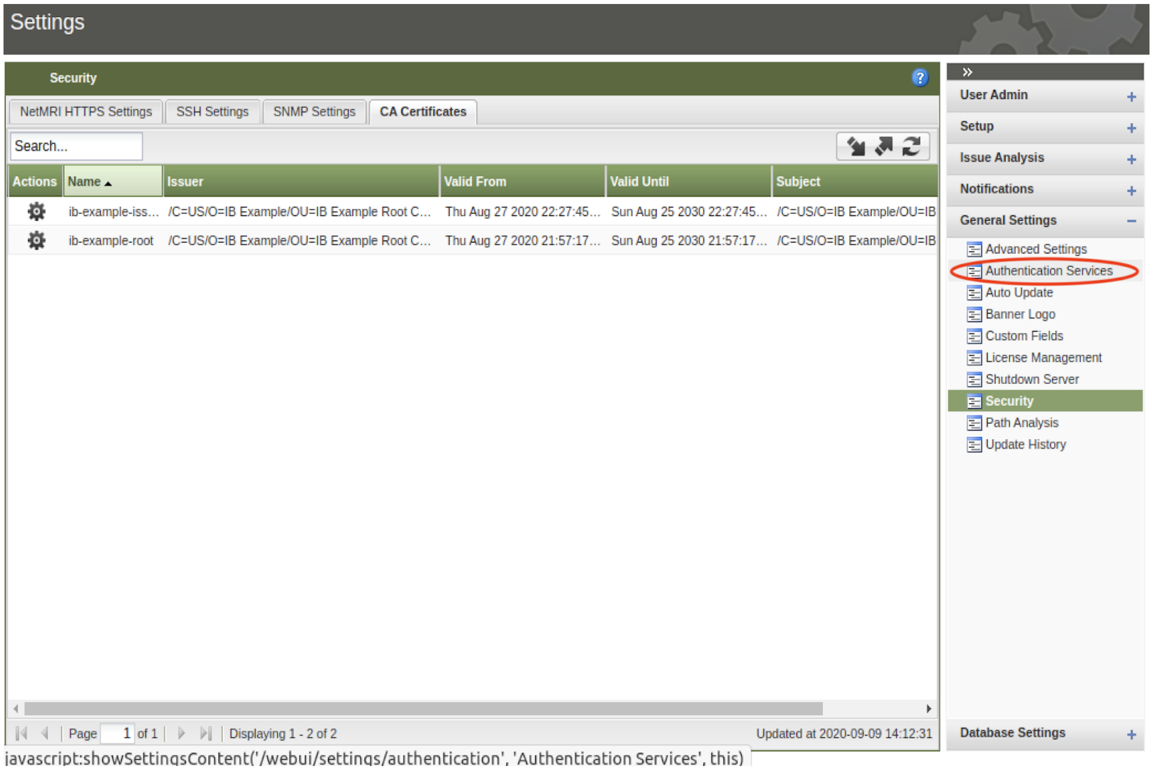
File to import: C:\fakepath\issuing-ca

Page 1 of 1 | No data to display

Updated at 2020-09-10 11:39:19

© 2020 Infoblox. Inc. All riahts reserved.

13. Repeat steps 10-12 for each certificate in your CA chain for your users and the OCSP Responder if they are different CA infrastructures.
14. Click on the Authentication Services tab where you will to add the OCSP responder.



Settings

Security

NetMRI HTTPS Settings | SSH Settings | SNMP Settings | CA Certificates

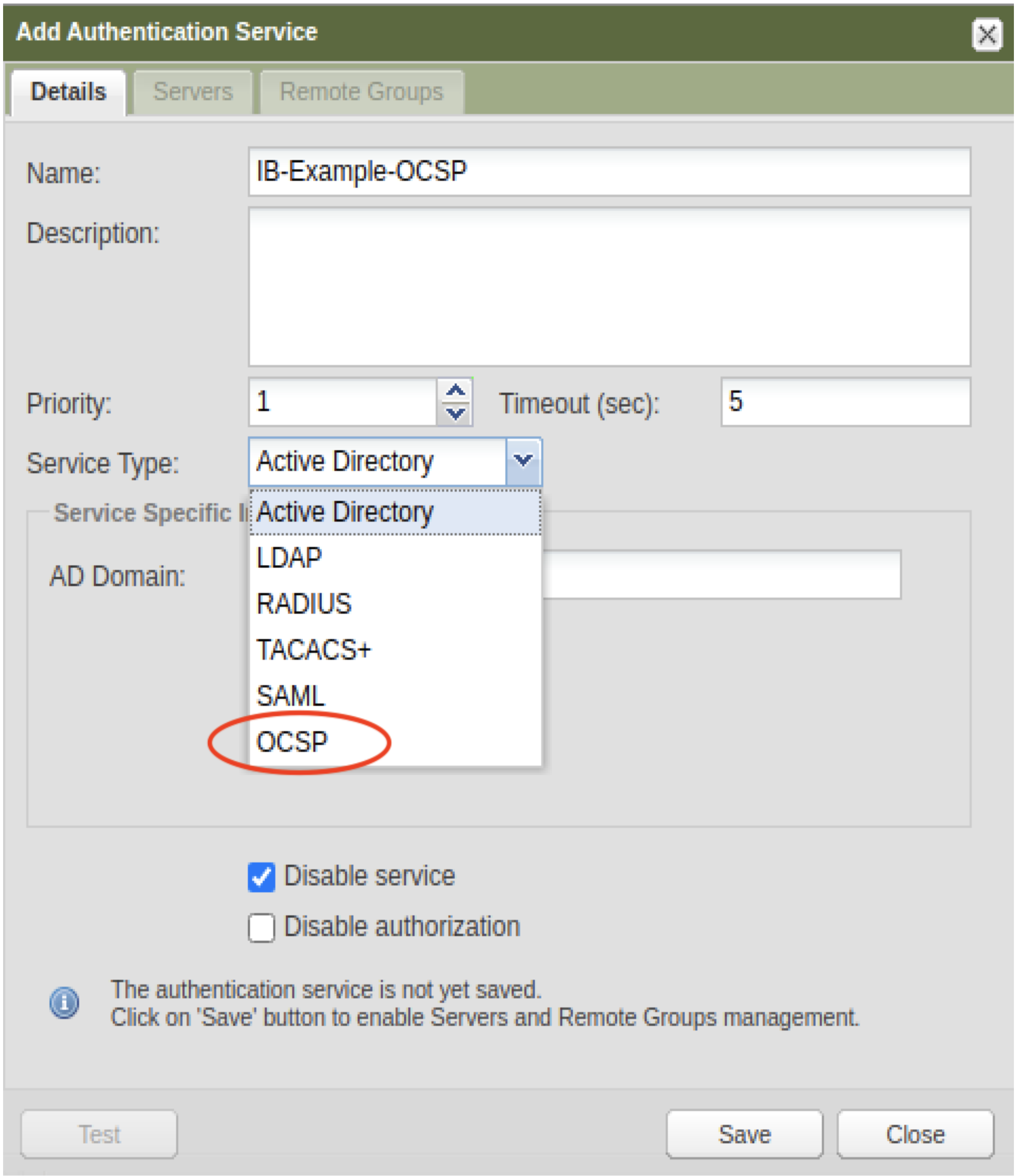
Search...

Actions	Name ▲	Issuer	Valid From	Valid Until	Subject
⚙	ib-example-iss…	/C=US/O=IB Example/OU=IB Example Root C…	Thu Aug 27 2020 22:27:45…	Sun Aug 25 2030 22:27:45…	/C=US/O=IB Example/OU=IB
⚙	ib-example-root	/C=US/O=IB Example/OU=IB Example Root C…	Thu Aug 27 2020 21:57:17…	Sun Aug 25 2030 21:57:17…	/C=US/O=IB Example/OU=IB

Page 1 of 1 | Displaying 1 - 2 of 2 | Updated at 2020-09-09 14:12:31

javascript:showSettingsContent('/webui/settings/authentication', 'Authentication Services', this)

15. Click on the ‘Details’ tab. Add the name of the OCSP responder. On the ‘Service Type’ drop down menu, select ‘OCSP’. Ensure the ‘Disable Service’ check box is checked.



Add Authentication Service

Name: IB-Example-OCSP

Description:

Priority: 1

Timeout (sec): 5

Service Type: Active Directory

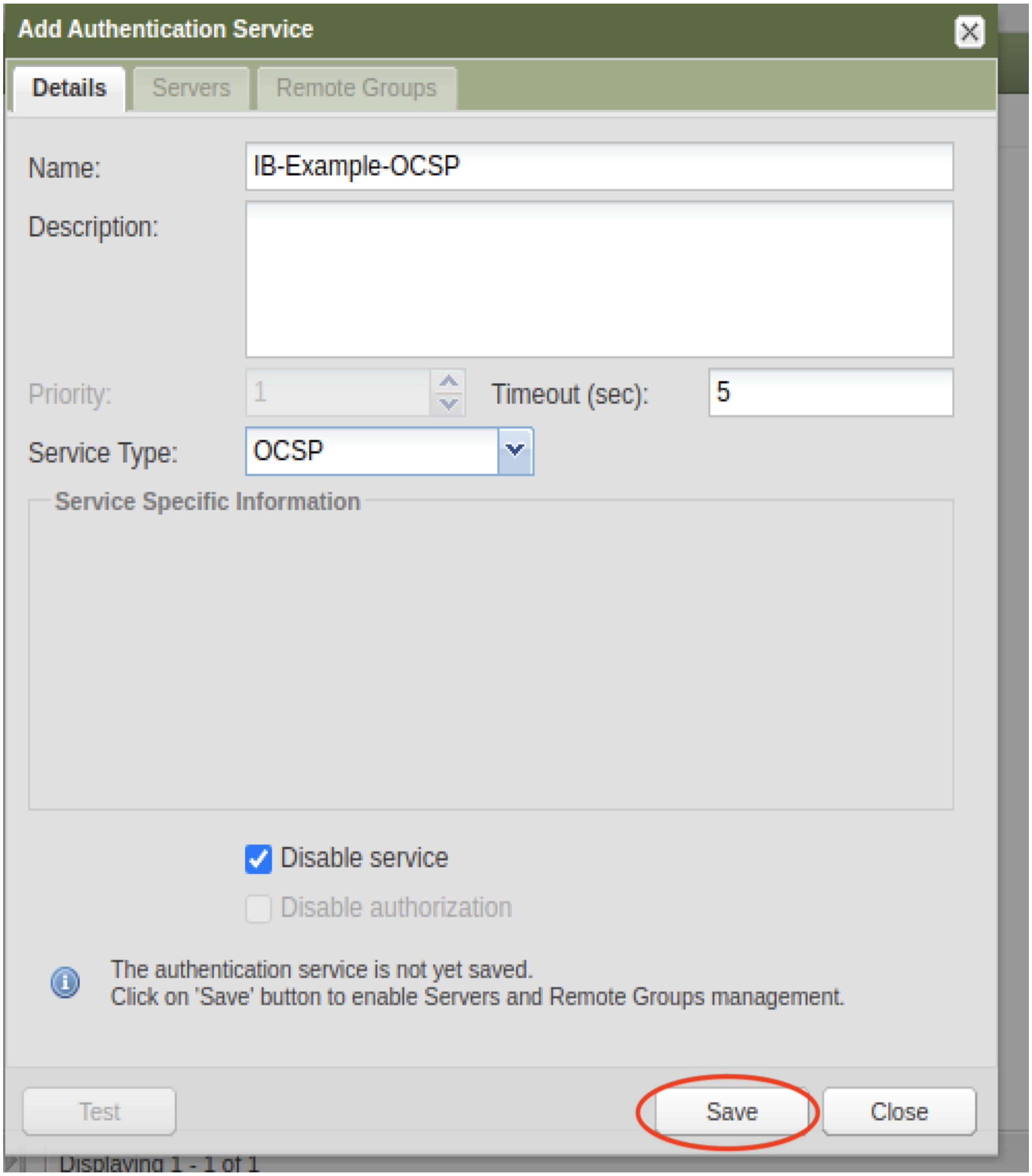
AD Domain:

☑ Disable service

□ Disable authorization

The authentication service is not yet saved.
Click on 'Save' button to enable Servers and Remote Groups management.

16. Click ‘Save’.



Name: IB-Example-OCSP

Description:

Priority: 1

Timeout (sec): 5

Service Type: OCSP

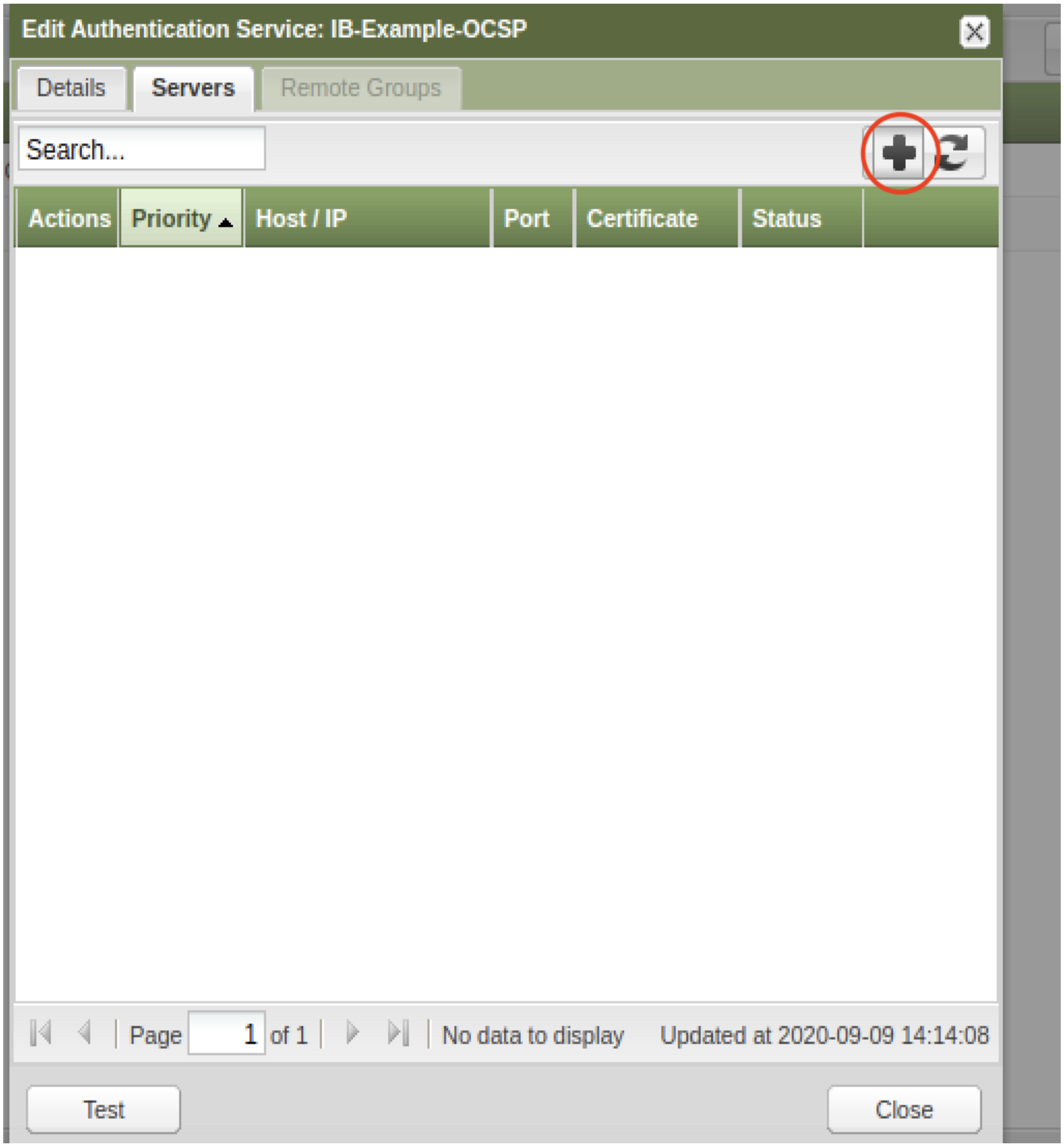
Service Specific Information

☑ Disable service

□ Disable authorization

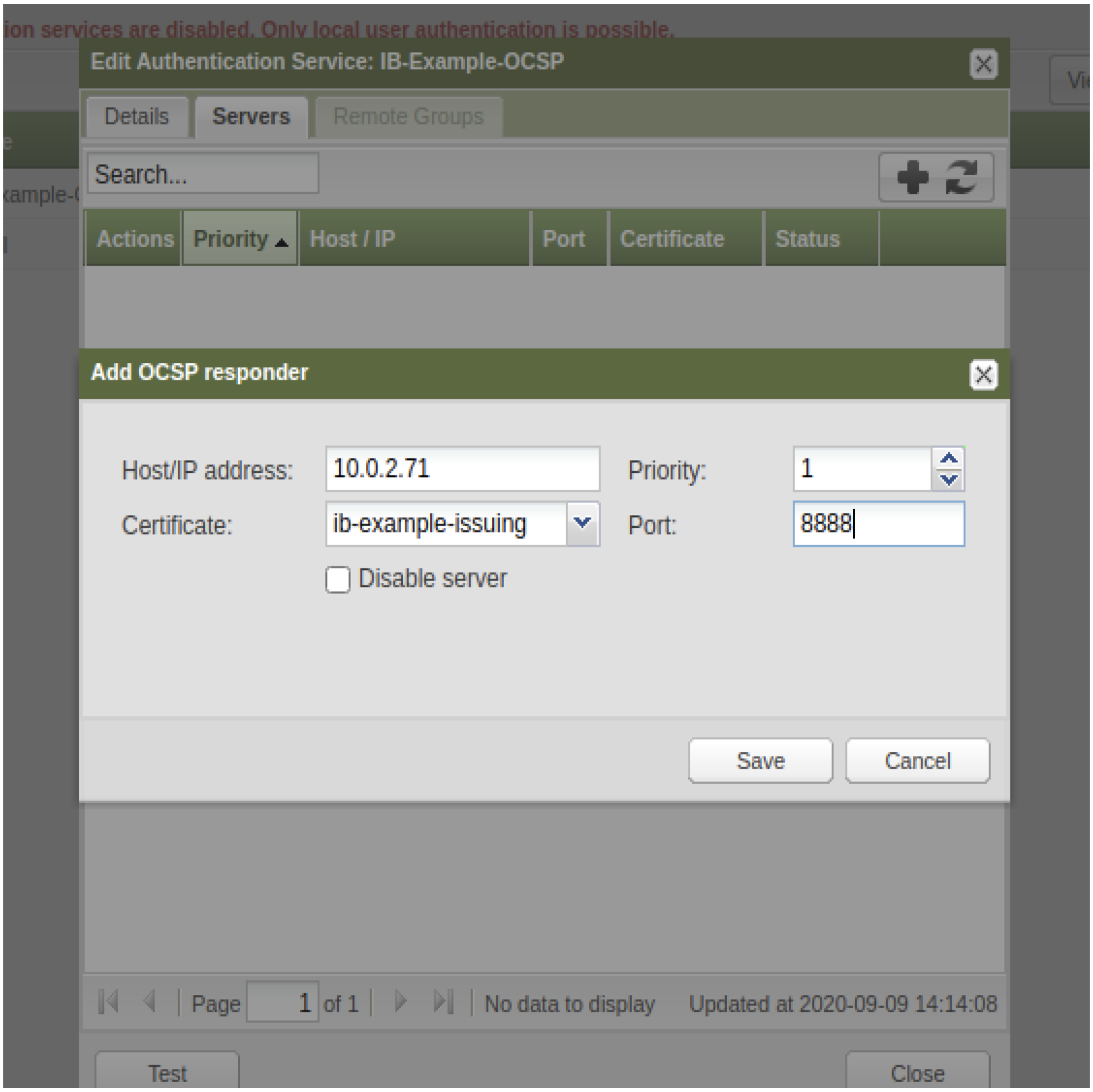
The authentication service is not yet saved.
Click on 'Save' button to enable Servers and Remote Groups management.

17. Click on the ‘Servers’ tab and then click on the ‘+’ button to add the server.



18. Enter the IP address of the OCSP responder, issuing certificate, and port number that is used to communicate with the OCSP responder. Ensure the ‘Disable server’ check box is unchecked. Click

‘Save’.



Host/IP address: 10.0.2.71

Priority: 1

Certificate: ib-example-issuing

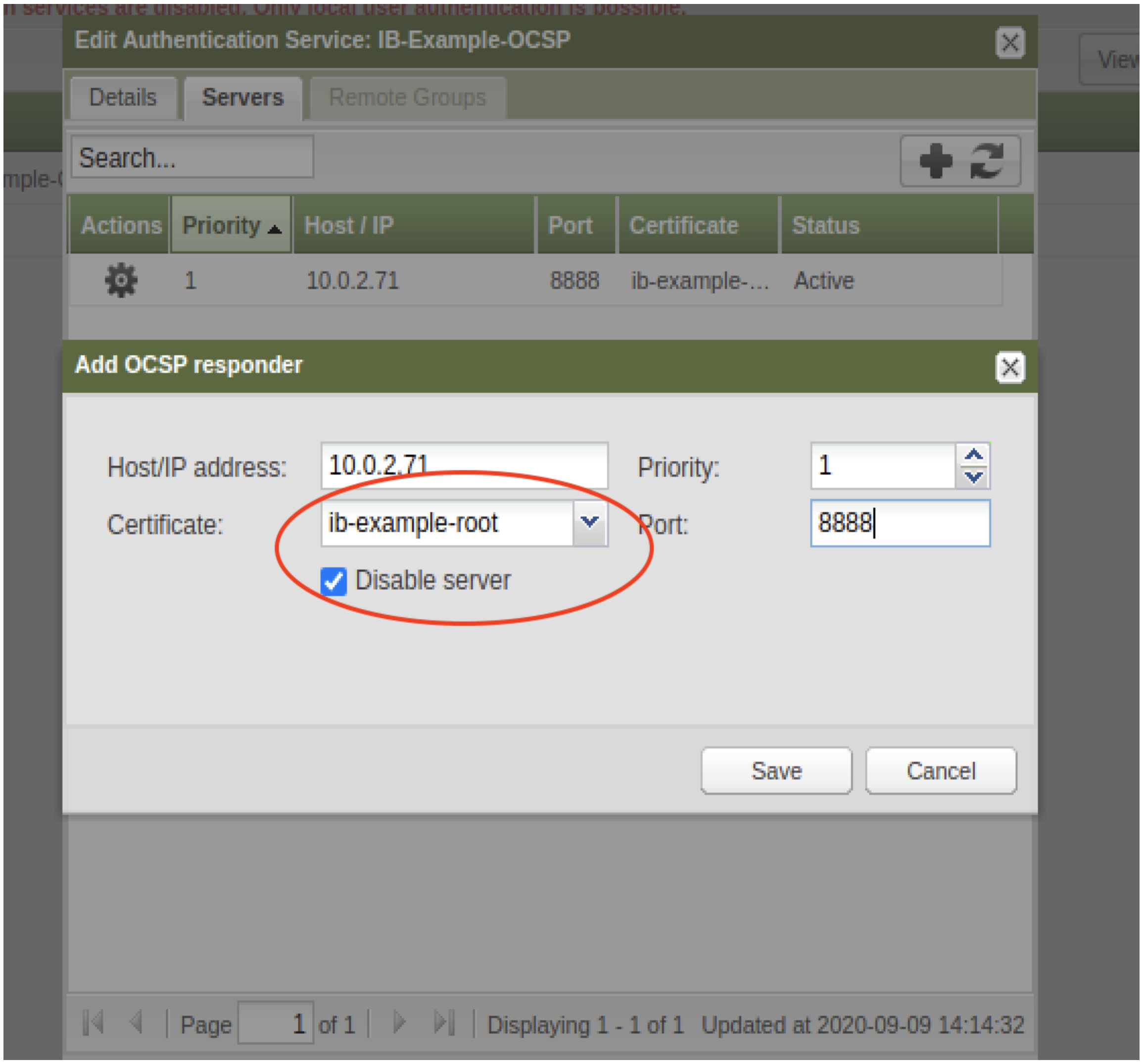
Port: 8888

☐ Disable server

Page 1 of 1

Updated at 2020-09-09 14:14:08

19. Add another OCSP server entry to add the root certificate. Ensure the ‘Disable server’ check box is checked to allow the certificate chains to form properly when both OCSP entries are entered.



n services are disabled. Only local user authentication is possible.

Edit Authentication Service: IB-Example-OCSP

Actions	Priority	Host / IP	Port	Certificate	Status
⚙	1	10.0.2.71	8888	ib-example-…	Active

Add OCSP responder

Host/IP address: 10.0.2.71

Priority: 1

Certificate: ib-example-root

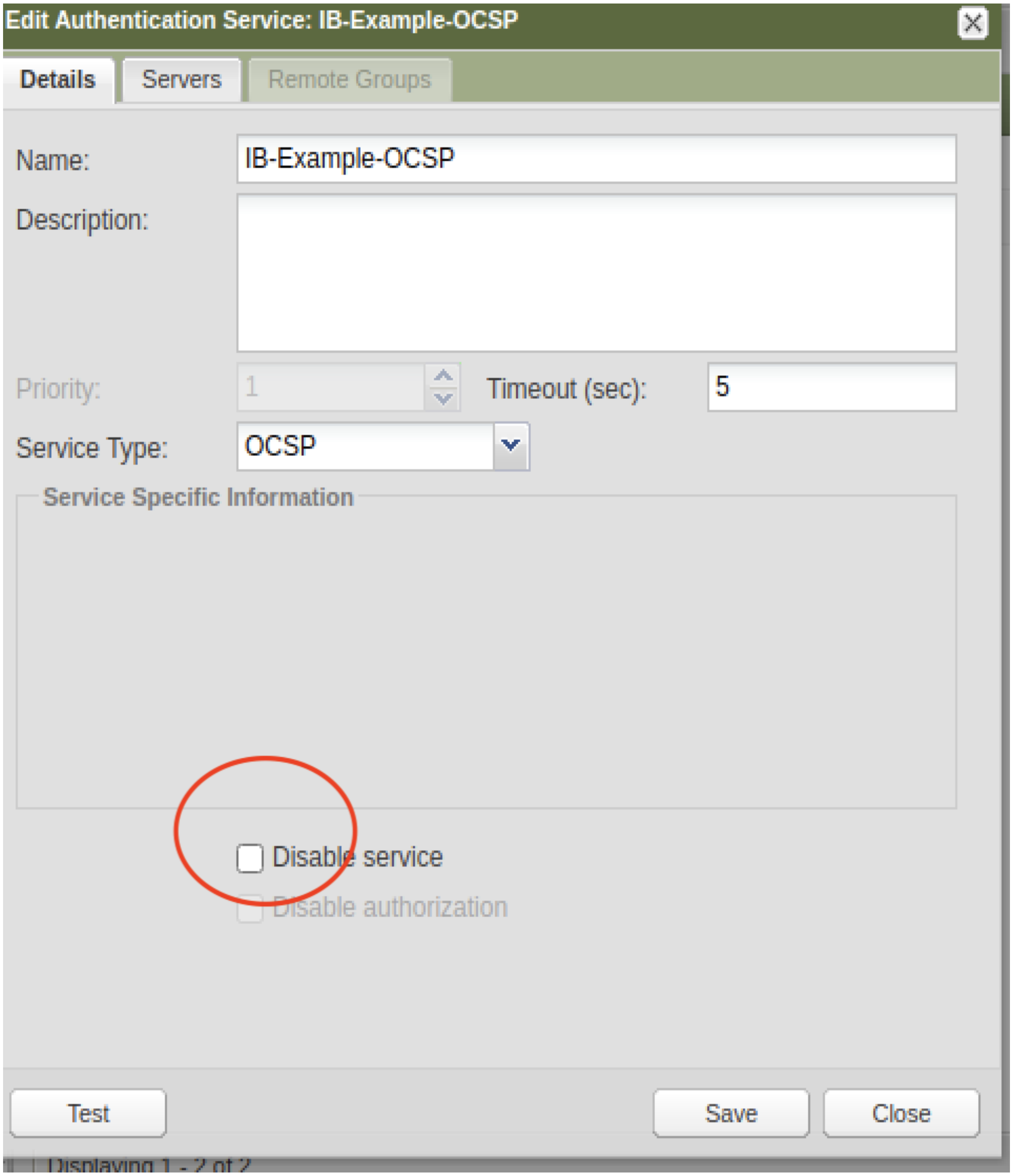
Port: 8888

☑ Disable server

Page 1 of 1 | Displaying 1 - 1 of 1 Updated at 2020-09-09 14:14:32

20. Repeat step 19 for each certificate in your OCSP Responder chain that did not issue the actual responder’s certificate.

21. In addition, enable the service from the 'Details' tab by unchecking the 'Disable service' check box.



Edit Authentication Service: IB-Example-OCSP

Name: IB-Example-OCSP

Description:

Priority: 1

Timeout (sec): 5

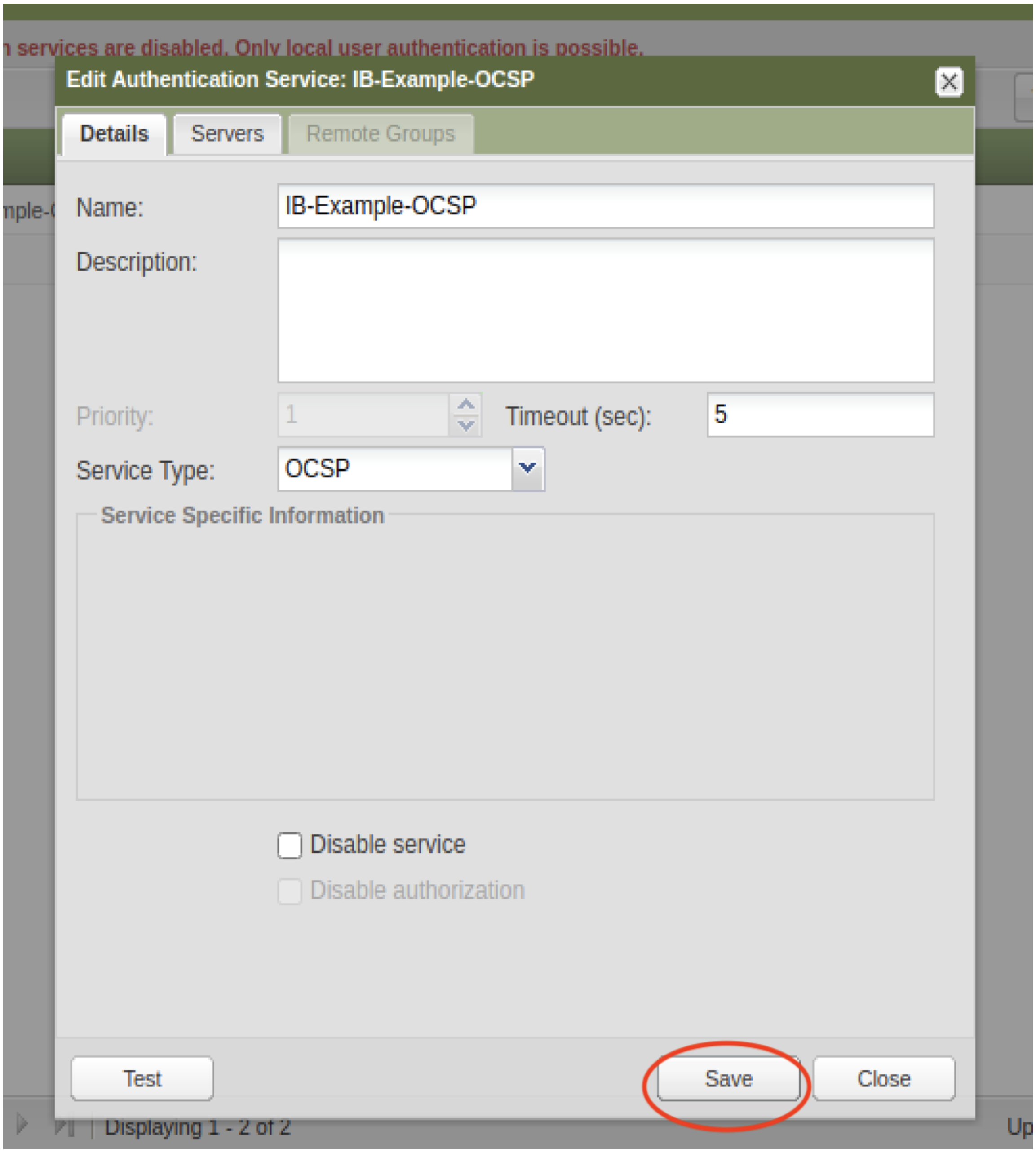
Service Type: OCSP

Service Specific Information

□ Disable service

□ Disable authorization

22. Click ‘Save’.



n services are disabled. Only local user authentication is possible.

Edit Authentication Service: IB-Example-OCSP

Name: IB-Example-OCSP

Description:

Priority: 1

Timeout (sec): 5

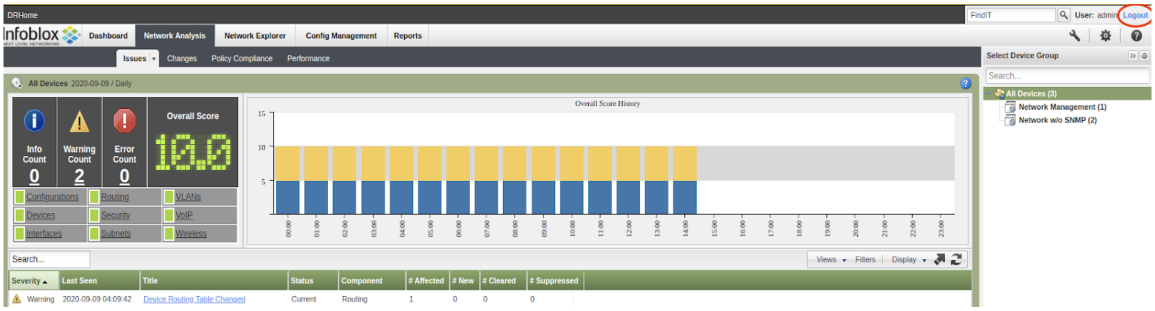
Service Type: OCSP

Service Specific Information

☐ Disable service

☐ Disable authorization

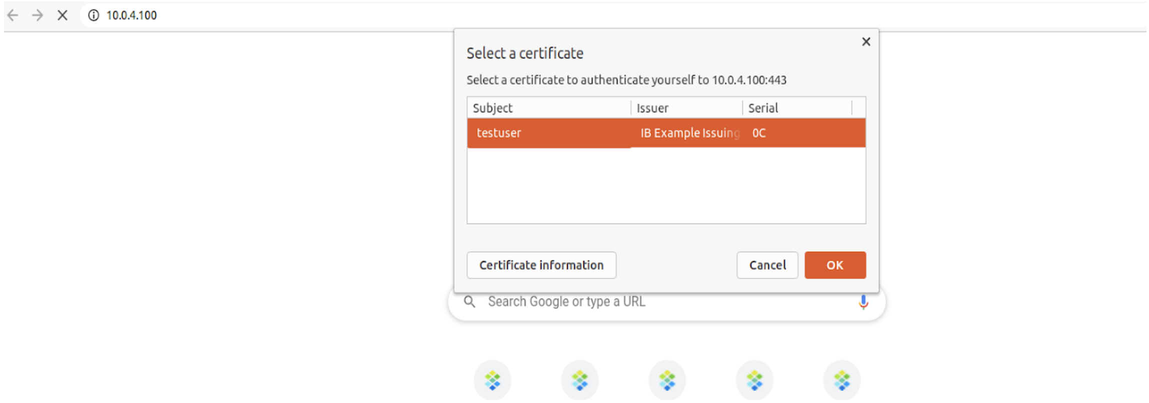
23. Logout of NetMRI by clicking on the ‘Logout’ button in the upper right corner of the screen.



All Devices 2020-09-09 / Daily

Severity ▲	Last Seen	Title	Status	Component	# Affected	# New	# Cleared	# Suppressed
⚠ Warning	2020-09-09 04:09:42	Device Routing Table Changed	Current	Routing	1	0	0	0

24. To ensure proper OCSP responder performance, reboot the NetMRI instance or appliance. After reboot is completed. Point your browser to the IP address or FQDN (fully qualified domain name). You should get a prompt to select the certificate. Select the certificate and click ‘OK’.



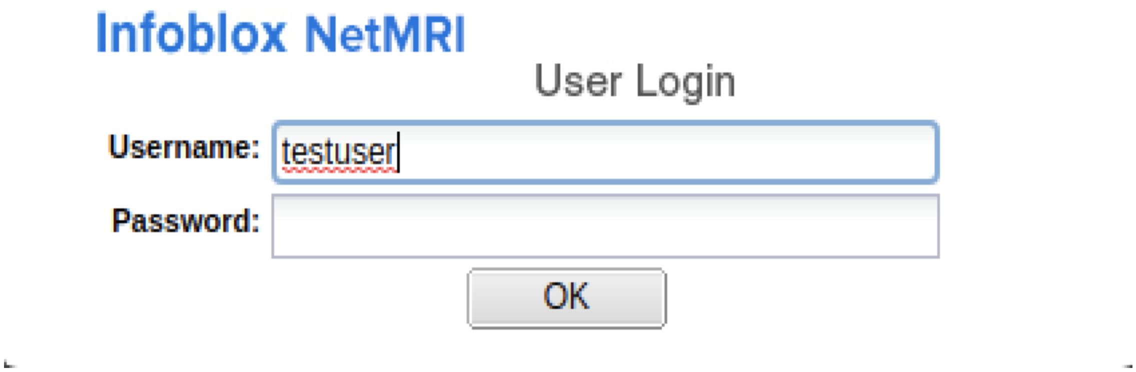
10.0.4.100

Select a certificate

Select a certificate to authenticate yourself to 10.0.4.100:443

Subject	Issuer	Serial
testuser	IB Example Issuing	0C

25. You should now get the NetMRI login screen. The username should be filled in for you and you will need to provide the user’s password and click ‘OK. If everything is configured correctly, the login should work.



Infoblox NetMRI

User Login

Username: testuser

Password:

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com