Isode

R2.0 Red/Black Evaluation Guide

How to create a Red/Black service monitoring environment.

Contents

Introduction

This guide details the process to create a Red/Black service monitoring framework environment using Isode's Red/Black product. Authentication and the configuration repository is provided via M-Vault/ OAuth. Additional/related products in the Isode product set are:

- M-Switch SMTP (SMTP Message Transfer Agent)
- M-Box (POP/IMAP Message Store)
- M-Switch X.400 (X.400 Message Transfer Agent)
- M-Store (X.400 Message Store)
- M-Switch MIXER (message gateway providing conversion between X.400 and Internet email according to the MIXER specifications)
- M-Switch User Server (Email Messaging with options for low-bandwidth and/or high-latency networks)
- M-Switch Gateway (Email Messaging for low-bandwidth and/or high-latency networks)
- Harrier Web (web-based email client)
- Icon 5066 (Stanag 5066 server)
- M-Vault (X500 Directory)
- M-Guard (XML Guard)

Isode products are widely deployed in the Government, Military, Intelligence, Civil Aviation and EDI markets.

***Use of TLS**: Due to UK Export Controls we are unable to provide Evaluation Activations that support TLS to certain geographic regions. This guide is written with the assumption that the reader is not a member of those regions and by default, we will provide a product activation that supports TLS. For customers whose region we have no current export control arrangement, further configuration information may be required and provided separately.*

Objectives

By the end of this guide you will have:

1. Created a Red/Black instance in the Red network.
2. Created a Red/Black instance in the Black network
3. Joined the Red and Black instances via an M-Guard
4. Configured a set of dummy devices to browse with Red/Black

You'll use the M-Vault console, Sodium CA, M-Guard administration tool and Cobalt to configure this. M-Vault console is Isode's directory configuration tool. Cobalt is Isode's system configuration tool. Sodium CA is a simple provider of PKI infrastructure.

Network Planning and Virtual Machine Configuration

Three networks are required to implement this evaluation. The following table summarises their configuration:

Host Name	Local Network	Red Network	Black Network
hqred.red.headquarters.net	192.168.56.1	10.178.0.1	None
hqblack.black.headquarters.net	192.168.56.2	None	192.168.106.1
guard.headquarters.net	192.168.56.3 (hn0)	10.178.0.2 (hn1)	192.168.106.2 (hn2)
Netmask	255.255.255.0	255.255.255.0	255.255.255.0

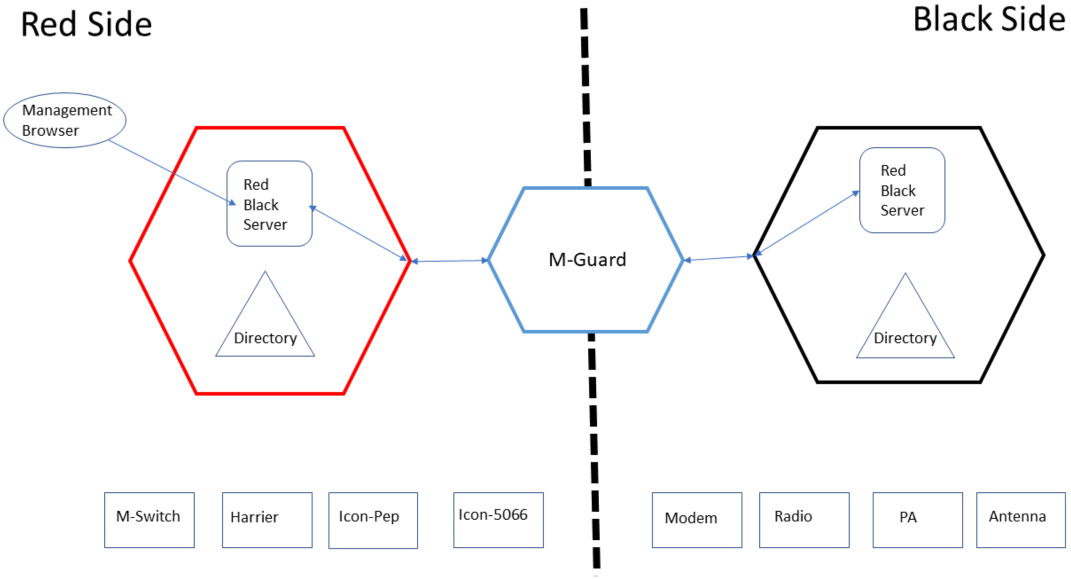
Within the hypervisor environment:

Create an Internal Virtual Switch called “Red Network”
Create an Internal Virtual Switch called “Black Network”
It is assumed that a Virtual switch exists for “Local Network”

Associate the first NIC of each machine to the “Local Network” and allocate an IP address. The table above suggests potential addresses.

The following diagram show the high-level overview of what you will be building.

High Level Overview



This guide is not intended to resemble a real-world managed system but to give you a basic environment you can test with and get used to how the Isode products and configuration GUIs work.

Using Isode Support

You will be given access to Isode support resources when carrying out your evaluation. Any queries you have during your evaluation should be sent to *support@isode.com*. Please note that access to the Self-Service Portal for web-based ticket submission and tracking is not available to evaluators.

Initial Instructions

The setup will be described for Red side. The instructions should then be repeated, substituting with values from Appendix A to create the Black side. The relevant substitutions are indicated with a number like $^{\text{this}}$
For convenience, passwords are assumed to be “Secret1+”
In Linux environments it is assumed all actions are executed as root

Preparing the Server Environment

Naming the Server

Make the machine name: hqred [1]
Make the primary dns suffix for the server red.headquarters.net [2]
Alternatively, you may use your own names or add dns entries in a dns server or hosts file.

Install the Isode Software

Follow the instructions in the release notes for the appropriate platform for the products. Remember to install an appropriate java runtime engine first (refer to product release notes). The highest version currently supported by M-Guard console is java 11 so use this version. In a Windows environment the visual c++ redistributable package.

Messaging Activation Server 1.1
M-Vault 19.0v1
Cobalt 1.3
Red/Black 2.0v5

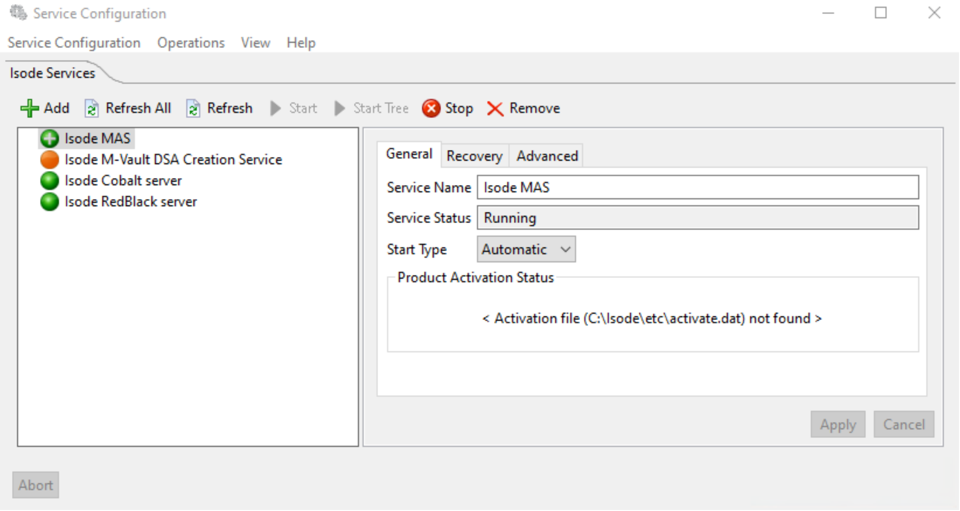
The M-Guard Version Used was 1.4.5 (Client and Server)

Please use a supported web browser as documented in the product release notes.

License the Products

Ensure the MAS server has started by using the Isode Service configuration tool.

Isode Service Configuration tool



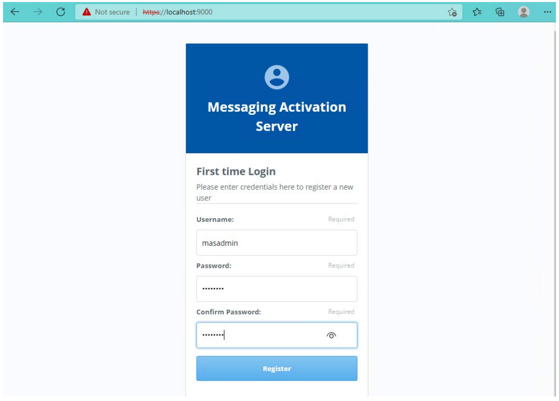
Isode MAS
Isode M-Vault DSA Creation Service
Isode Cobalt server
Isode RedBlack server

Service Name: Isode MAS
Service Status: Running
Start Type: Automatic
Product Activation Status
< Activation file (C:\Isode\etc\activate.dat) not found >

(Linux: “systemctl start mas”)

Browse to “https://localhost:9000”
The browser will provide a security warning. Choose an option to override the warning.

Register MAS administrator



Not secure | https://localhost:9000

Messaging Activation Server

First time Login

Please enter credentials here to register a new user

Username: Required

masadmin

Password: Required

••••••••

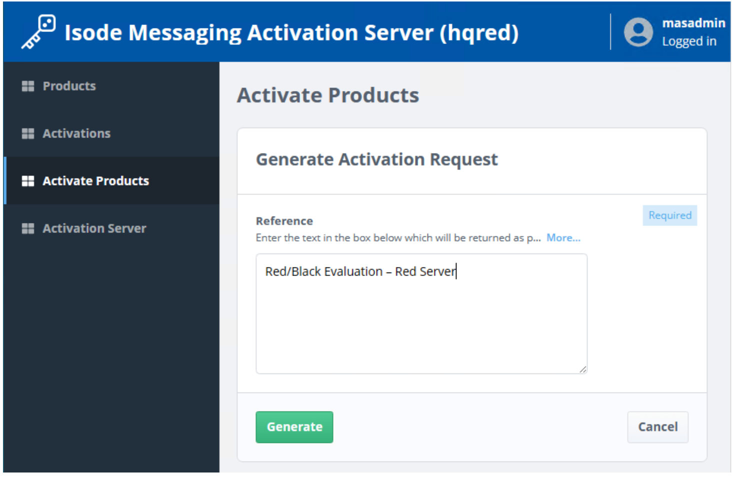
Confirm Password: Required

••••••••

In “Username” type “masadmin”
In “Password” type “Secret1+”
In “Confirm Password” type “Secret1+”
Press “Register”

Select “Activate Products”

Submit activation request



Activate Products

Generate Activation Request

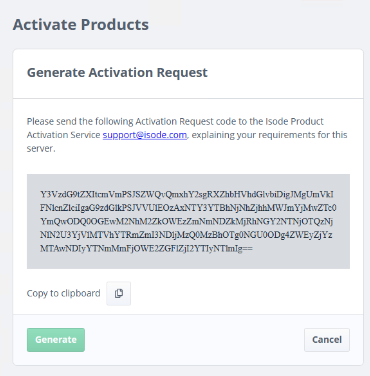
Reference Required

Enter the text in the box below which will be returned as p... More...

Red/Black Evaluation – Red Server

In “Reference” type “Red/Black Evaluation – Red Server” [3]
Press “Generate”

copy activation request



Activate Products

Generate Activation Request

Please send the following Activation Request code to the Isode Product Activation Service support@isode.com, explaining your requirements for this server.

Y3VzdG9tZXItcmVmPSJSZWQvQmxhY2sgRXZhbHVhdGlvbiDigJMgUmVkI
FNlcnZlciIgaG9zdGlkPSJVVU1EOzAxNTY3YTBhNjNhZjhhMWJmYjMwZTc0
YmQwODQ0OGEwM2NhM2ZkOWEzZmNmNDZkMjRhNGY2NTNjOTQzNj
NlN2U3YjVlMTVhYTRmZmI3NDljMzQ0MzBhOTg0NGU0ODg4ZWEyZjYz
MTAwNDIyYTNmMmFjOWE2ZGFlZjI2YTIyNTlmIg==

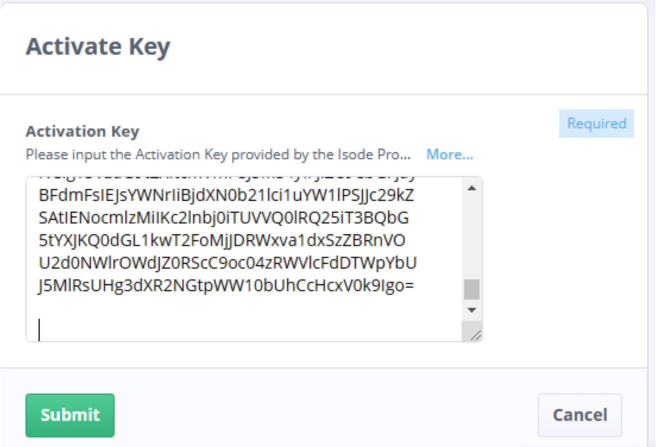
Copy the activation request code to your clipboard.

Send an email to Isode support asking for an activation for M-Vault, Cobalt and Red/Black for a Red/Black evaluation. Include the activation request code.

Isode support will supply a set of Product Activation keys.
It is likely that by the time you receive the activations, the MAS login will have timed out. Press the browser refresh button and log back into MAS.

Paste the keys into the “Activation Key” field.

submit product activation key



Activate Key

Activation Key

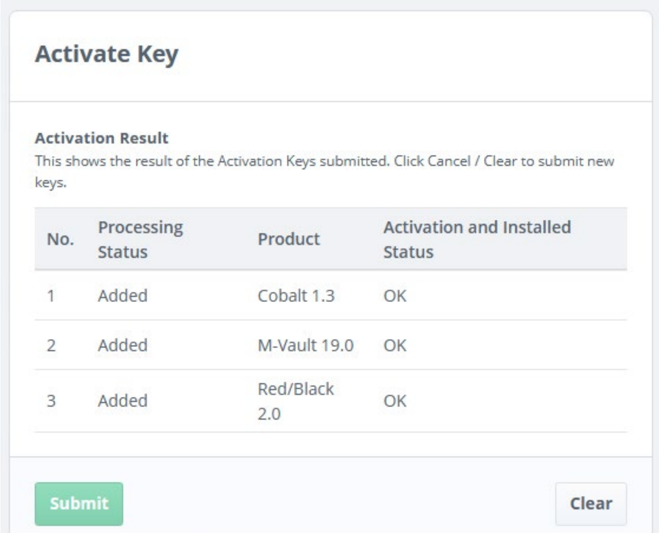
Please input the Activation Key provided by the Isode Pro... More...

```
BFdmFsIEJsYWNrIiBjdXN0b21lci1uYW1lPSJJc29kZ
SAtIENocmlzMiIKc2lnbj0iTUVVQ0lRQ25iT3BQbG
5tYXJKQ0dGL1kwT2FoMjJDRWxva1dxSzZBRnVO
U2d0NWlrOWdJZ0RScC9oc04zRWVlcFdDTWpYbU
J5MlRsUHg3dXR2NGtpWW10bUhCcHcxV0k9Igo=
```

Press “Submit”.

You will receive an “activation Result”:

Activation result



Activate Key

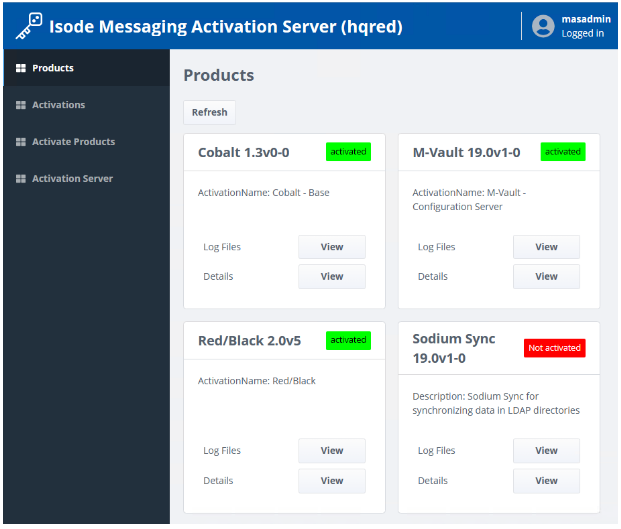
Activation Result

This shows the result of the Activation Keys submitted. Click Cancel / Clear to submit new keys.

No.	Processing Status	Product	Activation and Installed Status
1	Added	Cobalt 1.3	OK
2	Added	M-Vault 19.0	OK
3	Added	Red/Black 2.0	OK

Select “Products”
Press “Refresh”

activated products



Isode Messaging Activation Server (hqred)

masadmin
Logged in

Products

Cobalt 1.3v0-0 activated

ActivationName: Cobalt - Base

Log Files View

Details View

M-Vault 19.0v1-0 activated

ActivationName: M-Vault - Configuration Server

Log Files View

Details View

Red/Black 2.0v5 activated

ActivationName: Red/Black

Log Files View

Details View

Sodium Sync 19.0v1-0 Not activated

Description: Sodium Sync for synchronizing data in LDAP directories

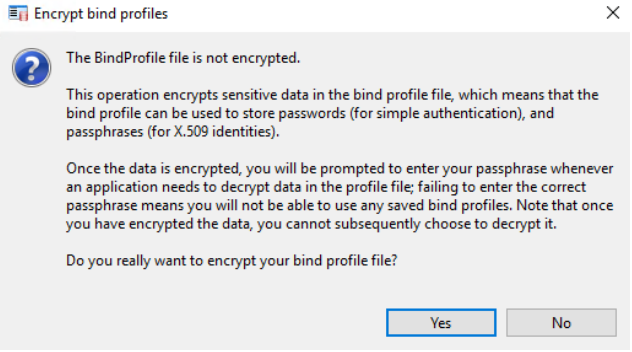
Log Files View

Details View

Configure M-Vault

Run “M-Vault Console” from the Windows Start menu (Linux: “/opt/isode/sbin/mvc”)

encrypt bind profile



The BindProfile file is not encrypted.

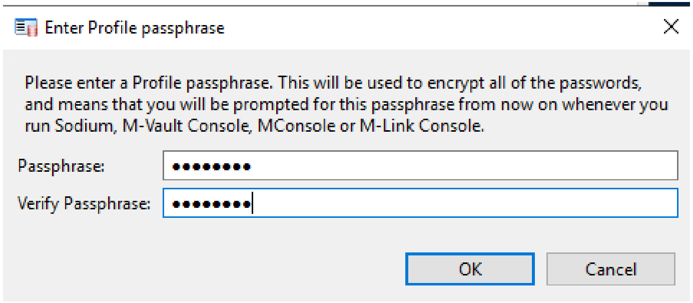
This operation encrypts sensitive data in the bind profile file, which means that the bind profile can be used to store passwords (for simple authentication), and passphrases (for X.509 identities).

Once the data is encrypted, you will be prompted to enter your passphrase whenever an application needs to decrypt data in the profile file; failing to enter the correct passphrase means you will not be able to use any saved bind profiles. Note that once you have encrypted the data, you cannot subsequently choose to decrypt it.

Do you really want to encrypt your bind profile file?

Press “Yes”

enter profile passphrase



Please enter a Profile passphrase. This will be used to encrypt all of the passwords, and means that you will be prompted for this passphrase from now on whenever you run Sodium, M-Vault Console, MConsole or M-Link Console.

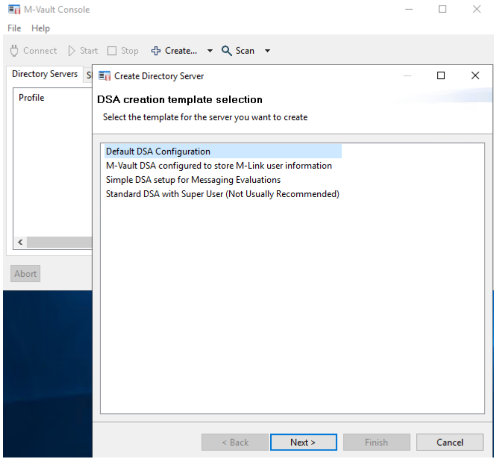
Passphrase: ••••••••

Verify Passphrase: ••••••••

On “Enter Profile passphrase” type “Secret1+” in “Passphrase” and “Verify Passphrase”
Click “OK”

On “The Bind Profile has been encrypted” press “OK”
On “No Managed DSA’s Configured” press “OK”
Press “Create/Directory Server”

create directory server



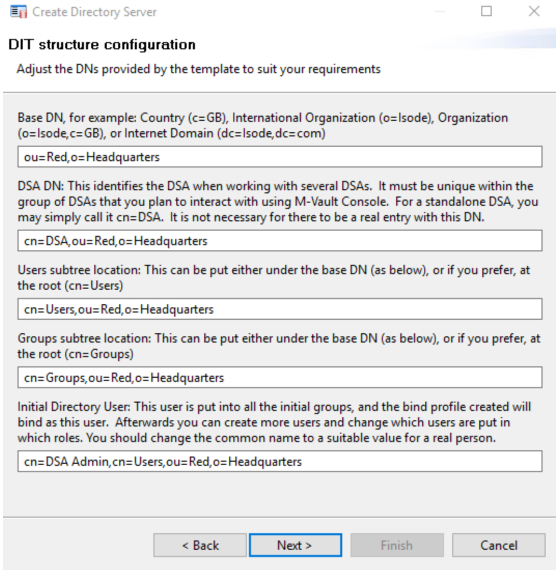
DSA creation template selection

Select the template for the server you want to create

Default DSA Configuration
M-Vault DSA configured to store M-Link user information
Simple DSA setup for Messaging Evaluations
Standard DSA with Super User (Not Usually Recommended)

Select “Default DSA Configuration “
Click “Next >”

DIT Structure Configuration



Create Directory Server

DIT structure configuration

Adjust the DNs provided by the template to suit your requirements

Base DN, for example: Country (c=GB), International Organization (o=Isode), Organization (o=Isode,c=GB), or Internet Domain (dc=Isode,dc=com)

ou=Red,o=Headquarters

DSA DN: This identifies the DSA when working with several DSAs. It must be unique within the group of DSAs that you plan to interact with using M-Vault Console. For a standalone DSA, you may simply call it cn=DSA. It is not necessary for there to be a real entry with this DN.

cn=DSA,ou=Red,o=Headquarters

Users subtree location: This can be put either under the base DN (as below), or if you prefer, at the root (cn=Users)

cn=Users,ou=Red,o=Headquarters

Groups subtree location: This can be put either under the base DN (as below), or if you prefer, at the root (cn=Groups)

cn=Groups,ou=Red,o=Headquarters

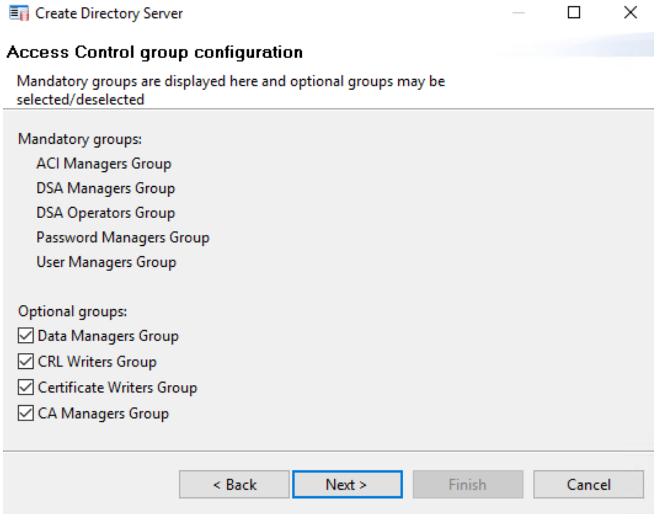
Initial Directory User: This user is put into all the initial groups, and the bind profile created will bind as this user. Afterwards you can create more users and change which users are put in which roles. You should change the common name to a suitable value for a real person.

cn=DSA Admin,cn=Users,ou=Red,o=Headquarters

In “Base DN” type “ou=Red,o=Headquarters” [4]
In “Initial directory user” replace “Thomas Atkins” with “DSA Admin”
Click “Next >”

On “Access control rule selection” leave defaults and click “Next >”

access control group configuration



Create Directory Server

Access Control group configuration

Mandatory groups are displayed here and optional groups may be selected/deselected

Mandatory groups:
- ACI Managers Group
- DSA Managers Group
- DSA Operators Group
- Password Managers Group
- User Managers Group

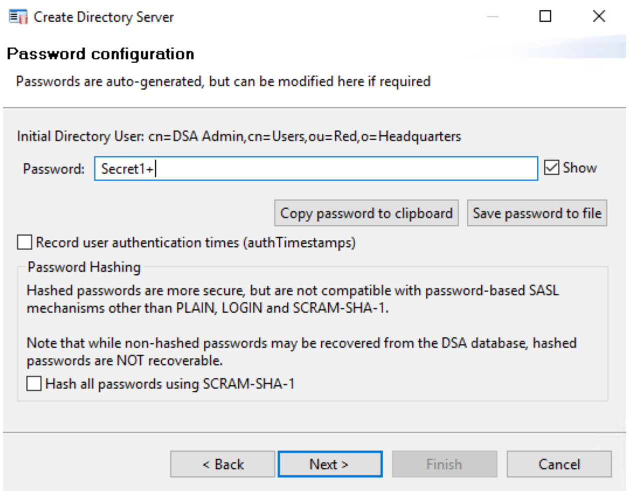
Optional groups:
- ☑ Data Managers Group
- ☑ CRL Writers Group
- ☑ Certificate Writers Group
- ☑ CA Managers Group

On “Access Control group configuration” select additional optional groups:

- CRL Writers Group
- Certificate Writers Group
- CA Managers Group

Click “Next >”

password configuration



Create Directory Server

Password configuration

Passwords are auto-generated, but can be modified here if required

Initial Directory User: cn=DSA Admin,cn=Users,ou=Red,o=Headquarters

Password: Secret1+ ☑ Show

☐ Record user authentication times (authTimestamps)

Password Hashing

Hashed passwords are more secure, but are not compatible with password-based SASL mechanisms other than PLAIN, LOGIN and SCRAM-SHA-1.

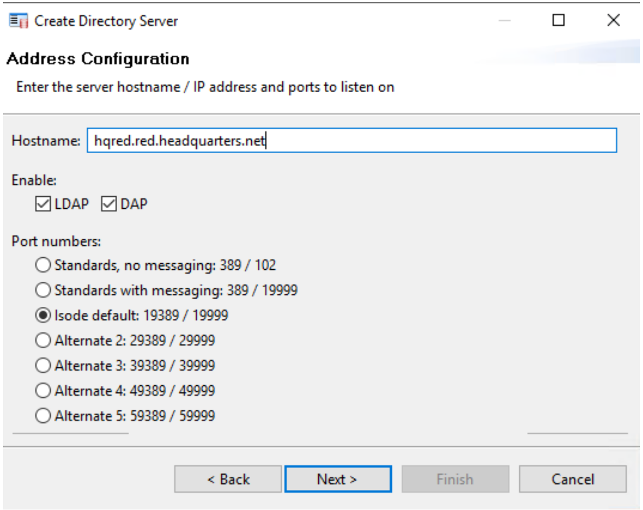
Note that while non-hashed passwords may be recovered from the DSA database, hashed passwords are NOT recoverable.

☐ Hash all passwords using SCRAM-SHA-1

On “Password configuration” change the password to “Secret1+”
Click “Next >”

On “Bind Profile Names and Filesystem Location” leave Defaults and click “Next >”

address configuration



Create Directory Server

Address Configuration

Enter the server hostname / IP address and ports to listen on

Hostname: hqred.red.headquarters.net

Enable:
☑ LDAP ☑ DAP

Port numbers:
- ○ Standards, no messaging: 389 / 102
- ○ Standards with messaging: 389 / 19999
- ● Isode default: 19389 / 19999
- ○ Alternate 2: 29389 / 29999
- ○ Alternate 3: 39389 / 39999
- ○ Alternate 4: 49389 / 49999
- ○ Alternate 5: 59389 / 59999

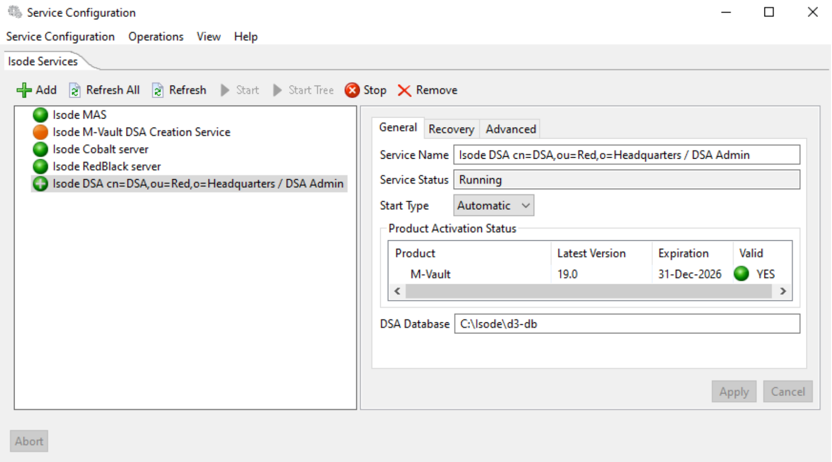
On “Address Configuration” change “Hostname” to “hqred.red.headquarters.net” [5]

Click “Next >”
On “Confirm Details” click “Finish”
On “Directory Server Created Successfully” click “Yes”

The next 4 steps are for Windows only:

Open “Isode Service Configuration” from the start menu
Select “Isode DSA”
Change “Start Type” to “Automatic”
Press “Apply”

configure dsa to start automatically



- Isode MAS
- Isode M-Vault DSA Creation Service
- Isode Cobalt server
- Isode RedBlack server
- Isode DSA cn=DSA,ou=Red,o=Headquarters / DSA Admin

Service Name: Isode DSA cn=DSA,ou=Red,o=Headquarters / DSA Admin

Service Status: Running

Start Type: Automatic

Product Activation Status

Product	Latest Version	Expiration	Valid
M-Vault	19.0	31-Dec-2026	● YES

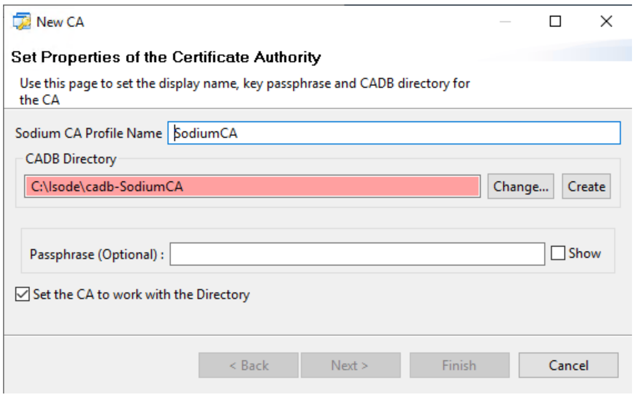
DSA Database: C:\Isode\d3-db

Select “Isode M-Vault DSA Creation Service”
Change “Start Type” to “Disabled”
In “DSA Database” type “x”
Press “Apply”

Configure CA

Create the directory “c:\IsodeCerts” (Linux : “/var/isode/certs”)
Open “Sodium CA” from the Windows start menu (Linux: “/opt/isode/sbin/sodiumca”)
Click “New”

create ca



New CA

Set Properties of the Certificate Authority

Use this page to set the display name, key passphrase and CADB directory for the CA

Sodium CA Profile Name: SodiumCA

CADB Directory: C:\Isode\cadb-SodiumCA

Passphrase (Optional) :

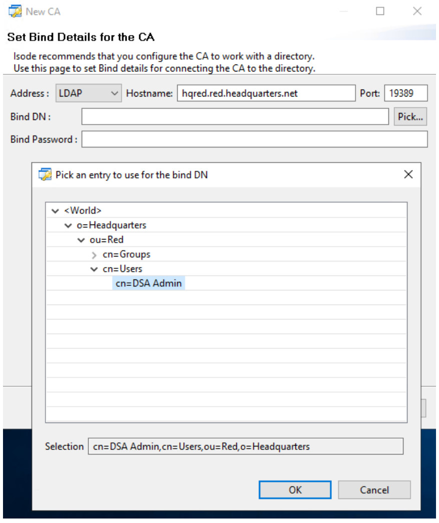
□ Show

☑ Set the CA to work with the Directory

On “Set Properties of the Certificate Authority” leave Defaults
Click “Create”
Click “Next >”

In “Hostname” type “hqred.red.headquarters.net” [5]

set bind details for the CA



New CA

Set Bind Details for the CA

Isode recommends that you configure the CA to work with a directory.
Use this page to set Bind details for connecting the CA to the directory.

Address : LDAP Hostname: hqred.red.headquarters.net Port: 19389

Bind DN :

Bind Password :

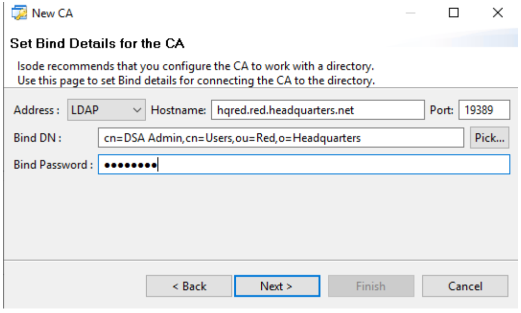
Pick an entry to use for the bind DN

```
<World>
  o=Headquarters
    ou=Red
      cn=Groups
      cn=Users
        cn=DSA Admin
```

Selection: cn=DSA Admin,cn=Users,ou=Red,o=Headquarters

Click “Pick”
Browse to “cn=DSA Admin, CN=Users, ou=Red,o=Headquarters” [6]
Click “OK”

set bind password for ca



New CA

Set Bind Details for the CA

Isode recommends that you configure the CA to work with a directory.
Use this page to set Bind details for connecting the CA to the directory.

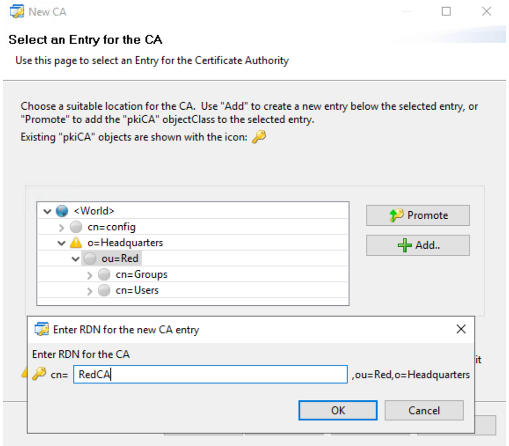
Address : LDAP Hostname: hqred.red.headquarters.net Port: 19389

Bind DN : cn=DSA Admin,cn=Users,ou=Red,o=Headquarters

Bind Password : ••••••••

In “Bind Password” type “Secret1+”
Click “Next >”

create ca directory entry



New CA

Select an Entry for the CA

Use this page to select an Entry for the Certificate Authority

Choose a suitable location for the CA. Use "Add" to create a new entry below the selected entry, or "Promote" to add the "pkiCA" objectClass to the selected entry.
Existing "pkiCA" objects are shown with the icon: 🔑

```
<World>
  cn=config
  o=Headquarters
    ou=Red
      cn=Groups
      cn=Users
```

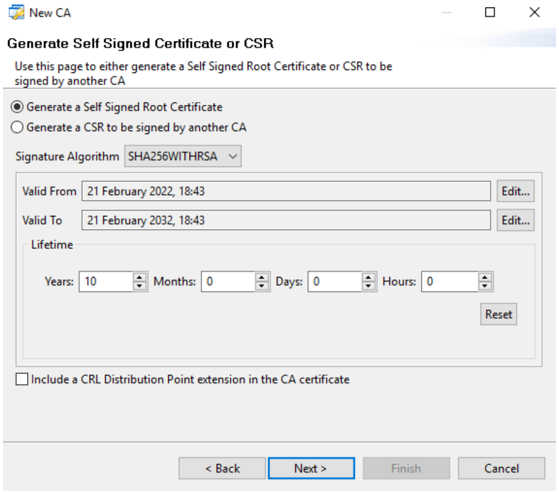
Enter RDN for the new CA entry

Enter RDN for the CA

cn= RedCA ,ou=Red,o=Headquarters

On “Select an Entry for the CA” browse to and select “ou=Red,o=Headquarters” [7]
Click “Add”
On “Enter RDN for the new CA” type “RedCA” [8]
Click “OK”
Click “Next >”
On “Set Key Type, Subject and Subject Alternative Names” leave default options.
Click “Next >”
On “Certificate Status Sharing” leave Defaults
Click “Next >”
On “Set the CRL Distribution Point for the CA” leave defaults
Click “Next >”
On “Set the Access Description List for the CA” leave defaults
Click “Next >”
On “Set Basic Constraints and KeyUsage Extension” leave defaults
Click “Next >”

generate self signed ca certificate



New CA

Generate Self Signed Certificate or CSR

Use this page to either generate a Self Signed Root Certificate or CSR to be signed by another CA

● Generate a Self Signed Root Certificate

○ Generate a CSR to be signed by another CA

Signature Algorithm: SHA256WITHRSA

Valid From: 21 February 2022, 18:43

Valid To: 21 February 2032, 18:43

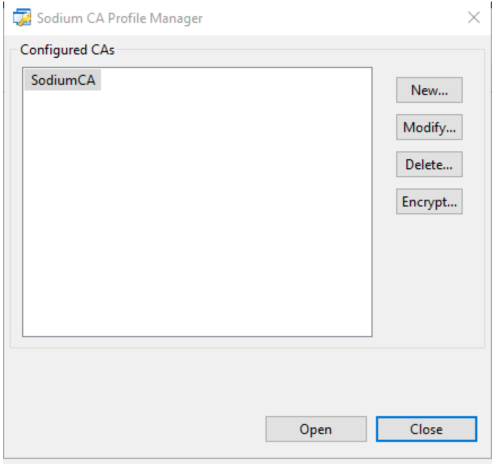
Lifetime

Years: 10 Months: 0 Days: 0 Hours: 0

□ Include a CRL Distribution Point extension in the CA certificate

On “Generate Self Signed Certificate or CSR” select “Generate a Self Signed Root Certificate”
Leave the defaults
Click “Next >”
On “Root CA Certificate” leave Defaults
Click “Next >”
On “Finish CA Configuration” press “Finish”

open configured ca



Sodium CA Profile Manager

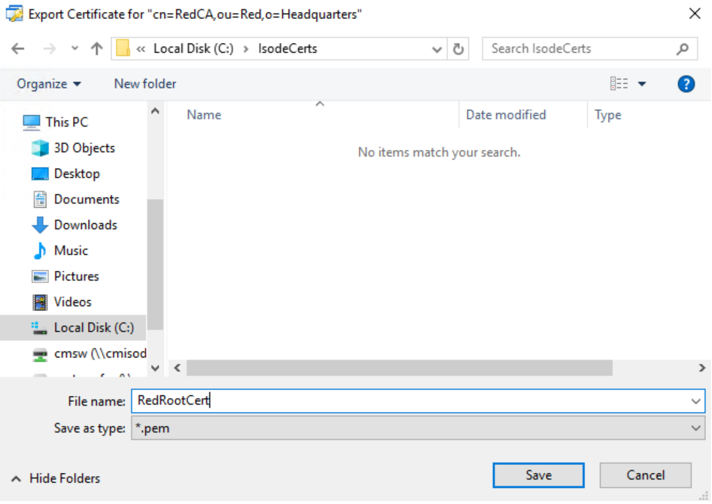
Configured CAs

SodiumCA

On “Sodium CA Profile Manager” select “SodiumCA”
Click “Open”

In “Password” type “Secret1+”
Click “OK”
Select “Certificate for cn=RedCA, ou=Red,o=Headquarters” [9]
Select “Export PEM ..”
On “Export Certificate for “cn=RedCA, ou=Red,o=Headquarters” [9], browse to “c:\IsodeCerts” (Linux : “/var/isode/certs”)
Change Filename to “RedRootCert.pem” [10]

export root certificate



Export Certificate for "cn=RedCA,ou=Red,o=Headquarters"

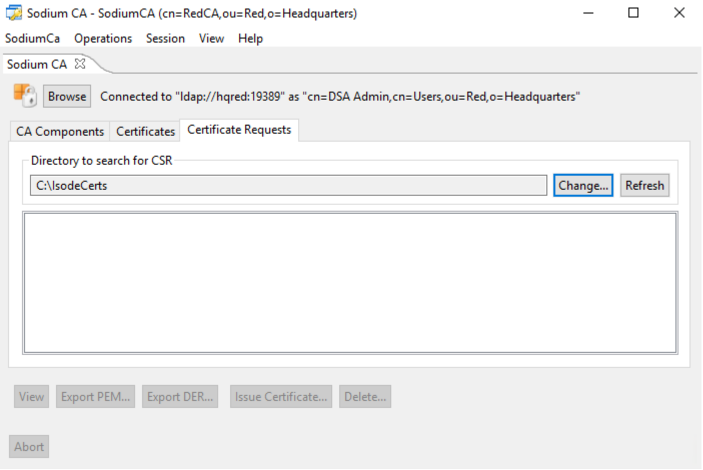
No items match your search.

File name: RedRootCert

Save as type: *.pem

Press “Save”
On “Certificate for” exported Click “OK”
Change to “Certificate Requests” tab
Change “Directory to Search for CSR” to “C:\IsodeCerts” (Linux: “/var/isode/certs”)

CSR directory changed



Sodium CA - SodiumCA (cn=RedCA,ou=Red,o=Headquarters)

Connected to "ldap://hqred:19389" as "cn=DSA Admin,cn=Users,ou=Red,o=Headquarters"

Directory to search for CSR: C:\IsodeCerts

Create a Certificate for M-Vault and Red/Black

Open a command prompt (Linux: a Terminal Session)
Change directory to “c:\IsodeCerts” (Linux: “/var/isode/certs”)
Create a certificate request by executing the following:

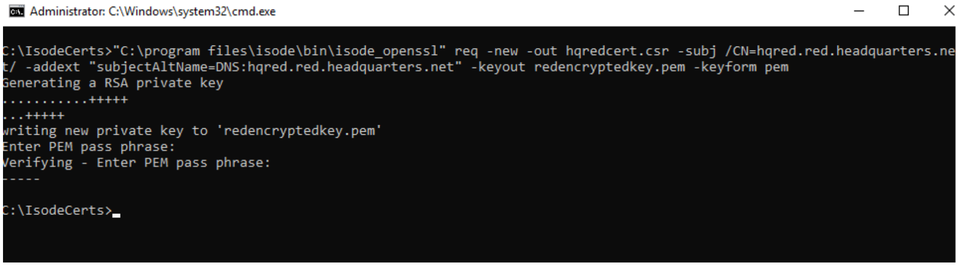
Windows:

“"C:\program files\isode\bin\isode_openssl" req -new -out hqredcert.csr -subj /CN=hqred.red.headquarters.net/ -addext "subjectAltName=DNS:hqred.red.headquarters.net" -keyout redencryptedkey.pem -keyform pem” [11]

Linux:

“"/opt/isode/bin/isode_openssl" req -new -out hqredcert.csr -subj /CN=hqred.red.headquarters.net/ -addext "subjectAltName=DNS:hqred.red.headquarters.net" -keyout redencryptedkey.pem -keyform pem” [12]

create certificate request



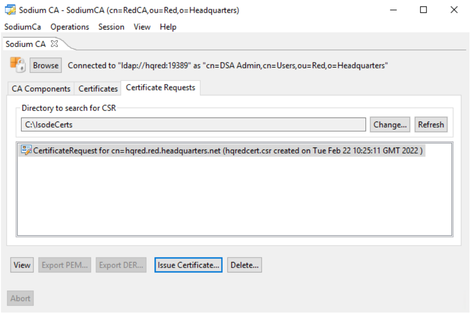
```
:\IsodeCerts>"C:\program files\isode\bin\isode_openssl" req -new -out hqredcert.csr -subj /CN=hqred.red.headquarters.ne
t/ -addext "subjectAltName=DNS:hqred.red.headquarters.net" -keyout redencryptedkey.pem -keyform pem
enerating a RSA private key
..........+++++
...+++++
riting new private key to 'redencryptedkey.pem'
nter PEM pass phrase:
erifying - Enter PEM pass phrase:
----

:\IsodeCerts>_
```

When asked “Enter PEM pass phrase” type “Secret1+” and press “Return”
When asked “Verifying – Enter PEM pass phrase:” type “Secret1+” and press “Return”

In Sodium CA, change to “Certificate Requests” tab.
Press “Refresh”
Ensure the recent request is highlighted.
Click “Issue Certificate”

issue certificate



Connected to "ldap://hqred:19389" as "cn=DSA Admin,cn=Users,ou=Red,o=Headquarters"

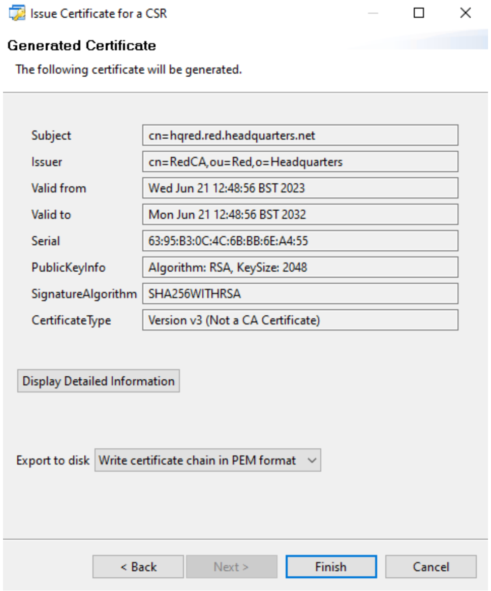
Directory to search for CSR: C:\IsodeCerts

CertificateRequest for cn=hqred.red.headquarters.net (hqredcert.csr created on Tue Feb 22 10:25:11 GMT 2022)

On “Certificate Signing Request” leave defaults
Click “Next >”
On “Select and Add Subject Alternative names” leave defaults

Click “Next >”
On “Select and Create X.509 Extensions” leave defaults
Click “Next >”
On “Set Validity and Signature Algorithm for the Certificate” leave defaults
Click “Next >”

Generated Certificate



Generated Certificate
The following certificate will be generated.

Subject: cn=hqred.red.headquarters.net
Issuer: cn=RedCA,ou=Red,o=Headquarters
Valid from: Wed Jun 21 12:48:56 BST 2023
Valid to: Mon Jun 21 12:48:56 BST 2032
Serial: 63:95:B3:0C:4C:6B:BB:6E:A4:55
PublicKeyInfo: Algorithm: RSA, KeySize: 2048
SignatureAlgorithm: SHA256WITHRSA
CertificateType: Version v3 (Not a CA Certificate)

Export to disk: Write certificate chain in PEM format

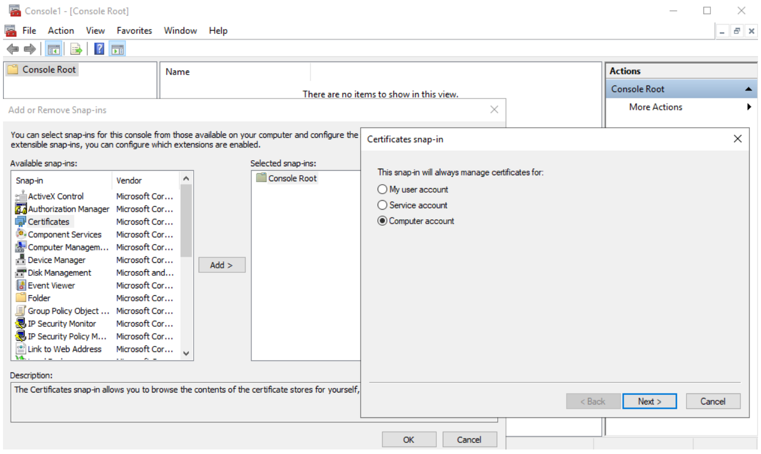
On “Generated Certificate”, choose “Write certificate chain in PEM format”
Click “Finish”
On “CSR Signed” Click “OK”

Copy the file “c:\IsodeCerts\hqredcert_cert_Chain.pem” [13] to the file “c:\IsodeCerts\hqredcert_cert.pem” [14]. The path will differ on Linux.
Edit the file: “c:\IsodeCerts\hqredcert_cert.pem” [14] using a text editor.
Delete the second certificate from the file (the CA Cert).
Save the file.

Import Root Certificate to Windows Certificate Store (Windows)

From the start menu Run “MMC”
Browse “File/Add or Remove Snap-in ..”

add certificate snap-in



There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself,

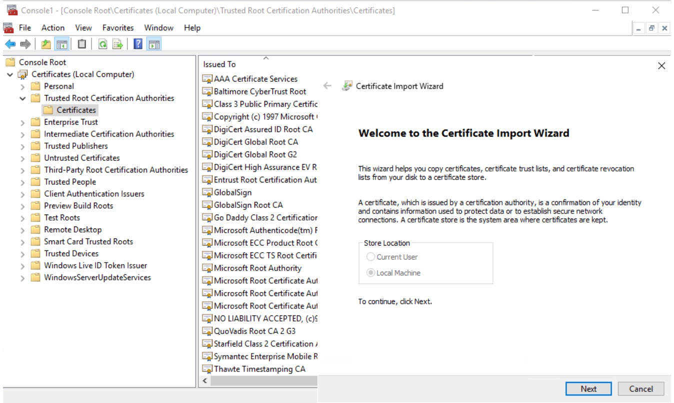
This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

Select “Certificates”
Press “Add”
Select “Computer Account”

Press “Next >”
On “Select Computer” leave defaults
Press “Finish”
On “Add or Remove Snap-ins Press “OK”
In the left-hand pane browse to and Select “Trusted Root Certification Authorities\Certificates”

import certificate


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Remote Desktop
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
WindowsServerUpdateServices
Certificate Import Wizard
Next
Cancel

Issued To
AAA Certificate Services
Baltimore CyberTrust Root
Class 3 Public Primary Certific
Copyright (c) 1997 Microsoft
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert Global Root G2
DigiCert High Assurance EV R
Entrust Root Certification Aut
GlobalSign
GlobalSign Root CA
Go Daddy Class 2 Certificatior
Microsoft Authenticode(tm) F
Microsoft ECC Product Root (
Microsoft ECC TS Root Certifi
Microsoft Root Authority
Microsoft Root Certificate Aut
Microsoft Root Certificate Aut
Microsoft Root Certificate Aut
NO LIABILITY ACCEPTED, (c)
QuoVadis Root CA 2 G3
Starfield Class 2 Certification /
Symantec Enterprise Mobile R
Thawte Timestamping CA

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

Right Click/All tasks/Import ..
On “Welcome to Certificate Import Wizard”, press “Next”
On “File to import” Browse to “C:\IsodeCerts”
In the “file types” dropdown select “All Files”
Select “RedRootCert.pem” [10] and “Open”
Press “Next >”
On “Certificate Store” leave defaults
Press “Next >”
On “Completing the Certificate Import Wizard” Press “Finish”
On “The import was successful”, press “OK”
Close the MMC.
On “Save console settings to Console1” Press “Yes”

On “Save As” in “File name:” field type “Certificates”
Saving the console as “Certificates”
Click “Save”

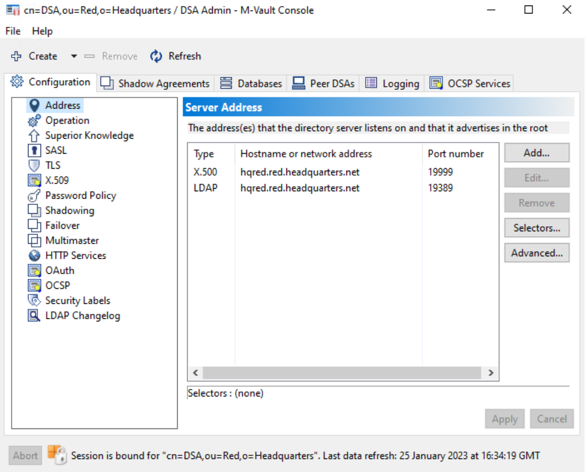
Import Root Certificate to Linux Certificate Store (Linux)

Open Firefox Browser
Select “Settings/Privacy and Security/View Certificates…”
Select “Authorities” tab.
Click “Import..”
Select “/var/isode/certs/RedRootCert.pem” [10]
Click “Open”
Check “Trust This CA to identify web sites”
Click “OK”
On “Certificate Manager” click “OK”

Configure M-Vault to Support TLS

Return to the open "M-Vault Console"

import certificate



cn=DSA,ou=Red,o=Headquarters / DSA Admin - M-Vault Console

Server Address

The address(es) that the directory server listens on and that it advertises in the root

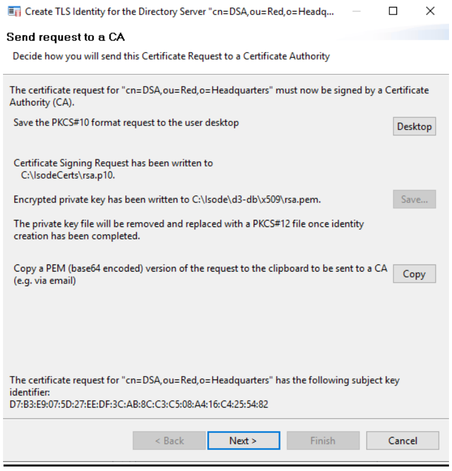
Type	Hostname or network address	Port number
X.500	hqred.red.headquarters.net	19999
LDAP	hqred.red.headquarters.net	19389

Selectors : (none)

Session is bound for "cn=DSA,ou=Red,o=Headquarters". Last data refresh: 25 January 2023 at 16:34:19 GMT

Select "TLS" on the left-hand side of the "Configuration" tab
On the "Identities" tab Press "Create .."
On "Set the Key parameters and edit Subject DN" leave defaults
Click "Next >"
On "Select and add Subject Alternative names and Clearance" leave defaults
Click "Next >"
On "Select X.509 Extensions" leave defaults
Press "Next >"
On "Certificate Request Contents" leave defaults
Press "Next >"
On "Send Request to a CA" press "Save …"
On "Choose a Directory" browse to "C:\IsodeCerts" (Linux: "/var/isode/certs")
Click "Select Folder" (Linux: "Open").
Back on "Send Request to CA" leave defaults

populated send request to CA



Create TLS Identity for the Directory Server "cn=DSA,ou=Red,o=Headq...

Send request to a CA

Decide how you will send this Certificate Request to a Certificate Authority

The certificate request for "cn=DSA,ou=Red,o=Headquarters" must now be signed by a Certificate Authority (CA).

Save the PKCS#10 format request to the user desktop

Certificate Signing Request has been written to
C:\IsodeCerts\rsa.p10.

Encrypted private key has been written to C:\Isode\d3-db\x509\rsa.pem.

The private key file will be removed and replaced with a PKCS#12 file once identity creation has been completed.

Copy a PEM (base64 encoded) version of the request to the clipboard to be sent to a CA (e.g. via email)

The certificate request for "cn=DSA,ou=Red,o=Headquarters" has the following subject key identifier:
D7:B3:E9:07:5D:27:EE:DF:3C:AB:8C:C3:C5:08:A4:16:C4:25:54:82

Click "Next >"

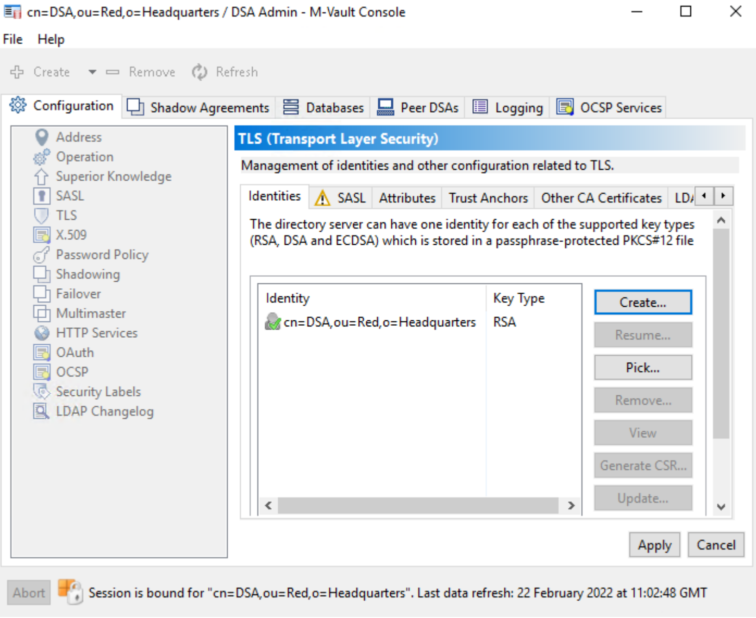
In Sodium CA:

Change to “Certificate Requests” Tab
Press “Refresh”
Ensure Certificate request is selected
Click “Issue Certificate ..”
On “Certificate Signing Request” leave defaults
Click “Next >”
On “Select and add Subject Alternative Names” leave defaults
Press “Next >”
On “Select and Create X.509 Extensions” leave defaults
Press “Next”
On “Set Validity and Signature Algorithm for the Certificate” leave defaults
Click “Next >”
On “Generated Certificate” press “Finish”
On “CSR Signed” Click “OK”.

Back in M-Vault Console:

Select “The CA has provided a certificate” and press “Next >”
On “User Certificate” leave defaults
Click “Next >”
On “Other Certificates” leave defaults
Click “Next >”
On “Finish directory servers Identity creation” leave defaults
Click “Finish”
On “Trust Root CA Certificate” dialogue click “Yes”
On “Configuration” tab press “Apply”

apply TLS identity



TLS (Transport Layer Security)

Management of identities and other configuration related to TLS.

The directory server can have one identity for each of the supported key types (RSA, DSA and ECDSA) which is stored in a passphrase-protected PKCS#12 file

Identity	Key Type
cn=DSA,ou=Red,o=Headquarters	RSA

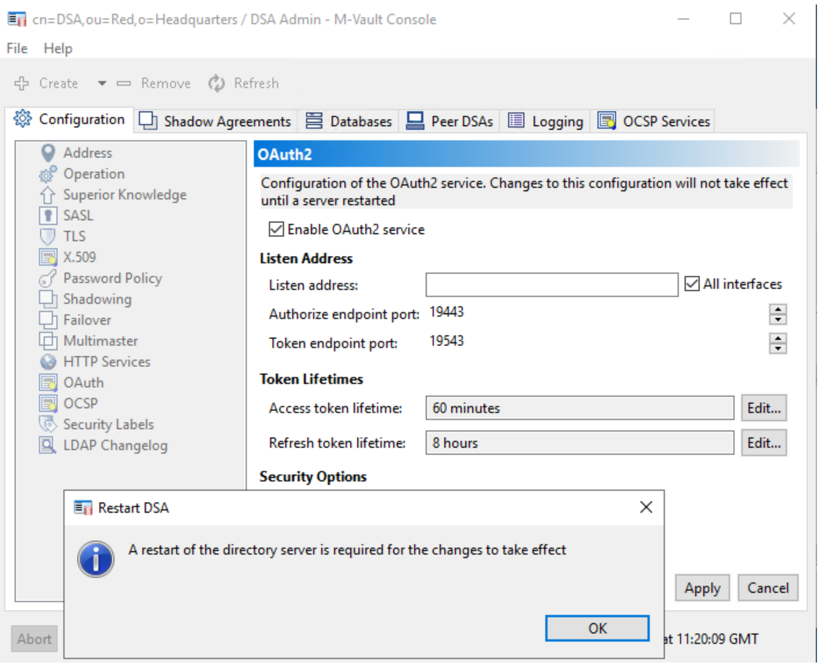
Session is bound for "cn=DSA,ou=Red,o=Headquarters". Last data refresh: 22 February 2022 at 11:02:48 GMT

Close M-Vault Console configuration dialogue
On “M-Vault Console” click “Stop”
Wait for the directory service to stop.
Select the “Managed Directory Server”
Click “Start”
On “Directory Server Started” click “Yes”

Configure M-Vault to Support OAuth

Select “OAuth”
Check “Enable OAuth2 service”
Press “Apply”
On “Restart DSA” press “OK”

enable OAuth2



Configuration of the OAuth2 service. Changes to this configuration will not take effect until a server restarted

☑ Enable OAuth2 service

Listen address: ☑ All interfaces
Authorize endpoint port: 19443
Token endpoint port: 19543

Access token lifetime: 60 minutes
Refresh token lifetime: 8 hours

A restart of the directory server is required for the changes to take effect

Close M-Vault Console configuration dialogue
On “M-Vault Console” click “Stop”
Wait for the directory service to stop.
Select the “Managed Directory Server”
Click “Start”
On “Directory Server Started” click “Yes”

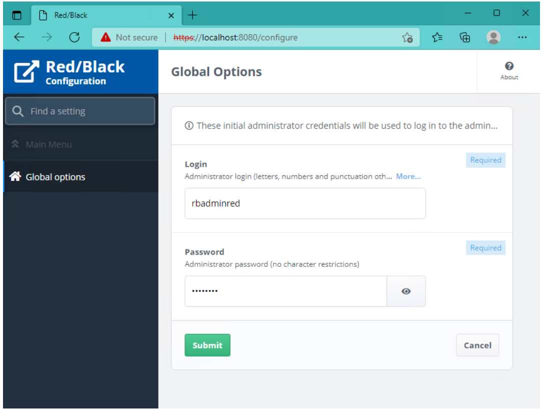
Configure Red/Black Server

On Windows, ensure the “Isode RedBlack server” service has started using the “Isode Service Configuration” tool

On Linux, after installing the package, enable and start the service by:
“systemctl enable redblack”
“systemctl start redblack”

If not already launched, browse to https://localhost:8080
The browser will warn of a security risk. Choose an option to override the warning.
In “Login” field type “rbadminred” [15]
In “Password” type “Secret1+”
Press “Submit”

configure Red/Black admin user



Red/Black

Not secure | ~~https~~://localhost:8080/configure

Red/Black Configuration

Global Options

Find a setting

Main Menu

Global options

These initial administrator credentials will be used to log in to the admin...

Login Required
Administrator login (letters, numbers and punctuation oth... More...
rbadminred

Password Required
Administrator password (no character restrictions)
••••••••

Submit

Cancel

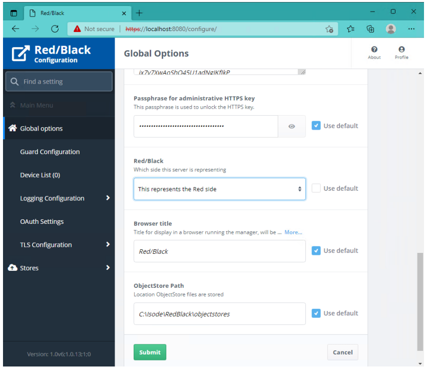
Configuration will occur and the application will log itself out.

Use the Isode Service Configuration tool to stop and start the “Isode RedBlack server” service. This will ensure that the product is correctly activated.

On the Red/Black login screen in “Username” type “rbadminred” [15]
In “Password” type “Secret1+”
Click “Login”

Scroll down the “Global options”

configure side



Red/Black — https://localhost:8080/configure/

Global Options

ix7v7XwAoShO45U1adNgIKfIkP

Passphrase for administrative HTTPS key
This passphrase is used to unlock the HTTPS key.
•••••••••••••••••••••••••••••••• ☑ Use default

Red/Black
Which side this server is representing
This represents the Red side ☐ Use default

Browser title
Title for display in a browser running the manager, will be ... More...
Red/Black ☑ Use default

ObjectStore Path
Location ObjectStore files are stored
C:\Isode\RedBlack\objectstores ☑ Use default

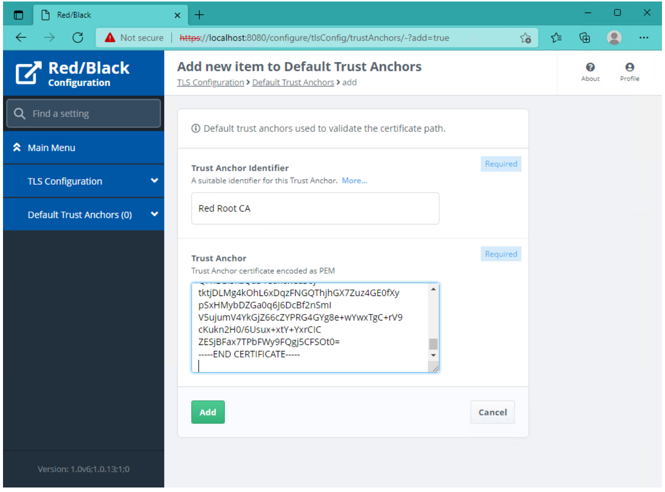
In “Red/Black” Select “This represents the Red Side” [16]

Press “Submit”

Configure Red/Black for TLS

Select “TLS Configuration”
Select “Default Trust Anchors”
Press “Add”

configure default trust anchor



Red/Black — https://localhost:8080/configure/tlsConfig/trustAnchors/-?add=true

Add new item to Default Trust Anchors
TLS Configuration › Default Trust Anchors › add

ⓘ Default trust anchors used to validate the certificate path.

Trust Anchor Identifier — Required
A suitable identifier for this Trust Anchor. More...
Red Root CA

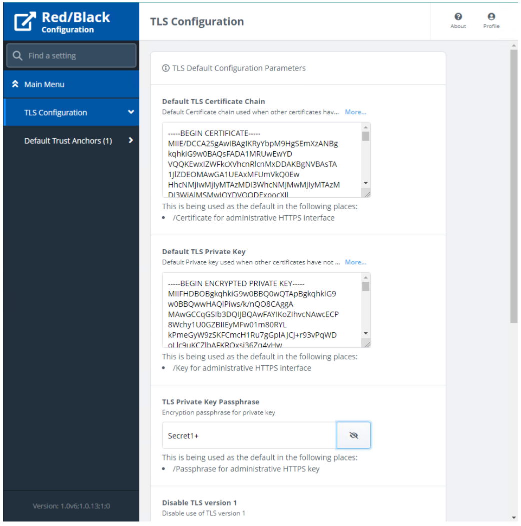
Trust Anchor — Required
Trust Anchor certificate encoded as PEM

```
tktjDLMg4kOhL6xDqzFNGQThjhGX7Zuz4GE0fXy
pSxHMybDZGa0q6J6DcBf2nSmI
V5ujumV4YkGjZ66cZYPRG4GYg8e+wYwxTgC+rV9
cKukn2H0/6Usux+xtY+YxrCIC
ZESjBFax7TPbFWy9FQgj5CFSOt0=
-----END CERTIFICATE-----
```

In “Trust Anchor Identifier” type “Red Root CA” [20]
In “Trust Anchor” field paste the contents of the file “C:\IsodeCerts\RedRootCert.pem” [10]
(Linux: “/var/isode/certs/RedRootCert.pem” [10])
Press “Add”

Select “TLS Configuration”

Red/Black TLS configuration



TLS Default Configuration Parameters

Default TLS Certificate Chain
Default Certificate chain used when other certificates hav... More...

```
-----BEGIN CERTIFICATE-----
MIIE/DCCA2SgAwIBAgIKRyYbpM9HgSEmXzANBg
kqhkiG9w0BAQsFADA1MRUwEwYD
VQQKEwxIZWFkcXVhcnRlcnMxDDAKBgNVBAsTA
1JlZDEOMAwGA1UEAxMFUmVkQ0Ew
HhcNMjIwMjIyMTAzMDI3WhcNMjMwMjIyMTAzM
DI3WjAlMSMwIQYDVQQDExpocXIl
```

This is being used as the default in the following places:
- /Certificate for administrative HTTPS interface

Default TLS Private Key
Default Private key used when other certificates have not ... More...

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9
w0BBQwwHAQIPiws/k/nQO8CAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECP
8Wchy1U0GZBIIEyMFw01m80RYL
kPmeGyW9zSKFCmcH1Ru7gGpIAJCJ+r93vPqWD
oLlc9uKCZlbAFKROxsi36Zq4vHw
```

This is being used as the default in the following places:
- /Key for administrative HTTPS interface

TLS Private Key Passphrase
Encryption passphrase for private key

Secret1+

This is being used as the default in the following places:
- /Passphrase for administrative HTTPS key

Disable TLS version 1
Disable use of TLS version 1

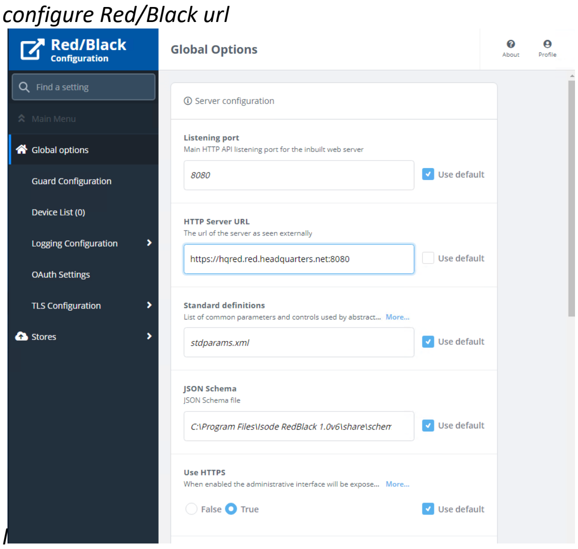
Delete the contents of the field “Default TLS Certificate Chain_”
Paste the contents of the file “C\IsodeCerts\hqredcert_Chain.pem” [13] into the field “Default TLS Certificate Chain” (Linux: “/var/isode/certs/hqredcert_Chain.pem” [13])
Delete the contents of the field “Default TLS Private Key”
Paste the contents of the file “C:\IsodeCerts\redencryptedkey.pem” [19] into the field “Default TLS Private Key” (Linux : “/var/isode/certs/redencryptedkey.pem”)
In the field “TLS Private Key Password” type “Secret1+”

Press “Submit”

If you are presented with a warning “Failed to Fetch”, refresh the page in the browser and try again.

Select “Main Menu” in the left-hand pane.

configure Red/Black url



Server configuration

Listening port
Main HTTP API listening port for the inbuilt web server
8080 ☑ Use default

HTTP Server URL
The url of the server as seen externally
https://hqred.red.headquarters.net:8080 □ Use default

Standard definitions
List of common parameters and controls used by abstract... More...
stdparams.xml ☑ Use default

JSON Schema
JSON Schema file
C:\Program Files\Isode RedBlack 1.0v6\share\schem ☑ Use default

Use HTTPS
When enabled the administrative interface will be expose... More...
○ False ● True ☑ Use default

In “HTTP Server URL” enter https://hqred.red.headquarters.net:8080 [21]
For “Use HTTPS” select “True”
Press “Submit”

Stop and Start the “Isode RedBlack server” using the “Isode Service Configuration” tool
(Linux: “systemctl restart redblack”)

It should now be possible to manage the product by browsing to the url “https://hqred.red.headquarters.net:8080” [21]

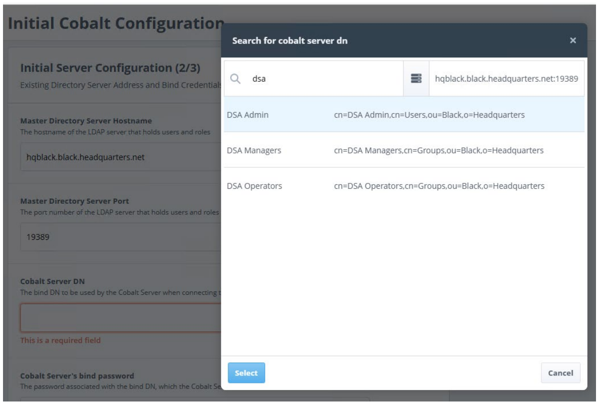
Install and configure Cobalt

On Windows, ensure the “Isode Cobalt server” service has started using the “Isode Service Configuration” tool.

On Linux, after installing the package, enable and start the service by:
“systemctl enable cobalt”
“systemctl start cobalt”

Browse to “https://localhost:8001”.
The browser will warn of a security risk. Choose an option to override the warning.
The “Initial Cobalt Configuration 1/3” page will be launched.
Ensure “Use an existing directory server” is checked and press “Next”.
The “Initial Cobalt Configuration 2/3” page will be launched.
In the “Master Directory Server Hostname” type “hqred.red.headquarters.net” [22]
Press “Choose” to the right of “Cobalt Server DN”

select Cobalt admin



Initial Cobalt Configuration

Initial Server Configuration (2/3)
Existing Directory Server Address and Bind Credentials

Master Directory Server Hostname
The hostname of the LDAP server that holds users and roles
hqblack.black.headquarters.net

Master Directory Server Port
The port number of the LDAP server that holds users and roles
19389

Cobalt Server DN
The bind DN to be used by the Cobalt Server when connecting t
This is a required field

Cobalt Server's bind password
The password associated with the bind DN, which the Cobalt Se

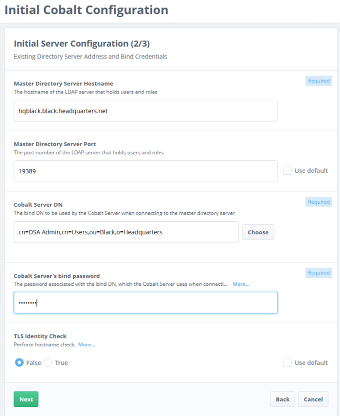
Search for cobalt server dn

dsa | hqblack.black.headquarters.net:19389

DSA Admin	cn=DSA Admin,cn=Users,ou=Black,o=Headquarters
DSA Managers	cn=DSA Managers,cn=Groups,ou=Black,o=Headquarters
DSA Operators	cn=DSA Operators,cn=Groups,ou=Black,o=Headquarters

In the “Search” field, type “DSA” and Select “DSA Admin”
Press “Select”

initial Cobalt server configuration



Initial Cobalt Configuration

Initial Server Configuration (2/3)
Existing Directory Server Address and Bind Credentials

Master Directory Server Hostname (Required)
The hostname of the LDAP server that holds users and roles
hqblack.black.headquarters.net

Master Directory Server Port
The port number of the LDAP server that holds users and roles
19389 □ Use default

Cobalt Server DN (Required)
The bind DN to be used by the Cobalt Server when connecting to the master directory server
cn=DSA Admin,cn=Users,ou=Black,o=Headquarters

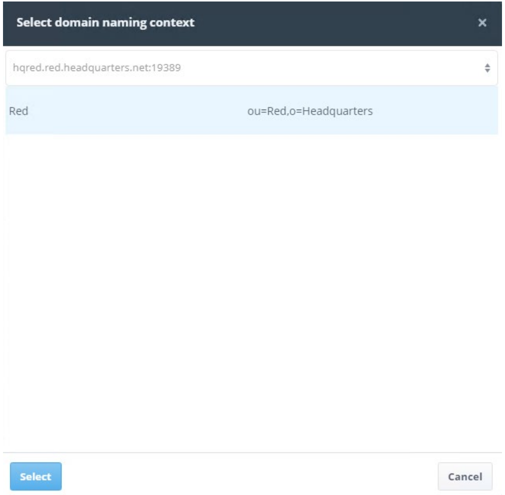
Cobalt Server's bind password (Required)
The password associated with the bind DN, which the Cobalt Server uses when connecti... More...
••••••••

TLS Identity Check
Perform hostname check. More...
● False ○ True □ Use default

In the “Cobalt Server’s bind password” field type “Secret1+”
Under “TLS Identity Check”, select “False”.
Press “Next”

In “Domain” type “red.headquarters.net” [23]
In “Admin’s Full Name” Type “Cobalt Admin”
In “Admin’s password” type “Secret1+”
To the right of “Domain Naming Context” press “Choose”

select Cobalt domain naming context

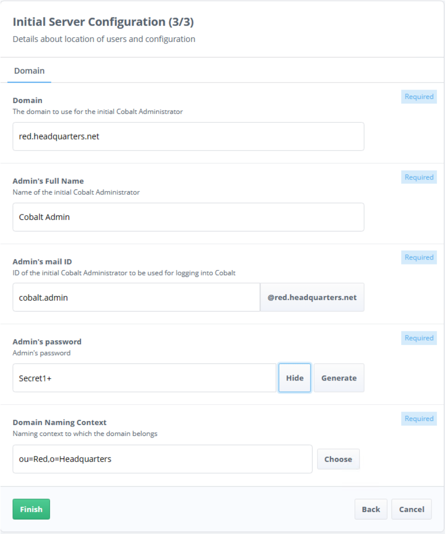

Select domain naming context

hqred.red.headquarters.net:19389

Red	ou=Red,o=Headquarters

On “Select domain naming context” select “ou=Red,o=Headquarters” [4]
Press “Select”

initial Cobalt configuration


Initial Server Configuration (3/3)
Details about location of users and configuration

Domain

Domain (Required)
The domain to use for the initial Cobalt Administrator
red.headquarters.net

Admin's Full Name (Required)
Name of the initial Cobalt Administrator
Cobalt Admin

Admin's mail ID (Required)
ID of the initial Cobalt Administrator to be used for logging into Cobalt
cobalt.admin @red.headquarters.net

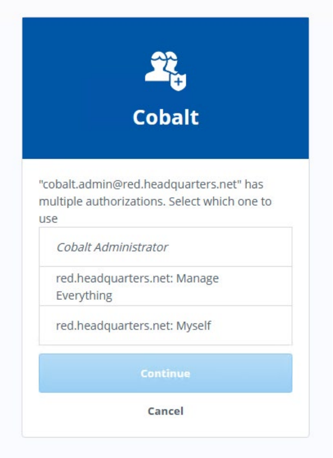
Admin's password (Required)
Admin's password
Secret1+

Domain Naming Context (Required)
Naming context to which the domain belongs
ou=Red,o=Headquarters

Press “Finish”

You will be redirected back to the Cobalt Login Screen.
In “Username” type cobalt.admin@red.headquarters.net [24]
In “Password” type “Secret1+”
Press “Login”

select Cobalt admin view

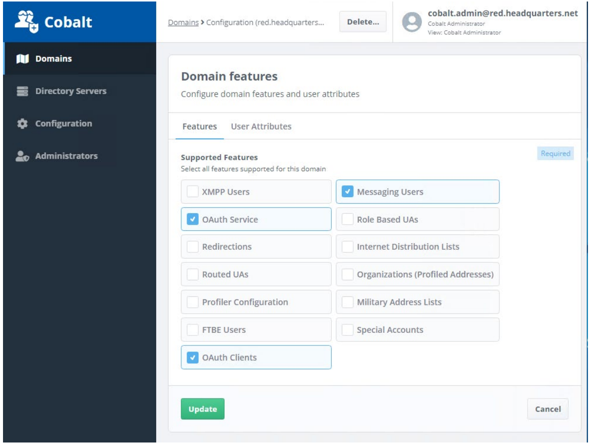


"cobalt.admin@red.headquarters.net" has multiple authorizations. Select which one to use

- *Cobalt Administrator*
- red.headquarters.net: Manage Everything
- red.headquarters.net: Myself

Select "Cobalt Administrator"
Press "Continue"
Press "Features"

select Cobalt features



Domain features

Configure domain features and user attributes

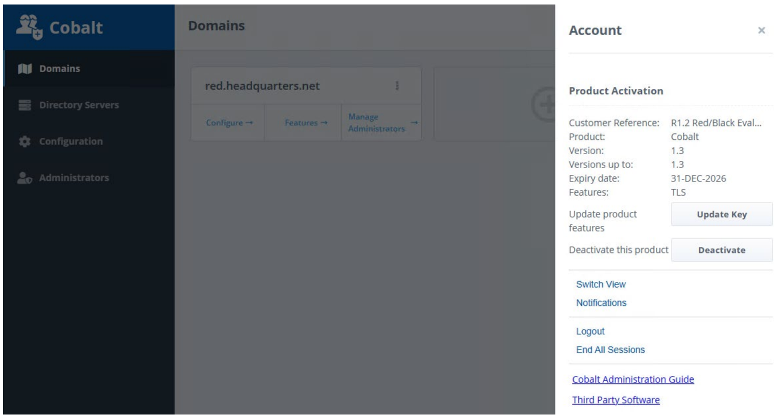
Supported Features

Select all features supported for this domain

□ XMPP Users	☑ Messaging Users
☑ OAuth Service	□ Role Based UAs
□ Redirections	□ Internet Distribution Lists
□ Routed UAs	□ Organizations (Profiled Addresses)
□ Profiler Configuration	□ Military Address Lists
□ FTBE Users	□ Special Accounts
☑ OAuth Clients	

Uncheck "XMPP Users"
Check "OAuth Service" and "OAuth Clients"
Press "Update"
In the top right hand corner press "cobalt.admin@red.headquarters.net" [24]

switch Cobalt view

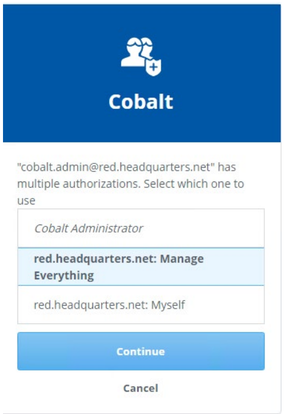


Product Activation

Customer Reference:	R1.2 Red/Black Eval...
Product:	Cobalt
Version:	1.3
Versions up to:	1.3
Expiry date:	31-DEC-2026
Features:	TLS
Update product features	Update Key
Deactivate this product	Deactivate

Press "Switch View"

select red.headquarters.net [23] *view*



Cobalt

"cobalt.admin@red.headquarters.net" has multiple authorizations. Select which one to use

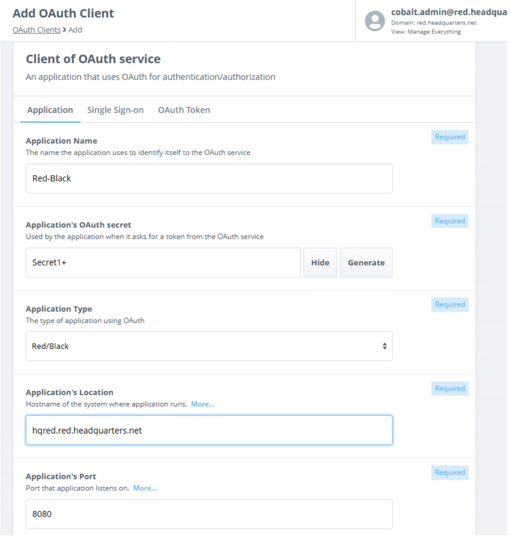
Cobalt Administrator
red.headquarters.net: Manage Everything
red.headquarters.net: Myself
Continue
Cancel

Select “red.headquarters.net[23]:Manage Everything”
Press “Continue”

Configure OAuth in Cobalt

Select “OAuth Clients”
Press “Add”

configure OAuth client



Add OAuth Client

OAuth Clients > Add

cobalt.admin@red.headqua
Domain: red.headquarters.net
View: Manage Everything

Client of OAuth service

An application that uses OAuth for authentication/authorization

Application Name
The name the application uses to identify itself to the OAuth service
Red-Black

Application's OAuth secret
Used by the application when it asks for a token from the OAuth service
Secret1+

Application Type
The type of application using OAuth
Red/Black

Application's Location
Hostname of the system where application runs. More...
hqred.red.headquarters.net

Application's Port
Port that application listens on. More...
8080

In “Application Name” type “Red-Black”
In “Application’s OAuth secret” type “Secret1+”
In “Application Type” Select “Red/Black”
In “Application’s Location” ensure “hqred.red.headquarters.net” [26]

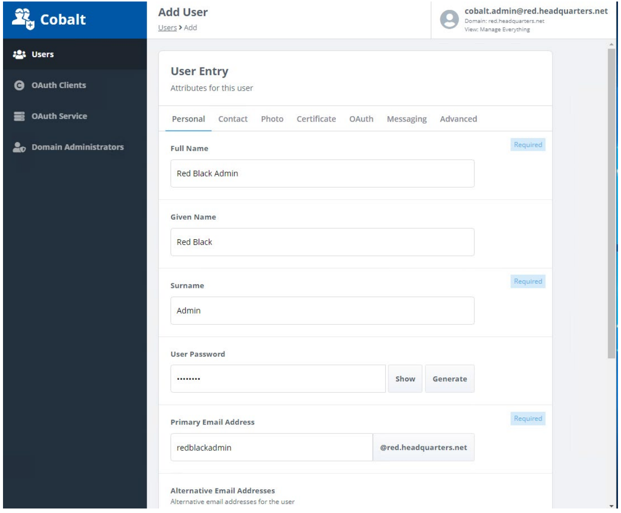
Copy the “Redirect URI” to a text file for later use

Press “Add”

Create the Red/Black Admin User in Cobalt

Select “Users”
Press “Add”

Configure Red/ Black Admin User



Add User
Users > Add

cobalt.admin@red.headquarters.net
Domain: red.headquarters.net
View: Manage Everything

User Entry
Attributes for this user

Full Name: Red Black Admin

Given Name: Red Black

Surname: Admin

User Password: ••••••••

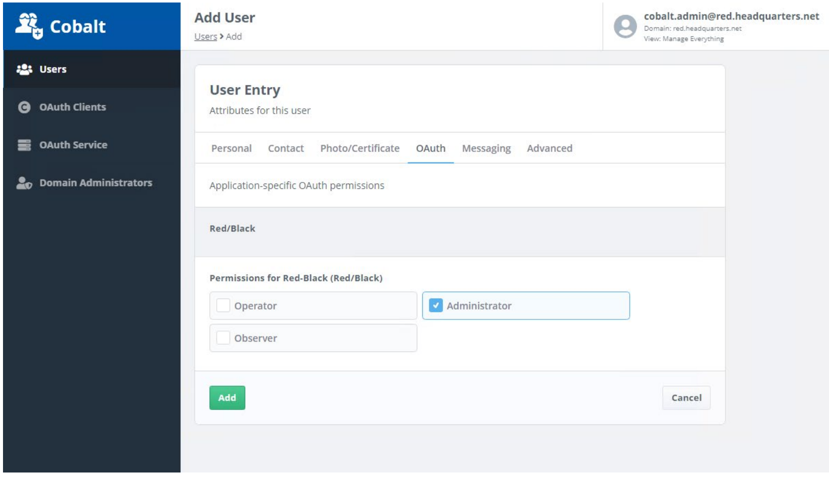
Primary Email Address: redblackadmin @red.headquarters.net

Alternative Email Addresses
Alternative email addresses for the user

In “Full Name” type “Red Black Admin”
In “User Password” type “Secret1+”
Change “Primary Email Address” to “redblackadmin”

Change to “OAuth” tab

Add Red/Black Admin user



Add User
Users > Add

cobalt.admin@red.headquarters.net
Domain: red.headquarters.net
View: Manage Everything

User Entry
Attributes for this user

Application-specific OAuth permissions

Red/Black

Permissions for Red-Black (Red/Black)

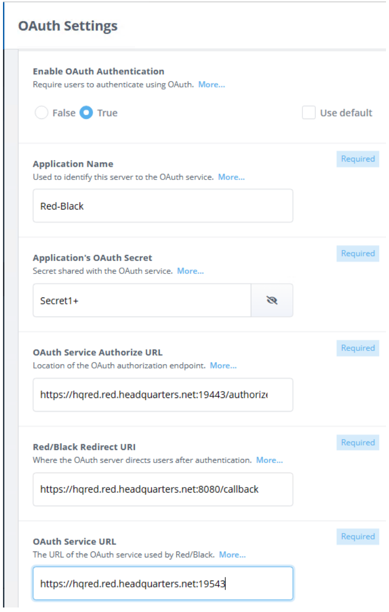
☐ Operator ☑ Administrator
☐ Observer

Check “Administrator”
Press “Add”

Configure Red/Black to Use OAuth

Return to “Red/Black Configuration” in the browser
You may need to log back in.
Select “OAuth Settings”
Set “Enable OAuth Authentication” to “True”

configure Red/Black OAuth



OAuth Settings

Enable OAuth Authentication
Require users to authenticate using OAuth. More...
○ False ● True □ Use default

Application Name Required
Used to identify this server to the OAuth service. More...
Red-Black

Application's OAuth Secret Required
Secret shared with the OAuth service. More...
Secret1+

OAuth Service Authorize URL Required
Location of the OAuth authorization endpoint. More...
https://hqred.red.headquarters.net:19443/authorize

Red/Black Redirect URI Required
Where the OAuth server directs users after authentication. More...
https://hqred.red.headquarters.net:8080/callback

OAuth Service URL Required
The URL of the OAuth service used by Red/Black. More...
https://hqred.red.headquarters.net:19543

In “Application Name” type “Red-Black”
In “Application’s OAuth Secret” type “Secret1+”
In the “OAuth Service Authorize URL” enter “https://hqred.red.headquarters.net:19443/authorize”[27]
In “Red/Black Redirect URI” paste the value previously saved from Cobalt
In the “OAuth Service URL” enter “https://hqred.red.headquarters.net:19543 [28]

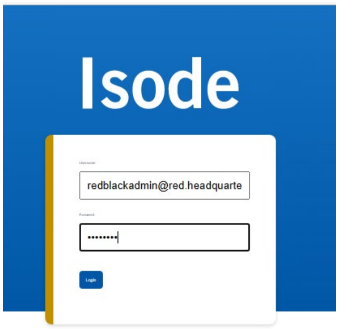
Press “Submit”

In the top right-hand corner of the page, press “Profile”
Press “Logout”

Continue Configuring Red/Black Authenticating Using OAuth

Browse to https://hqred.red.headquarters.net:8080/ [21]

login to Red/Black using OAuth

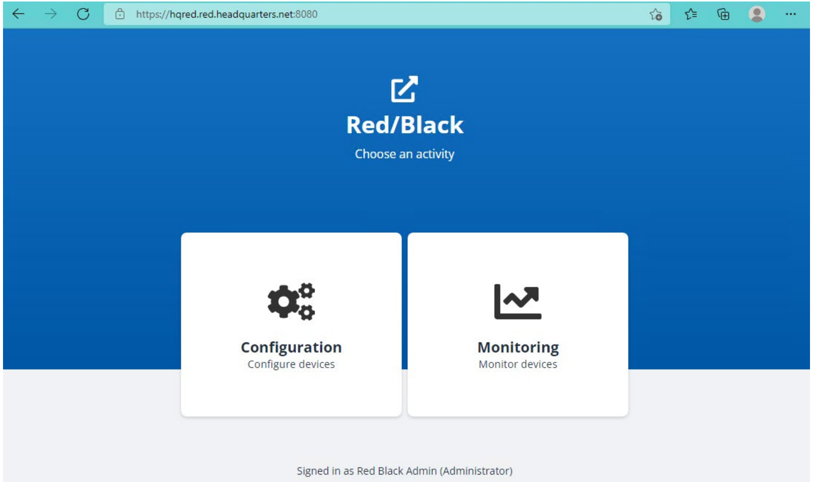


redblackadmin@red.headquarte

••••••••

In “User” type “redblackadmin@red.headquarters.net” 29
In “Password” type “Secret1+”
Press “Login”

select Red/Black configuration

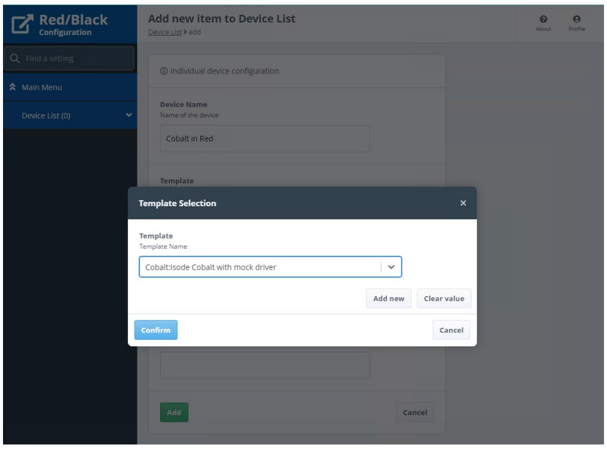


https://hqred.red.headquarters.net:8080

Signed in as Red Black Admin (Administrator)

Press “Configuration”
Select “Device List” [30]
Press “Add”
In “Device Name” type “M-Switch in Red”
Press “Edit”

add device



Add new item to Device List

Device List > add

Individual device configuration

Device Name
Name of the device
Cobalt in Red

Template Selection

Template
Template Name
Cobalt:Isode Cobalt with mock driver

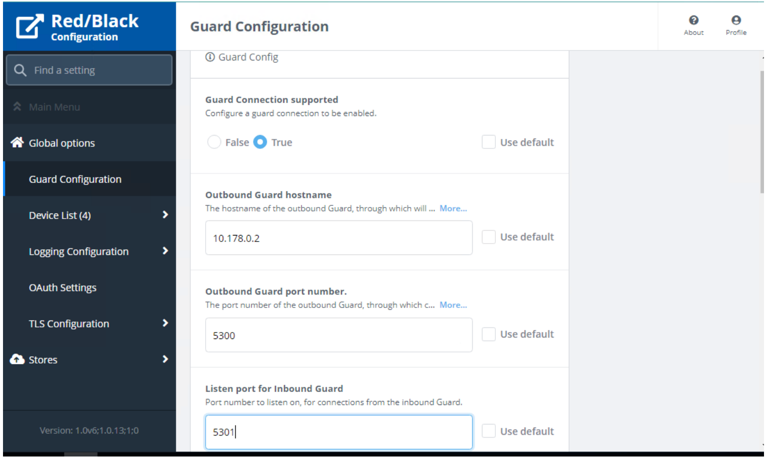
In “Template Selection” Select “MSwitch:Isode M-Switch Server”
Press “Confirm”
Press “Add”
Press “Add Another”
Repeat for the following name/template pairs:

Name : Harrier in Red
Template : Harrier:Isode Harrier Server
Name : Icon-5066 in Red
Template : Icon5066 : Isode Icon-5066 Server
Name : Icon-PEP in Red
Template: IconPEP:Isode Icon-PEP Server
Name : M-Guard
Template: MGuard:Represents a single M-Guard Guard

Configure Red/Black for Guard

Select “Main Menu”
Select “Guard Configuration”

Red/Black guard connection



Guard Configuration

Guard Config

Guard Connection supported
Configure a guard connection to be enabled.
○ False ● True □ Use default

Outbound Guard hostname
The hostname of the outbound Guard, through which will ... More...
10.178.0.2 □ Use default

Outbound Guard port number.
The port number of the outbound Guard, through which c... More...
5300 □ Use default

Listen port for Inbound Guard
Port number to listen on, for connections from the inbound Guard.
5301 □ Use default

Set “Guard Connection Supported” to “True”
In “Outbound Guard Hostname” type “10.178.0.2” [31]

In “Outbound Guard port Number” type “5300” [32]
In “Listen Port for Inbound Guard” type “5301” [33]
Press “Submit”

Setting Up the Black Side

Follow the above steps for the red side changing the data marked like ^{this} with that referenced in Appendix A.

Copy the “C:\Isode\Certs\BlackRootCert.pem” on hqblack to the same directory on hqred (Linux : ”/opt/isode/certs”)

Set up the M Guard Appliance on Hyper-V

Use the “M-Guard Evaluation guide” for guidance to set up the M-Guard Appliance by following the section “Installation on Hyper-V”.

Follow the instructions for “Installation on Hyper-V”

Follow the guide notes modifying with the following information:

On the new M-Guard virtual machine, change the Virtual switch mapped to your first Network adaptor from “M-Guard Management” to the Virtual Switch currently mapped to your Red/Black machines. This is probably your local network.
Copy the M-Guard console software (folder mgc-x.y.z) to c:\on the machine “hqred” (Linux : “/opt/isode”)
Rename the folder “M-GuardConsole”
Create the Folder “C:\M-GuardConsole\M-GuardEval” (Linux: “/opt/isode/M-GuardConsole/M-GuardEval”)
Complete the section “Configuring the M-Guard Appliance with M-Guard Console (Part 1)” using the software in “c:\M-GuardConsole (Linux:” /opt/isode/M-GuardConsole”).
Place the project in C:\M-Guard Console\M-Guard Eval. (Linux: “/opt/isode/M-GuardConsole/M-GuardEval”)
Name the project “Red Black Guard”
Place the ssh keys in C:\M-Guard Console\M-Guard Eval (Linux: “/opt/isode/M-GuardConsole/M-GuardEval”)
In the comment field use rbadminred@red.headquarters.net
For the password use “Secret1+”
When Adding Appliance use the Name: “Red Black Guard”
After logging in, change password to “Secret1+”

Follow The Instructions for “Configuring the Appliance”

Use the suggested host name for the guard: eval.guard.net

Configure Guard Networks

Associate the Second NIC on the Guard Virtual Machine with the Red Network
Associate the third NIC on the Guard Virtual Machine with the Black Network
Associate the second NIC on “hqred.red.headquarters.net” with the Red Network and configure the suggested IP address (see table).
Associate the second NIC on “hqblack.black.headquarters.net” with the Black Network and configure the suggested IP address (see table).
Repeat the step in “Configuring the appliance” that sets the ip address for guard interface hn0 for guard interface hn1 and hn2. Use the table to select ip addresses.

Configure the M-Guard Appliance (Part 2)

Follow the M-Guard Evaluation Guide section “Configuring the M-Guard Appliance with M-Guard Console (Part 2)”

Save the file “mguard_csr” in “C:\IsodeCerts”

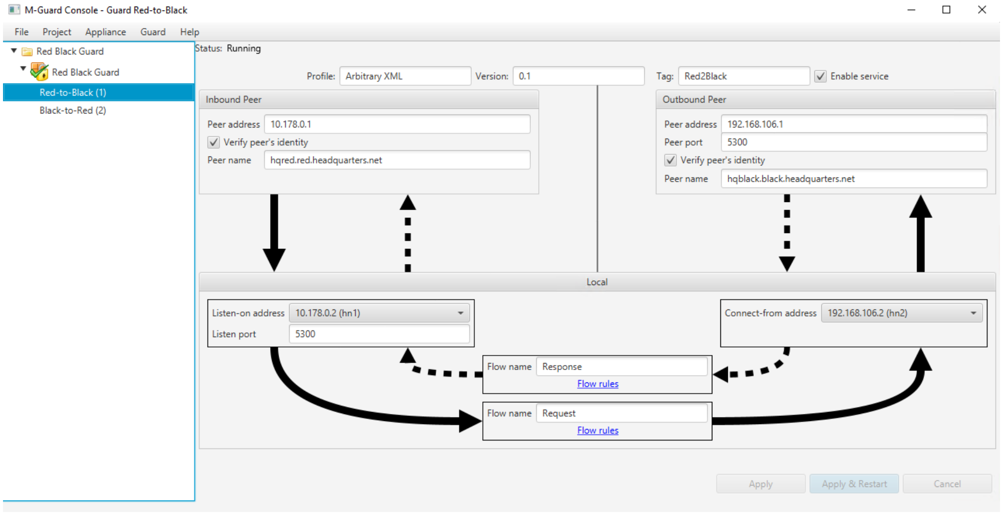
Note that on the “Generated Certificate” dialogue, the “Export to Disk” option should be set to “Write Certificate chain in PEM format”.

Add the two guard instances as described substituting the following information:

Data for Red to Black Guard:

Name: Red-to-Black
GXCP Application Profile: Arbitrary XML
Allow GXCP responses in response flow
Tag: Red2Black
Inbound peer address: 10.178.0.1
Inbound peer name: hqred.red.headquarters.net
Inbound “Listen-on address”: 10.178.0.2 (hn1)
Inbound “Listen Port”: 5300
Outbound Peer IP address: 192.168.106.1
Outbound Peer Port: 5300
Outbound Peer name: “hqblack.black.headquarters.net”
Outbound Peer “Connect From Address”: 192.168.106.2 (hn2)
Enable the Service

Red to Black guard configuration



Status: Running

Profile: Arbitrary XML
Version: 0.1
Tag: Red2Black
☑ Enable service

Inbound Peer
Peer address: 10.178.0.1
☑ Verify peer's identity
Peer name: hqred.red.headquarters.net

Outbound Peer
Peer address: 192.168.106.1
Peer port: 5300
☑ Verify peer's identity
Peer name: hqblack.black.headquarters.net

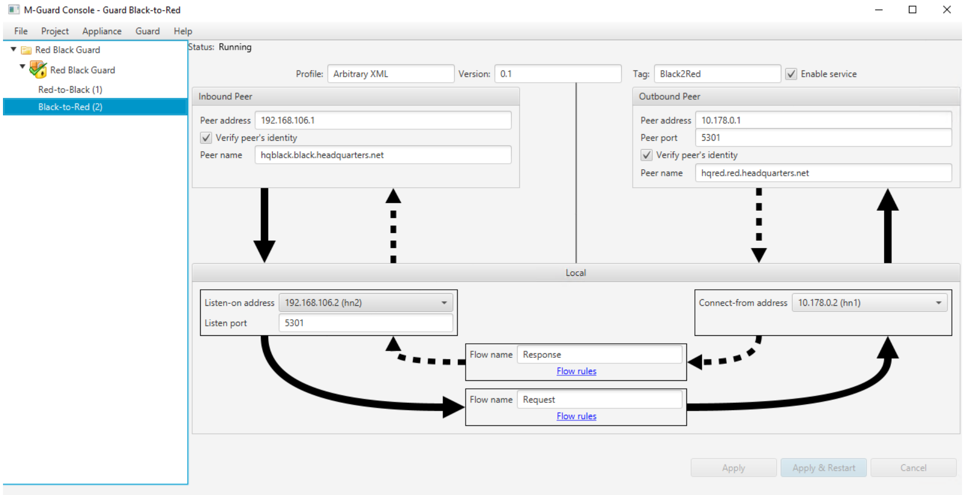
Local
Listen-on address: 10.178.0.2 (hn1)
Listen port: 5300
Connect-from address: 192.168.106.2 (hn2)
Flow name: Response
Flow name: Request

Data for Black to Red Guard :

Name: Black-to-Red
GXCP Application Profile: Arbitrary XML
Allow GXCP responses in response flow
Tag: Black2Red
Inbound peer address: 192.168.106.1

Inbound peer name: hqblack.black.headquarters.net
Inbound “Listen-on address”: 192.168.106.2 (hn2)
Inbound “Listen Port”: 5301
Outbound Peer IP address: 10.178.0.1
Outbound Peer Port: 5301
Peer name: “hqred.red.headquarters.net”
Outbound Peer “Connect From Address”: 10.178.0.2 (hn1)
Enable Service

Black to Red guard configuration



M-Guard Console - Guard Black-to-Red

Status: Running

Profile: Arbitrary XML
Version: 0.1
Tag: Black2Red
☑ Enable service

Inbound Peer
Peer address: 192.168.106.1
☑ Verify peer's identity
Peer name: hqblack.black.headquarters.net

Outbound Peer
Peer address: 10.178.0.1
Peer port: 5301
☑ Verify peer's identity
Peer name: hqred.red.headquarters.net

Local
Listen-on address: 192.168.106.2 (hn2)
Listen port: 5301
Connect-from address: 10.178.0.2 (hn1)
Flow name: Response
Flow name: Request

Configure ports in Firewall …

Select Appliance/Setup/Configure Firewall
In GXCP Ports, add two values comma separated: “5300,5301”
Press “OK”

In the M-Guard Console:

Select “Appliance/Setup/Load TLS Trust Anchor”
Browse to “c:\Isode\Certs\BlackRootCert.pem” (Linux: ”/opt/isode/certs/BlackRootCert.pem”)
On “Trust Anchor Successfully Uploaded” press “OK”
Select “Appliance/Save Configuration ..”
On “Confirmation” press “OK”
On “The appliance returned the following:” press “Close”

Configure Syslog Logging

Download and install “Visual Syslog server” to hqred.red.headquarters.net
Follow the section for “Configure Syslog Logging”
The option is now called “Remote Logging”
Selector: daemon.*
Protocol/Transport: syslogOverTcp
Logging server address: 10.178.0.1
Logging Server Port: 514
Press “Save”

Select “Appliance/Save Configuration ..”
On “Confirmation” press “OK”
On “The appliance returned the following:” press “Close”

Explore Services With Red/Black

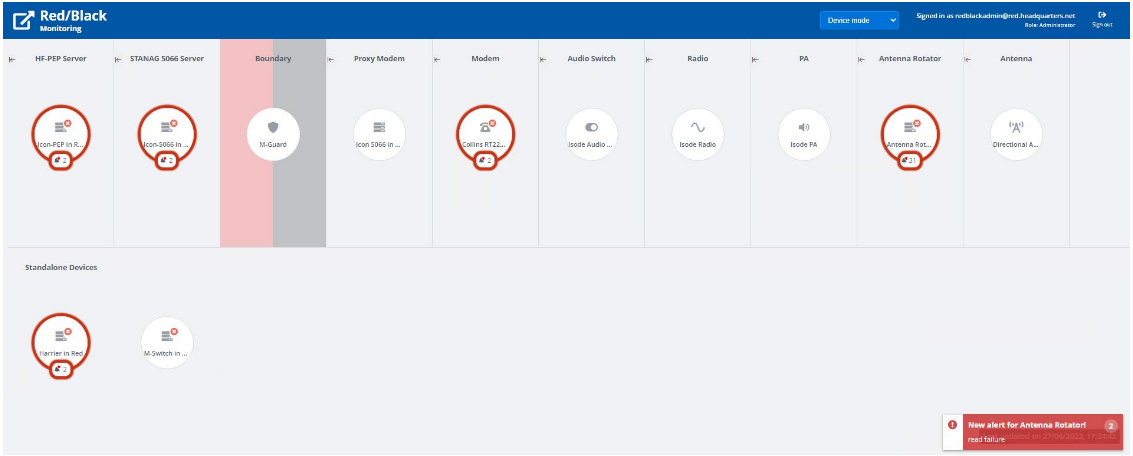
You have now completed the configuration of the simple Red/Black environment.

In order to use the product …

Browse to “https://hqred.red.headquarters.net:8080/”
In “User” type “redblackadmin@red.headquarters.net”
In “Password” type “Secret1+”

Press “Monitoring”

monitor Red/Black



Signed in as redblackadmin@red.headquarters.net
Role: Administrator

New alert for Antenna Rotator!
read failure
Last updated on 27/06/2023, 17:24:42

Appendix A - A list of substitutions for Black

1. Machine Name: hqblack
2. Primary DNS suffix: black.headquarters.net
3. Product activation reference: “Red/Black Evaluation – Black Server”
4. Base DN: ou=Black,o=Headquarters
5. Hostname: hqblack.black.headquarters.net
6. Bind DN: “cn=DSA Admin,CN=Users,ou=Black,o=Headquarters”
7. CA Location: ou=Black,o=Headquarters
8. CA RDN: BlackCA
9. Root CA DN: cn=BlackCA,ou=Black,o=Headquarters
10. Root Cert Name: BlackRootCert.pem
11. To Create a Certificate on Windows: “ "C:\program files\isode\bin\isode_openssl" req -new -out hqblackcert.csr -subj /CN=hqblack.black.headquarters.net/ -addext "subjectAltName=DNS:hqblack.black.headquarters.net" -keyout blackencryptedkey.pem -keyform pem “
12. To Create a Certificate on Linux: "/opt/isode/bin/isode_openssl" req -new -out hqblackcert.csr -subj /CN=hqblack.black.headquarters.net/ -addext "subjectAltName=DNS:hqblack.black.headquarters.net" -keyout blackencryptedkey.pem -keyform pem
13. Certificate Chain Filename: “c:\IsodeCerts\hqblackcert_cert_Chain.pem”
14. Certificate File name: “c:\IsodeCerts\hqblackcert_cert.pem”
15. Red Black admin: rbadminblack
16. Red Black side: “This represents the Black side”
17. Name of the windows certificate file: “C:\IsodeCerts\hqblackcert.pem”
18. Name of the linux certificate file: “/var/isode/certs/ hqblackcert.pem.pem”
19. Name of encrypted key name: file “C:\IsodeCerts\blackencryptedkey.pem”
20. Trust anchor identifier: Black Root CA
21. HTTP Server URL: “https://hqblack.black.headquarters.net:8080”
22. Cobalt Master directory server hostname: hqblack.black.headquarters.net
23. Initial cobalt operator domain: black.headquarters.net
24. Cobalt login id: cobalt.admin@black.headquarters.net
25. Oauth Server Name: Black HQ
26. Red Black Application Location: hqblack.black.headquarters.net
27. OAuth service URL: https://hqblack.black.headquarters.net:19443/authorize
28. OAuth Server Base URL: enter https://hqblack.black.headquarters.net:19543
29. Red Black admin user: redblackadmin@black.headquarters.net
30. 7 Device Name pairs to add:

Name: Collins RT2200A Modem
Device: CollinsRT2200A:Collins RT-2200A Modem
Name: Icon 5066 in Black
Device: Icon5066BlackSide:Icon-5066 Black Side
Name: Isode Audio Switch
Device: IsodeAudioSwitch:Audio Switch
Name: Isode PA
Device: IsodePA:Power Amplifier
Name: Antenna
Device: Antenna:An antenna placeholder

Name: Antenna Rotator

Device: IESAROTORPST71D:iessrl

Name: Isode Radio

Device: IsodeRadio:Basic Radio

31. Outbound guard hostname: 192.168.106.2

32. Outbound Guard Port Number: 5301

33. Listen port for Inbound Guard: 5300