



# Requirements & Install

Module 2 – Single Engine Installation

# Requirements



Requirement	Minimum	Optimum
Processor	Intel Core 2 @ 2GHz	Dual Processor Xeon 3.0 GHz
Memory	2 GB RAM	8 GB RAM
Disk Space	2 GB	5GB
Monitor Resolution	1024x768 resolution	1280x1024 resolution or higher
Operating System	Windows 2008 Server R2	Windows 2008 Server R2
Web Administration	Internet Explorer 8 Firefox 10 ESR	Internet Explorer 8 Firefox 10 ESR

# Requirements Continued



Requirement	Minimum	Optimum
	Install the following components from: Start Menu =>Administration Tools => Manage Server =>Add Server Roles	
<b>Operating System Component</b>	<ul style="list-style-type: none"><li>• IIS 7.5<sup>1</sup></li><li>• Network COM+ Access</li></ul>	<ul style="list-style-type: none"><li>• IIS 7.5<sup>1</sup></li><li>• Network COM+ Access</li></ul>
<b>.NET Framework</b>	.NET Framework 4.0	.NET Framework 4.5 (required for certificate enrollment with VeriSign) Director 8.0.1 required

<sup>1</sup>IIS 6 compatibility mode is required if you are provisioning to IIS 7 or IIS 7.5

# Database Requirements



Requirement	
Database Version	<ul style="list-style-type: none"><li>• Microsoft SQL Server 2008 and 2012</li><li>• Oracle 10g R2 or Oracle 11g R2</li></ul>
Oracle Client	<ul style="list-style-type: none"><li>• Oracle 11g Database Client with Oracle Data Access Components (ODAC) version 11.1.0.6.20</li></ul> <p>Note: For the Oracle 11g R2 client, you must install Patch 5 or higher (patch set 9966926)</p>
Database size	25 GB*

\*Database size requirements very greatly depending upon a number of different factors including log retention policy, number of certificates, number of Director servers, and licensing levels.

# Database Access



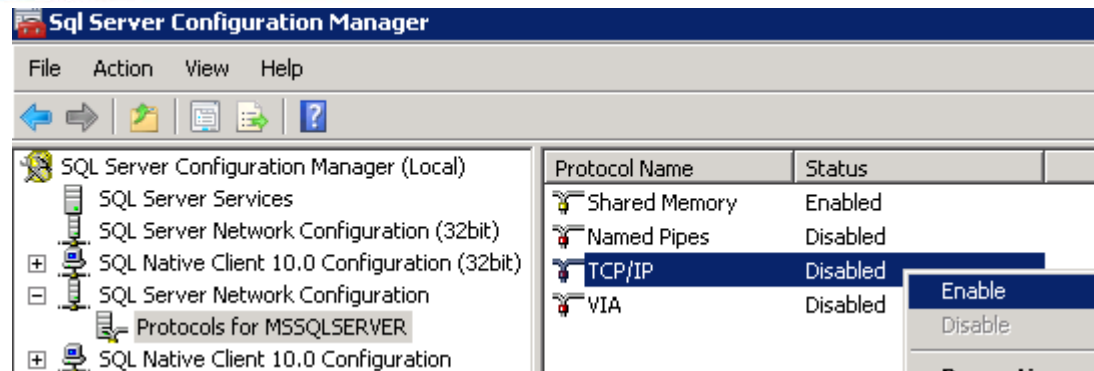
- For MSSQL, SQL Authentication and Windows Authentication are both supported
  - A dedicated account for Venafi Director SQL access is recommended
  - db\_datareader and db\_datawriter are the required permissions for Director to function properly after installation
- For Oracle, the database scripts provided with Director will create the database user account

# Database Setup



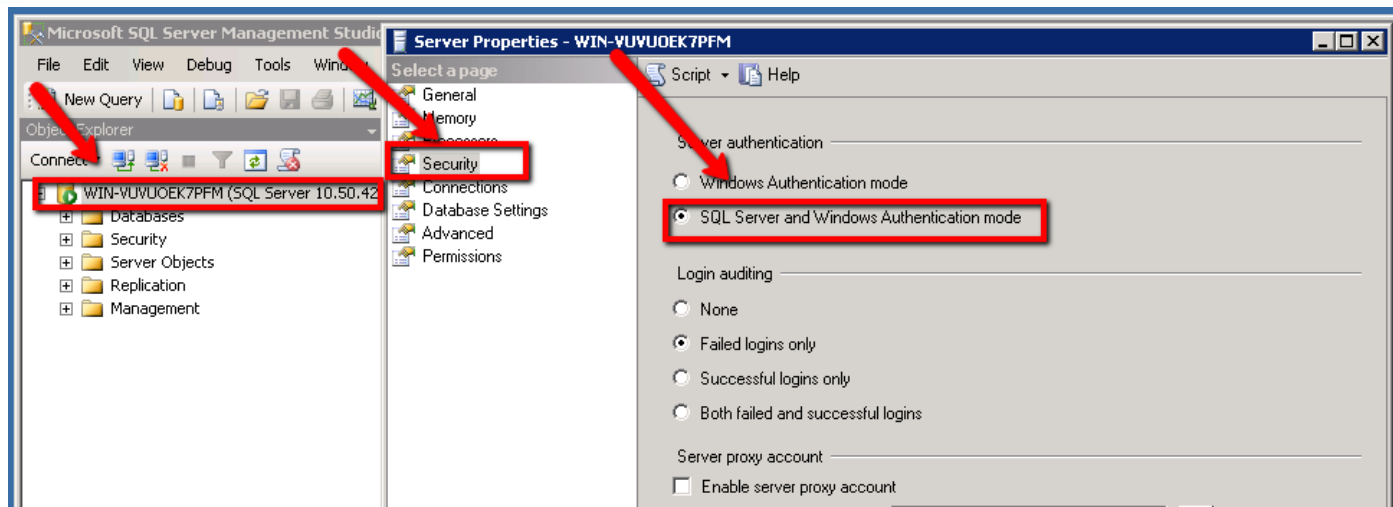
1. Enable TCP/IP Protocol for SQL Services (disabled by default but required)
2. Configure MS SQL for SQL Authentication (if desired)
3. Create Director Database
4. Create SQL login and assign rights
5. Run Database scripts to create tables and configure database

# Enable TCP/IP on MSSQL



1. Start SQL Server Configuration Manager. Click **Start**, point to **All Programs**, and click **Microsoft SQL Server**. Click **Configuration Tools**, and then click **SQL Server Configuration Manager**.
2. In SQL Server Configuration Manager, in the console pane, expand **SQL Server Network Configuration**.
3. In the console pane, click **Protocols for MSSQLSERVER**
4. In the details pane, right-click **TCP/IP**, and then click **Enable**.
5. Restart SQL Services

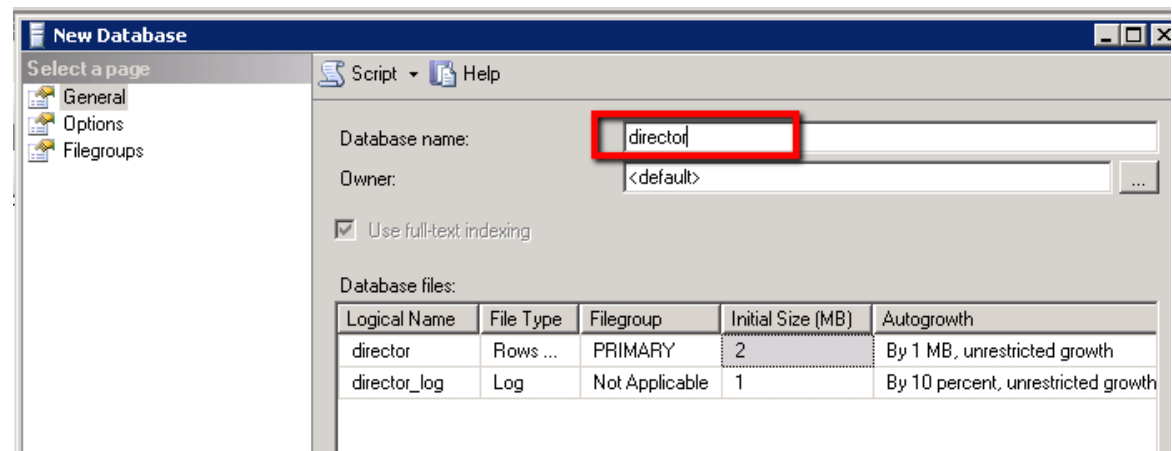
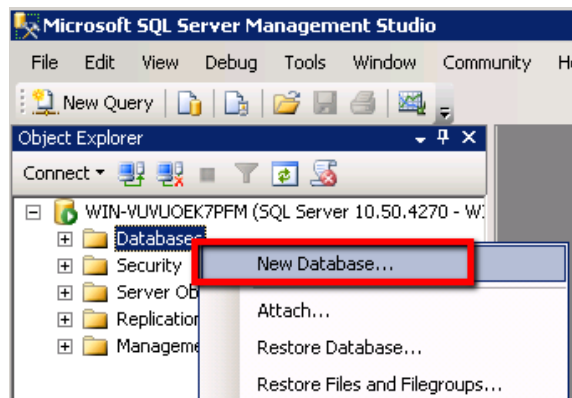
# Enable SQL Authentication



1. In SQL Server Management Studio Object Explorer, right-click the server, and then click **Properties**.
2. On the **Security** page, under **Server authentication**, select the new server authentication mode, and then click **OK**.
3. Restart SQL Services



# Create Director Database

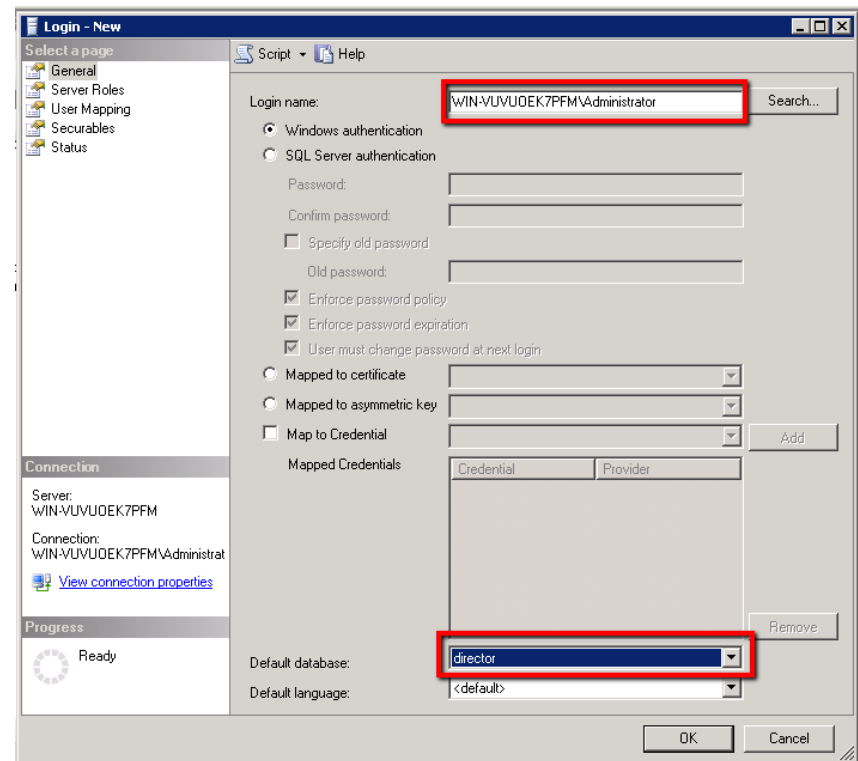
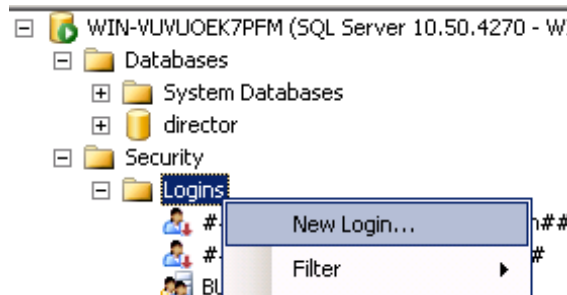


1. Right click on "Databases" and choose "New Database..."
2. Choose a name for the new database, for example "director"
3. Click "OK" on the New Databases dialog.

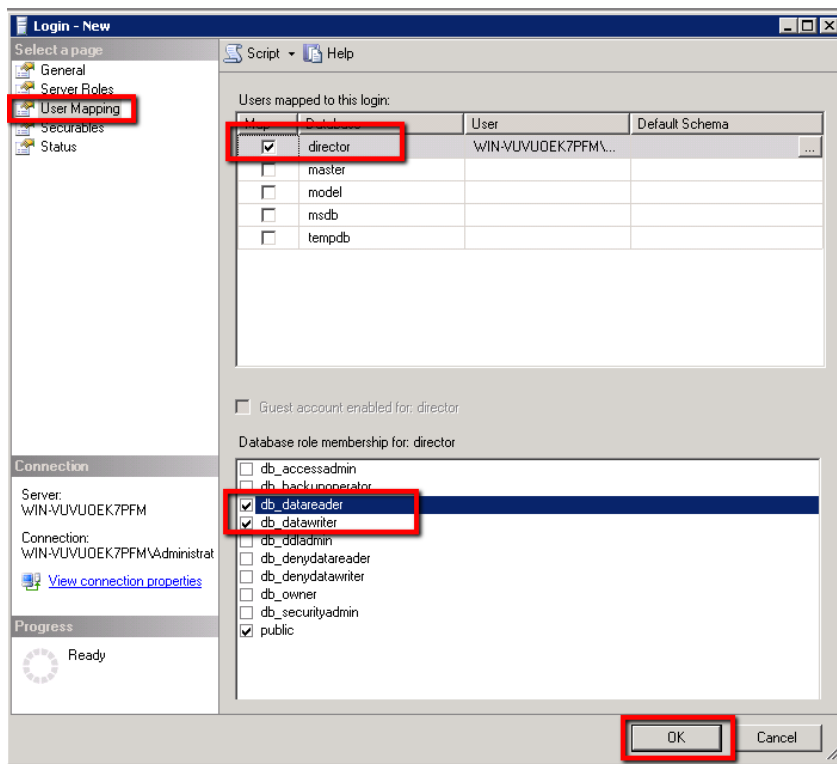
# Create Login & Assign Rights



1. Expand Security
2. Right click on "Logins" and choose "New Login..."
3. Chose domain account (for Win Auth) or chose new username and password (for SQL Server Auth)
4. Change Default database to Director database

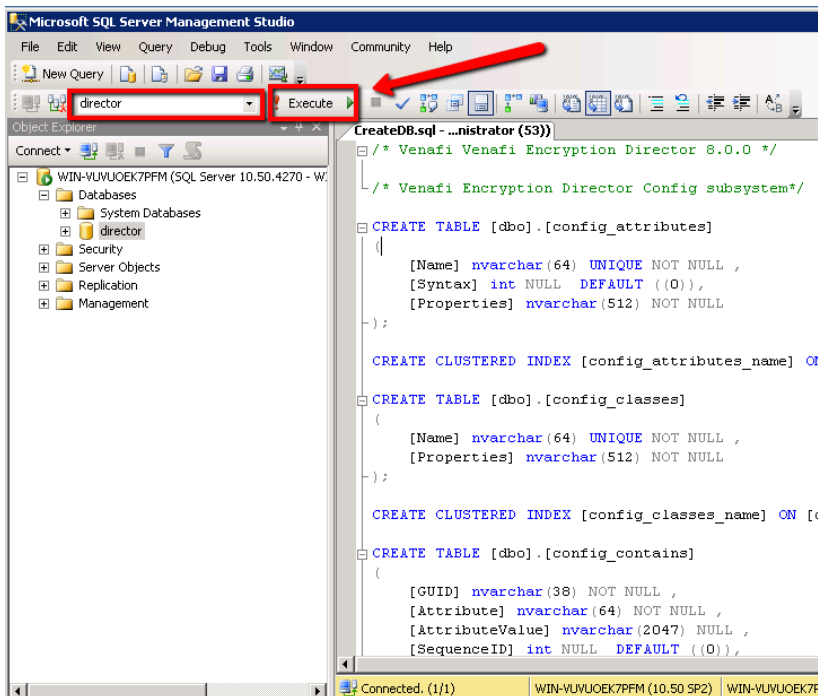


# Create Login & Assign Rights

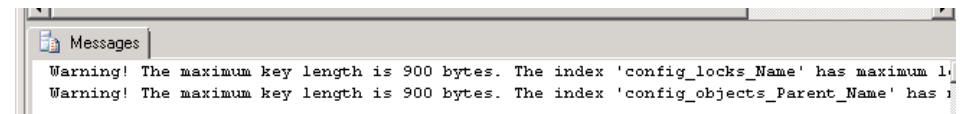


1. Select "User Mapping" page
2. Place a checkbox for the Director database
3. Provide the Login "db\_datareader" and "db\_datawriter" rights
4. Click OK to save changes

# Run Database Create Script



1. Double Click on “Venafi Encryption Director 8.0.0\Database Scripts\MSSQL\CreateDB.sql”
2. Make sure the Director database is selected
3. Click the “Execute” button
4. Some warning messages are expected



# Install Director



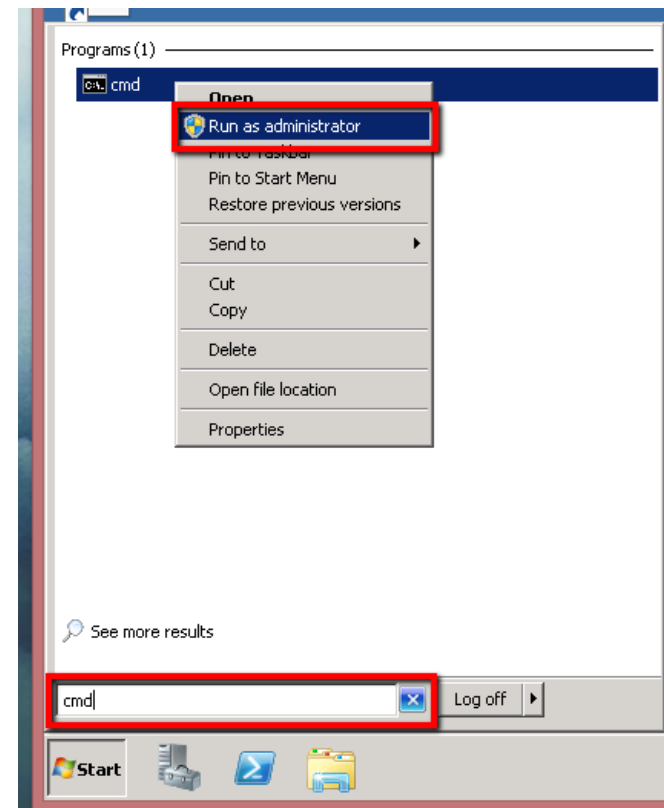
1. Execute MSI Installer from elevated command prompt
2. Accept licensing and choose installation location
3. Choose products to install
4. Choose product components to install
5. Configure connection to primary and failover Venafi Log Servers
6. Configure and verify database connection
7. Create Local Master Administrator credentials for Director software
8. Configure credentials for Microsoft Certificate Authority if component was selected
9. Review configuration summary and initiate product configuration

# Execute MSI



- Venafi Director only available in 64-bit
- Start an “elevated command prompt” by right clicking on command prompt and choosing “Run as administrator”

Note: This is required because the MSI does not request the necessary permissions from the operating system during configuration. Hence the required permissions must be manually given.



# Execute the MSI

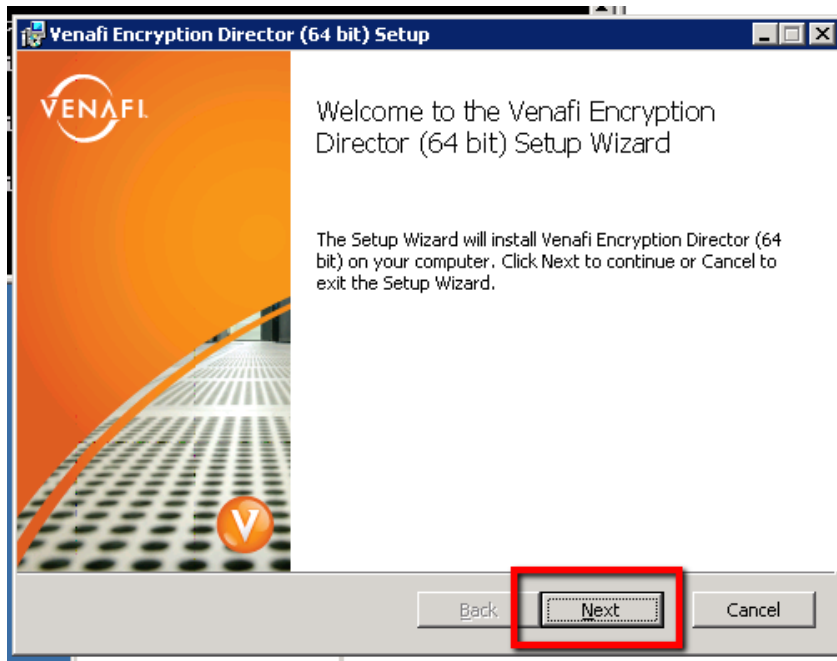
A screenshot of a Windows command prompt window running as Administrator. The title bar reads "Administrator: C:\Windows\System32\cmd.exe". The window content shows the following text:

```
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>cd "C:\Users\Administrator\Desktop\Uenafi Encryption Director 8.0.0"  
  
C:\Users\Administrator\Desktop\Uenafi Encryption Director 8.0.0>DirectorInstallx64.msi_  
_
```

The "Administrator:" part of the title bar is highlighted with a red box. The window also shows standard Windows window controls and a menu bar with "Organize", "Include in library", "Share with", and "New folder".

- Command prompt title bar will start with "Administrator" if successfully started with elevated administrative rights.
- Change your working directory to the folder the MSI is stored using the "cd" command
- Type in the filename of the MSI and hit Enter.  
By default the file is named "DirectorInstallx64.msi"

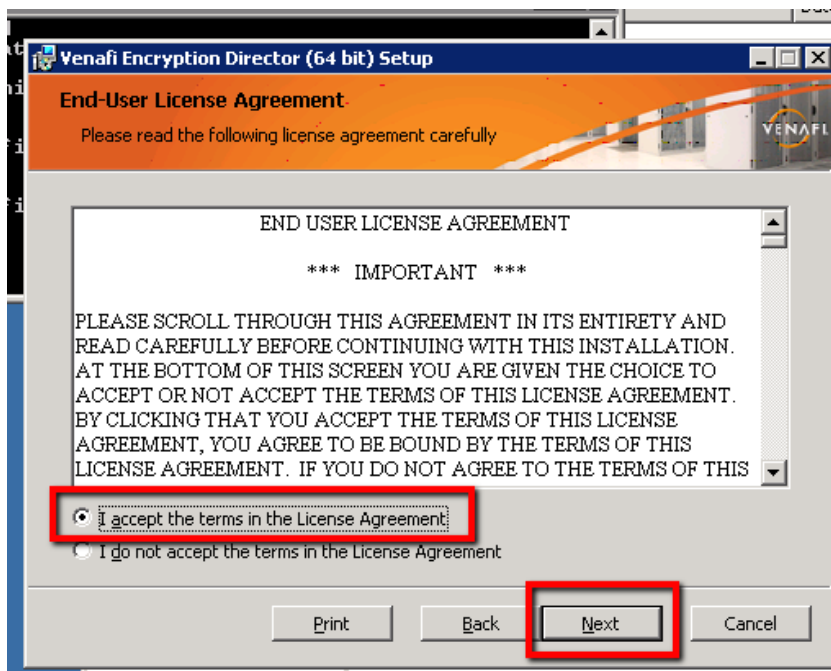
# Windows Install Shield



- Windows Install Shield will launch

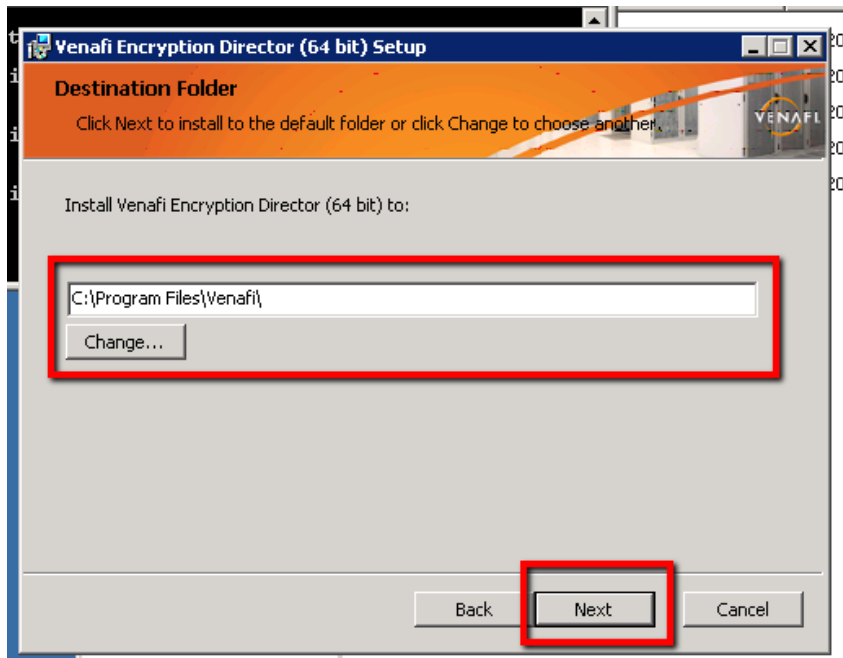


# Windows Install Shield



- Read the End User License Agreement
- Accept the terms of the agreement

# Windows Install Shield



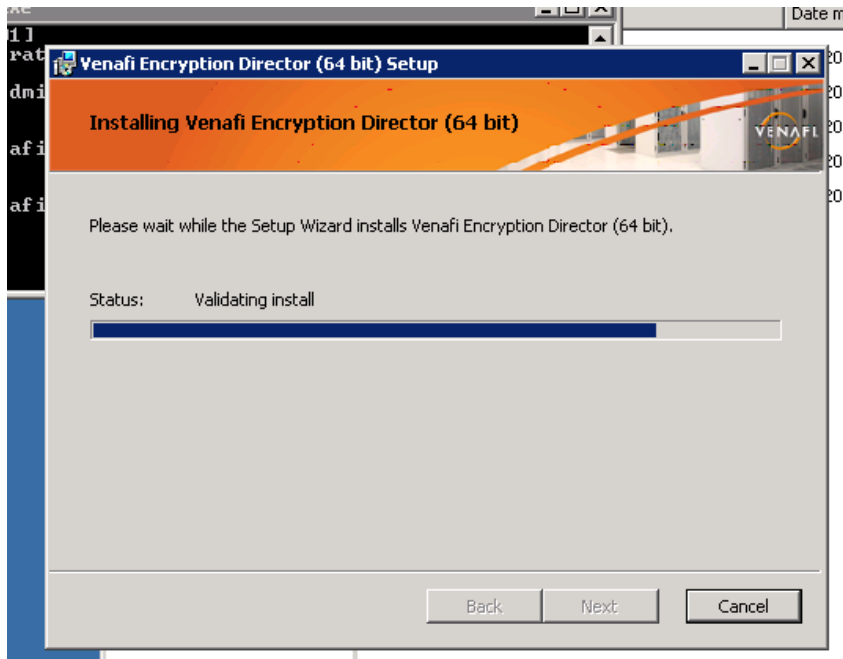
- Set the installation location or leave the default
- It is common to change the installation location to a drive other than the System drive.

# Windows Install Shield



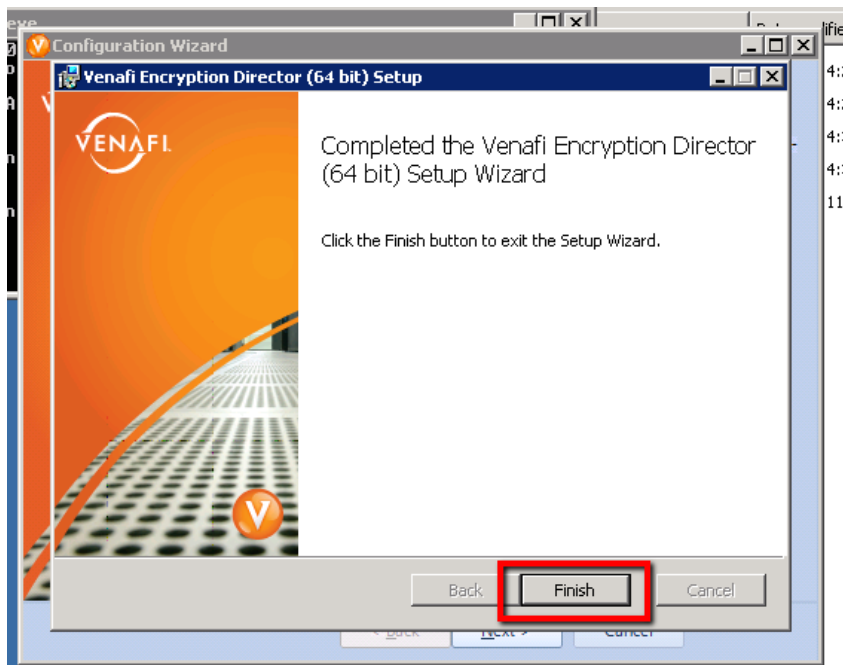
- Clicking “Install” will copy the binaries of the software to the desired location and register it with the Windows operating system.
- It does not configure the software.

# Windows Install Shield



- Installation usually only takes a couple of minutes

# Windows Install Shield



- After the Windows Installer finishes, the Director Control Center (DCC) wizard will automatically launch to walk you through the configuration of the software and prepare it for use.
- You can safely click “Finish” on the setup screen to close it.

# Director Control Center Wizard



- Welcome screen for DCC
- Can be reran anytime to change installation options by launching “dcc.exe – wizard” from an elevated command prompt found in “Venafi\Platform”

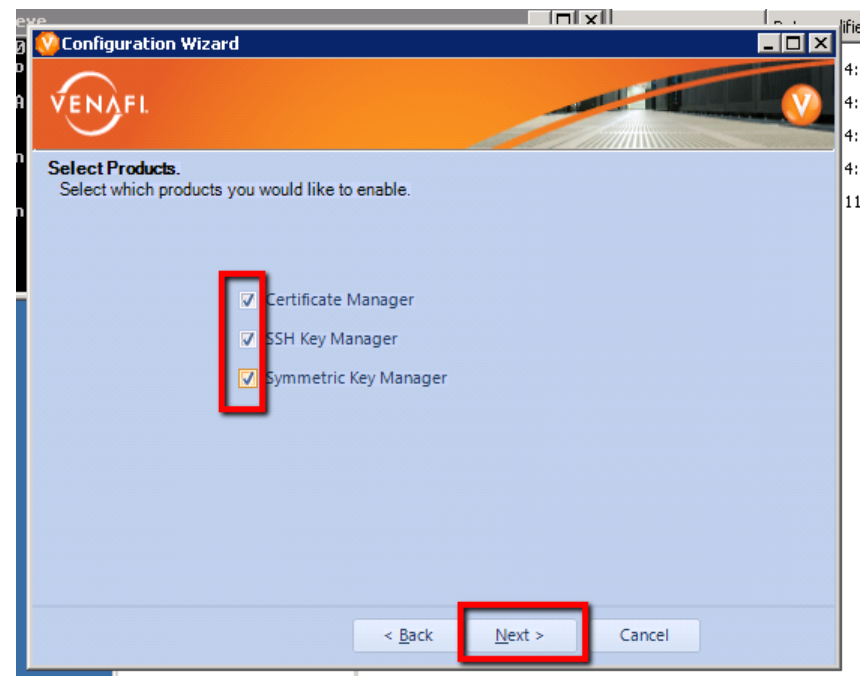


# Director Control Center Wizard



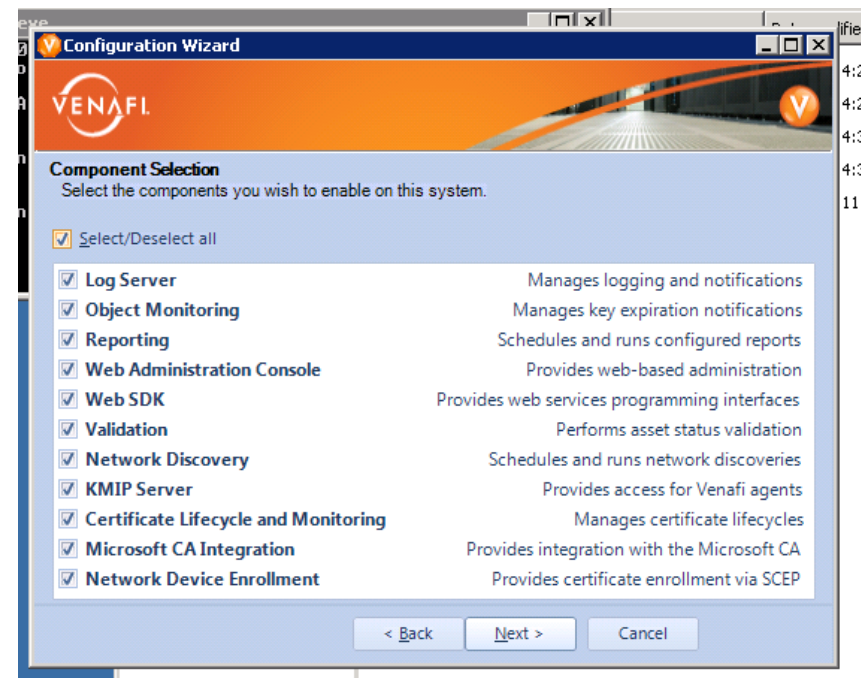
- Select which of the product(s) your organization is licensed for and would like to install in this environment.

Note: Director 8 does not currently implement software license enforcement. Although you can technically install and use all aspects of the software, you can only legally use what you have purchased and licensed. Contact your Venafi Account Manager or Customer Support to find out what your organization is licensed for.



# Component Selection

- Components will be visible based on the products you chose to install
- By default all components are selected
- You may want to uncheck components that you will not be utilizing in your environment or on this particular server



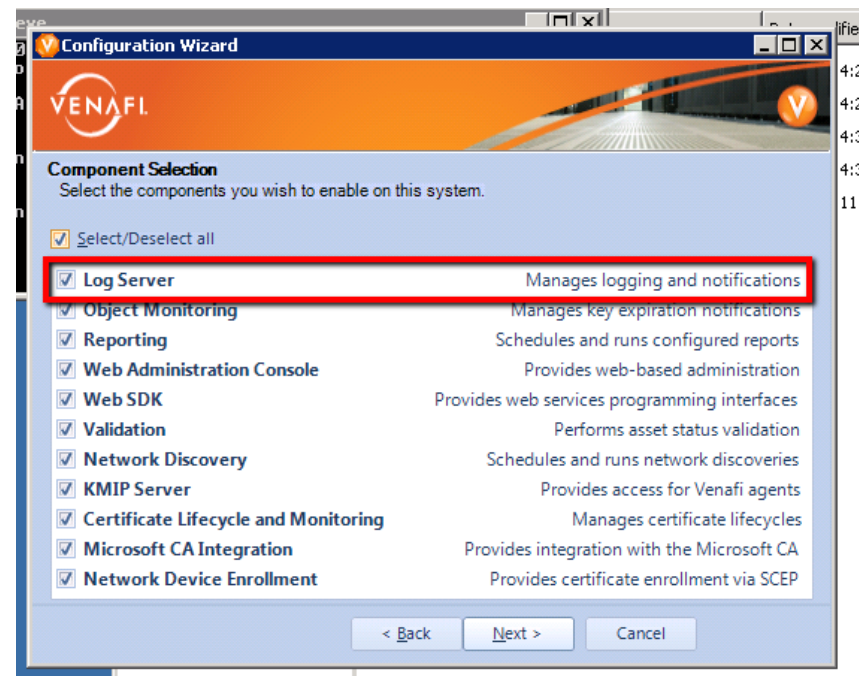


# Component Selection



## Log Server

- Log Server is a Windows service that collects event data from other services and consoles and sends the event data to predefined locations (ex: logs table in database)
- The Log Server windows service will be installed on all servers. This box controls whether DCC will enable or disable the windows service
- Each Director environment can only have one primary Log Server and one failover Log Server. If you already have these servers defined you may want to uncheck this component

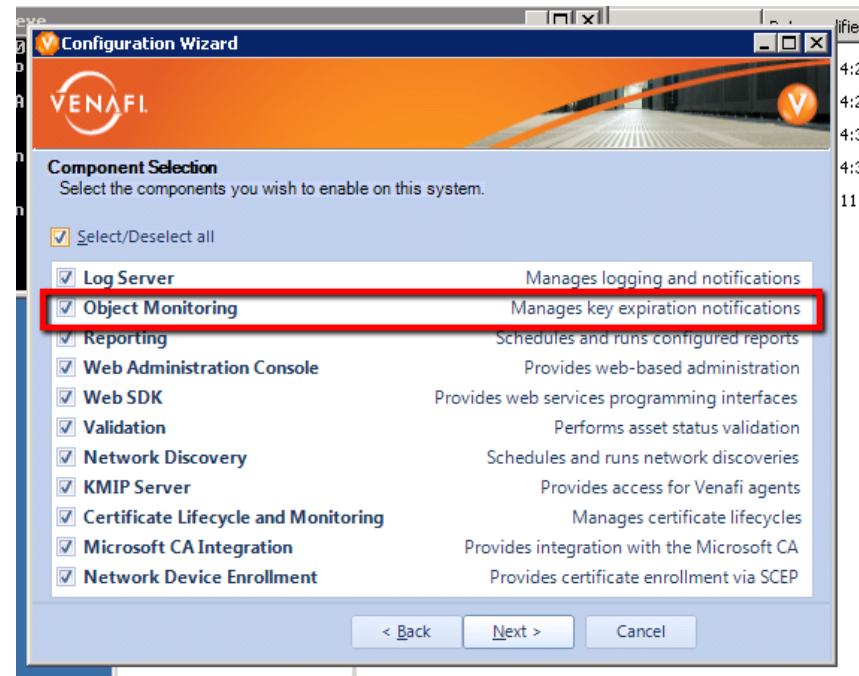


# Component Selection



## Object Monitoring

- Monitors the expiration of credential resources, SSH keys, and symmetric keys in Director
- Generates expiration events when objects near the expiration date

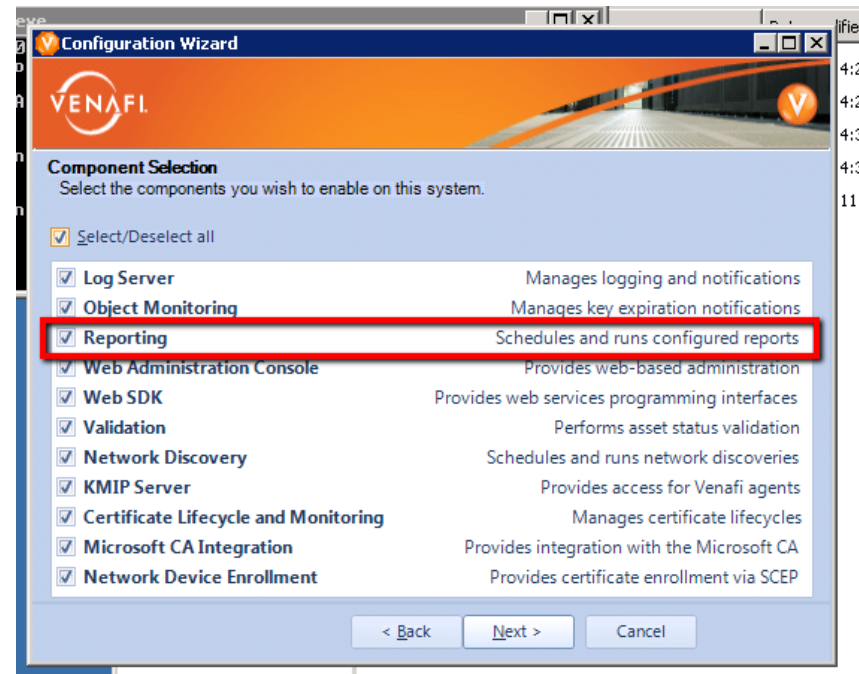


# Component Selection



## Reporting

- Generates and delivers configured reports either on demand or via a schedule

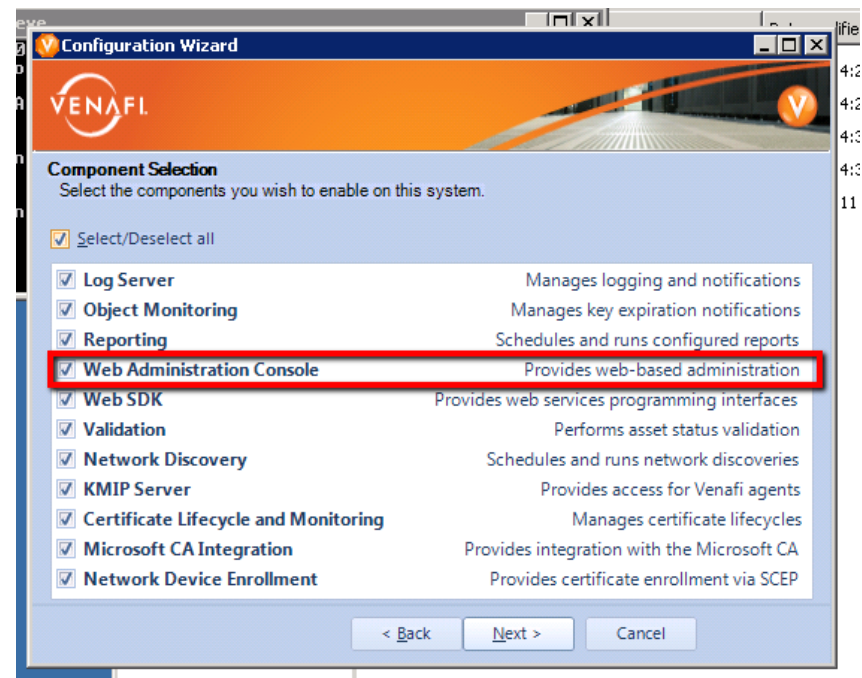


# Component Selection



## Web Administration Console

- Provides remote access to daily administrative functions
- It is recommended that the Web Administration Console (Web Admin) be installed on at least one server. Some management functions can only be performed in Web Admin
- If checked, DCC will configure the “VedAdmin” web application within the “Venafi” site in IIS.

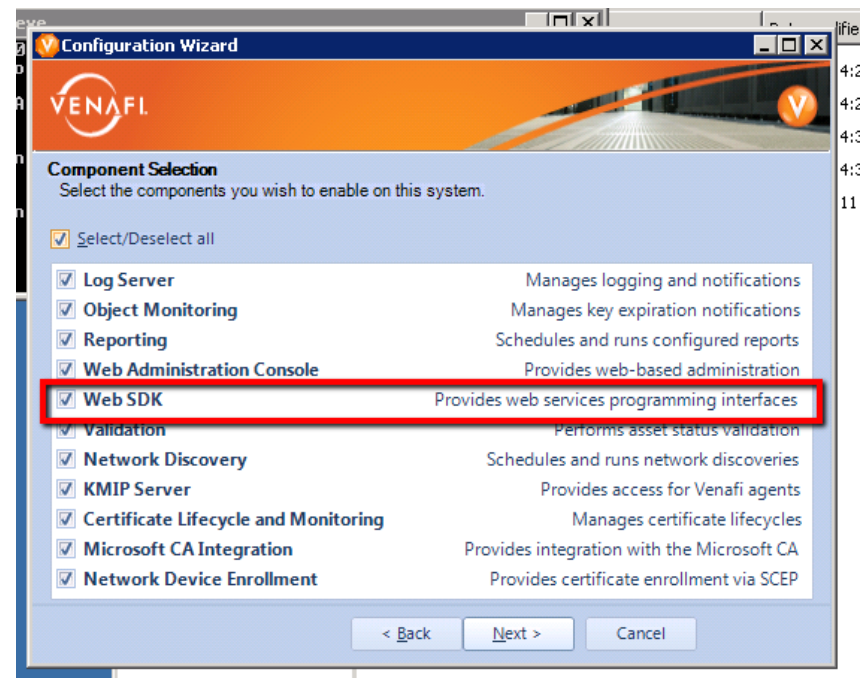


# Component Selection



## Web SDK

- Provides a programming interface for third party applications through Director's web services REST API
- If checked, DCC will configure the "WebSDK" web application within the "Venafi" site in IIS
- Documentation can be found at <https://support.venafi.com>

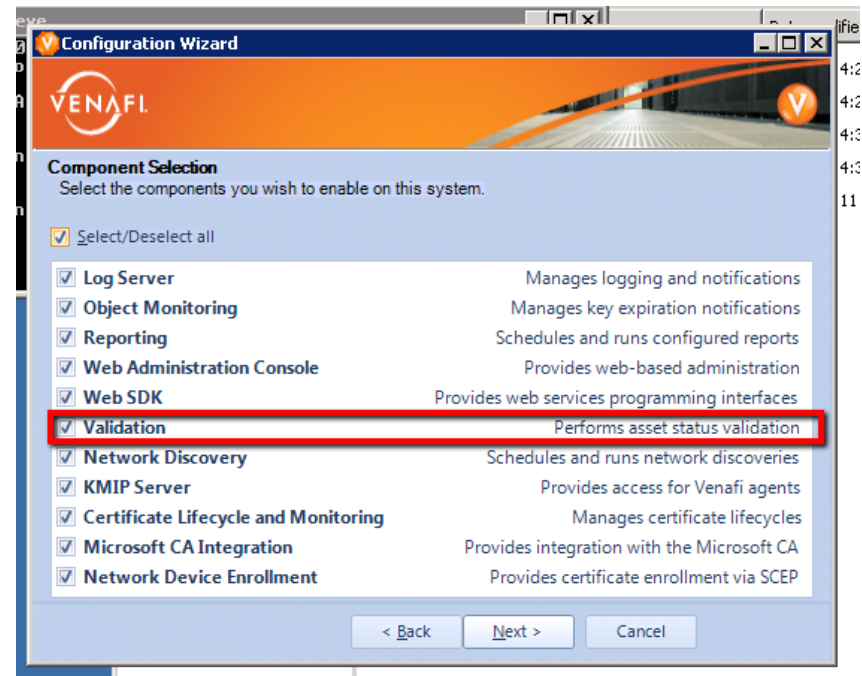


# Component Selection



## Validation

- Runs daily and on-demand validation to ensure correct certificates and SSH keys are installed and functioning properly
- Component only available for Certificate Manager and SSH Key Manager products

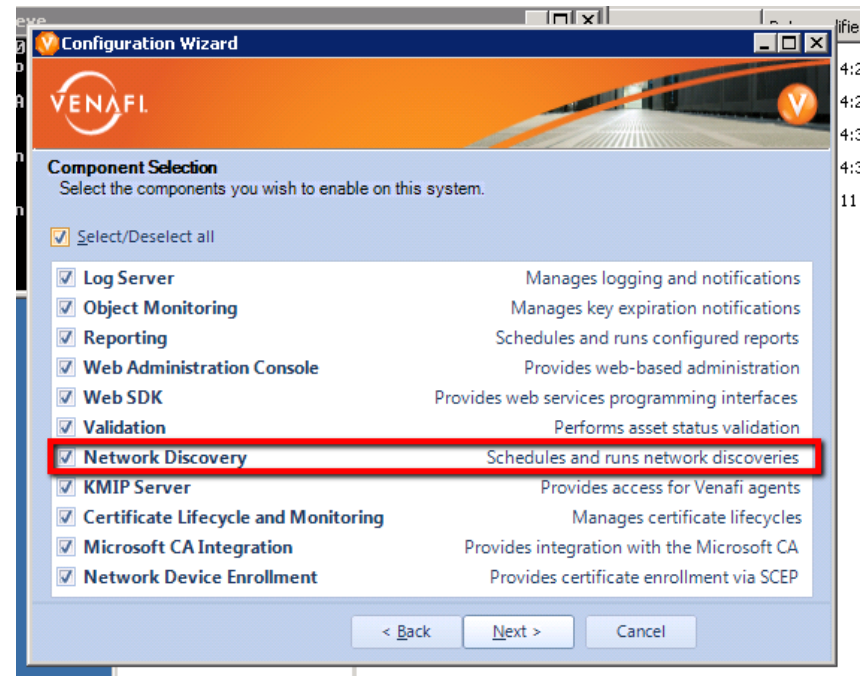


# Component Selection



## Network Discovery

- Runs schedulable and on-demand network discoveries of certificates and SSH keys
- Component only available for Certificate Manager and SSH Key Manager products

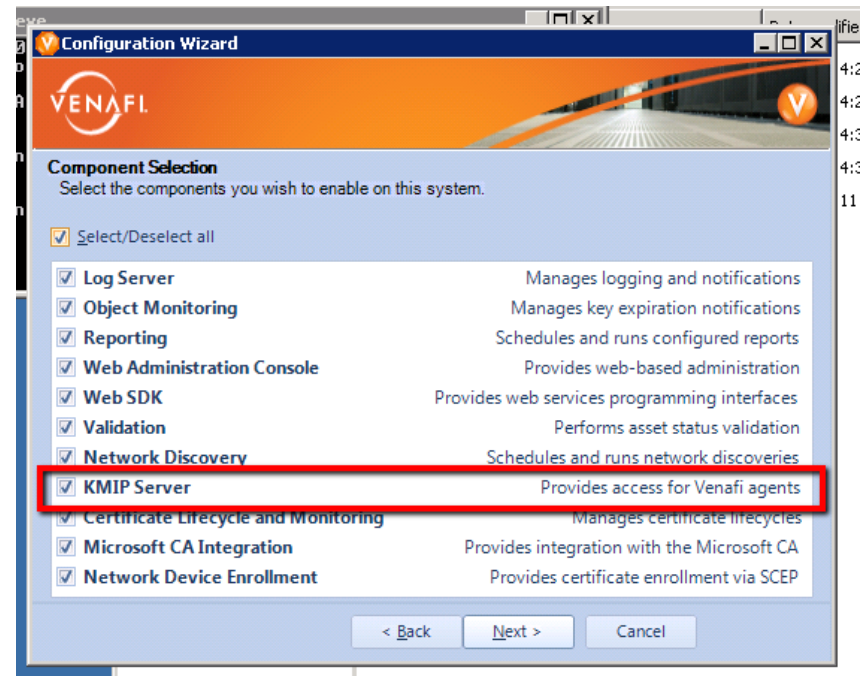


# Component Selection



## KMIP Server

- Enables Director services to listen for incoming connections from the Director Agent
- Component only available for Certificate Manager and SSH Key Manager products



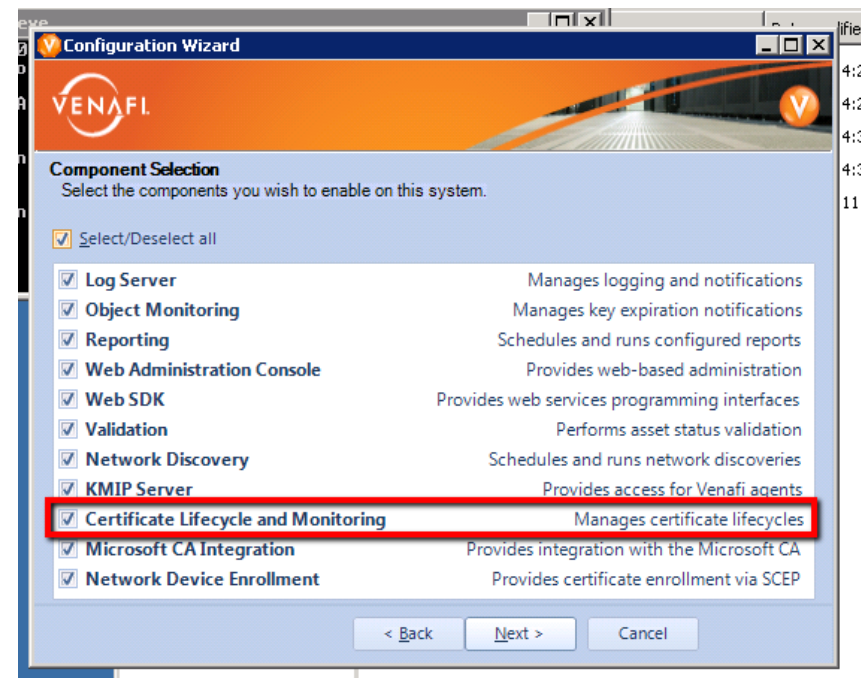


# Component Selection



## Certificate Lifecycle and Monitoring

- Monitors expiration for certificates. Also responsible for key and CSR generation, enrollment and provisioning
- Component only available for Certificate Manager product

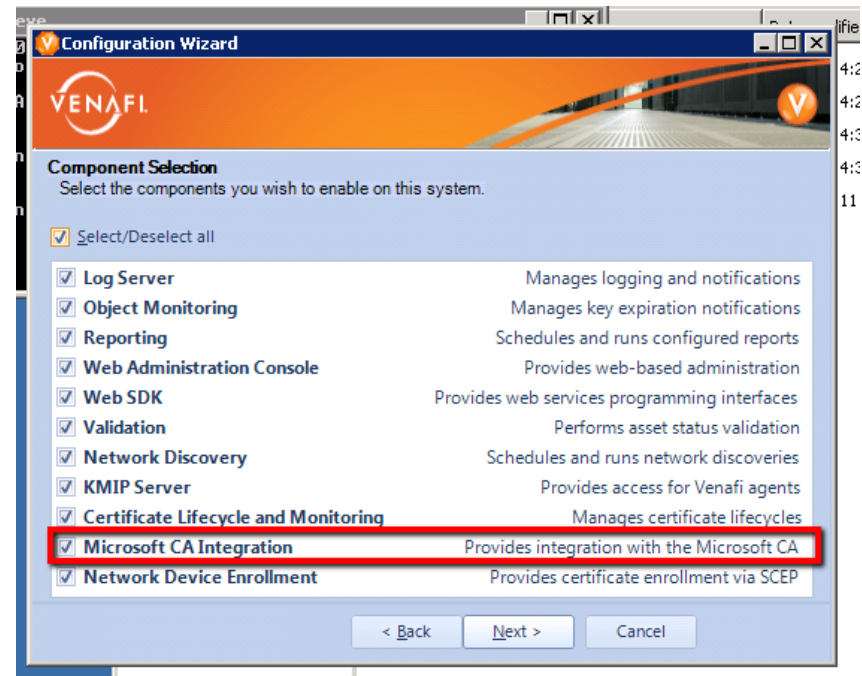


# Component Selection



## Microsoft CA Integration

- Director uses Microsoft DCOM technology to communicate with Microsoft Certificate Authority (MSCA)
- If checked, Director will prompt for the domain account used to authenticate with MSCA so that DCC can configured DCOM permissions on the local Director server
- Component only available for Certificate Manager product

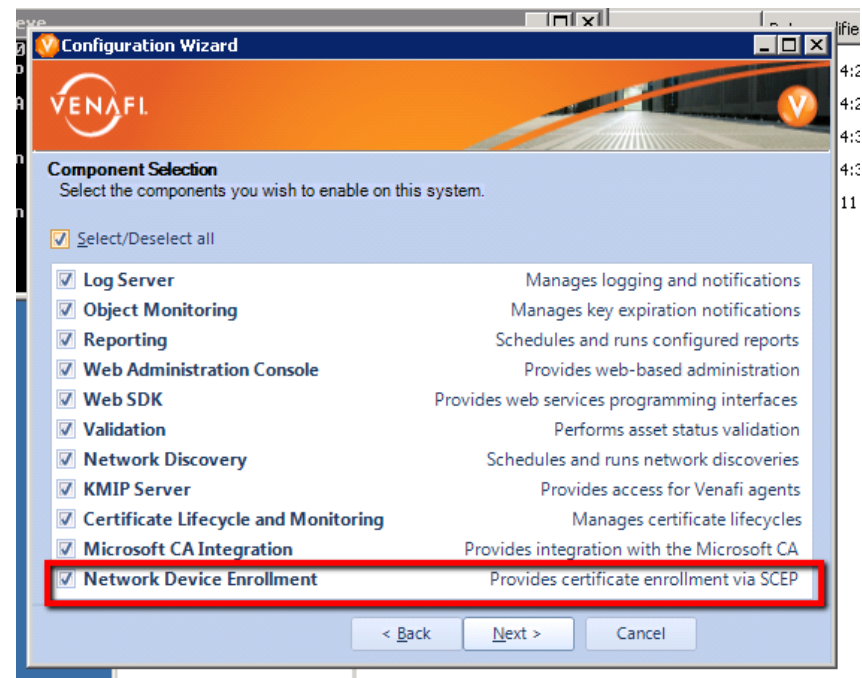


# Component Selection



## Network Device Enrollment

- Enables Director to be able to enroll certificates via SCEP protocol
- Typically used with mobile device management platforms and network appliances
- If checked, DCC will configure the “NDE” web application within the “Venafi” site in IIS
- Component only available for Certificate Manager product



# Director Control Center Wizard



## Shared Encryption Key

- Director uses a shared symmetric encryption key to encrypt sensitive portions of the database
- If this is the first server in a new environment, click “Next” and a key will be generated for you
- If this server will be joining an existing Director environment, type in the key password and paste the Encoded key
- Shared Encryption Key is often referred to as the “DPAPI Key” because it is protected by Microsoft’s Data Protection API

The screenshot shows the 'Configuration Wizard' window for Vena. The title bar reads 'Configuration Wizard'. The Vena logo is in the top left, and a small Vena logo icon is in the top right. The main content area is titled 'Shared Encryption Key' and contains the following text: 'If you are installing into an existing database, select 'Use Shared Key', specify a 'Key Password' and enter the 'Encoded Key' information below.' Below this text are three input fields: a checkbox labeled 'Use Shared Key:', a 'Key Password:' text box, and a larger 'Encoded Key:' text area. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red rectangular border.

# Director Control Center Wizard



## Log Server Addresses

- Type in the IP address of the Primary Log Server and Secondary Log Server
- If there will only be on Director server in your environment then leave the defaults and click "Next"
- If a multi-engine environment (multiple Director server), type in the IP address of the Secondary Log Server
- IPv4 and IPv6 both accepted

**Configuration Wizard**

**VENAFI**

**Log Server Selection**  
Please provide the address of your primary and (optionally) secondary log server.

Primary Log Server Address: 127.0.0.1

Secondary Log Server Address:

Create default log channels and notifications

Always leave "Create default log channels and notifications" checked.

< Back **Next >** Cancel

# Director Control Center Wizard



## Database Configuration

- Select the type of database
- If using Windows Authentication for MS SQL Server, check the box
- Type in the connection information. All fields required
- Click "Verify" and DCC will attempt to use the information provided to test the connection to the database
- Problems will result in an error message. Success will result in "Next" becoming enabled to click on

# Director Control Center Wizard



## Create Local Master Admin Account

- Create the first account used to login to Director
- Master Admin account has all rights to all aspects of Director
- Used to join other servers to environment and perform upgrades
- Can create multiple Master Admin accounts within Director
- Username chosen here, but cannot be renamed later.

Configuration Wizard

VENAFI

**Admin Account Credentials**  
Please provide the credentials for the Venafi Encryption Director administrative account.

Administrator Account: Admin

Admin Password: ••••••••

Repeat Admin Password: ••••••••

< Back   Next >   Cancel

# Director Control Center Wizard



## Microsoft Certificate Authority Credentials

- Username can be in NTLM or UPN format
- If windows account does not exist, DCC will error out at the end of the wizard when it attempts to configure permissions for Windows DCOM

The screenshot shows a window titled "Configuration Wizard" with the VENAFI logo. The main heading is "Microsoft Certificate Authority Credentials" with the instruction "Please provide the credentials required to access your Microsoft Certificate Authority." Below this, there are two input fields: "Username:" containing "companyx.local\CertAdmin" and "Password:" containing a masked password. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a red box.

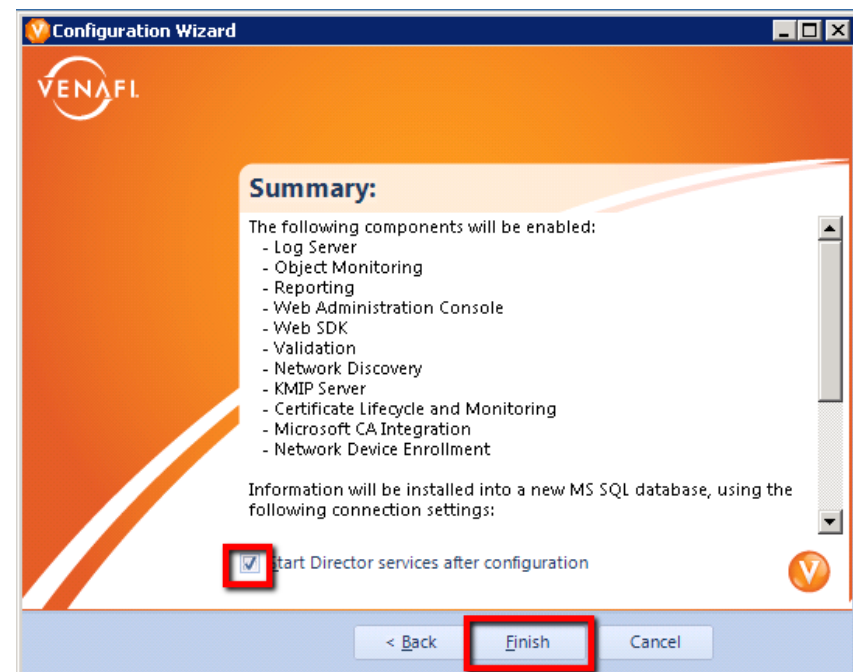


# Director Control Center Wizard



## Summary

- Scroll through the summary to review the information collected during the DCC Wizard
- Select the box to start Director services
- Click Finish

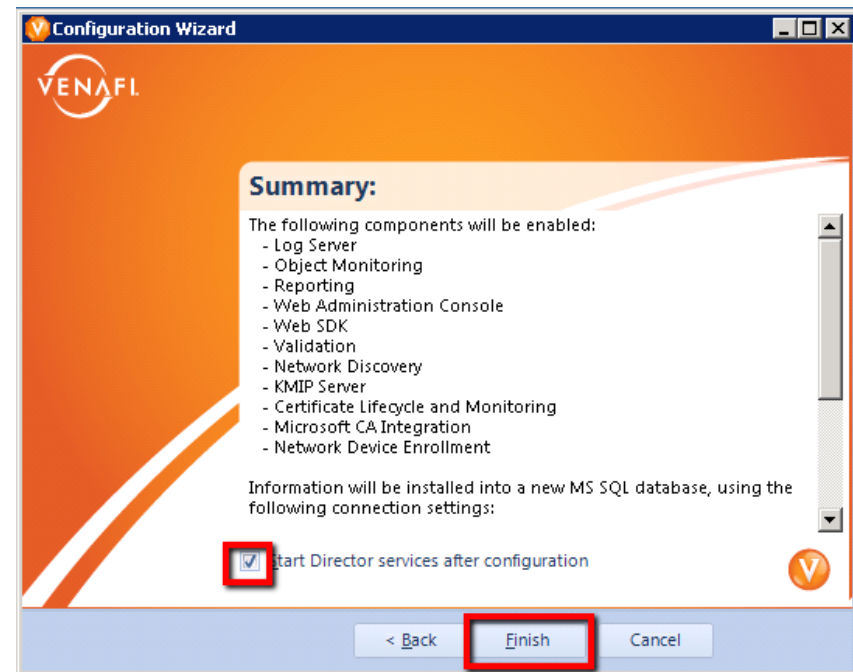


# Director Control Center Wizard



## Configuring Director Services and Components

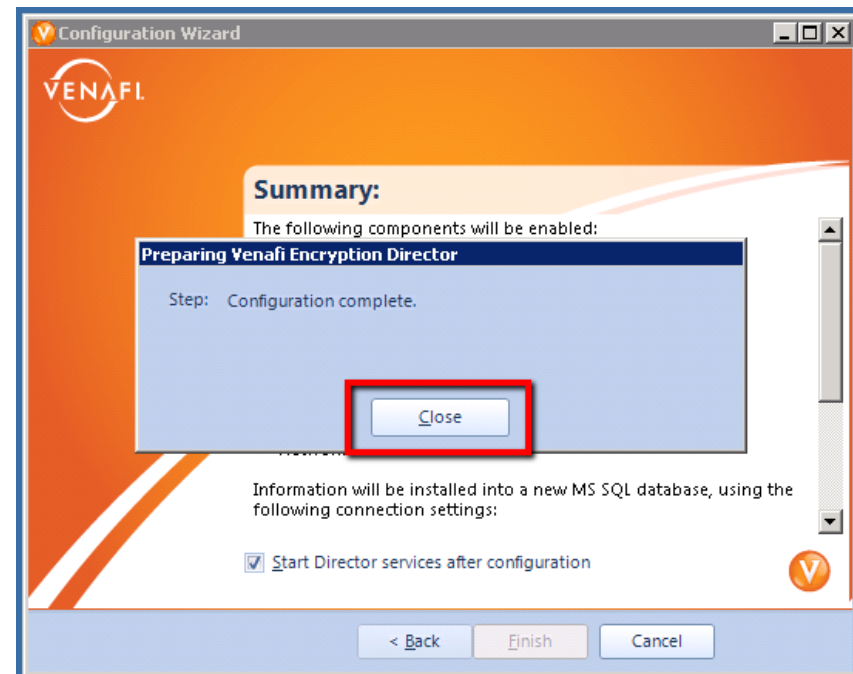
- Scroll through the summary to review the information collected during the DCC Wizard
- Select the box to start Director services
- Click Finish



# Director Control Center Wizard



- Director is now successfully installed
- Click the "Close" button to exit the Director Control Center Wizard



# Director Control Center Wizard



## Re-Run Wizard

- Type in "dcc.exe -wizard" from Venafi\Platform folder
- Can change what components are installed on server
- Can Change DCOM Credentials for Microsoft Certificate Authority
- Must have existing Master Admin credentials to complete wizard

```
Administrator: Windows Command Processor
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd "c:\Program Files\Venafi\Platform"
c:\Program Files\Venafi\Platform>dcc.exe -wizard_
```



# Multi-Engines Setups

Module 3 – Setting up a 2<sup>nd</sup> Director Server

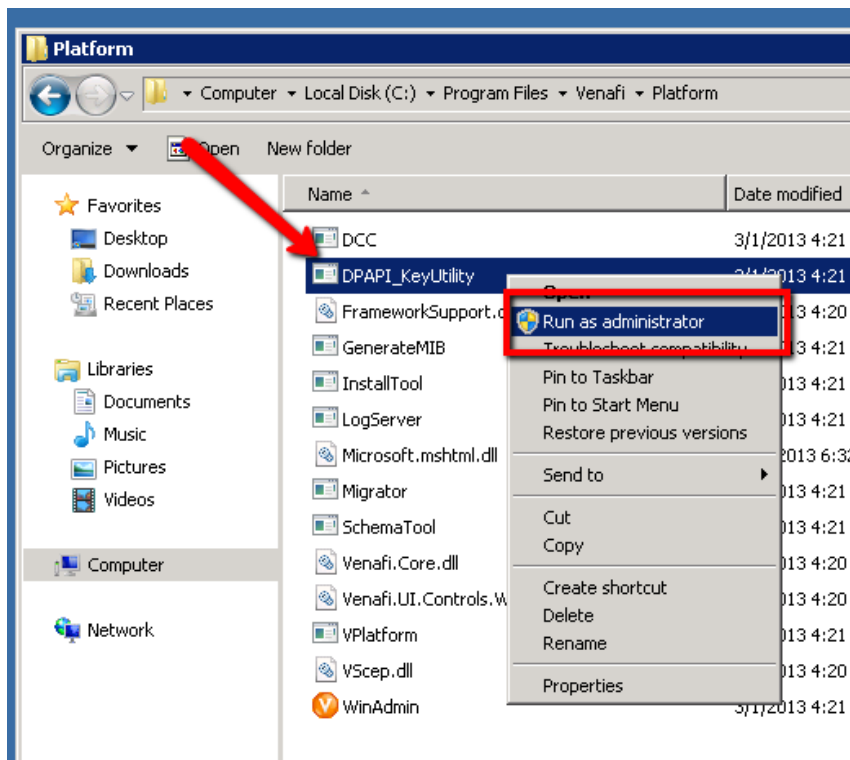
# Multi-Engine Setup



Director's architecture allows it to scales across multiple servers for:

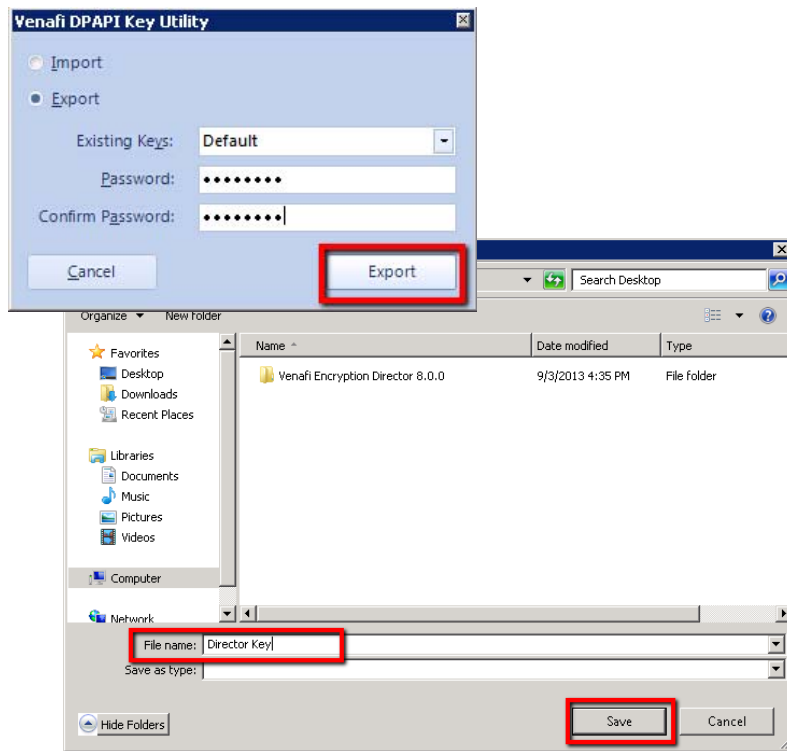
- Load Balancing
  - When the work is spread across multiple engines, the work is performed faster
- Fault Tolerance
  - When an engine goes offline, other engines with the same roles can resume the work
- Enhanced Network Access
  - Deploy Director engines to restricted network segments for discovery, validation, and provisioning

# Export Shared Encryption Key



1. Browse to Venafi\Platform
2. Right Click on "DPAPI\_KeyUtility.exe"
3. Choose "Run as administrator"

# Export Shared Encryption Key



4. Choose a password to encrypt the key file
5. Click "Export"
6. Choose a File Name (File Type will be left blank)
7. Click "Save"
8. Store the Shared Encryption Key file in a safe and protected space
9. Temporarily copy to servers you will be installing Director on



## Install Director on Additional Engine



Installing Director on Additional Servers is very similar to installing it on your first server. There are some key differences:

- Skip database setup on database server, it has already been done
- Choose different components depending upon the role of the server
- Enter the Shared Encryption Key instead of having DCC create a new one
- Enter your Master Admin credentials instead of creating them

## Launch MSI



- Launch the MSI from an elevated command prompt the same way done on the original Director Server
- Accept End User License Agreement
- Install it to the same physical path (not required but recommended)

# Log Server Configuration



The screenshot shows the 'Log Server Selection' step of the VENAFI Configuration Wizard. The window title is 'Configuration Wizard'. The header features the VENAFI logo and a navigation icon. The main content area is titled 'Log Server Selection' and includes the instruction: 'Please provide the address of your primary and (optionally) secondary log server.' There are two text input fields: 'Primary Log Server Address' with the value 'ec2-54-221-95-26.compute-1.amazonaws.com' and 'Secondary Log Server Address' with the value 'ec2-54-211-161-0.compute-1.amazonaws.com'. A checkbox labeled 'Create default log channels and notifications' is checked. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

- Enter the hostname/IP of the first director server
- Put hostname/IP for the secondary server

# Shared Encryption Key



**Configuration Wizard**

**Shared Encryption Key**  
If you are installing into an existing database, select 'Use Shared Key', specify a 'Key Password' and enter the 'Encoded Key' information below.

Use Shared Key:

Key Password: .....

Encoded Key: D5014IrBVUpIVsbUQCgzCDsamqtyWVjO6p3NoKHtuIIIiYRjnXNKgBfcX9Qg2LSJ  
0jJI7dpIThH5af8oaUPS0iThg5pptDuj8gg6u0FQs2VRkbcf15qer+ MpPitghDKx  
Ple+ mHnm8DX3RQw4oCnEuKj/UDTJEUc5MjMqrvoyPthvQ3LUOec  
+ Qa69vGHg/TeR  
FdCavG7q258HH2TFT0/OFVikPwFk9sjG/QLHV1wH6g4uB+ JHFUxLJfDt+ TtUskKz  
E3WU7WfrM/Zi/ksY9APP+ HGVsrBgmQPriUPNEEJyaf7esAnTy55TSAbwW9tmI4JA  
VkiErtqd824fsc8vpSFkDuOpf6zCYbH3RzMTnTlas7IWB4sIQfQ3RukSaWID7IE  
Ppsfja/nUz48htPEubOIDK+ JHfgUEv0  
-----END VED ENCRYPTED KEY-----

< Back **Next >** Cancel

- Check "Use Shared Key"
- Paste the encoded key into the space provided
- Type the corresponding password for the encoded key that was created when you exported the key

# Database Settings



**Configuration Wizard**

**VENAFI**

**Database Configuration**  
Please enter the details about your database (which should already have been prepared with the Venafi Encryption Director tables.)

MS SQL Server  Use Windows Authentication

MySQL Server

Oracle

Username: sa Password: .....

Host: ec2-54-221-95-26.compute-1.amazonaws.com Port: 1433

Database: director **Verify**

< Back Next > Cancel

- Type in the connection information to connect to the database

Note: Windows Authentication can only be used to connect when the director server is in a trusted domain of the database server

# Master Credential Verification



Configuration Wizard

VENAFI

**Admin Account Credentials**  
Please provide the credentials for the Venafi Encryption Director administrative account.

Administrator Account: Admin

Admin Password: ••••••••

Verify

< Back   Next >   Cancel

- Type in a set of local master administrative credentials

Note: These are typically the credentials created during the Director Control Center wizard on the first server – but can be any local master admin credentials if more were created later