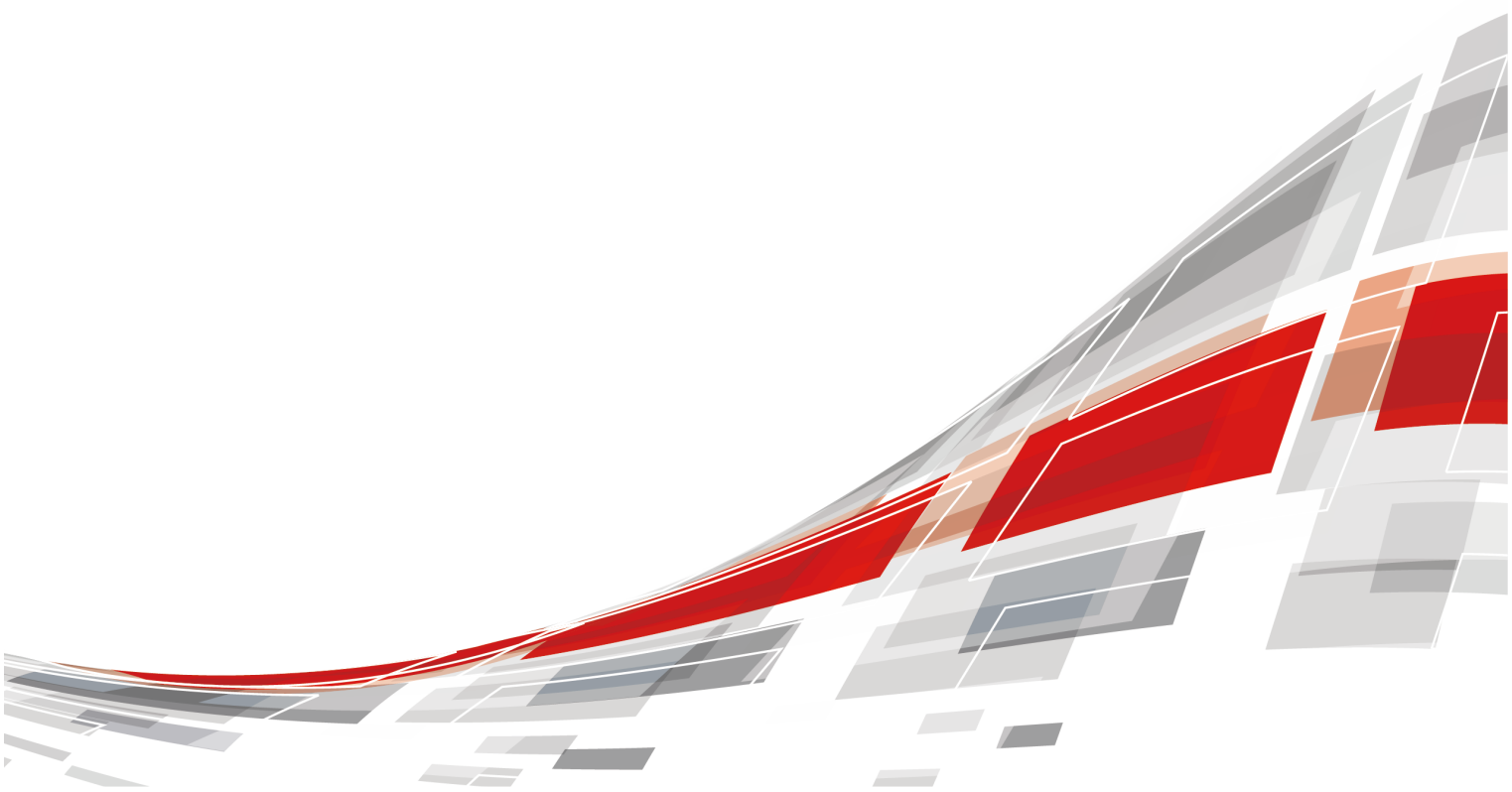
XFUSION FusionDirector For SCOM Plug-in 1.0.19

User Guide

Issue	02
Date	2023-09-30



xFusion Digital Technologies Co., Ltd.

Trademarks and Permissions

XFUSION and other xFusion trademarks are trademarks of xFusion Digital Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

In this document, "xFusion" is used to refer to "xFusion Digital Technologies Co., Ltd." for concise description and easy understanding, which does not mean that "xFusion" may have any other meaning. Any "xFusion" mentioned or described hereof may not be understood as any meaning other than "xFusion Digital Technologies Co., Ltd.", and xFusion Digital Technologies Co., Ltd. shall not bear any liability resulting from the use of "xFusion".

The purchased products, services and features are stipulated by the contract made between xFusion and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

xFusion Digital Technologies Co., Ltd.

Address: 9th Floor, Building 1, Zensun Boya Square, Longzihu Wisdom Island
Zhengdong New District 450046
Zhengzhou, Henan Province
People's Republic of China

Website: https://www.xfusion.com

About This Document

Purpose

This document describes how to install and uninstall the SCOM plug-in, add and delete FusionDirector, and view server information and status, alarm lists, and server topologies by using FusionDirector For SCOM Plugin.

Intended Audience

This document is intended for:

- Technical support engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue	Date	Description
02	2023-09-30	Added upgrade function.
01	2023-03-30	This issue is the first official release.

Contents

About This Document ii

1 Overview 1

2 Installing and Uninstalling the SCOM Plug-in 3

2.1 Installing the SCOM Plug-in 3

2.2 Uninstalling the SCOM Plug-in 11

2.2.1 Uninstalling the SCOM Plug-in from the Control Panel 11

2.2.2 Uninstalling the SCOM Plug-in from the Installation Directory 13

2.3 Upgrading the SCOM plug-in 15

3 Configuring FusionDirector 19

3.1 Adding FusionDirector 19

3.2 Editing FusionDirector 23

3.3 Deleting FusionDirector 25

4 Viewing Plug-in System Information 27

4.1 Viewing the Basic Plug-in System Information and Status 27

4.2 Viewing a Plug-in System Event List 28

4.3 Viewing a Plug-in System Alarm List 30

5 Viewing Chassis Information 32

5.1 Viewing the Basic Chassis Information and Status 32

5.2 Viewing a Chassis Topology 35

5.3 Viewing a Chassis Alarm List 36

6 Viewing Server Information 38

6.1 Viewing the Basic Server Information and Status 38

6.2 Viewing a Server Topology 40

6.3 Viewing a Server Alarm List 41

6.4 Viewing Server Performance Curves 43

6.4.1 Viewing the CPU Usage 43

6.4.2 Viewing the Air Inlet Temperature 43

6.4.3 Viewing the PSU Power 44

7 FAQs 46

7.1 How Do I Fix a Communication Failure Caused by an Incorrect Default FusionDirector Certificate? 46

7.2 How Do I Replace the Server Certificate?.....54
7.3 What Do I Do If the System Displays a Message Indicating that the SSL/TLS Secure Channel Fails to Be Created When FusionDirector Is Added?.....65
7.4 How Do I Disable the Insecure TLS Protocol?.....68
7.5 How to Disable System Unsafe Encryption Algorithm Kits.....69
A Glossary.....72
B Public IP Addresses.....73
C Obtaining Technical Support.....75
D Communication Matrix.....76

1 Overview

The SCOM plug-in is a plug-in integrated in the System Center Operations Manager (SCOM for short) software and used for server management. By adding FusionDirector, it can monitor the health status and alarm information of servers. A maximum of 1000 servers can be monitored.

You can implement the following functions by using the SCOM plug-in:

- View the information of servers and chassis.
- View the health status of servers and chassis.
- View the alarm information of servers and chassis.
- View the topologies of servers and chassis.
- View the performance curves of servers.

NOTICE

The actual functions depend on the functions provided by FusionDirector.

Servers supported by SCOM Plug-in

Type	Server or Chassis Model
Rack server	1288H V5
	2288 V5
	2288H V5
	2488 V5
	2488H V5
	RH2288H V3
	1288H V6
	2288H V6

Type	Server or Chassis Model
	1288H V7
	2288H V7
	5288 V7
Blade server	CH121 V3
	CH242 V3
	CH121 V5
	CH242 V5
	E9000 (MM920)
KunLun server	9008 V5

Matching Versions

Software	Matching Versions
FusionDirector	FusionDirector: 1.6.0.SPC1 or later

Software Requirements

Type	Version
SCOM	SCOM 2012R2
	SCOM 2016
	SCOM 2019
	SCOM 2022

2 Installing and Uninstalling the SCOM Plug-in

2.1 Installing the SCOM Plug-in

2.2 Uninstalling the SCOM Plug-in

2.3 Upgrading the SCOM plug-in

2.1 Installing the SCOM Plug-in

Prerequisites

You have obtained the SCOM plug-in software package and verified its integrity.

1. Obtain the SCOM plug-in software package (for example, **XFUSION_FusionDirector_For_SCOM_Plugin_1.0.18.zip**) and its SHA256 verification file (for example, **XFUSION_FusionDirector_For_SCOM_Plugin_1.0.18.sha256.sum**) from **GitHub**.
2. Verify the integrity of the SCOM plug-in software package(Windows OS).
   a. Open the CMD and go to the directory where the plug-in software package is stored.
   b. Run the **certutil -hashfile** *"software package name"* **sha256** command to check the SHA256 hash value of the software package.

      Example: **certutil -hashfile "XFUSION_FusionDirector_For_SCOM_Plugin_1.0.18.zip" sha256**
   c. Check whether the SHA256 hash value of the software package is the same as that of the SHA256 verification file.
      - If yes, the software package has not been tampered with and can be used.
      - If no, the software package has been tampered with. Obtain a new software package.

Procedure

Step 1 Upload the SCOM plug-in installation package to the server.

Step 2 Log in to the server.

Step 3 Decompress the SCOM plug-in installation package.

Obtain the installation application, for example, **XFUSION_FusionDirector_For_SCOM_Plugin_*x.x.xx.xxx*.exe**.

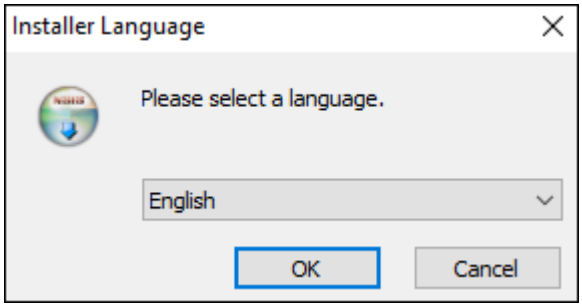
Step 4 Double-click **XFUSION_FusionDirector_For_SCOM_Plugin_*x.x.xx.xxx*.exe**.

NOTE

If you set up the SCOM environment as an administrator and log in to the server as a non-administrator in **Step 2**, you need to run the plug-in installation program as an administrator.

The **Installer Language** window is displayed, as shown in **Figure Installer Language**.

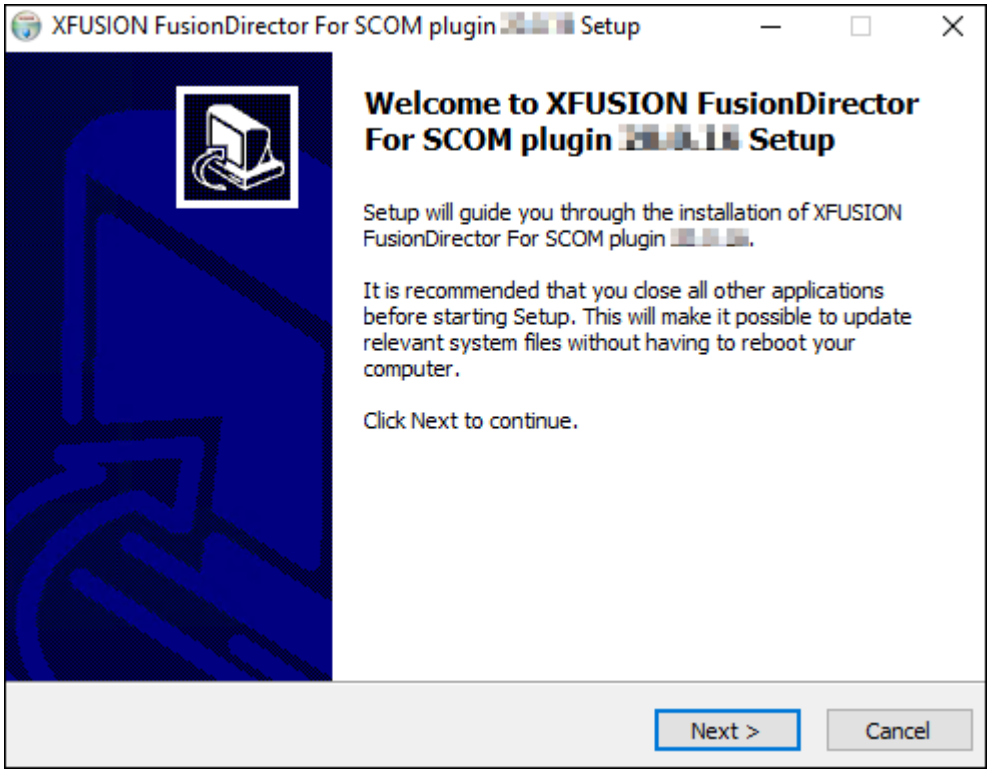
Figure 2-1 Installer Language



Step 5 Select **English**, and click **OK**.

The welcome to the setup wizard window is displayed, as shown in **Figure 2-2**.

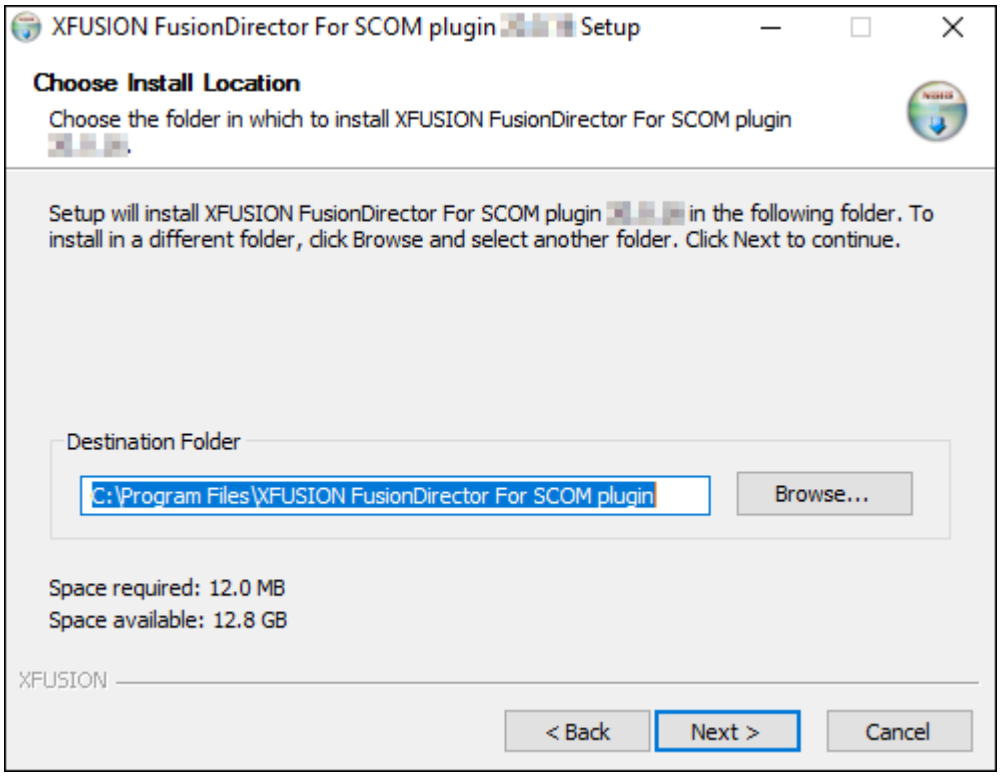
Figure 2-2 Welcome to the setup



Step 6 Click **Next**.

The **Choose Install Location** window is displayed, as shown in **Figure 2-3**.

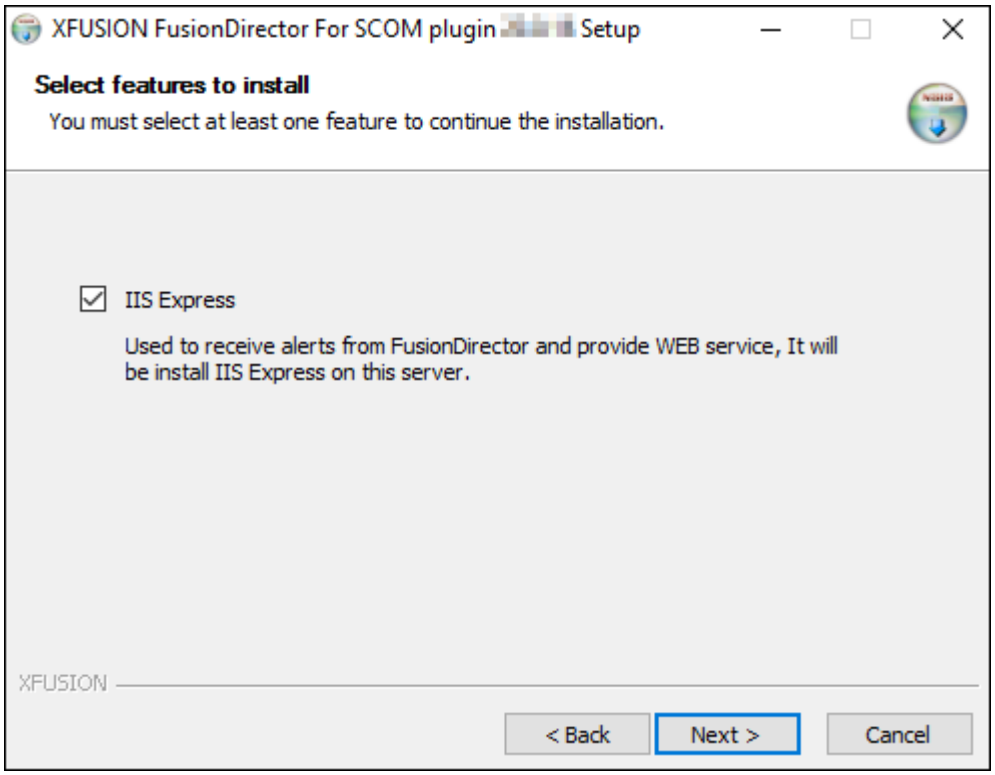
Figure 2-3 Choose Install Location



Step 7 Retain the default installation path or click **Browse** to change the installation path, and click **Next**.

The **Select features to install** window is displayed, as shown in **Figure 2-4**.

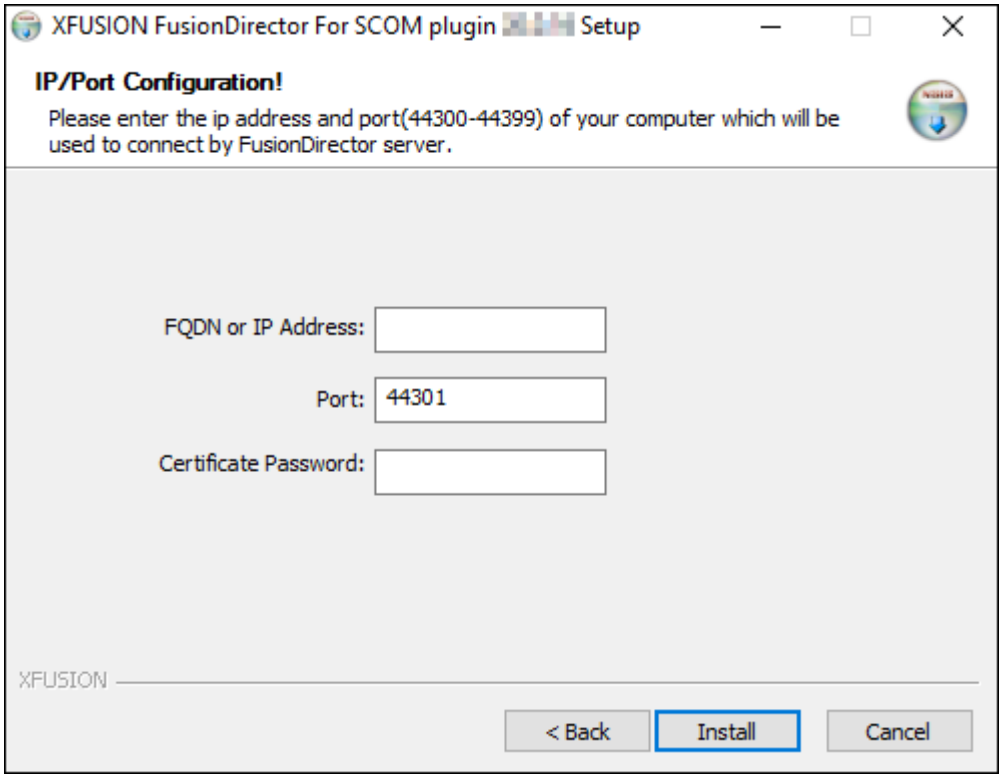
Figure 2-4 Select features to install



Step 8 **IIS Express** is selected by default. Click **Next**.

The **IP/Port Configuration** window is displayed, as shown in **Figure 2-5**.

Figure 2-5 IP/Port Configuration



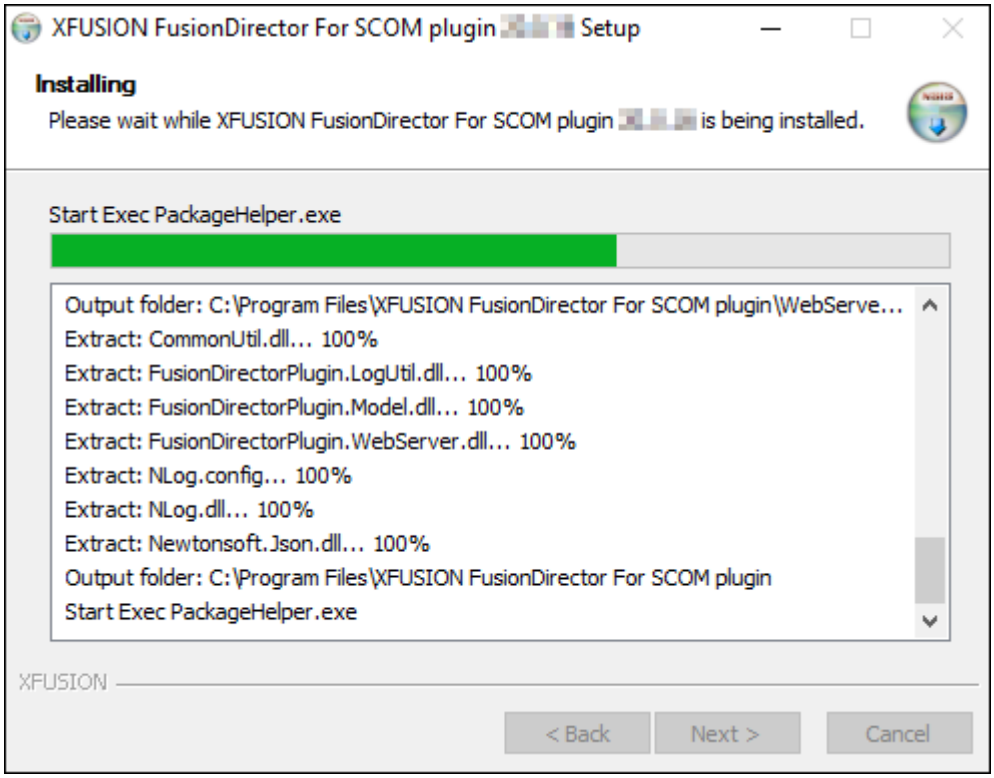
Step 9 Enter the FQND or IP address, port number and certificate password of the server that is used to connect to FusionDirector. Click **Install**.

NOTE

- The port number ranges from 44300 to 44399. You are advised to retain the default value **44301**.
- Default certificate password is **FusionCA**.

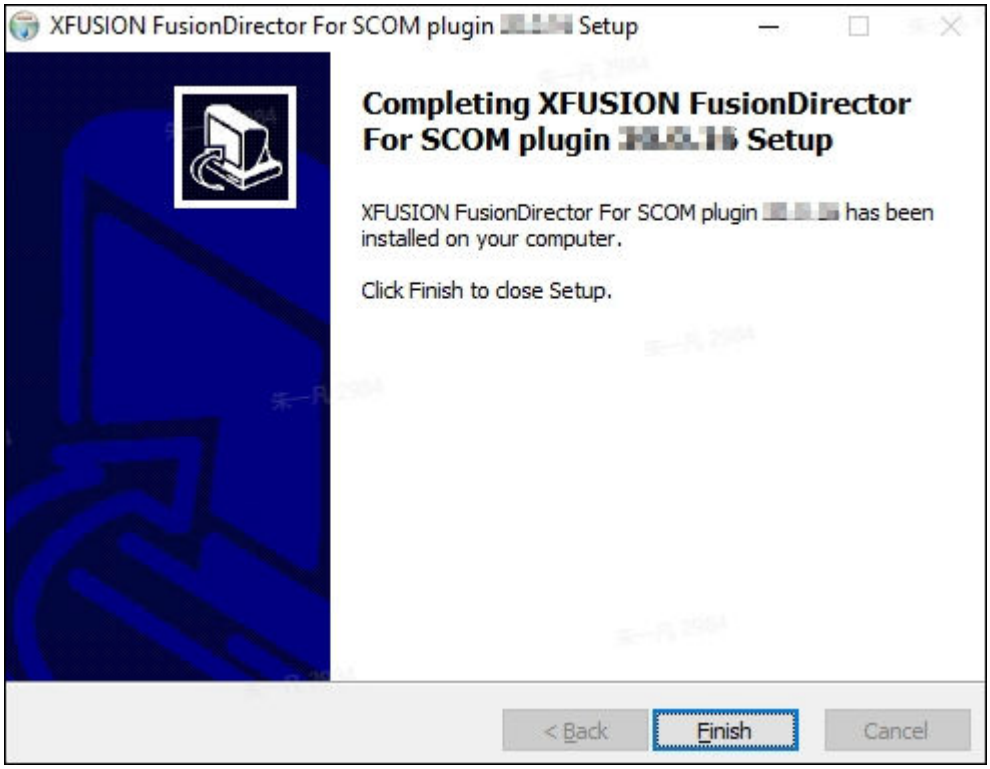
The SCOM plug-in installation starts, as shown in **Figure Installing the SCOM plug-in**.

Figure 2-6 Installing the SCOM plug-in



After the installation is complete, the completing the setup wizard is displayed, as shown in **Figure 2-7**.

Figure 2-7 Completing the setup



Step 10 Click **Finish**.

The SCOM plug-in installation is complete.

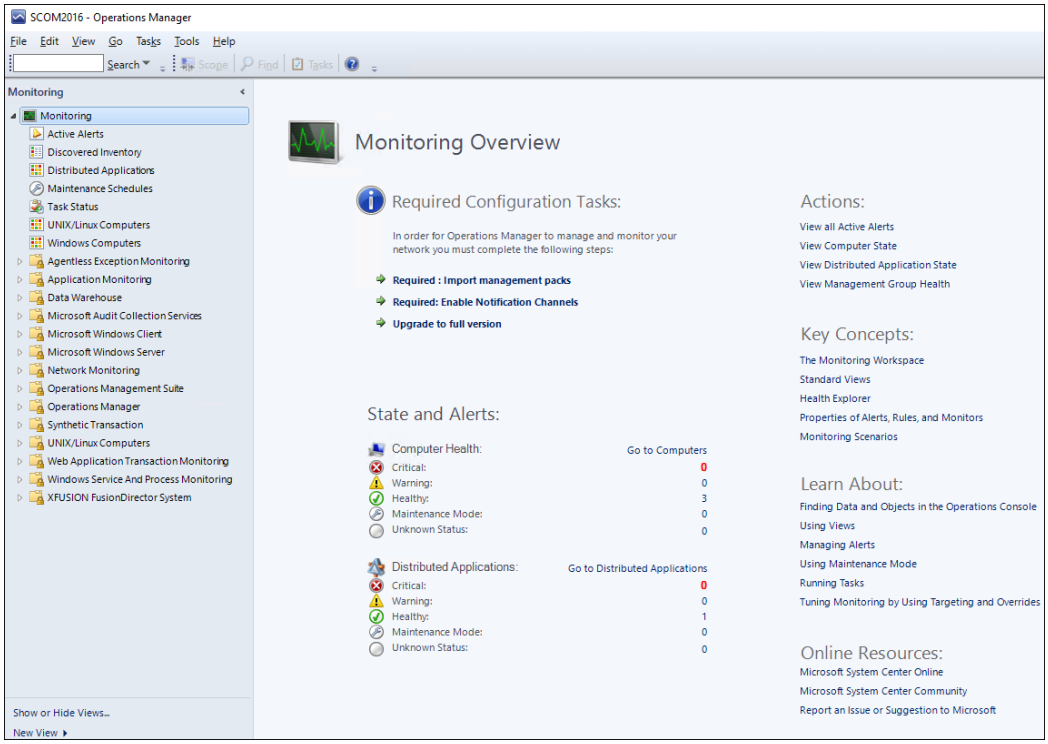
NOTE

After installation, replace the certificate as custom certificate. For details, see **How Do I Replace the Server Certificate?**.

Step 11 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed, as shown in **Figure 2-8**.

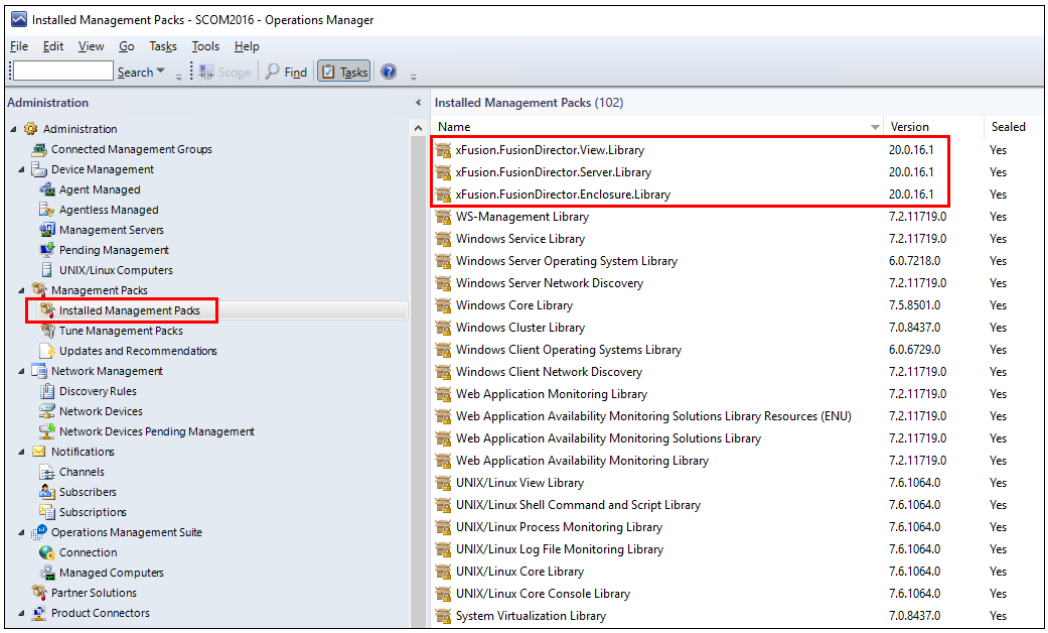
Figure 2-8 SCOM main window



Step 12 Choose **Administration** > **Management Packs**> **Installed Management Packs**.

The **Installed Management Packs** window is displayed, as shown in **Figure Installed Management Packs**.

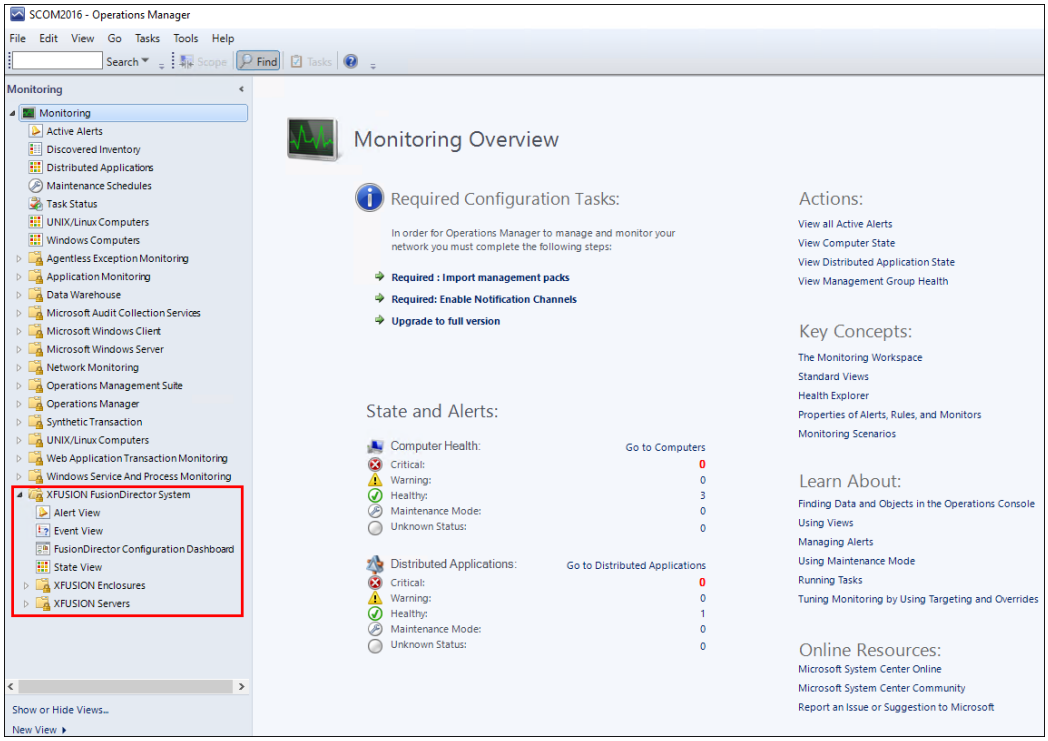
Figure 2-9 Installed Management Packs



After the SCOM plug-in is successfully installed, the Manage Package (MP) packages in the red box are displayed in the **Management Packs** window.

After the MP packages are successfully installed, the nodes in the red box are displayed in the SCOM main window, as shown in **Figure SCOM main window**.

Figure 2-10 SCOM main window



----End

2.2 Uninstalling the SCOM Plug-in

NOTE

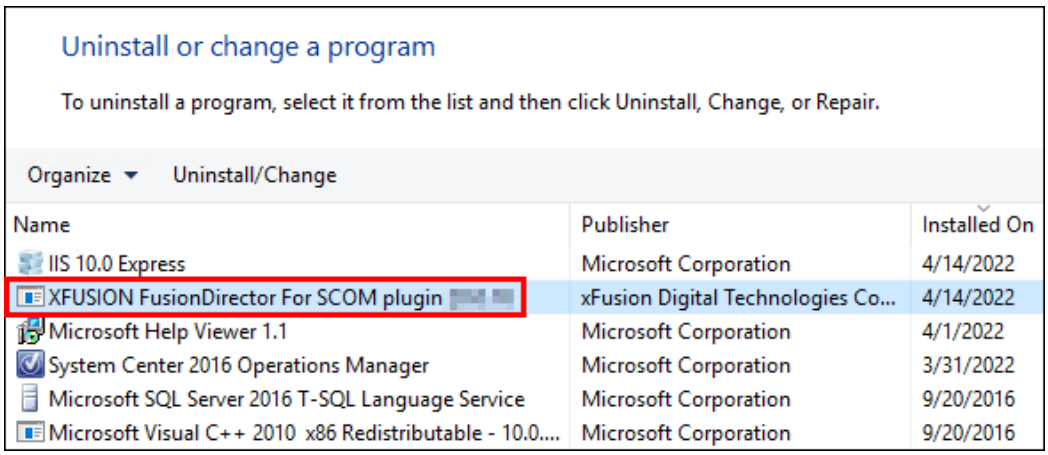
You need to close the SCOM window before uninstalling the SCOM plug-in.

2.2.1 Uninstalling the SCOM Plug-in from the Control Panel

Step 1 Choose **Start** > **Control Panel** > **Programs and Features** > **Uninstall a program**.

The **Uninstall or change a program** window is displayed, as shown in **Figure Uninstall or change a program**.

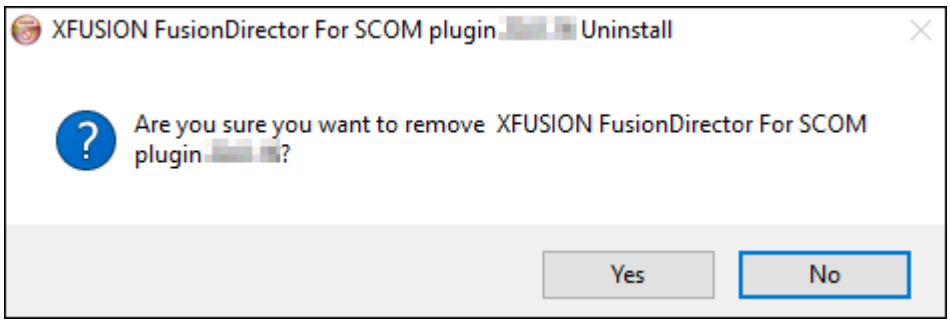
Figure 2-11 Uninstall or change a program



Step 2 Double-click the SCOM plug-in (for example,**XFUSION FusionDirector For SCOM plugin x.x.xx**).

A confirmation dialog box is displayed, as shown in **Figure Dialog box**.

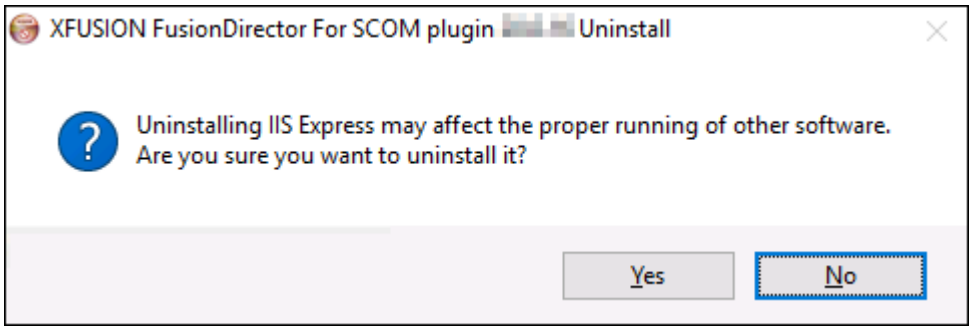
Figure 2-12 Dialog box



Step 3 Click **Yes**.

The dialog box asking you whether to uninstall IIS Express is displayed, as shown in **Figure 2-13**.

Figure 2-13 Dialog box



NOTE

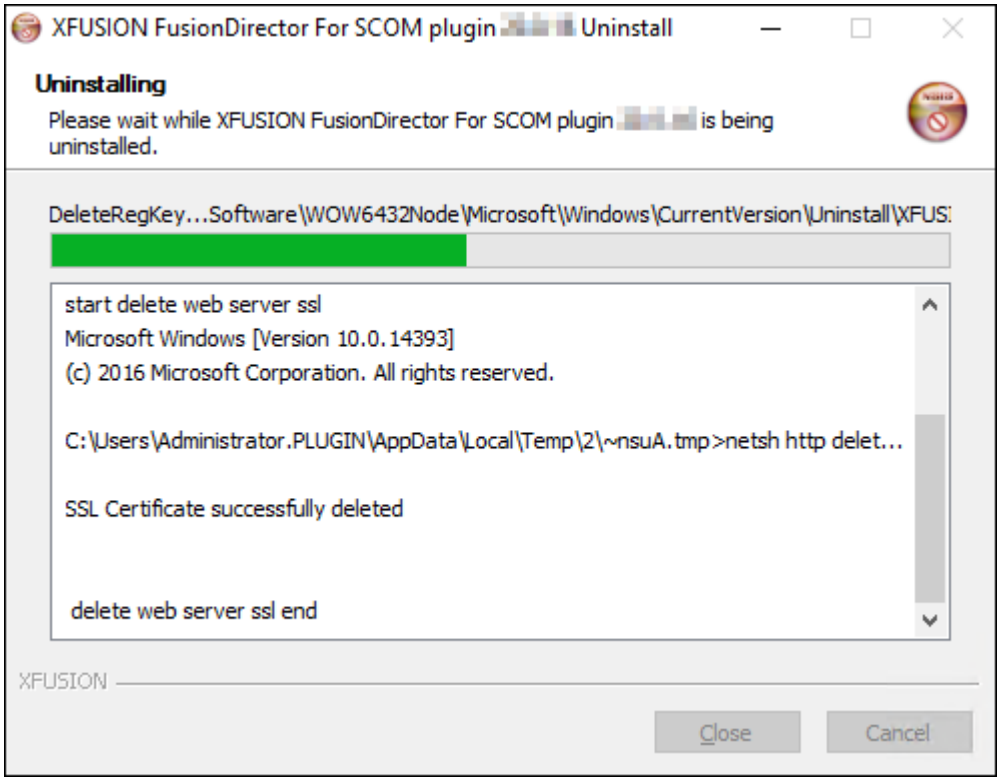
- IIS Express is responsible for the communication between the plug-in and FusionDirector. Uninstalling IIS Express may affect the proper running of other software. Exercise caution when performing this operation.
- If you uninstall IIS Express, it will be reinstalled when you install the SCOM plug-in again.

- If IIS Express needs to be uninstalled, click **Yes**.
- If IIS Express does not need to be uninstalled, click **No**.

Step 4 Click **Yes** or **No**.

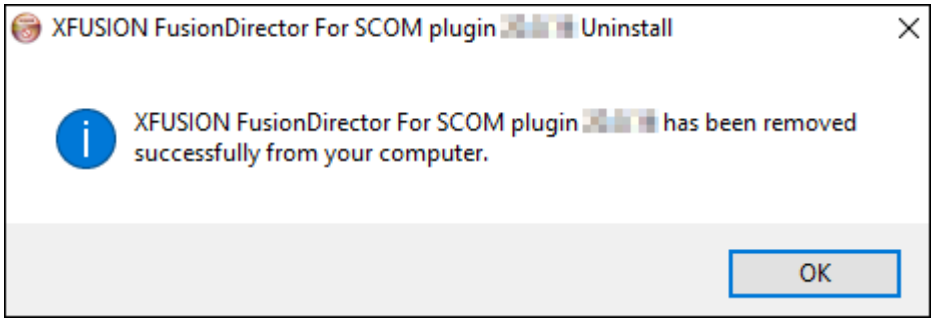
The SCOM plug-in uninstallation starts, as shown in **Figure Uninstalling the SCOM plug-in**.

Figure 2-14 Uninstalling the SCOM plug-in



After the uninstallation is complete, the dialog box shown in **Figure Uninstallation completed** is displayed.

Figure 2-15 Uninstallation completed



Step 5 Click **OK**.

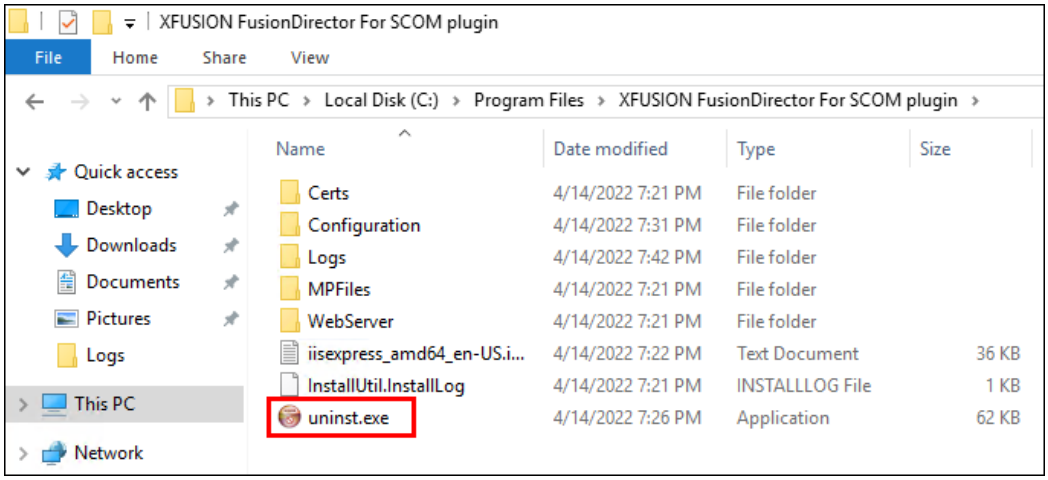
The SCOM plug-in is uninstalled.

----End

2.2.2 Uninstalling the SCOM Plug-in from the Installation Directory

Step 1 Go to the installation directory of the SCOM plug-in (**C:\Program Files\XFUSION Fusion Director For SCOM plugin** by default), as shown in **Figure Installation directory of the SCOM plug-in**.

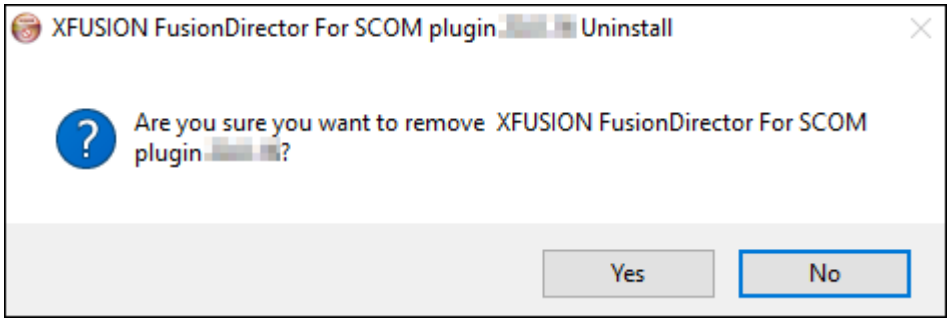
Figure 2-16 Installation directory of the SCOM plug-in



Step 2 Double-click **uninst**.

A confirmation dialog box is displayed, as shown in **Figure Dialog box**.

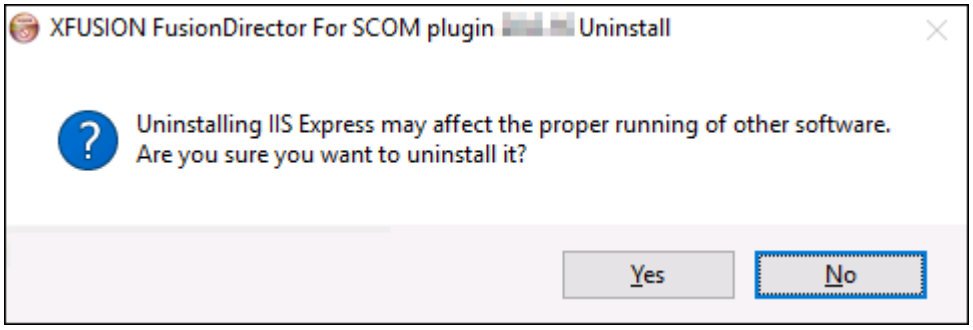
Figure 2-17 Dialog box



Step 3 Click **Yes**.

The dialog box asking you whether to uninstall IIS Express is displayed, as shown in **Figure 2-18**.

Figure 2-18 Dialog box



NOTE

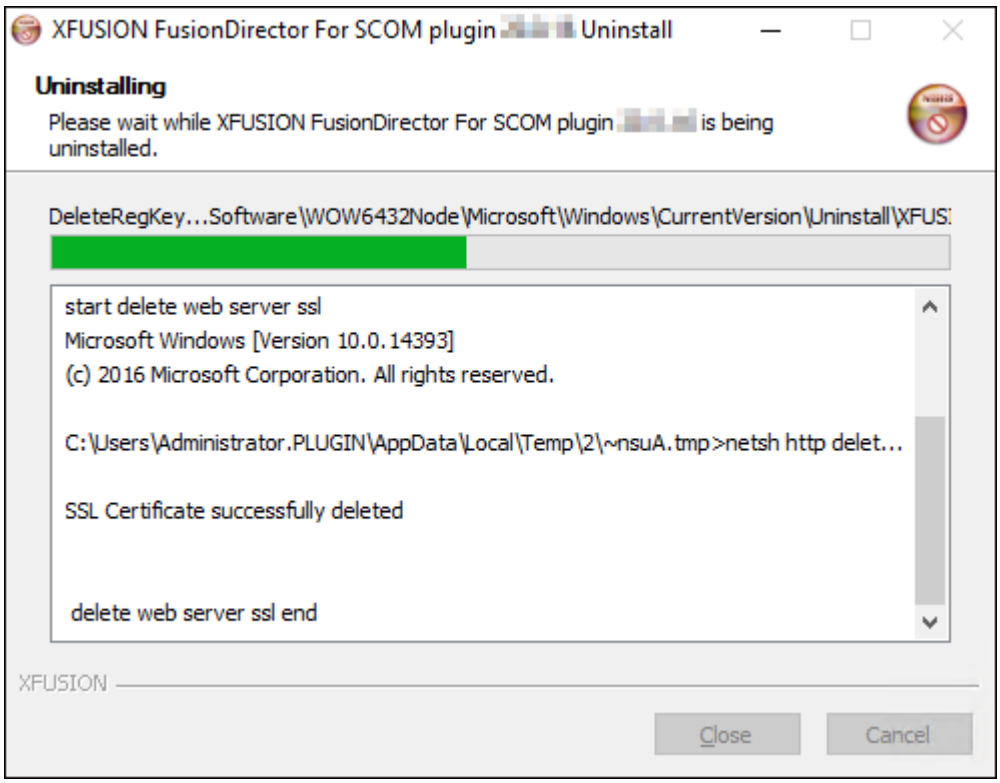
- IIS Express is responsible for the communication between the plug-in and FusionDirector. Uninstalling IIS Express may affect the proper running of other software. Exercise caution when performing this operation.
- If you uninstall IIS Express, it will be reinstalled when you install the SCOM plug-in again.

- If IIS Express needs to be uninstalled, click **Yes**.
- If IIS Express does not need to be uninstalled, click **No**.

Step 4 Click **Yes** or **No**.

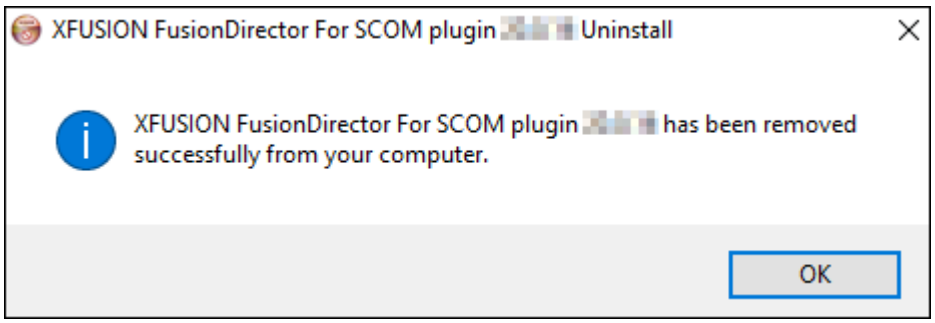
The SCOM plug-in uninstallation starts, as shown in **Figure Uninstalling the SCOM plug-in**.

Figure 2-19 Uninstalling the SCOM plug-in



After the uninstallation is complete, the dialog box shown in **Figure Uninstallation completed** is displayed.

Figure 2-20 Uninstallation completed



Step 5 Click **OK**.

The SCOM plug-in is uninstalled.

----End

2.3 Upgrading the SCOM plug-in

Step 1 Upload the installation package of the later version of the SCOM plug-in to the server.

Step 2 Log in to the server.

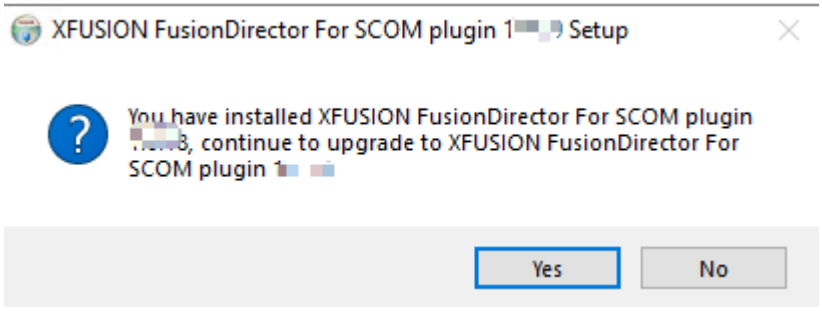
Step 3 Decompress the SCOM plug-in installation package of a later version.

Obtain the installation application, for example, **XFUSION_FusionDirector_For_SCOM_Plugin_*x.x.xx.xxx*.exe**.

Step 4 Double-click **XFUSION_FusionDirector_For_SCOM_Plugin_*x.x.xx.xxx*.exe**.

The confirmation dialog box is displayed, as shown in**Figure 2-21**.

Figure 2-21 Dialog box



Step 5 Click **Yes**.

The welcome to the setup wizard window is displayed, as shown in **Figure 2-22**.

NOTE

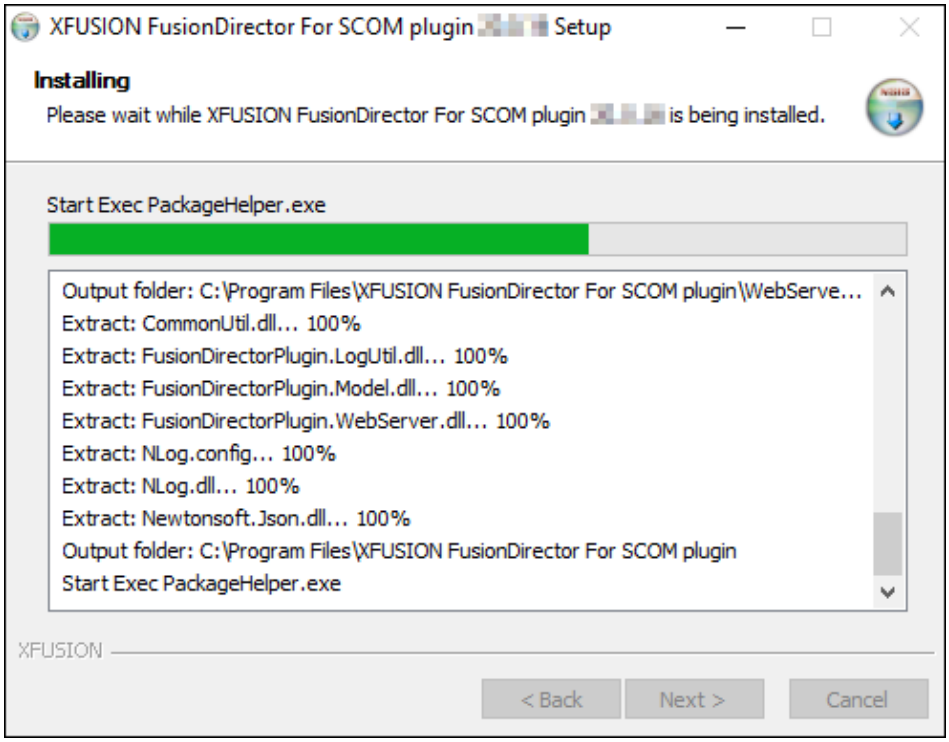
If the SCOM program has been already started during the SCOM plug-in upgrade, you need to close the program.

Figure 2-22 Welcome to the setup

Step 6 Click **Next**.

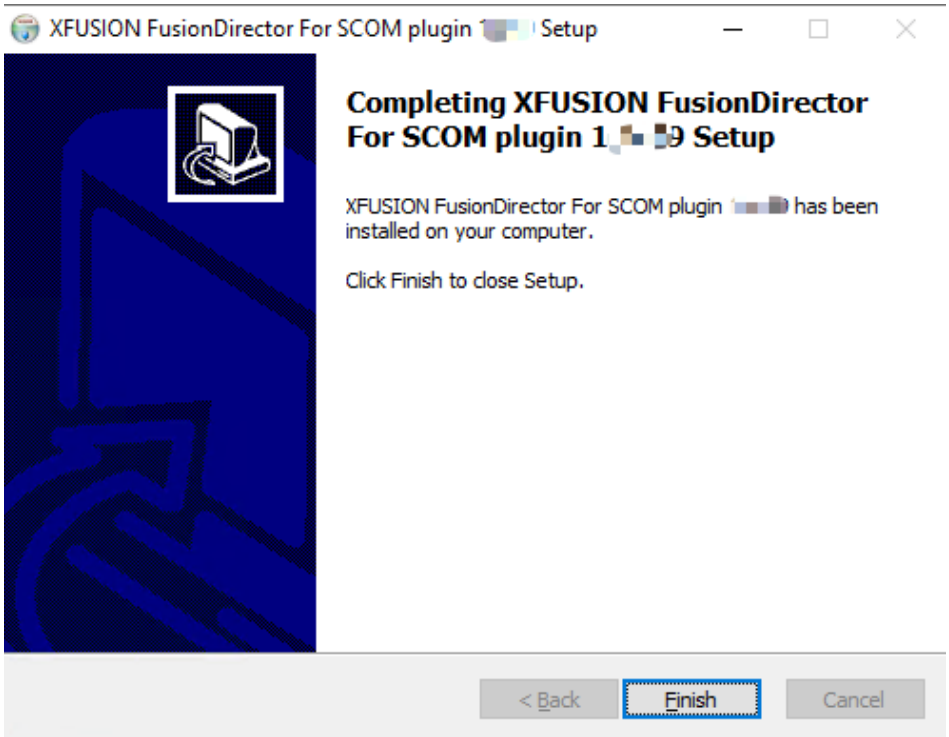
The **Choose Install Location** window is displayed, as shown in **Figure 2-23**.

Figure 2-23 Choose Install Location



After the installation is complete, the completing the setup wizard is displayed, as shown in **Figure 2-24**.

Figure 2-24 Completing the setup



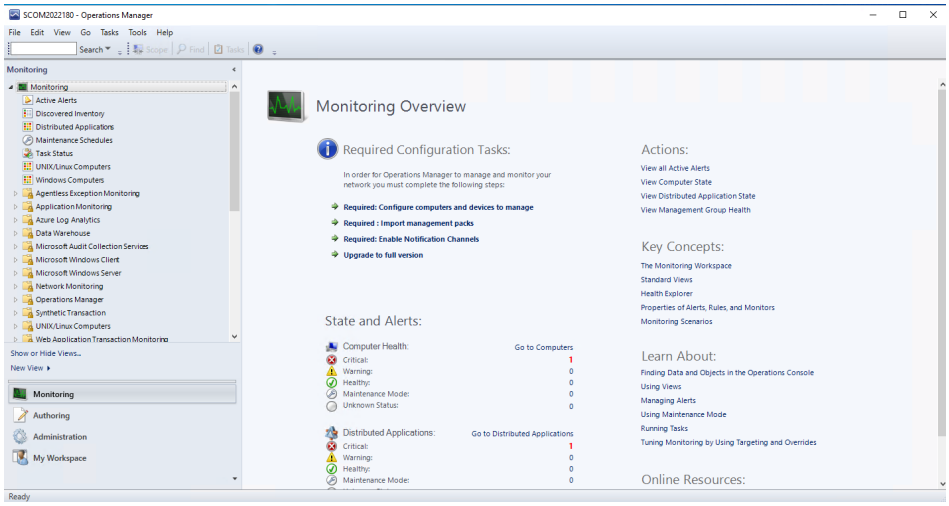
Step 7 Click **Finsh**.

After the SCOM plug-in is upgraded, a dialog box is displayed indicating the immediate start of SCOM.

Step 8 Click **Yes**.

The SCOM main window is displayed, as shown in **Figure 2-25**.

Figure 2-25 SCOM main window



----End

3 Configuring FusionDirector

3.1 Adding FusionDirector
3.2 Editing FusionDirector
3.3 Deleting FusionDirector

3.1 Adding FusionDirector

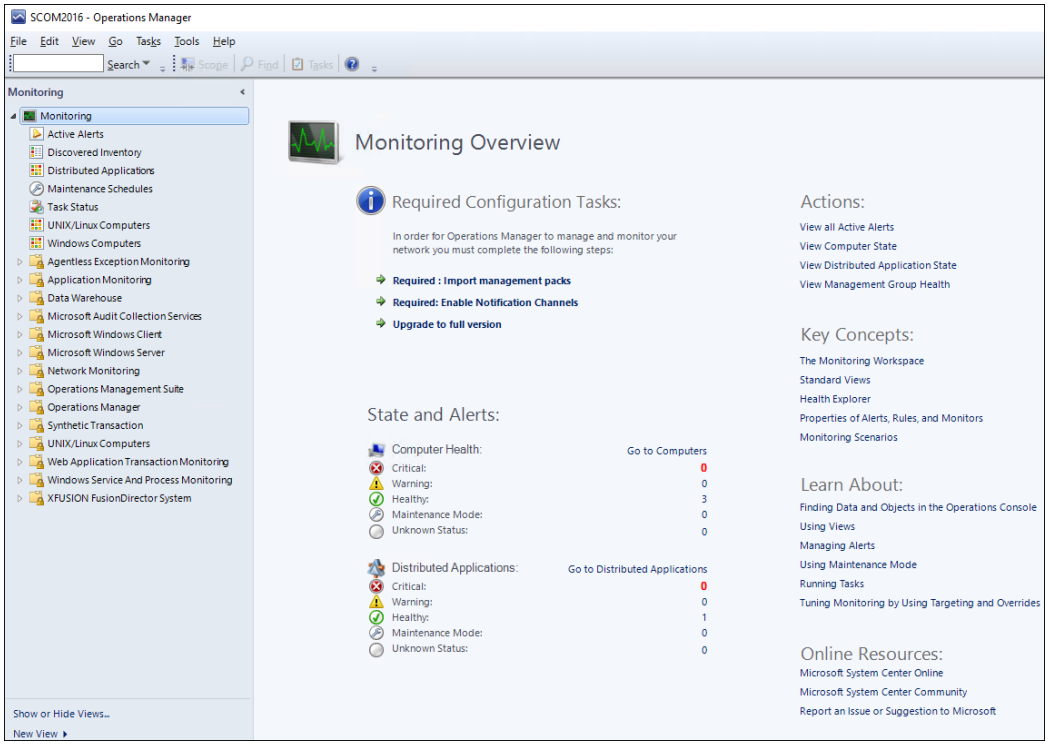
NOTE

- A maximum of 10 FusionDirector instances can be added.
- When adding FusionDirector 1.6.1 or later on the Windows Server 2012 R2 environment with SCOM installed, you need to install the Windows OS patch (2919355) and add the cipher suite supported by FusionDirector. For details, see **7.3 What Do I Do If the System Displays a Message Indicating that the SSL/TLS Secure Channel Fails to Be Created When FusionDirector Is Added?**.

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed, as shown in **Figure 3-1**.

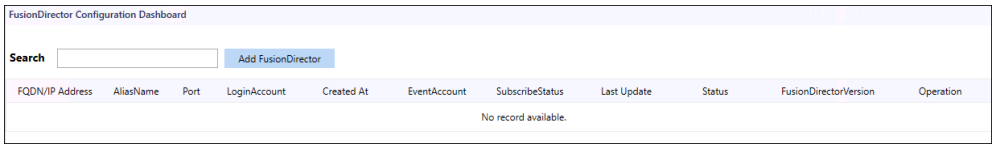
Figure 3-1 SCOM main window



Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **FusionDirector Configuration View**.

The **FusionDirector Configuration Dashboard** window is displayed, as shown in **Figure FusionDirector Configuration Dashboard**.

Figure 3-2 FusionDirector Configuration Dashboard



Step 3 Click **Add FusionDirector**.

The **Add FusionDirector** dialog box is displayed, as shown in **Figure 3-3**.

Figure 3-3 Add FusionDirector

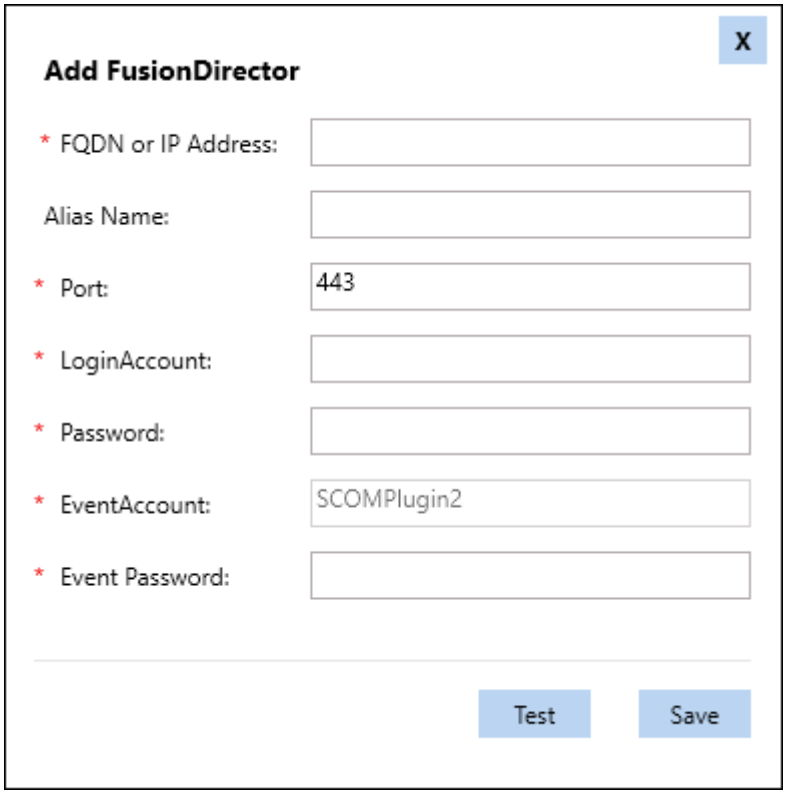


Table 3-1 describes the parameters in this dialog box.

Table 3-1 Parameter description

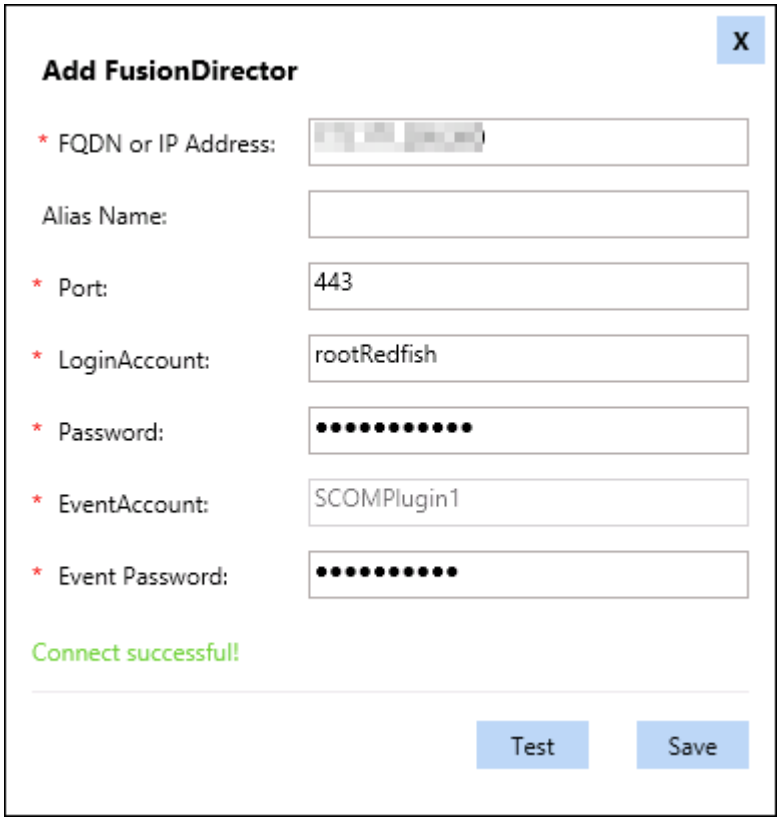
Parameter	Description	Value	Mandatory
FQDN or IP Address	FQDN or IP address of FusionDirector.	The IP address format is XXX.XXX.XXX.XXX. Each X must be an integer.	Yes
Alias Name	Customized FusionDirector name.	The value is a string of 1 to 100 characters, including letters, digits, underscores (_), hyphens (-), and dots (.).	No
Port	FusionDirector port number.	The default value is **443**.	Yes
LoginAccount	FusionDirector user name.	The default value is **rootRedfish**.	Yes
Password	FusionDirector password.	The default value is **Machine@123**.	Yes
Event Account	Alarm service account.	The value is automatically generated by the system.	Yes

Parameter	Description	Value	Mandatory
Event Password	Alarm service password.	The password contains 8 to 32 characters, including uppercase letters, lowercase letters, digits, and special characters. Special characters include '~!@$%^&*()-_=+|[{}];:'",<>/?.	Yes

Step 4 Enter FusionDirector information, and click **Test** to test whether the server can connect to FusionDirector.

If the test is successful, "Connect successful" is displayed, as shown in **Figure 3-4**. If the test fails, the failure cause is displayed. Modify FusionDirector information as prompted.

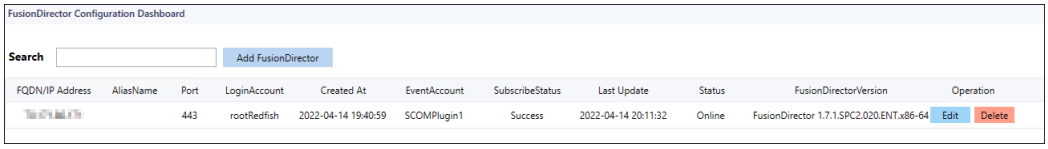
Figure 3-4 Successful test



Step 5 Click **Save**.

The FusionDirector is added successfully, as shown in **Figure 3-5**.

Figure 3-5 FusionDirector added successfully



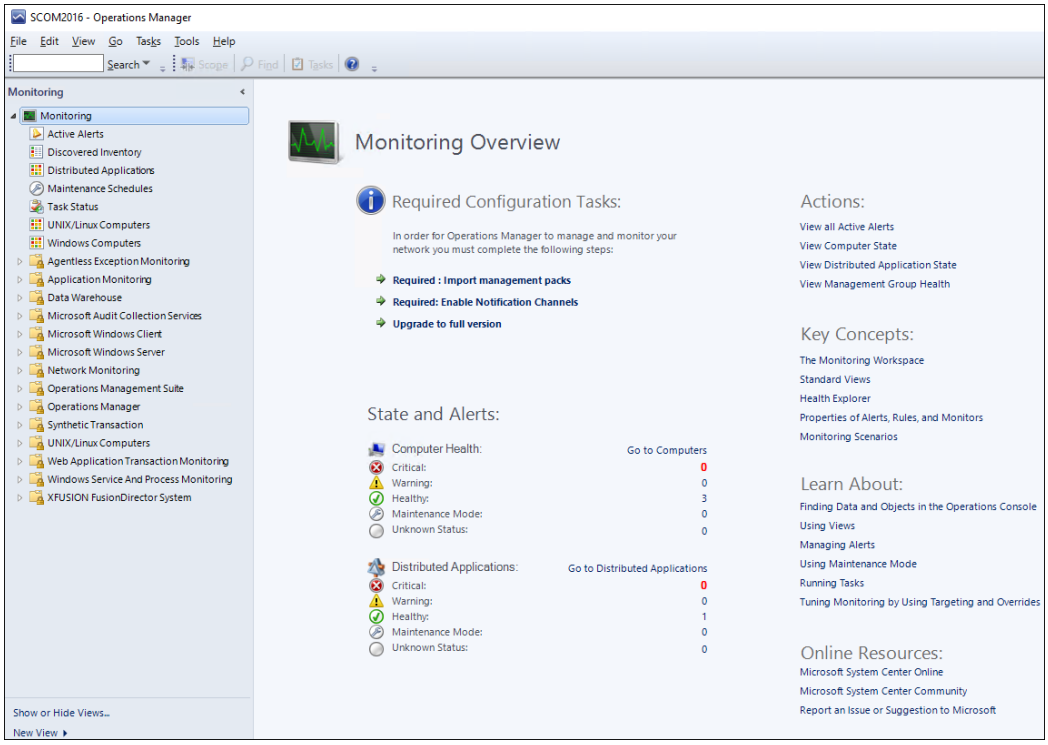
----End

3.2 Editing FusionDirector

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed, as shown in **Figure 3-6**.

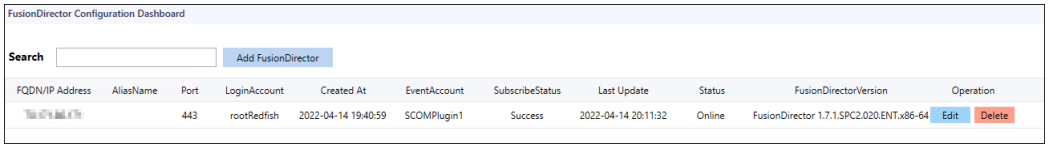
Figure 3-6 SCOM main window



Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **FusionDirector Configuration Dashboard**.

The **FusionDirector Configuration Dashboard** window is displayed, as shown in **Figure FusionDirector Configuration Dashboard**.

Figure 3-7 FusionDirector Configuration Dashboard



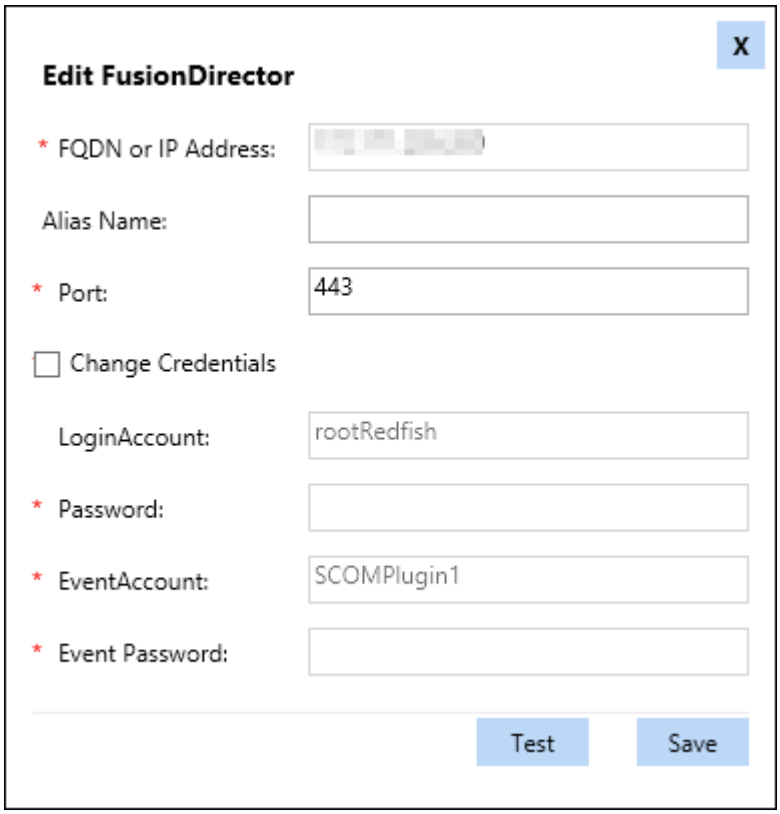
NOTE

If the FusionDirector information is empty, no FusionDirector is added.

Step 3 In the **Operation** column, click Edit.

The **Edit FusionDirector** dialog box is displayed, as shown in **Figure 3-8**.

Figure 3-8 Edit FusionDirector



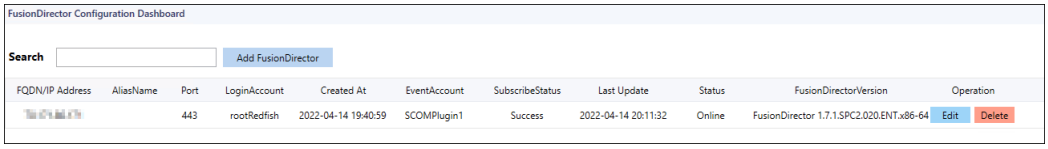
Step 4 Edit the FusionDirector information according to **Table 3-1**, and click **Save**.

NOTICE

- The FusionDirector IP address cannot be modified.
- You can change the FusionDirector user name and password only after selecting **Change Credentials**. After changing the user name and password, click **Test**.

The FusionDirector is successfully edited, as shown in **Figure 3-9**. In this window, you can check whether the modified information is consistent with the target.

Figure 3-9 Modified FusionDirector information



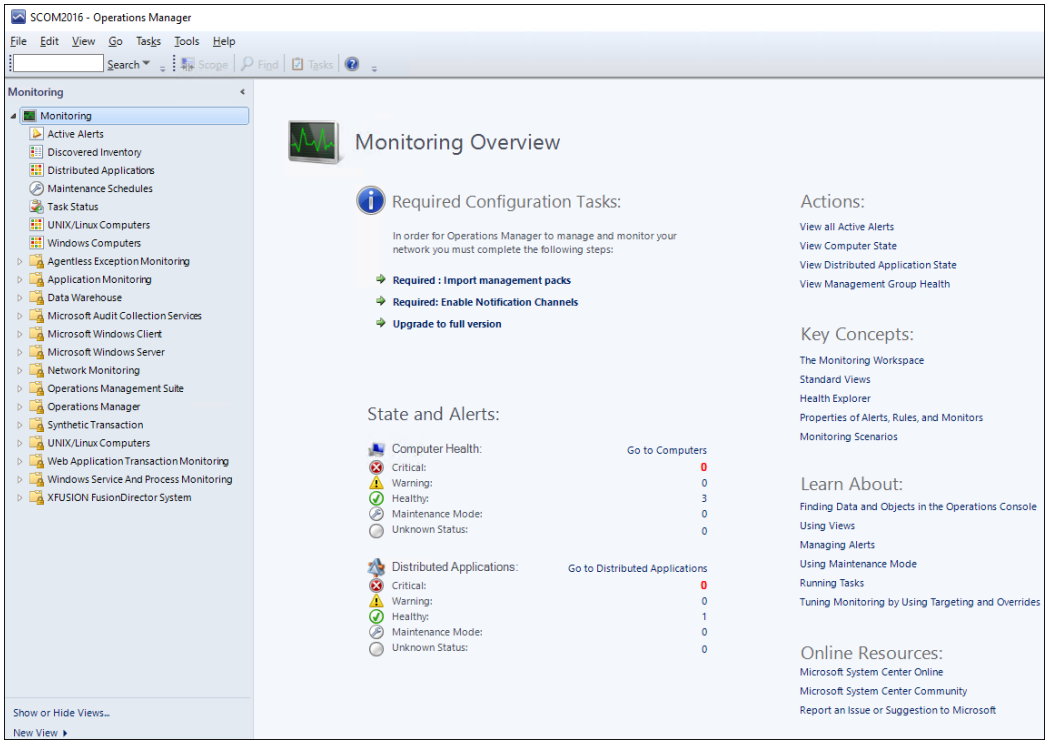
----End

3.3 Deleting FusionDirector

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed, as shown in **Figure 3-10**.

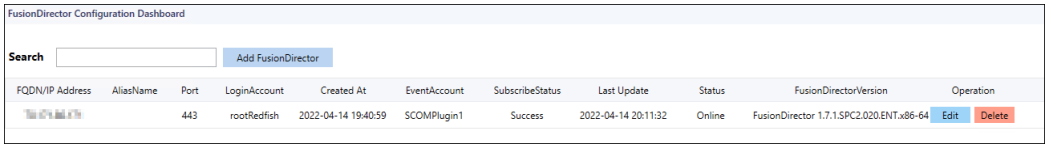
Figure 3-10 SCOM main window



Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **FusionDirector Configuration Dashboard**.

The **FusionDirector Configuration Dashboard** window is displayed, as shown in **Figure FusionDirector Configuration Dashboard**.

Figure 3-11 FusionDirector Configuration Dashboard



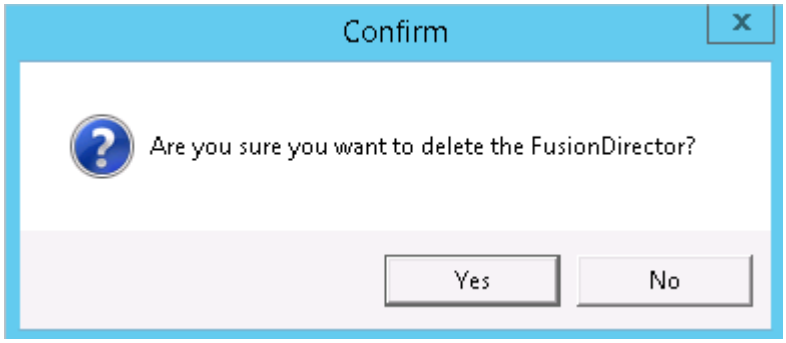
NOTE

If the FusionDirector information is empty, no FusionDirector is added.

Step 3 In the **Operation** column, click **Delete**.

The **Delete FusionDirector** dialog box is displayed, as shown in **Figure 3-12**.

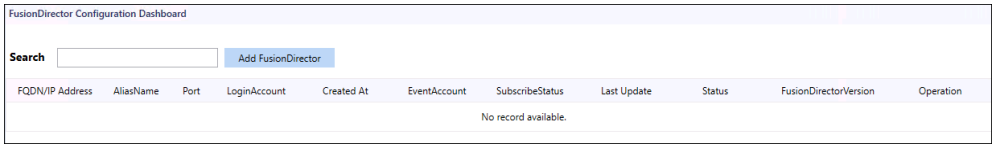
Figure 3-12 Delete FusionDirector



Step 4 Click **OK**.

The FusionDirector is successfully deleted, as shown in **Figure 3-13**. In this window, you can check whether the target FusionDirector is deleted.

Figure 3-13 FusionDirector deleted successfully



----End

4 Viewing Plug-in System Information

4.1 Viewing the Basic Plug-in System Information and Status

4.2 Viewing a Plug-in System Event List

4.3 Viewing a Plug-in System Alarm List

4.1 Viewing the Basic Plug-in System Information and Status

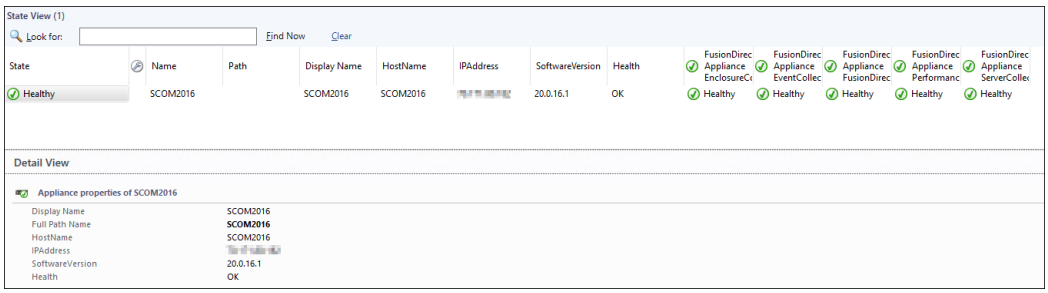
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **State View**.

The **State View** window is displayed, as shown in **Figure 4-1**.

Figure 4-1 State View



Each column in this window displays the running status of each function of the plug-in.

- **FusionDirector Appliance EnclosureCollection**: chassis monitoring function
- **FusionDirector Appliance EventCollection**: event monitoring function
- FusionDirector Appliance FusionDirectorCollection: FusionDirector monitoring function

- **FusionDirector Appliance PerformanceCollection**: performance curve monitoring function
- **FusionDirector Appliance ServerCollection**: server monitoring function

You can click anywhere in the row of the plug-in in the **State View** area to view details about the plug-in in the **Detail View** area.

NOTE

The component health status is described as follows:

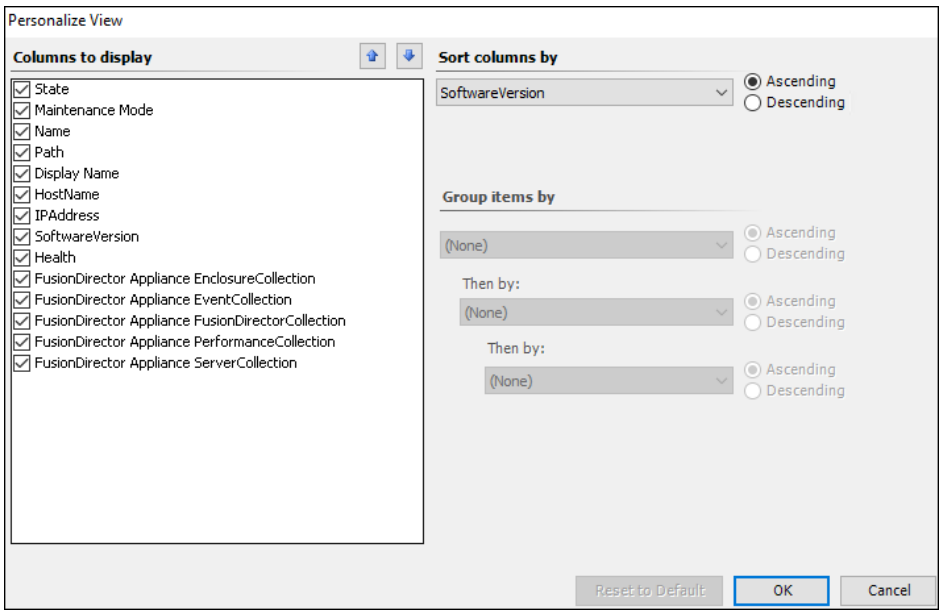
- Healthy: healthy
- Warning: minor alarms
- Critical: major or critical alarms

Step 3 Set the parameters to be displayed.

1. Right-click a plug-in name or monitoring status and choose **Personalize View...** from the shortcut menu.

   The **Personalize View** window is displayed, as shown in **Figure 4-2**.

   Figure 4-2 Personalize View



2. Select parameters to be viewed and click **OK**.

   The parameters to be viewed are modified successfully.

----End

4.2 Viewing a Plug-in System Event List

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **Event View**.

The **Event View** window is displayed. You can click the event to be viewed to view the details of the event in the **Event Data** area, as shown in **Figure 4-3**.

Figure 4-3 Event View

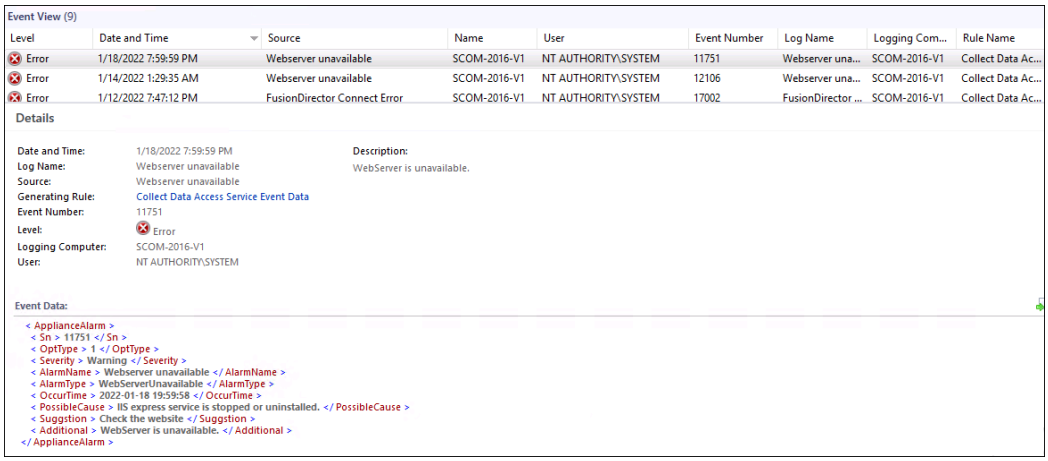


Table 4-1 describes the parameters.

Table 4-1 Parameter description

Parameter	Description
Level	Event type. The options are as follows: ● **Information**: running event ● **Warning**: minor alarm ● **Error**: major or critical alarm
Date and Time	Date and time when the event is generated.
Source	Event source, which is the component where the event is generated.
Name	Device where the event is generated.
User	Current user.
Event Number	Event number.
Log Name	Event name.
Logging Computer	Current login device.
Rule Name	Rule name.

----End

4.3 Viewing a Plug-in System Alarm List

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **Alert View**.

The **Alert View** window is displayed. You can click an alarm to view its details, as shown in **Figure 4-4**.

Figure 4-4 Alert View

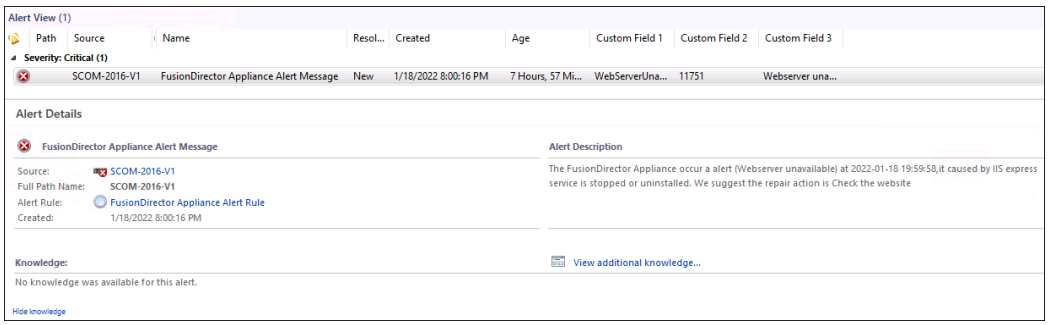


Table 4-2 describes the parameters.

Table 4-2 Parameter description

Parameter	Description
Icon	Alarm type. The options are as follows: • **Warning**: minor alarm • **Critical**: major or critical alarm
Path	Sensor that generates the alarm.
Source	Device where the alarm is generated.
Maintenance Mode	Maintenance mode.
Name	Alarm name.
Resolution State	Handling status.
Created	Time when the alarm is generated.
Age	Duration of the alarm.
Owner	Owner.
Priority	Priority.
Latency	Latency.

Parameter	Description
Description	Alarm description.
Class	Alarm type.
Time in State	Alarm duration.
Repeat Count	Number of repeated occurrence times.
Custom Field 1	Alarm type.
Custom Field 2	Alarm code.
Custom Field 3	Alarm name.
Custom Field 4	Possible cause.
Custom Field 5	Remarks.
Custom Field 6	Alarm clearance suggestion.
Custom Field 7	Alarm occurrence time.

----End

5 Viewing Chassis Information

5.1 Viewing the Basic Chassis Information and Status

5.2 Viewing a Chassis Topology

5.3 Viewing a Chassis Alarm List

5.1 Viewing the Basic Chassis Information and Status

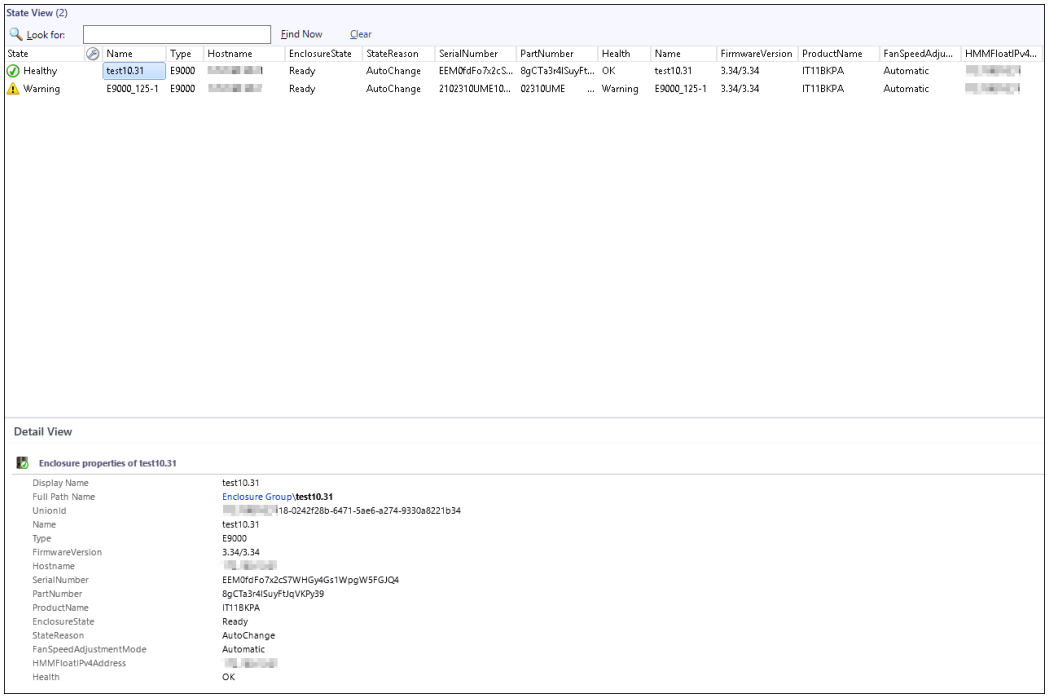
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** >**XFUSION Enclosures** > **State View**.

The **State View** window is displayed, as shown in **Figure 5-1**. In this window, the managed chassis are displayed in different rows and monitoring parameters of chassis are displayed in different columns.

Figure 5-1 State View



In the **State View** area, you can click any position in the row of a chassis to view details about the chassis in the **Detail View** area.

NOTE

The chassis health status is described as follows:

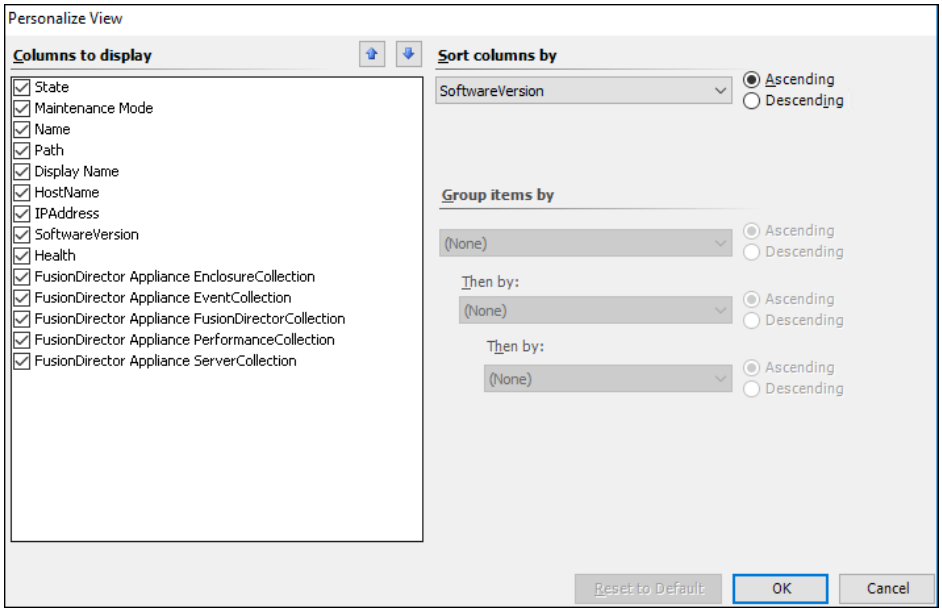
- Healthy: healthy
- Warning: minor alarms
- Critical: major or critical alarms

Step 3 Set the parameters to be displayed.

1. Right-click a chassis name and choose **Personalize View...** from the shortcut menu.

   The **Personalize View** window is displayed, as shown in **Figure 5-2**.

Figure 5-2 Personalize View



2. Select parameters to be viewed and click **OK**.

   The parameters to be viewed are modified successfully.

   Table 5-1 describes the parameters that can be viewed by the SCOM plug-in.

Table 5-1 Components and parameters that can be viewed

Parameter	Description
State	Chassis presence status.
Name	Server name.
Type	Server model.
Hostname	Host name.
StateReason	Reason of the chassis presence status.
SerialNumber	Serial number.
PartNumber	Component number.
Health	Chassis health status.
FirmwareVersion	HMM version.
ProductName	Product name.
FanSpeedAdjustmentMode	Fan speed adjustment mode.
HMMFloatIPv4Address	HMM floating IP address.

----End

5.2 Viewing a Chassis Topology

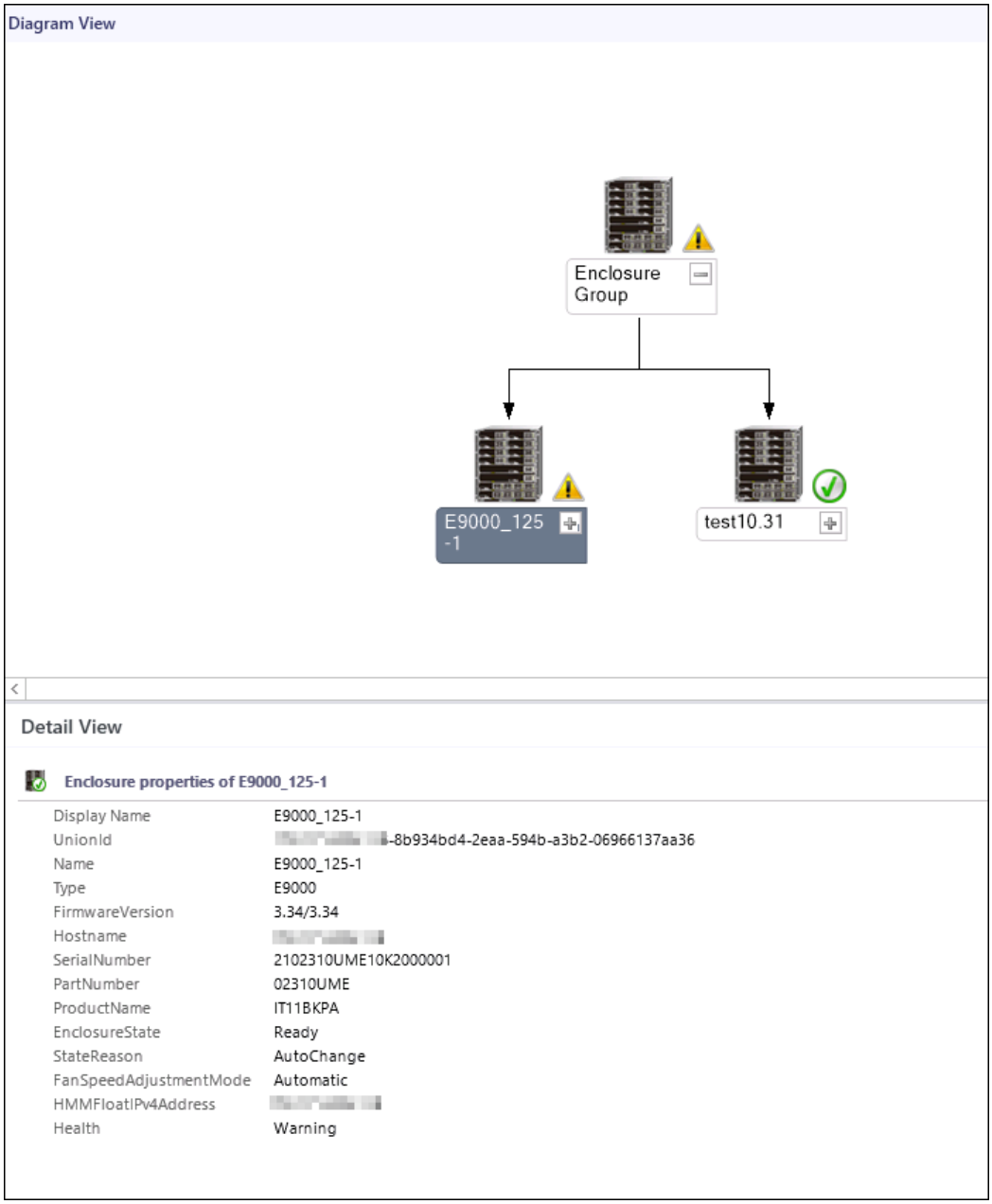
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** >**XFUSION Enclosures** > **Diagram View**.

The **Diagram View** window is displayed, as shown in **Figure 5-3**.

Figure 5-3 Diagram View



NOTE

If the topology is not refreshed in time, you can perform the following steps to refresh it:

1. Open the CLI of the server.
2. Access the SCOM installation path (**C:\Program Files\System Center Operations Manager 2012\Console**) on the CLI.
3. Run the following command to refresh the SCOM window:

   Microsoft.EnterpriseManagement.Monitoring.Console.exe" /clearcache

----End

5.3 Viewing a Chassis Alarm List

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Enclosures** > **Alert View**.

In the **Alert View** window that is displayed, click an alarm to view its details, as shown in **Figure 5-4**.

NOTE

The FusionDirector that is added for the first time synchronously displays historical alarms that are not cleared.

Figure 5-4 Alert View

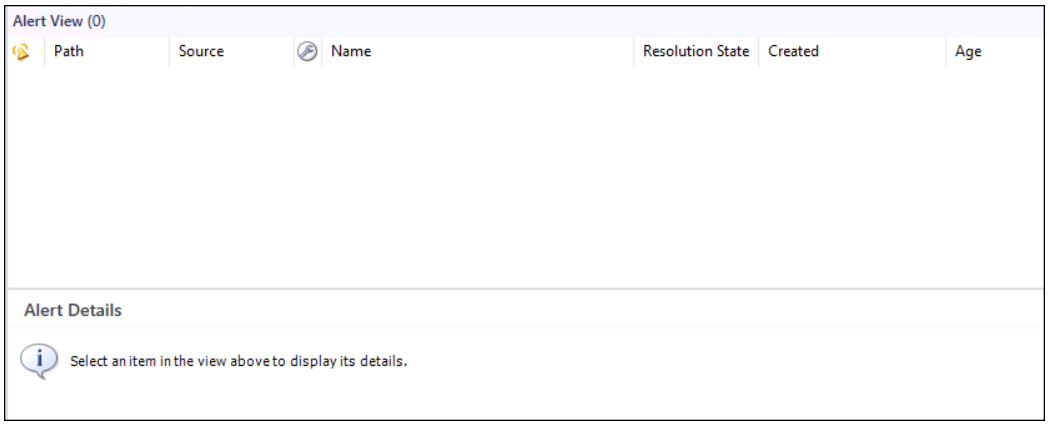


Table 5-2 describes the parameters.

Table 5-2 Parameter description

Parameter	Description
Icon	Alarm type. The options are as follows: ● **Warning**: minor alarm ● **Critical**: major or critical alarm
Path	Sensor that generates the alarm.
Source	Device where the alarm is generated.
Maintenance Mode	Maintenance mode.
Name	Alarm name.
Resolution State	Handling status.
Created	Time when the alarm is generated.
Age	Duration of the alarm.
Owner	Owner.
Priority	Priority.
Latency	Latency.
Description	Alarm description.
Class	Alarm type.
Time in State	Alarm duration.
Repeat Count	Number of repeated occurrence times.

----End

6 Viewing Server Information

6.1 Viewing the Basic Server Information and Status

6.2 Viewing a Server Topology

6.3 Viewing a Server Alarm List

6.4 Viewing Server Performance Curves

6.1 Viewing the Basic Server Information and Status

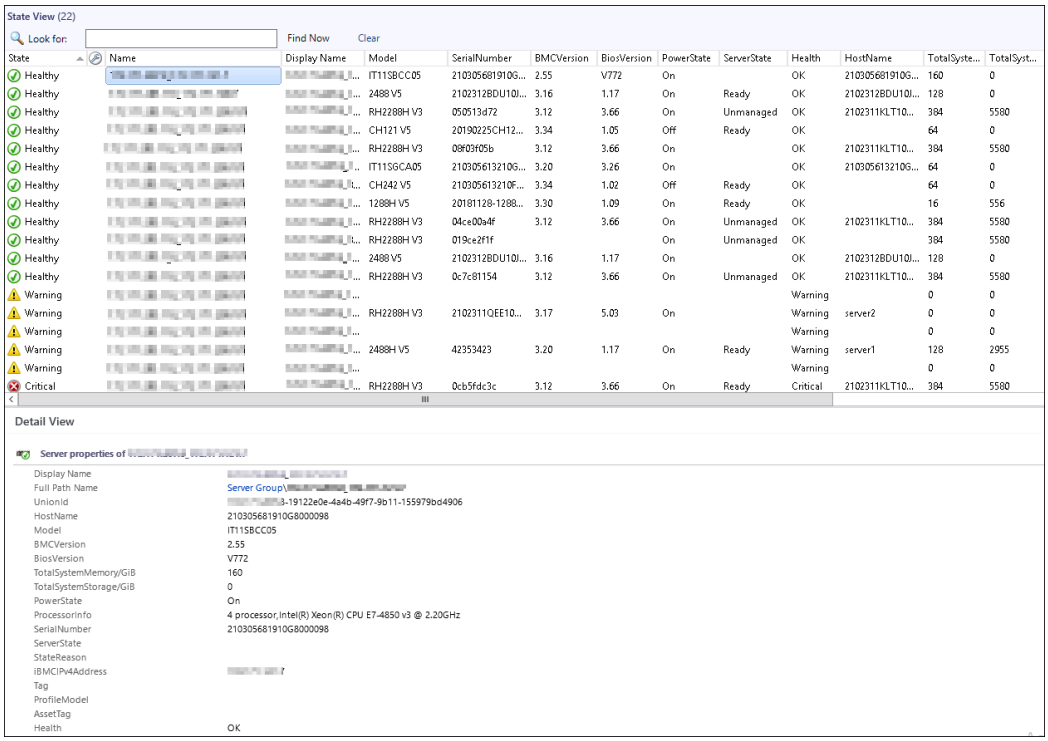
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Servers** > **State View**.

The **State View** window is displayed, as shown in **Figure 6-1**. In this window, the managed servers are displayed in different rows and status monitoring parameters of monitored components on each server are displayed in different columns.

Figure 6-1 State View



In the **State View** area, you can click any position in the row of a server to view details about the server in the **Detail View** area.

NOTE

- The server information is updated at most every four hours.
- The server health status is described as follows:
  - Healthy: healthy
  - Warning: minor alarms
  - Critical: major or critical alarms

Step 3 Set the parameters to be displayed. For details, see **Step 3** in **5.1 Viewing the Basic Chassis Information and Status**.

Table 6-1 describes server parameters that can be monitored by the SCOM plug-in.

Table 6-1 Parameter description

Parameter	Description
State	Server presence status.
Model	Server model.
SerialNumber	Serial number.
Tag	Server tag.

Parameter	Description
AssetTag	Asset tag.
BMCVersion	iBMC version.
BiosVersion	BIOS version.
PowerState	Power status.
Health	Server health status.
HostName	Host name.
TotalSystemMemory/GiB	Memory size.
TotalSystemStorage/GiB	Storage size.
ProcessorInfo	CPU information.
StateReason	Reason of the server presence status.
iBMCIPv4Address	iBMC IP address.
ProfileModel	Configuration file type.
UUID	Universally Unique Identifier.

----End

6.2 Viewing a Server Topology

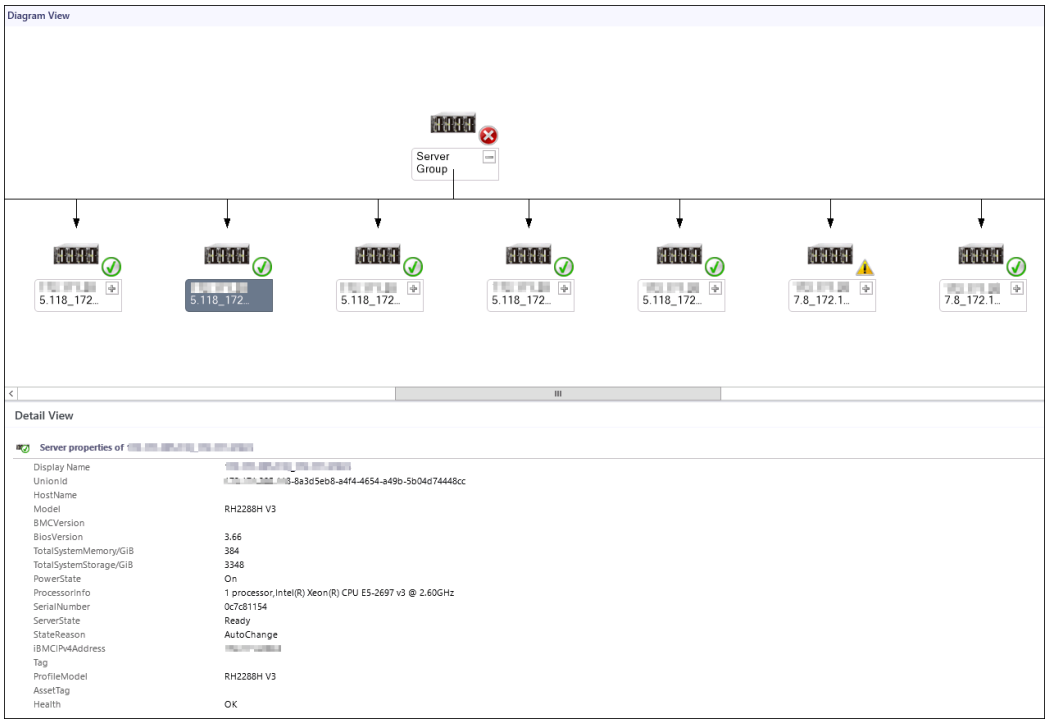
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Servers** > **Diagram View**.

The **Diagram View** window is displayed, as shown in **Figure 6-2**.

Figure 6-2 Diagram View



NOTE

If the topology is not refreshed in time, you can perform the following steps to refresh it:

1. Open the CLI of the server.
2. Access the SCOM installation path (**C:\Program Files\System Center Operations Manager 2012\Console**) on the CLI.
3. Run the following command to refresh the SCOM window:

   Microsoft.EnterpriseManagement.Monitoring.Console.exe" /clearcache

----End

6.3 Viewing a Server Alarm List

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **xFuson FusionDirector System** > **XFUSION Servers** > **Alert View**.

In the **Alert View** window that is displayed, click an alarm to view its details, as shown in **Figure 6-3**.

NOTE

The FusionDirector that is added for the first time synchronously displays historical alarms that are not cleared.

Figure 6-3 Alert View

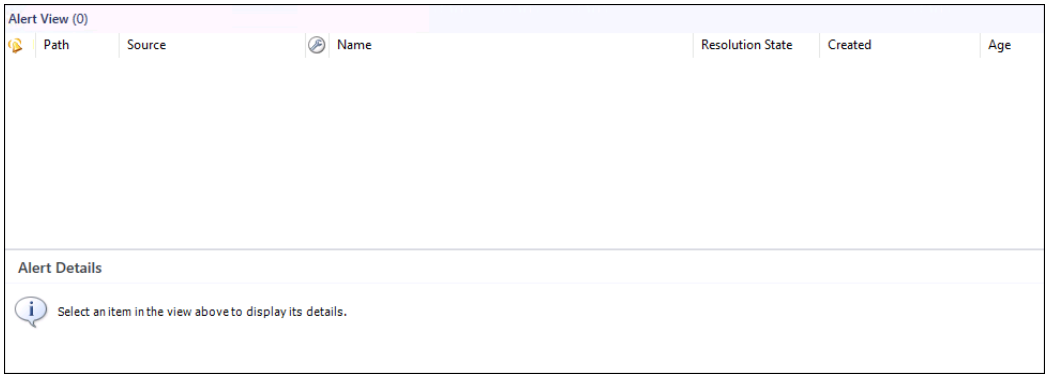


Table 6-2 describes the parameters.

Table 6-2 Parameter description

Parameter	Description
Icon	Alarm type. The options are as follows: ● **Warning**: minor alarm ● **Critical**: major or critical alarm
Path	Sensor that generates the alarm.
Source	Device where the alarm is generated.
Maintenance Mode	Maintenance mode.
Name	Alarm name.
Resolution State	Handling status.
Created	Time when the alarm is generated.
Age	Duration of the alarm.
Owner	Owner.
Priority	Priority.
Latency	Latency.
Description	Alarm description.
Class	Alarm type.
Time in State	Alarm duration.
Repeat Count	Number of repeated occurrence times.

----End

6.4 Viewing Server Performance Curves

You can view performance curves only of servers whose **ServerState** is **Ready**.

6.4.1 Viewing the CPU Usage

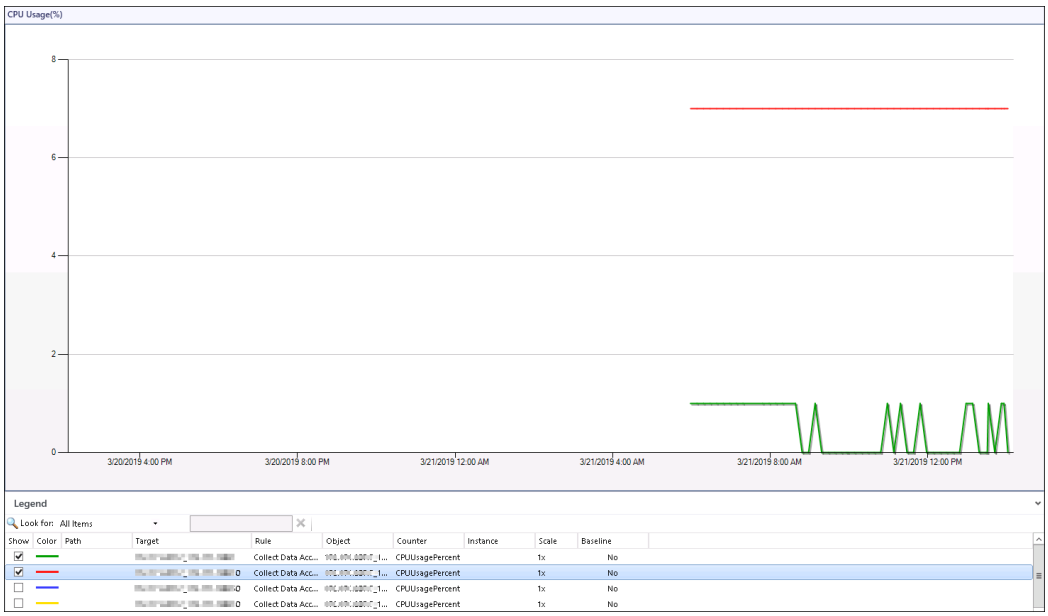
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Servers** > **Performance View** > **CPU Usage(%)**.

The **CPU Usage(%)** window is displayed, as shown in **Figure 6-4**.

Figure 6-4 CPU Usage(%)



Step 3 Select servers in the **Legend** area to view the CPU usage curves of the servers.

----End

6.4.2 Viewing the Air Inlet Temperature

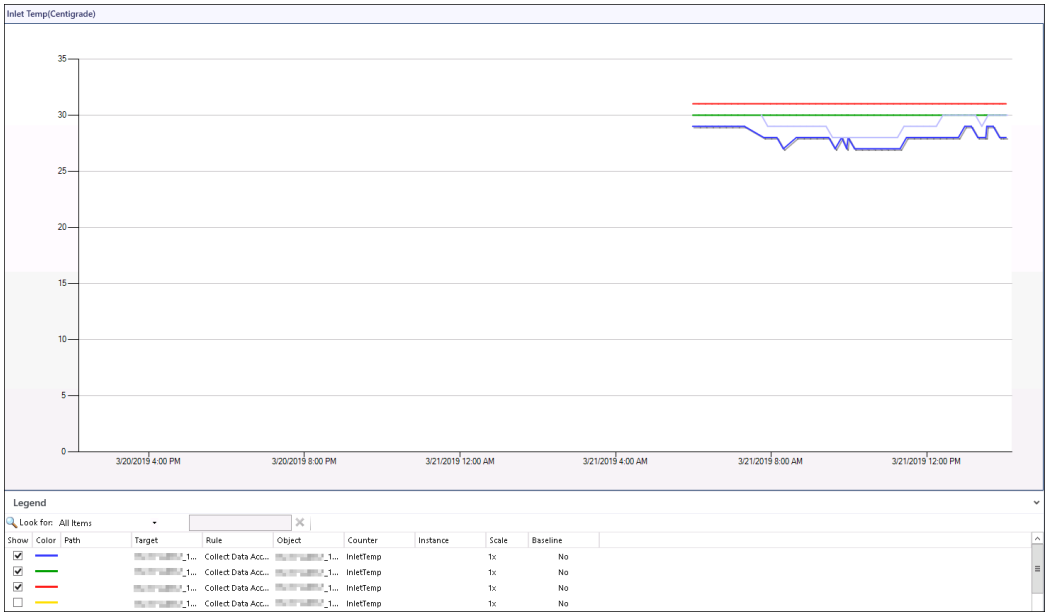
Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Servers** > **Performance View** > **Inlet Temp(Centigrade)**.

The **Inlet Temp(Centigrade)** window is displayed, as shown in **Figure 6-5**.

Figure 6-5 Inlet Temp(Centigrade)



Step 3 Select servers in the **Legend** area to view the air inlet temperature curves of the servers.

----End

6.4.3 Viewing the PSU Power

Step 1 Choose **Start** >  > **Operations Console**.

The SCOM main window is displayed.

Step 2 Choose **Monitoring** > **XFUSION FusionDirector System** > **XFUSION Servers** > **Performance View** > **Power Consumed(Watts)**.

The **Power Consumed(Watts)** window is displayed, as shown in **Figure 6-6**.

Figure 6-6 Power Consumed(Watts)

Step 3 Select servers in the **Legend** area to view the PSU power curves of the servers.

----End

7 FAQs

7.1 How Do I Fix a Communication Failure Caused by an Incorrect Default FusionDirector Certificate?

7.2 How Do I Replace the Server Certificate?

7.3 What Do I Do If the System Displays a Message Indicating that the SSL/TLS Secure Channel Fails to Be Created When FusionDirector Is Added?

7.4 How Do I Disable the Insecure TLS Protocol?

7.5 How to Disable System Unsafe Encryption Algorithm Kits

7.1 How Do I Fix a Communication Failure Caused by an Incorrect Default FusionDirector Certificate?

Symptom

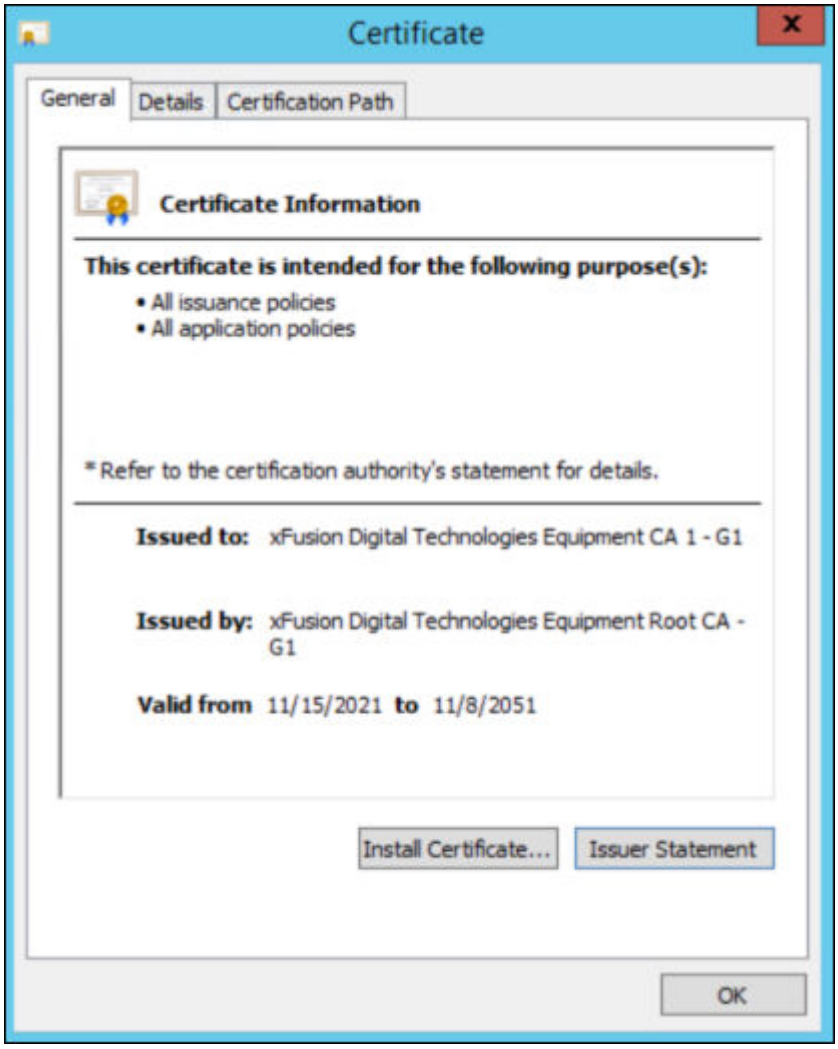
If the default FusionDirector certificate is modified or replaced after this plug-in is added to FusionDirector, the plug-in fails to communicate with FusionDirector.

Solution

Manually upload the modified or replaced Fusion Director certificate. The following procedure uses upload of the FusionDirector certificate as an example.

- Uploading the Root Certificate
  a. Double-click the root certificate **xFusionE...** of FusionDirector.
     The **Certificate** window is displayed, as shown in **Figure 7-1**.

Figure 7-1 Certificate



b. Click **Install Certificate...**.

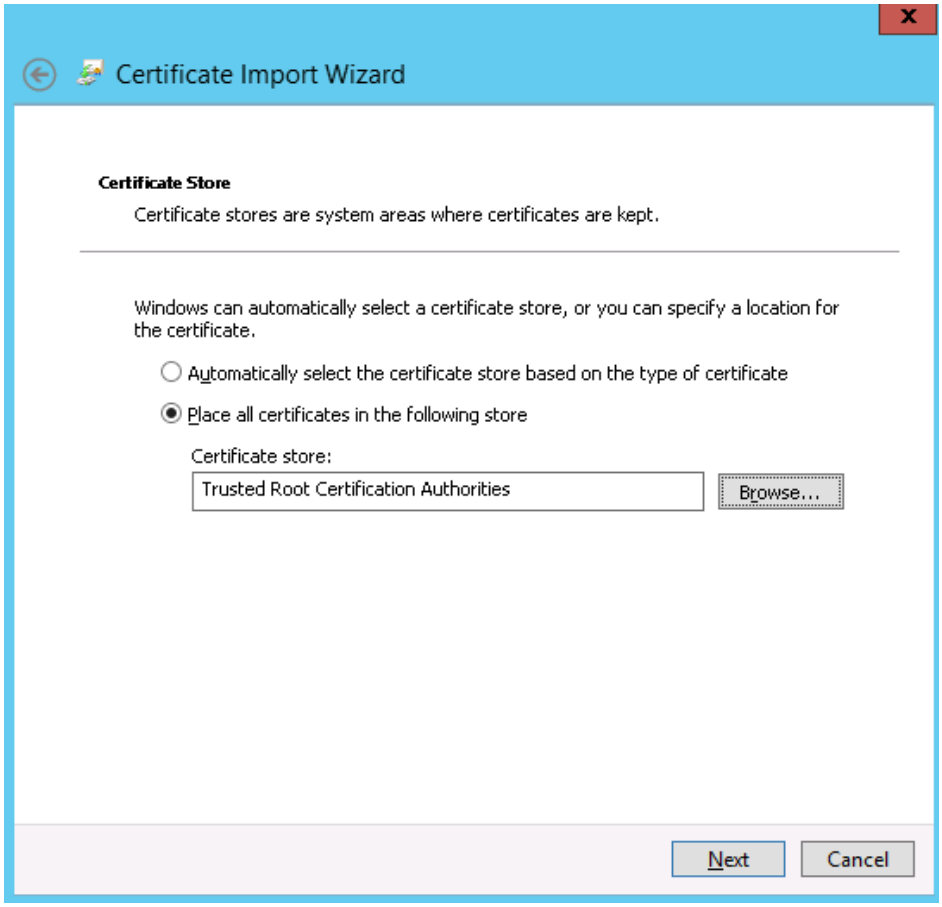
The **Certificate Import Wizard** window is displayed, as shown in **Figure 7-2**.

Figure 7-2 Certificate Import Wizard

c. Select **Local Machine** and click **Next**.

The **Certificate Store** window is displayed, as shown in **Figure 7-3**.

Figure 7-3 Certificate Stone

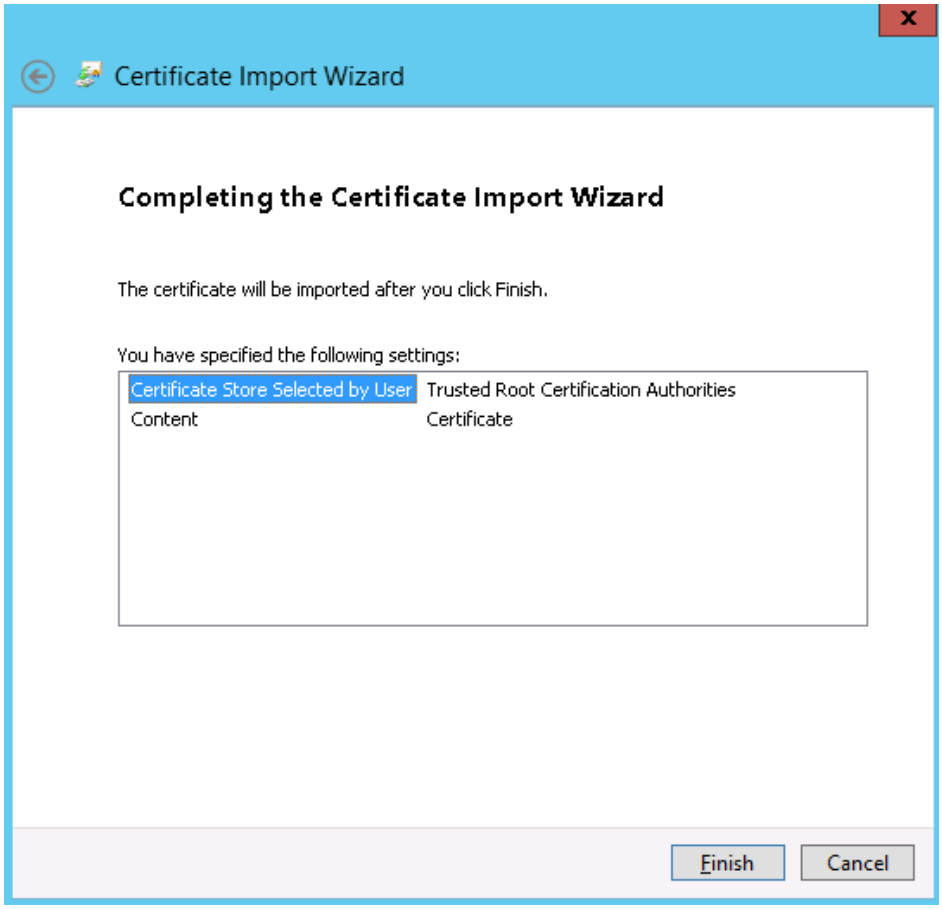


d. Select **Place all Certificates in following store**.

e. Click **Browse…**, select **Trusted Root Certification Authorities**, and click **Next**.

The **Completing the Certificate Import Wizard** window is displayed, as shown in **Figure 7-4**.

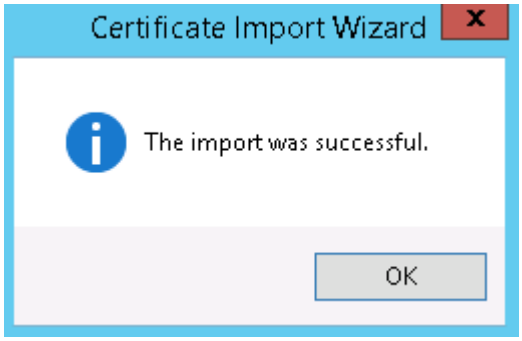
Figure 7-4 Completing the Certificate Import Wizard



f. Click **Finish**.

A dialog box indicating import success is displayed, as shown in **Figure 7-5**.

Figure 7-5 Import success



g. Click **OK**.

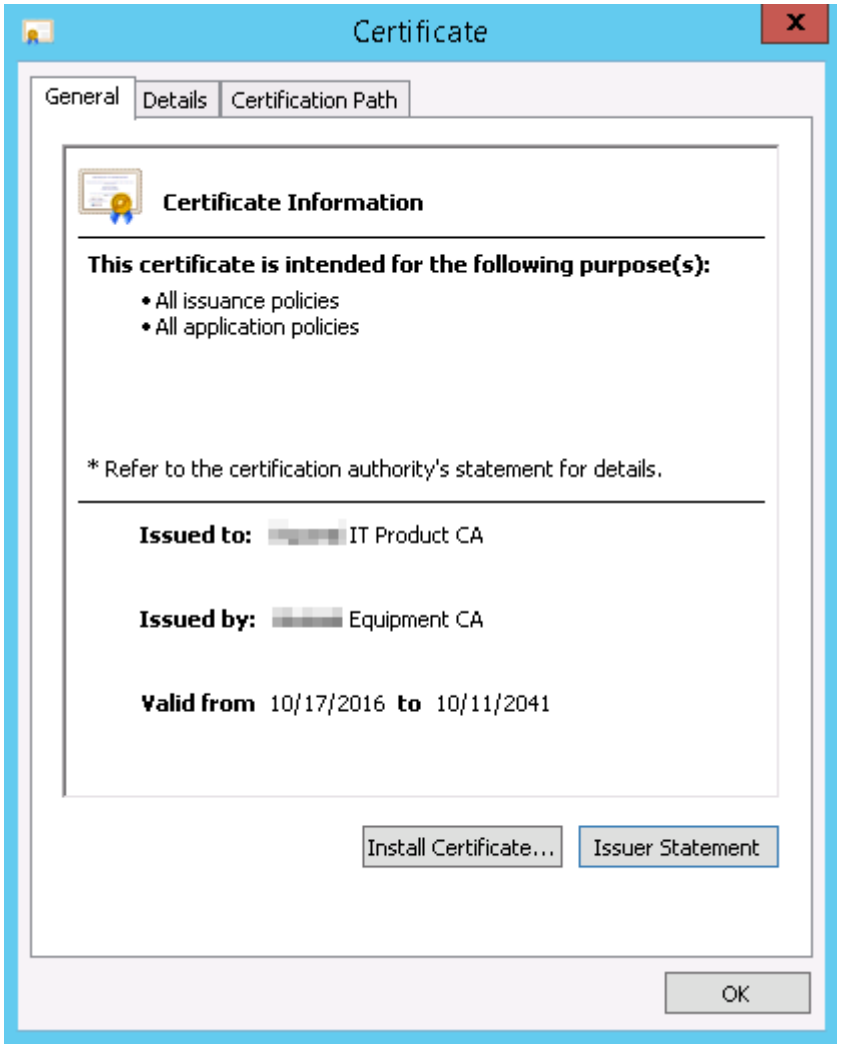
h. On the **Figure 7-1** page, click **OK**. The certificate is imported.

- Uploading the Product Certificate

  a. Double-click the product certificate **xFusionITProductCA** of FusionDirector.

  The **Certificate** window is displayed, as shown in **Figure 7-6**.

Figure 7-6 Certificate



b. Click **Install Certificate...**.

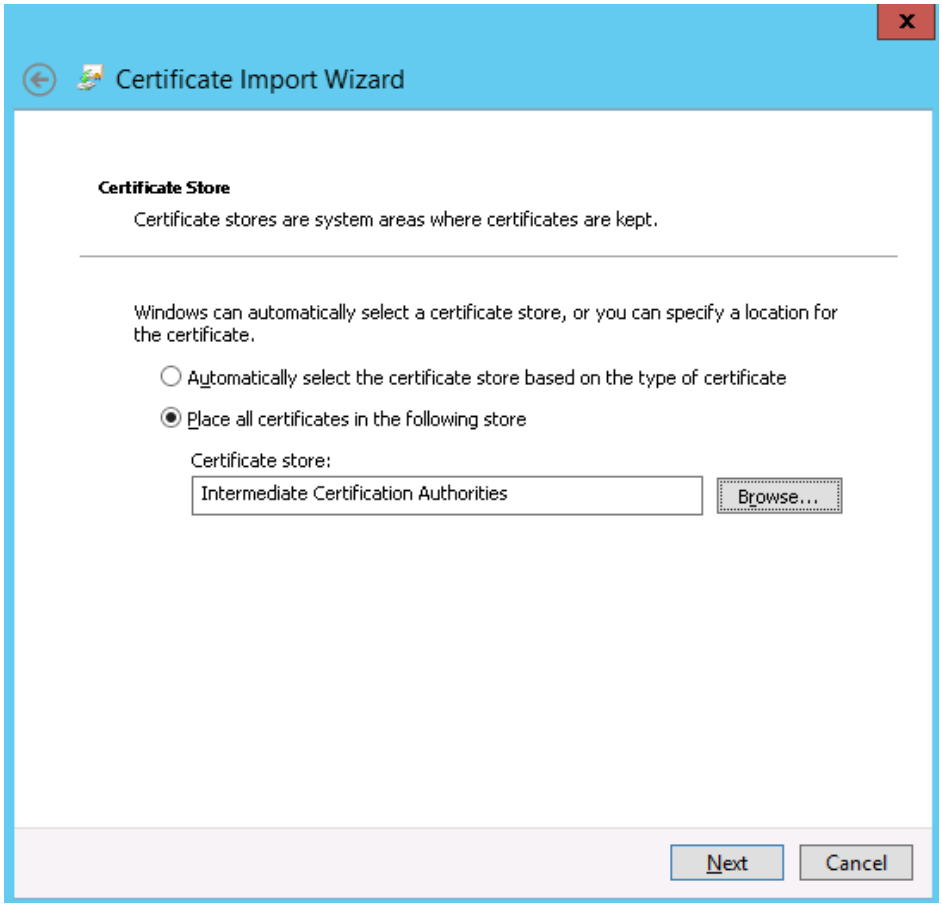
The **Certificate Import Wizard** window is displayed, as shown in **Figure 7-7**.

Figure 7-7 Certificate Import Wizard

c. Select **Local Machine** and click **Next**.

The **Certificate Store** window is displayed, as shown in **Figure 7-8**.

Figure 7-8 Certificate Store

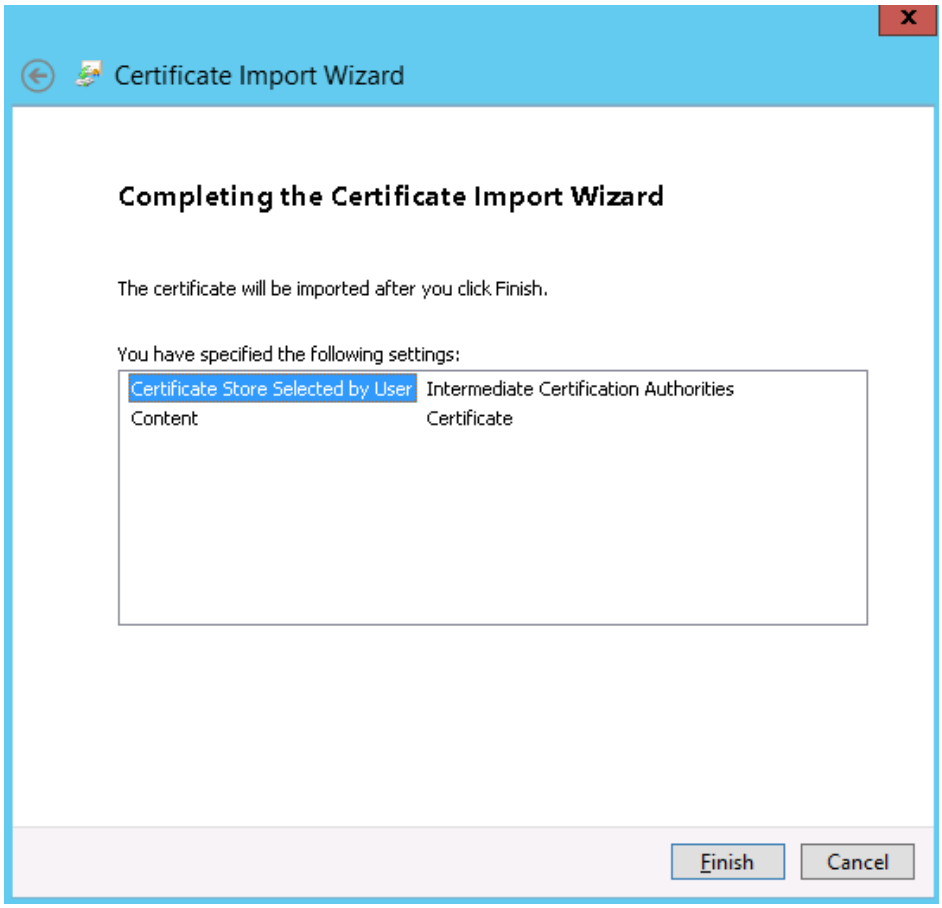


d. Select **Place all Certificates in following store**.

e. Click **Browse…**, select **Intermediate Certification Authorities**, and click **Next**.

The **Completing the Certificate Import Wizard** window is displayed, as shown in **Figure 7-9**.

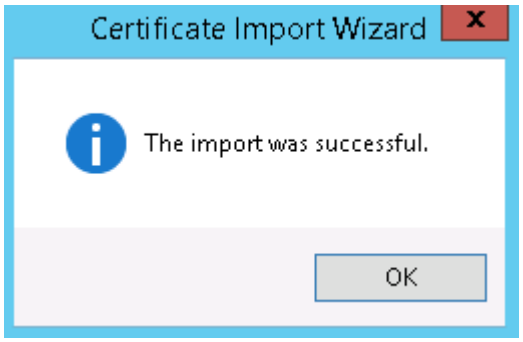
Figure 7-9 Completing the Certificate Import Wizard



f. Click **Finish**.

A dialog box indicating import success is displayed, as shown in **Figure 7-10**.

Figure 7-10 Import success



g. Click **OK**.

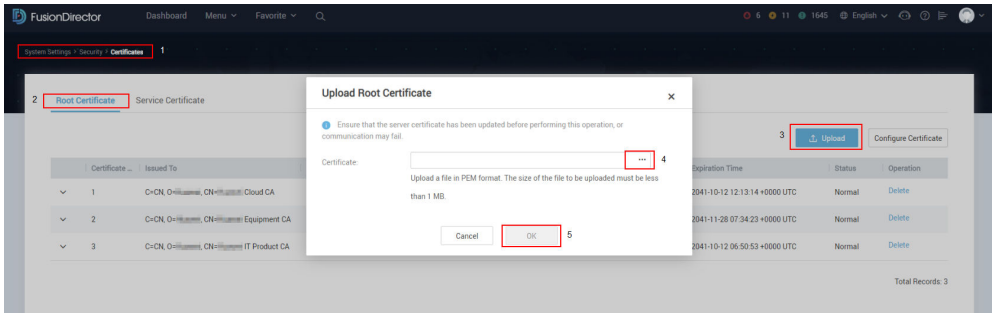
h. On the **Figure 7-6** page, click **OK**. The certificate is imported.

7.2 How Do I Replace the Server Certificate?

Step 1 Import the root certificate on the FusionDirector WebUI.

1. Choose **System Settings** > **Security** > **Certificates**. The **Certificate** page is displayed, as shown by (1) in **Figure 7-11**.

Figure 7-11 Importing the root certificate



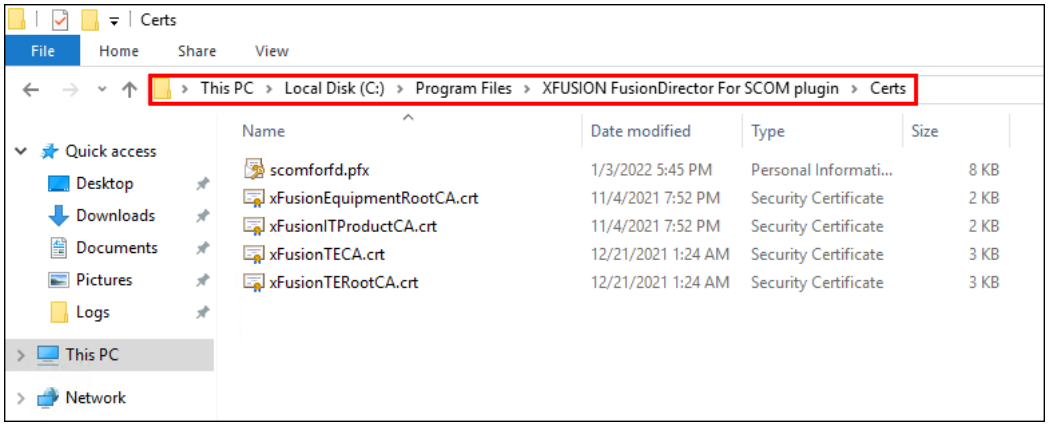
2. Choose **Root Certificate**, as shown by (2) in **Figure 7-11**.
3. On the **Root Certificate** page, click **Upload**, as shown by (3) in **Figure 7-11**.

   The **Upload Root Certificate** dialog box is displayed.
4. Select the root certificate to be imported and click **OK**, as shown by (4) and (5) in **Figure 7-11**.

Step 2 In the SCOM plug-in environment, save the server certificate to be imported to the following path, as shown in **Figure 7-12**.

C:\Program Files\XFUSION Fusion Director For SCOM plugin\Certs

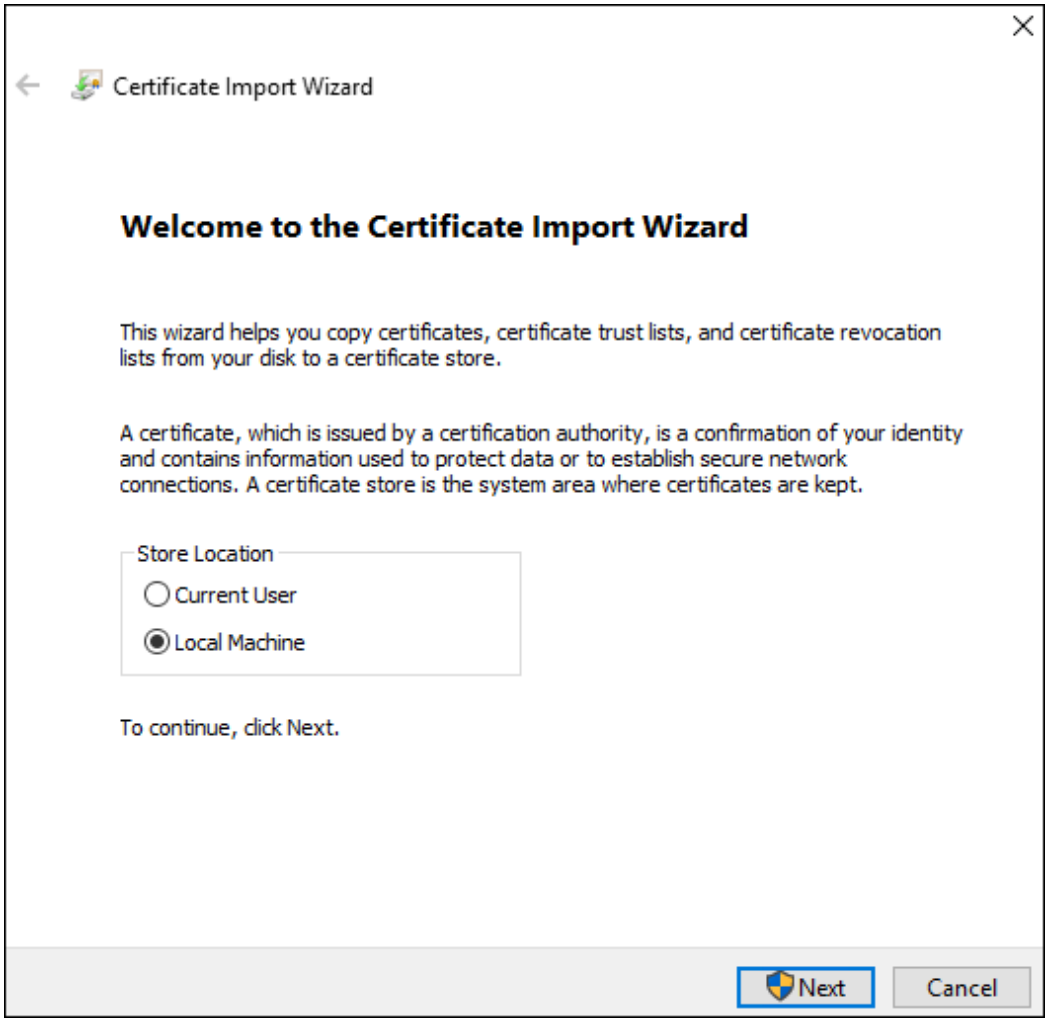
Figure 7-12 Certificate path



Step 3 Double-click the certificate to start the installation.

The **Welcome to the Certificate Import Wizard** page is displayed, as shown in **Figure 7-13**.

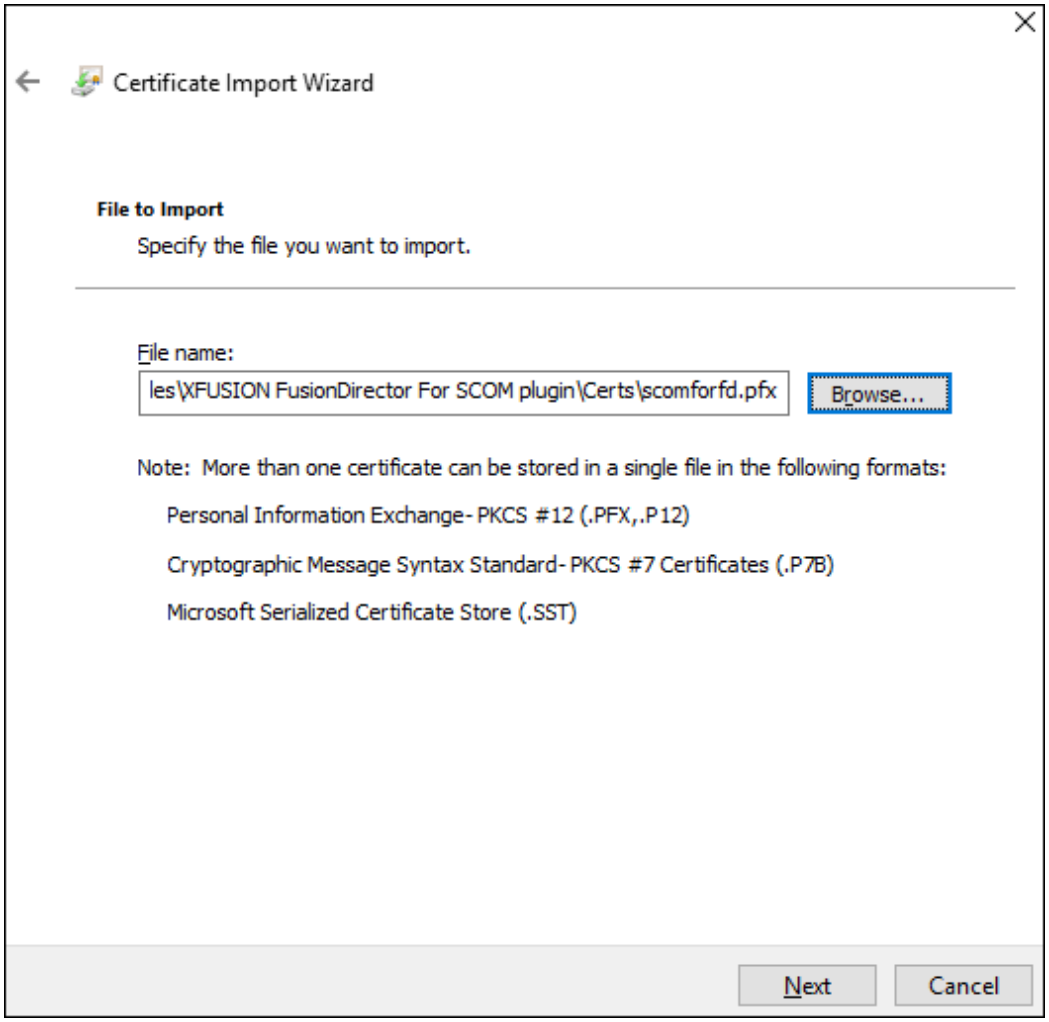
Figure 7-13 Welcome to the Certificate Import Wizard page



Step 4 Select **Local Machine** and click **Next**.

The **File to Import** page is displayed, as shown in **Figure 7-14**.

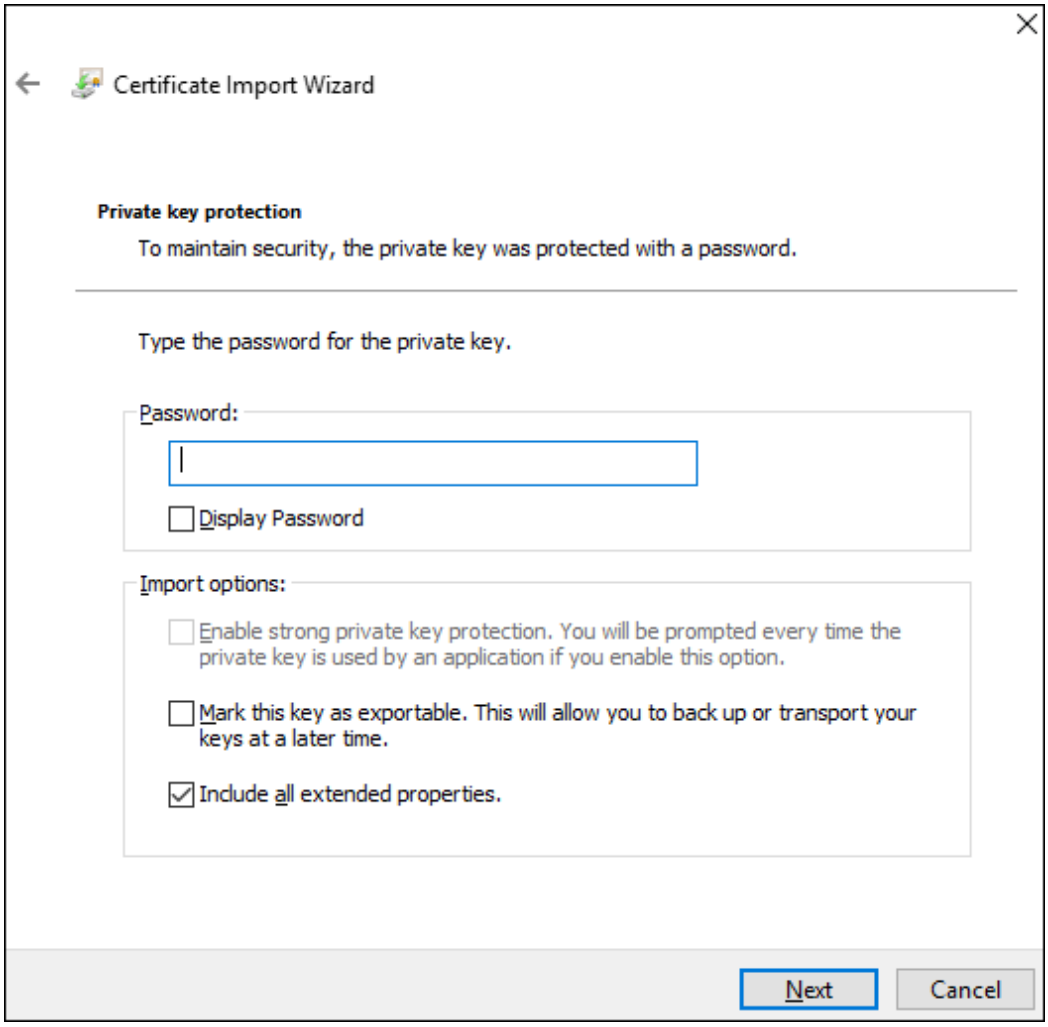
Figure 7-14 File to Import page



Step 5 Retain the default file path and click **Next**.

The **Private key protection** page is displayed, as shown in **Figure 7-15**.

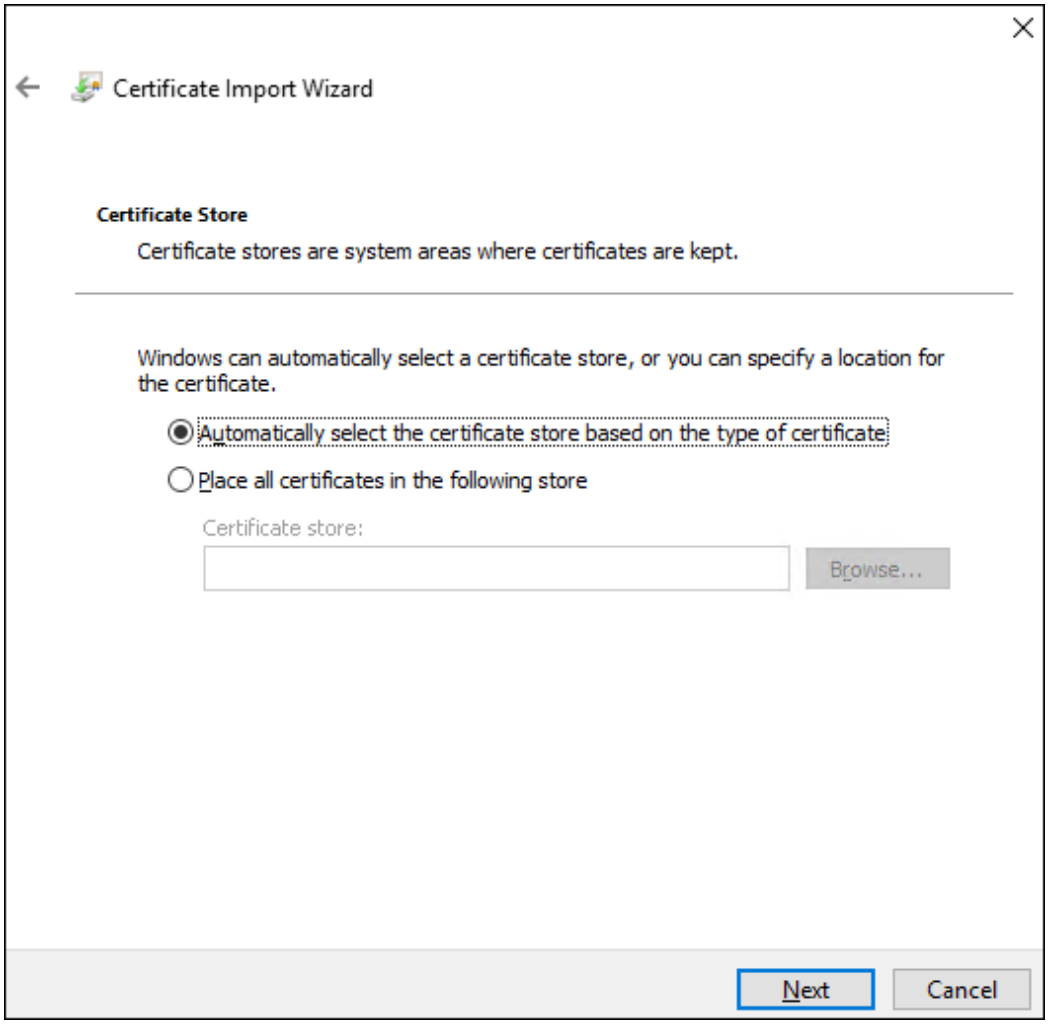
Figure 7-15 Private key protection page



Step 6 Enter the password (which is set by the user during certificate generation) and click **Next**.

The **Certificate Store** page is displayed, as shown in **Figure 7-16**.

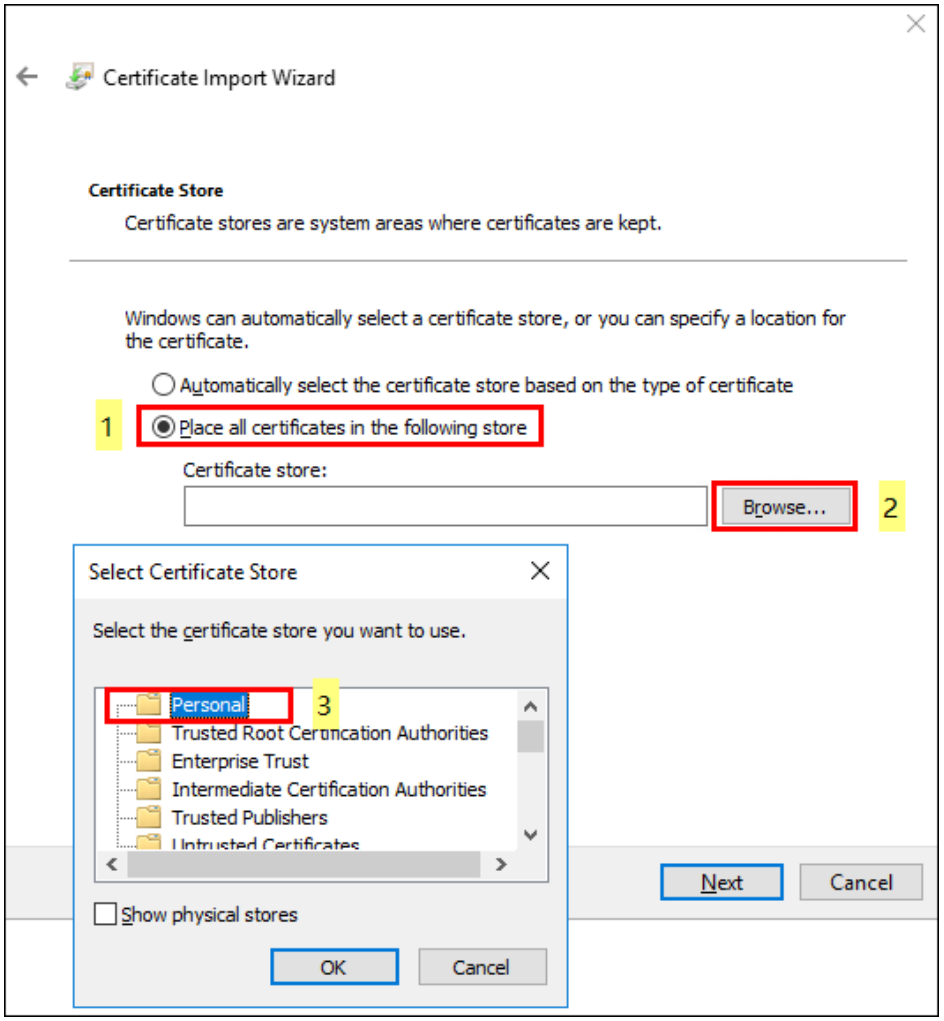
Figure 7-16 Certificate Store page 1



Step 7 On the **Certificate Store** page:

1. Select **Place all certificates in the following store**, as shown by (1) in **Figure 7-17**.

Figure 7-17 Certificate Store page 2



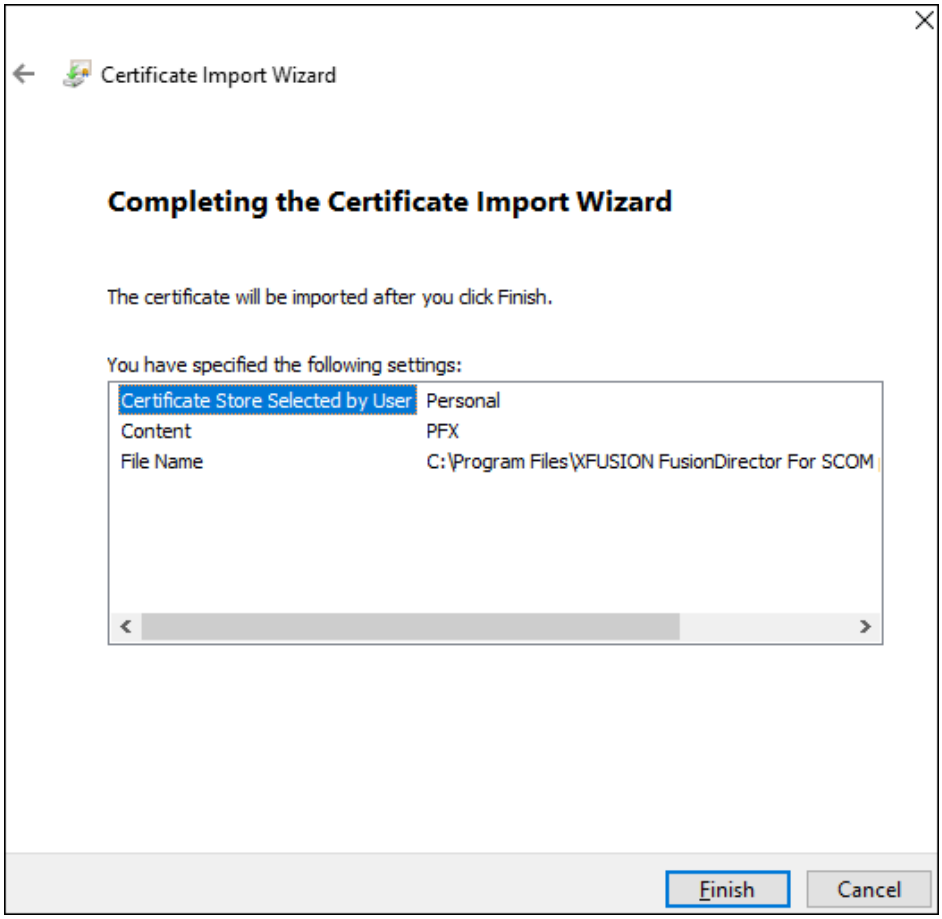
2. Click **Browse**, as shown by (2) in **Figure 7-17**.

   The **Select Certificate Store** dialog box is displayed.

3. Select Personal, as shown by (3) in **Figure 7-17**.
4. Click **OK**, as shown by (4) in **Figure 7-17**.
5. Click **Next**, as shown by (5) in **Figure 7-17**.

   The **Completing the Certificate Import Wizard** page is displayed, as shown in **Figure 7-18**.

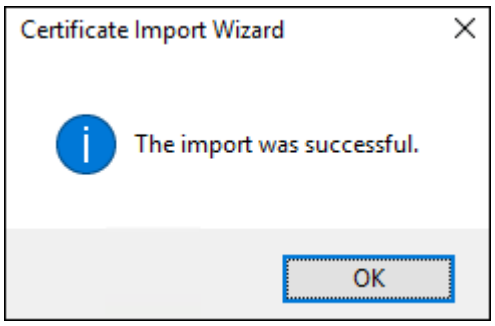
Figure 7-18 Completing the Certificate Import Wizard page



Step 8 Click **Finish** to import the certificate.

A dialog box is displayed indicating that the certificate is successfully imported, as shown in **Figure 7-19**.

Figure 7-19 Imported successfully



Step 9 Click **OK**.

Step 10 Run the following command to delete the existed certificate:

netsh http delete sslcert ipport=0.0.0.0:*Port*

NOTE

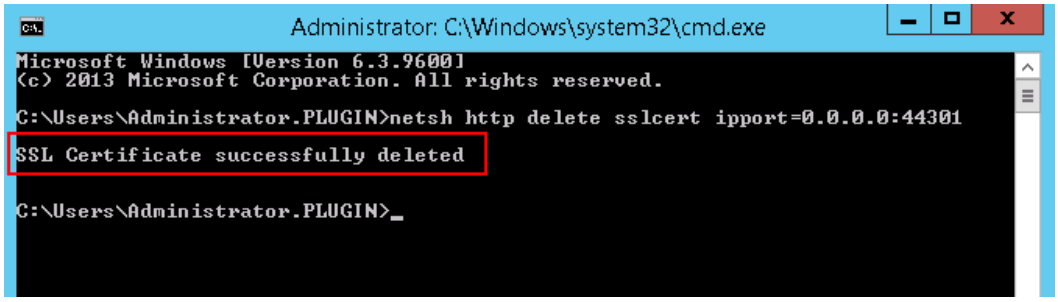
Port indicates the port number set during the SCOM plug-in installation.

For example, run the following command:

netsh http delete sslcert ipport=0.0.0.0:44301

The "SSL Certificate successfully deleted" information is returned, as shown in **Figure 7-20**.

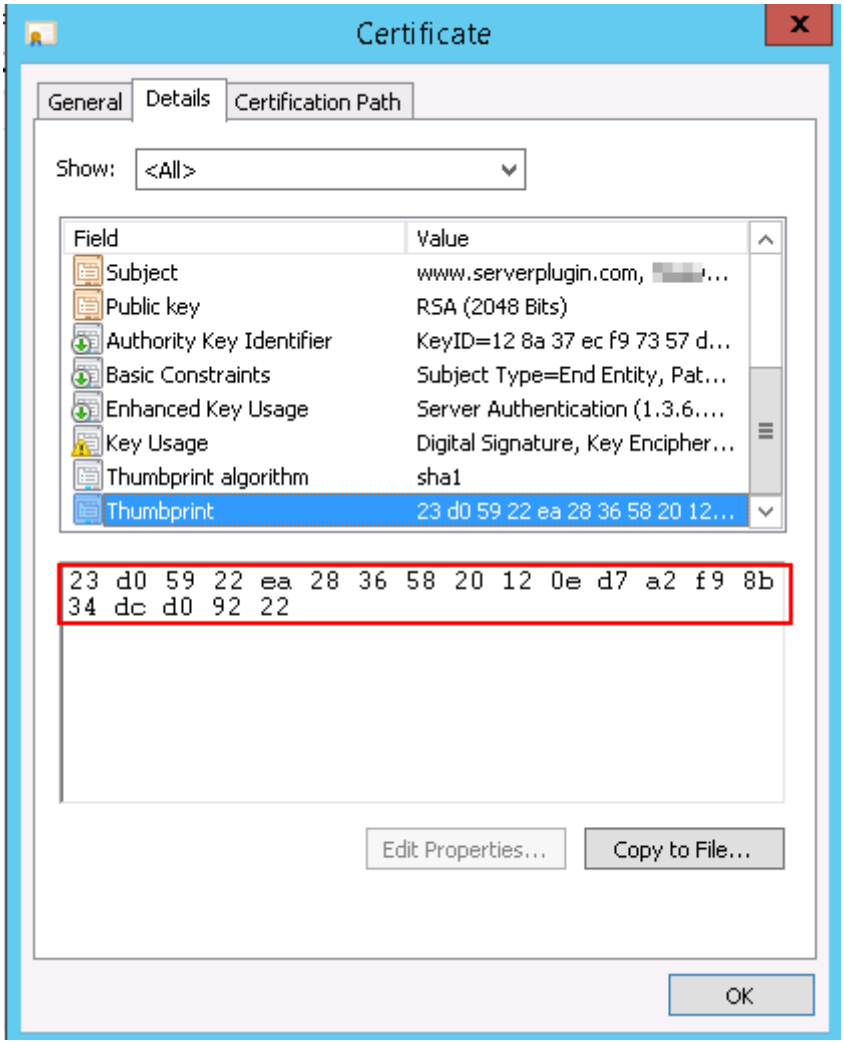
Figure 7-20 Returned information 1



Step 11 Copy the certificate thumbprint.

1. In the server certificate list, locate and open the page for manually importing the certificate.
2. On the **Details** tab page, find and click **Thumbprint**.
3. Copy the displayed certificate fingerprint, as shown in **Figure 7-21**.

Figure 7-21 Copying the certificate thumbprint



Step 12 Run the following command to replace the certificate:

netsh http add sslcert ipport=0.0.0.0:*Port* certhash=*Thumbprint* appid={214124cd-d05b-4309-9af9-9caa44b2b74a}

NOTE

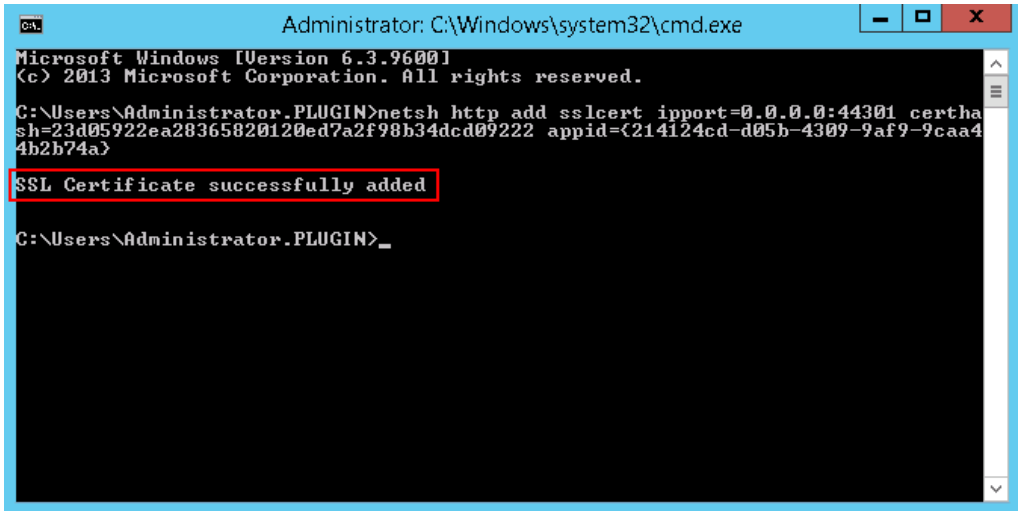
- *Port* indicates the port number set during the SCOM plug-in installation.
- The spaces in the certificate thumbprint must be deleted.

For example, run the following command:

netsh http add sslcert ipport=0.0.0.0:44301 certhash=23d05922ea28365820120ed7a2f98b34dcd09222 appid={214124cd-d05b-4309-9af9-9caa44b2b74a}

The "SSL Certificate successfully added" information is returned, as shown in **Figure 7-22**.

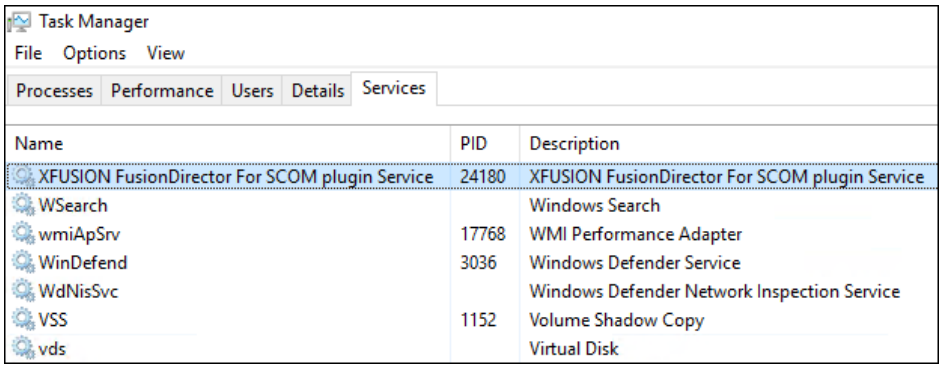
Figure 7-22 Returned information 2



Step 13 Restart the service.

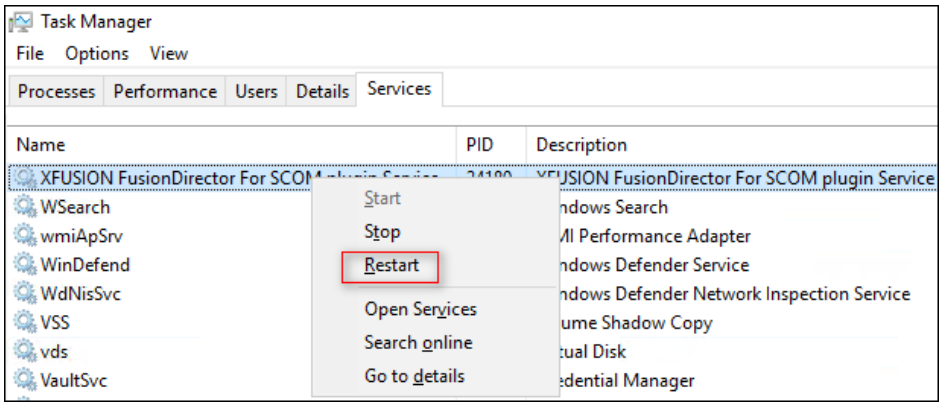
1. Open **Task Manager**.
2. On the **Services** tab page, find **XFUSION FusionDirector For SCOM plugin Service**, as shown in **Figure 7-23**.

Figure 7-23 Restarting the service 1



3. Right-click the service and choose **Restart** to restart the service, as shown in **Figure 7-24**.

Figure 7-24 Restarting the service 2

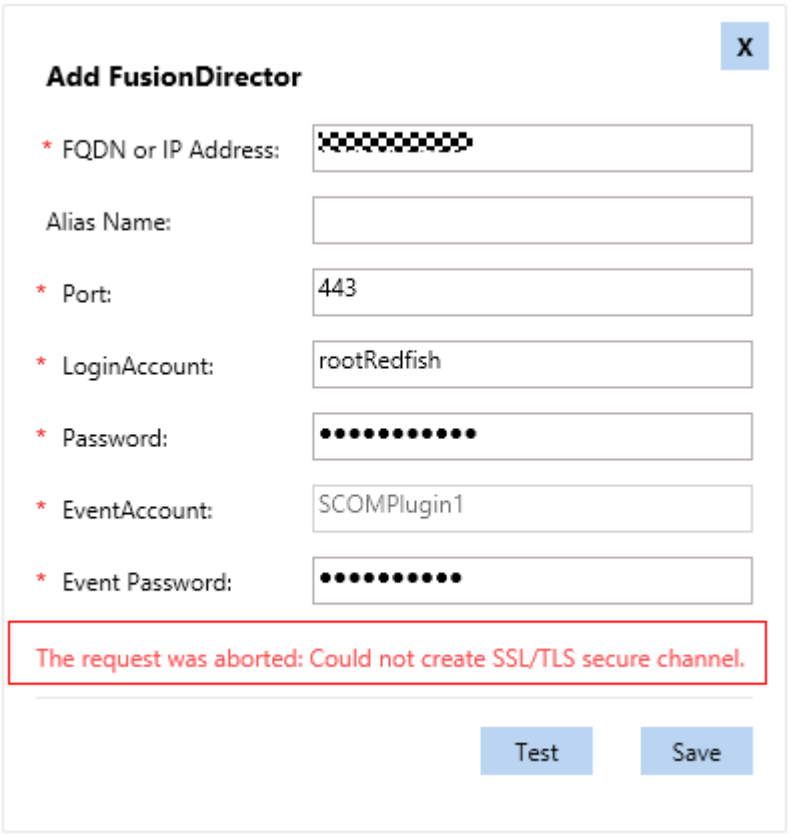


----End

7.3 What Do I Do If the System Displays a Message Indicating that the SSL/TLS Secure Channel Fails to Be Created When FusionDirector Is Added?

Symptom

When you add FusionDirector 1.6.1 or later to the SCOM Windows Server 2012 R2 server, the system displays a message indicating that the SSL/TLS secure channel fails to be created, as shown in the following figure.



Problem Cause

The SCOM Windows Server 2012 R2 server does not contain the cipher suite supported by FusionDirector 1.6.1 or later. As a result, the SSL/TLS secure channel fails to be created when FusionDirector 1.6.1 or later is added.

Solution

Before adding FusionDirector 1.6.1 or later to the SCOM Windows Server 2012 R2 server, install the Windows OS patch (2919355) and add the cipher suite supported by FusionDirector 1.6.1 or later. The procedure is as follows:

Step 1 Log in to the SCOM Windows Server 2012 R2 server.

Step 2 Install the Windows OS patch 2919355.

For details about the 2919355 patch package and how to install it, see the following documents:

https://support.microsoft.com/en-us/help/2919355/windows-rt-8-1-windows-8-1-windows-server-2012-r2-update-april-2014

Step 3 Add the cipher suite supported by FusionDirector.

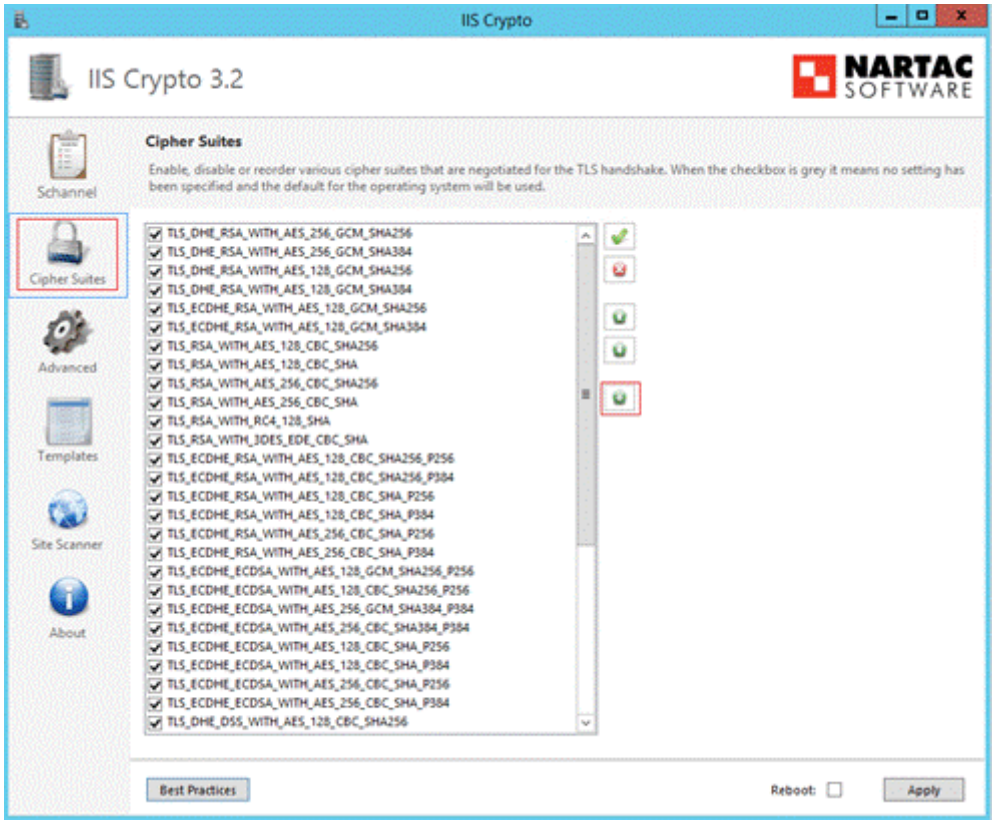
NOTE

To view the encryption algorithm kits supported by FusionDirector, log in to FusionDirector, and click **Menu > System Settings > Security > Configuration Management**. They are displayed in the **TLS Cipher Suite Configuration** field. For details, see the chapter ***Configuration Management in the FusionDirector Operation Guide***.

The following uses the IIS Crypto tool as an example.

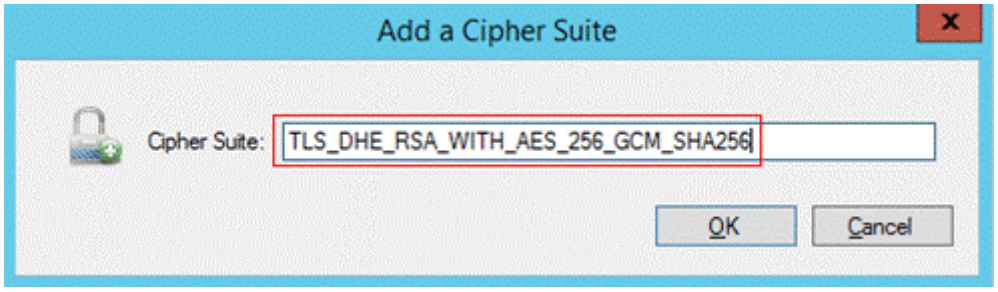
1. On the SCOM Windows Server 2012 R2 server, open the IIS Crypto tool.
2. Click **Cipher Suites** in the menu bar on the left, and then click  in the operation column on the right, as shown in the following figure.

Figure 7-25 Cipher Suites page



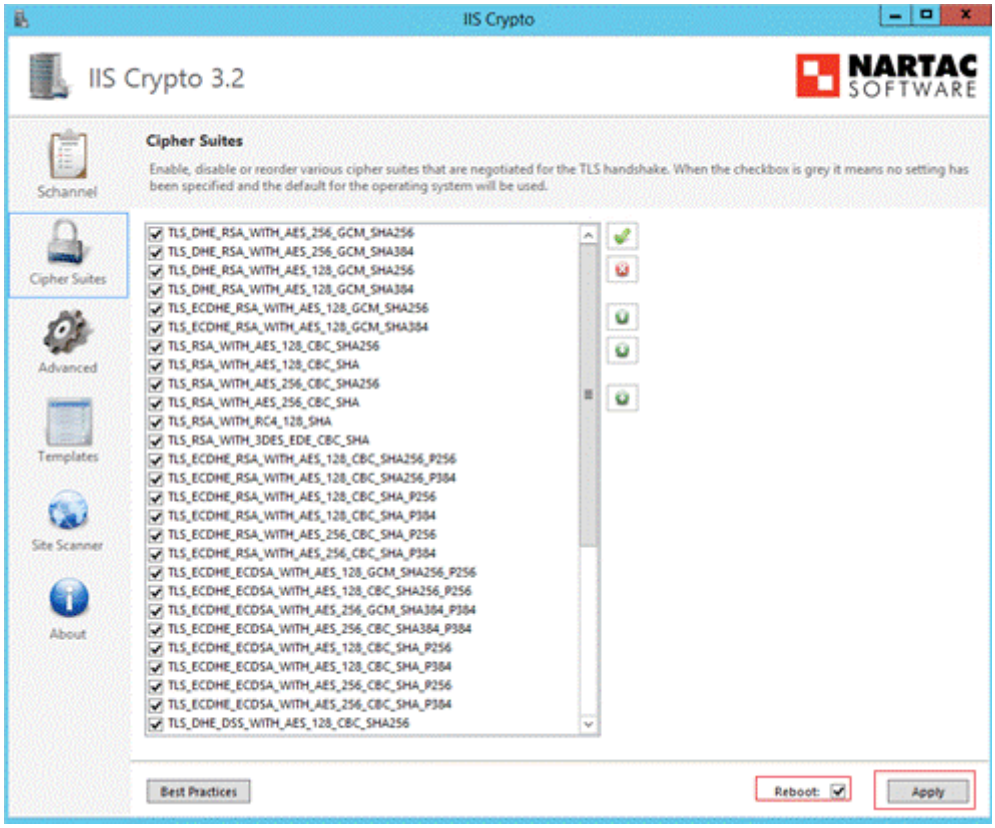
3. In the **Add a Cipher Suite** dialog box, enter the cipher suite supported by FusionDirector, as shown in the following figure.

Figure 7-26 Entering the cipher suite supported by FusionDirector (example)



4. Click **OK**.
5. Select **Reboot** and click **Apply** for the settings to take effect, as shown in the following figure.

Figure 7-27 Restarting the system for the settings to take effect



----End

7.4 How Do I Disable the Insecure TLS Protocol?

Symptom

If the system does not close the insecure TLS protocol such as TLS1.0 or TLS1.1, the plugin will generate a warning.

Solution

Disable the insecure TLS protocol as follows while ensuring software and system functions.

NOTICE

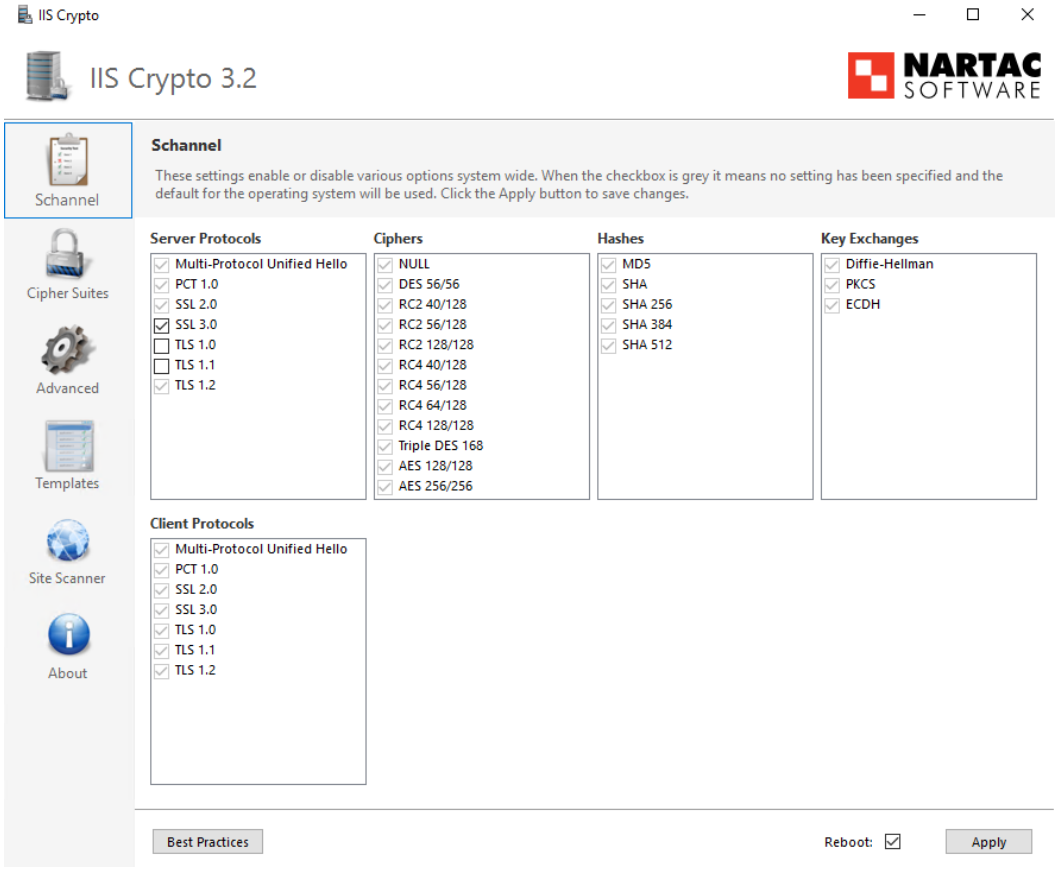
This operation may affect other software running properly.

The following uses IIS Crypto as an example to show how to disable the protocol.

Step 1 Open the IIS Crypto on the SCOM Windows Server.

Step 2 Click **Schannel** in the left menu and uncheck **TLS1.0** and **TLS1.1**, shown as below:

Figure 7-28 Schannel interface



Step 3 Check **Reboot** and click **Apply** to reboot the device. The configuration will be validated.

----End

7.5 How to Disable System Unsafe Encryption Algorithm Kits

Symptom

If some unsafe encryption algorithm kits are not disabled, bug prompts will be displayed when the safe scan is conducted.

Solution

To avoid safety risks, it is suggested to only enable safe encryption algorithm kits without affecting software and system functions.

NOTE

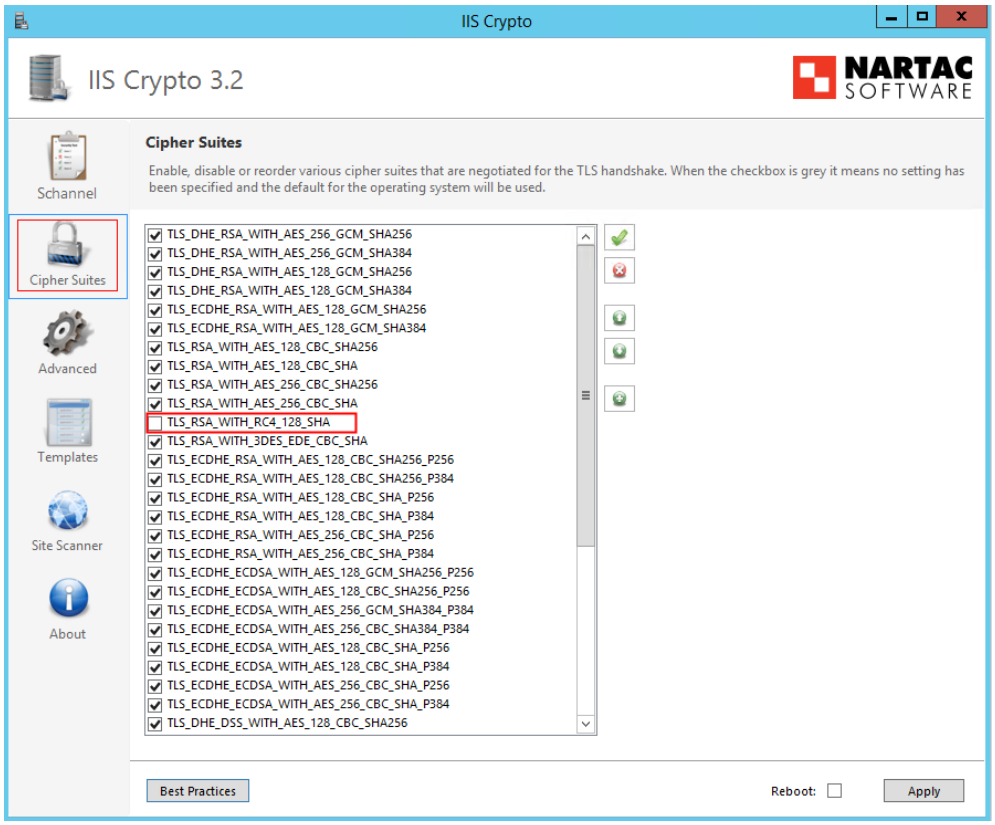
The safe encryption algorithm kits that match with FusionDirector, log in to FusionDirector, and click **Menu > System Settings > Security > Configuration Management**. They are displayed in the **TLS Cipher Suite Configuration** field. For details, see the chapter ***Configuration Management in the FusionDirector Operation Guide***.

The following uses IIS Crypto as an example to show how to disable the protocol.

Step 1 Open the IIS Crypto on the SCOM Windows Server.

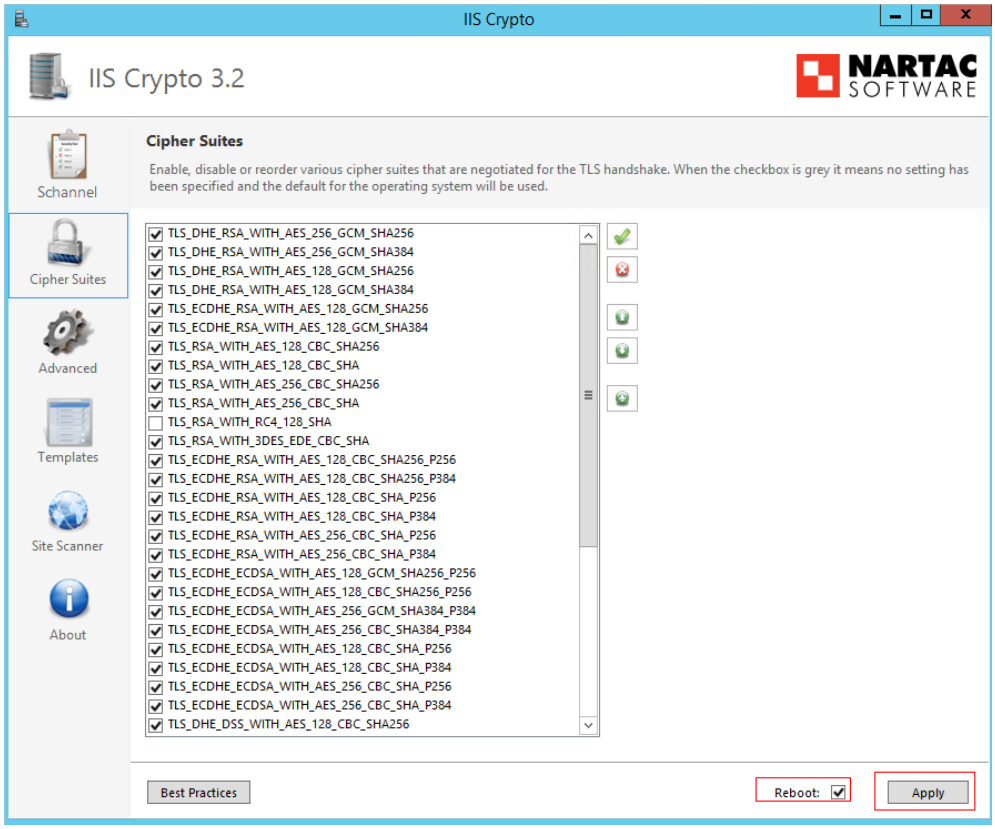
Step 2 Click **Cipher Suites** in the left menu bar, and cancel checking unsafe encryption algorithm kits. As shown in **Figure 7-29**.

Figure 7-29 Disabling System Unsafe Encryption Kits



Step 3 Select **Reboot** and click **Apply** for the settings to take effect, as shown in the following figure.

Figure 7-30 Restarting the system for the settings to take effect



----End

A Glossary

F

FusionDirector	A unified server O&M management software.

N

NetFramework	Microsoft .NET Framework is a new hosting code programming model used for Windows. It combines powerful functions with new technologies to construct applications with excellent user experience, implement seamless communications across technical boundaries, and support various service processes.

S

SCOM	System Center Operation Manager (SCOM) refers to the Microsoft system center operation manager. SCOM monitors servers, application systems, and clients in the network. It provides a GUI for administrators to monitor faults and alarms of target computers.

B Public IP Addresses

The *Public IP Addresses of FusionDirector For SCOM* describes the public IP addresses of the open-source and third-party software used in *FusionDirector For SCOM*. For details, see **Table Public IP Addresses of FusionDirector For SCOM**.

Table B-1 Public IP Addresses of FusionDirector For SCOM

Component	URL	Function
NSIS	**http://nsis.sf.net/**	This URL links to NISI's official website. It will not be triggered by any public address.
	https://schemas.microsoft.com/*	This URL links to document type definition for reference purpose. It will not be triggered by any public address.
	http://*.microsoft.com/*	This URL links to Microsoft's official website. It will not be triggered by any public address.
iisexpress	**https://www.iis.net/**	This URL links to IIS's official website. It will not be triggered by any public address.
Microsoft.EnterpriseManagement.Core.dll	**http://tempuri.org/***	This URL links to document type definition for reference purpose. It will not be triggered by any public address.

Component	URL	Function
	http://www.w3.org/*	This URL links to document type definition for reference purpose. It will not be triggered by any public address.
Newtonsoft.Json	**http://james.newtonking.com/projects/json**	This URL links to author blogs on Newtonsoft.Json. It will not be triggered by any public address.
	https://www.newtonsoft.com/*	This URL links to Newtonsoft.Json official website. It will not be triggered by any public address.
	https://www.nuget.org/*	This URL links to Nuget's official webiste. It will not be triggered by any public address.
	https://*.digicert.com/*	This URL links to Digicer's official website. It will not be triggered by any public address.
Nlog	**https://nlog-project.org/***	This URL links to Nlog's official website. It will not be triggered by any public address.
	http://schemas.xmlsoap.org/*	This URL links to document type definition for reference purpose. It will not be triggered by any public address.
	http://schemas.datacontract.org/*	This URL links to document type definition for reference purpose. It will not be triggered by any public address.

C Obtaining Technical Support

To obtain assistance, contact technical support as follows:

- Contact customer service center at **support@xfusion.com**.
- Contact technical support personnel.

D Communication Matrix

Source Device	Source IP Address	Source Port Number	Destination Device	Destination IP Address	Destination Port Number	Protocol	Port Description	Destination Port Configurable	Authentication Mode	Encryption Mode
Device of the plug-ins	Device IP address of the plug-ins	Random	Device to which FusionDirector belongs	IP address of the device to which FusionDirector belongs	443	TCP	HTTPS (web) port, the protocol can be modified. Plug-in, as a client, accesses the FusionDirector server.	No	Token	TLS
Client	Client IP address	Random	Device of the plug-ins	Device IP address of the plug-ins	44300-44399 Note: The port number ranges from 44300 to 44399.	TCP	The port that receives the report events of FusionDirector is enabled by default to 44301.	Yes	User name and password	TLS

