Hewlett Packard Enterprise

HPE IMC Centralized Deployment Guide with Local Database

Abstract

This document describes the processes and procedures to follow when deploying the HPE Intelligent Management Center in addition to the procedures for upgrading, removing, registering, backup, and restore. This document is intended for use by network engineers or system administrators responsible for installing network software and components.

Part number: 5200-2706

Software version: IMC PLAT 7.3 (E0501)

Acknowledgments

Contents

Overview

The following information describes how to deploy IMC in centralized mode and to use a local database. This deployment scheme scales to networks from 50 to 500 devices.

IMC components

IMC includes the IMC platform and service components.

IMC platform

The IMC platform is the base component to provide IMC services and includes the following subcomponents:

- Resource Management
- Alarm Management
- User Selfservice Management
- Guest Access Management
- Intelligent Configuration Center
- Report Management
- Network Element (NE) Management
- Performance Management
- ACL Management
- Network Asset Management
- Security Control Center
- General Search Service Management
- Syslog Management
- VLAN Management
- Virtual Resource Management
- Server & Storage Automation

Service components

Service components are optional and purchased separately from the IMC platform. The IMC platform is the basis for implementing various services and must be installed before service component deployment.

IMC includes the following service components:

- **User Access Manager (UAM)**—Provides policy-based Authentication, Authorization and Accounting (AAA) services. UAM software extends management to wired, wireless and remote network users and enables the integration of network device, user, guest and terminal management on a single unified platform.
- **TACACS+ Authentication Manager (TAM)**—Provides basic AAA functions for network device or IT users for network device management security. TAM can assign users with different privileges, monitor login and command execution operations, and simplify user management.

- **Endpoint Admission Defense (EAD) Security Policy**—Endpoint Admission Defense integrates security policy management and endpoint posture assessment to identify and isolate risks at the network edge. The security policy component allows administrators to control endpoint admission based on an endpoint's identity and posture.
- **MPLS VPN Manager (MVM)**—Provides functions such as VPN autodiscovery, topology, monitoring, fault location, auditing, and performance evaluation, as well as VPN and service deployment. MVM also contains a traffic engineering component that helps operators monitor an entire network and deliver service quality by distributing suitable network resources as needed.
- **IPsec VPN Manager (IVM)**—Provides features for all aspects of IPSec VPN management. IVM allows administrators to construct an IPSec VPN network, effectively monitor the operation and performance of the VPN network, and quickly locate device faults for full IPSec VPN lifecycle management.
- **Voice Service Manager (VSM)**—Provides a solution for reducing the voice network maintenance cost and improving maintenance efficiency. VSM is designed for enterprise-level voice networks.
- **Wireless Service Manager (WSM)**—Provides unified management of wired and wireless networks, adding network management functions into existing wired network management systems. WSM software offers wireless LAN (WLAN) device configuration, topology, performance monitoring, RF heat mapping, and WLAN service reports.
- **Network Traffic Analyzer (NTA)**—Is a graphical network-monitoring tool that provides realtime information about users and applications consuming network bandwidth. A reliable solution for enterprise and campus network traffic analysis, NTA defends the network against virus attacks and applies varying levels of bandwidth traffic to different services and applications.
- **User Behavior Auditor (UBA)**—Provides comprehensive log collection and audit functions supporting log formats such as NAT, flow, NetStreamV5, and DIG. UBA provides DIG logs to audit security-sensitive operations and digest information from HTTP, FTP, and SMTP packets.
- **Service Operation Manager (SOM)**—Allows IT organizations to adhere to ITIL v3.0, including IT services such as policy design, operation, and improvement. Based on a unified configuration management database (CMDB), SOM provides configurable flows and options for self service, as well as management of asset configuration, change, fault events, problem recognition, and auto-generation of a knowledge base.
- **Application Manager (APM)**—Allows administrators to visualize and measure the health of critical business applications and their impact on network performance. With the available data, administrators can easily determine which business process is affected and which application issues to prioritize.
- **QoS Manager (QoSM)**—Enhances visibility and control over QoS configurations and helps administrators focus on QoS service planning by providing a robust set of QoS device and configuration management functions. It allows administrators to organize traffic into different classes based on the configured matching criteria to provide differentiated services, committed access rate (CAR), generic traffic shaping (GTS), priority marking, queue scheduling, and congestion avoidance.
- **Service Health Manager (SHM)**—Provides visual service quality management functions. SHM integrates the alarm, performance, NTA, and NQA data. It uses key quality indexes and service level agreements to monitor and measure service health.
- **VAN Connection Manager (VCM)**—Provides a solution for physical network configuration migration. VCM tracks the startup, stopping, and migration of virtual machines (VMs), and according to the latest VM location, VCM deploys a physical network configuration. VCM allows collaboration for physical and virtual networks. It also provides compatibility between physical and virtual networks of different vendors.
- **Branch Intelligent Management System (BIMS)**—Provides support for service operations, delivering high reliability, scalability, flexibility, and IP investment returns. Based on the TR-

069 protocol, IMC BIMS offers resource, configuration, service, alarm, group, and privilege management. It allows the remote management of customer premise equipment (CPE) in WANs.

- **Remote Site Manager (RSM)**—Securely extends the IMC core platform capability to remote sites by deploying remote agents. These agents manage and monitor the remote network, and apply policies and configurations to the remote network devices on behalf of the central IMC server.
- **Resource Automation Manager (RAM)**—Provides a solution for customizing network services for users and automatically deploying network services.
- **VAN SDN Manager (SDNM)**—Manages OpenFlow-based SDN. SDNM allows you to manage an OpenFlow network through RESTful APIs provided by H3C VCF Controller or HPE SDN controllers. Combined with the device management, reports, and home page widgets functions in the IMC platform, SDNM also allows you to perform visual management and monitoring on the OpenFlow network.
- **VAN Fabric Manager (VFM)**—Provides an integrated solution for managing both the LANs and SANs in data centers by working with HP devices. VFM depends on VRM to obtain virtual machine (VM) migration information.
- **Unified Communications Health Manager (UCHM)**—Provides a solution for monitoring the health status of networks deployed with Microsoft Lync Server. It allows you to manage network resources including the Lync Servers, PSTN gateways, and Lync client endpoints.
- **Intelligent Analysis Reporter (iAR)**—Extends the reporting capabilities within IMC to include customized reporting. iAR includes a report designer, which can save designs into report templates. Report formats include charts. Reports can be automatically generated at specified intervals and distributed to key stakeholders.

IMC editions

The following editions of IMC are available:

- Enterprise
- Standard
- Basic

Table 1 Differences between IMC editions

Item	Basic	Standard	Enterprise
Number of nodes	50	Extensible	Extensible
Hierarchical Network Management	Not supported	Lower-level NMS only	Supported
Distributed deployment	Not supported	Supported	Supported
Operating system	Windows	Windows and Linux	Windows and Linux
Embedded database	Supported	Supported only on Windows	Not supported
Separate database	Supported	Supported	Supported

For information about installing a separate database for IMC on Windows, see the following documents:

- *SQL Server 2008 Installation and Configuration Guide*
- *SQL Server 2008 R2 Installation and Configuration Guide*
- *SQL Server 2012 Installation and Configuration Guide*

- *SQL Server 2014 Installation and Configuration Guide*
- *MySQL 5.5 Installation and Configuration Guide (for Windows)*
- *MySQL 5.6 Installation and Configuration Guide (for Windows)*

For information about installing a separate database for IMC on Linux, see the following documents:

- *Oracle 11g Installation and Configuration Guide*
- *Oracle 11g R2 Installation and Configuration Guide*
- *Oracle 12c Installation and Configuration Guide*
- *MySQL 5.5 Installation and Configuration Guide (for Linux)*
- *MySQL 5.6 Installation and Configuration Guide (for Linux)*

Installation and deployment

IMC uses the install + deploy model:

- **Install**—The installation package of the IMC component is copied to the server and loaded to the Intelligent Deployment Monitoring Agent.
- **Deploy**—The installation package is decompressed on the server and database scripts are created for the component.

The IMC components are operational only after they are deployed. In centralized deployment, all IMC components are installed and deployed on the same server.

IMC automatically creates a database user for each component when the component is deployed. As a best practice, do not modify the database user configuration, including the database user password and password policy.

If the deployment or upgrade process is interrupted, IMC automatically stores logs as a compressed file in the **\tmp** directory of the IMC installation path. You can use the logs to quickly locate the issue or error.

Preparing for installation

Hardware requirements

The tables in this section use the following terminology:

- **Node**—IMC servers, database servers, and devices managed by IMC are called nodes.
- **Collection unit**—The number of collection units equals the total number of performance instances collected at 5-minute intervals. If the collection interval is greater than 5 minutes, the number of collection units decreases. If the collection interval is smaller than 5 minutes, the number of collection units increases.

  For example, if performance instances listed in Table 2 are collected every 5 minutes, the total collection units are the same as the number of performance instances, which is 24. If the collection unit is twice as the 5-minute interval (10 minutes), the number of collection units is half the total number of performance instances, which is 12.

  Table 2 Performance instances

Monitored item	Number	Performance index	Performance instance
CPU	1	CPU usage	1
Memory	1	Memory usage	1
Interface	10	Receiving rate	10
		Sending rate	10
Device	1	Unreachability rate	1
		Response time	1
		Total	24

- **Java heap size**—Java heap size that can be used by the IMC Web server.

  To set the Java heap size for IMC:

  - On Windows, run the **setmem.bat** *heap size* script in the **\client\bin** directory of the IMC installation path.
  - On Linux, run the **setmem.sh** *heap size* script in the **/client/bin** directory of the IMC installation path.

  Set *heap size* to a value in the range of 256 to 1024 for a 32-bit OS, or in the range of 256 to 32768 for a 64-bit OS. The java heap size cannot exceed the physical memory size.

To improve the I/O performance, follow these guidelines:

- When the number of the collection units is from 100 K to 200 K, install two or more disks and a RAID card with a cache of at least 256 MB.
- When the number of collection units is from 200 K to 300 K, install two or more disks and a RAID card with a cache of at least 512 MB.
- When the number of collection units is 300 K to 400 K, install four or more disks and a RAID card with a cache of at least 1 GB.

Optimal hardware requirements vary with scale, other management factors, and are specific to each installation. Consult Hewlett Packard Enterprise Support, or your local account teams, for exact requirements. If service components are added to the IMC platform, be sure to read the release notes of each component.

Table 3 Hardware requirements for a 32-bit Windows operating system

Management scale			System minimum requirements				
Nodes	**Collection units**	**Online operators**	**CPU**	**Server memory**	**Java heap size**	**Disk space for installation**	**Disk space for data storage**
0 to 200	0 to 5 K	20	2 cores	4 GB	512 MB	3 GB	30 GB
0 to 200	5 K to 50 K	10	2 cores	4 GB	512 MB	3 GB	60 GB
200 to 500	0 to 10 K	30	4 cores	6 GB	1 GB	3 GB	50 GB
200 to 500	10 K to 100 K	10	4 cores	6 GB	1 GB	3 GB	100 GB

Table 4 Hardware requirements for a 64-bit Windows operating system

Management scale			System minimum requirements				
Nodes	**Collection units**	**Online operators**	**CPU**	**Server memory**	**Java heap size**	**Disk space for installation**	**Disk space for data storage**
0 to 200	0 to 5 K	20	2 cores	4 GB	2 GB	3 GB	30 GB
0 to 200	5 K to 50 K	10	2 cores	4 GB	2 GB	3 GB	60 GB
200 to 1 K	0 to 10 K	30	4 cores	8 GB	2 GB	3 GB	50 GB
200 to 1 K	10 K to 100 K	10	4 cores	8 GB	2 GB	3 GB	100 GB
1 K to 2 K	0 to 20 K	30	6 cores	12 GB	4 GB	4 GB	60 GB
1 K to 2 K	20 K to 200 K	10	6 cores	12 GB	4 GB	4 GB	200 GB
2 K to 5 K	0 to 30 K	40	8 cores	24 GB	8 GB	5 GB	80 GB
2 K to 5 K	30 K to 300 K	20	8 cores	24 GB	8 GB	5 GB	250 GB
5 K to 10 K	0 to 40 K	50	16 cores	32 GB	12 GB	7 GB	100 GB
5 K to 10 K	40 K to 400 K	20	16 cores	32 GB	12 GB	7 GB	300 GB
10 K to 15 K	0 to 40 K	50	24 cores	64 GB	16 GB	10 GB	200 GB
10 K to 15 K	40 K to 400 K	20	24 cores	64 GB	16 GB	10 GB	600 GB

Table 5 Hardware requirements for a 32-bit Linux operating system

Management scale			System minimum requirements				
Nodes	**Collection units**	**Online operators**	**CPU**	**Server memory**	**Java heap size**	**Disk space for installation**	**Disk space for data storage**
0 to 200	0 to 5 K	20	2 cores	6 GB	512 MB	3 GB	30 GB
0 to 200	5 K to 50 K	10	2 cores	6 GB	512 MB	3 GB	60 GB
200 to 500	0 to 10 K	30	4 cores	8 GB	1 GB	3 GB	50 GB
200 to 500	10 K to 100 K	10	4 cores	8 GB	1 GB	3 GB	100 GB

Table 6 Hardware requirements for a 64-bit Linux operating system

Management scale			System minimum requirements				
Nodes	**Collection units**	**Online operators**	**CPU**	**Server memory**	**Java heap size**	**Disk space for installation**	**Disk space for data storage**
0 to 200	0 to 5 K	20	2 cores	6 GB	2 GB	3 GB	30 GB
0 to 200	5 K to 50 K	10	2 cores	6 GB	2 GB	3 GB	60 GB
200 to 1 K	0 to 10 K	30	4 cores	12 GB	4 GB	3 GB	50 GB
200 to 1 K	10 K to 100 K	10	4 cores	12 GB	4 GB	3 GB	100 GB
1 K to 2 K	0 to 20 K	30	6 cores	16 GB	6 GB	4 GB	60 GB
1 K to 2 K	20 K to 200 K	10	6 cores	16 GB	6 GB	4 GB	200 GB
2 K to 5 K	0 to 30 K	40	8 cores	24 GB	8 GB	5 GB	80 GB
2 K to 5 K	30 K to 300 K	20	8 cores	24 GB	8 GB	5 GB	250 GB
5 K to 10 K	0 to 40 K	50	16 cores	32 GB	12 GB	7 GB	100 GB
5 K to 10 K	40 K to 400 K	20	16 cores	32 GB	12 GB	7 GB	300 GB
10 K to 15 K	0 to 40 K	50	24 cores	64 GB	16 GB	10 GB	200 GB
10 K to 15 K	40 K to 400 K	20	24 cores	64 GB	16 GB	10 GB	600 GB

Software requirements

Table 7 Software requirements

Item	Requirement	Remarks
Windows		
Operating system	Windows Server 2008 (32-bit)	Service Pack 2
	Windows Server 2008 (64-bit)	Service Pack 2
	Windows Server 2008 R2	Service Pack 1
	Windows Server 2012	KB2836988
	Windows Server 2012 R2	N/A
Database	SQL Server 2008	Service Pack 3
	SQL Server 2008 R2	Service Pack 2
	SQL Server 2012	Service Pack 2
	SQL Server 2014	N/A
	SQL Server 2008 R2 SP2 Express	Used as the embedded database for SNS and standard editions only.
Linux		
Operating system	Red Hat Enterprise Linux Server 5.5 (32-bit)	N/A
	Red Hat Enterprise Linux Server 5.5 (64-bit)	N/A
	Red Hat Enterprise Linux Server 5.9 (32-bit)	N/A
	Red Hat Enterprise Linux Server 5.9 (64-bit)	N/A
	Red Hat Enterprise Linux Server 6.1 (64-bit)	N/A
	Red Hat Enterprise Linux Server 6.4 (64-bit)	N/A
Database	Oracle 11*g* Release 1	N/A
	Oracle 11*g* Release 2	N/A
Both Linux and Windows		
Database	MySQL Enterprise Server 5.1	A maximum of 1000 devices are supported.
	MySQL Enterprise Server 5.5	
	MySQL Enterprise Server 5.6	

VM requirements

As a best practice, install IMC on a physical server.

Table 8 Hypervisor platform requirements

OS	Hypervisor
Windows	VMware ESX Windows Hyper-V
Linux	VMware ESX

Table 9 Hypervisor platform requirements

Vendor	Hypervisor
VMware	VMware Workstation 6.5.x VMware Workstation 9.0.x VMware ESX Server 4.x VMware ESX Server 5.x
Hyper-V	Windows Server 2008 R2 Hyper-V Windows Server 2012 Hyper-V

If IMC is installed on a virtual machine, do not change the following virtual machine configuration settings:

- CPU cores
- Number, model, and MAC addresses of network adapters
- Number of disk drives
- Storage paths
- Assignment of storage

If the settings are changed, IMC might not operate correctly.

Preparing the installation environment

To ensure the correct installation and operation of IMC, do not install IMC with other network management products on the same server.

Do not install IMC in an IPv6 environment.

Uninstalling previous versions of IMC

If IMC was previously installed on the system, then thoroughly uninstall it first. For information about uninstalling IMC, see "Uninstalling IMC."

After you uninstall IMC:

- On Windows, delete the **iMC-Reserved** folder from the **WINDOWS** folder of the system disk.
- On Linux, delete the **iMC-Reserved** folder from the **/etc** directory.

Checking ports and firewalls

Make sure the IMC Web service ports and database listening ports are open in the firewall. Table 10 lists the default IMC Web service ports and database listening ports.

Table 10 IMC port requirements

Server	Usage: protocol/default port	Direction
Web	HTTP: TCP/8080 HTTPS: TCP/8443	Browser to IMC
Database	SQL Server database: TCP/1433 Oracle database: TCP/1521 MySQL database: TCP/3306	IMC and components to the database

NOTE:

Other IMC components might have additional port requirements. For more information, see "Security settings."

Make sure the **javaw.exe** and **java.exe** programs are not blocked by the firewall. In Windows, these programs are located in the **\common\jre\bin** directory of the IMC installation path. In Linux, these programs are located in the **/common/jre/bin/java** directory of the IMC installation path.

Use tools such as **netstat -a** and **telnet hostname port** to verify access between systems.

Checking the database configuration

Before installing non-basic editions of IMC, first install the database server and configure the database services to automatically start with the operating system.

For example, to use a SQL Server database for IMC, install the database before IMC installation and set the startup type of the **SQL Server** and **SQL Server Agent** services to **Automatic**. To view the startup type of the database services, click **Start**, and then select **Administrative Tools** > **Services**.

Checking the installation environment

The IMC installation package provides a tool (envcheck) to check the system environment and database connectivity.

To use the envcheck tool:

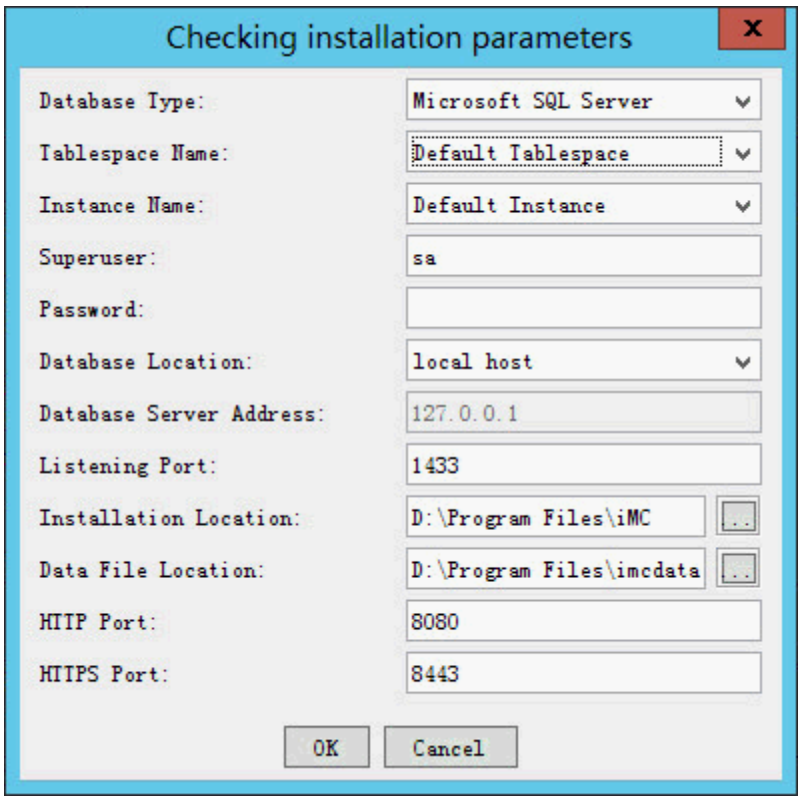
1. Copy the envcheck tool (**envcheck.bat** for Windows or **envcheck.sh** for Linux) from the **tools** folder to the **install** folder of the IMC installation package.
2. Run the tool.

   The **Checking installation environments** dialog box opens.

   The system checks the port availability, free physical memory, and legacy database server or client.

   After the checks are complete, the **Checking installation parameters** dialog box opens, as shown in Figure 1. The following information uses Windows and Microsoft SQL Server as an example.

Figure 1 Checking installation parameters



3. Configure the parameters for checking database connectivity:
   - **Database Type**—Select the database type. Options are **Microsoft SQL Server**, **MySQL**, and **Oracle**. The default is **Microsoft SQL Server**.
   - **Tablespace Name**—To connect to the default tablespace of the database, select **Default Tablespace**. To connect to a named tablespace, select **Other Tablespace**, and then enter the tablespace name.
   - **Instance Name**—To connect to the default instance of the database, select **Default Instance**. To connect to a named instance, select **Other Instance**, and then enter the instance name.

     NOTE:

     If you install IMC on Linux and use an Oracle database, the **Network Service Name** parameter is displayed instead of **Instance Name**. You can select a network service name or click the **Add Network Service Name** icon to add a network service name. For more information about configuring the network service name, see *Oracle 11g Installation and Configuration Guide* or *Oracle 11g R2 Installation and Configuration Guide*.

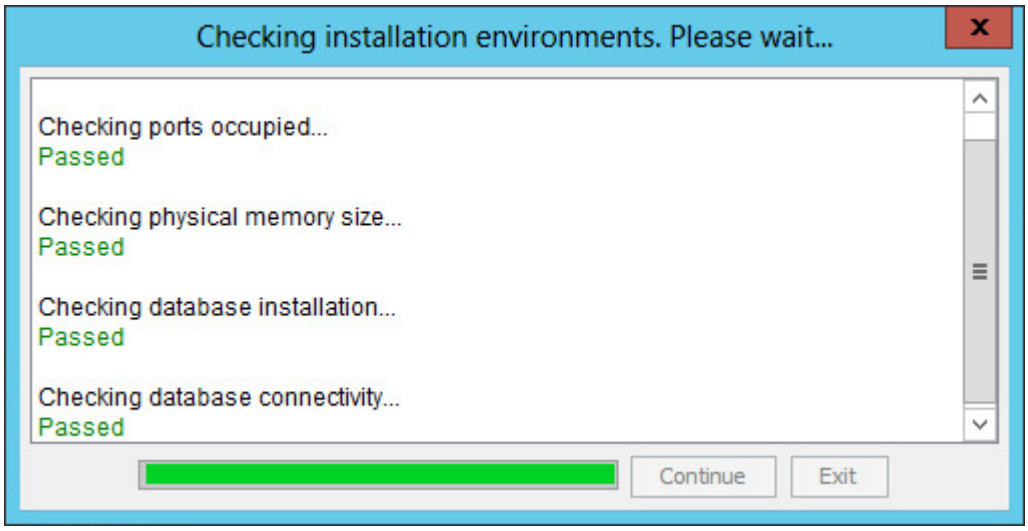
   - **Superuser**—Enter the database superuser name. The default is **sa**.
   - **Password**—Enter the password of the superuser.
   - **Database Location**—Select **local host** from the list.
   - **Database Server Address**—This field is automatically populated with **127.0.0.1** and cannot be modified.
   - **Listening Port**—Enter the listening port of the database server. The default is **1433**.
   - **Installation Location**—Specify the local directory for storing the IMC installation package.
   - **Data File Location**—Specify the local directory for storing the data files.
   - **HTTP Port**—Enter the HTTP port number for the IMC Web server. The default is 8080.

- **HTTPS Port**—Enter the HTTPS port number for the IMC Web server. The default is 8443.

4. Click **OK**.

   The **Checking installation environments** dialog box displays the check results, as shown in Figure 2.

   Figure 2 Check results



5. Click **Exit**.

Fix any failed check items according to the check results.

Superuser account

Before IMC installation, obtain the password of the database superuser account or other database user accounts that have superuser privileges.

During the IMC platform installation, IMC uses the superuser account and password for database access, and then creates database files and user accounts for each deployed component. The deployed IMC platform subcomponents and service components use their own user accounts for database access.

If the password of the superuser account is changed after IMC deployment, be sure to update the password in IMC. If the password is not promptly updated, you cannot view database information on the **Environment** tab, deploy new components, or update existing components for IMC.

To update the database user password in IMC:

1. Start the Intelligent Deployment Monitoring Agent, and then click the **Environment** tab.
2. Click **Change Password**.

   The **Change Password** button is displayed only when the Intelligent Deployment Monitoring Agent detects the incorrect database user password.

3. Enter the new database password, and then click **OK**, as shown in Figure 3.

Figure 3 Changing the superuser password

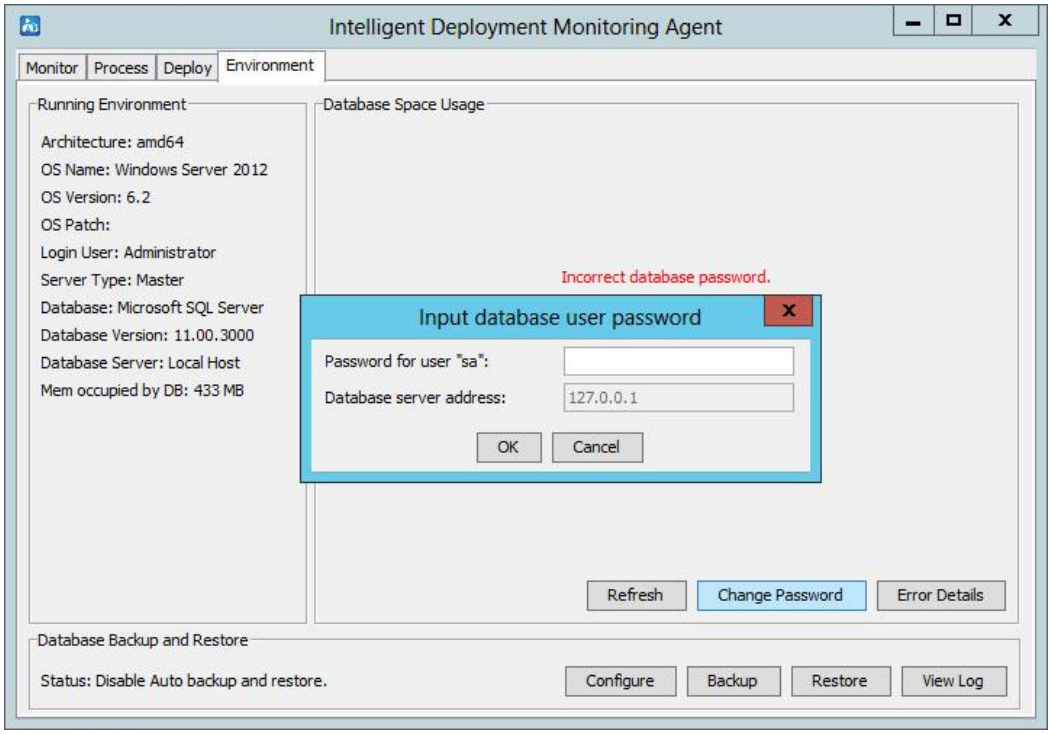


Table 11 lists the default superuser accounts of SQL Server, MySQL, and Oracle databases.

Table 11 Database superuser accounts

Database	Superuser
SQL Server	sa
Oracle	• system • sys
MySQL	root

Setting the system time

As a best practice, configure the following settings:

- Set the time zone to GMT or Coordinated Universal Time.
- Do not enable seasonal time adjustments such as daylight savings time.
- Before installing IMC, verify that the system time, date, and time zone settings on the server are correct.

Do not modify the system time on the server after IMC is started. If you modify the system time, the following issues might occur:

- When jumping to a future time, the system might get so occupied in processing the sudden burst of expired data that realtime data sampling will be delayed. The delay is automatically recovered after the processing of expired data is complete.
- When you modify the system time to a past time, data with overlapping time occurs, and data processing might become abnormal. After the overlapping time is past, data processing becomes normal again.

Installing and deploying the IMC platform

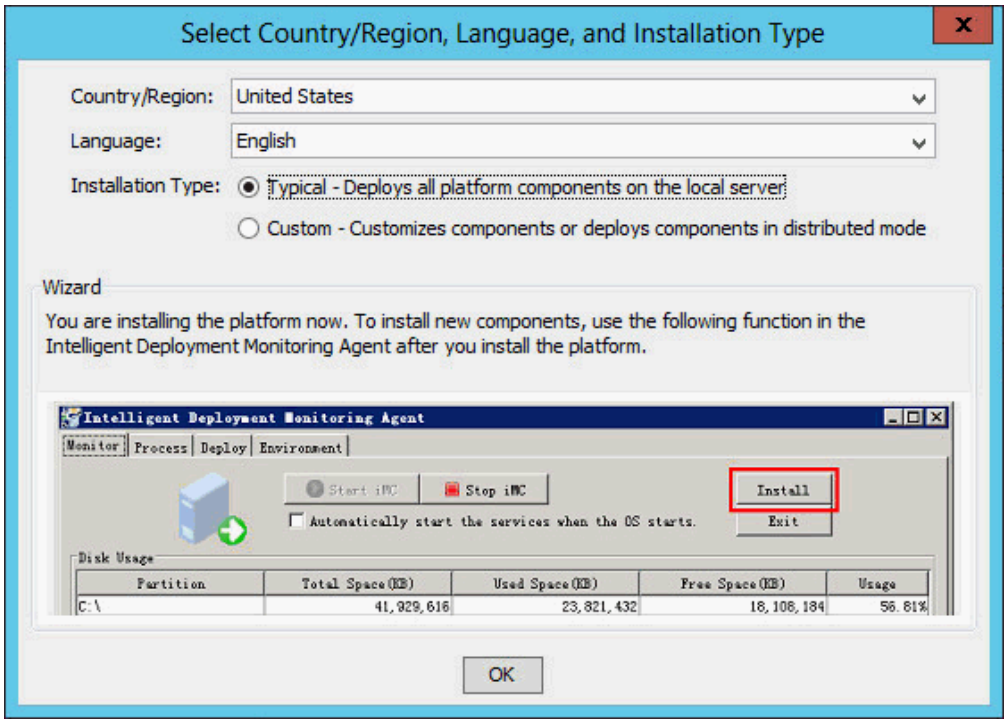
The following information describes how to install and deploy the IMC platform on a Windows host that is already installed with a SQL Server database.

Selecting the installation type

1. Log on to Windows as an administrator.
2. Run the **install.bat** script in the **install** directory of the IMC installation package.

   The **Select Country/Region, Language, and Installation Type** dialog box appears, as shown in Figure 4.

Figure 4 Select Country/Region, Language, and Installation Type dialog box



3. Select the country/region, language, and installation type.

   IMC supports typical and custom installations.

   - **Typical**—All platform subcomponents are automatically installed and deployed on the local host without manual intervention.
   - **Custom**—You can select desired platform subcomponents to install on the local host. After installation is complete, manually deploy the platform subcomponents.
4. Click **OK**.

To install the IMC platform on a Linux host, use the following guidelines:

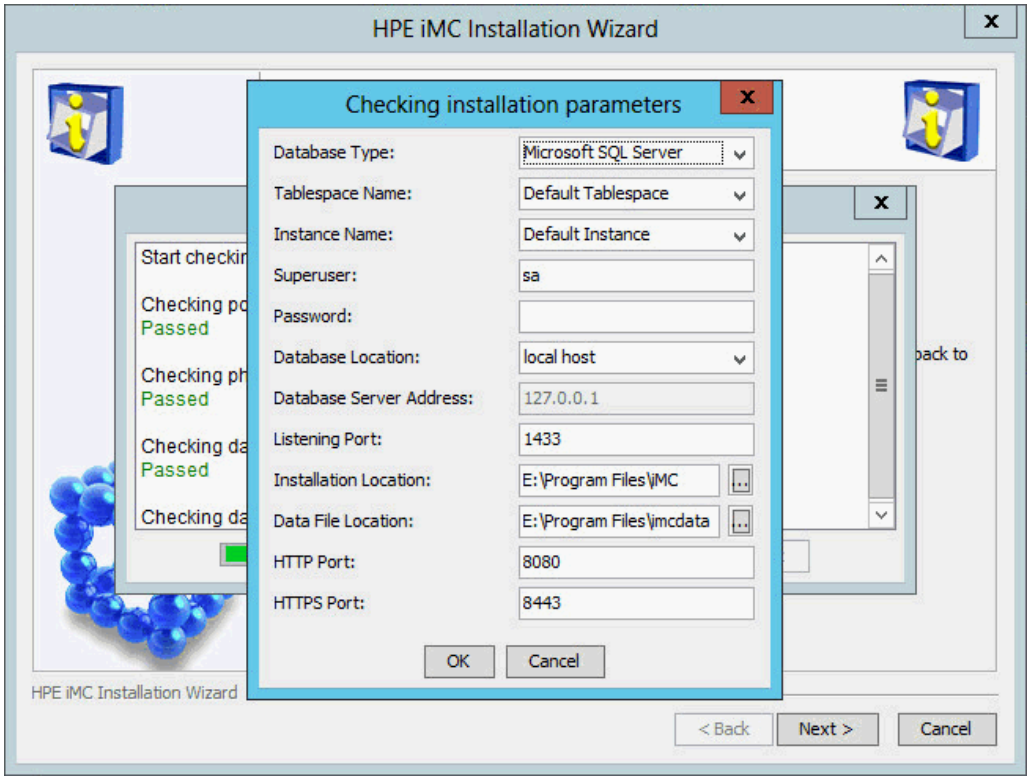
- Run the **install.sh** script in the **install** directory of the IMC installation package as a root user.
- If Linux 6.x is used, copy the IMC installation package to a local directory before you run the **install.sh** script.
- If the IMC installation package is transferred through FTP, grant read access to the **install.sh** script by executing **chmod –R 775 install.sh** in the directory of the script.

Installing the IMC platform in typical mode

1. In the **Select Locale** dialog box, select the **Typical** installation type, and then click **OK**.

   The **Checking installation parameters** dialog box opens, as shown in Figure 5.

   Figure 5 Checking installation environment



2. Configure the parameters as needed.

   In this example, enter the password of the database superuser **sa**, use the default settings for other parameters, and then click **OK**.

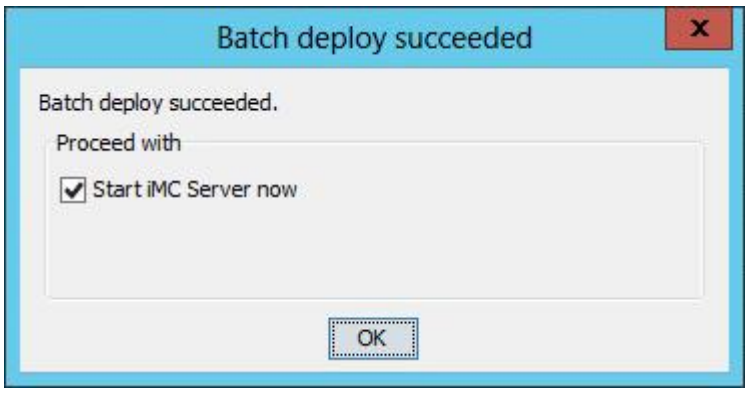
   The system checks the installation environment and database connectivity, and then displays the check results.

   Fix any failed check items according to the check results.

   After the checks are passed, the system installs and deploys all IMC platform subcomponents.

   After IMC installation and deployment is complete, the **Batch deploy succeeded** dialog box opens, as shown in Figure 6.

Figure 6 Batch deploy succeeded



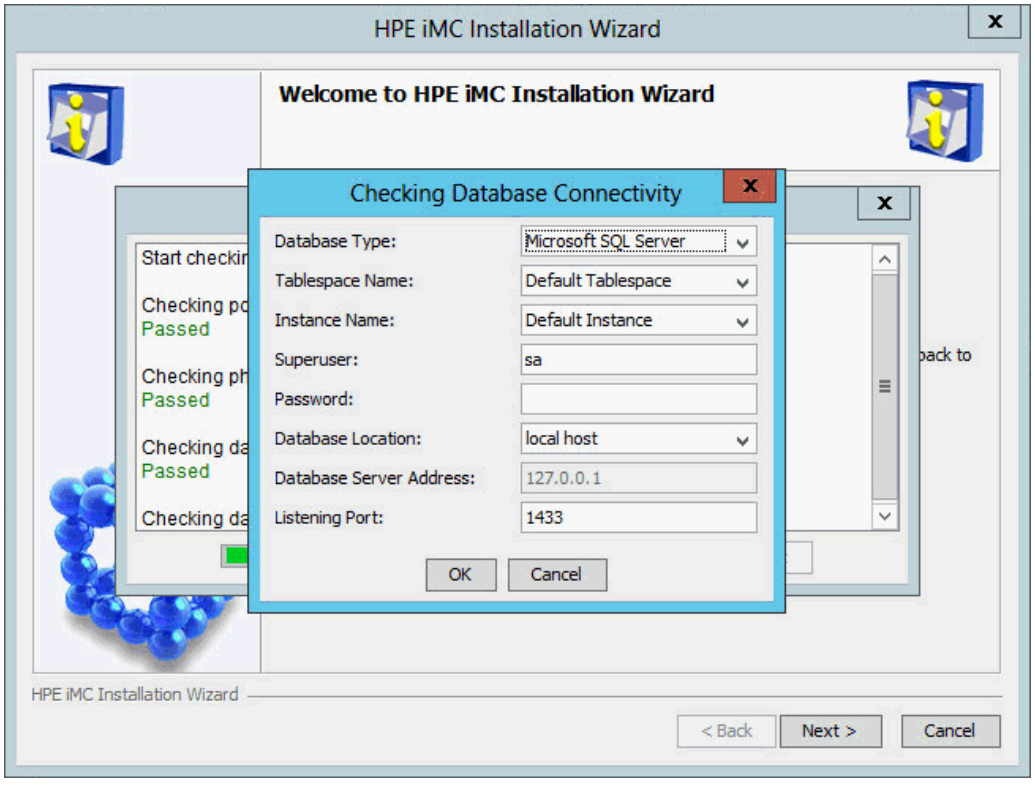
3. Click **OK**.

Installing the IMC platform in custom mode

1. In the **Select Locale** dialog box, select the **Custom** installation type, and then click **OK**.

   The **Checking Database Connectivity** dialog box opens, as shown in Figure 7.

   Figure 7 Checking Database Connectivity dialog box



2. Configure the parameters as needed.

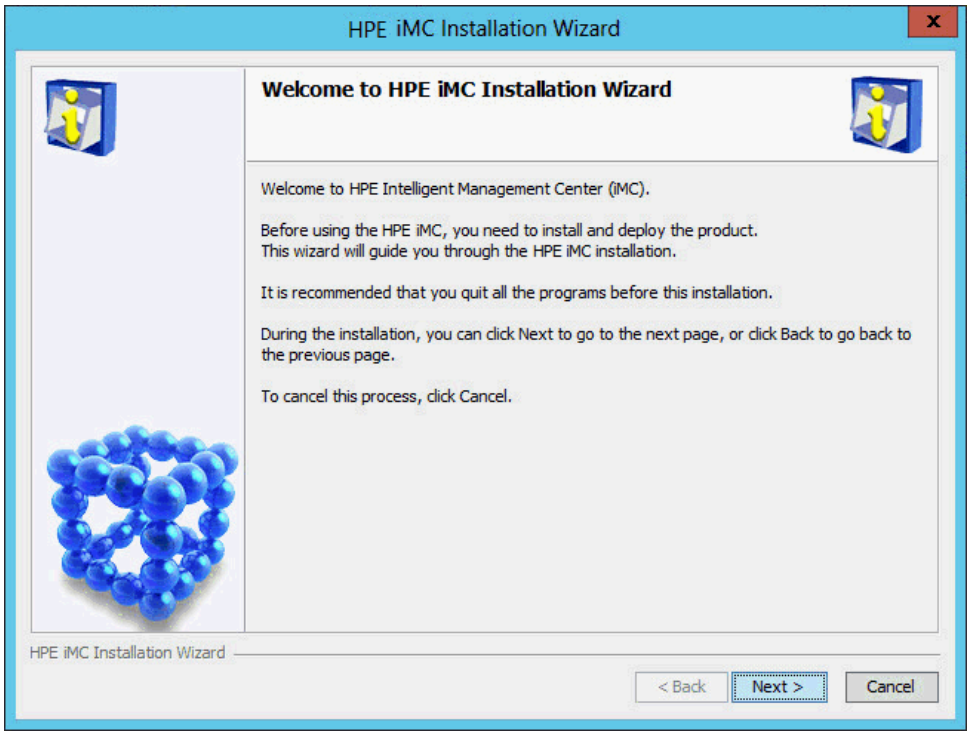
   In this example, enter the password of the database superuser **sa**, use the default settings for other parameters, and then click **OK**.

   The system checks the installation environment and database connectivity, and then displays the check results.

   Fix any failed check items according to the check results.

After the checks are passed, the IMC installation wizard opens, as shown in Figure 8.

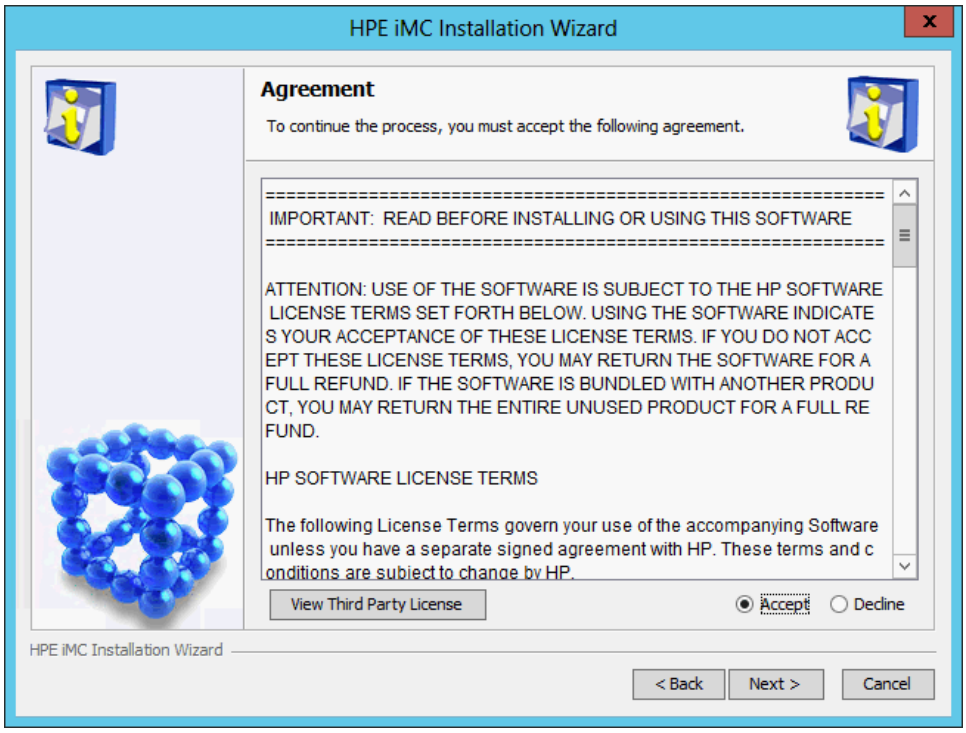
Figure 8 IMC installation wizard



3. Click **Next**.

   The **Agreement** page opens, as shown in Figure 9.

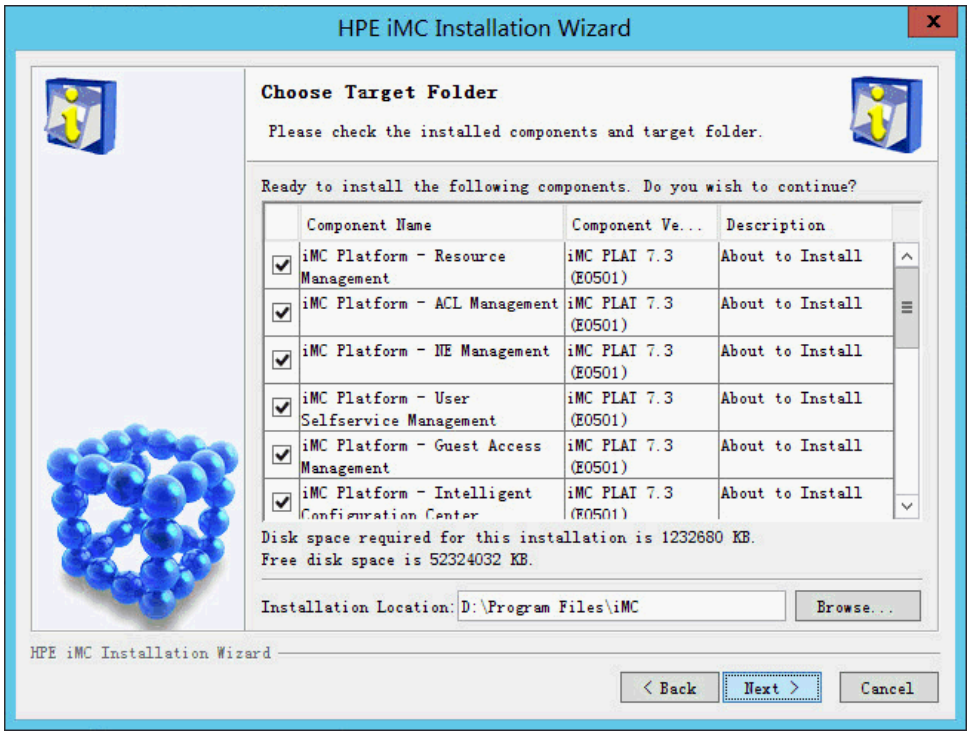
   Figure 9 Agreement page



4. Read the license agreement, select **Accept**, and then click **Next**.

The **Choose Target Folder** page opens, as shown in Figure 10.

Figure 10 Choose Target Folder page



5. Select the components you want to install and specify a local path as the installation location.

   The installation program checks whether the specified installation path contains any files. If the path contains files, a message is displayed. Click **OK** to delete the files.

   The default installation location is *X*:**\Program Files\iMC**, where *X* is the drive letter of the disk with the largest amount of free space.

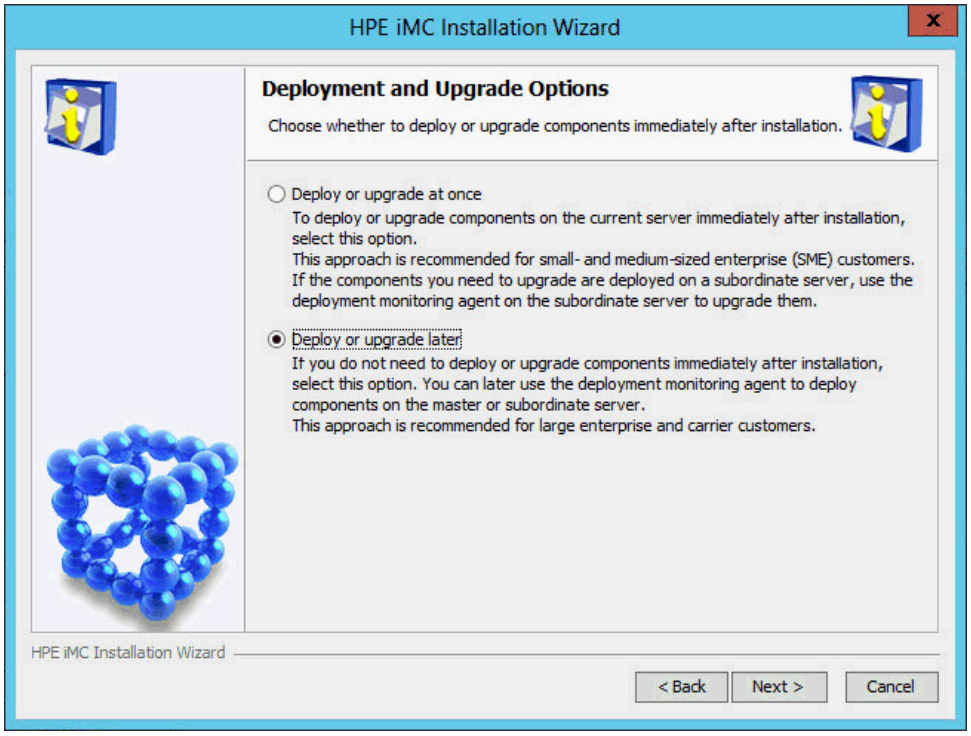
   NOTE:

   - If you install the IMC platform on a Linux host, do not use a symlink path as the installation location.
   - In Linux, the default installation location is **/opt/iMC**.

6. Click **Next**.

   The **Deployment and Upgrade Options** page opens, as shown in Figure 11.

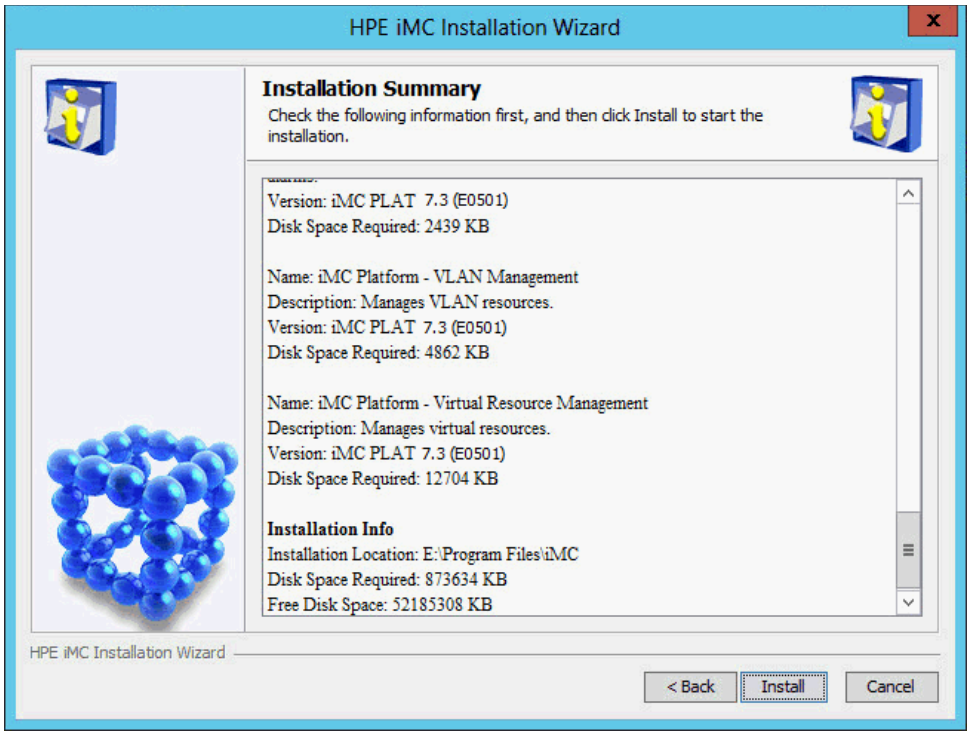
Figure 11 Deployment and Upgrade Options page



7. Select **Deploy or upgrade later**.
8. Click **Next**.

   The **Installation Summary** page opens, as shown in Figure 12.

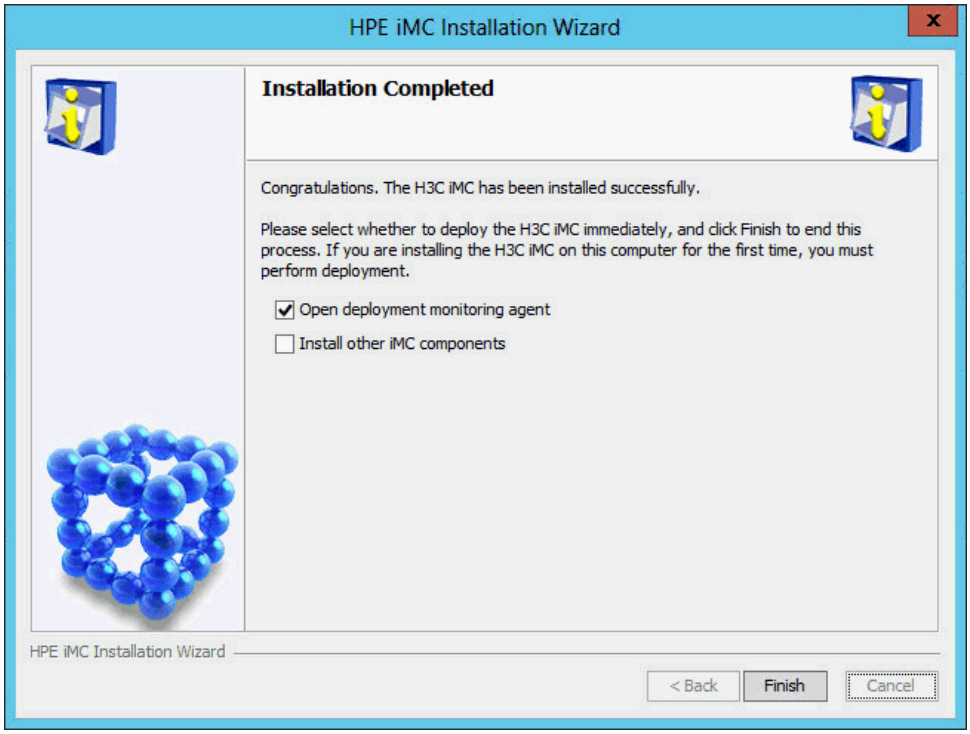
Figure 12 Installation Summary page



9. Verify the installation summary, and then click **Install**.

After the installation is complete, the **Installation Completed** page opens, as shown in Figure 13.

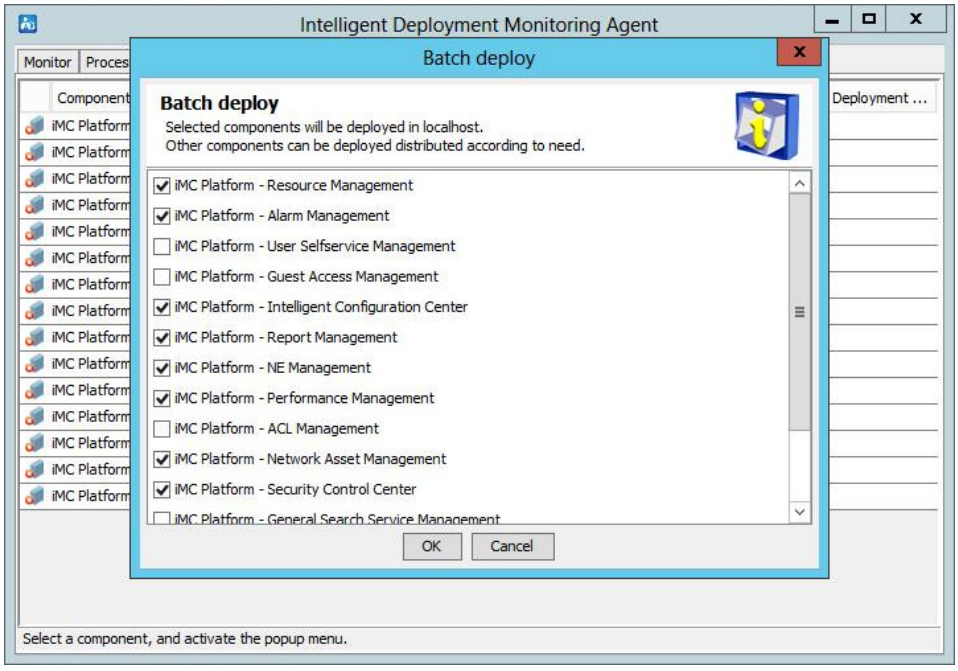
Figure 13 Installation Completed page



10. Select **Open deployment monitoring agent**, and then click **Finish**.

    The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** dialog box, as shown in Figure 14.

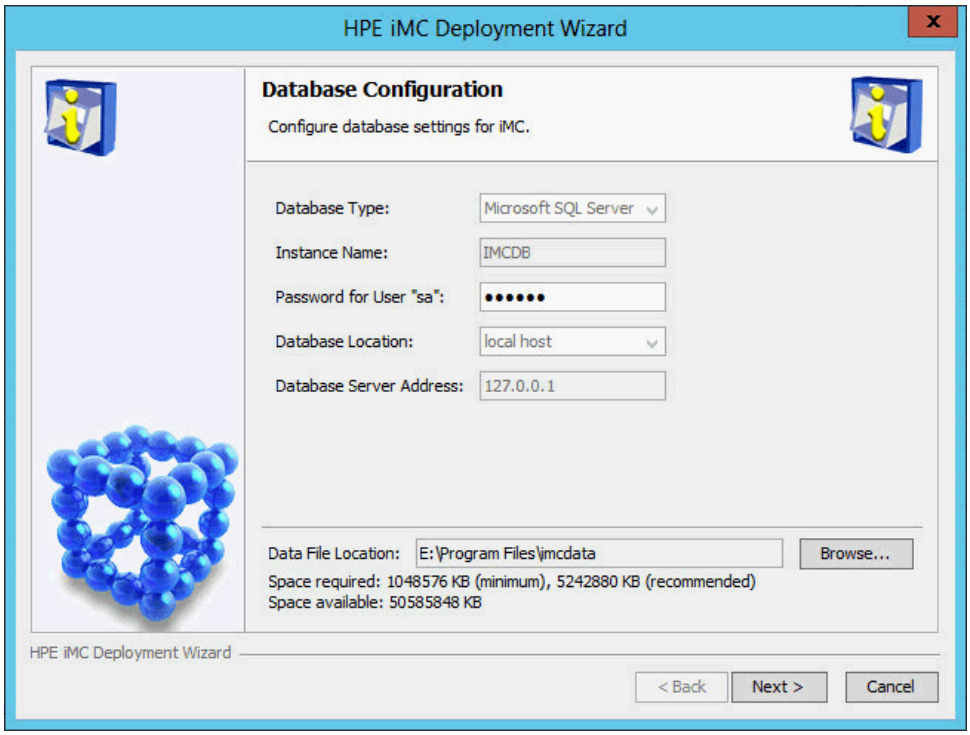
Figure 14 Batch deploy dialog box



11. Select the components to be deployed, and then click **OK**.

The **Database Configuration** page opens, as shown in Figure 15.

Figure 15 Database Configuration page



12. Enter the password of the superuser.
13. Set the data file location.

    Make sure the specified data file location is on a readable, writable, and uncompressed disk drive and does not include any files.

    The default data file location is *X*:**\Program Files\imcdata**, where *X* is the drive letter of the disk that has the largest amount of free space.

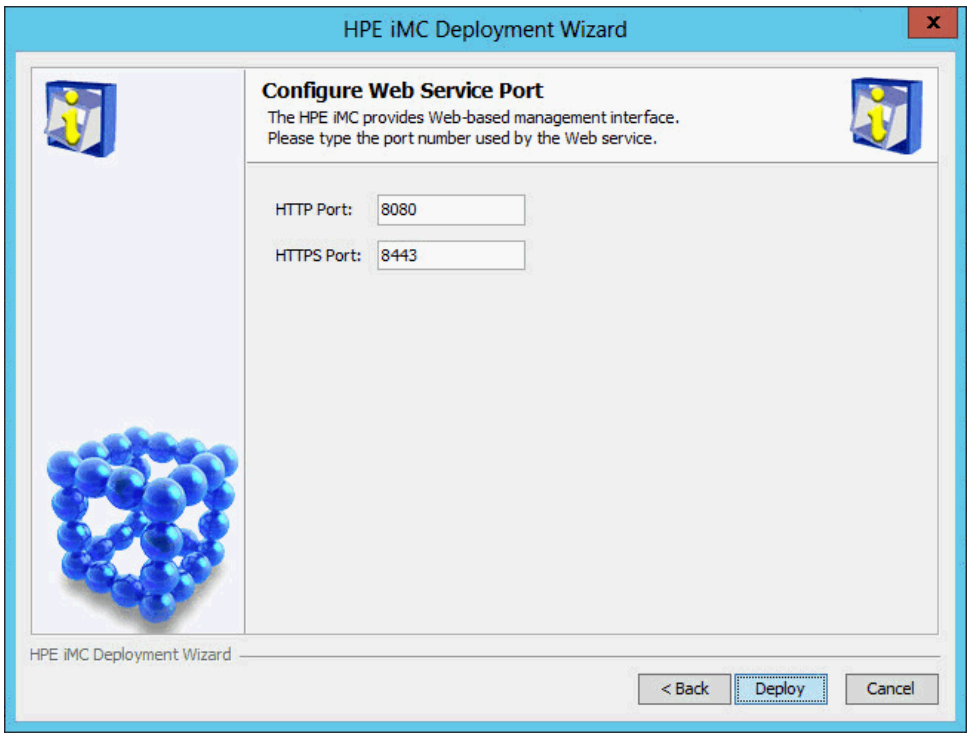
NOTE:

On Linux, the default data file location is **/opt/imcdata**.

14. Click **Next**.

    The **Configure Web Service Port** page opens, as shown in Figure 16.

Figure 16 Configure Web Service Port page



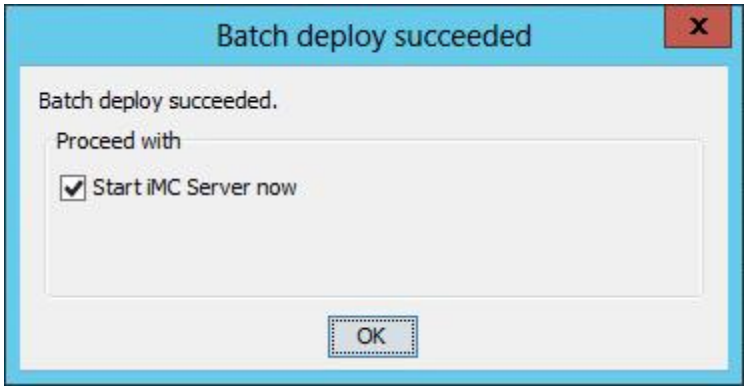
15. Enter the HTTP and HTTPS port numbers. This example uses the default port numbers 8080 and 8443.

If you specify other port numbers, make sure the specified ports are not used by other services.

16. Click **Deploy**.

After the deployment is complete, the **Batch deploy succeeded** dialog box opens, as shown in Figure 17.

Figure 17 Batch deploy succeeded dialog box



17. Click **OK**.

Managing IMC by using the Intelligent Deployment Monitoring Agent

The Intelligent Deployment Monitoring Agent is automatically installed after the IMC platform is installed.

As the IMC management and maintenance tool, the Intelligent Deployment Monitoring Agent provides IMC operation information as well as a variety of management options, such as:

- Starting and stopping IMC.
- Installing new components.
- Upgrading IMC components.
- Deploying and removing components.

Starting the Intelligent Deployment Monitoring Agent

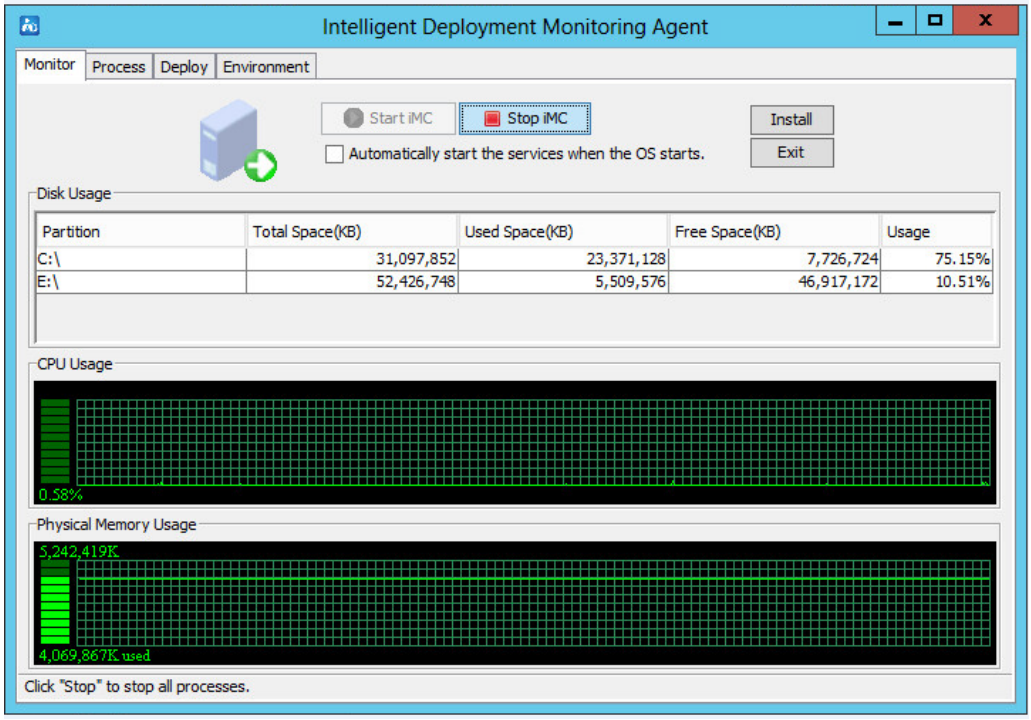
Click **Start**, and then select **All Programs** > **HP Intelligent Management Center**.

The Intelligent Deployment Monitoring Agent opens.

As shown in Figure 18, the agent contains the following tabs: **Monitor**, **Process**, **Deploy**, and **Environment**. By default, the **Monitor** tab is displayed.

The following information describes the functionality of each tab.

Figure 18 Intelligent Deployment Monitoring Agent



NOTE:

To start the Intelligent Deployment Monitoring Agent on Linux, run the **dma.sh** script in the **/deploy** directory of the IMC installation path.

Monitor tab

As shown in Figure 19, the **Monitor** tab displays the performance information of the IMC server, including the disk, CPU, and physical memory usage information.

The tab also provides the following options:

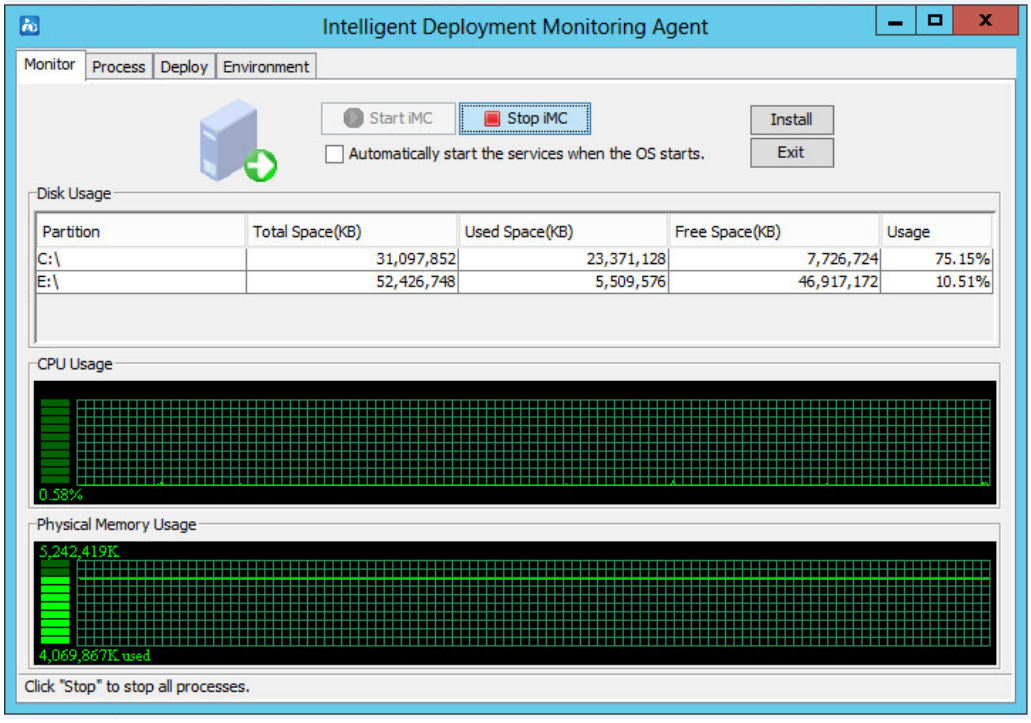
- **Start iMC**—Click this button to start IMC. This button is available when IMC is stopped.

IMPORTANT:

For correct operation, start the **HP iMC Server** service with an account that has read/write permissions on the IMC installation folder. By default, the **HP iMC Server** service starts with the **Local System** account.

- **Stop iMC**—Click this button to stop IMC. This button is available when IMC is already started.
- **Automatically start the services when the OS starts**—Select this option to automatically start IMC when the operating system starts.
- **Install**—Click this button to install new components or upgrade existing components.
- **Exit**—Click this button to exit the Intelligent Deployment Monitoring Agent.

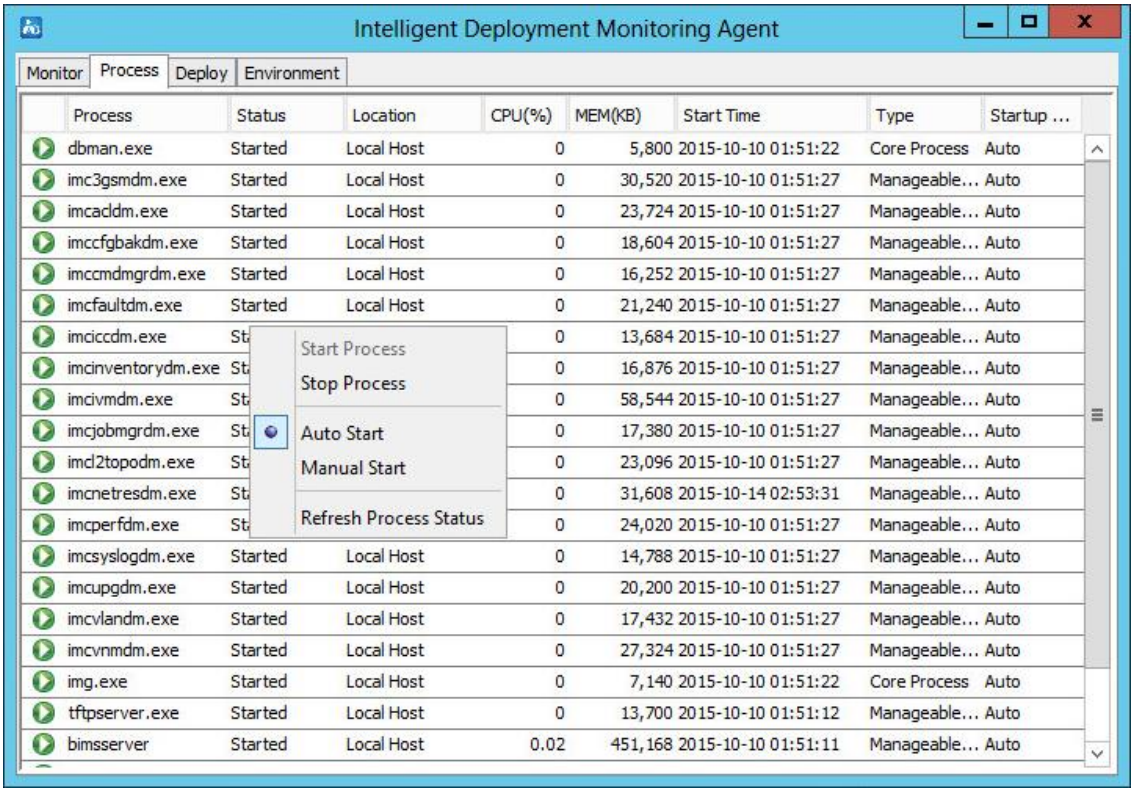
Figure 19 Monitor tab of the Intelligent Deployment Monitoring Agent



Process tab

As shown in Figure 20, the **Process** tab displays IMC process information.

Figure 20 Process tab of the Intelligent Deployment Monitoring Agent



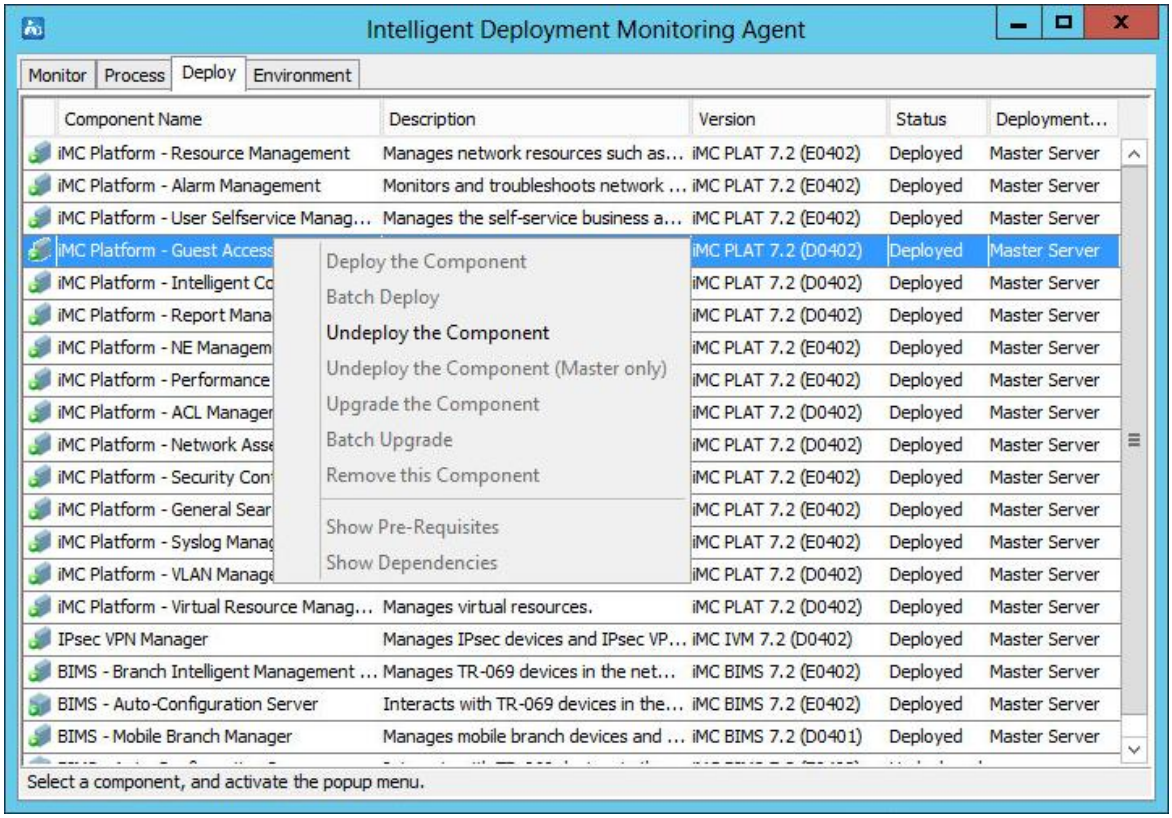
The right-click menu of a manageable process provides the following options:

- **Start Process**—Select this option to start the process. This option is available when the process is stopped.
- **Stop Process**—Select this option to stop the process. This option is available when the process is started.
- **Auto Start**—Select this option to enable automatic startup of the process when IMC is started.
- **Manual Start**—Select this option to require manual startup of the process.
- **Refresh Process Status**—Select this option to refresh the status of the process.

Deploy tab

As shown in Figure 21, the **Deploy** tab displays information about all deployed components.

Figure 21 Deploy tab of the Intelligent Deployment Monitoring Agent



The right-click menu of a component provides the following options:

- **Deploy the Component**—Select this option to deploy the component on the local host.

  This option is available only when the selected component is in **Undeployed** state.
- **Batch Deploy**—Select this option to batch deploy components on the local host.

  Components can be deployed only when they have been installed but in **Undeployed** state.
- **Undeploy the Component**—Select this option to undeploy the component.

  This option is available only when the selected component is in **Deployed** state.
- **Undeploy the Component (Master only)**—Select this option to delete component deployment information from the master server.

  This option is available only when the subordinate server where the component is deployed cannot operate correctly.
- **Upgrade the Component**—Select this option to upgrade the component.
- **Batch Upgrade**—Select this option to upgrade components in batches.
- **Remove this Component**—Select this option to remove the component from the host.

  This option is available only when the selected component is in **Undeployed** state.
- **Show Pre-Requisites**—Select this option to view all components that the selected component depends on. The component can be deployed only after the dependent components have been deployed.

  This option is unavailable if the component does not depend on any other components.
- **Show Dependencies**—Select this option to view all components that depend on the selected component.

  This option is unavailable if no other components depend on the selected component.

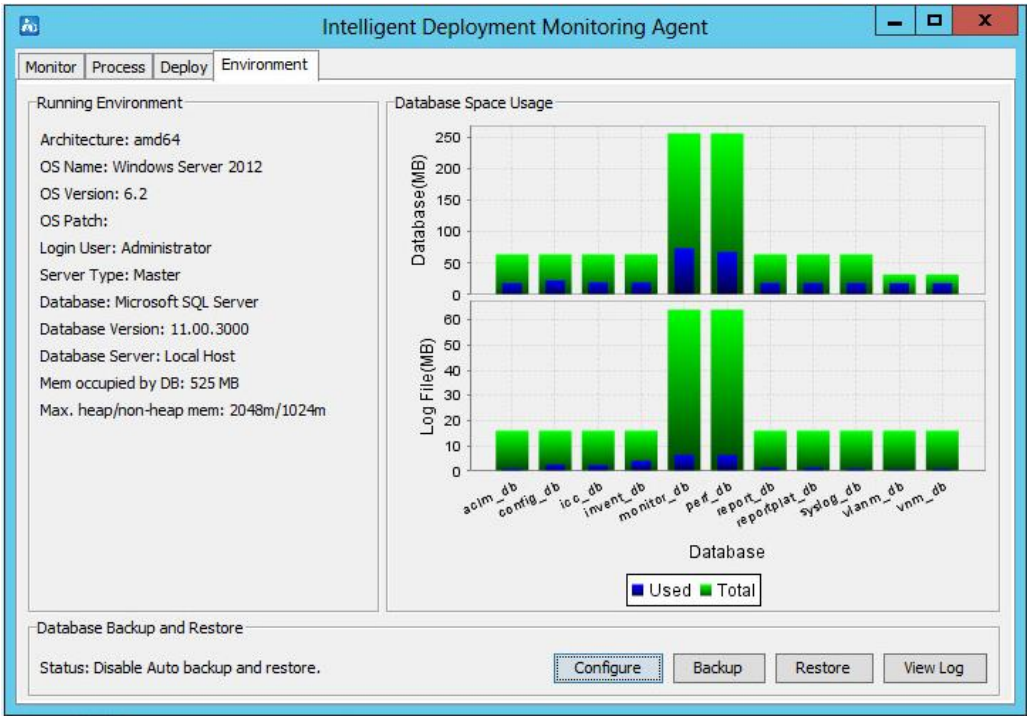
Environment tab

As shown in Figure 22, the **Environment** tab displays the software, hardware, and database information for the current IMC server.

The tab also provides database backup and restoration options in the **Database Backup and Restore** area.

For more information about the **Environment** tab, see "Backing up and restoring the database."

Figure 22 Environment tab of the Intelligent Deployment Monitoring Agent



Installing and deploying IMC service components

The following information describes how to install and deploy the service components. Table 12 lists all service components and subcomponents in IMC.

Table 12 Service components and subcomponents

Component	Subcomponent
User Access Manager	• Intelligent Strategy Proxy • User Access Management • User Access Management Sub Server • Portal Server • EIP Server • EIP Sub Server • Policy Server • Policy Proxy Server • User SelfService • Third-Party Page Publish Server
TACACS+ Authentication Manager	TACACS+ Authentication Manager
EAD Security Policy	• Security Policy Configuration • Desktop Asset Manager • Desktop Asset Manager Proxy Server
iNode DC	iNode Dissolvable Client
MPLS VPN Manager	• MPLS VPN Management • MPLS TE management • L2VPN Management
IPsec VPN Manager	IPsec VPN Manager
Voice Service Manager	Voice Service Manager
Wireless Service Manager	• Wireless Service Manager • Wireless Intrusion Prevention System • Wireless Location Manager • Wireless Location Engine
Network Traffic Analyzer	• Network Traffic Analyzer • Network Behavior Analyzer • Network Traffic Analyzer Server • Network Behavior Analyzer Server
User Behavior Auditor	• User Behavior Auditor • User Behavior Auditor Server • Network Behavior Analyzer • Network Behavior Analyzer Server
Service Operation Manager	• CMDB Management • Service Desk
Application Manager	Application Manager
QoS Manager	QoS Management
Service Health Manager	• Service Health Management

Component	Subcomponent
	• NQA Collector Management
VAN Connection Manager	VAN Connection Management
Branch Intelligent Management System	• Branch Intelligent Management System • Auto-Configuration Server
Resource Automation Manager	Resource Automation Manager
VAN SDN Manager	VAN SDN Manager
VAN Fabric Manager	VAN Fabric Manager
UC Health Manager	UC Health Manager

All service components can be installed in the same way, but their deployment procedure might differ. Based on the deployment procedure, the service components can be classified into several categories, as listed in Table 13.

Table 13 Service components classified by deployment procedure

Example component	Similar components
NTA	IVM, VSM, WSM, UBA, SOM, APM, QoSM, SHM, VCM, BIMS, RSM, RAM, SDNM, VFM, UCHM, iNode DC
UAM	EAD, TAM
MVM	N/A

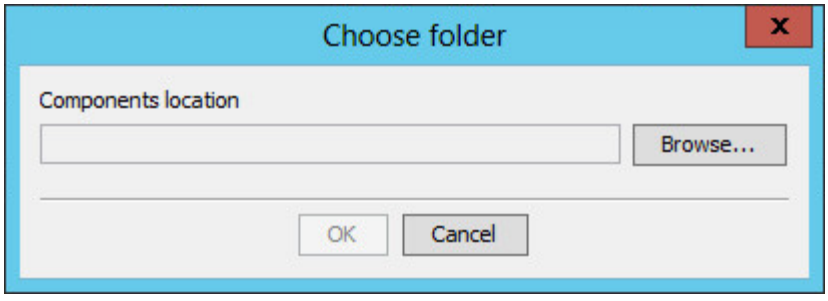
The following information describes how to install and deploy NTA, UAM, and MVM.

Installing and deploying IMC NTA

1. Start the Intelligent Deployment Monitoring Agent, and then click **Install** on the **Monitor** tab.

   The **Choose folder** dialog box opens, as shown in Figure 23.

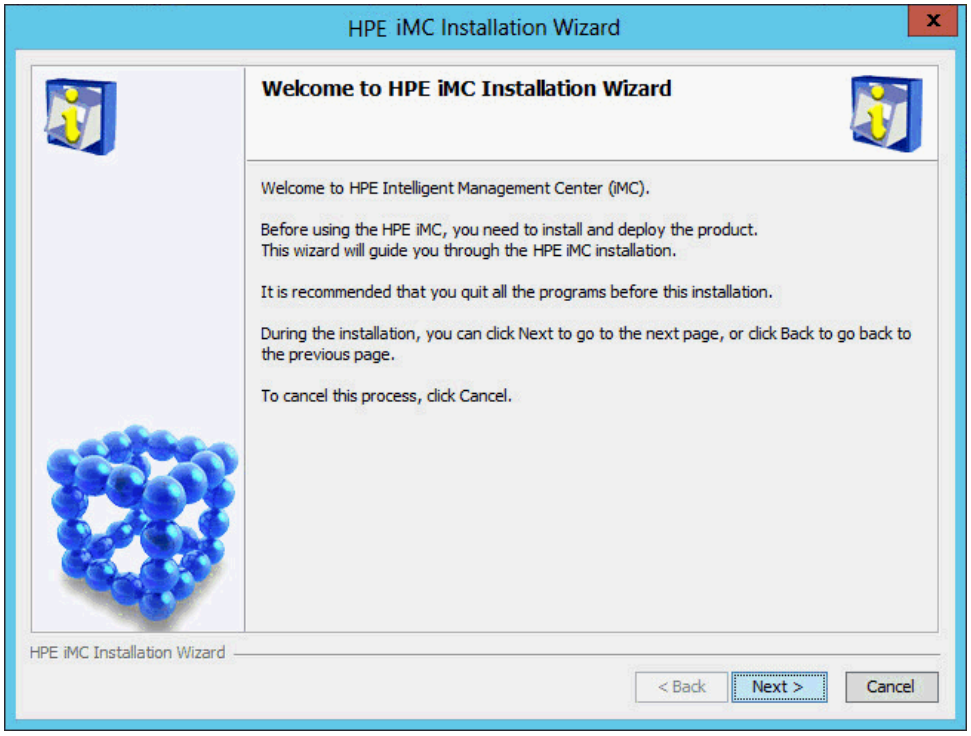
   Figure 23 Choose folder dialog box

2. Click **Browse**, and then select the **install\components** folder in the NTA installation package.
3. Click **OK**.

   The IMC installation wizard opens, as shown in Figure 24.

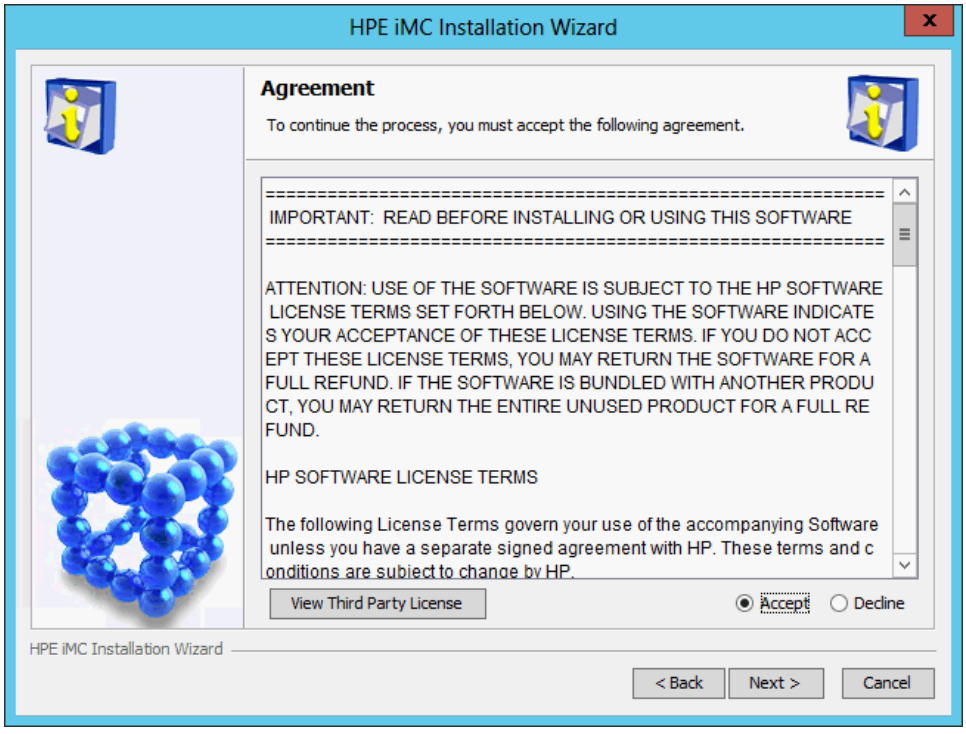
Figure 24 IMC installation wizard



4. Click **Next**.

   The **Agreement** page opens, as shown in Figure 25.

Figure 25 Agreement page

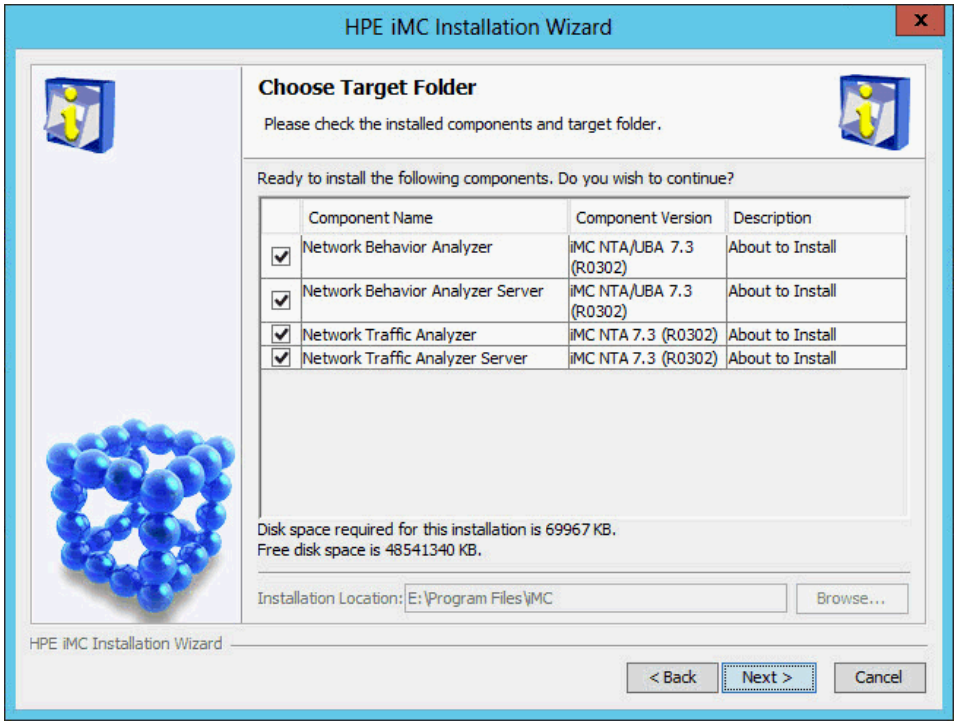


5. Read the license agreement and third-party license, and then select **Accept**.
6. Click **Next**.

The **Choose Target Folder** page opens, as shown in Figure 26.

The **Installation Location** field is automatically populated with the installation location of the IMC platform and cannot be modified.

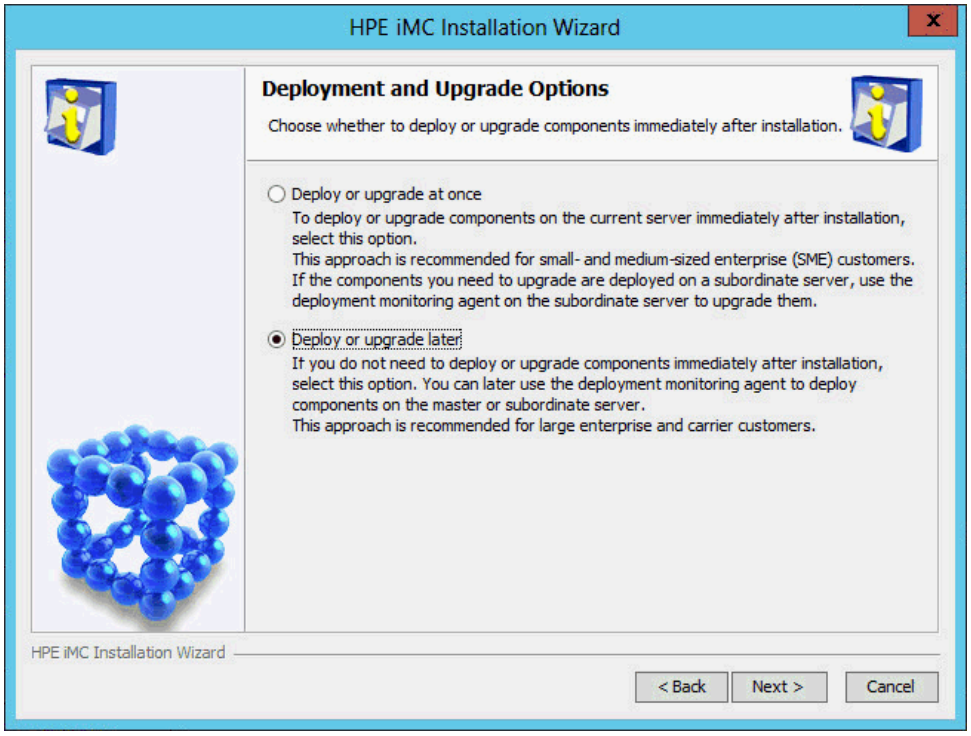
Figure 26 Choose Target Folder page



7. Select the NTA subcomponents you want to install in the component list.
8. Click **Next**.

   The **Deployment and Upgrade Options** page opens, as shown in Figure 27.

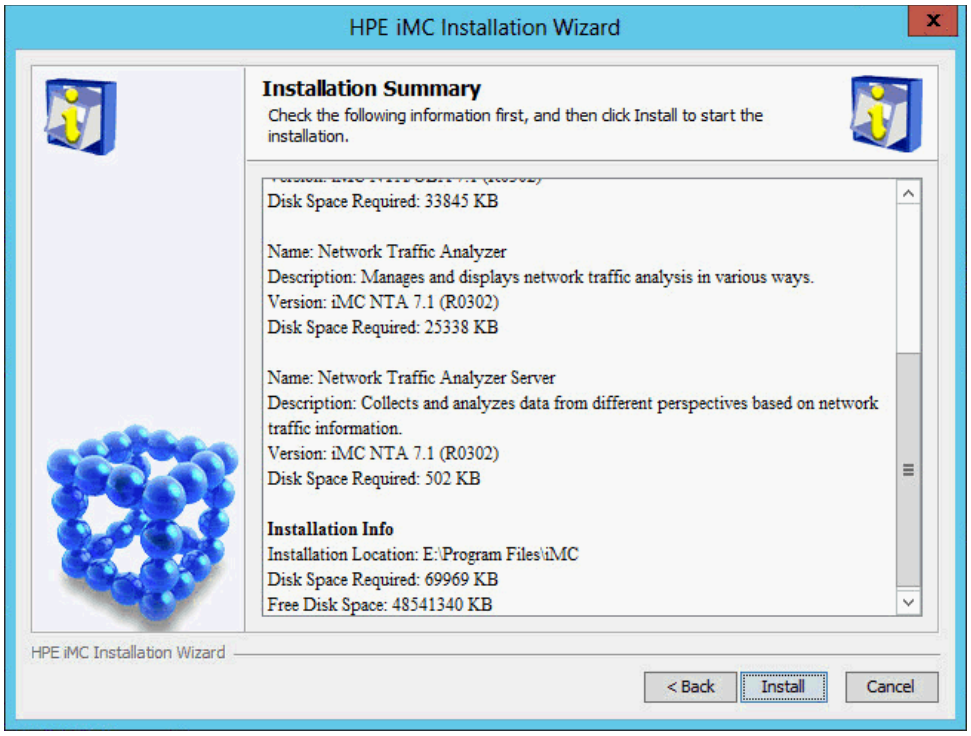
Figure 27 Deployment and Upgrade Options page



9. Select **Deploy or upgrade later**.
10. Click **Next**.

    The **Installation Summary** page opens, as shown in Figure 28.

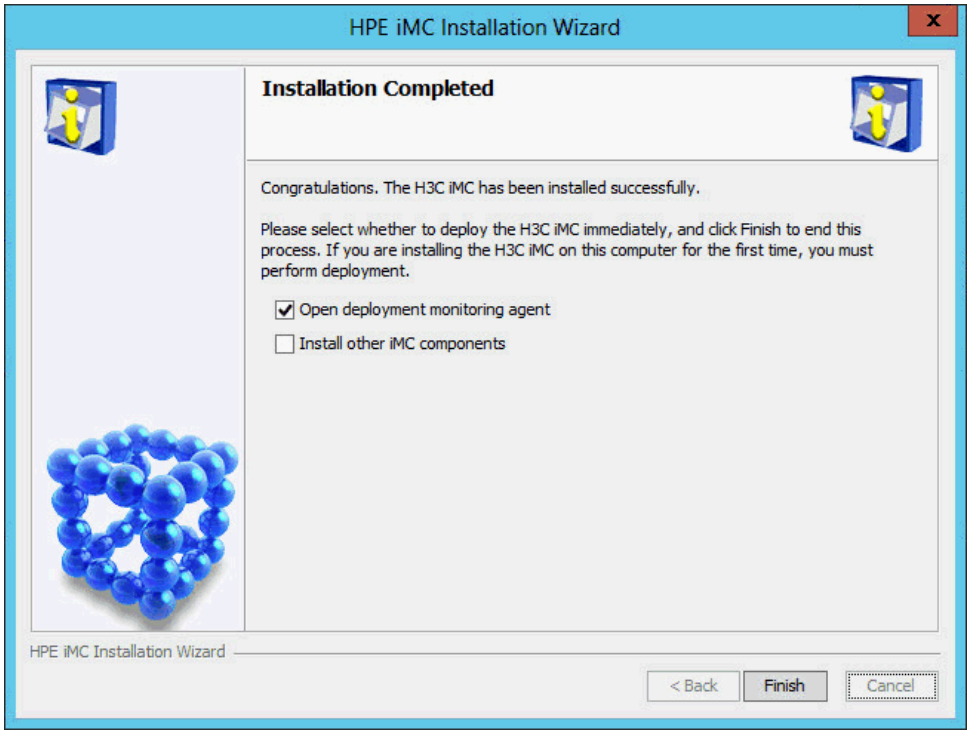
Figure 28 Installation Summary page



11. Verify the installation information, and then click **Install**.

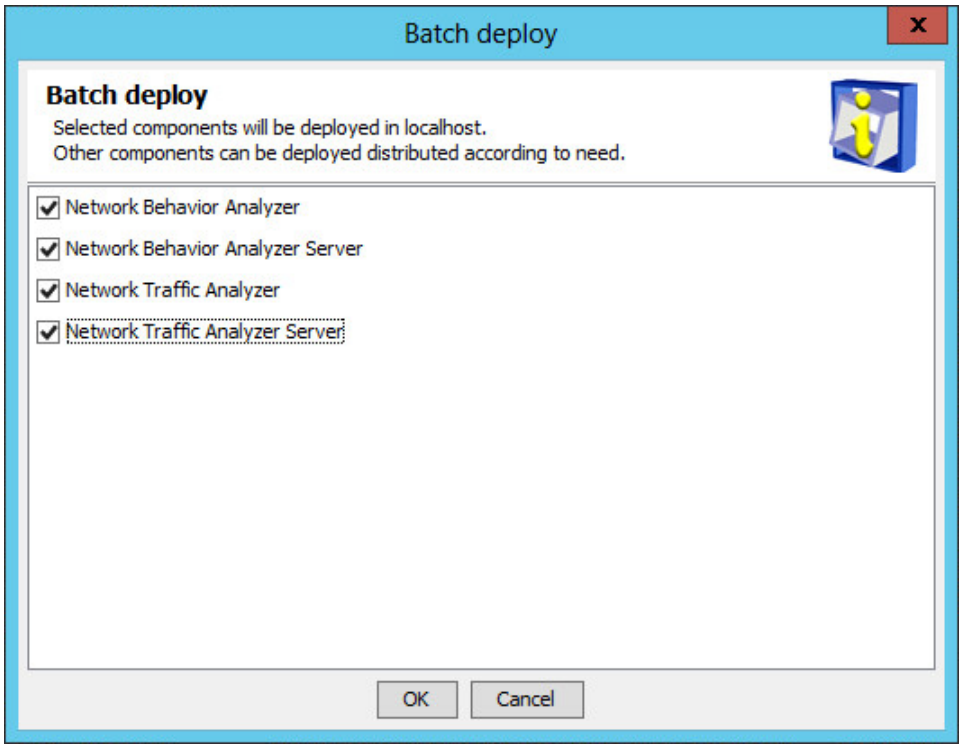
After the installation is complete, the **Installation Completed** page opens, as shown in Figure 29.

Figure 29 Installation Completed page



12. Select **Open deployment monitoring agent**, and then click **Finish**.
The **Batch deploy** dialog box opens, as shown in Figure 30.

Figure 30 Batch deploy dialog box



13. Select the NTA subcomponents you want to deploy.

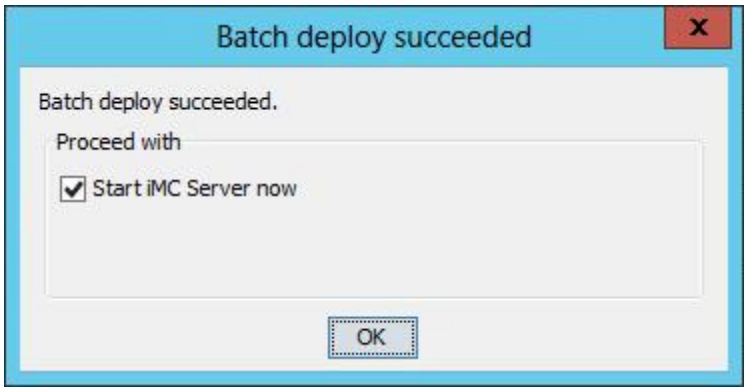
    In this example, select all the NTA subcomponents.

14. Click **OK**.

    The system starts to deploy the selected NTA subcomponents.

    After the deployment is complete, the **Batch deploy succeeded** dialog box opens, as shown in Figure 31.

    Figure 31 Batch deploy succeeded dialog box

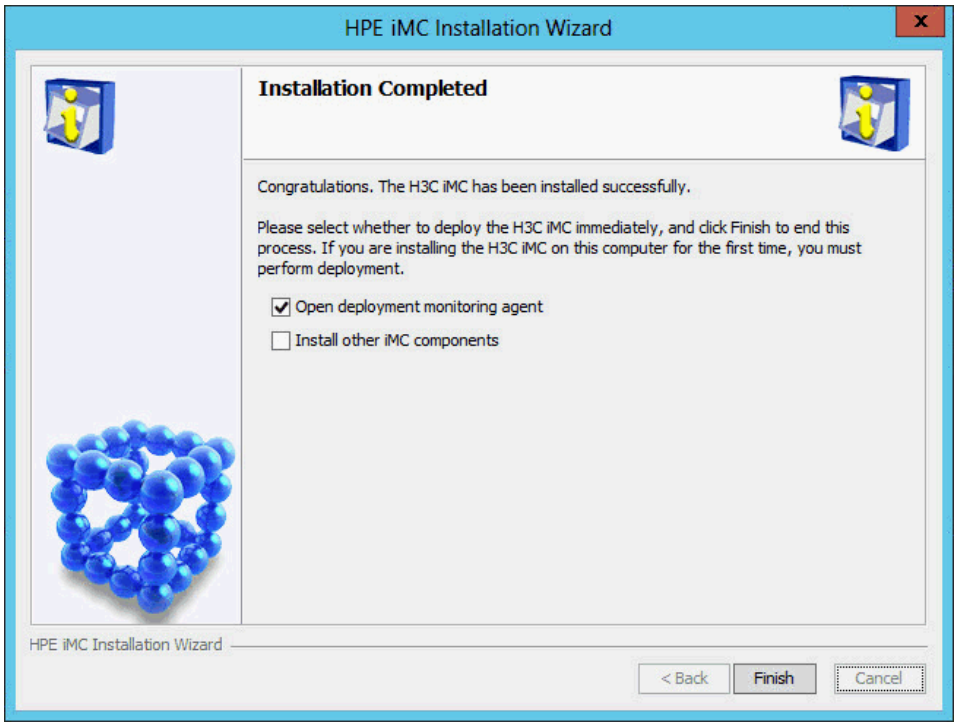


15. Configure the **Start iMC Server now** option as needed, and then click **OK**.

Installing and deploying IMC UAM

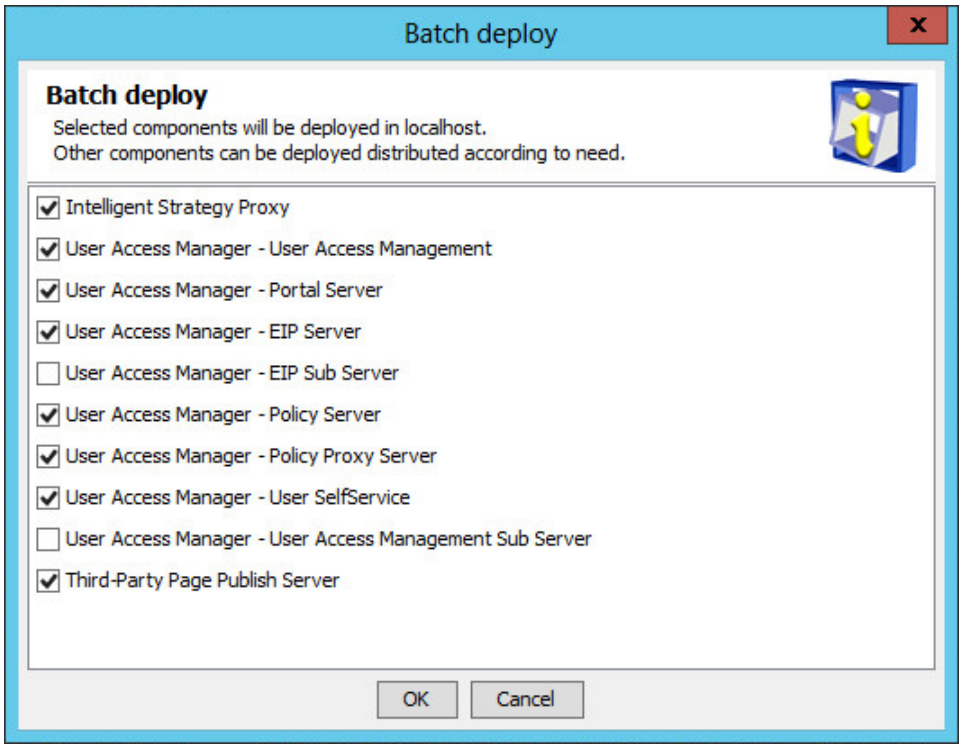
1. Install IMC UAM in the same way IMC NTA is installed. For information about the installation procedures, see "Installing and deploying IMC NTA."
2. On the **Installation Completed** page shown in Figure 32, select **Open deployment monitoring agent**, and then click **Finish**.

    Figure 32 Installation Completed page



The **Batch deploy** dialog box opens, as shown in Figure 33.

Figure 33 Batch deploy dialog box



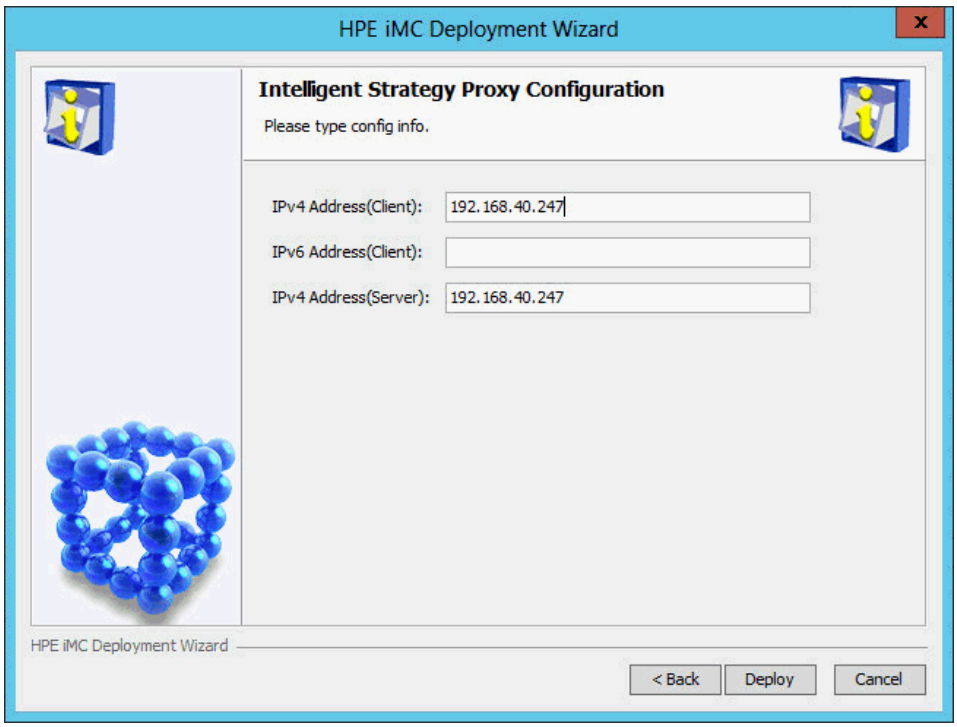
3. Select the UAM subcomponents you want to deploy, and then click **OK**.

   In this example, select all the UAM subcomponents except EIP Sub Server and User Access Management Sub Server.

   The EIP Sub Server and User Access Management Sub Server subcomponents must be deployed on subordinate servers in distributed deployment.

   The IMC deployment wizard starts and displays the **Intelligent Strategy Proxy Configuration** page, as shown in Figure 34.

Figure 34 Intelligent Strategy Proxy Configuration page

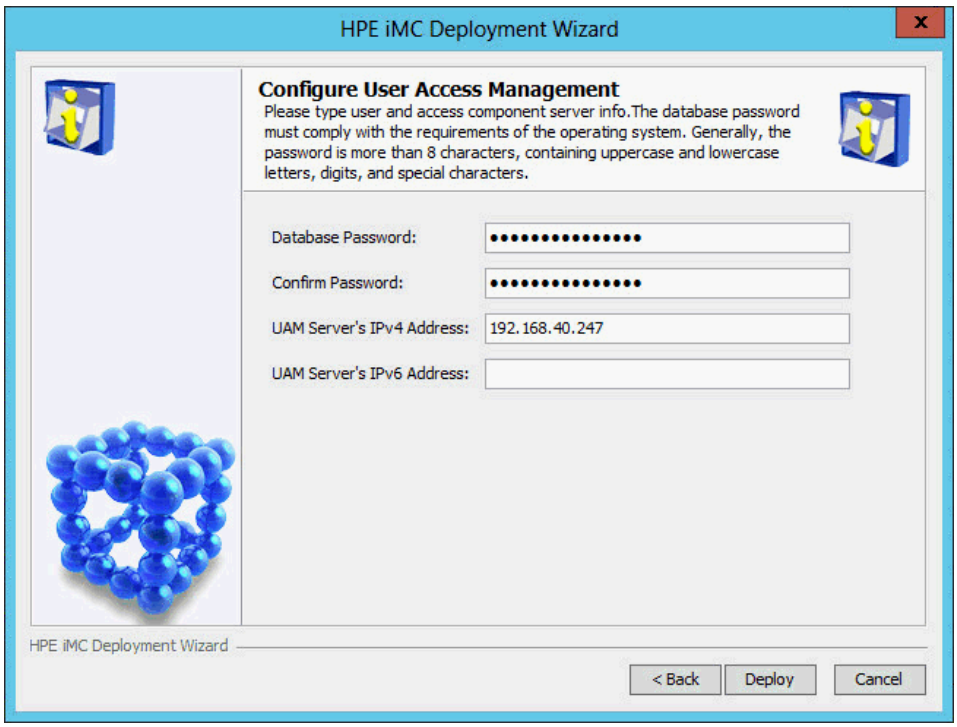


4. Configure the following parameters:
   - **IPv4 Address(Client)**—Enter the IP address of the Intelligent Strategy Proxy component. By default, this field is automatically populated with the IP address of the local host.
   - **IPv4 Address(Server)**—Enter the IP address of the User Access Management component. By default, this field is automatically populated with the IP address of the local host.

   Modify the default settings only when the local host has multiple NICs and you want to associate Intelligent Strategy Proxy and User Access Management with different NICs.
5. Click **Deploy**.

   The **Configure User Access Management** page opens, as shown in Figure 35.

Figure 35 Configure User Access Management page

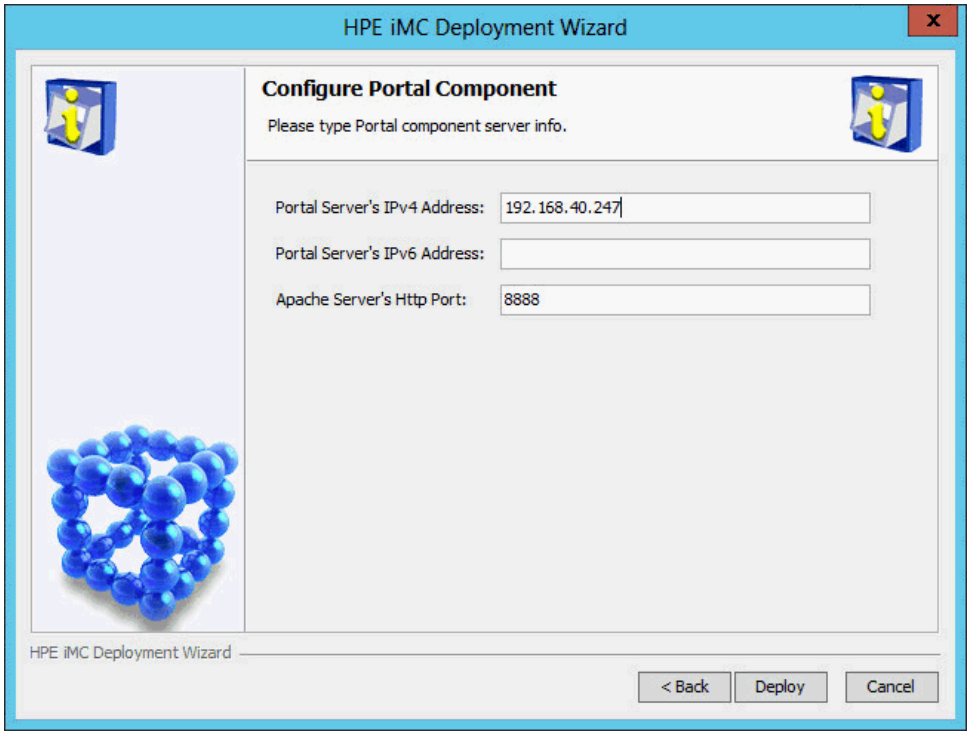


6. Configure the following parameters:
   - **Database Password/Confirm Password**—These fields are automatically populated with the password of the database superuser **sa** specified during IMC platform installation.

     If the database user password is changed after IMC platform installation, enter the new password in these fields.
   - **UAM Server's IPv4 Address**—This field is automatically populated with the IP address of the local host.
7. Click **Deploy**.

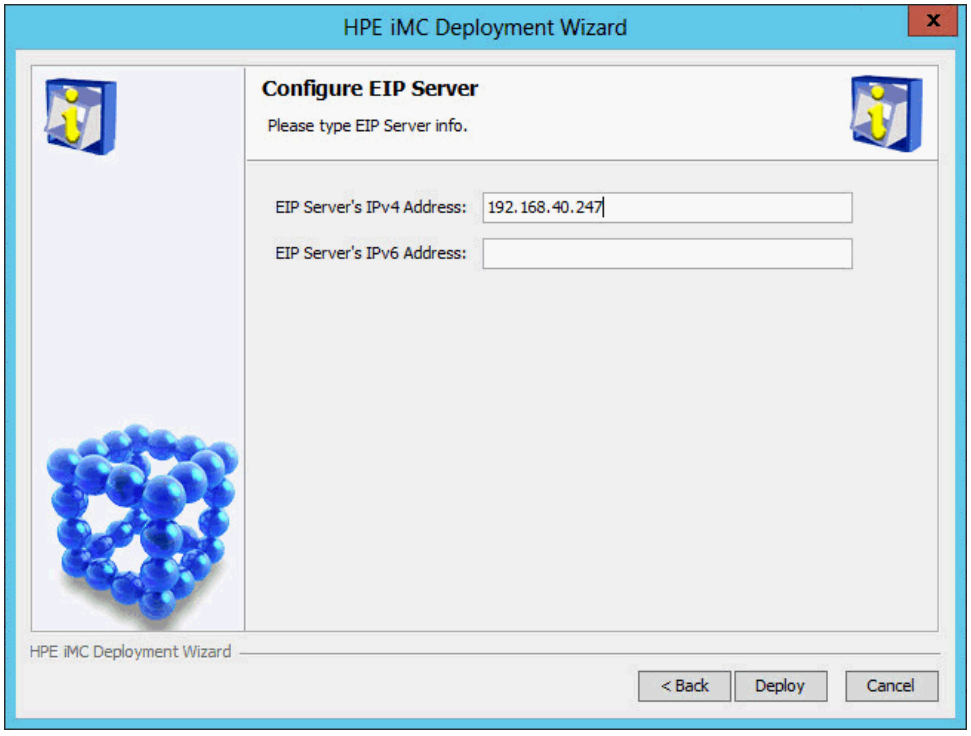
   The **Configure Portal Component** page opens, as shown in Figure 36.

Figure 36 Configure Portal Component page



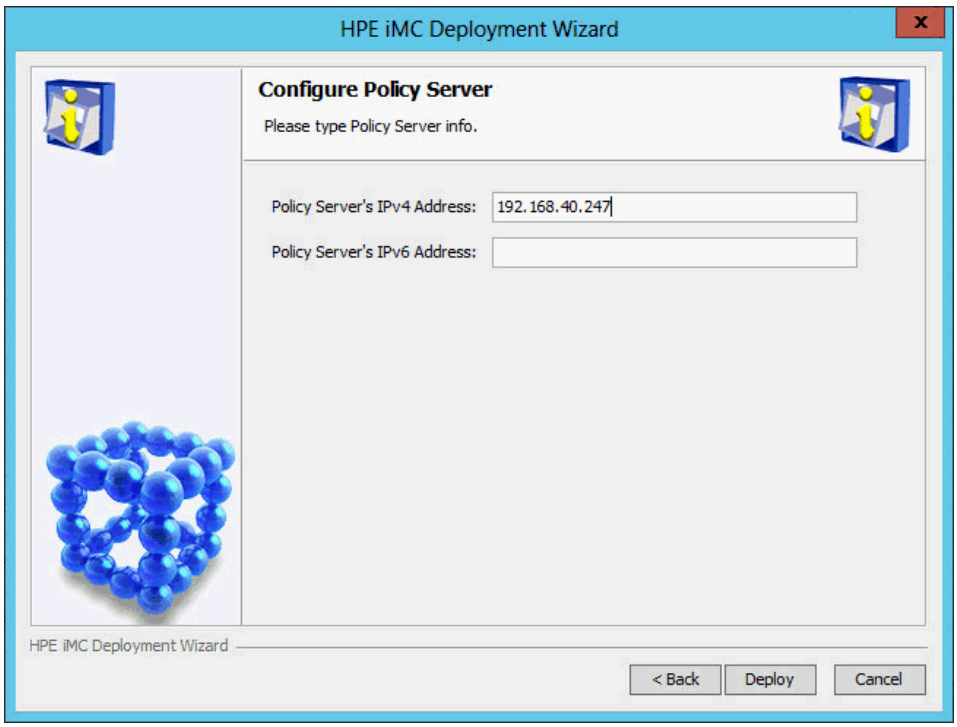
8. Use the default settings, and then click **Deploy**.
   The **Configure EIP Server** page opens, as shown in Figure 37.

Figure 37 Configure EIP Server page



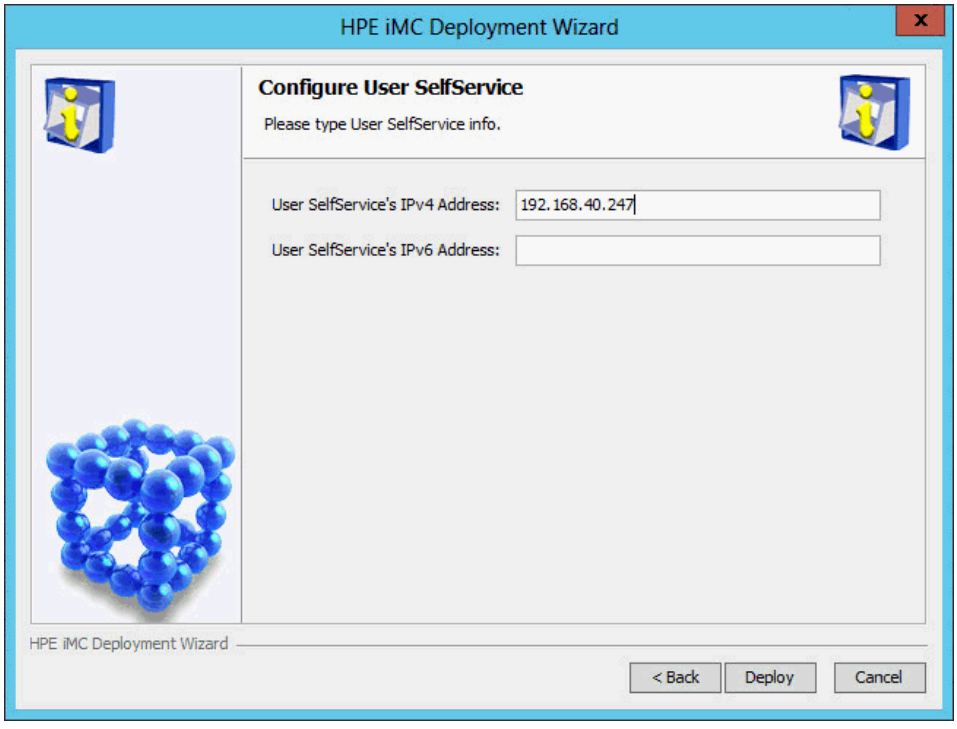
9. Use the default settings, and then click **Deploy**.
   The **Configure Policy Server** page opens, as shown in Figure 38.

Figure 38 Configure Policy Server page



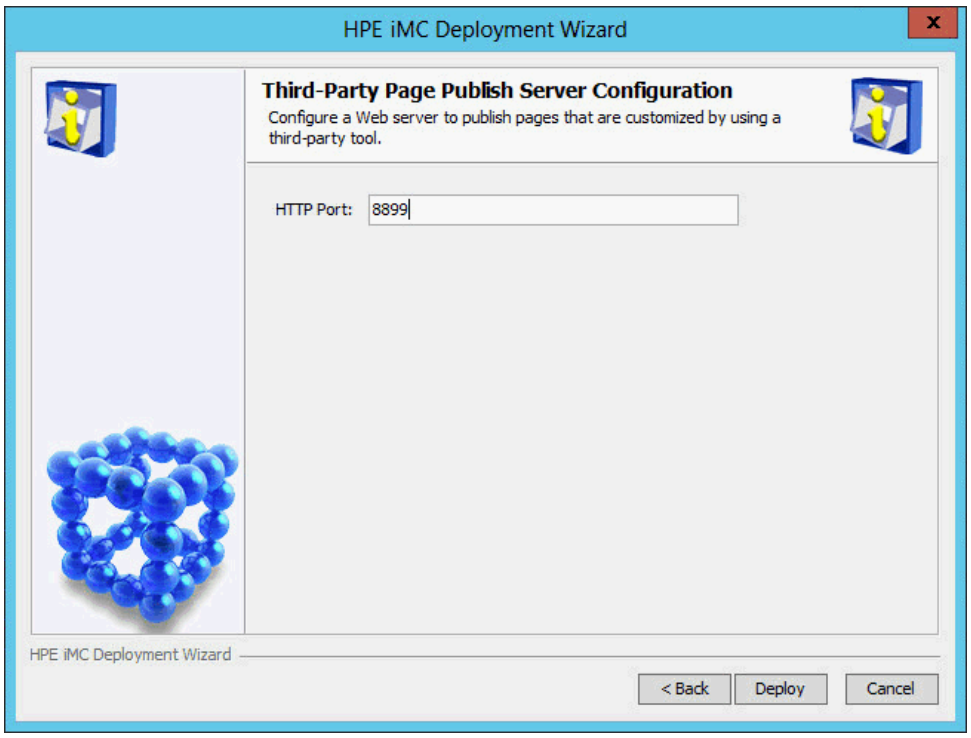
10. Use the default settings, and then click **Deploy**.
The **Configure User SelfService** page opens, as shown in Figure 39.

Figure 39 Configure User SelfService page



11. Use the default settings, and then click **Deploy**.
The **Third-Party Page Publish Server Configuration** page opens, as shown in Figure 40.

Figure 40 Third-Party Page Publish Server Configuration page

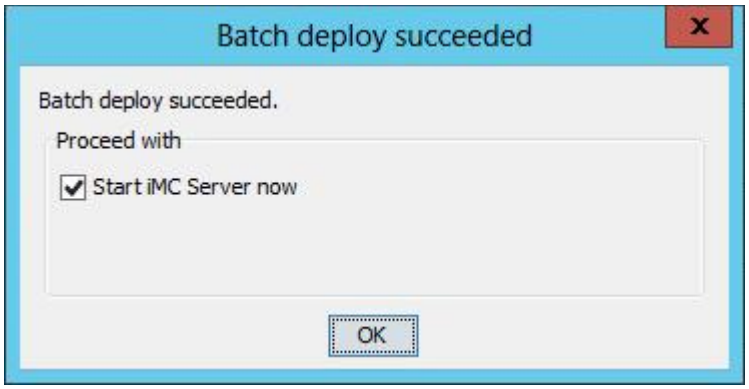


12. Use the default settings, and then click **Deploy**.

    All the selected UAM subcomponents are deployed.

    The **Batch deploy succeeded** dialog box opens, as shown in Figure 41.

    Figure 41 Batch deploy succeeded dialog box

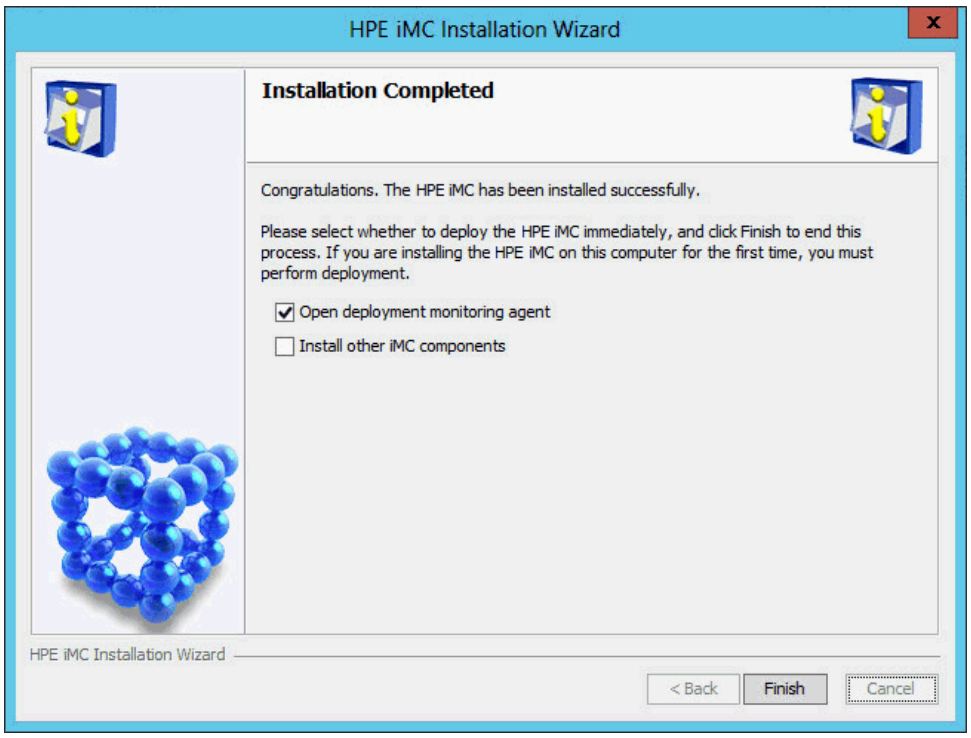


13. Configure the **Start iMC Server now** option as needed, and then click **OK**.

Installing and deploying IMC MVM

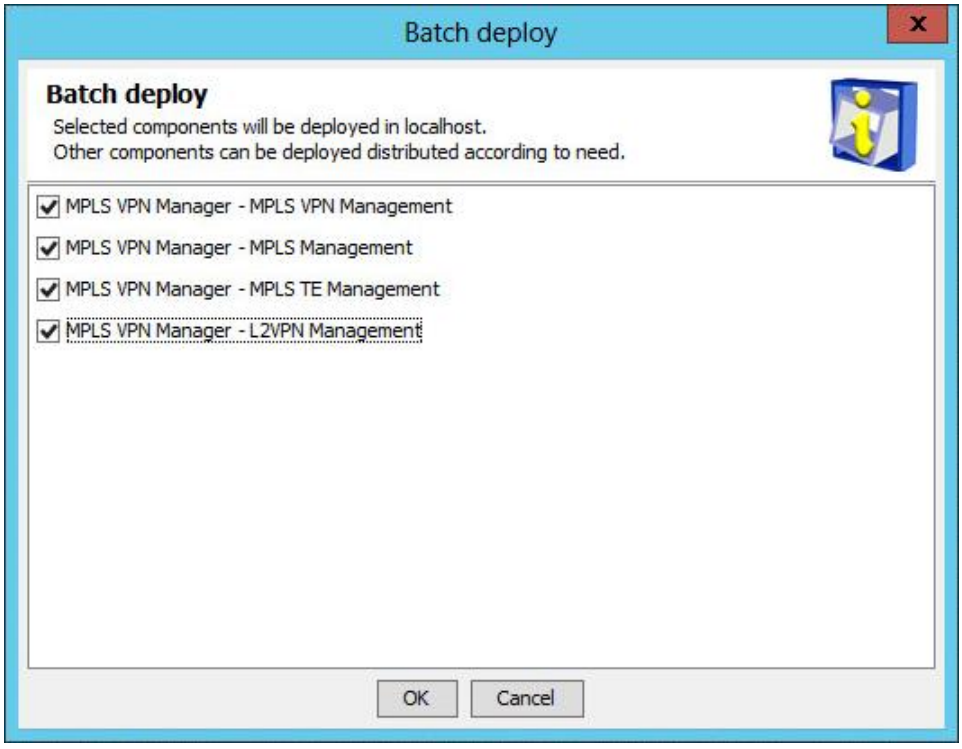
1. Install IMC MVM in the same way IMC NTA is installed. For information about the installation procedure, see "Installing and deploying IMC NTA."
2. On the **Installation Completed** page shown in Figure 42, select **Open deployment monitoring agent** and click **Finish**.

Figure 42 Installation Completed page



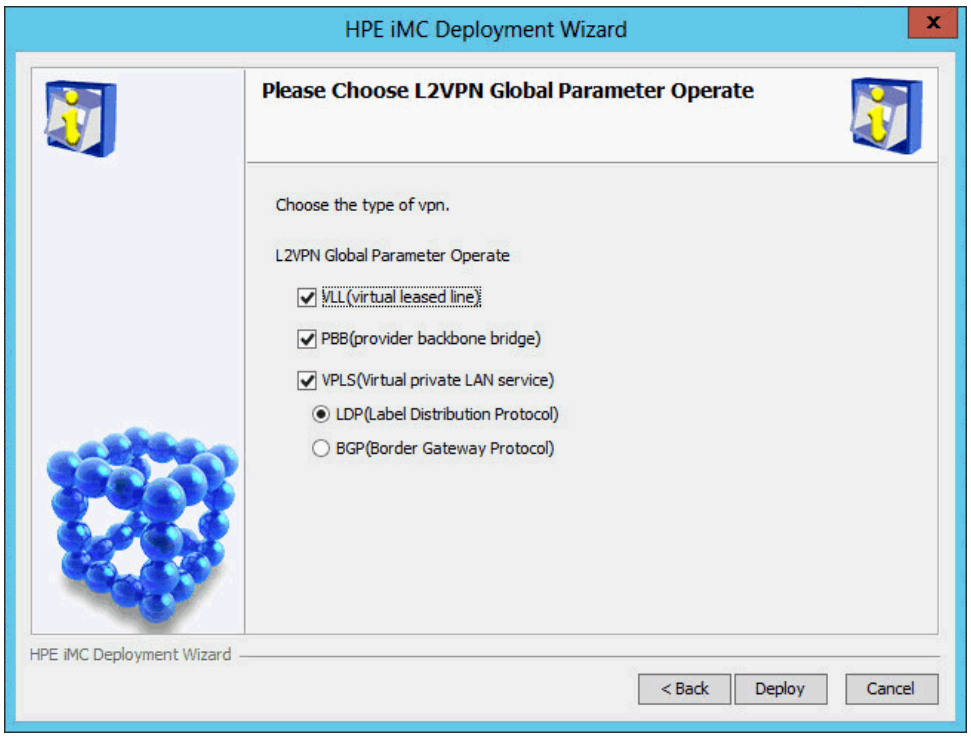
The **Batch deploy** dialog box opens, as shown in Figure 43.

Figure 43 Batch deploy dialog box



3. Select the MVM subcomponents you want to deploy, and then click **OK**.
   In this example, select all the MVM subcomponents.
   The **Please Choose L2VPN Global Parameter Operate** page opens, as shown in Figure 44.

Figure 44 Please Choose L2VPN Global Parameter Operate page



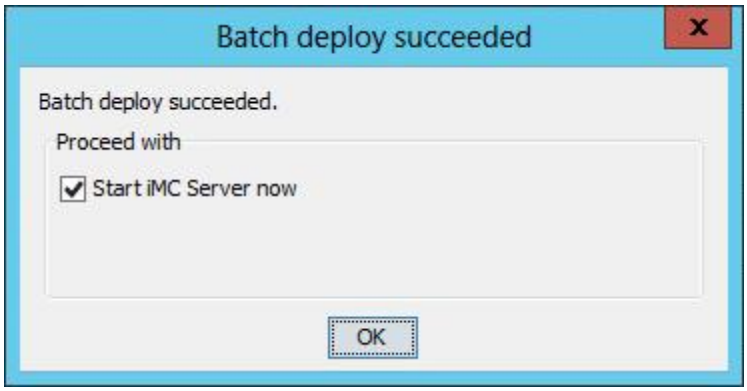
4. Configure the L2VPN parameters as needed.

   VPLS can use either LDP or BGP for signaling. When BGP is selected, the VLL and PBB options become unavailable.

5. Click **Deploy**.

   After the deployment is complete, the **Batch deploy succeeded** dialog box opens, as shown in Figure 45.

Figure 45 Batch deploy succeeded dialog box



6. Configure the **Start iMC Server now** option as needed, and then click **OK**.

Installing plug-ins

Installing DHCP plug-ins

To enable IMC to obtain endpoint names from a DHCP server, install the DHCP plug-in on the DHCP server.

Installing a DHCP plug-in on an MS DHCP server

1. On the IMC server, edit the **qvdm.conf** file to enable IMC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the**\server\conf** directory of the IMC installation path, use Notepad to open the **qvdm.conf** file.
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and close the file.
   d. Restart IMC in the Intelligent Deployment Monitoring Agent.
2. On the MS DHCP server, edit the **imf.cfg** file so that the DHCP server can communicate with IMC:
   a. Transfer the plug-in installation package **dhcp-plug-windows.zip** from the **\windows\tools** directory of the IMC installation package on the IMC server to the MS DHCP server.
   b. Decompress the installation package.
   c. Use Notepad to open the **imf.cfg** file in the **\dhcp-plug-windows\server\imf\server\conf** directory.
   d. Edit the **imf.cfg** file as follows:
      – Set the value of **IMGAddress** to the IP address of the IMC server.
      – Set the value of **IMGPort** to the IMG port number, which is 8800 by default.
   e. Save and close the file.
3. Run the **install.bat** script in the **dhcp-plug-windows** directory.
   After the installation is complete, a new service **iMC DHCP Plug** is added to the system services.
4. Start the **iMC DHCP Plug** service:
   a. Click **Start**, and then select **Administrative Tools** > **Component Services**.
   b. On the **Component Services** page, select **Services (Local)** from the navigation tree.
   c. On the **Services (Local)** list, right-click the **iMC DHCP Plug** service and select **Start**.

To uninstall the DHCP plug-in, run the **uninstall.bat** script in the **dhcp-plug-windows** directory.

IMPORTANT:

Do not delete the directory where the plug-in installation package **dhcp-plug-windows.zip** is decompressed. If you delete the directory, you cannot uninstall the DHCP plug-in completely.

Installing a DHCP plug-in on a Linux DHCP server

1. On the IMC server, edit the **qvdm.conf** file to enable IMC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the **\server\conf** directory of the IMC installation path, use Notepad to open the **qvdm.conf** file.
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and close the file.
   d. Restart IMC in the Intelligent Deployment Monitoring Agent.
2. On the Linux DHCP server, edit the **imf.cfg** file so that the DHCP server can communicate with IMC.
   a. Transfer the plug-in installation package **dhcp-plug-linux.zip** from the **tools** directory of the IMC installation package on the IMC server to the Linux DHCP server.
   b. Decompress the installation package.
   c. Use the vi editor to open the **imf.cfg** file in the **/dhcp-plug-linux/server/imf/server/conf/** directory.
      ```
      vi imf.cfg
      ```
   d. Edit the **imf.cfg** file:
      - Set the value of **IMGAddress** to the IP address of the IMC server.
      - Set the value of **IMGPort** to the IMG port number, which is 8800 by default.
   e. Save and close the file.
3. Set the path of the **dhcpd.leases** file, which stores DHCP address allocation information:
   a. Determine the path of the **dhcpd.leases** file. The default path is **/var/lib/dhcp**.
   b. Use the vi editor to open the **qvdm.conf** file in the **/dhcp-plug-linux/server/imf/server/conf/** directory, and then add the following line to the file:
      ```
      DhcpPlugIpAllocPath=<file path>/dhcpd.leases
      ```
      Replace *<file path>* with the path of the **dhcpd.leases** file.
   c. Save and close the file.
4. Run the **install.sh** script in the **dhcp-plug-linux** directory.

After the installation is complete, the system automatically starts the **dhcp-plug** service and adds the service to the system services.

To manually start the **dhcp-plug** service, execute the **service dhcp-plug start** command.

To stop the **dhcp-plug** service, execute the **service dhcp-plug stop** command.

To uninstall the DHCP plug-in, run the **uninstall.sh** script in the **dhcp-plug-linux** directory of the plug-in installation package.

IMPORTANT:

Do not delete the directory where the plug-in installation package **dhcp-plug-linux.zip** is decompressed. If you delete the directory, you cannot uninstall the DHCP plug-in completely.

Installing VRM plug-ins

Virtual Resource Management (VRM) is a subcomponent of the IMC platform to manage virtual networks. VRM plug-ins include VRM Windows agents and VRM Linux agents.

Installing a VRM Windows agent

CAUTION:

VRM Windows agents can be installed on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. A Windows server can have only one VRM Windows agent.

Install VRM Windows agents for IMC to manage Microsoft Hyper-V servers on the network.

When the Microsoft Hyper-V servers are managed by Microsoft VMM servers, install VRM Windows agents on Microsoft VMM servers as a best practice. A VRM Windows agent can manage up to 50 Hyper-V servers. If more than 50 Hyper-V servers exist on the network, install additional VRM Windows agents.

Before you run the VRM agent installer, make sure the .NET Framework 4.5 and PowerShell 3.0 applications are already installed on the server. The applications are available on the Microsoft website.

To install a VRM Windows agent:

1. Decompress the **vrm-plug-windows.zip** file in the **tools** directory of the IMC installation package.
2. Save the decompressed files to a local directory on the server to install the VRM agent.
3. Run **Register.bat** in the **vrm-plug-windows** directory.

   The installation program verifies installation of .NET Framework 4.5 and PowerShell 3.0. Then, it installs the VRM Windows agent and automatically closes after the installation is complete.

   Do not delete the **vrm-plug-windows** directory or the files in the directory after installation. It is the service registration path.
4. Use Notepad to open the **imf.cfg** file in the **\vrm-plug-windows\serverimf\server\conf** directory.
5. Edit the **imf.cfg** file:
   - Set the value of **IMGAddress** to the IP address of the IMC server.
   - Set the value of **IMGPort** to the IMG port number, which is 8800 by default.
6. Save and close the file.
7. Start the **iMC VRM Agent** service:
   a. Click **Start** and select **Administrative Tools** > **Component Services**.
   b. On the **Component Services** page, select **Services (Local)** from the navigation tree.
   c. On the **Services (Local)** list, right-click **iMC VRM Agent** and select **Start**.

If a VRM Windows agent was previously installed, run the **UnRegister.bat** script in the **vrm-plug-windows** directory to uninstall the VRM Windows agent first.

Installing a VRM Linux agent

VRM uses a Linux agent to manage KVM virtual networks for Red Hat, Ubuntu, Fedora, and Citrix XenServer virtual networks. With the agent, VRM can obtain virtual network data of KVM and Xen, and set the virtual network parameters. Each VRM Linux agent can manage up to 200 physical KVM and Xen servers. You can install multiple VRM Linux agents as needed.

VRM Linux agents can run on Red Hat Linux 6.0 or later versions.

Installation prerequisites

A VRM Linux agent is a 32-bit program and applies to 32-bit and 64-bit Red Hat Linux.

To install the VRM Linux agent on 32-bit Red Hat Enterprise Linux, make sure the Linux supports

the Web server function and has the **sshpass-1.05-1.el5.rf.i386.rpm** software package installed.

To install the VRM Linux agent on 64-bit Red Hat Enterprise Linux, first install the following 32-bit software packages:

- compat-libcap1-1.10-1.i686.rpm
- glibc-2.12-1.107.el6.i686.rpm
- keyutils-libs-1.4-4.el6.i686.rpm
- krb5-libs-1.10.3-10.el6.i686.rpm
- libaio-0.3.107-10.el6.i686.rpm
- libcom_err-1.41.12-14.el6.i686.rpm
- libgcc-4.4.7-3.el6.i686.rpm
- libidn-1.18-2.el6.i686.rpm
- libssh2-1.4.2-1.el6.i686.rpm
- libstdc++-4.4.7-3.el6.i686.rpm
- nspr-4.9.2-1.el6.i686.rpm
- nss-3.14.0.0-12.el6.i686.rpm
- nss-softokn-freebl-3.12.9-11.el6.i686.rpm
- nss-util-3.14.0.0-2.el6.i686.rpm
- openldap-2.4.23-31.el6.i686.rpm
- sshpass-1.05-1.el6.rf.i686.rpm
- openssl-1.0.0-27.el6.i686.rpm

This section uses Red Hat Enterprise Linux 6.4 as an example. For other Linux 6 versions, the package names might include different versions.

To install the required software packages:

1. Log in to Red Hat Enterprise Linux as **root**.
2. Insert the Linux installation disk into the CD-ROM drive and enter the directory where packages are saved.
3. Save the packages to a local directory, and then download **sshpass-1.05-1.el6.rf.i686.rpm** from the Internet.
4. Launch a terminal window, and then enter the local directory where the packages are saved.
5. Install packages, where xxx indicates the package name.

   ```
   rpm -i --nodeps xxx
   ```

Installation procedure

1. Decompress the **vrm-plug-linux.zip** file in the **tools** directory of the IMC installation package.
2. Save the decompressed files to a local directory.
3. Run the **install.sh** script in the **vrm-plug-linux** folder.
4. Enter the IP address of the IMC server. The default setting is **localhost**.
5. Verify that the installation is successful.

   ```
   ps -ef | grep imcvnmagent
   ```

   When the agent is successfully installed, the **imcvnmagent** process is running.

If a VRM Linux agent was previously installed, run the **uninstall.sh** script in the **vrm-plug-linux** directory to uninstall the VRM Linux agent first.

Installing LLDP plug-ins

When the VRM component is deployed, you must install an LLDP plug-in for topology calculation.

An LLDP plug-in contains the following packages:

- lldp-agent-redhat.zip
- lldp-agent-ubuntu.zip
- lldp-agent-windows.zip

Packages **lldp-agent-redhat.zip** and **lldp-agent-ubuntu.zip** apply to KVM servers and the **lldp-agent-windows.zip** package applies to Microsoft Hyper-V servers.

Before you install the LLDP plug-ins, save and decompress the packages to the target servers.

Make sure the **lldp-agent-windows.zip** package is saved to a non-system disk.

IMPORTANT:

Do not delete the folder where the decompressed installation packages are located after the LLDP agent installation. If you delete the folder, the LLDP plug-ins cannot be uninstalled completely.

Installing an LLDP Windows agent

LLDP Windows agents support 32-bit and 64-bit Windows operating systems.

To install and configure an LLDP Windows agent:

1. Run the **install.bat** script in the LLDP Windows agent installation path.

   The LLDP Windows agent is installed.
2. Configure the LLDP Windows agent.

   The LLDP Windows agent supports either LLDP or CDP, but not both at the same time. By default, the agent supports LLDP.

   To enable the LLDP agent to support CDP and set the packet sending interval:

   a. Open the **lldpagent.conf** file in the **\Program Files\lldpAgent** directory on the Windows system disk.
   b. Delete the pound sign (#) from the string **#Agent=CDP**.
   c. Delete the pound sign (#) from the string **#INTERVAL=10**, and then set the interval as needed.

      The default setting is 300 seconds.
   d. Save and close the file.
3. Restart the **lldp-agent** service.

Installing an LLDP Linux agent

The installation procedures for packages **lldp-agent-redhat.zip** and **lldp-agent-ubuntu.zip** are the same. The following information describes the installation procedure for the **lldp-agent-redhat.zip** package.

An LLDP Linux agent must be installed on 64-bit Linux, including Red Hat 5.5, Ubuntu 11.0, and their later versions.

To install and configure an LLDP Linux agent:

1. Set the executable permission to the **install.sh** script, and then run the script in the LLDP Linux agent installation path.

The LLDP Linux agent is installed.

2. Configure the LLDP Linux agent.

   The LLDP Linux agent supports either LLDP or CDP, but not both at the same time. By default, the agent supports LLDP.

   To enable the LLDP agent to support CDP and set the packet sending interval:

   a. Open the **lldpagent.conf** file in the **conf** directory.

      ```
      vi lldpagent.conf
      ```

   b. Delete the pound sign (#) from the string **#Agent=CDP**.

   c. Delete the pound sign (#) from the string **#INTERVAL=10**, and then set the interval as needed.

      The default setting is 300 seconds.

   d. Save and close the file.

3. Restart the **lldp-agent** service.

   ```
   service lldp-agent restart
   ```

Accessing IMC

IMC is a browser-based management tool accessible from PCs. IMC of the Enterprise edition is also accessible from a mobile device.

Hardware, software, and browser requirements

Table 14 lists the hardware, software, and browser requirements for accessing IMC.

Table 14 Requirements for accessing IMC from a PC

OS	Hardware and software	Browser version	Browser setting requirements
Windows	• Recommended resolution: 1280 pixels in width. • JRE 1.6.0_update27 or later is installed.	• IE 10 or 11 • Firefox 30 or later • Chrome 35 or later	• Turn off the popup blocker. • Enable Cookies. • Add IMC as a trusted site.

Accessing IMC from a PC

Accessing IMC

1. Enter a Web address in either of the following formats in the address bar of the browser:
   - http://*ip-address*:*port*/imc
   - https://*ip-address*:*port*/imc

   In the Web address, *ip-address* is the IP address of the IMC server, and *port* is the HTTP or HTTPS port number used by IMC. By default, IMC uses HTTP port 8080 and HTTPS port 8443.

   The IMC login page opens.
2. Enter the user name and password, and then click **Login**.

   By default, the IMC superuser name and password are **admin** and **admin**.

IMPORTANT:

- For security purposes, change the password of the IMC superuser **admin** immediately after the first login.
- When you attempt to access IMC using HTTPS, a certificate error message might be displayed. For more information, see *HPE Getting Started Guide*.

Accessing the UAM self-service center

When the UAM User SelfService subcomponent is deployed, access the user self-service center by entering a Web address in either of the following formats in the browser's address bar:

- http://*ip-address*:*port*
- http://*ip-address*:*port*/selfservice

In the Web address, *ip-address* is the IP address of the IMC server where the UAM User SelfService subcomponent is deployed and *port* is the HTTP port number used by IMC.

Accessing the SOM service desk

When the SOM Service Desk subcomponent is deployed, access the SOM service desk by entering the following Web address in the browser's address bar:

http://*ip-address*:*port*/servicedesk

In the Web address, *ip-address* is the IP address of the IMC server where the SOM service desk is deployed and *port* is the HTTP port number used by IMC.

Accessing IMC from a mobile device

1. Open the browser on the mobile device.
2. Enter http://i*p-address*:*port*/imc in the browser's address bar.

   In the Web address*, ip-address* is the IP address of the IMC server and *port* is the HTTP port number of IMC. The default HTTP port number is 8080.

   The IMC login page opens.
3. Enter the user name and the password in **Operator** and **Password** fields.

   The operator must have been added to IMC. The operator account used for login must belong to an operator group that has the **iMC Platform - Resource Management > Mobile Client Access** operation privilege.
4. Select **Mobile** or **PC** as needed.

   The PC version of IMC requires complex operations and provides all functions. The mobile version of IMC allows you to perform the following operations:

   - View information about faulty devices and interfaces.
   - Query devices.
   - View device alarms.
   - Receive realtime alarms.
   - Test device reachability by using a **ping** or **tracert** command.
   - View custom views and device views.
5. Click **Login**.

Securing IMC

As a best practice, perform the following tasks to secure IMC:

- Change the password of the IMC superuser **admin** immediately after the first login.
- Tie the administrative accounts to a central AAA server through LDAP or RADIUS.
- Retain one administrative account (not named **admin**) with a local password to recover from loss of access to the AAA server.
- Enable the verification code feature on the IMC login page.

Displaying a user agreement

A user agreement on the IMC login page informs operators of the rights and obligations for an IMC login. To log in to IMC, operators must accept terms of the user agreement.

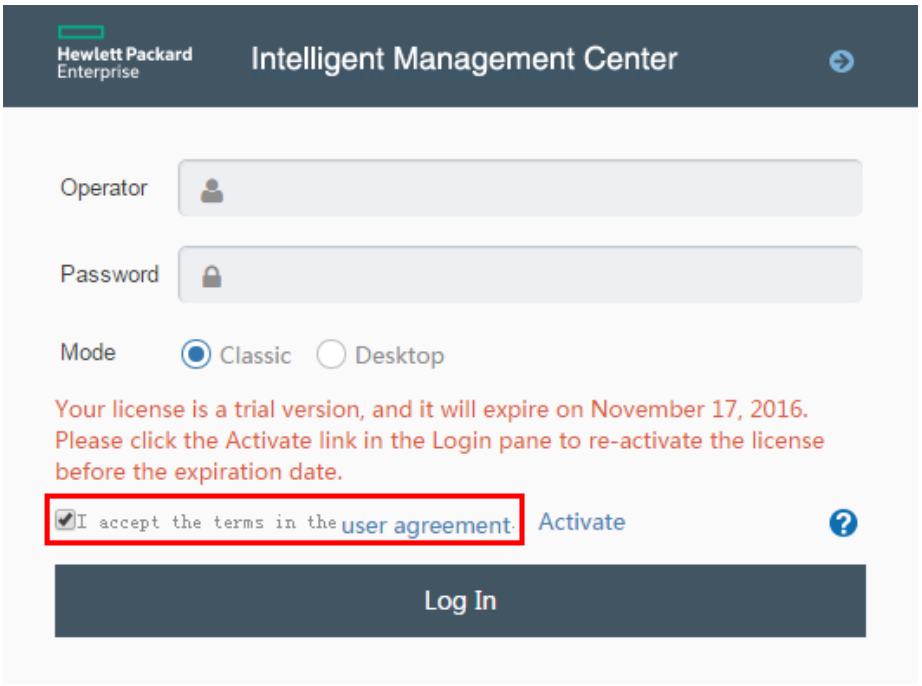
To display a user agreement on the IMC login page:

1. On the IMC server, enter the **\client\conf** directory of the IMC installation path (**/client/conf** on Linux).

2. Use Notepad (or vi on Linux) to open the **commonCfg.properties** file.
3. Change the value of the **enableTerms** parameter to **true**.
4. Save and close the **commonCfg.properties** file.
5. Prepare a user agreement in HTML format named **terms.html**.
6. Save the **terms.html** file to the **\client\web\apps\imc** directory of the IMC installation path (**/client/web/apps/imc** on Linux).
7. Display the IMC login page.

   A **User agreement** link is displayed, as shown in Figure 46. Operators can click the link to view terms of the user agreement.

Figure 46 Viewing the user agreement on the login page



Upgrading IMC

The following example describes how to upgrade the IMC platform. Upgrade IMC service components in the same way the IMC platform is upgraded.

Preparing for the upgrade

Before you upgrade the IMC platform, complete the following tasks:

- Obtain the upgrade packages for the IMC platform and all the deployed service components. After the IMC platform upgrade, upgrade all the service components to match the new IMC platform version.
- Back up the IMC database files using DBMan manual backup (see "Backing up and restoring the database"). Stop all IMC processes, and then save the IMC installation directory to a backup path. If the upgrade fails, you can use these files to restore IMC.

Upgrading IMC

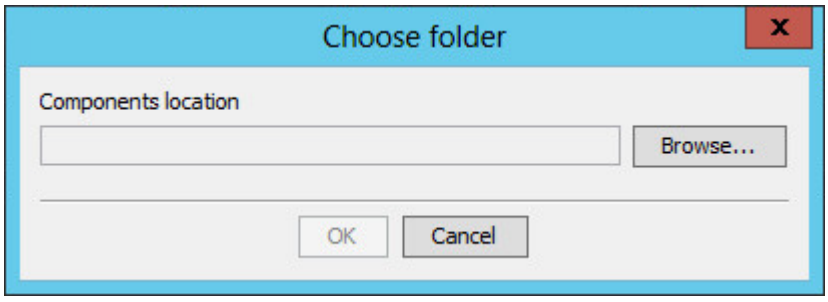
CAUTION:

- Make sure you have compatible upgrade packages for all deployed IMC components. If components do not have upgraded packages, they cannot be upgraded after the IMC platform upgrade and might become invalid.
- Do not upgrade IMC by running the **install\install.bat** script in the IMC installation path.
- If the reporting function of an upgraded service component relies on the Report Management component, upgrade the Report Management component to match the service component version.

Upgrading the IMC platform

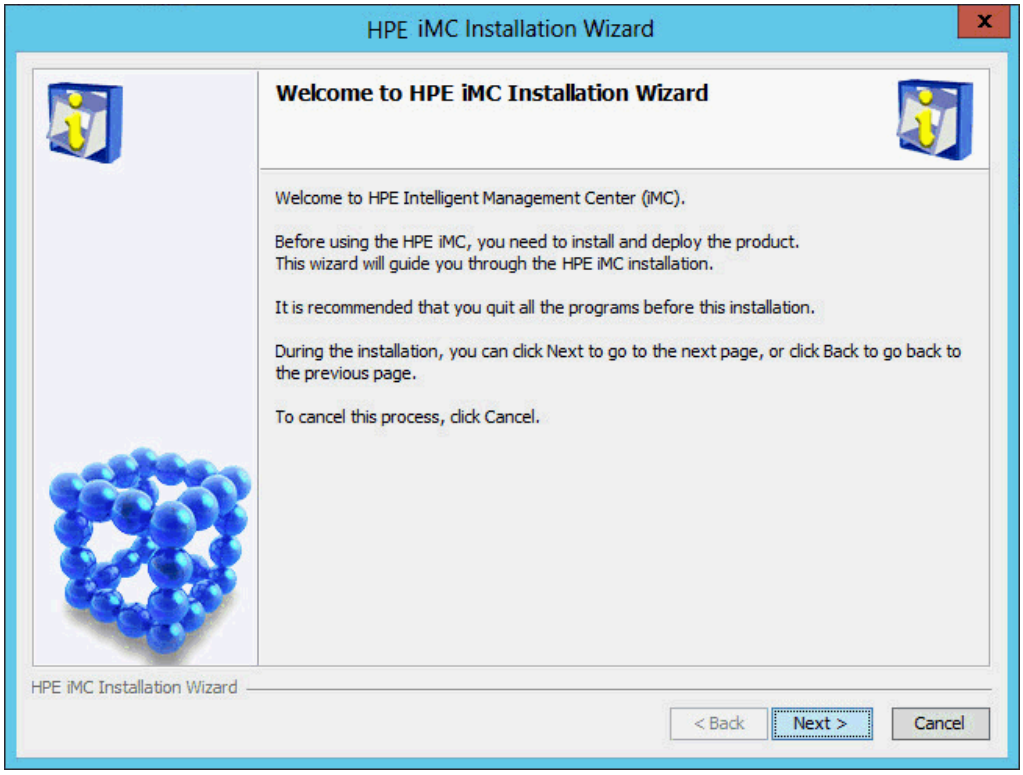
1. Start the Intelligent Deployment Monitoring Agent, and then click **Install** on the **Monitor** tab.
   The **Choose folder** dialog box opens, as shown in Figure 47.

   Figure 47 Choose folder dialog box

2. Click **Browse**, and then select the **install\components** directory in the upgrade package.
3. Click **OK**.
   The IMC installation wizard opens, as shown in Figure 48.

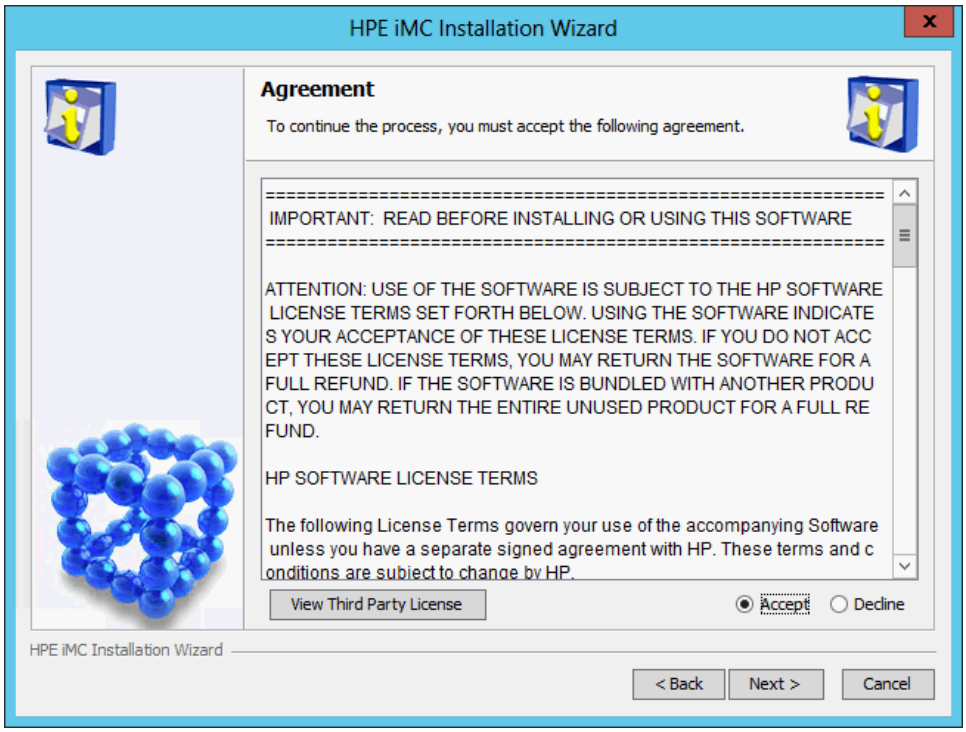
Figure 48 IMC installation wizard



4. Click **Next**.

   The **Agreement** page opens, as shown in Figure 49.

Figure 49 Agreement page



5. Read the license agreement, select **Accept**, and then click **Next**.

The **Upgrade Common Components** dialog box opens, as shown in Figure 50.

NOTE:

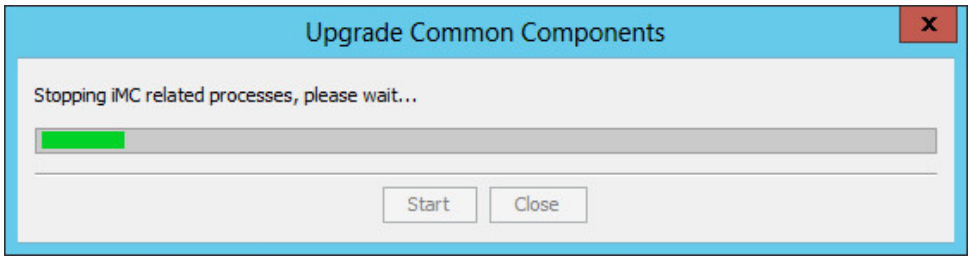
Common components include the Intelligent Deployment Monitoring Agent and common background services.

Figure 50 Upgrade Common Components dialog box

6. Click **OK**.

   The system automatically upgrades common components and displays the upgrade progress, as shown in Figure 51.

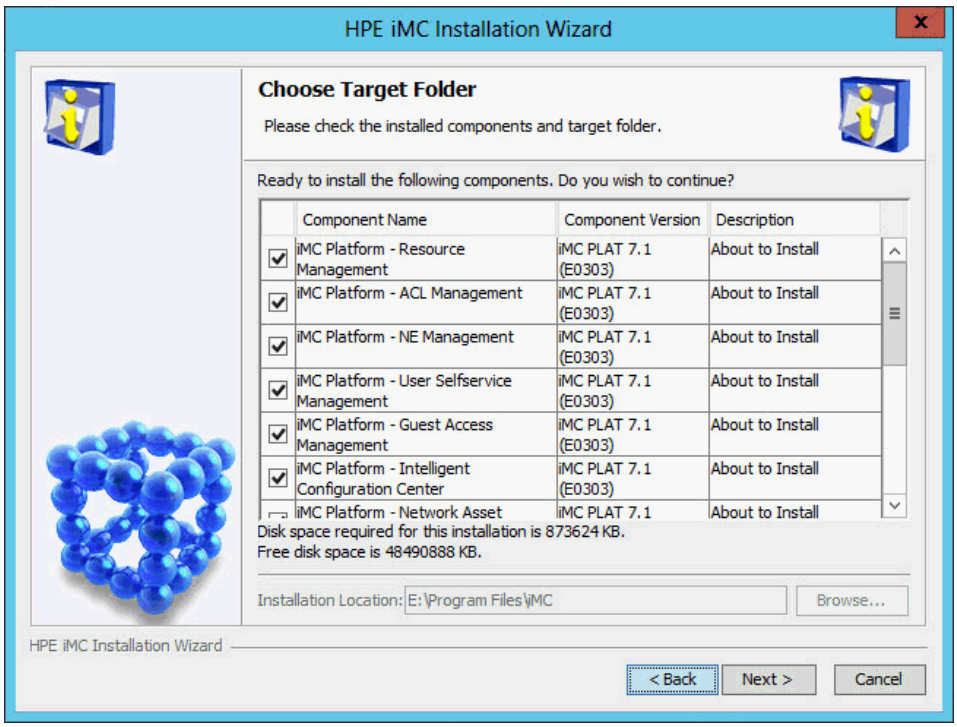
Figure 51 Upgrading common components



After the common components are upgraded, the **Choose Target Folder** page opens, as shown in Figure 52.

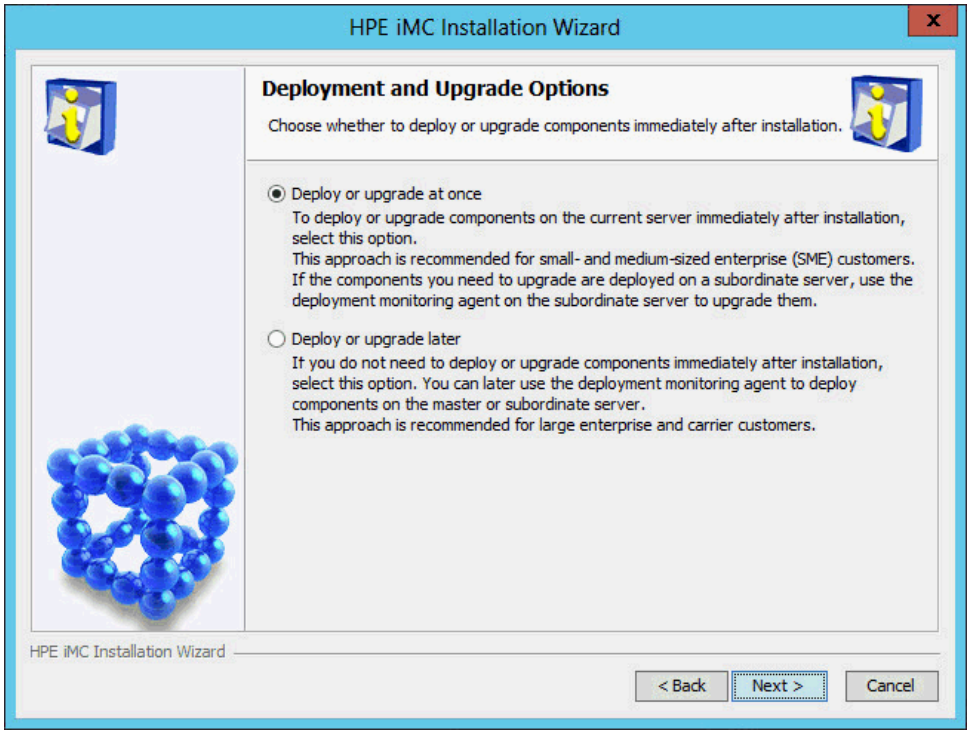
The page displays the components whose upgrade packages are to be installed and the installation location.

Figure 52 Choose Target Folder page



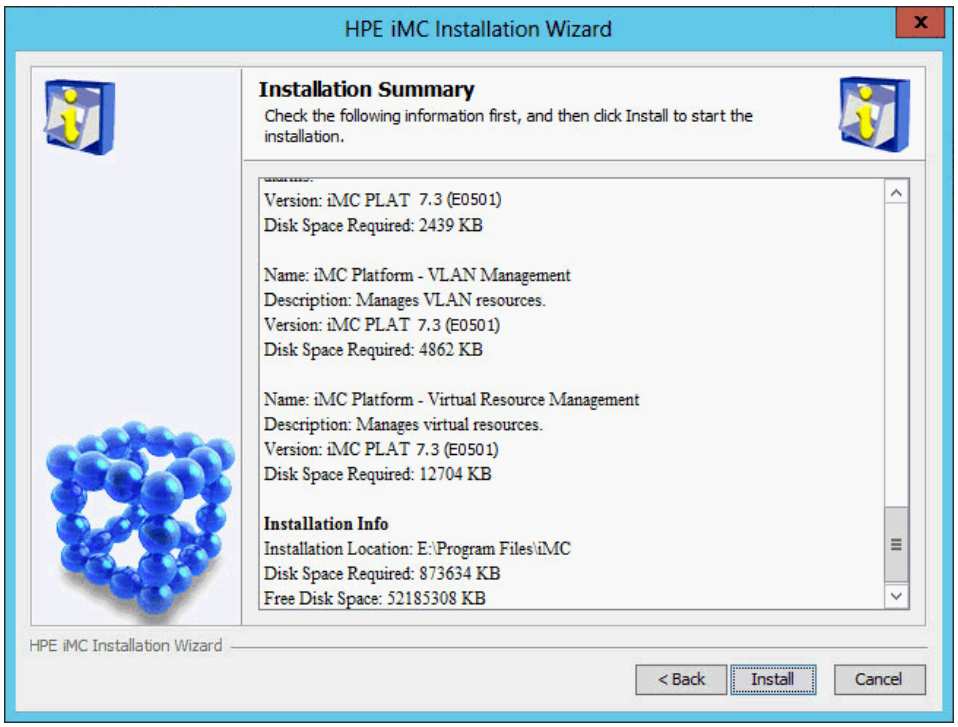
7. Verify the information, and then click **Next**.
   The **Deployment and Upgrade Options** page opens, as shown in Figure 53.

Figure 53 Deployment and Upgrade Options page



8. Select **Deploy or upgrade at once**, and then click **Next**.
   The **Installation Summary** page opens, as shown in Figure 54.

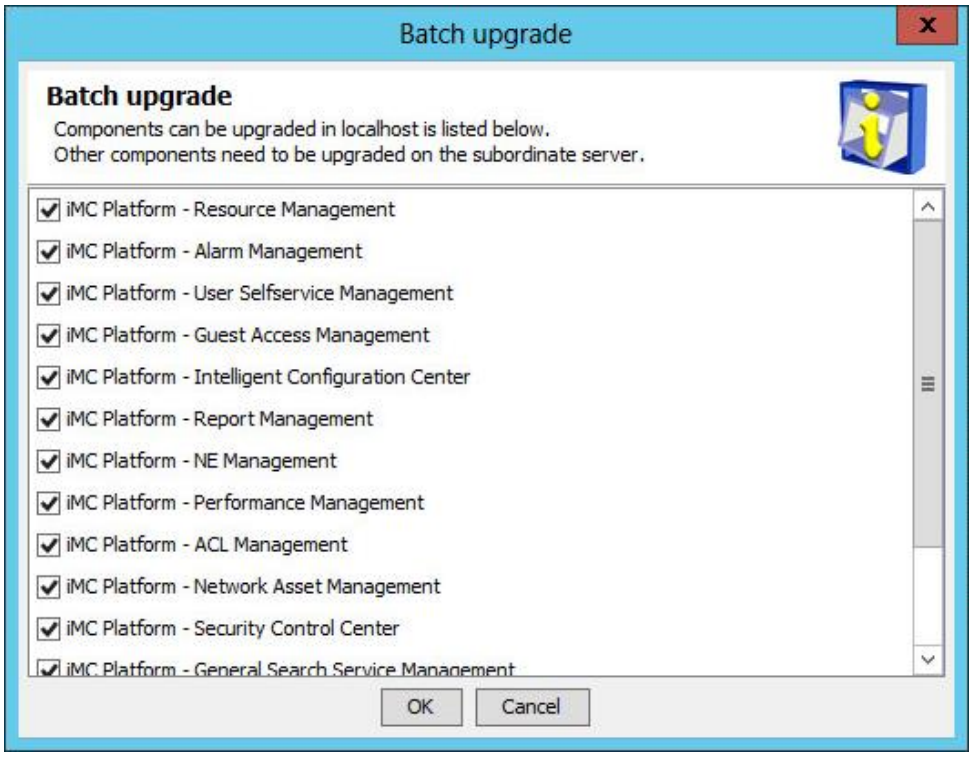
Figure 54 Installation Summary page



9. Verify the installation summary, and then click **Install**.

   After the installation is complete, the **Batch upgrade** dialog box opens, as shown in Figure 55.

Figure 55 Batch upgrade dialog box



10. Select the components you want to upgrade, and then click **OK**.

After the upgrade is complete, the **Batch upgrade result** dialog box shown in Figure 56 or Figure 57 opens. The dialog box content varies depending on whether auto backup and restoration settings have been configured in DBMan before the upgrade.

Figure 56 Batch upgrade result

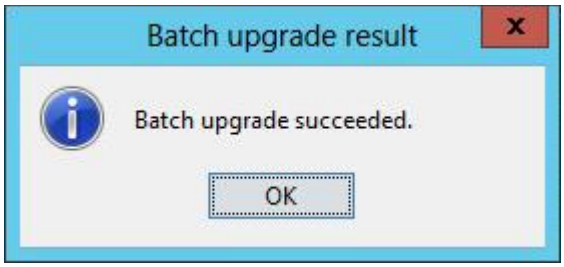
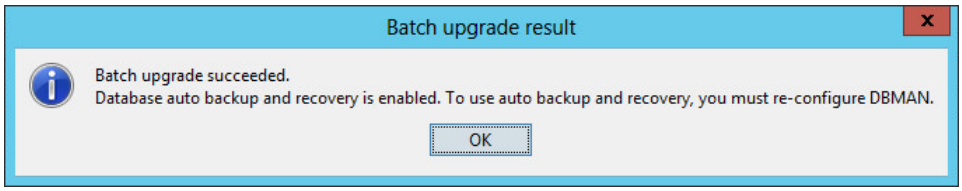


Figure 57 Batch upgrade result with auto backup and restoration



11. Click **OK**.
12. If the **Auto Backup and Recovery Settings** dialog box opens, configure the auto backup and restoration settings, and then click **OK**.
13. To start IMC, click **Start iMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

Restoring IMC

If the IMC upgrade fails, restore IMC to the version before the upgrade:

1. Manually restore the IMC database. For more information, see manual restoration described in "Backing up and restoring the database."
2. After the database restoration is complete, stop IMC in the Intelligent Deployment Monitoring Agent.
3. Close the Intelligent Deployment Monitoring Agent.
4. Stop HP iMC Server by selecting **Start** > **All Programs** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
5. In the IMC installation directory, back up the log files necessary for upgrade failure analysis, and then delete all the files in the directory.
6. Copy the backup IMC installation directory to the IMC installation path.
7. Start HP iMC Server by selecting **Start** > **All Programs** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
8. Start IMC in the Intelligent Deployment Monitoring Agent.

For IMC running in stateful failover mode, restore IMC only on the primary server in the failover system.

Uninstalling IMC

Uninstall IMC component by component or uninstall all components at one time.

To reinstall IMC, complete the following tasks before the reinstallation:

- If you have reinstalled the database after IMC is uninstalled, manually delete the folder that stores data files of the previous IMC system. The default folder is **imcdata**.
- If IMC installation or uninstallation interrupts with an error, manually delete the IMC installation directory and the **iMC-Reserved** folder. The **iMC-Reserved** folder is located in the **WINDOWS** directory or the Linux **etc** directory.

Uninstalling an IMC component

Before uninstalling an IMC component, uninstall all components that depend on it.

To uninstall an IMC component:

1. Open the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop IMC**.
3. On the **Deploy** tab, right-click the component to be uninstalled, and then select **Undeploy the Component**.

   A confirmation dialog box opens.
4. Click **OK**.

   The Intelligent Deployment Monitoring Agent undeploys the component. After the undeployment is complete, an operation success dialog box opens.
5. Click **OK**.
6. On the **Deploy** tab, right-click the undeployed component and select **Remove this Component**.

   A confirmation dialog box opens.
7. Click **OK**.

   The Intelligent Deployment Monitoring Agent uninstalls the component. After the uninstallation is complete, an operation success dialog box opens.
8. Click **OK**.

Uninstalling all IMC components at a time

1. Open the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop IMC**.
3. On Windows, select **Start** > **All Programs** > **HP Intelligent Management Center** > **Uninstall HP Intelligent Management Center**.

   On Linux, run the **uninstall.sh** script in the **/deploy** directory of the IMC installation path.

   An uninstall wizard opens.
4. Click **Uninstall**.

   A confirmation dialog box opens.
5. Click **OK**.

   The Intelligent Deployment Monitoring Agent uninstalls all components. After the uninstallation is complete, the **Uninstallation Completed** dialog box opens.
6. Clear the OS reboot option, and then click **OK**.

7. Delete the **iMC-Reserved** folder in the **WINDOWS** folder or the Linux **/etc** directory.
8. Reboot the operating system.

Registering IMC and incremental node licenses

An unregistered IMC version delivers the same functions as those of a registered version, but can be used only for 60 days since the date the service was first started. To unlock the time limitation or add extra nodes to IMC, you must purchase and register the IMC licenses.

The IMC registration procedures on Windows and Linux systems are similar. The following describes how to register IMC on a Windows Server 2008 R2 machine. Ensure you register IMC before any additional node licenses.

NOTE:

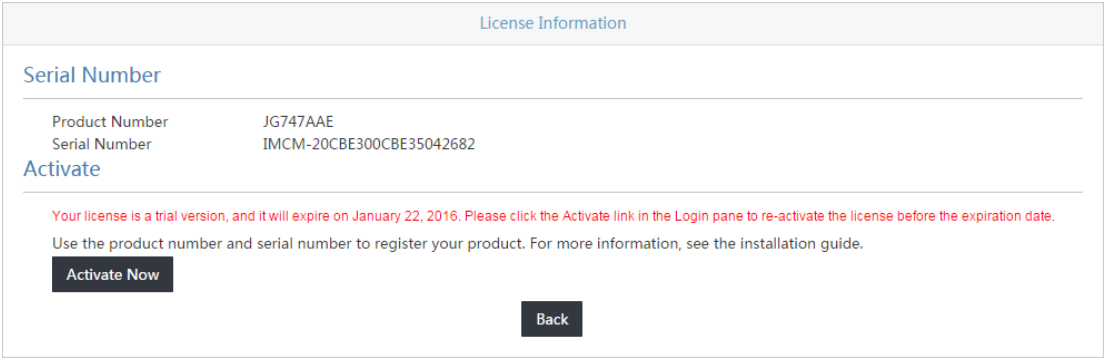
To transfer an existing license to a different Serial Number, contact Hewlett Packard Enterprise Support.

Registering IMC

1. On the IMC login page, click **Activate**.

   The **License Information** page appears, as shown in Figure 58.

   Figure 58 License Information page



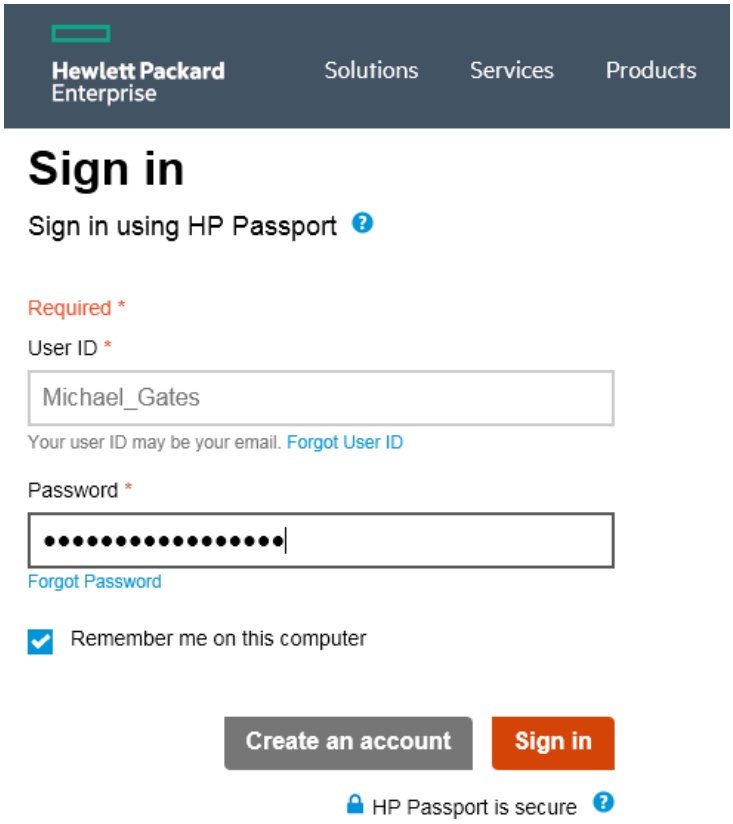
2. Select and copy or make a note of the Serial Number (this is unique to your installation of IMC).

Registering first license

1. Go to the HPE My Networking system website (http://hpe.com/networking/mynetworking/) and log in to My Networking portal.

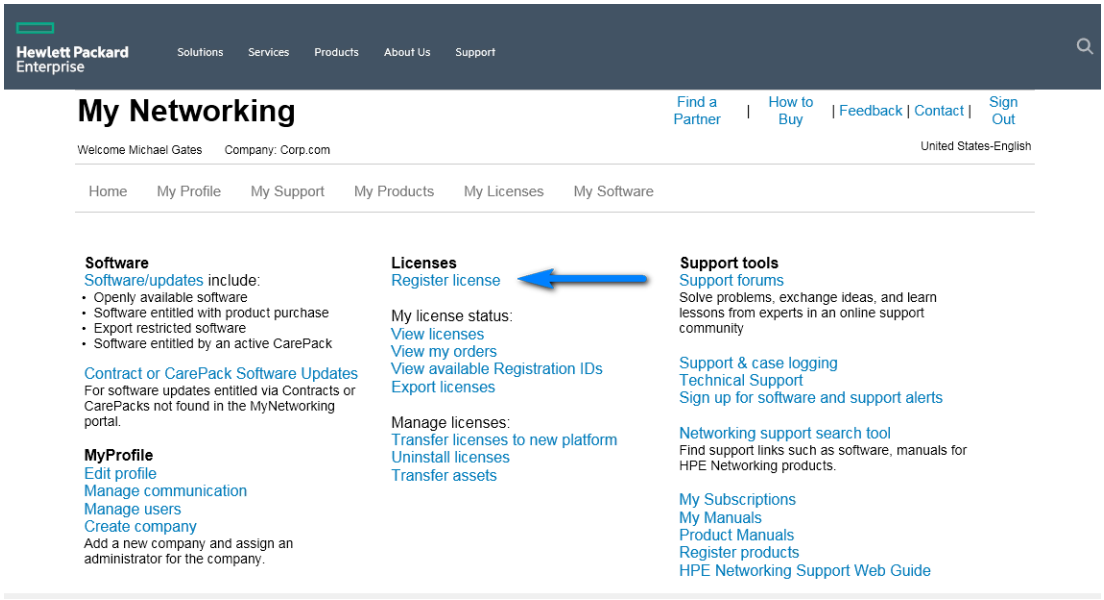
   The **HPE Passport sign-in** page appears, as shown in Figure 59.

Figure 59 HPE Passport sign-in page



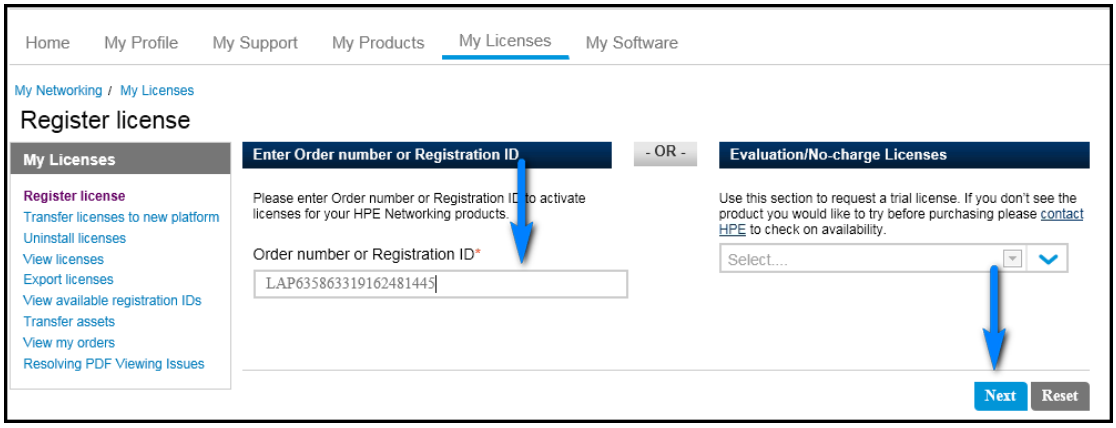
2. Enter the user ID and password and click **Sign in**.
   The **Home** page appears, as shown in Figure 60.

Figure 60 Home page



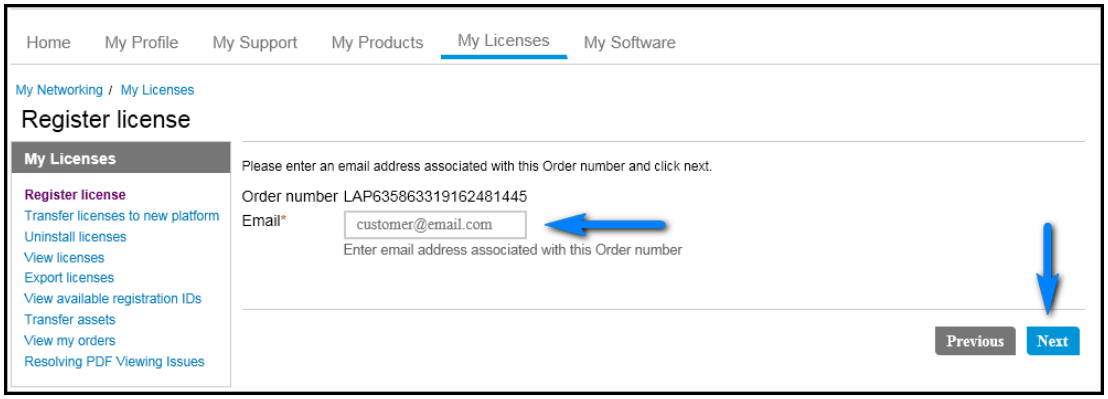
3. Click **Register license** under the **Licenses** section of the **Home** page.
   The **Enter Order number** or **Registration ID** page appears, as shown in Figure 61.

Figure 61 Enter Order number or Registration ID page



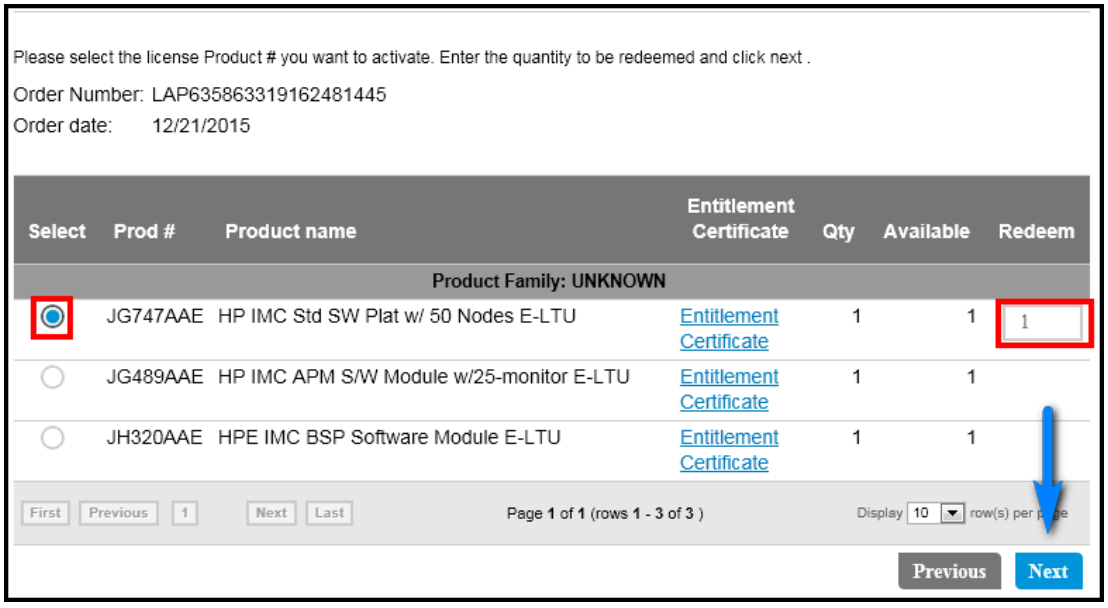
4. Enter the Order number or Registration ID, and click Next.
   The **Enter the email associated with Order number** page appears, as shown in Figure 62.

Figure 62 Enter the email associated with Order number page



5. Enter an email address associated with the **Order number** and click **Next**.
   The **Select the Product License** page appears, as shown in Figure 63.

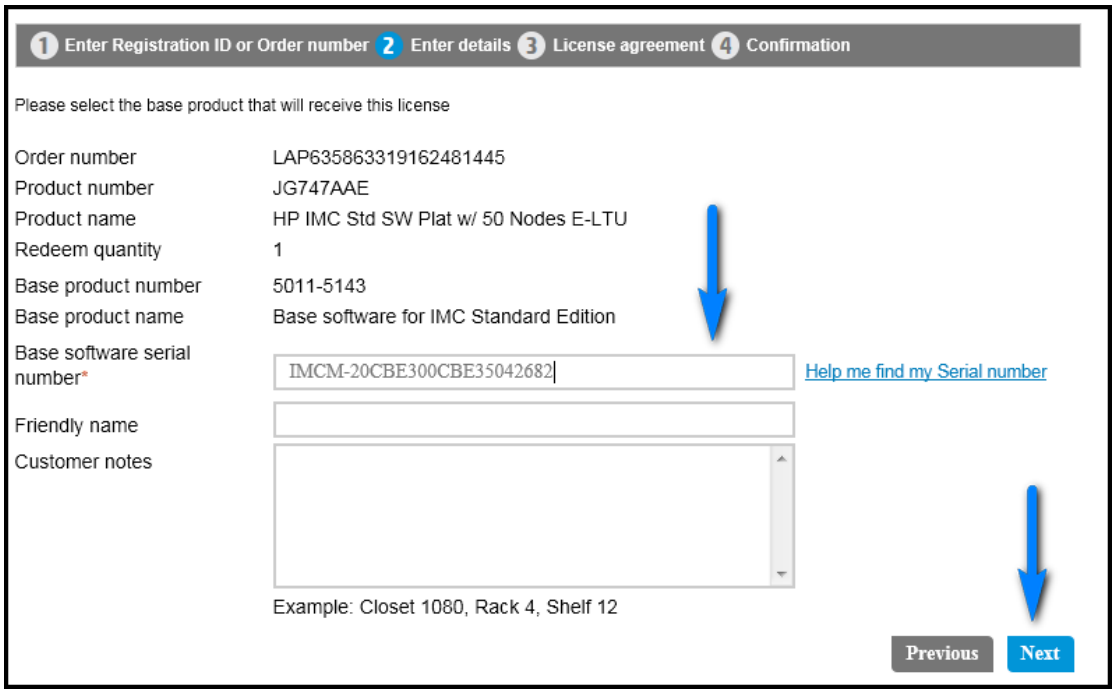
Figure 63 Select the Product License page



6. Select the product you want to register by activating the radio button to the left of the license Product #.
7. Enter the quantity to be redeemed and click **Next**.

   The **Enter details** page appears, as shown in Figure 64.

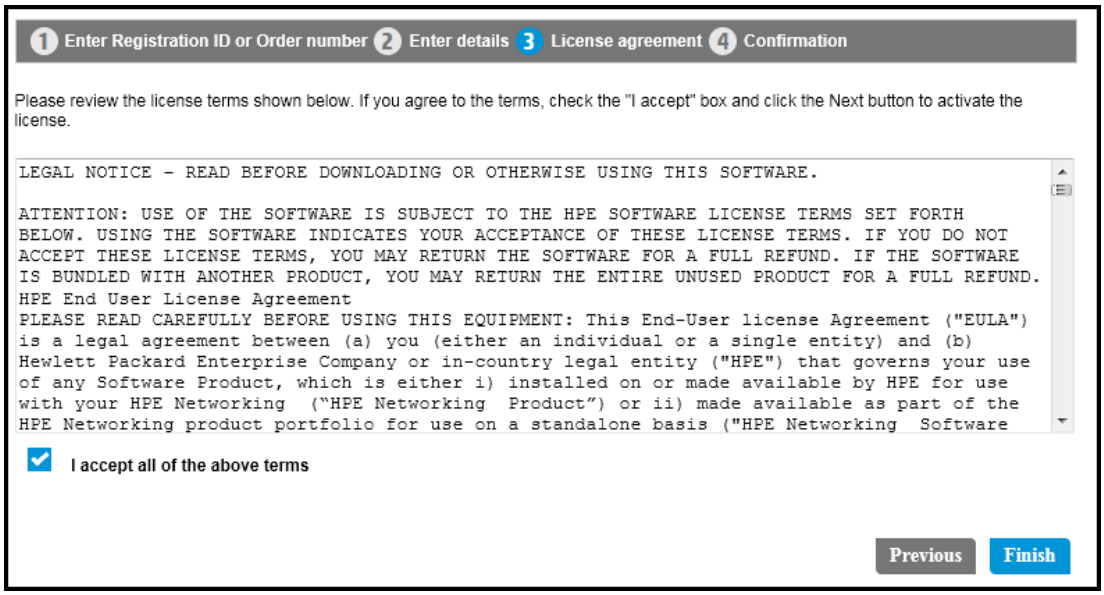
Figure 64 Enter details page



8. Enter the IMC software serial number and click **Next**.

   The **License agreement** page appears, as shown in Figure 65.

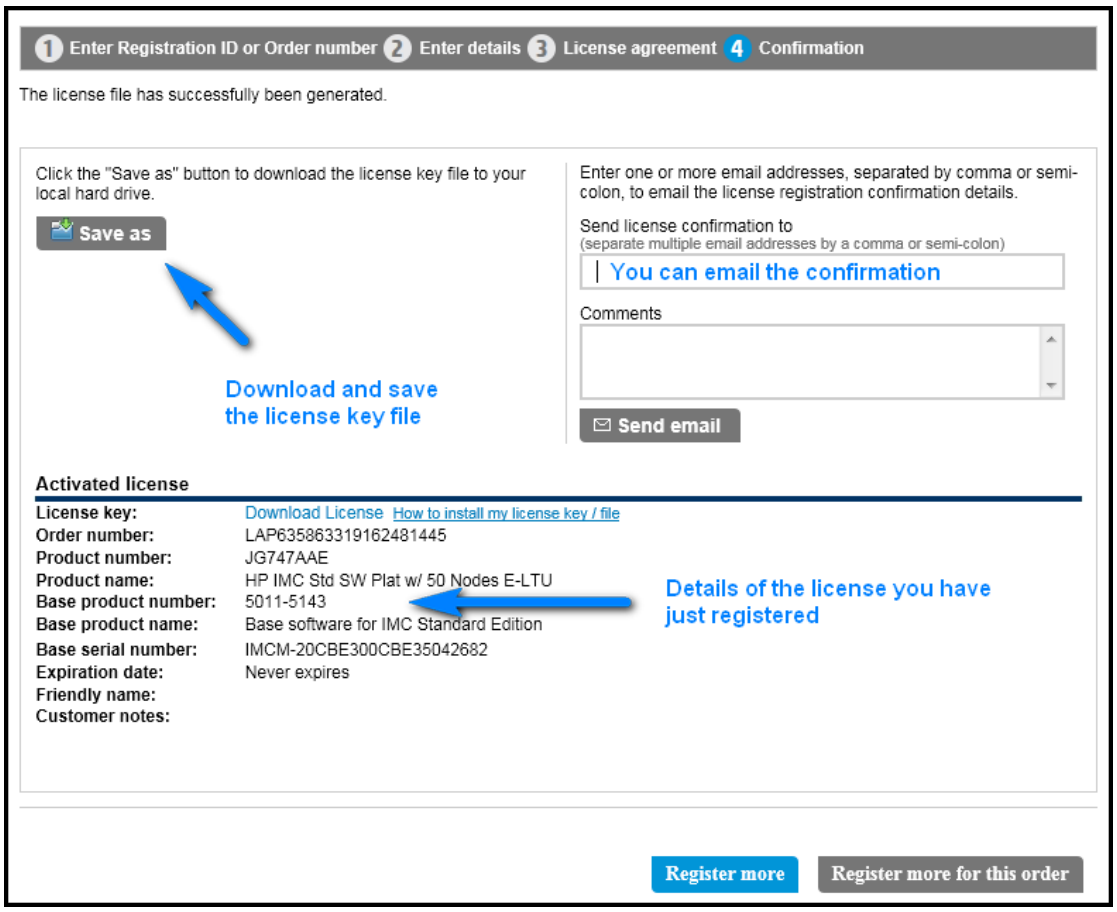
Figure 65 License agreement page



9. Read the license agreement, select **I accept all of the above terms**, and click **Finish**.

   The **Confirmation** page appears, as shown in Figure 66.

Figure 66 Confirmation page



10. Click **Save as** to download and save the license key file.

    Remember the location and file name for the next step of Activating the License in IMC.

11. If you want to email the confirmation information and license key file, enter the recipient's email address in the **Send license confirmation** to field, add any **Comments** and click **Send email**. Also, you can view the details of the license you have registered.

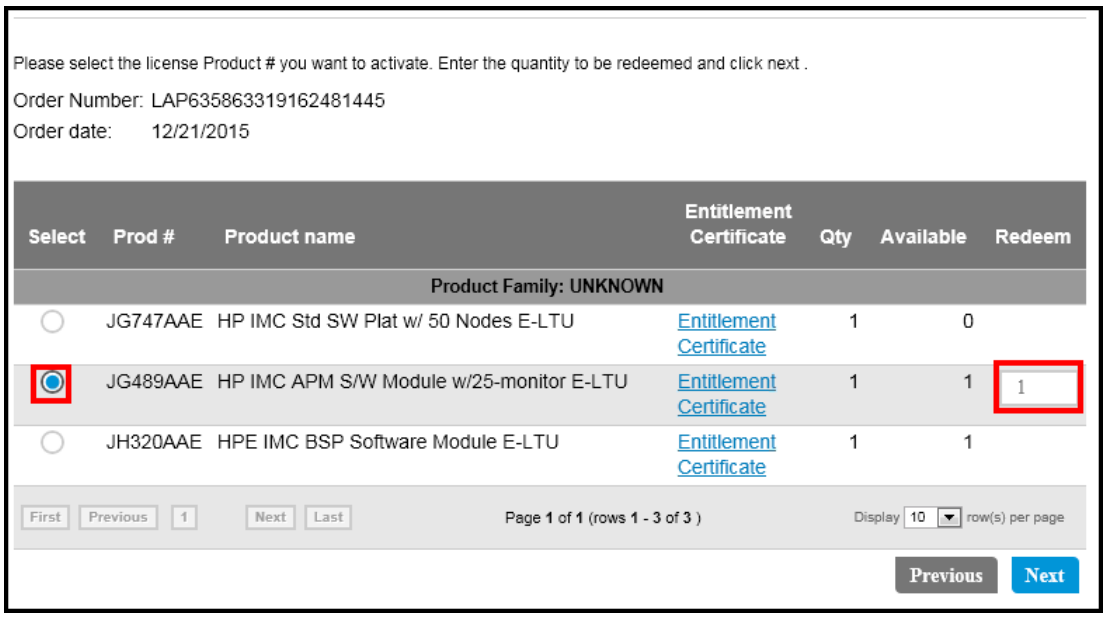
Registering incremental node licenses

Registering an Incremental Node License is similar to registering the first license. The following information describes only the differences between them.

To register an Incremental Node license:

1. Select the Incremental Node License you want to register on the **Select the Product License** page.

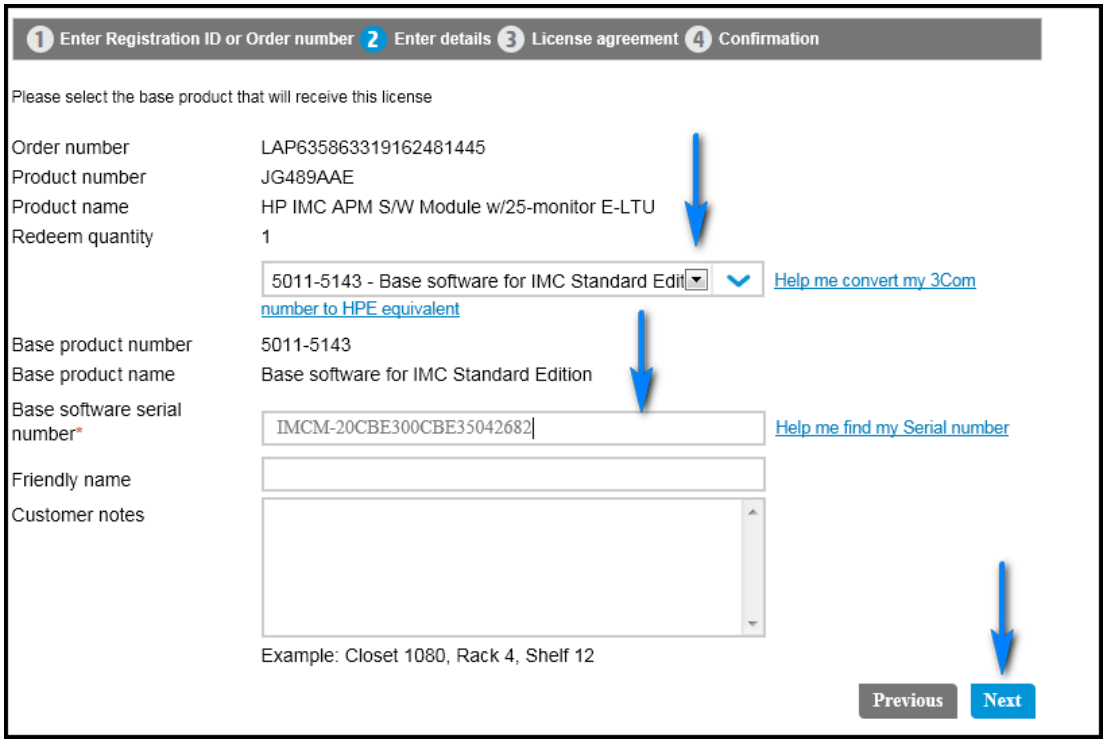
Figure 67 Select the Product License page



2. Click **Next**.

   The **Enter details** page appears, as shown in Figure 68.

Figure 68 Enter details page



3. Select the base product, enter the base software serial number, and click **Next**.

   The **Confirmation** page appears.

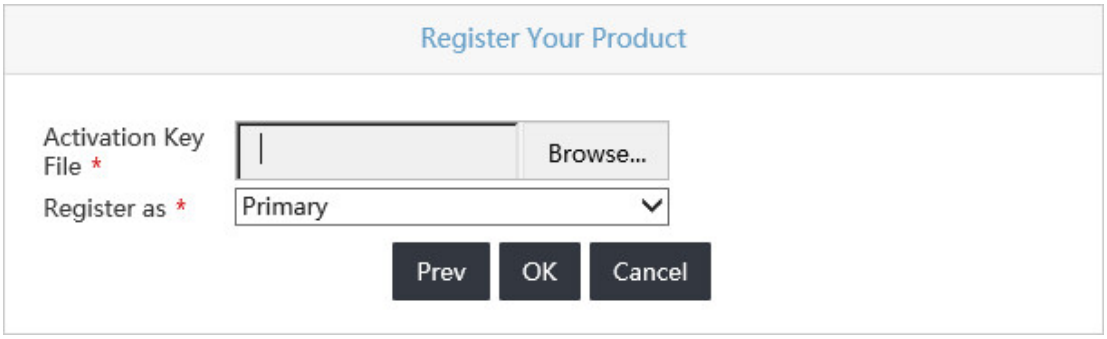
4. Click **Save as** to download and save the license key file.

   Remember the location and file name for activating the license in IMC.

Activating IMC

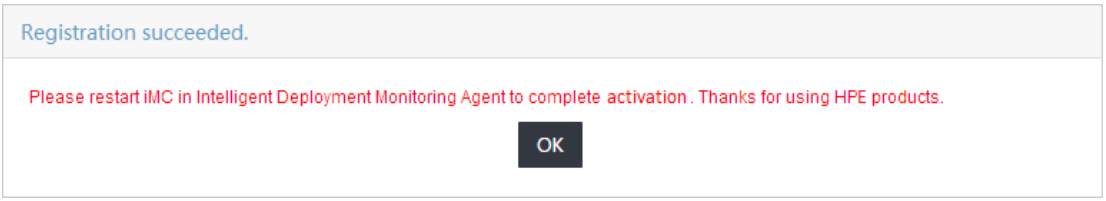
1. Access the **License Information** page, as shown in Figure 58.
2. Select **Activate Now**.
   The **Register Your Product** page appears, as shown in Figure 69.

   Figure 69 Register Your Product page



3. Select the license file in TXT format.
4. Select **Primary** from the **Register as** list.
5. Click **OK**.
   The **Registration Succeeded** dialog box appears, as shown in Figure 70.

   Figure 70 Registration succeeded dialog box



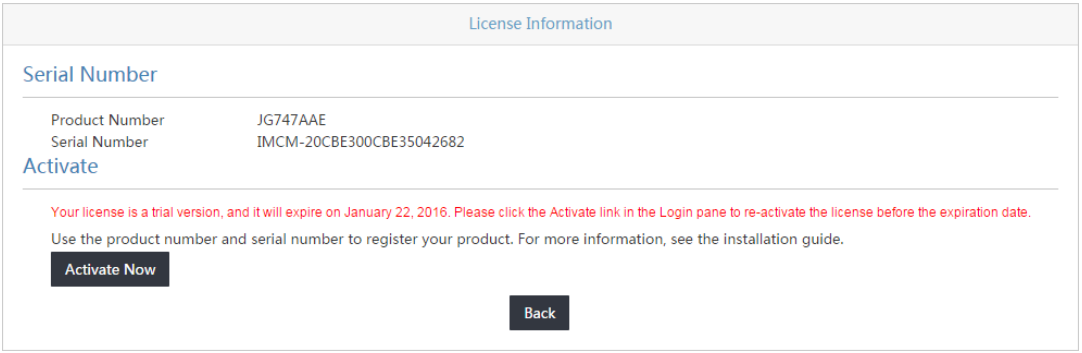
6. Restart IMC in the Intelligent Deployment Monitoring Agent.
   IMC has been successfully registered and activated.

Registering the IMC license for stateful/stateless failover

Registering the IMC license for stateful failover

1. Run IMC on the primary server.
2. After the IMC starts up, access the IMC login page.
3. Click **Activate**.
   The **License Information** page appears, as shown in Figure 71.

Figure 71 License information



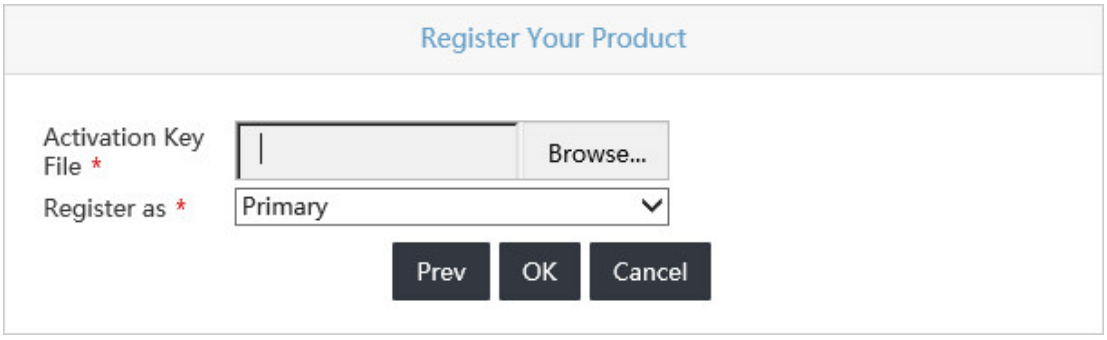
4. Record the serial number of the primary server that is displayed in the **Serial Number** area.
5. Switch the IMC services to the backup server and access the IMC login page again.
6. Click **Activate**.

   The **License Information** page appears.
7. Record the serial number of the backup server in the **Serial Number** area.
8. Log in to the HPE My Networking system website (http://hpe.com/networking/mynetworking/), enter required information, and enter the serial numbers of the host and the IMC stateful server.
9. Download and save the IMC license file locally. For more information, see "Registering first license."
10. Switch the IMC services back to the primary server and access the IMC login page again.
11. On the IMC login page, click **Activate**.

    The **License Information** page appears.
12. Click **Activate Now**.

    The registration page appears, as shown in Figure 72.

Figure 72 Registering your product



13. Click **Browse** to select the locally saved IMC license file.
14. Select **Primary** from the **Register as** list.
15. Click **OK**.
16. Restart IMC in the Intelligent Deployment Monitoring Agent.

    IMC has been successfully activated.

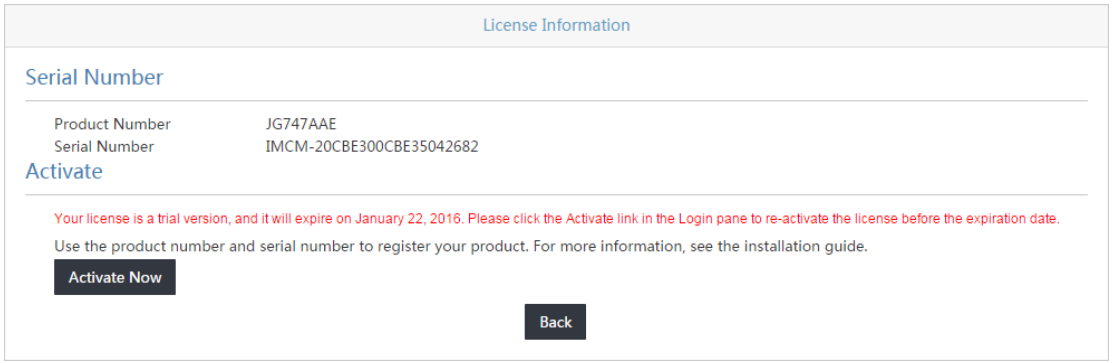
Registering the IMC license for stateless failover

When registering the IMC license for stateless failover, only the serial number of the primary server is required to get the license file. Use this file on both the IMC primary server and the IMC backup server to activate the license.

1. Start IMC on the primary server.
2. After the IMC starts up, access the IMC login page of the primary server.
3. Click **Activate**.

   The **License Information** page appears, as shown in Figure 73.

   Figure 73 License information

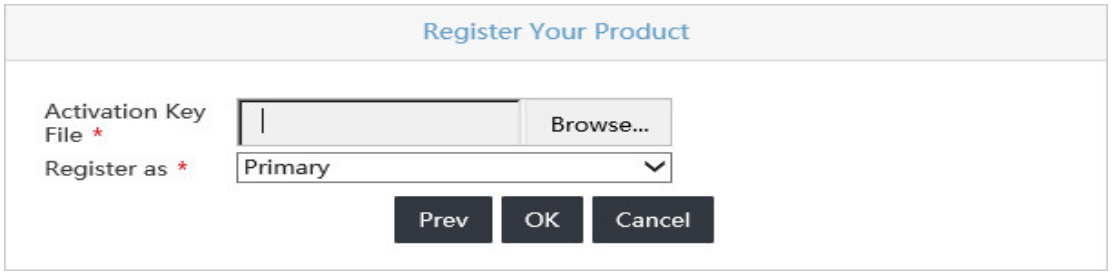
4. Record the serial number of the primary server that is displayed in the **Serial Number** area.
5. Log in to the HPE My Networking system website (http://hpe.com/networking/mynetworking/), enter required information, and enter the serial number of the host.
6. Download and save the IMC license file locally.

   For more information, see "Registering first license."
7. Access the IMC login page of the primary server again.
8. Click **Activate**.

   The License Information page appears.
9. Click **Activate Now**.

   The registration page appears, as shown in Figure 74.

   Figure 74 Registering your product

10. Click **Browse** to select the locally saved Activation key file.
11. Select **Primary** from the **Register as** list.
12. Click **OK**.
13. Restart IMC in the Intelligent Deployment Monitoring Agent.

    IMC has been successfully activated on the primary server.
14. Access the IMC login page of the backup server.

15. Click **Activate**.

    The **License Information** page appears.

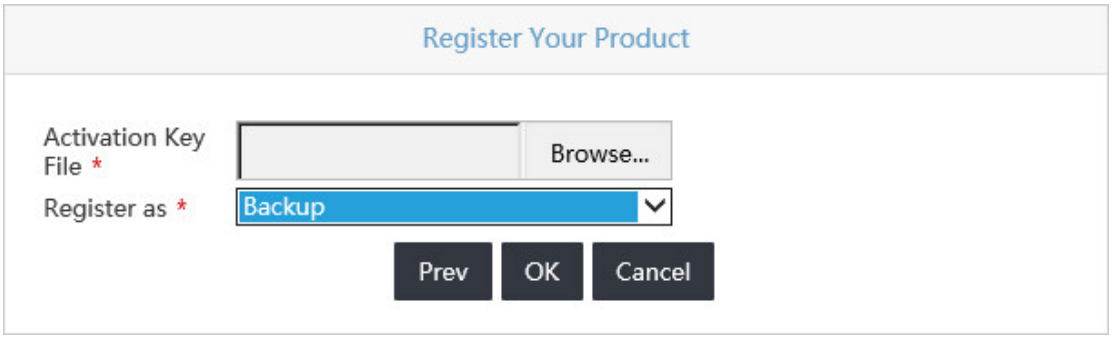
16. Click **Activate Now**.

    The registration page appears.

17. Click **Browse** to select the locally saved IMC license file. This license file is the same as the file used for the IMC registration on the host.

18. Select **Backup** from the **Register as** list.

    Figure 75 Registering your product



19. Click **OK**.

20. Restart IMC in the Intelligent Deployment Monitoring Agent.

    IMC has been successfully activated on the backup server.

Security settings

Antivirus software

As a best practice to improve security, install antivirus software on IMC servers and keep the virus definitions up to date.

Port settings

As a best practice, use a firewall to protect the IMC server cluster by filtering the non-service data sent to the cluster.

NOTE:

- Do not use a switch to filter data packets by using ACLs, because the switch might filter out packet fragmentations.
- NTA/UBA typically uses probes for log collection. When a firewall is deployed between the probes and IMC, configure ACLs on the firewall to allow IP packets sent by the probes to IMC.

Make sure the ports used by the IMC components (listed in Table 15 and Table 16) are not blocked by the firewall.

Table 15 Port numbers used by the IMC platform

Default port number	Usage	Location
UDP 161	Port to add a device to the IMC	Device
UDP 22	Port for SSH operations	Device
TCP 23	Port for Telnet operations	Device
UDP 514, 515	Port for syslog operations	IMC server
UDP 162	Port for trap operations	IMC server
TCP 8080, configurable	HTTP access to IMC	IMC server
TCP 8443, configurable	HTTPS access to IMC	IMC server
UDP 69	Port for Intelligent Configuration Center to perform configuration management through TFTP	IMC server
TCP 20, 21	Port for Intelligent Configuration Center to perform configuration management through FTP	IMC server
TCP 2810	Port for data file backup and restoration by using DBMan	IMC server

Table 16 Port numbers used by the IMC NTA/UBA

Default port number	Usage	Location
UDP 9020, 9021, 6343	Port for the IMC server to receive logs	IMC server
TCP 8051	Listening port used to monitor the command for stopping the NTA/UBA service	IMC server
TCP 9099	JMX listening port for the NTA/UBA service	IMC server

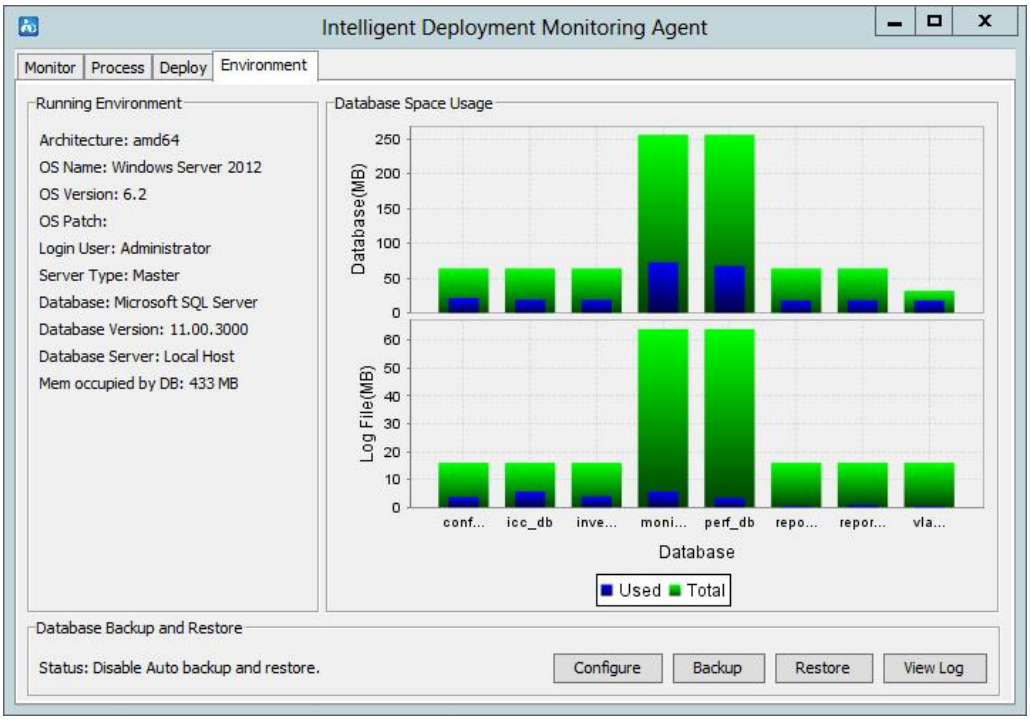
Default port number	Usage	Location
UDP 18801, 18802, 18803	Communication ports between NTA and UBA	IMC server

Backing up and restoring the database

DBMan is the automatic backup and restoration tool for the IMC platform and service component databases, and provides a full-range system disaster backup solution. DBMan uses a standard SQL backup and restoration mechanism to process the complete databases.

DBMan supports both manual and automatic database backup and restoration. It is integrated in the **Environment** tab of the Intelligent Deployment Monitoring Agent, as shown in Figure 76.

Figure 76 Environment tab



The **Environment** tab includes the following areas:

- **Running Environment**—Displays the software and hardware information on the IMC server.
- **Database Space Usage**—Displays the database and log file usage information on the IMC server.
- **Database Backup and Restore**—Provides the following database backup and restoration options:
  - **Configure**—Allows you to configure automatic database backup and restoration settings. The automatic backup and restoration function is typically used in stateless failover scenarios.
  - **Backup**—Immediately backs up all IMC data files (including configuration files and database files) to a specified path.
  - **Restore**—Immediately restores previously backed up database files on the IMC server.
  - **View Log**—Allows you to view the database backup and restoration logs.

Configuration restrictions and guidelines

To ensure correct operation, do not back up and restore IMC databases between different operating systems.

When you use DBMan to back up and restore IMC databases, follow these restrictions and guidelines:

- In automatic backup configuration, use the **Upload to Backup System** option to back up database files to a backup IMC system or an FTP server.
- The **Upload to Backup System** option requires one of the following conditions:
  - The **Master Server IP of Backup System** is specified for database backup.
  - An FTP server is configured in the **dbman_ftp.conf** file in the **\dbman\etc** directory of the IMC installation path. For example:

    ```
    ftp_ip=1.1.1.1
    ftp_user=admin
    ftp_password=1234
    ```
- To add additional backup and restoration settings, edit the **dbman_addons.conf** file in the **\dbman\etc** directory of the IMC installation path. The settings take effect immediately after the file is saved.

  For example, add the following strings to the **dbman_addons.conf** file to specify tasks to perform before or after database restoration:

  ```
  BeforeSQLScript_monitor_db_IMC_monitor = D:\1.bat
  AfterSQLScript_monitor_db_IMC_monitor = D:\2.bat
  ```

Backing up and restoring databases for a single IMC system

Backing up databases

A single IMC system supports both manual and automatic backup:

- **Manual backup**—Immediately backs up all IMC data files to the specified location on the IMC server.
- **Automatic backup**—Allows you to schedule a task to automatically back up selected data files at the specified time.

Manual backup

1. On the **Environment** tab, click **Backup**.

   A confirmation dialog box opens.
2. Click **OK**.

   The **Select database backup path** dialog box opens.
3. Specify a local path to save the backed up data files.

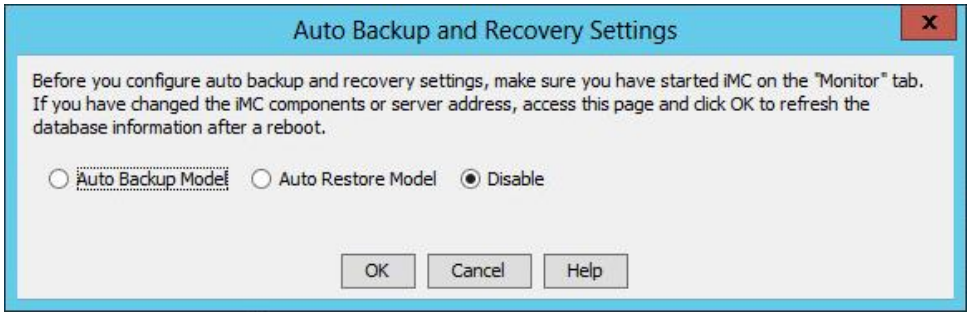
   Make sure the specified path has enough space.
4. Click **OK**.

Automatic backup

1. On the **Environment** tab, click **Configure**.

   The **Auto Backup and Recovery Settings** dialog box opens, as shown in Figure 77.

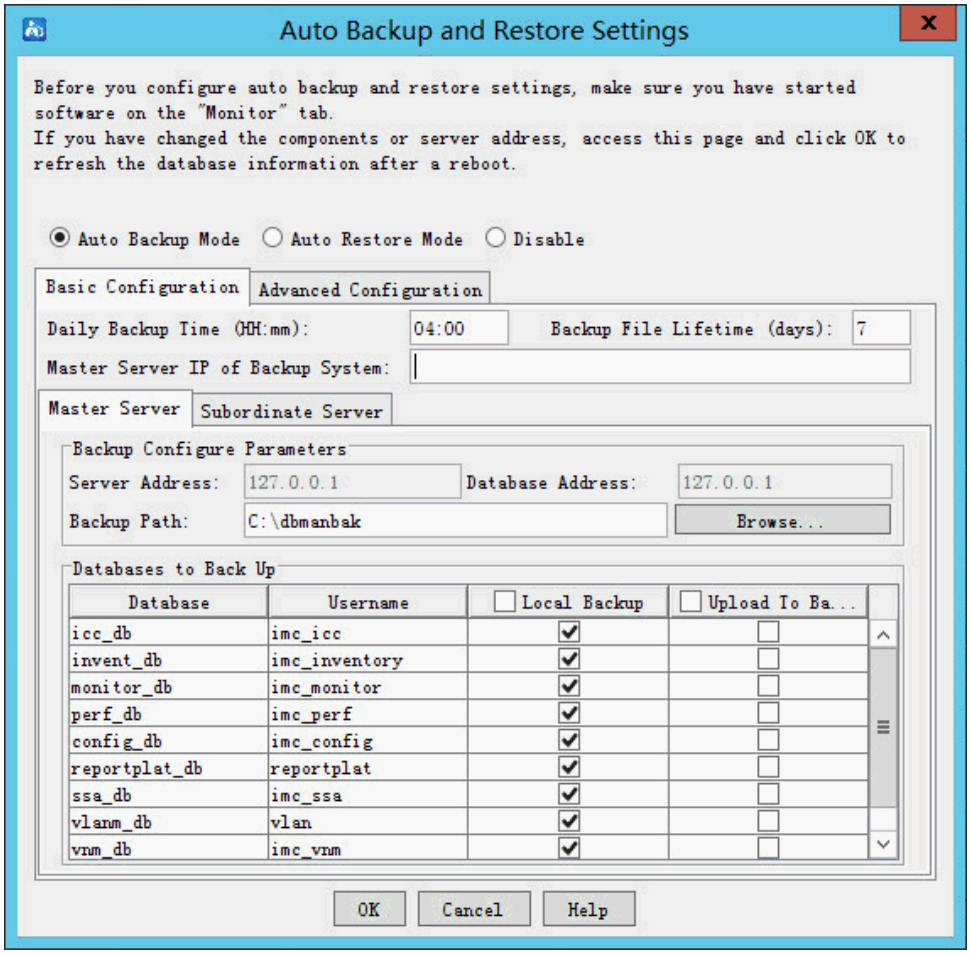
Figure 77 Auto Backup and Recovery Settings



2. Read information in the **Auto Backup and Recovery Settings** dialog box, select **Auto Backup Model**, and then click **OK**.

   The page for configuring automatic backup settings opens, as shown in Figure 78.

Figure 78 Configuring automatic backup settings



3. On the **Basic Configuration** tab, configure the **Daily Backup Time (HH:mm)** parameter. Enter the time at which the automatic backup operation starts every day. By default, the daily backup time is 04:00.
4. Click the **Master Server** tab, and then configure the following parameters:
   - **Backup Path**—Enter or browse to a local path to store the backup data files.
   - **Local Backup**—Select the databases to back up locally. By default, all databases are selected.

- **Upload To Backup System**—Select the database to upload to an FTP server or the master server of a backup system. By default, no database is selected. When you select **Upload To Backup System** for a database, the **Local Backup** option is forcibly selected for the database. To configure the FTP server, see "Configuration restrictions and guidelines."

5. Click the **Advanced Configuration** tab, and then configure the following parameters:
   - **Backup file lifetime (days)**—Enter how many days a backup file can be kept. Expired files are automatically deleted.
   - **Delete local files after upload even if upload fails**—Specify whether to delete local backup files after they are uploaded.
6. Click **OK**.

Restoring databases

A single IMC system supports only manual restoration of the databases. Manual restoration immediately replaces the current database files with previously backed up files.

When you perform manual restoration, follow these restrictions and guidelines:

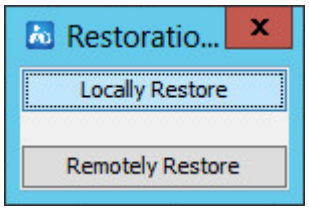
- Make sure IMC has been started at least once after installation before you restore the IMC databases.
- Restore database files for the IMC platform and service components together. If you restore only some of the database files, data loss or inconsistency might occur.
- During manual database restoration, the IMC service and database service are automatically stopped and restarted.

To perform a manual restoration:

1. On the **Environment** tab, click **Restore**.

   The **Restoration Type** dialog box opens, as shown in Figure 79.

   Figure 79 Restoration Type dialog box

2. Click **Locally Restore**.

   A confirmation dialog box opens.
3. Click **Yes**.

   The **Select the data file to be restored** dialog box opens.
4. Select database files to be restored, and then click **OK**.

   The **Confirm** dialog box opens.
5. Click **Yes**.

   The system starts restoring the database files.

   The **Message** dialog box opens after the restoration is complete.
6. Click **OK**.

   The IMC service will start automatically.

Backing up and restoring databases in stateless failover scenarios

A typical stateless failover scenario includes a primary IMC system and a backup IMC system. For stateless failover, configure automatic backup on the primary IMC system and configure automatic restoration on the backup IMC system.

During automatic backup and restoration, DBMan of the primary IMC system performs the following operations:

1. Periodically backs up database files locally.
2. Uploads the backed up database files to the backup IMC system.
3. Instructs the backup IMC system to restore the received database files locally.

As a best practice, restore database files for all components together. If you restore databases for only some of the components, the other components might become unavailable.

Backing up databases

In stateless failover, configure automatic backup on the master server of the primary IMC system.

Before the configuration, make sure the following settings are consistent on the primary and backup IMC systems:

- OS
- Database type and version
- IMC version and patches

For more information about how to configure automatic backup, see "Automatic backup."

Restoring databases

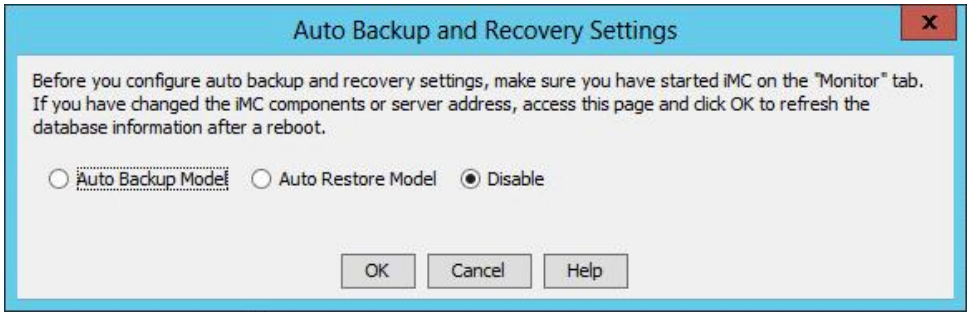
This example describes the automatic restoration settings on a backup IMC system that is deployed in centralized mode and uses a local database.

To configure automatic restoration:

1. On the **Environment** tab, click **Configure**.

   The **Auto Backup and Recovery Settings** dialog box opens, as shown in Figure 80.

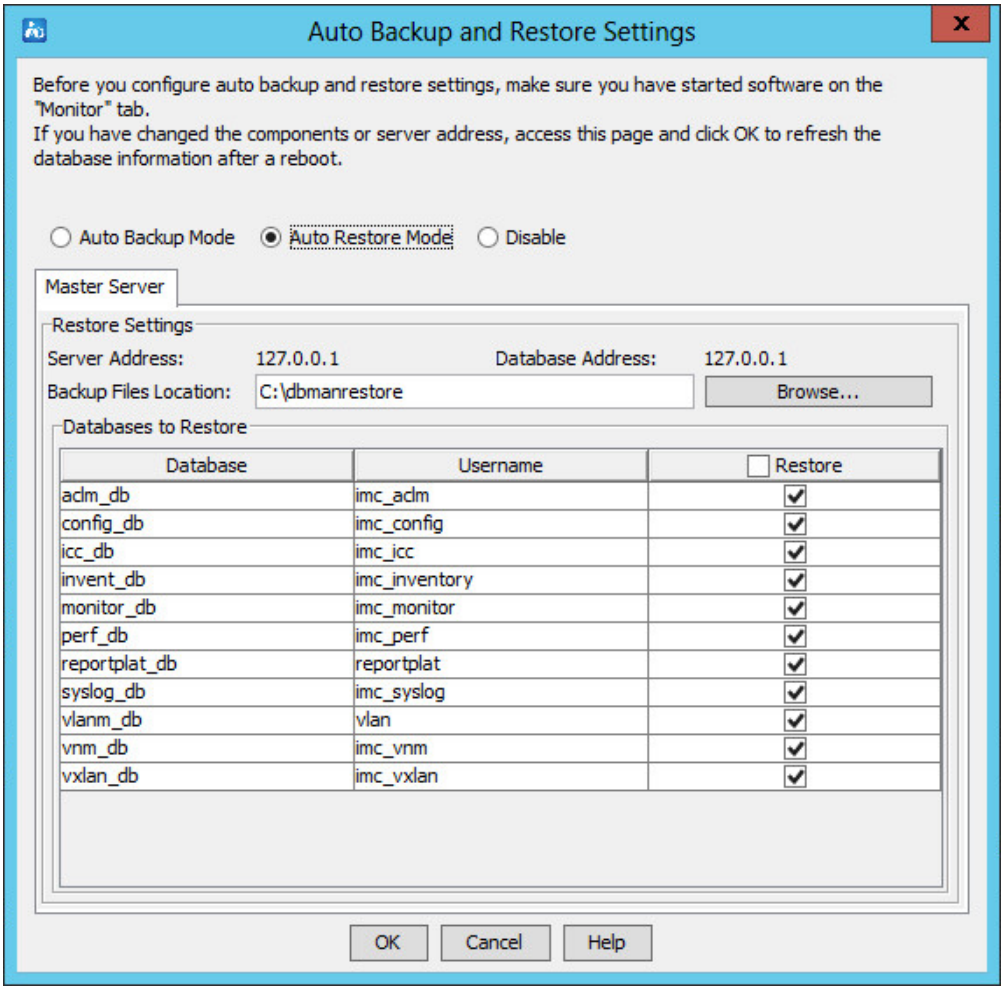
   Figure 80 Auto Backup and Recovery Settings dialog box

2. Read information in the **Auto Backup and Recovery Settings** dialog box, select **Auto Restore Model**, and then click **OK**.

   The page for configuring auto restoration settings opens, as shown in Figure 81.

Figure 81 Configuring auto restoration settings



3. Click the **Master Server** tab, and then configure the following parameters:
   - **Backup Files Location**—Enter or browse to a local path that stores the backup data files uploaded by the primary IMC system.
   - **Databases to Restore**—Select databases to restore. By default, all databases are selected.
4. Click **OK**.

FAQ

How do I install the Java running environment on Linux so that I can use Firefox to access IMC?

To install the Java running environment, install and configure JDK or JRE for Firefox. This example uses JDK.

1. Download the JDK installation file from the Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/index.html

   Make sure the installation file matches the requirements of the operating system. For example, download **jdk-6u12-linux-i586-rpm.bin** for x86-based Linux.

2. Copy the JDK installation file to a local directory. In this example, save the installation file in the **/tmp** directory and install JDK:

   ```
   cd /tmp
   sh jdk-6u12-linux-i586-rpm.bin
   ```

3. Press the spacebar to view the copyright information, and then enter **yes** to finish the JDK installation.

   JDK is installed in the **/usr/java/jdk1.6.0_12** directory. At the same time, a **/usr/java/default** link pointing to the **/usr/java/jdk1.6.0_12** directory is generated automatically, equivalent to JDK being installed in the **/usr/java/default** directory.

4. Configure JDK for Firefox.

   On the Linux operating system, execute the following commands:

   ```
   cd /var/local/firefox/plugins/
   ln -s /usr/java/default/jre/plugin/i386/ns7/libjavaplugin_oji.so
   ```

After the installation, run **/var/local/firefox/firefox** to access IMC.

After IMC installation is complete, how do I change the database file storage path?

1. Stop the IMC service by using the Intelligent Deployment Monitoring Agent.
2. Transfer the databases of IMC components to the new storage path on the database server. This example uses **D:\imcdata**.
3. At the CLI, access the **\deploy** directory of the IMC installation path, and then modify the database file storage path.

   ```
   pwdmgr.bat -changeDataDir "D:\imcdata"
   ```

   Figure 82 shows that the storage path has been successfully modified.

Figure 82 Modifying the database file storage path

4. Start the IMC service.

In Linux, the time on the server (such as the login time and operation log record time) is different from the time on the server, and the difference might be several hours.

This issue occurs because the current time zone setting on the server is different from that when IMC was installed. Use the **tzselect** command to modify the time zone of the server.

After IMC is installed in the Windows Server 2003 64-bit OS, the IMC background processes cannot be started.

For correct IMC operation on Windows Server 2003 64-bit OS, install the **WindowsServer2003-KB942288-v4-x64.exe** patch on the OS:

1. Stop IMC.
2. Install the patch.
3. Execute **vcredist.exe** in the **\deploy\components\server** directory of the IMC installation path.

During the component deployment process, a deployment failure occurs and the system displays a database script execution error message. The log file includes an error message that the object dbo.qv.id already exists. How do I resolve the issue?

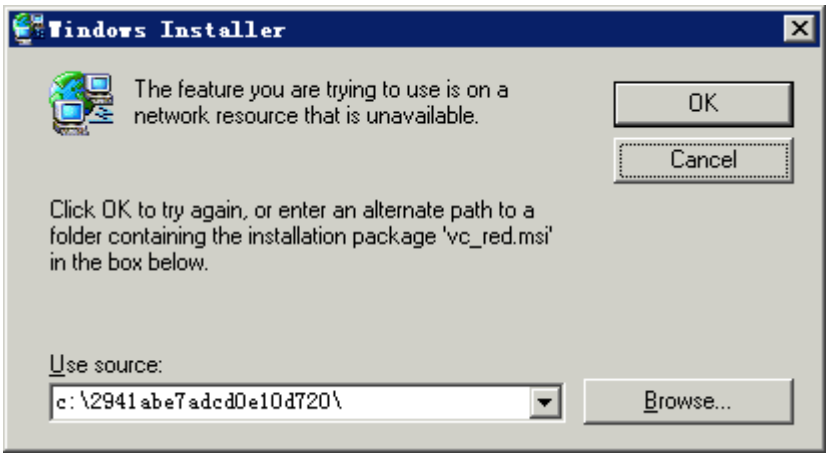
1. Log in to the Query Analyzer of SQL Server as **sa**, and then execute the following commands:

```
use model
EXEC sp_droptype 'qv_id'
```

2. Redeploy the component that failed to be deployed.

When installing IMC on Windows Server 2008 R2, the system indicates that the Windows Installer cannot be installed, as shown in Figure 83.

Figure 83 Windows Installer dialog box



To resolve the issue:

1. In the **Windows Installer** dialog box, click **Browse**.
2. Select the **vc_red.msi** file in a folder whose name contains digits and **abcdef** in the root directory of the disk.
3. Click **OK**.
4. Continue the installation.

In Linux, how do I start JavaService when Xwindows is closed?

Use the **service IMCdmsd start** command to start the JavaService.

In Windows, IMC service processes cannot be started or stopped after IMC runs for a period of time.

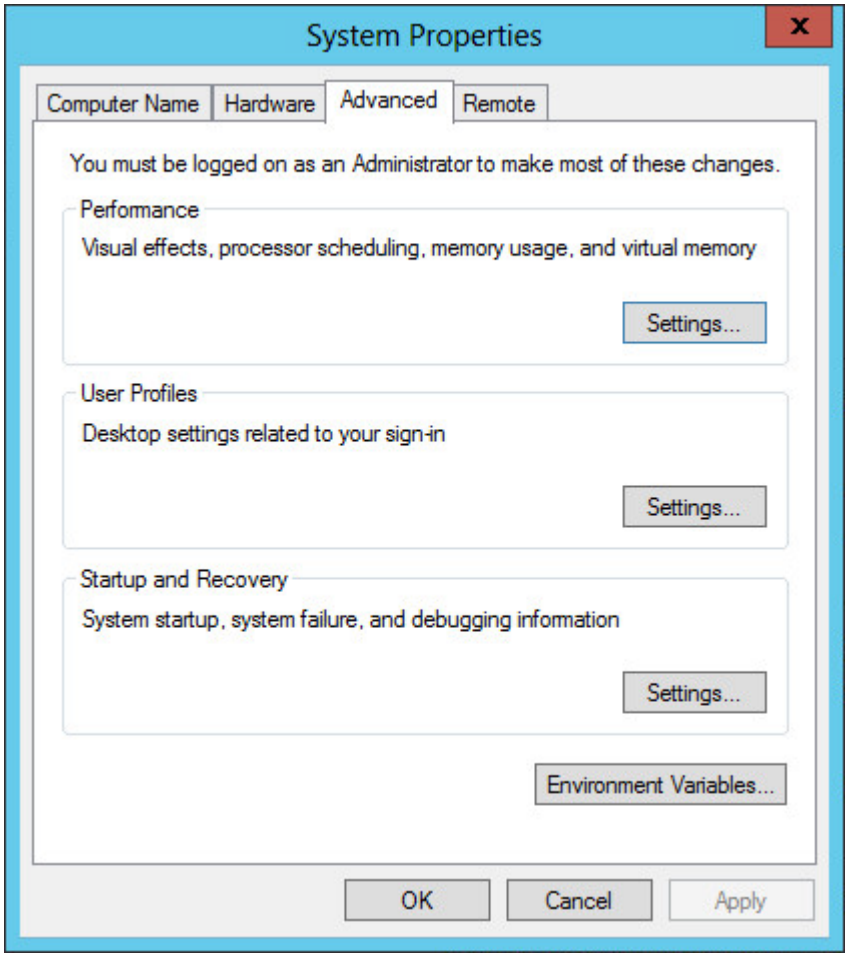
This issue is caused by insufficient virtual memory.

To resolve this issue, set the virtual memory to the system managed size:

1. On the IMC server, click **Control Panel**, and then click the **System** icon.

   The **System Properties** dialog box opens, as shown in Figure 84.

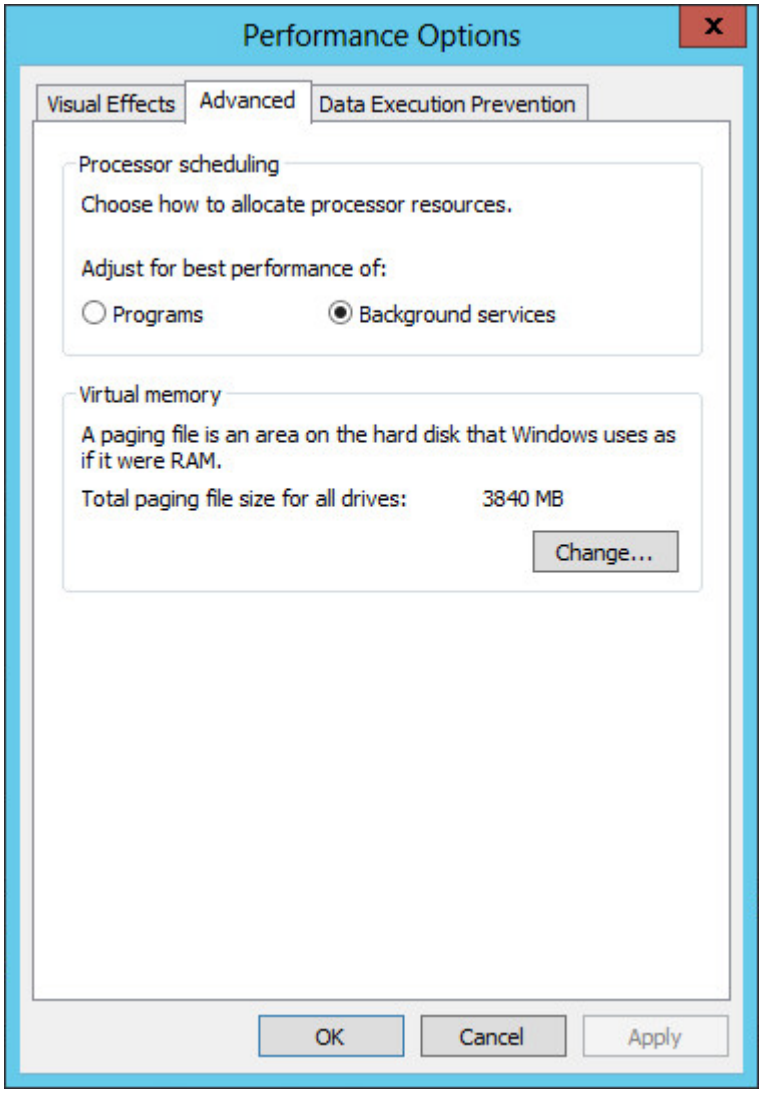
Figure 84 System Properties dialog box



2. Click the **Advanced** tab, and then click **Settings** in the **Performance** area.

   The **Performance Options** dialog box opens, as shown in Figure 85.

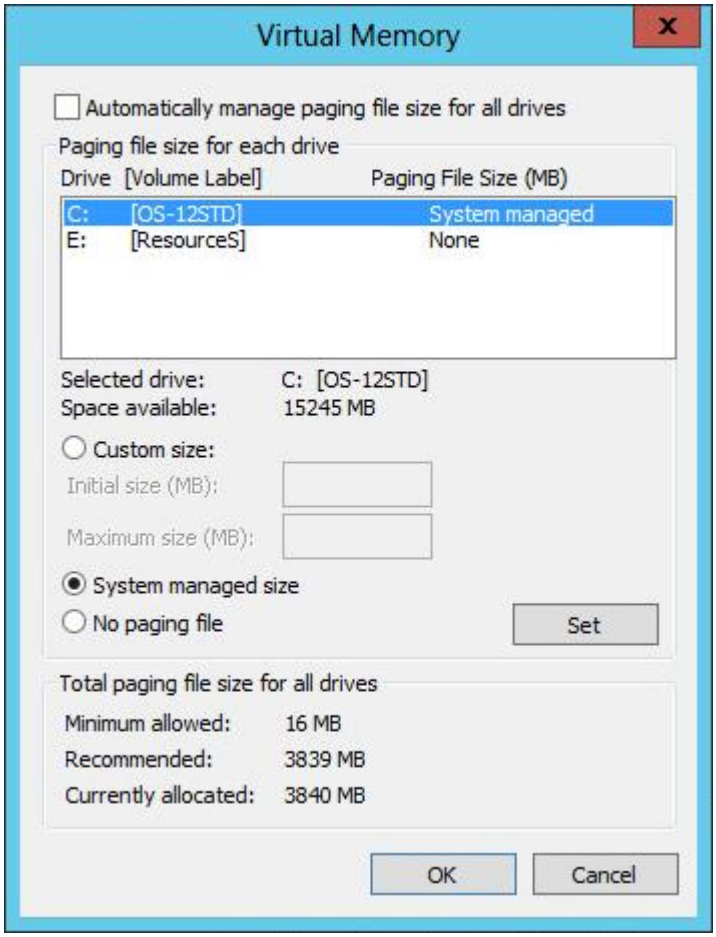
Figure 85 Performance Options dialog box



3. Click the **Advanced** tab, and then click **Change** in the **Virtual memory** area.

   The **Virtual Memory** dialog box opens, as shown in Figure 86.

Figure 86 Virtual Memory dialog box



4. Select **System managed size**, and then click **Set**.
5. Click **OK**.

In Linux, popup windows cannot be found during IMC deployment or upgrade.

When Xshell or Xstart is used for remote GUI access on Linux, a window might open on top of popup windows. To resolve this issue, move the window away to view the popup windows.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast

and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.