HP IMC Centralized Deployment Guide with Local Database

Abstract

This document describes the processes and procedures to follow when deploying the HP 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.

Software version: IMC PLAT 7.0 (E0102)

Document version: 5PW100-20130911

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

1 Introduction to Intelligent Management Center

This document describes how to deploy IMC in centralized mode and to use a local database.

This scheme is applicable to small enterprises with 50 to 500 employees and 50 to 500 managed devices.

IMC components

IMC includes the IMC Platform and service components.

IMC Platform

The IMC Platform is the base component for providing IMC services and includes the following subcomponents:

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

Service components

Service components are optional and purchased separately from the IMC Platform. Their installation and deployment are based on the IMC Platform.

Primary service components are as follows:

- **Application Manager (APM)**—Allows system and network administrators to remotely manage application programs and resources. It also allows them to monitor various types of programs and services running on the network, such as:
  - Web application programs

    - Application servers
    - Web servers
    - Databases
    - Network services
    - Systems
- **VAN Connection Manager (VCM)**—Provides a solution for physical network configuration migration. It tracks the startup, stopping, and migration of virtual machines (VMs), and according to the latest VM location, it deploys a physical network configuration. The VCM allows collaboration for physical and virtual networks. It also provides compatibility between physical and virtual networks of different vendors.
- **Endpoint Admission Defense (EAD) Security Policy**—Endpoint Admission Defense enforces enterprise security policies on terminals to enhance terminal defense capabilities, control network access, and ensure network security.
- **IPsec VPN Manager (IVM)**—Provides unified management of IPsec VPN configurations. It offers high-efficiency management and flexible deployment for network domains, IPsec device configurations, and security proposal templates.
- **MPLS VPN Manager (MVM)**—Provides topology discovery for BGP/MPLS VPNs, status/performance monitoring, fault location, and service deployment.
- **Network Traffic Analyzer (NTA)**—Network Traffic Analyzer simplifies bandwidth usage monitor on enterprise networks and provides easy-to-understand reports.
- **QoS Manager(QoSM)**—Manages QoS configurations on network devices to control and manage QoS for the overall network.
- **Remote Site Manager (RSM)**—Remotely manages branch networks that might be isolated by firewalls or NAT devices, and greatly reduces the network management costs by eliminating the need to deploy network management software and IT staff on each branch.
- **Service Health Manager (SHM)**—Provides visual service quality management functions. It integrates the alarm, performance, NTA, and NQA data. It uses key quality indexes and service level agreements to monitor and measure the service health, also visually manage the service health.
- **Service Operation Manager (SOM)**—Provides a solution to the operation and maintenance of enterprise IT networks. It focuses on the key service switching and operation part in the ITIL lifecycle, and supports for flows related with IT network operation and maintenance. With the flow management capability, Service Operation Manager makes all IT operation and maintenance activities controllable, measurable, and auditable.
- **User Access Manager (UAM)**—Provides the following features:
    - **Access user management**—Uses centralized mode and is integrated with device and topology management.
    - **Access and admission control**—Authenticates and authorizes the use of access services, and cooperates with user management and network resource management to provide enhanced access service management.
- **User Behavior Auditor(UBA)**—For increasingly complex service application environments and more network facilities, User Behavior Auditor provides a simple, efficient log auditing tool to help operators quickly and accurately view the network access information to locate problems.
- **Wireless Service Manager (WSM)**—Provides WLAN management functions to implement unified wired and wireless network management.

With WSM, administrators can add wireless management functions to the existing wired network management system, saving investment and maintenance costs.

- **Branch Intelligent Management System (BIMS)**—Allows remote monitoring and management of the two types of devices that cannot be managed through SNMP or Telnet:
  - Devices that use dynamic IP addresses.
  - Devices that are located behind the NAT gateways.

  Branch Intelligent Management System provides a cost-effective and efficient solution to manage large numbers of geographically dispersed devices that have similar service requirements.

For information about all service components, see *HP IMC Getting Started Guide*.

The IMC Platform is the basis for implementing various services and must be installed before service component deployment.

IMC editions

Three editions of IMC are available:

- Enterprise
- Standard
- Basic

Table 1 Differences between IMC editions

Item	Basic	Enterprise	Standard
Number of nodes	1000	Extensible	Extensible
Hierarchical Network Management	Not supported	Supported	Lower-level NMS only
Operating system	Windows	Windows and Linux	Windows and Linux
Distributed deployment	Not supported	Supported	Supported
Embedded database	Supported	Not supported	Supported only on windows
Remote database server	Not supported	Supported	Supported

The embedded database uses SQL Server 2008 R2 SP2 Express. For information about the database installation procedures, see *SQL Server 2008 R2 Installation and Configuration Guide*.

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

- *SQL Server 2005 Installation and Configuration Guide*
- *SQL Server 2008 Installation and Configuration Guide*
- *SQL Server 2008 R2 Installation and Configuration Guide*
- *SQL Server 2012 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*

- *MySQL 5.5 Installation and Configuration Guide (for Linux)*
- *MySQL 5.6 Installation and Configuration Guide (for Linux)*

Installation and deployment

To improve server performance, IMC uses the Install and Deploy model. IMC Install copies the IMC installation file to the master server and IMC Deploy decompresses the installation package and creates a database script on the master server or subordinate servers as needed.

Before IMC deployment, you must install the target components on the server. The components of IMC are operational only after they are deployed.

IMC automatically creates a database user when a service component is deployed. HP recommends not modifying the database user configuration, including the user's password and password security strategy.

When the deployment or upgrade process is interrupted, IMC automatically stores logs as a compressed file in the **\tmp** directory of the IMC installation path. With the logs, you can quickly locate the problem or error that occurred in IMC deployment or upgrade.

Obtaining IMC installation and deployment methods

Installing IMC on Windows and Linux is similar. This guide uses Windows Server 2008 R2 and the SQL Server 2008 R2 database.

The IMC software is available on the HP website.

2 Preparing for installation

This chapter describes detailed information about the IMC installation requirements for both hardware and software.

Hardware requirements

Tables in this section list the server requirements for the operating system on which IMC is installed. They use the following terms:

- **Node**—IMC servers, database servers, and devices managed by IMC are called "nodes." The **Nodes** column of the tables displays the sum of IMC servers, database servers, and devices managed by IMC.
- **Collection unit**—Represents a performance instance that is collected every 5 minutes. When a performance instance uses another collection interval, it corresponds to a number of collection units calculated with the formula: 5 minutes/instance collection interval in minutes.

  For example, the collection interval is set to 10 minutes for all performance instances. A monitored device contains 1 CPU, 1 memory bar, and 10 interfaces. To collect performance data for CPU, memory, response time, reachability rate, and interface send and receive rates, the total collection units of the device are: (1+1+1+1+(10×2))×5/10=12.
- **CPU**[1]—The frequency of the CPU must be no less than 2.5 GHz.
- **Java heap size**—Maximum memory size to be used by Java processes on the IMC Web Server.

The hardware requirements of IMC vary with the components and networking circumstances. For more information, see the release notes of each component.

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 256 MB or more.
- 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 512 MB or more.
- 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 1 GB or more.
- HP recommends that you set the RAID level to 0. When you want to set the RAID level to 5 or 10, install the proper number of parity disks.

Table 2 Server requirements in a 32-bit Windows operating system

Management scale			System minimum requirements				
Node	**Collection unit**	**Online operator**	**CPU**[1]	**Memory size**	**Java heap size**	**Storage required for installation**	**Storage required for operation**
0 to 200	0 to 5 K	20	2 cores	4 GB	512 MB	3 GB	30 GB
	5 K to 50 K	10					60 GB
200 to 500	0 to 10 K	30	4 cores	6 GB	1 GB	3 GB	50 GB
	10 K to 100 K	10					100 GB

Table 3 Server requirements in a 64-bit Windows operating system

Management scale			System minimum requirements				
Node	Collection unit	Online operator	CPU[1]	Memory size	Java heap size	Storage required for installation	Storage required for operation
0 to 200	0 to 5 K	20	2 cores	4 GB	2 GB	3 GB	30 GB
	5 K to 50 K	10					60 GB
200 to 1 K	0 to 10 K	30	4 cores	8 GB	2 GB	3 GB	50 GB
	10 K to 100 K	10					100 GB
1 K to 2 K	0 to 20 K	30	6 cores	12 GB	4 GB	4 GB	60 GB
	20 K to 200 K	10					200 GB

Table 4 Server requirements in a 32-bit Linux operating system

Management scale			System minimum requirements				
Node	Collection unit	Online operator	CPU[1]	Memory size	Java heap size	Storage required for installation	Storage required for operation
0 to 200	0 to 5 K	20	2 cores	6 GB	512 MB	3 GB	30 GB
	5 K to 50 K	10					60 GB
200 to 500	0 to 10 K	30	4 cores	8 GB	1 GB	3 GB	50 GB
	10 K to 100 K	10					100 GB

Table 5 Server requirements in a 64-bit Linux operating system

Management scale			System minimum requirements				
Nodes	Collection unit	Online operator	CPU[1]	Memory size	Java heap size	Storage required for installation	Storage required for operation
0 to 200	0 to 5 K	20	2 cores	6 GB	2 GB	3 GB	30 GB
	5 K to 50 K	10					60 GB
200 to 1 K	0 to 10 K	30	4 cores	12 GB	4 GB	3 GB	50 GB
	10 K to 100 K	10					100 GB
1 K to 2 K	0 to 20 K	30	6 cores	16 GB	6 GB	4 GB	60 GB
	20 K to 200 K	10					200 GB

Software requirements

Table 6 Software requirements

Item	Requirement	Remarks
Windows		
Operating system	Windows Server 2003 (32bit)	Service Pack 2 is required.
	Windows Server 2003 (64bit)	Service Pack 2 (64-bit) and KB942288 are required.
	Windows Server 2003 R2 (32bit)	Service Pack 2 is required.
	Windows Server 2003 R2 (64bit)	Service Pack 2 (64-bit) and KB942288 are required.
	Windows Server 2008 (32bit)	Service Pack 2 is required.
	Windows Server 2008 (64bit)	Service Pack 2 (64-bit) is required.
	Windows Server 2008 R2	Service Pack 1 is required.
	Windows Server 2012 (64bit)	None
Database	SQL Server 2005 SQL Server 2008 SQL Server 2008 R2 SQL Server 2012	Service Pack 4 is required for SQL Server 2005. Service Pack 3 is required for SQL Server 2008. Service Pack 2 is required for SQL Server 2008 R2. Service Pack 1 is required for SQL Server 2012 These databases can be used for both Standard and Professional editions. Make sure the latest database service packs are installed.
	SQL Server 2008 R2 SP2 Express	The database is the embedded database of Standard and SNS editions.
	MySQL 5.5	None
	MySQL 5.6	None
Linux		
Operating system	Red Hat ProfessionaL Linux Server 5 (32bit)	None
	Red Hat ProfessionaL Linux Server 5 (64bit)	None
	Red Hat ProfessionaL Linux Server 5.5 (32bit)	None
	Red Hat ProfessionaL Linux Server 5.5 (64bit)	None
	Red Hat ProfessionaL Linux Server 5.9 (64bit)	None
	Red Hat ProfessionaL Linux Server 6.1 (64bit)	None
	Red Hat ProfessionaL Linux Server 6.4 (64bit)	None

Item	Requirement	Remarks
Database	Oracle 11*g*	None
	Oracle 11*g* Release 2	None
	MySQL 5.5	None
	MySQL 5.6	None

Setting the Java memory size on 32-bit OS

HP recommends using a 64-bit operating system for the server when simultaneously deploying IMC Platform and service components.

When the server runs a 32-bit operating system, manually modify the assignable memory size of Java after deployment using the following method:

1. Use the editor (such as WordPad in Windows or vi in Linux) to run the **\client\bin\startup.bat** script or the **startup.sh** script on Linux,
2. Replace **set JAVA_OPTS=-server –Xmx512m -Xrs -XX:PermSize=64m -XX:MaxPermSize=386m ...** with **set JAVA_OPTS=-server -Xmx1024m -Xrs -XX:PermSize=64m -XX:MaxPermSize=576m ...**.
3. Save the file and restart the jserver process.
   - When the jserver process cannot start up, decrease the above values until it can start up.
   - When an out of memory error occurs after the jserver process starts up, use a 64-bit operating system.

Installing IMC on a virtual machine

HP recommends installing IMC on a physical server.

You can install IMC on a VMware virtual machine. Before installation, set the path where the virtual machine is located and hardware information including:

- Types and number of CPUs
- Number, models, and MAC addresses of network adapters
- Number and space of disk drives

After you install IMC, do not change the previous configuration or IMC installation path. Although changing them does not affect VM migration, IMC cannot operate properly.

Checking the installation environments

For database installation instructions, see related database documents.

All of the requirements, listed in Table 7, must be met before installation.

CAUTION:

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

Table 7 Installation environments

Item	Requirements
Hardware	Meets the specifications of CPU, memory, and hard disk in the contract.
Software	Make sure the type and version of the operating system and database meet the IMC installation requirements. The server is restarted after database installation.
Auto startup of SQL Server service and SQL Server Agent	Select **Control Panel** > **Administrative Tools** > **Services** and make sure the **Startup Type** items of MSSQLSERVER and SQLSERVERAGENT are set to **Automatic**.
Uninstallation of IMC software	A thorough uninstallation is required when IMC was previously installed on the system. For instructions on removing IMC, see "Removing IMC." Reboot the system after the IMC is uninstalled. To completely remove IMC: • **Windows**: After you remove IMC, locate and delete the **IMC-Reserved** folder in the **WINDOWS** folder of the system disk. • **Linux**: Locate and delete the **IMC-Reserved** folder in the **/etc/** directory.
Firewall settings check	To deploy IMC in centralized mode, open the IMC Web service port and database listening port in the firewall settings. The default Web service port of IMC is 8080 (HTTP) and 8443 (HTTPS). The default database listening port is: • SQL server database: 1433 • Oracle database: 1521 • MySQL database: 3306

Installing Java Runtime Environment (JRE)

Use either of the following methods to install JRE 6.0:

- Method 1:

  Download the program from **http://www.oracle.com/technetwork/java/index.html** and install it.

- Method 2:

  Run the JRE 6.0 setup in the IMC package as follows:

  a. On the subordinate server, launch the Web browser and enter **http://192.168.4.44:8080/imc** (192.168.4.44 is the IP address of the master server, and 8080 is the HTTP port number) in the address bar.

  b. On the login page, enter the username and password.

  c. Click **Login** to enter the **Home** tab.

  d. Select the **System** tab and click **Deploy Components**.

  e. Click **When fail to start Remote Installation Wizard, download and install JRE**.

  f. In the popup **jre.exe** file download window, click **Save** or click **Run**.

IMPORTANT:

- Make sure you have installed a 64-bit browser and 64-bit JRE on Windows Server 2008 R2 SP2 (64bit). Otherwise, IMC errors might occur.
- To use Firefox for accessing IMC on Linux, install JRE 6.0 or JDK first. For more information, see "12 FAQ."

Checking installation environments

IMC installation package provides a tool to check the system environments, database connectivity, and database installation environments.

The system environments check includes:

- Whether or not the service port to be used by IMC is idle. If it is used by another program, you must remove that program or modify the service port of that program.
- Physical memory is at least 2 GB.
- Whether or not database software is installed.

The database connectivity check requires you to enter various parameters for test. For example, if you are using a SQL Server database, the tool requires you to enter the following parameters:

- **Database Type**—Select the database type, SQL Server, MySQL, or Oracle.
- **Instance Name**—Use the default instance or select **Other Instance** to specify a user-defined instance.
- **Superuser**—Enter the database superuser name, default name **sa** or another account who has the superuser privileges.
- **Password**—Enter the password of the superuser.
- **Database Location**—Select the location of the database server from the list, **local host** or **other server**.
- **Database Server Address**—Enter the IP address of the database server. This field is editable only when **other server** is selected as the database location. Otherwise, this field displays **127.0.0.1**.
- **Listening Port**—Enter the listening port of the database server. The default is **1433**.
- **Installation Location**—Enter or browse to the local directory where the IMC installation package is stored.
- **Data File Location**—Enter or browse to the local or remote directory where the database files are stored. If a remote database server is used, make sure the directory already exists on the database server, and IMC will verify the read and write access to that directory.
- **HTTP Port**—Enter the HTTP port number. The default is 8080.
- **HTTPS Port**—Enter the HTTPS port number. The default is 8443.

The database installation environments check includes the following items:

- Whether or not IMC supports the operating system version and patches.
- Whether or not .Net Framework 2.0 SP2 is installed.
- Free disk space is at least 512 MB.

To check the IMC installation environments:

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

2. Run the tool.

   The tool starts to check the system environments. If the check is passed, the system tests the database connectivity in the **Checking Installation Parameters** window or tests the installation environments for installing the embedded database.

3. View the check result.

   If not all check items are passed, adjust your installation environments and run the tool again.

4. Click **Exit**.

Superuser

IMC installation requires you to enter a superuser account to test the database connectivity. You can use the default superuser account **sa** (for SQL Server) or enter another account who has the superuser privileges.

IMC uses this superuser account to create database files and user accounts for IMC Platform subcomponents and service components during deployment. After deployment, IMC Platform subcomponents and service components use their respective user accounts to for database access, instead of using the superuser account.

If the password of the superuser account has changed since IMC deployment, update the password by clicking **Change Password** on the **Environment** tab of the Intelligent Deployment Monitoring Agent. Otherwise, you cannot view database information on the **Environment** tab, deploy new components, or update existing components.

Checking the system time

Before installing IMC, check that the system time, date, and time zone settings on the server are correct. When the settings on the server are incorrect, you need to adjust the settings.

After IMC is started, do not modify the system time of the server; otherwise, the following or other intermittent problems can occur.

- When you modify the system time to a future time that differs from the current time, the system can take a long time to process a large amount of data. It can exceed the maximum time that the data can be saved in the database.

  This affects the current data sampling speed and results in delay. After the processing of such data is complete, the delay is gradually recovered.

- When you modify the system time to a past time, data with overlapping time can occur, and data processing might become abnormal. After the overlapping time is past, data processing becomes normal again.

Setting the time zone

Before installing IMC in the Windows Server 2008 R2 operating system, deselect **automatically adjust clock daylight saving changes** when you set the time zone in the **Date & Time** window.

3 Installing SQL Server 2008 R2

To deploy IMC in centralized mode and use a local database, you must install and configure the database on IMC server. This chapter describes how to install and set up SQL Server 2008 R2 SP2. For instructions on installing other databases, see the related documents.

Installing the SQL Server 2008 R2

1. Run the setup program.

   The **SQL Server Installation Center window** appears.

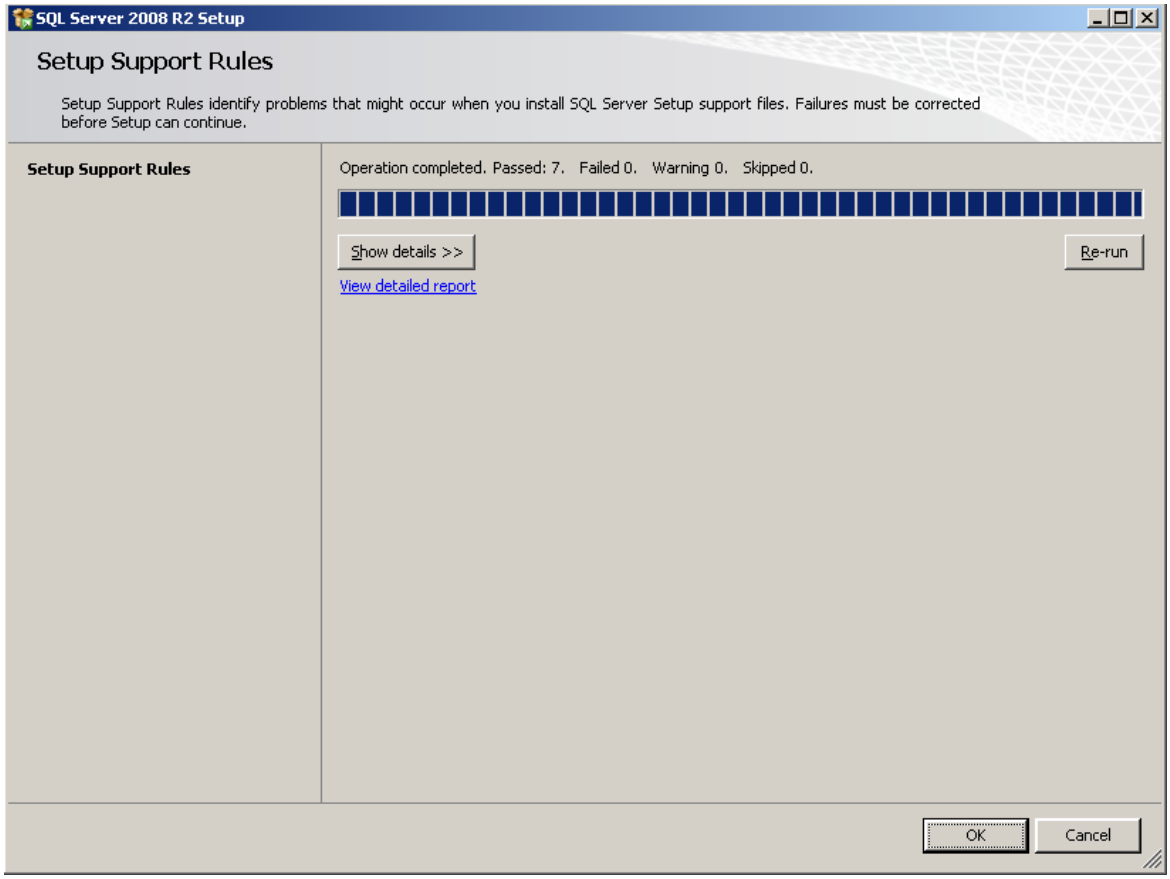
Figure 1 SQL Server Installation Center window

2. Select **Installation** from the navigation tree and click **New installation or add features to an existing installation**.

   The **Setup Support Rules** page appears, as shown in Figure 2.

   The system runs a check to identify problems that might occur when you install SQL Server Setup support files.

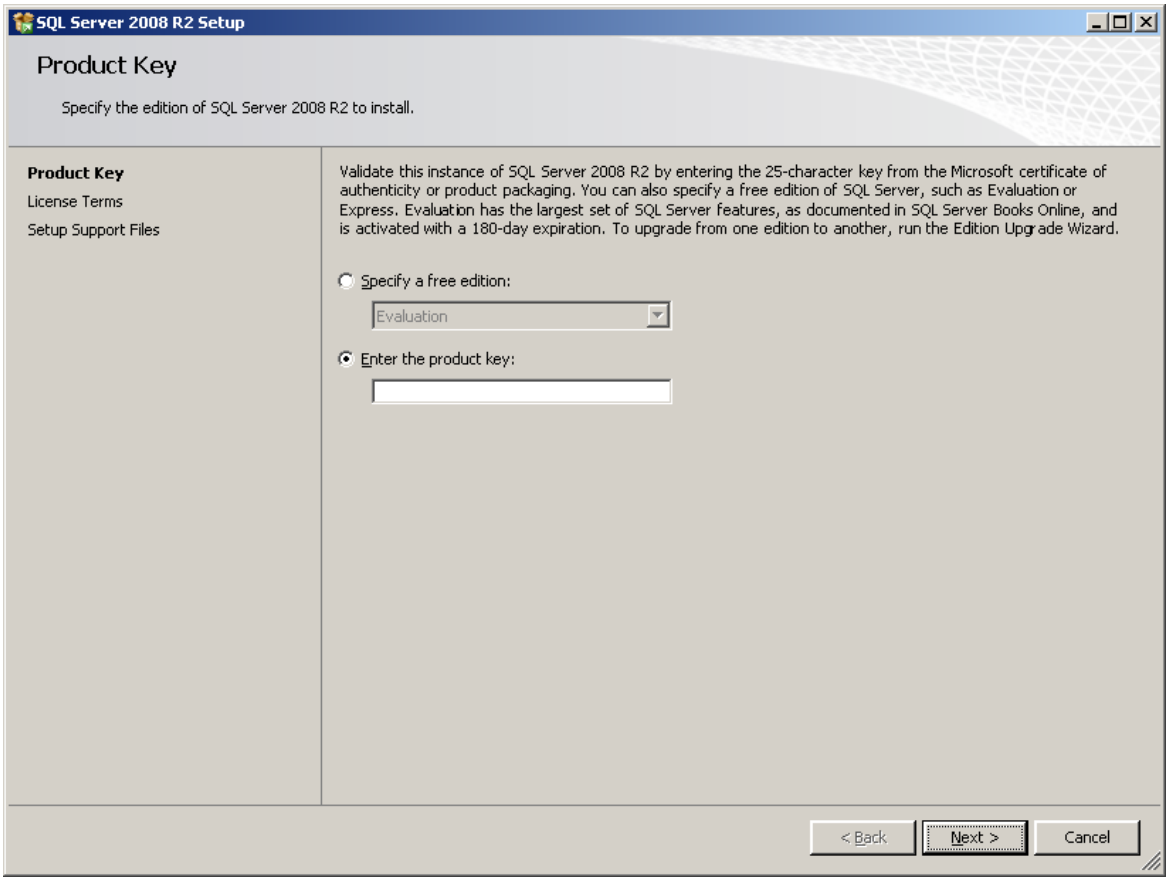
Figure 2 Setup Support Rules page



3. After the check is passed, click **OK**.

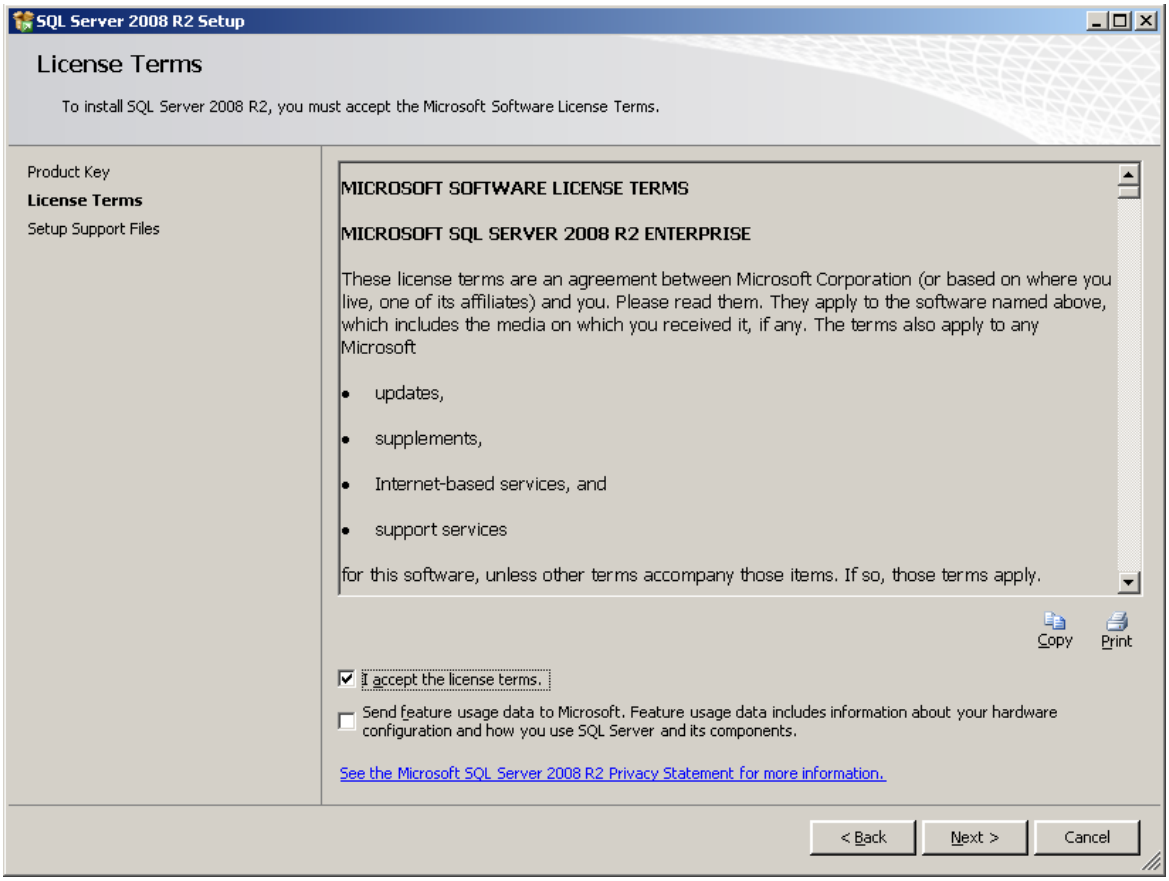
   The **Product Key** page appears.

Figure 3 Product Key page



4. Enter the product key and click **Next**.
   The **License Terms** page appears.

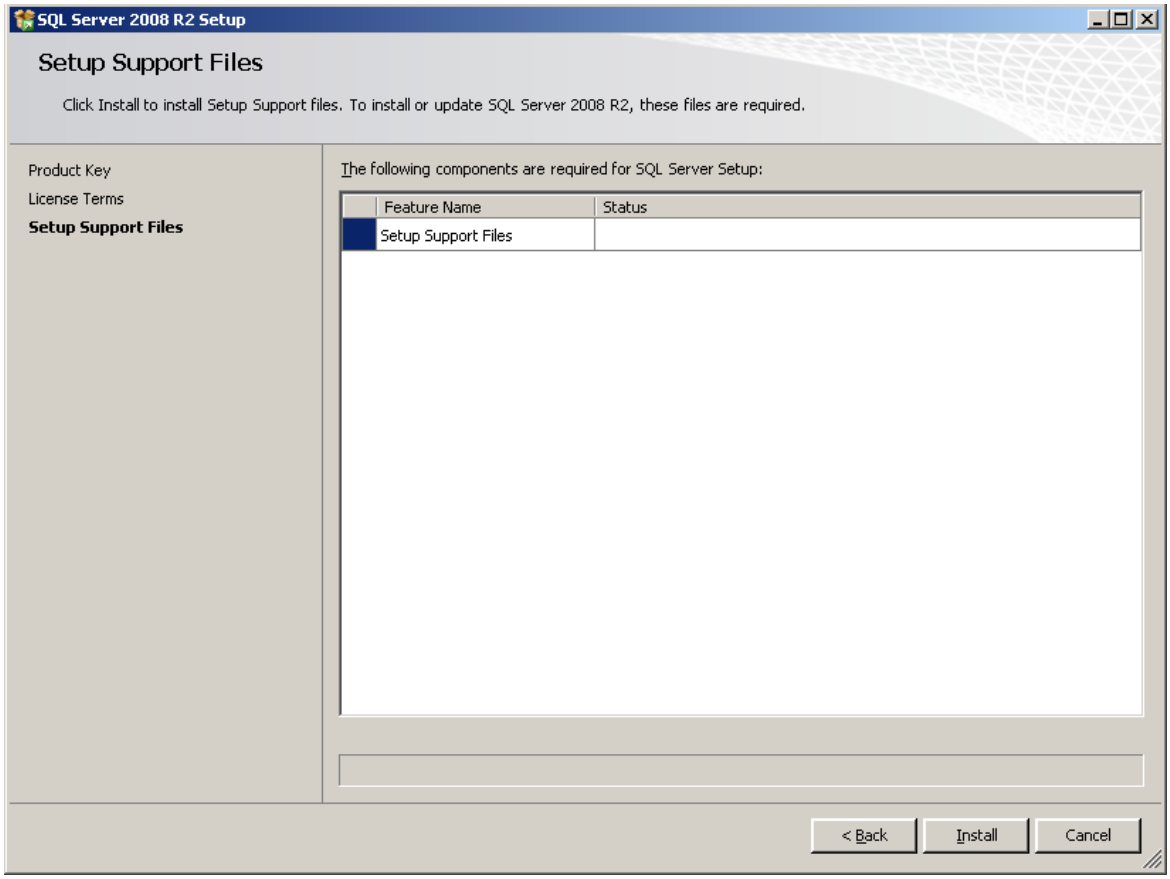
Figure 4 License Terms page



5. Select **I accept the license terms** and click **Next**.

   The **Setup Support Files** page appears.

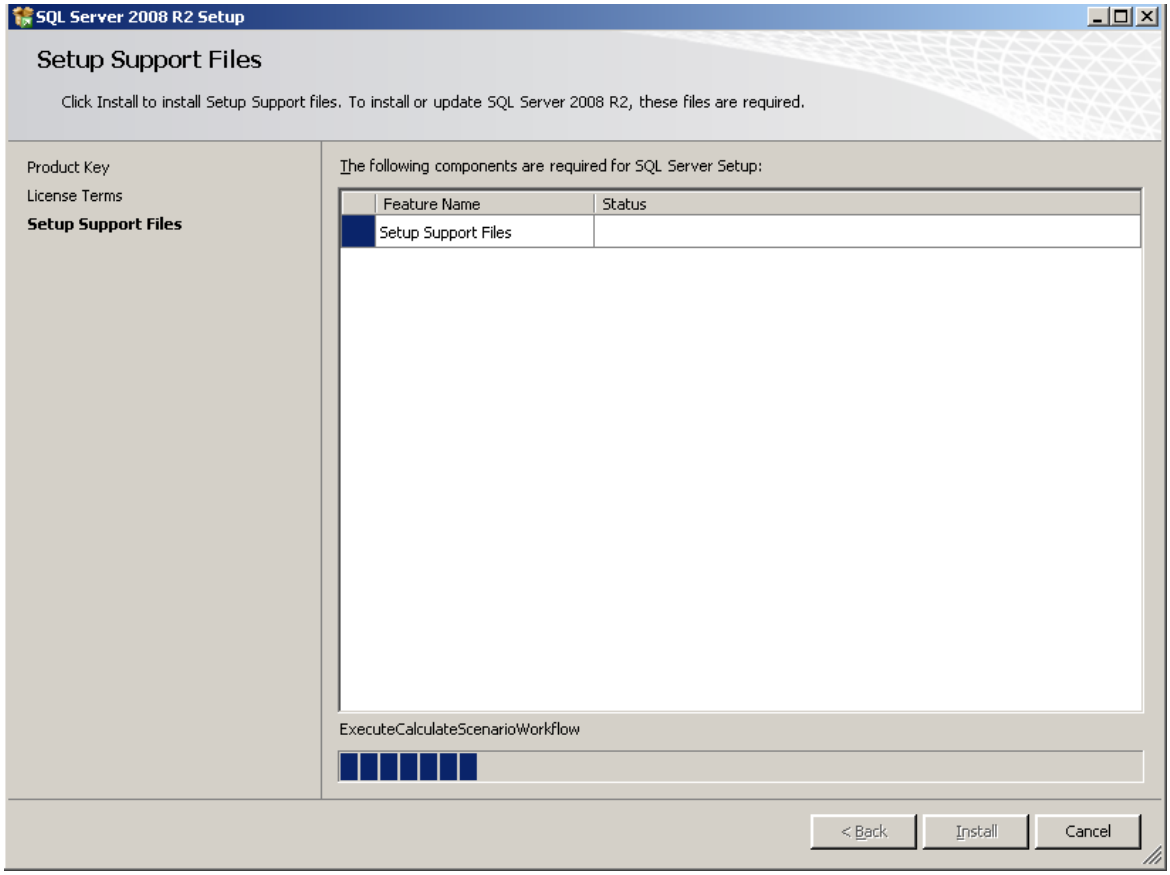
Figure 5 Setup Support Files page



6. Click **Install** to start installing setup support files.

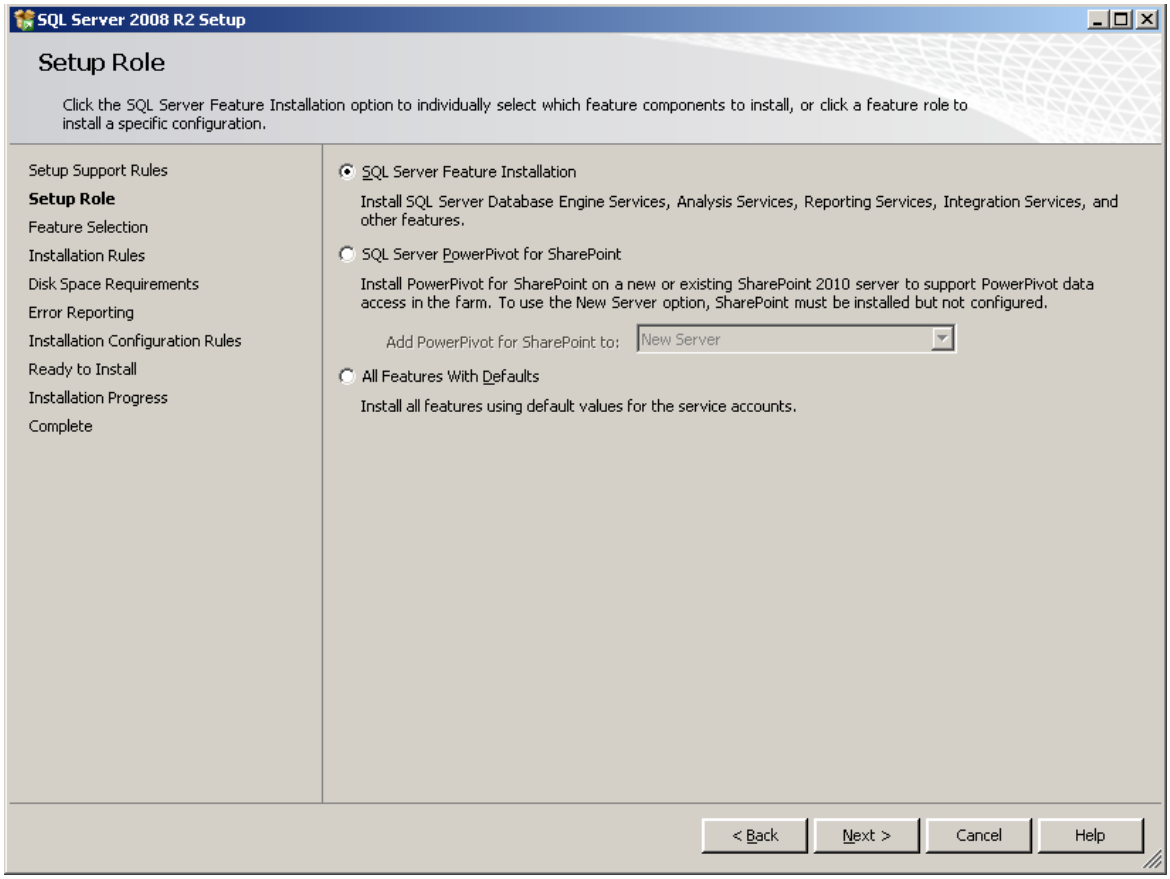
   The **Setup Support Files** page appears.

Figure 6 Setup Support Files page



Upon completion of the installation, the **Setup Role** dialog box appears.

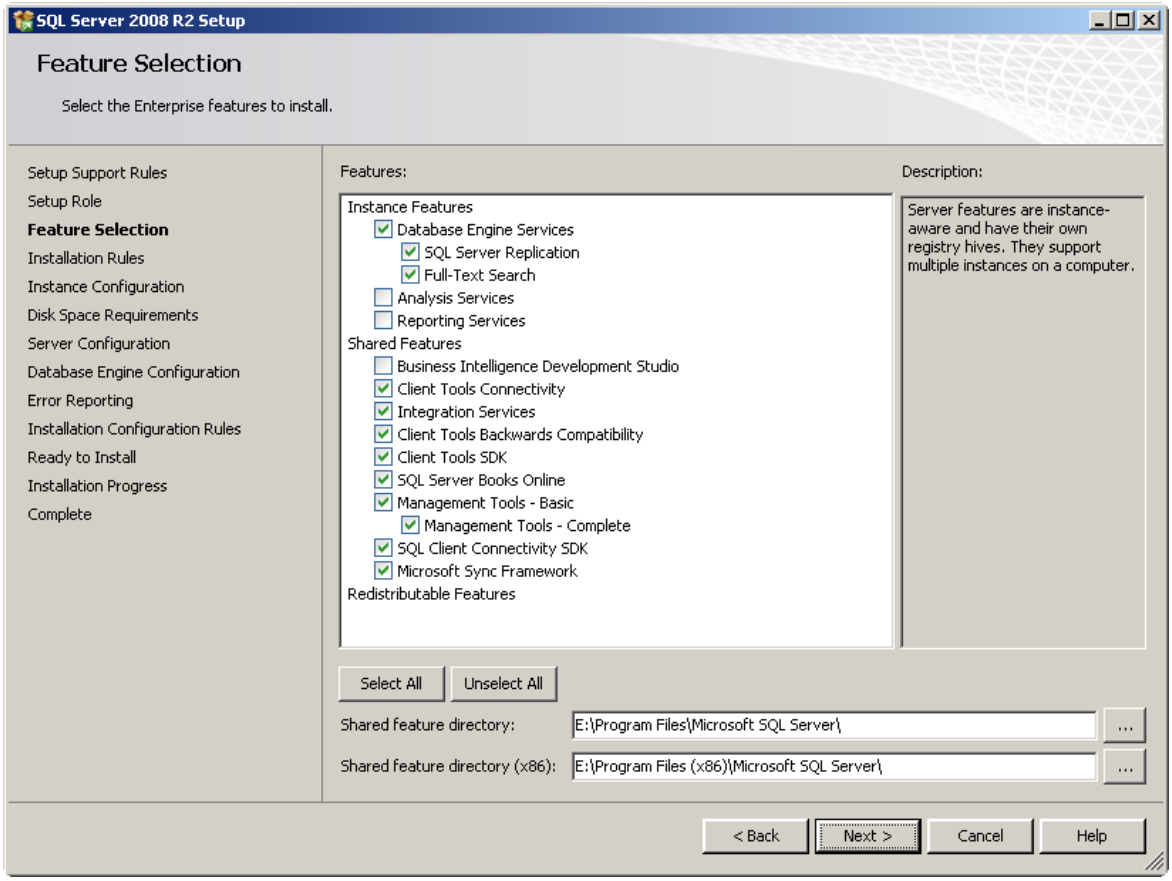
Figure 7 Setup Role page



7. Select **SQL Server Feature Installation** and click **Next**.

   The **Feature Selection** page appears.

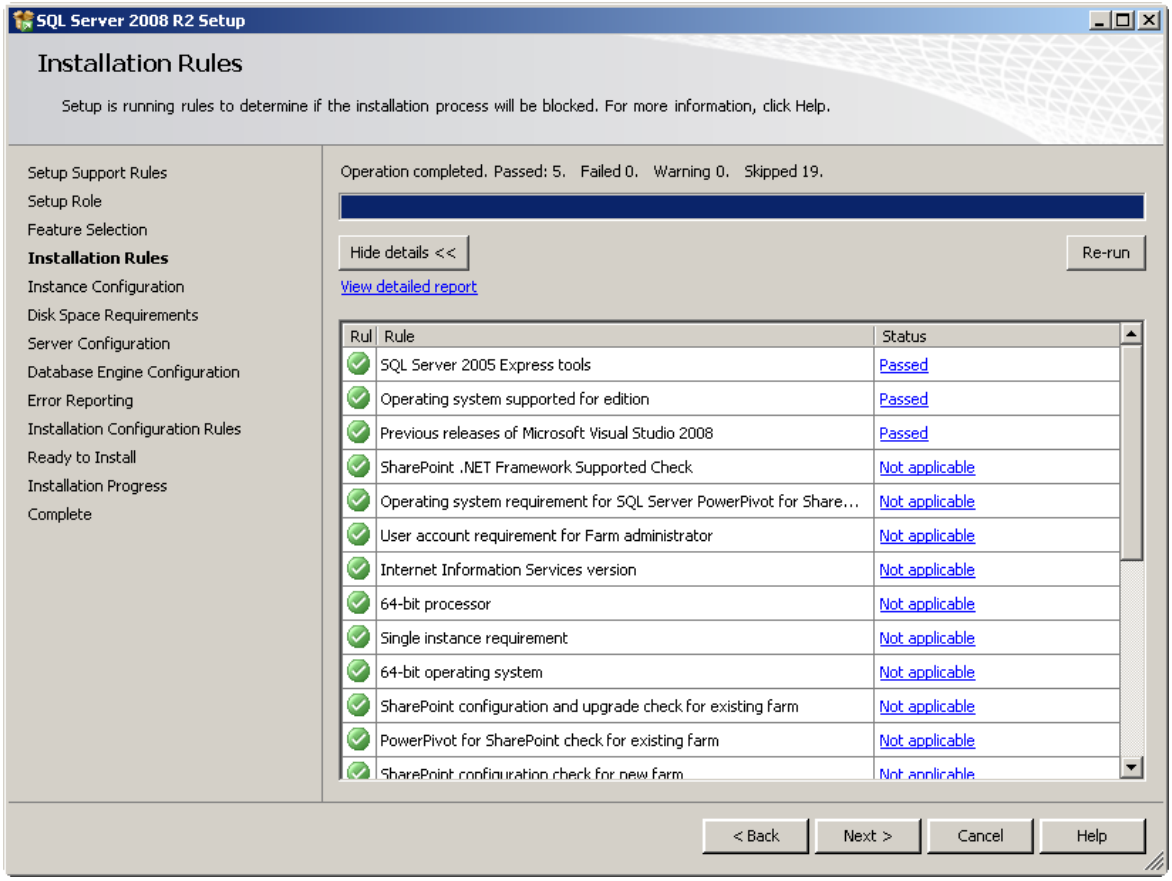
Figure 8 Feature Selection page



8. Select the features you want to install and click **Next**.

   The **Installation Rules** page appears.

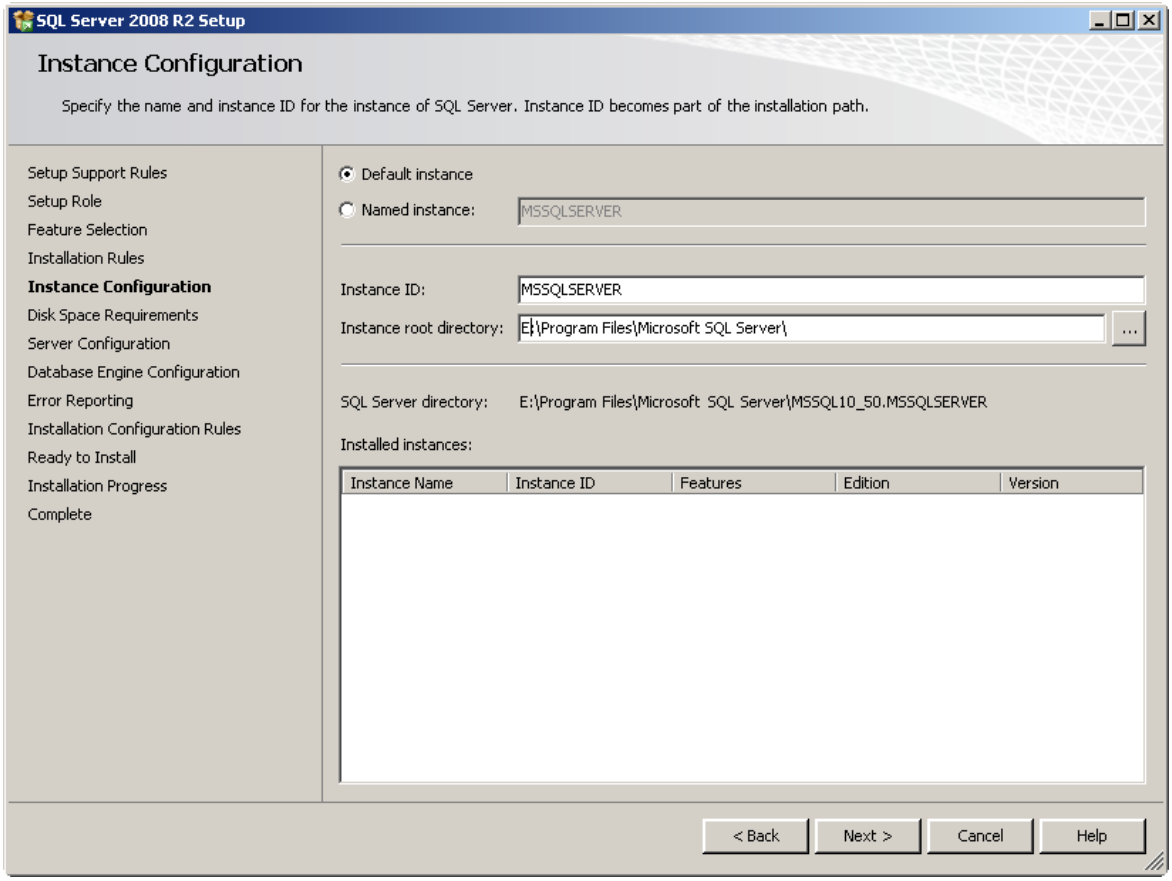
Figure 9 Installation Rules page



9. Click **Next**.

   The **Instance Configuration** page appears.

Figure 10 Instance Configuration page



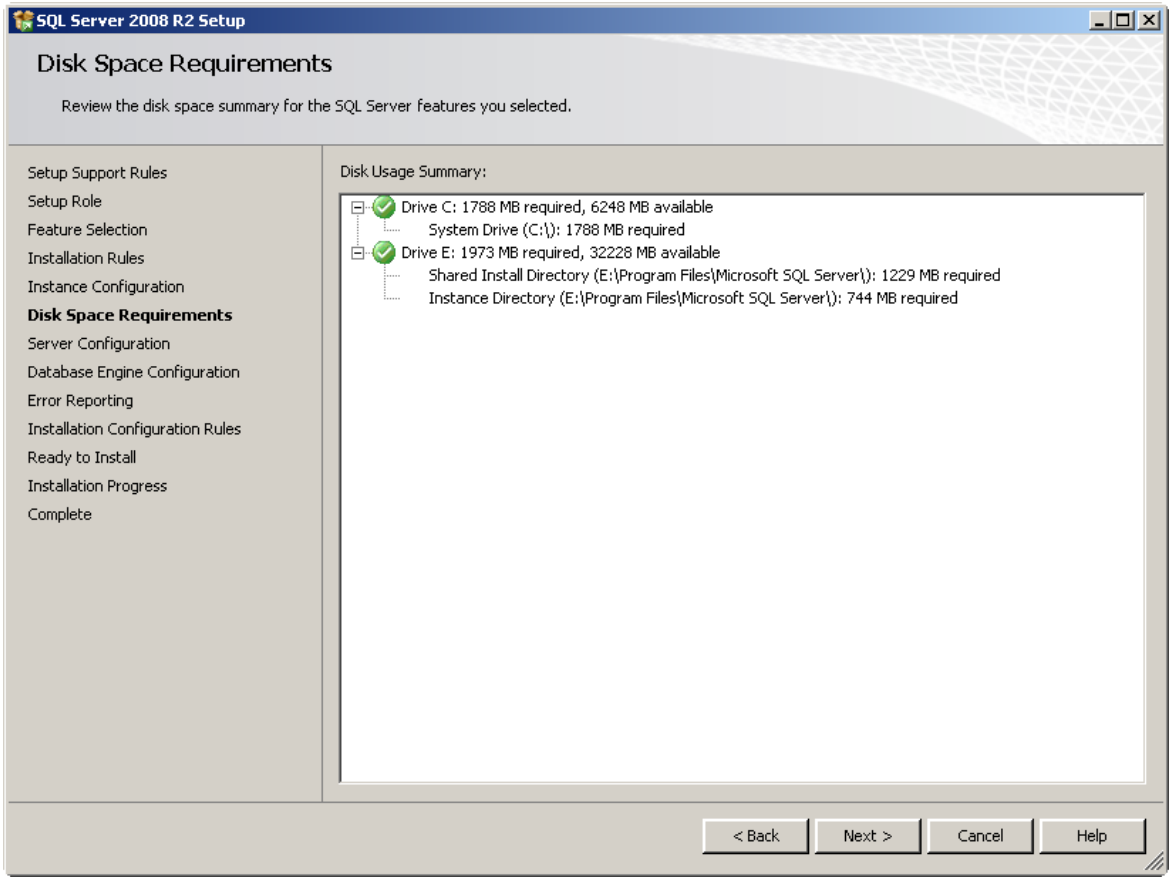
10. Select **Default instance** and use the default instance **MSSQLSERVER**. Do not modify the default instance ID.

    An advanced user can select **Named instance** and enter a custom instance ID. For more information about the installation procedure, see *SQL Server 2008 R2 Installation and Configuration Guide*.

11. Click **Next**.

    The **Disk Space Requirements** page appears.

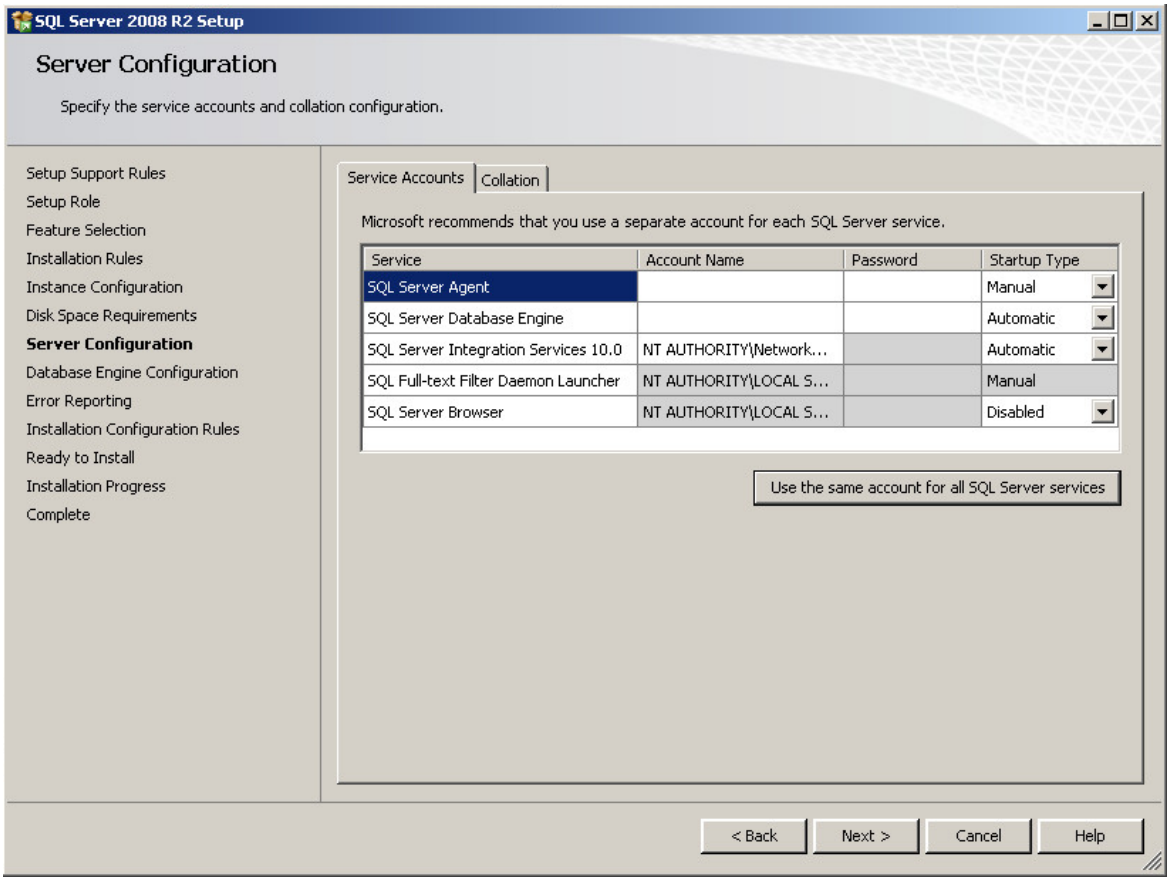
Figure 11 Disk Space Requirements page



12. Click **Next**.

    The **Server Configuration** page appears.

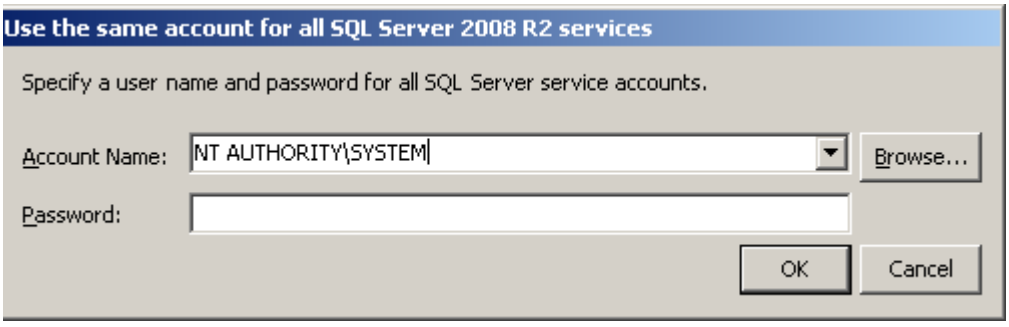
Figure 12 Server Configuration page



13. Click **Use the same account for all SQL Server services**.

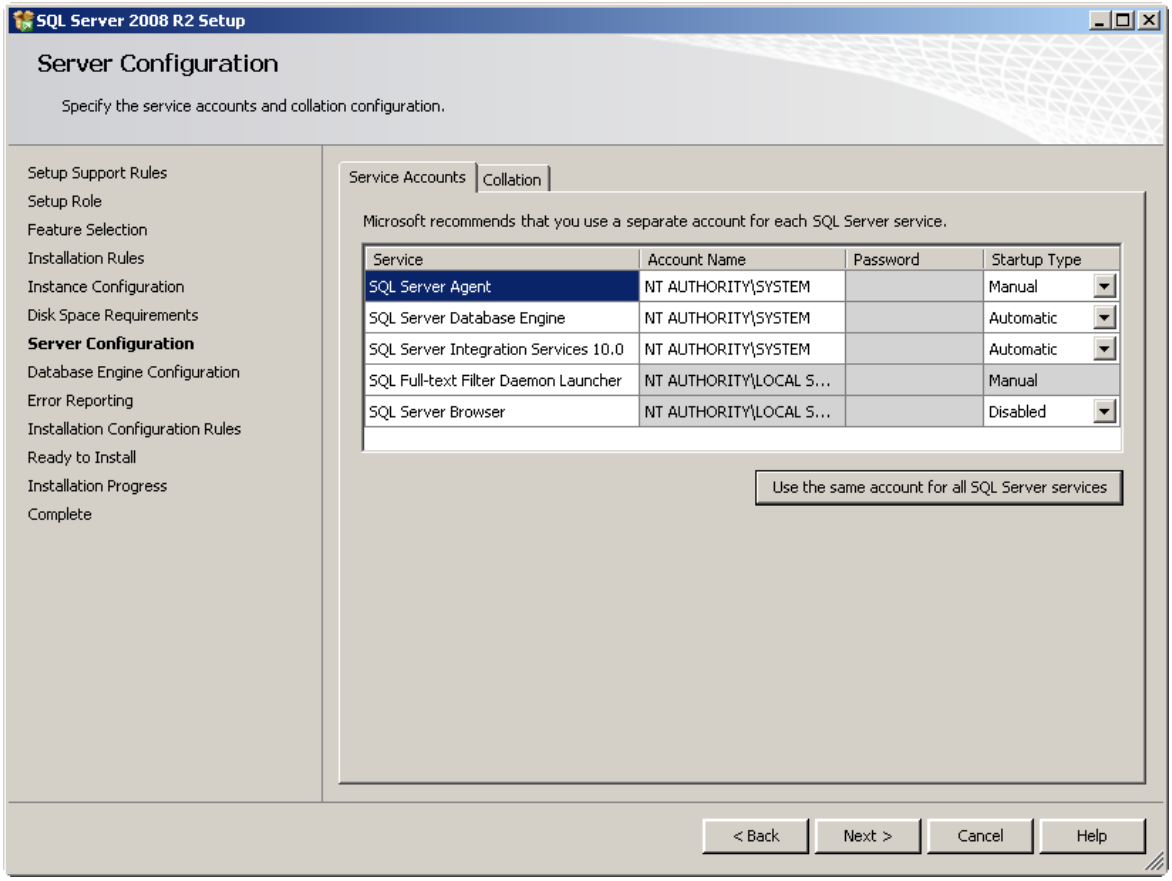
    The **Use the same account for all SQL Server 2008 R2 services** page appears.

Figure 13 Use the same account for all SQL Server 2008 R2 services page



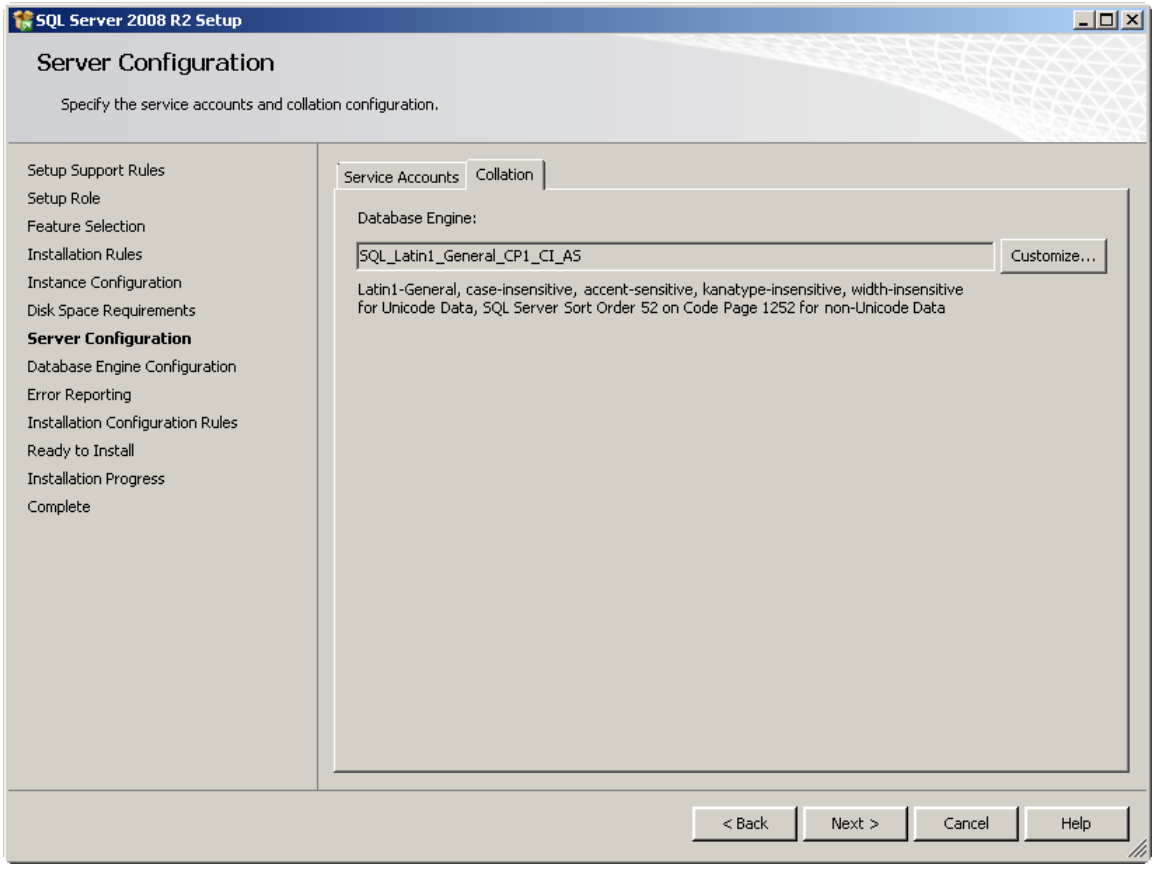
14. Specify the account name and password and click **OK** to go back to the **Server Configuration** page.

Figure 14 Server Configuration page



15. Click the **Collation** tab.

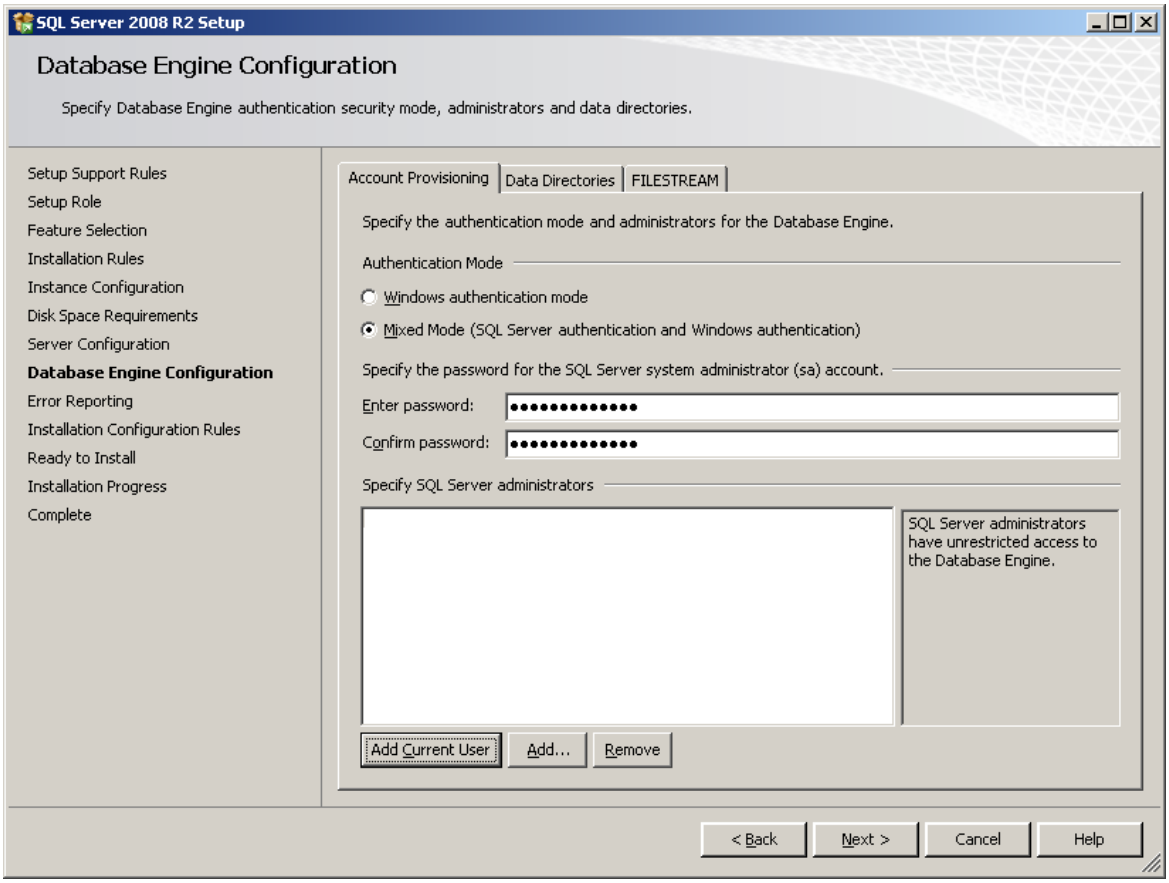
Figure 15 Collation tab page



16. Use the default settings and click **Next.**

    The **Database Engine Configuration** page appears.

Figure 16 Database Engine Configuration page



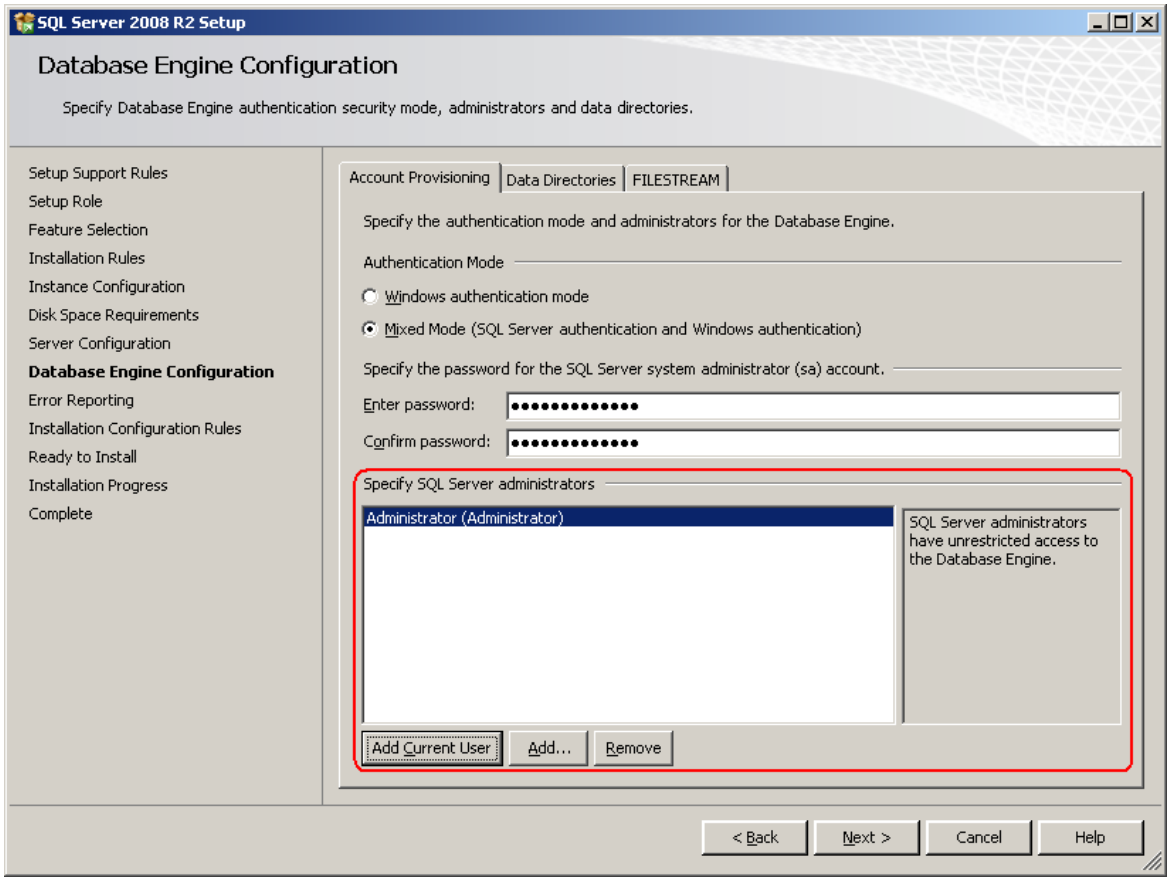
17. In the **Authentication Mode** area, select **Mixed Mode**, and set the password for user **sa**, and add an SQL Server administrator, as shown in Figure 17.

    SQL Server 2008 R2 has password complexity requirements. For information, see the online help on SQL Server 2008 R2.

    For IMC to correctly identify the **sa** logon password during installation, make sure the password does not contain any of the following characters: left bracket (<), right bracket (>), vertical bar (|), and \t.

    If you do not want to change the password of the **sa** user, create a user with **sa** user privileges and make sure the password does not contain any of the previous characters. For more information about creating a database user, see *SQL Server 2008 R2 Installation and Configuration Guide*.

Figure 17 Specifying SQL Server administrators



18. Use the default settings of the **Data Directions** (Figure 18) and the **FILESTREAM** tab (Figure 19).

Figure 18 Data Directories tab page

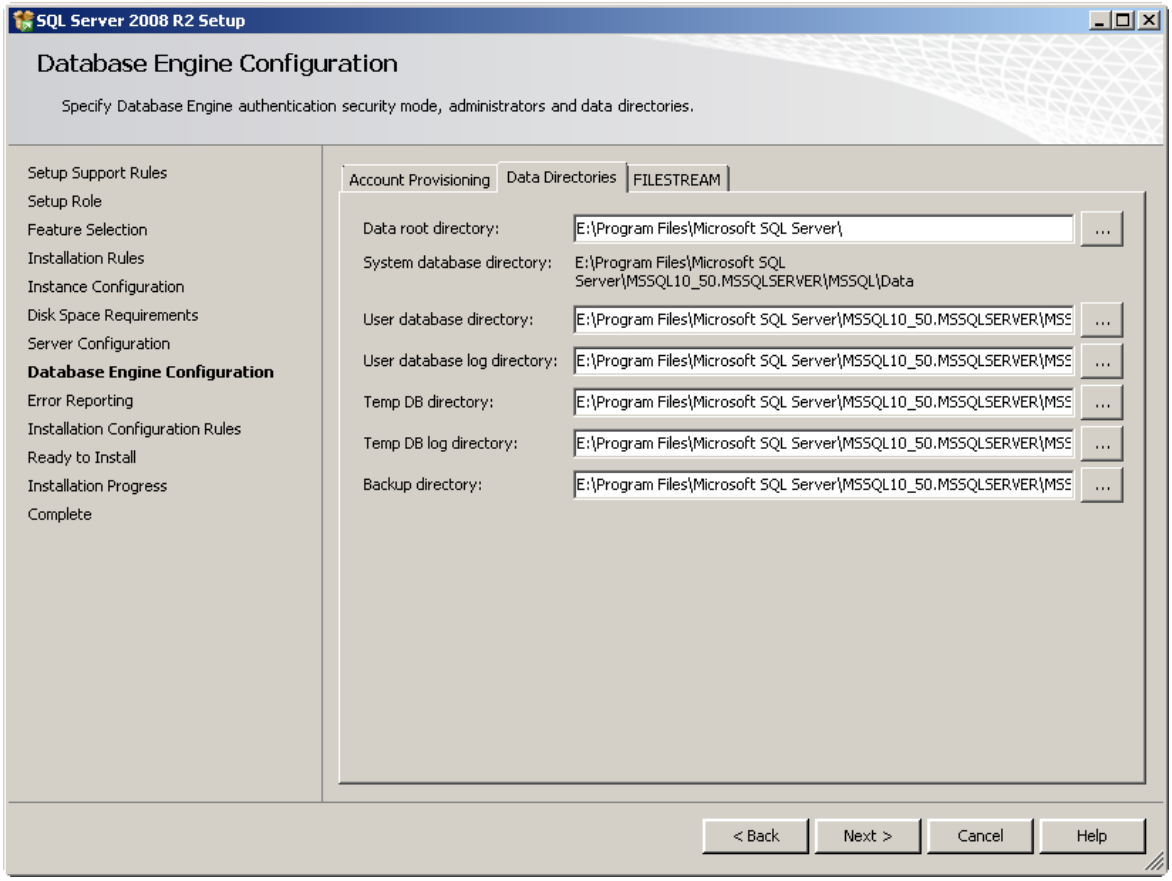
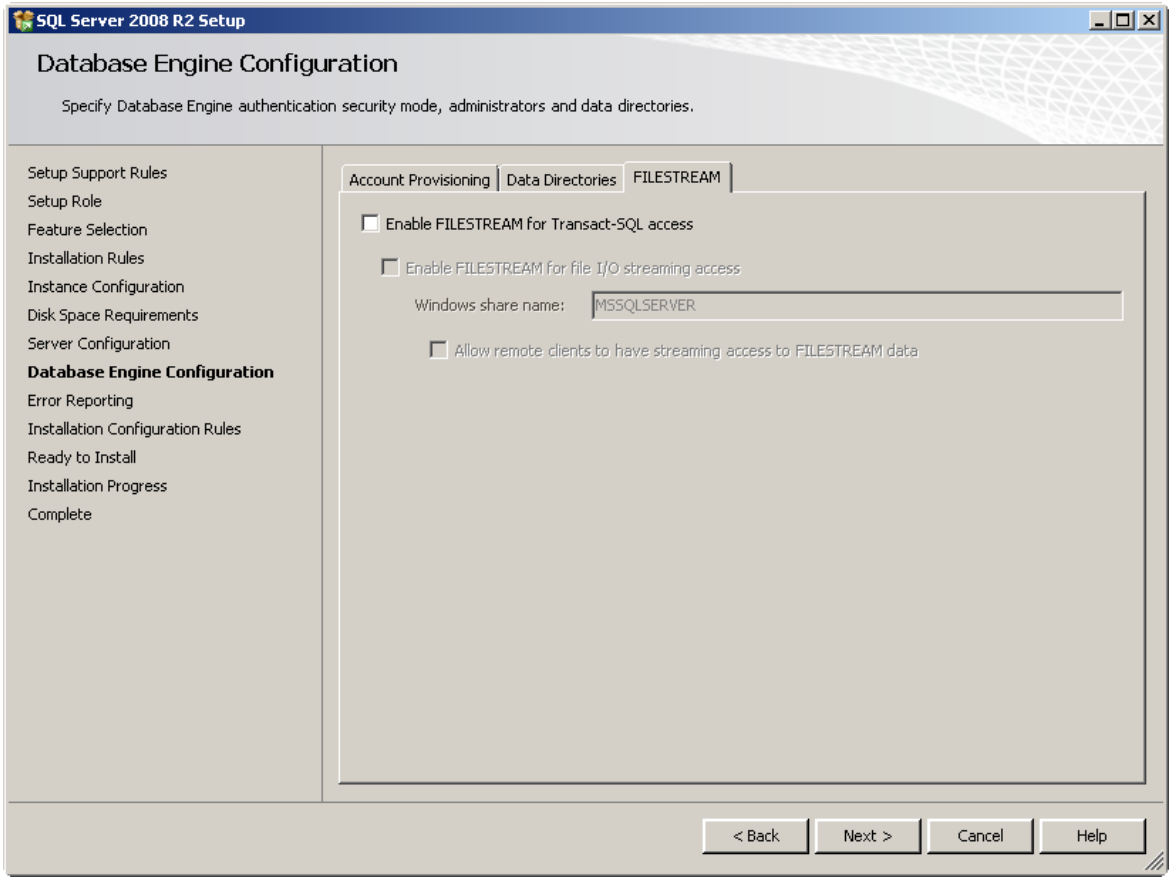


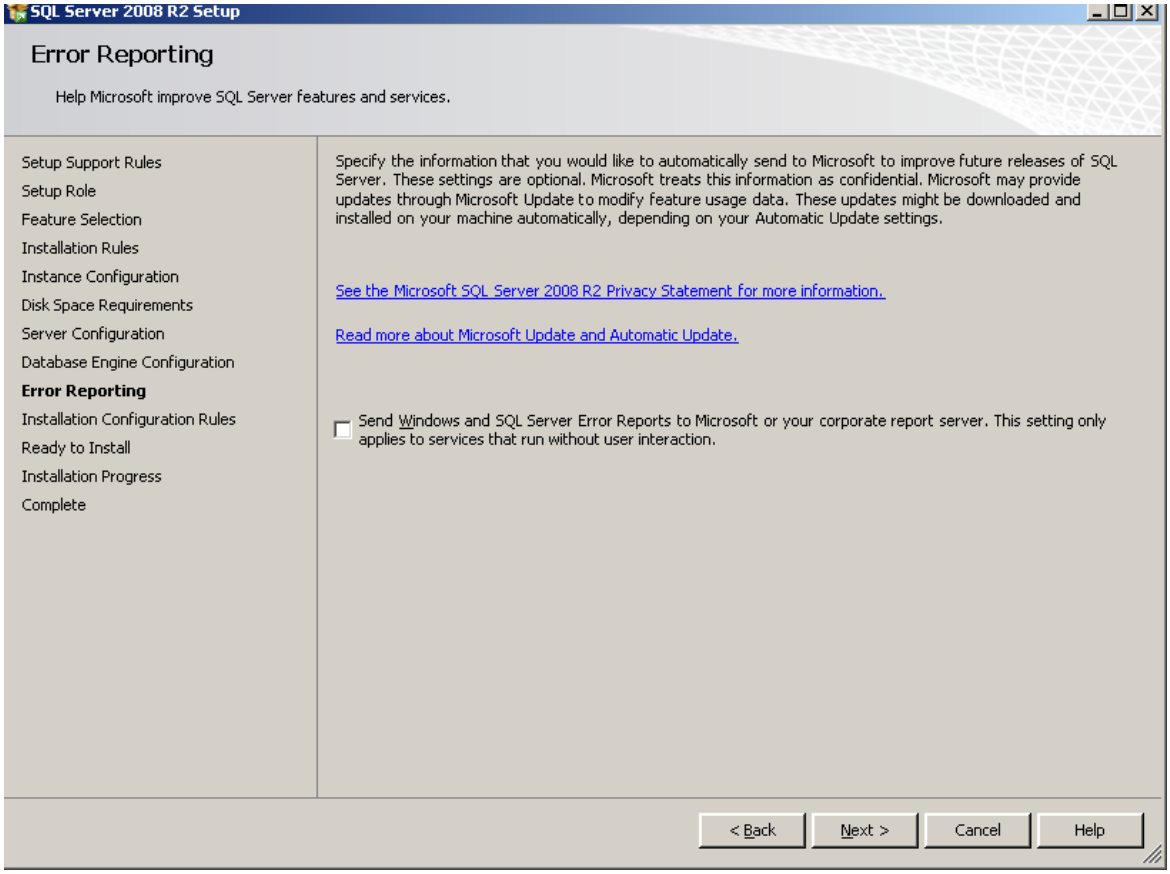
Figure 19 FILESTREAM tab page



19. Click **Next**.

    The **Error Reporting** page appears.

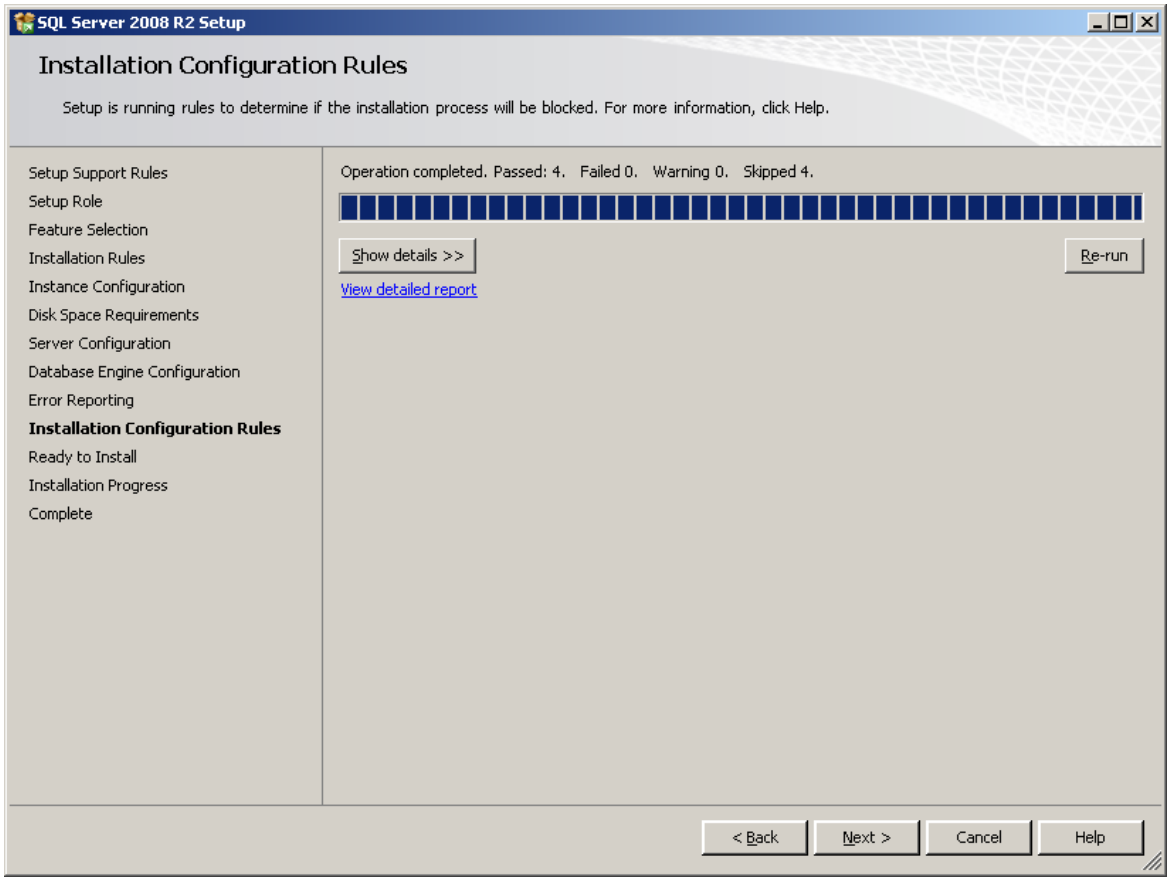
Figure 20 Error Reporting page



20. Click **Next**.

    The **Installation Rules** page appears.

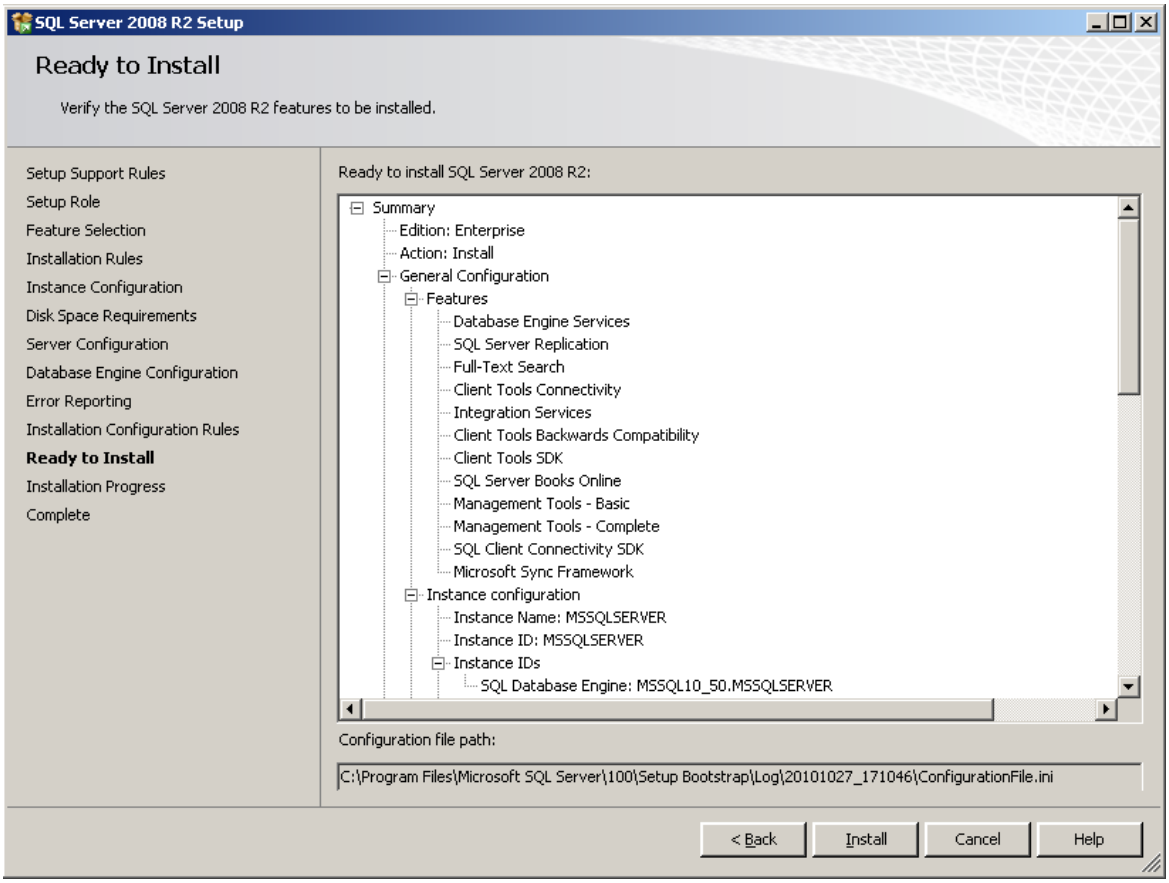
Figure 21 Installation Rules page



21. Click **Next**.

    The **Ready to Install** page shows a tree view of installation options that were specified during Setup.

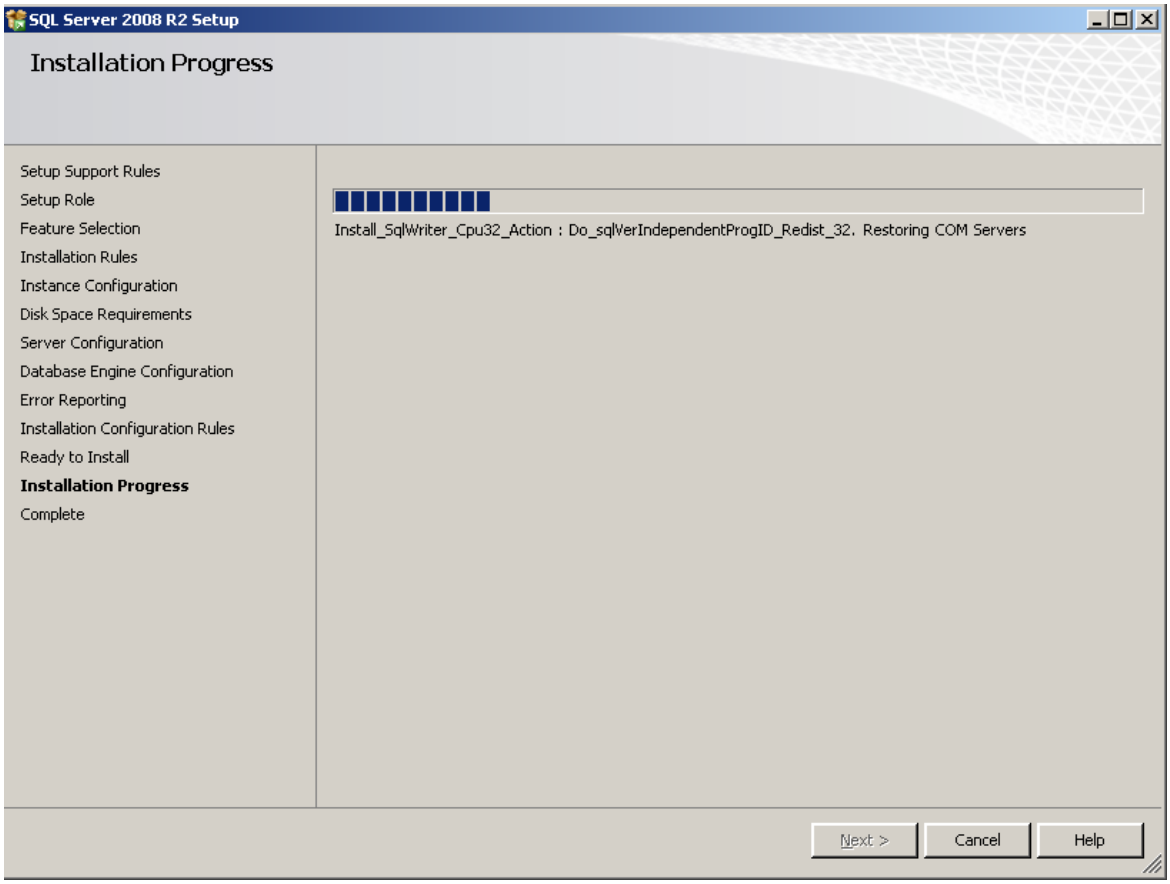
Figure 22 Ready to Install page



22. To continue, click **Install**.

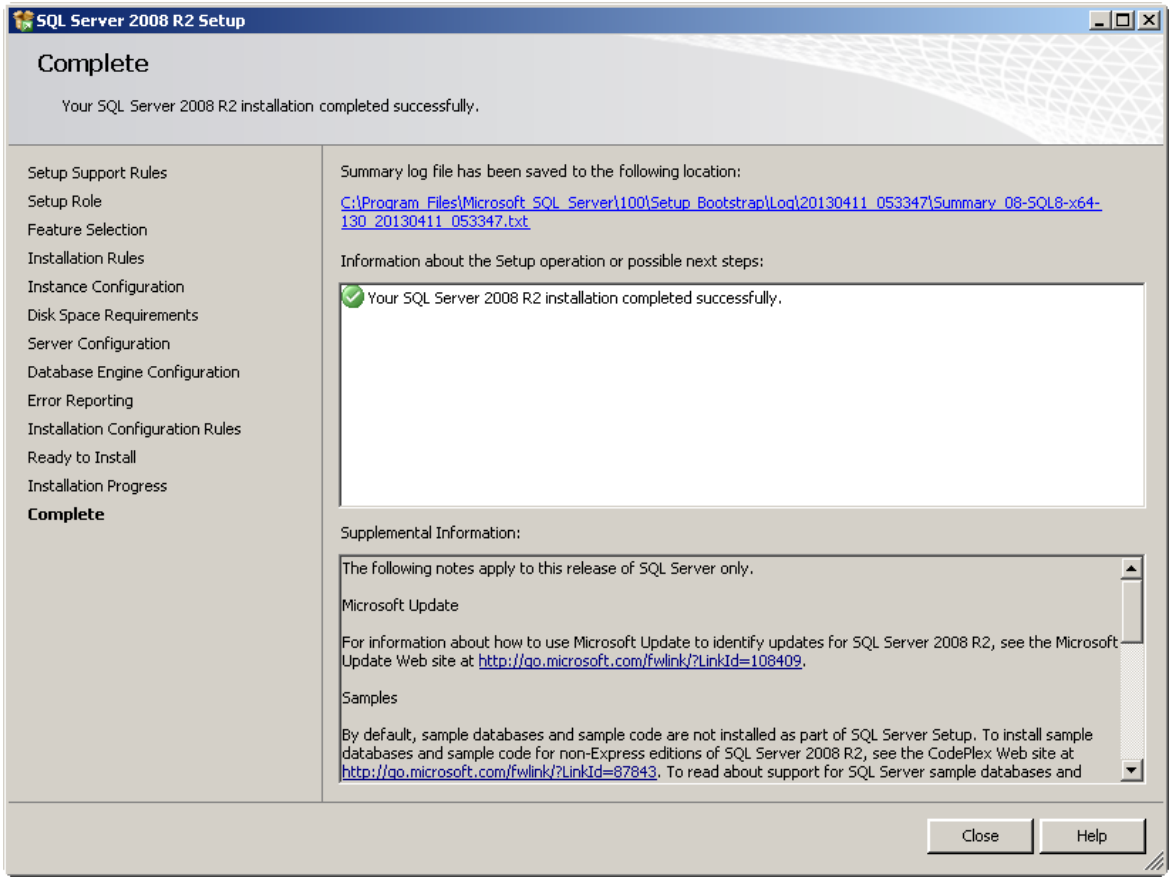
    The **Installation Progress** page appears.

Figure 23 Installation Progress page



23. After installation, the **Complete** page provides a link to the summary log file for the installation and other important notes, as shown in Figure 24.
24. Click **Close**.

Figure 24 Complete page



Configuring TCP/IP properties for SQL Server 2008 R2

After you finish the database installation, configure the TCP/IP properties for the database.

1. Select **Start** > **All Programs** > **Microsoft SQL Server 2008 R2** > **Configuration Tools** > **SQL Server Configuration Manager**, as shown in Figure 25.

   The **SQL Server Configuration Manager** page appears, as shown in Figure 26.

Figure 25 SQL Server Configuration Manager

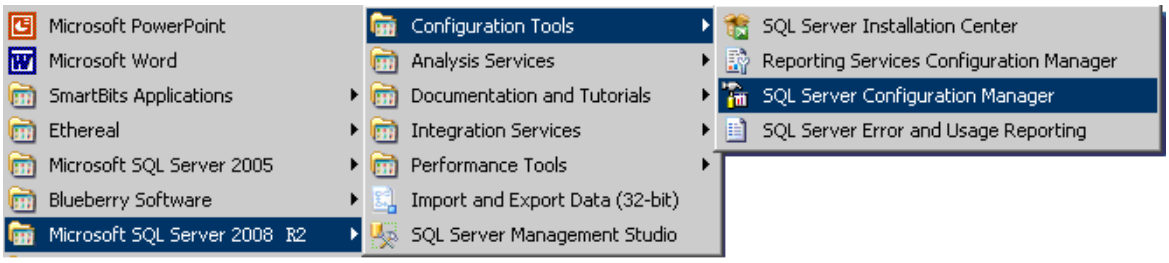
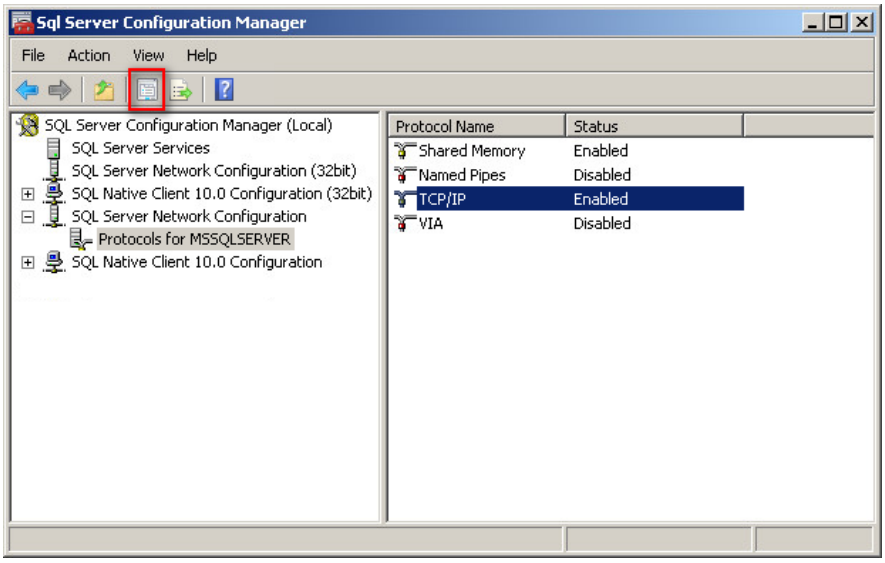


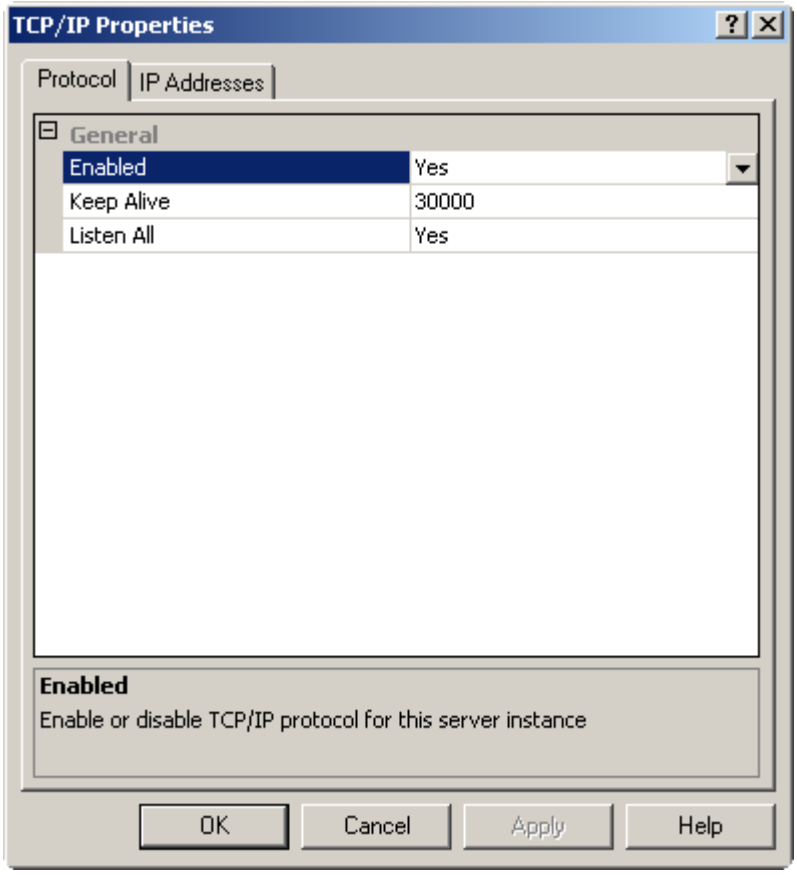
Figure 26 SQL Server Configuration Manager window



2. In the **SQL Server Configuration Manager** window, select **SQL Server Network Configuration** > **Protocols for MSSQLSERVER** from the navigation tree, and then double-click **TCP/IP** on the main pane, or you can select **TCP/IP** and click the **Properties** icon on the toolbar.

   The **TCP/IP Properties** dialog box appears.

Figure 27 Configuring TCP/IP properties

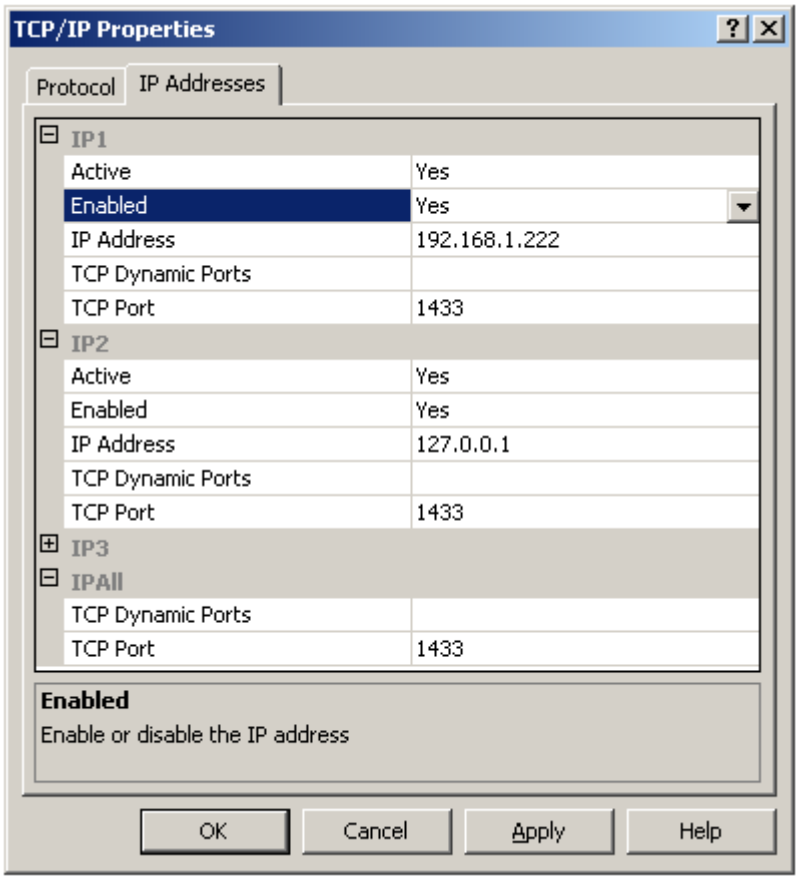


3. On the **Protocol** tab, make sure **Yes** is selected for **Listen All**.

4. Click the **IP Address** tab, select **Yes** for the **Enabled** option of each IP address, and set **TCP Port** to 1433 (the default setting). Make sure the **TCP Dynamic Ports** field is null for IPAll and each IPn (such as IP1, IP2, IP3, etc), as shown in Figure 28.

   You can also specify another TCP port, but you must make sure the specified ports are open in the firewall settings and are not being used by another services.

Figure 28 Configuring IP addresses for TCP/IP



5. Click **OK** to save the configuration.

   The following message appears:

   Any changes made will be saved; however, they will not take effect until the service is stopped and restarted.

6. Click **OK**.

Restart the SQL server to validate the configuration.

NOTE:

- If you did not select **Yes** for **Listen All** on the **TCP/IP Properties** dialog box, enter the dialog box to update the previously-configured IP addresses if the server IP address changes after installing SQL Server 2008 R2. Otherwise, you cannot connect to the database.
- The master and subordinate servers must use the same listening port.

4 Installing and deploying the IMC Platform

After the database installation is complete, you can start installing and deploying the IMC Platform.

The following information describes the installation and recommended deployment schemes of the IMC Platform.

Installing the IMC Platform

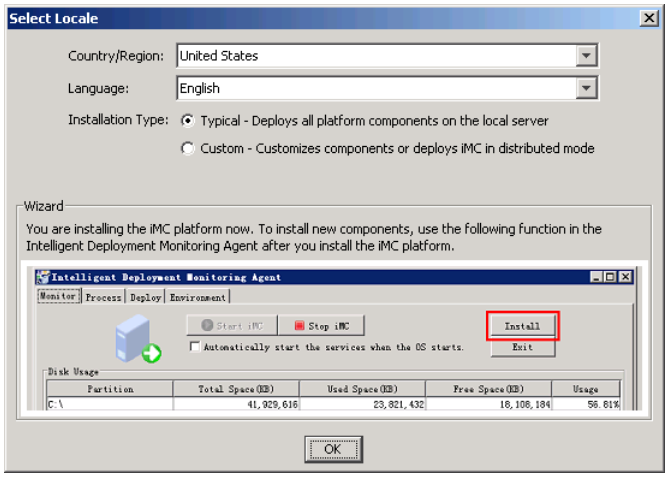
To install the IMC Platform:

1. Log in to the operating system as a user with administrator privileges.
2. Decompress the installation file.
3. Run the **install\install.bat** script in the downloaded installation package to install IMC. A window will appear, as shown in Figure 29.

When you are using other Windows server operating systems or Linux, follow these guidelines:

- To install IMC in Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator.
- To install IMC in Windows Server 2008 or Windows Server 2008 R2, right-click the **install.bat** script and select **Run as Administrator** from the shortcut menu, or modify the **User Account Control Settings** and restart the OS. After installing IMC, you can restore the related settings as needed.
- To modify the user account control settings, click **Start** > **Control Panel** > **System and Security. C**lick **Change User Account Control Settings** in the **Action Center. Se**t the **Choose when to be notified about changes to your compute**r to **Never notify** in the **User Account Control Settings** window.
- To install IMC on Linux except Red Hat Linux 6, start the IMC installation wizard by running the **install.sh** script in the downloaded installation package as a root user.
- To install IMC on Red Hat Linux 6, copy all installation files from the IMC installation DVD to the local server and run the **install.sh** script on the local server.
- When the installation file is obtained via FTP, you must first authorize the **install.sh** script by executing **chmod –R 775 install.sh** in the directory of the script.

Figure 29 Select Locale



4. Select a country/region, language, and installation type

IMC supports typical and custom installation.

- **Typical installation**—Allows you to quickly install and deploy all platform components on the master server. Before performing the typical installation, you must first configure the installation parameters, such as database connectivity, installation location, and Web service port numbers. Typical installation applies to centralized deployment. All subcomponents of the IMC Platform must use a local database, embedded or separate.
- **Custom installation**—Allows you to select certain platform components to install and deploy on the master server and specify a remote database server. This installation method is available for both local and remote databases.

The following sections describe the two installation types separately.

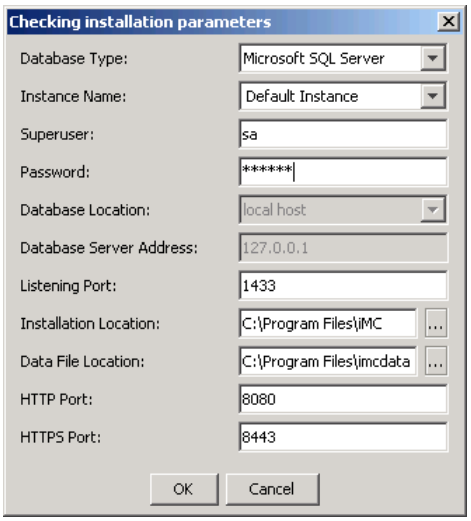
Typical installation

If you select typical installation, the installation program automatically installs and deploys all subcomponents for the IMC Platform on the server:

1. In Figure 29, select the country or region and language, click **Typical**, and click **OK**.

   The window for checking installation parameters appears.
2. Configure the installation parameters to check before you can install and deploy IMC components. See Figure 30.

Figure 30 Checking installation parameters



   a. Select the database type and instance name. Use the default instance or select **Other Instance** from the list to specify an instance name.

   b. Enter the database superuser name (**sa** by default), password, and listening port (**1433** by default).

      These parameters appear only when you install IMC on Windows.

   c. Select a network service name or click  to add a network service name.

      This parameter appears only when you install IMC on Linux to use an Oracle database. In this example, a local separate database is used, you must configure a network service name for

connecting to the local database address. For more information, see *Oracle 11g Installation and Configuration Guide* or *Oracle 11g R2 Installation and Configuration Guide*.

d. Use the default installation location and database file location, or customize the installation location and database file location as needed.

e. Configure the Web service port numbers (**8080** for **HTTP** and **8443** for **HTTPS** by default). You can also use other service port numbers that are not used by other services.

3. Click **OK**.

   The system starts to check the installation environment.

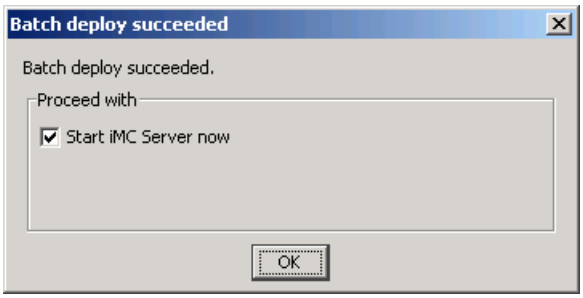
   When the installation environment fails the check, modify parameters according to the check results and proceed with the installation.

4. Click **Continue** even if you see a message reminding you of less than 2 GB free space for the installation environment.

   When the check is passed, the system installs and deploys all IMC Platform subcomponents.

5. After IMC installation and deployment is complete, the **Batch deploy succeeded** window appears.

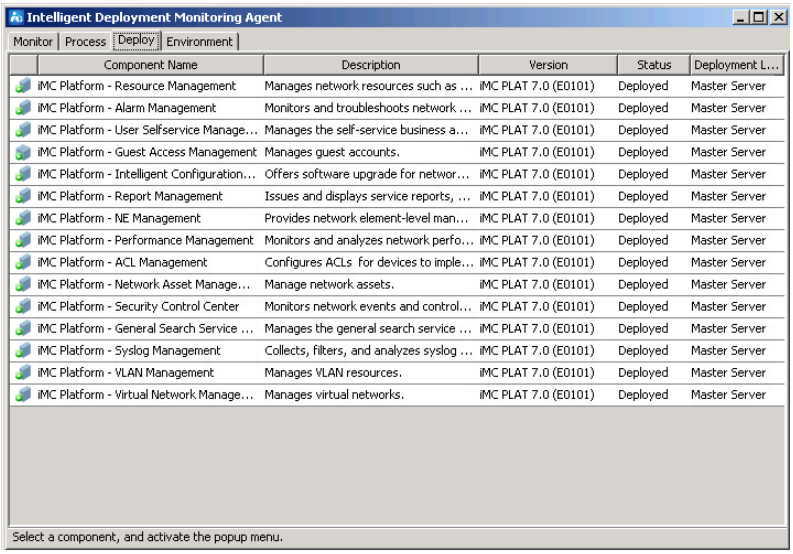
Figure 31 Batch deploy succeeded



To start IMC immediately, select **Start IMC Server now** and click **OK**. The **Intelligent Deployment Monitoring Agent** window appears, as shown in Figure 32.

To start IMC later, click **OK**. When you want to start IMC, click **Start IMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

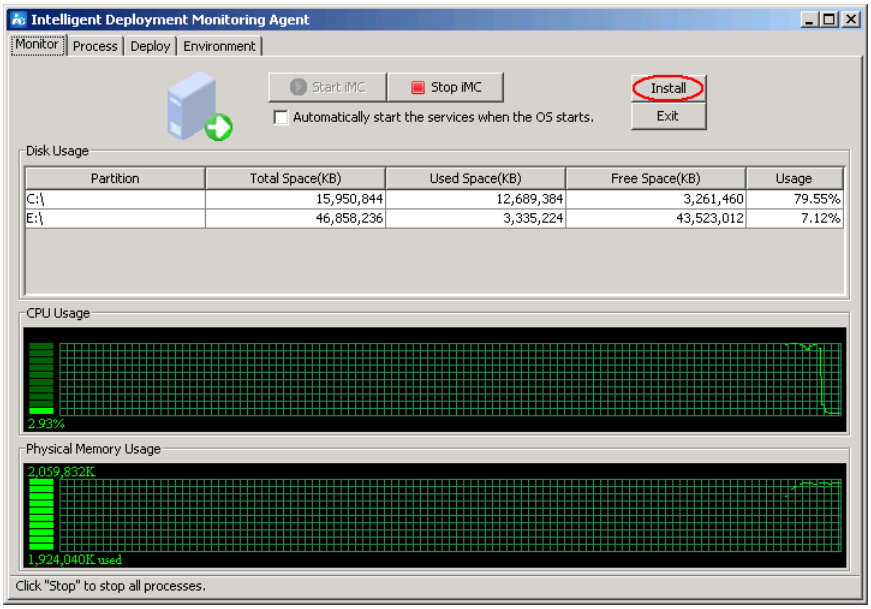
Figure 32 Intelligent Deployment Monitoring Agent



The **Intelligent Deployment Monitoring Agent** window allows you to perform the following operations:

- Click the **Deploy** tab to view the deployed components. The **Deploy** tab shown in Figure 32 contains two data analyzer components, one in Deployed state and the other in Undeployed state, because the component can be deployed on multiple servers (one for each server).
- Click the **Process** tab to view the running process information.
- Click the **Monitor** tab to view the IMC startup information, as shown in Figure 33. When the startup is complete, the **Start IMC** button is grayed out.
- To disable IMC, click **Stop IMC**.
- You can select **Automatically start the services when the OS starts** when you want IMC to automatically start at the system startup.
- To install new components, click **Install**, as shown in Figure 33, or right-click the **Intelligent Deployment Monitoring Agent** icon on the Windows system tray and select **Install** from the shortcut menu. For more information, see "5 Installing and deploying IMC service components."

Figure 33 Intelligent Deployment Monitoring Agent

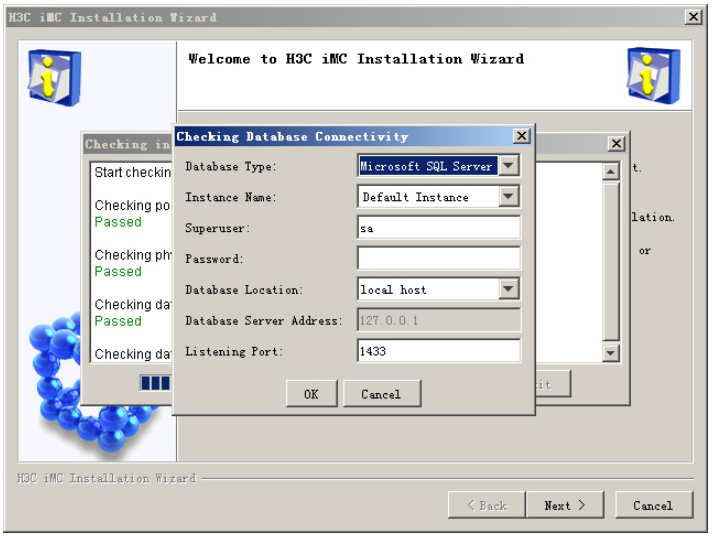


Custom installation

Custom installation allows you to install and deploy only the desired subcomponents for the IMC Platform.

1. In Figure 29, select the country or region and language, click **Custom**, and click **OK**, The window for checking database connectivity appears.

Figure 34 Checking Database Connectivity dialog box



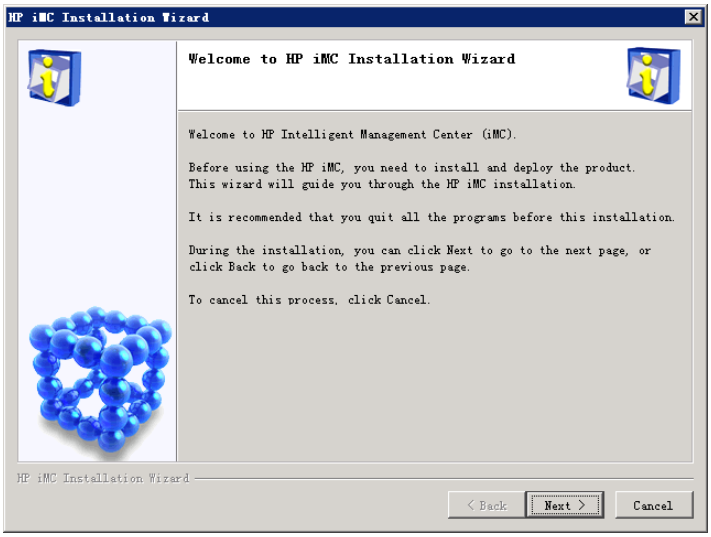
2. Enter parameters for checking the database connectivity:
   - Select the database type and instance name. Use the default instance or select **Other Instance** from the list to specify an instance name.
   - Enter the database superuser name (**sa** by default), password, and listening port number (**1433** by default). You can also use another port number that is not used by another service. These parameters appear only when you install IMC on Windows.
   - Select a network service name or click  to add a network service name. In this example, a local separate database is used, you must configure a network service name for connecting to the local database address.

     This parameter appears only when you are installing IMC on Linux that uses an Oracle database. For more information about network service name configuration, see *Oracle 11g Installation and Configuration Guide* or *Oracle 11g R2 Installation and Configuration Guide*.
   - Select **local host** as the database location and enter the superuser name and password.
3. Click **OK**.

   The system starts to check the database connectivity. After the installation environment check, the **HP IMC Installation Wizard** appears.
4. Click **Continue** even if you see a message reminding you of less than 2 GB free space for the installation environment.

   When the check is passed, the **Welcome to HP IMC Installation Wizard** window appears.

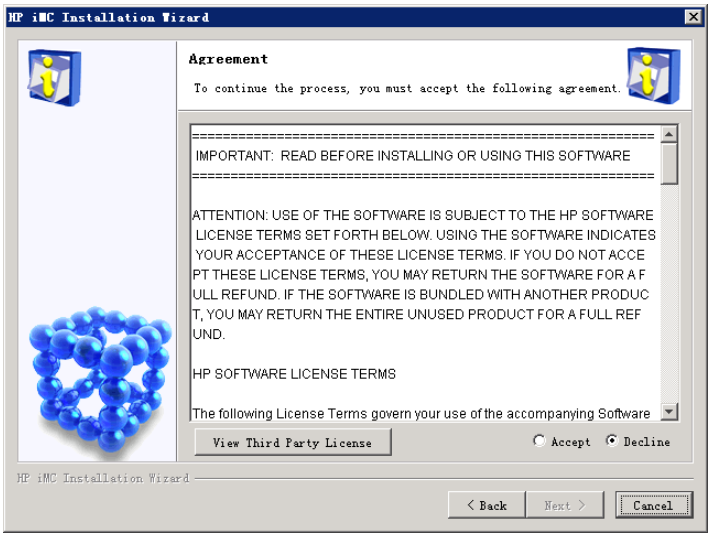
Figure 35 Welcome to HP IMC Installation Wizard



5. Click **Next**.

   The **Agreement** window appears.

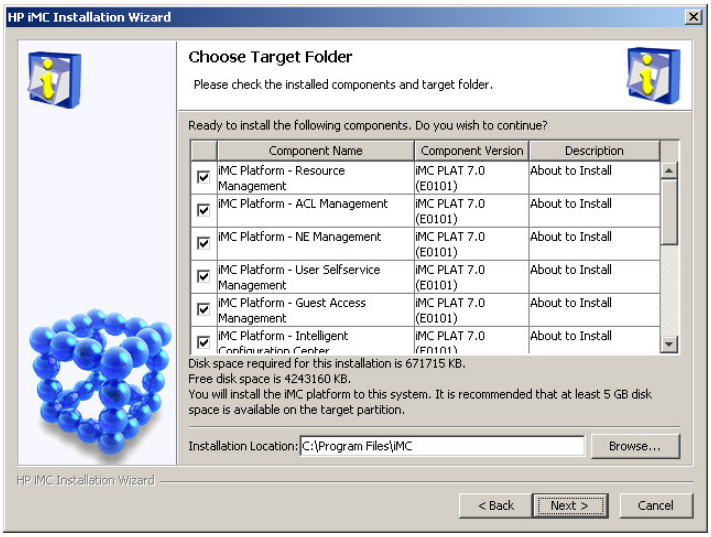
Figure 36 Agreement



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

   The **Choose Target Folder** window appears.

Figure 37 Choose Target Folder



The **Choose Target Folder** window displays the components.

7. Select the components you want to install and specify the installation location.

   By default, IMC is installed in **C:\Program Files\IMC** (or in **/opt/IMC** on Linux). You can enter a path or click **Browse** to select a path to install it in another folder.

CAUTION:

- In the partition where you want to install the IMC software, at least 5 GB free space must be available.
- You must choose a local installation path.
- Linux does not support the IMC installation in a **symlink** path.

   In the **Choose Target Folder** window, you can also view information about the components that you want to install.

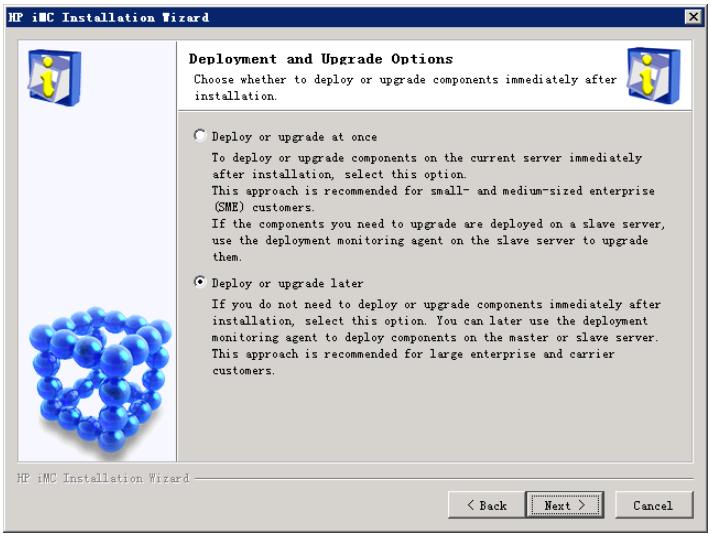
   These components includes:

   - Resource Manager
   - NE Management
   - Alarm Management
   - Performance Management.

8. Click **Next**.

   The **Deployment and Upgrade Options** window appears.

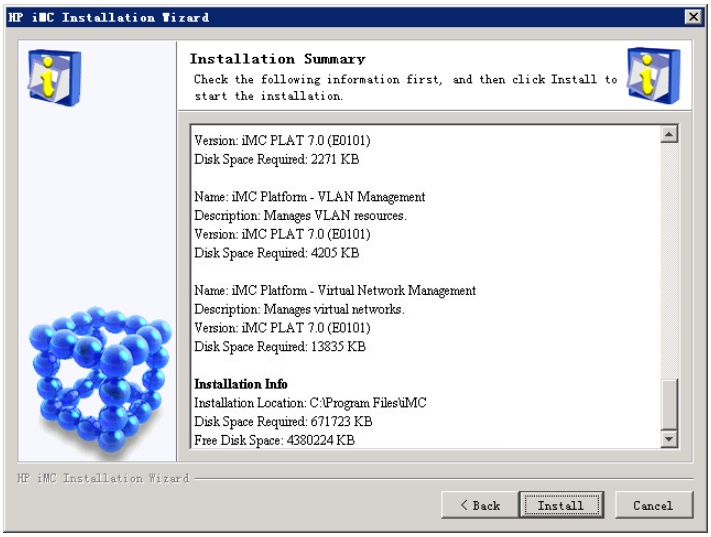
Figure 38 Deployment and Upgrade Options



9. Select an option according to the option descriptions in the window and click **Next**.

   The **Deploy or upgrade later** option is selected in this example. The **Installation Summary** window appears.

Figure 39 Installation Summary



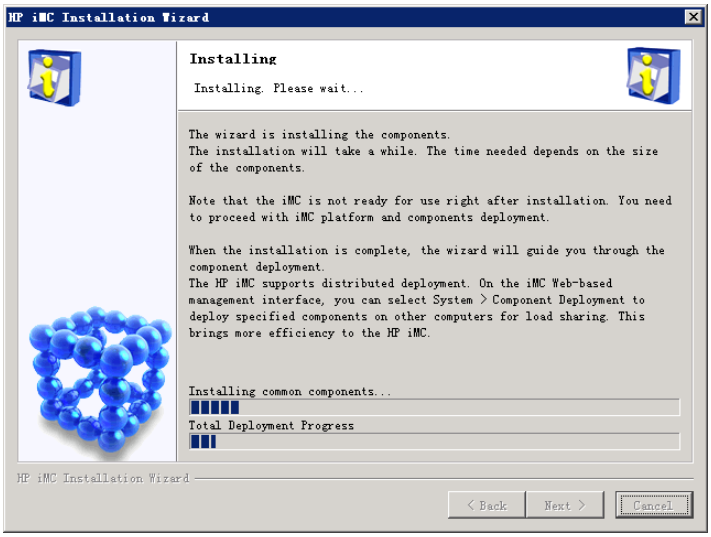
   The **Installation Summary** window provides the following information:

   - Name, description, version, and disk space required by each component to be installed
   - IMC installation location
   - Total disk space required by the installation
   - Free disk space of the partition where IMC is to be installed

10. Click **Install**.

    The **Installing common components** window appears.

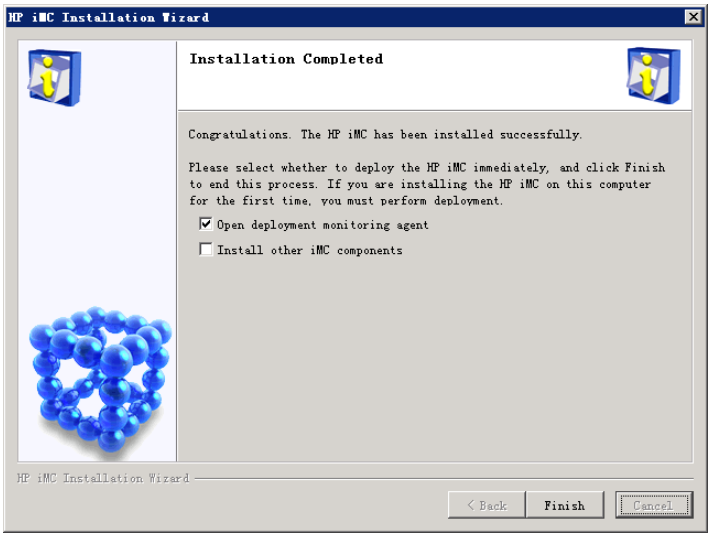
Figure 40 Installing common components



The wizard shows the process of component installation.

After the installation is complete, the **Installation Completed** window appears.

Figure 41 Installation Completed



In the **Installation Completed** window, you can perform the following tasks:

- When you install only the IMC Platform without any service component, select the **Open deployment monitoring agent** box and click **Finish** to start deployment.
- When you continue to install other service components, decompress the installation file, select the **Install other IMC Components** box and click **Finish**. For more information, see "5 Installing and deploying IMC service components."
- You can click **Finish** to close the window without selecting any of the two boxes.

  To open the Intelligent Deployment Monitoring Agent on Windows, select **Start** > **All Programs** > **HP Intelligent Management Center** > **HP Deployment Monitoring Agent**.

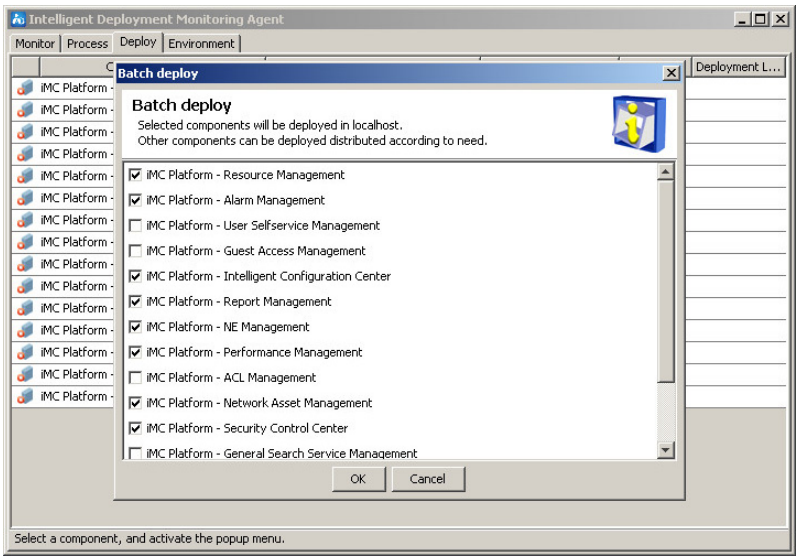
  To open the Intelligent Deployment Monitoring Agent on Linux, run the **dma.sh** script in **/deploy** of the IMC installation path.

Deploying the IMC Platform

If the IMC Platform is installed in custom installation mode, you must manually deploy the IMC platform components.

1. After installation, in the window shown in Figure 41, select **Open deployment monitoring agent** and click **Finish**. The system automatically starts the Intelligent Deployment Monitoring Agent. For the first deployment, a **Batch deploy** window appears.

Figure 42 Batch deploy



2. You can also start the Intelligent Deployment Monitoring Agent by selecting **Start** > **All Programs** > **HP Intelligent Management Center** > **HP Deployment Monitoring Agent** (or running the **dma.sh** script in /deploy of the IMC installation path on Linux). Then select the **Deploy** tab, select **Batch Deploy** from the right-click menu of the target components to start batch deployment.

   In the **Batch deploy** window, the components to be deployed by default include:

   - Alarm Management
   - Intelligent Configuration Center
   - NE Management
   - Performance Management
   - Report Management
   - Resource Management
   - Network Asset Management
   - Security Control Center
   - User Self-service Management

   Optional subcomponents include:

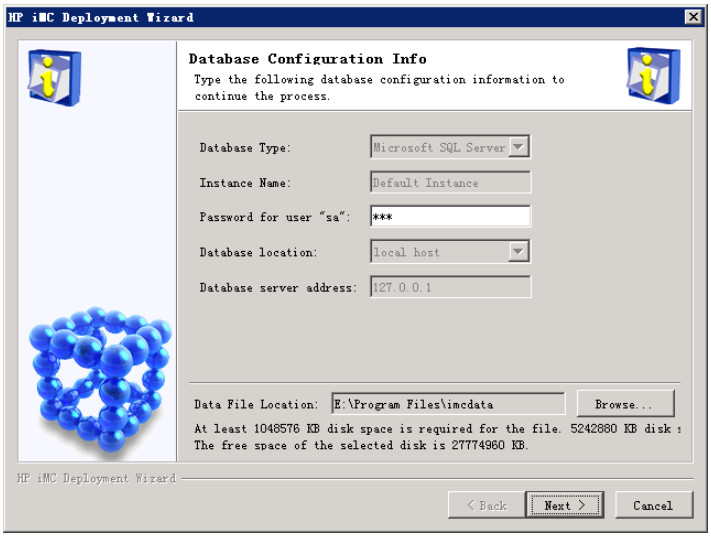
   - ACL Management
   - General Search Service Management
   - Guest Access Manager
   - Syslog Management
   - Virtual Network Management

- VLAN Management

3. You can also select the components to be deployed as needed, except that the Resource Management component is required. In this example, select all the components, Click **OK**.

   The **Database Configuration Info** window appears.

Figure 43 Database Configuration Info



4. Enter the password for the superuser, which you used for installing the IMC database.
5. Select the location for saving data files. The data files are stored in **C:\Program Files\imcdata** on windows or **/opt/imcdata** on Linux by default. You can also click **Browse** to customize the data file location.

NOTE:

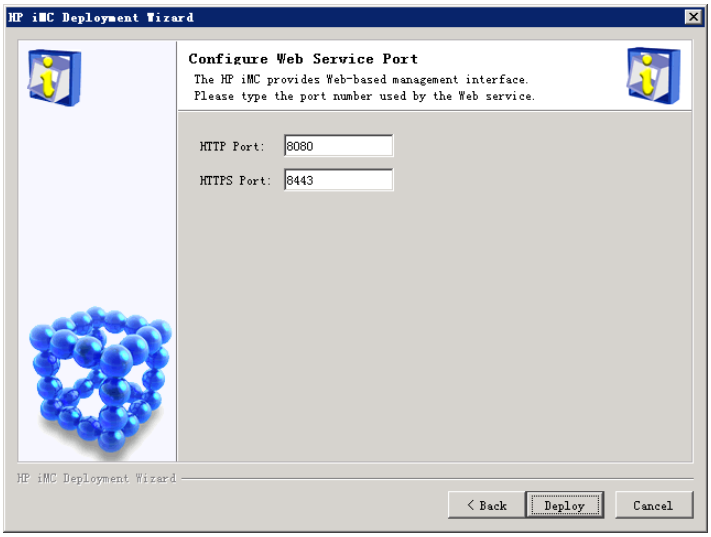
You must select a writable, uncompressed local disk drive. When you do not, an error can occur during IMC deployment. To change the compression setting of a disk drive:

- Right-click the disk name and select **Properties** from the shortcut menu.
- On the **General** tab of the disk properties window that appears, clear the selection of **Compress drive to save disk space**.
- Click **OK**.

6. Select a path to save the data files and click **Next**.

   The **Configure Web Service Port** window appears.

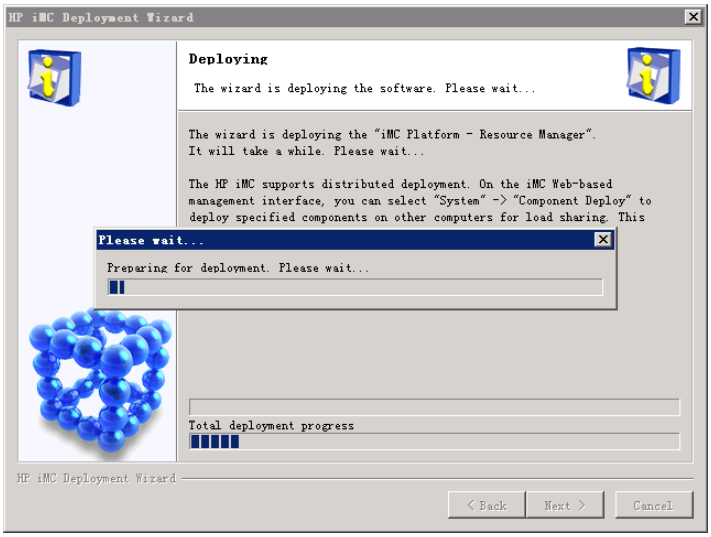
Figure 44 Configure Web Service Port



7. The default port for HTTP access is 8080 and that for HTTPS access is 8443. You can change these port numbers as needed. Make sure the specified ports are open in the firewall settings and are not being used by another services.
8. Click **Deploy**.

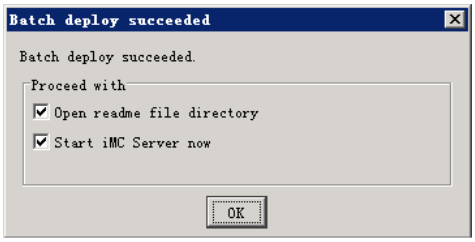
   The **Deploying** window appears.

Figure 45 Deploying IMC components



After the deployment, the **Batch deploy succeeded** window appears.

Figure 46 Batch deploy succeeded



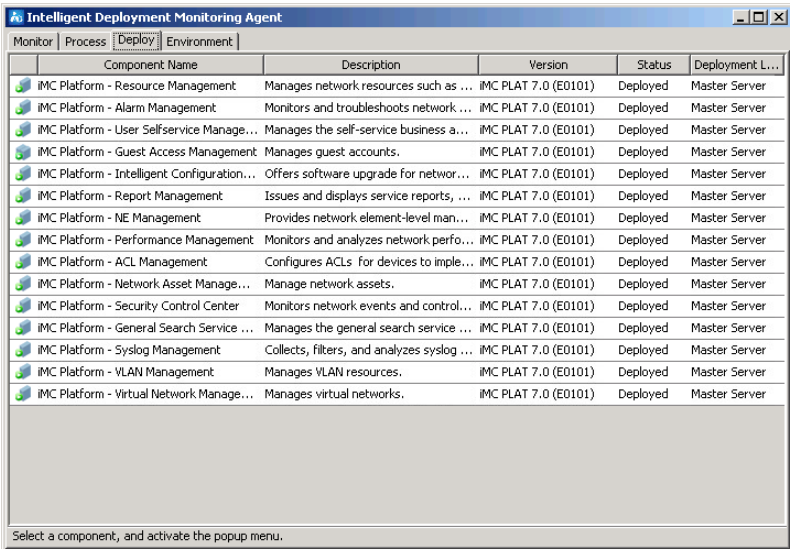
9. In the **Batch deploy succeeded** window, select **Open readme file directory**, **Start IMC Server now**, or both.

   In this example, select **Start IMC Server now** and click **OK**.

   The system immediately starts the IMC service and opens the **Intelligent Deployment Monitoring Agent** window, as shown in Figure 47.

   In this window, select the **Deploy** tab to view information about the component deployment.

Figure 47 Information about component deployment



   The Data Analyzer can be deployed to multiple servers (once for each server). Therefore, after this component is deployed, another Data Analyzer with status **Undeployed** appears in the component list.

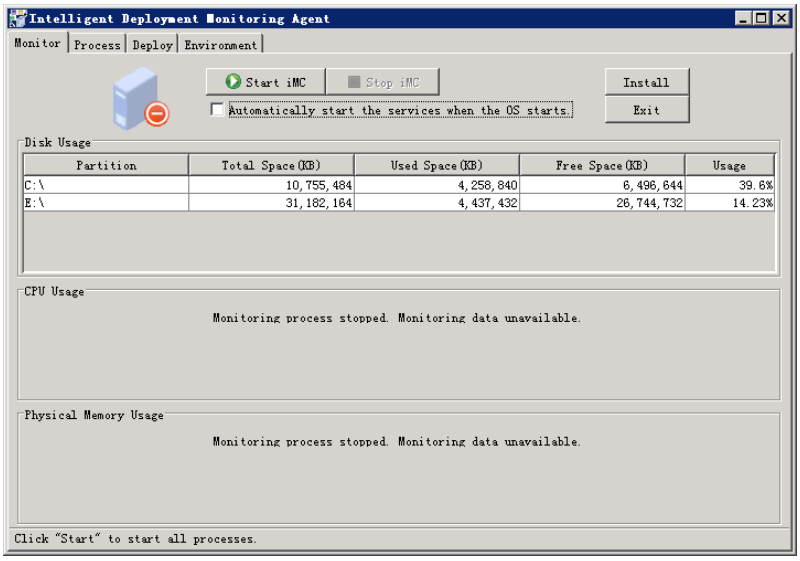
10. After the deployment is finished, follow these steps to start the IMC service:

    a. In the **Intelligent Deployment Monitoring Agent** window, select the **Monitor** tab, as shown in Figure 48.

    b. Click **Start IMC**.

    c. You can also select the **Automatically start the services when the OS starts** box to start IMC with the operating system.

Figure 48 Intelligent Deployment Monitoring Agent



d. To view the enabling and running status of each process, click the **Process** tab to enter the process management window.

Deploying a single IMC component

To deploy a single IMC component, use either of the following methods in the window, as shown in Figure 47.

- Method 1:

  Right-click the target component and select **Deploy the Component** from the shortcut menu.

- Method 2:

  a. Select any target component and select **Batch deploy** from the shortcut menu.

  The **Batch deploy** dialog box appears.

  b. Select the component and click **OK**.

Some IMC components depend on others. When deploying such components, consider the dependencies between components. On the **Deploy** tab, select **Show Dependencies** from the right-click menu of a component to view the components in which the selected component depends. When the component does not depend on any components, **Show Dependencies** is grayed out.

The detailed deployment procedure for a single component is similar to the batch deployment.

IMC service logon accounts

By default, the IMC system service **HP IMC Server** is logged on and started using the **LocalSystem** account. To use another account for IMC service logon, you must grant the account read and write access to the IMC installation folder, and then start IMC by using the Intelligent Deployment Monitoring Agent.

5 Installing and deploying IMC service components

This following information describes the recommended IMC Platform plus service components deployment mode, how to install, and deploy the service components.

IMC common service components include:

- Application Manager
- Branch Intelligent Management System
- Connection Resource Manager
- EAD Security Policy
- IPsec VPN Manager
- MPLS VPN Manager
- Network Traffic Analyzer and User Behavior Auditor
- QoS Manager
- Remote Site Manager
- Service Operation Manager
- User Access Manager

Table 8 IMC subcomponents and deployment requirements

Component	Subcomponents	Remarks
Application Manager	Application Manager	N/A
VAN Connection Manager	VAN Connection Manager	N/A
EAD Security Policy	Security Policy Configuration	N/A
BIMS	Branch Intelligent Management System	N/A
	Auto-Configuration Server	N/A
	Mobile Branch Manager	N/A
iNode Dissolvable Client	iNode Dissolvable Client	N/A
IPsec VPN Manager	IPsec VPN Manager	N/A
MPLS VPN Manager	MPLS VPN Management	N/A
	MPLS TE management	N/A
	L2VPN Management	N/A
Network Traffic Analyzer	Network Traffic Analyzer	N/A
	Network Traffic Analyzer Server	N/A
	Network Behavior Analyzer	N/A
	Network Behavior Analyzer Server	N/A

Component	Subcomponents	Remarks
QoS Manager	QoS Management	N/A
Remote Site Manager	Remote Site Manager	N/A
Service Operation Manager	CMDB Management	N/A
	Service Desk	N/A
Service Health Manager	Service Health Management	N/A
	NQA Collector Management	N/A
User Behavior Auditor	User Behavior Auditor	N/A
	User Behavior Auditor Server	N/A
	Network Behavior Analyzer	N/A
	Network Behavior Analyzer Server	N/A
User Access Manager	User Access Management	Set the database password (defaults to **IMC5_uamead**) and the **UAM Server IP Address**, which is the IP address of the network adapter providing services externally of the server where UAM is deployed.
	Portal Web Server and Portal Proxy	N/A
	Portal Server	Set the **Portal Server IP Address**, which is the IP address of the network adapter providing services externally of the server where the Portal server component is deployed.
	Policy Server	Set the **Policy Server IP Address**, which is the IP address of the network adapter providing services externally of the server where the policy server component is deployed.
	Policy Proxy Server	Set the **Policy Proxy Server IP Address**, which is the IP address of the network adapter providing services externally of the server where the policy proxy server component is deployed.
	User SelfService	Set the **User SelfService IP Address**, which is the IP address of the network adapter providing services externally of the server where the user selfservice component is deployed.
	Desktop Asset Manager	Set the database password (defaults to **IMC5_uamead**), and the **DAM Server IP Address**, which is the IP address of the network adapter providing services externally of the server where DAM is deployed.

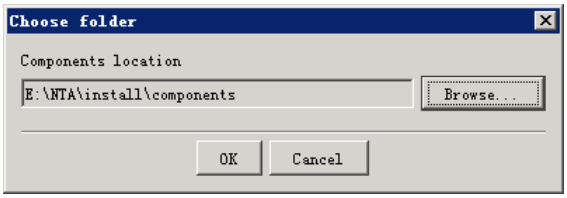
Component	Subcomponents	Remarks
	Desktop Asset Manager Proxy Server	Set the **DAM Proxy Server IP Address**, which is the IP address of the network adapter providing services externally of the server where the DAM proxy server component is deployed.
Voice Service Manager	Voice Service Manager	N/A
Wireless Service Manager	Wireless Service Manager	N/A

The installation and deployment procedures for the common service components are similar. This section takes the installation of NTA as an example.

Installing IMC Network Traffic Analyzer (NTA)

1. In the **Installation Completed** window (see Figure 41), select the **Install other IMC Components** box.
2. Click **Finish** to enter the **Choose folder** dialog box.

Figure 49 Choose folder



NOTE:

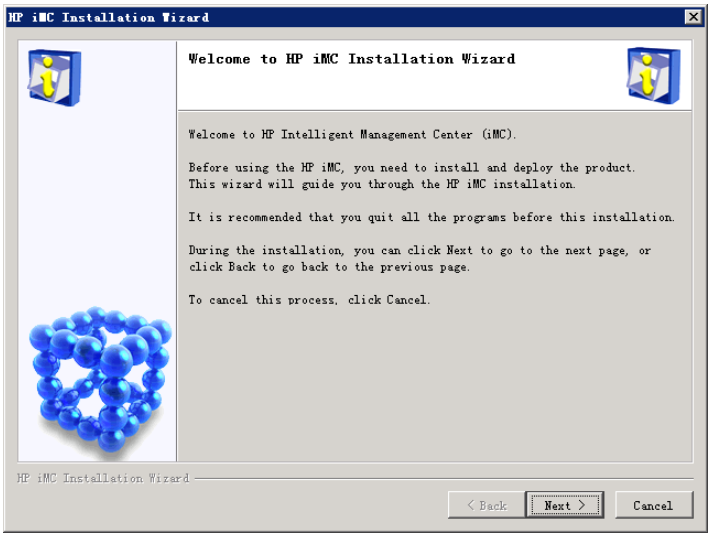
You can also install a new component with either of the following methods:

- Select **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** and click **Install** in the Monitor tab to begin installation.
- In the system tray, right-click the **Intelligent Deployment Monitoring Agent** icon and select **Install** from the popup menu to install a new component.

3. In the **Choose folder** window, click **Browse**.
4. Select the **install\components** folder in the IMC NTA downloaded installation package.
5. Click **OK**.

   A welcome window appears to guide you through the IMC installation.

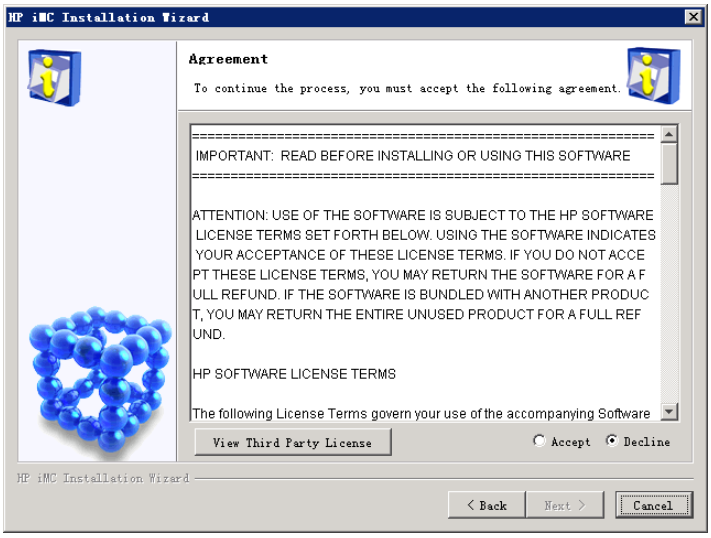
Figure 50 Welcome to HP IMC Installation Wizard



6. Click **Next**.

   The **Agreement** window appears.

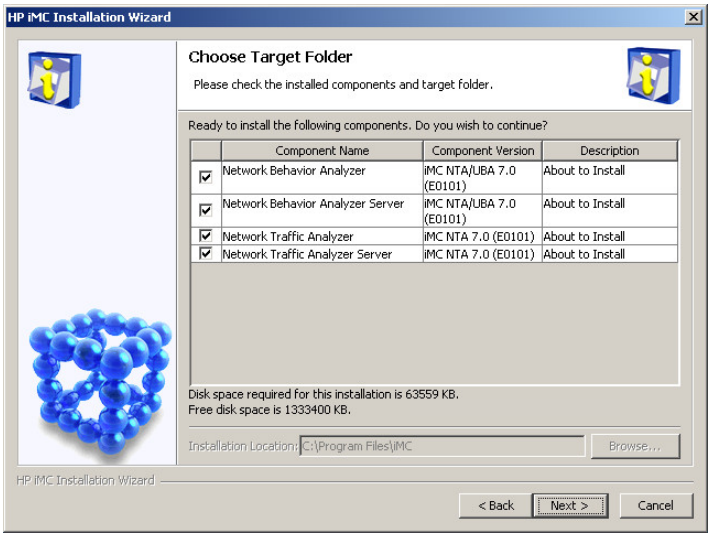
Figure 51 Agreement



7. Read the license agreement and third party license and select **Accept**.
8. Click **Next**.

   The **Choose Target Folder** window appears.

Figure 52 Choose Target Folder



The **Choose Target Folder** window displays information about the NTA.

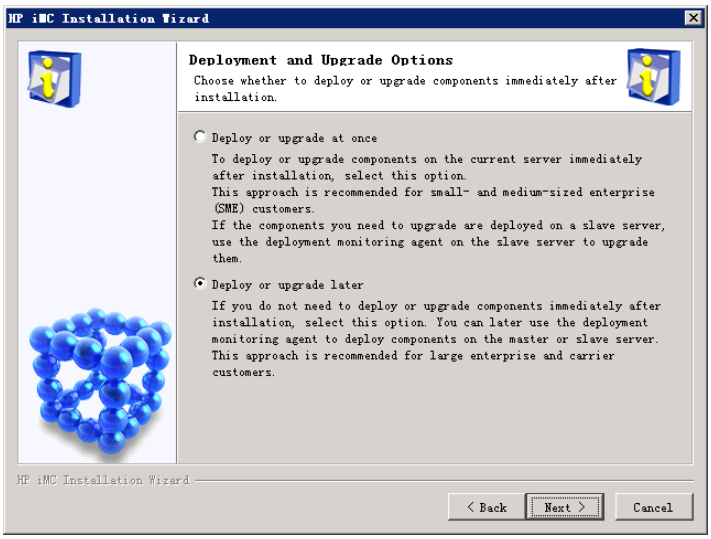
Some IMC components depend on other components to function. When the latter are not installed, the **Description** of a dependent component to be installed in the **Choose Target Folder** window might be **Do Not Install**. In this case, you can view which components that this component depends on by selecting **Show Dependent Influence** from the right-click menu in the component list.

In centralized deployment, the system specifies the installation location of the NTA as the installation location of the IMC Platform by default.

9. After confirmation, click **Next**.

   The **Deployment and Upgrade Options** window appears.

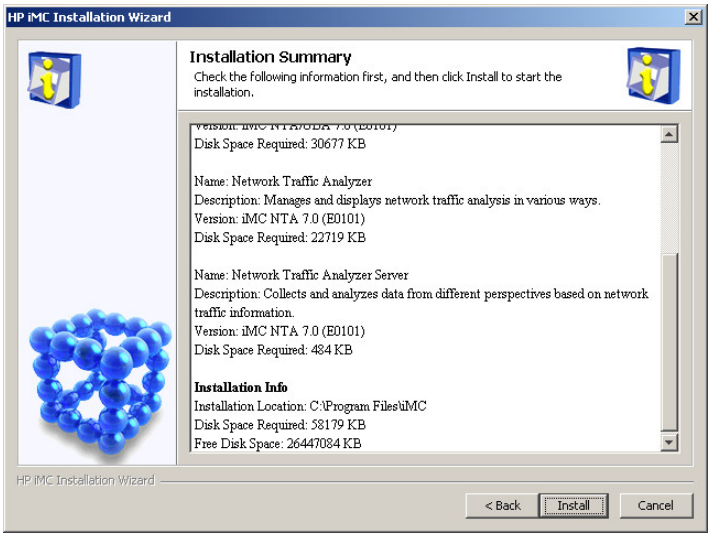
Figure 53 Deployment and Upgrade Options



10. Select an option as needed. This example uses **Deploy or upgrade later**.
11. Click **Next**.

    The **Installation Summary** window appears.

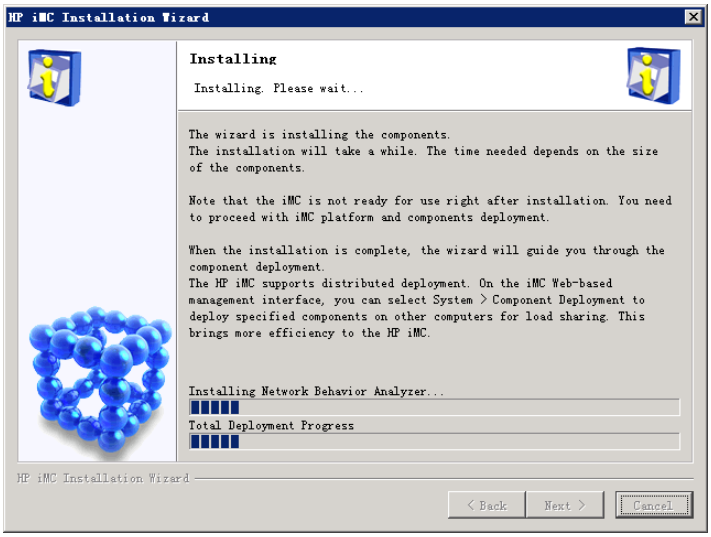
Figure 54 Installation Summary



12. After confirming the related installation information, click **Install**.

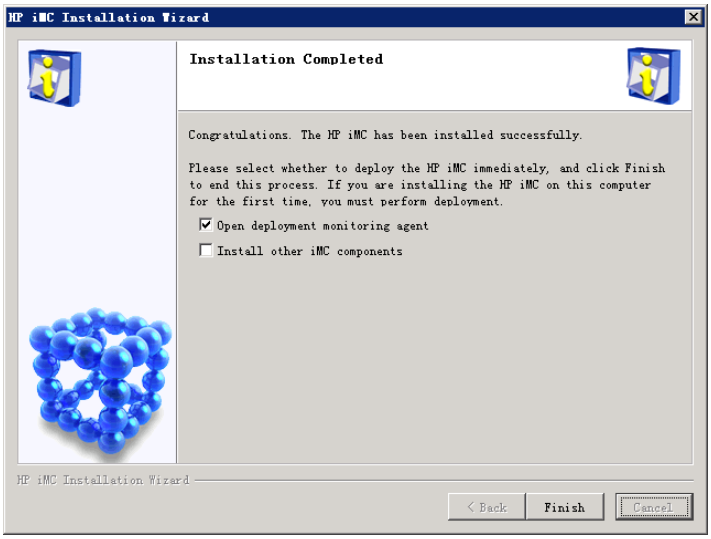
    The **Installing** window appears.

Figure 55 Installing



The wizard is installing the component. After the installation is finished, the **Installation Completed** window appears.

Figure 56 Installation Completed



13. Select **Open deployment monitoring agent** in the **Installation Completed** window and click **Finish**.

    To install other IMC common components, select **Install other IMC Components** in the **Installation Completed** window and click **Finish** to begin the installation. The installation procedure is similar to that of NTA.

    In addition to the previous installation methods, you can also start a new component installation wizard with either of the following methods:

- Method 1:

  After installing and deploying IMC:

  a. Select **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** (or run the **dma.sh** script in **/deploy** of the IMC installation path on Linux) to start the Intelligent Deployment Monitoring Agent.

  b. Click **Install** in the **Monitor** tab to begin installation.

CAUTION:

- To install IMC in Windows Server 2008 or Windows Server 2008 R2, you must first modify the User Account Control Settings. After installing IMC, you can restore the related settings as needed.

  c. Modify the User Account Control Settings, click **Start > Control Panel > System and Security.**

     Click **Change User Account Control Settings** in the **Action Center**, and the **User Account Control Settings** window appears.

     In the window, set the **Choose when to be notified about changes to your computer** to **Never notify**.

- Method 2:

  In the system tray, right-click the **Intelligent Deployment Monitoring Agent** icon and select **Install** from the popup menu to install a new component.

  The detailed installation procedure is the same as the previously described.

Deploying IMC Network Traffic Analyzer (NTA)

In this example, the NTA components are deployed in centralized mode. The NTA components include Network Behavior Analyzer, NTA Network Traffic Analyzer Server, Network Behavior Analyzer, and Network Traffic Analyzer Server.

1. After installation, in the window, as shown in Figure 56, select **Open deployment monitoring agent** and click **Finish**.

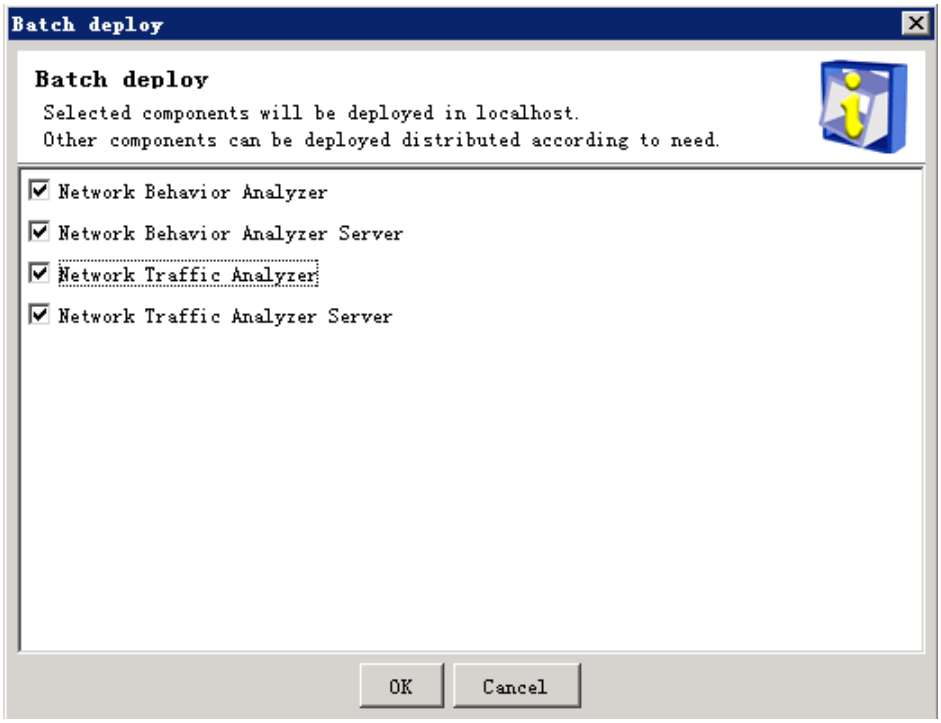
   The system automatically starts the Intelligent Deployment Monitoring Agent. A **Batch deploy** window appears at the same time, as shown in Figure 57.

   You can also start the Intelligent Deployment Monitoring Agent by selecting:

   a. **Start > All Programs > HP Intelligent Management Center > HP Deployment Monitoring Agent** (or running the **dma.sh** script in /deploy of the IMC installation path on Linux).

   b. Then the **Deploy** tab, selecting **Batch Deploy** from the right-click menu of the target components to start batch deployment.

Figure 57 Batch deploy



2. In the **Batch deploy** window, select the components to deploy.

   In this example, select **Network Traffic Analyzer** and **Network Behavior Analyzer**.

3. Click **OK** to start deploying the components.

   After the deployment is complete, the **Batch deploy result** dialog box prompting **Batch deploy succeeded** appears.

4. Click **OK**.

5. On the Intelligent Deployment Monitoring Agent that appears, select the **Monitor** tab, and click **Start IMC** to start IMC.

   After IMC is normally started, you can perform deployments on the subordinate servers.

6 Installing plug-ins

To support some IMC functions, you must install necessary plug-ins.

Installing DHCP plug-ins

A DHCP server installed with a DHCP plug-in lets IMC obtain the names of terminals, such as servers, PCs, and printers, from the DHCP server. To accomplish this task, ensure that:

- At least one DHCP server exists in the network.
- All DHCP servers in the network have DHCP plug-ins installed.

To view the names obtained from the DHCP server, select **Terminal Access** > **Unauthorized Access List** or **History Access Log List** from the navigation tree.

The following information describes how to install DHCP plug-ins on MS DHCP and Linux DHCP servers respectively.

On the MS DHCP server

1. Modify the file **qvdm.conf**, so that the IMC supports getting the terminal name or terminal domain name through the MS DHCP server.
   a. Enter the**\server\conf** directory in the IMC installation path, open the file **qvdm.conf** in Wordpad, and add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   b. Save and exit the file.
   c. Restart IMC in the Intelligent Deployment Monitoring Agent.
2. Install the IMC DHCP plug-in on the MS DHCP server.
   The DHCP plug-in installer dhcp-plug-windows.zip is saved in the **windows\tools** directory of the IMC installer.
   a. Copy the plug-in installer to the MS DHCP server.
   b. Decompress the installer.
   c. Use Wordpad to open the **imf.cfg** file in the **\server\imf\server\conf** directory of the **dhcp-plug-windows** folder.
   d. Modify the IMGAddress into the master server IP address and IMGPort (which is 8800 by default) to the IMG port number.
   e. Save and exit the file.
3. Run the **install.bat** script in the dhcp-plug-windows folder.
   After the installation, a new service **IMC DHCP Plug** is added to the system services.
4. Start the IMC DHCP plug service.
   a. Click **Start**, and select **Administrative Tools** > **Component Services** to open the **Component Services** window.
   b. Select **Services (Local)** from the navigation tree.

c. Right-click the **IMC DHCP Plug** service on the **Services (Local)** list and select **Start** to start the IMC DHCP plug service.

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

CAUTION:

Do not remove the directory which the plug-in installer **dhcp-plug-windows.zip** is extracted to. Otherwise, the DHCP plug-in cannot be uninstalled completely.

On the Linux DHCP server

1. Modify the file **qvdm.conf**, so that IMC supports getting the terminal DNS name or terminal name through the Linux DHCP server.
   a. Use the VI editor to open the **qvdm.conf** file in the **/server/conf** directory of the IMC installation path:
      ```
      vi qvdm.conf
      ```
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and exit the file, and restart IMC in the Intelligent Deployment Monitoring Agent.
2. Install the IMC DHCP plug-in on the Linux DHCP server.

   The DHCP plug-in installer **dhcp-plug-linux.zip** is saved in the tools directory of the IMC Linux installer.
   a. Copy the plug-in installer to the Linux DHCP server.
   b. Decompress the installer.
   c. Use the VI editor to open the imf.cfg file in the **/server/imf/server/conf/** directory of the **dhcp-plug-linux** folder.
      ```
      vi imf.cfg
      ```
   d. Modify the IMGAddress into the IMC server IP address, and modify the IMGPort (which is 8800 by default) to the IMG port number that you set when installing IMC.
   e. Save and exit the file.
3. Check whether the path of the DHCP server IP allocation information file, **dhcpd.leases,** is correct.
   a. Enter the **/var/lib/dhcp** directory of the Linux operating system, and check whether the **dhcpd.leases** file exists.
   b. When the file does not exit, enter the **server/conf/** directory of the **dhcp-plug-linux** folder, use the VI editor to open the **qvdm.conf** file, and add the following line to the file to specify the path of the **dhcpd.leases** file.
      ```
      DhcpPlugIpAllocPath=<Current path>/dhcpd.leases
      ```
   c. Save and exit the file.
4. Execute the **install.sh** script in the **dhcp-plug-linux** folder.

After the installation is complete, the **dhcp-plug** service is added to the system services, and has been automatically started.

You can use the **server dhcp-plug stop** command to stop the service or use the **server dhcp-plug start** command to start the service.

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

CAUTION:

Do not remove the directory to which the plug-in installer dhcp-plug-windows.zip is extracted. Otherwise, the DHCP plug-in cannot be uninstalled completely.

Installing VNM agent plug-ins

Virtual Network Management (VNM) is a module on the IMC Platform to manage virtual networks. It must work with a VNM Windows or Linux agent for virtual network management.

Installing a VNM Windows agent

When Microsoft Hyper-V servers exist in the network, install VNM Windows agents for IMC to manage the Hyper-V servers.

A VNM Windows agent must be installed on one Windows server. When the Microsoft Hyper-V servers are managed by Microsoft VMM servers, HP recommends that you install VNM Windows agents on the Microsoft VMM server. A VNM Windows agent can work for up to 50 Hyper-V servers. When more than 50 Hyper-V servers exist in the network, install more VNM Windows agents.

CAUTION:

VNM Windows agents can only be installed on Windows server 2008 R2 SP1/2012 that can access all Hyper-V servers. A Windows server can be installed with only one VNM Windows agent.

A VNM Windows agent is dependent on .NET Framework 4.5, and PowerShell 3.0. Before you install a VNM Windows agent, make sure that all the software applications are installed. For the Windows Server 2008 R2 system, they are installed in by default; for other Windows operating systems, go to the Microsoft official website to download and install them.

1. The installation file **vnm-plug-windows.zip** of a VNM Windows agent is stored in tools folder of the IMC installation package. Decompress the file and copy the file to any directory of the server where the VNM Windows agent is to be installed.
2. Run **Register.bat** in the **vnm-plug-windows** folder. When all the related software applications are installed, the installation process is complete. Otherwise, the system prompts you to install the required software and quit the installation process. In this case, install the required software and restart the installation process.

   Do not delete the **vnm-plug-windows** folder or the files in the folder after installation. It becomes the service registration path.
3. Use Wordpad to open the **imf.cfg** file in the **vnm-plug-windows/serverimf/server/conf** directory. Modify IMGAddress as the IP address of the master IMC server and IMGPort as the MBP port number (8800 by default).
4. Save your settings and quit.
5. Start the IMC VNM plug service.
   a. Click **Start** and select **Administrative Tools > Component Services** to open the **Component Services** window.
   b. Select **Services (Local)** from the navigation tree, right-click **IMC VNM Agent** on the **Services (Local)** list, and select **Start** to start the VNM agent service.

To uninstall a VNM agent plug-in, run the file **UnRegister.bat** in the **vnm-plug-windows** directory.

Installing a VNM Linux agent

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

VNM Linux agents can run on 32-bit or 64-bit Red Hat 6.0 or later versions.

A VNM Linux agent plug-in contains an SSH key deployment tool "ssh-key-tool" and an agent installation tool. Linux uses SSH key pairs for authentication. The communication between a KVM server and a VNM Linux agent or another KVM server is based on SSH key trust. Before you install a VNM Linux agent, establish SSH key trust among KVM servers and between each KVM server and the agent.

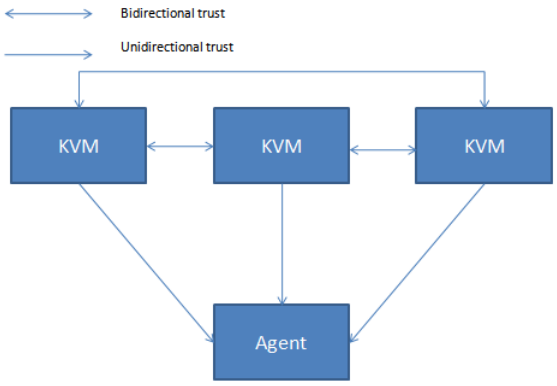
Introduction to the SSH key deployment tool

Use this tool to establish SSH key trust relationships, including global SSH key trust establishment, KVM trust adding, and SSH key trust maintenance.

- Establishing global SSH key trust relationships

  The first time you install a KVM Linux agent, establish the global trust relationships among KVM servers and between each KVM server and the agent.

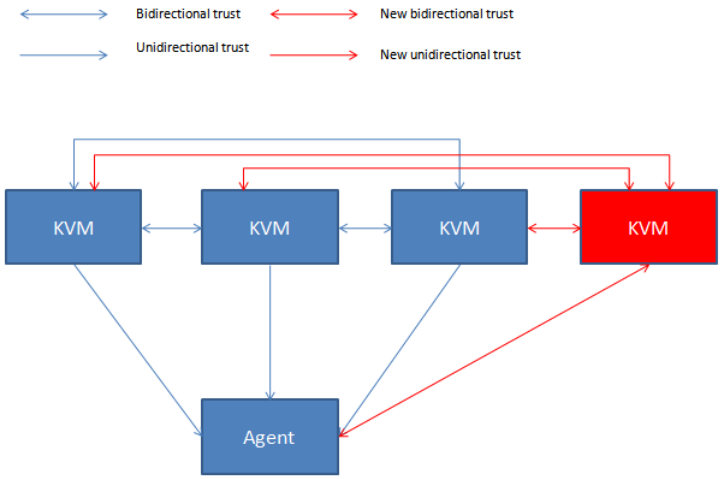
Figure 58 Global trust relationships



- Adding SSH key trust relationships for new KVM servers

  After the KVM Linux agent is installed, you can add SSH key trust relationships for new KVM servers that are added to the network.

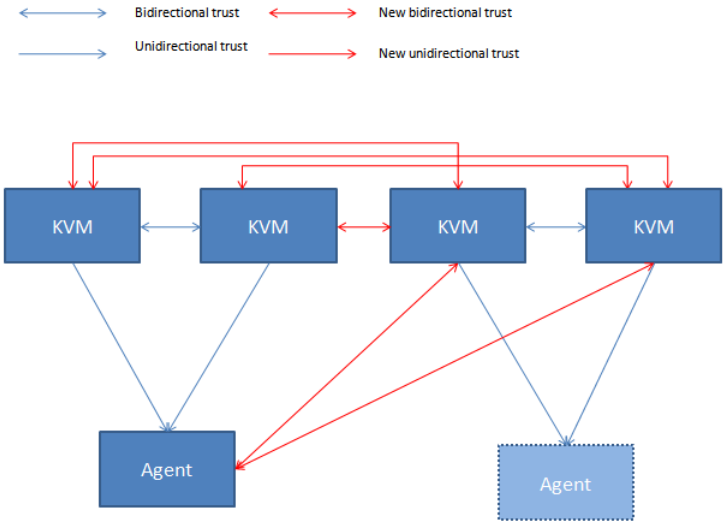
Figure 59 KVM trust adding



- Maintaining SSH key trust relationships

  When multiple KVM Linux agents are installed, you might need to shut down some of the agents or change their management scopes. Use SSH key deployment tool to maintain the trust relationships among the KVM servers and between a KVM server and the agent.

Figure 60 Trust relationship maintenance



Installation prerequisites

The VNM Linux agent is a 32-bit program and applies only to Red Hat. To install the VNM Linux agent on 64-bit Red Hat, first install the following 32-bit program compatibility packages:

- Library for getting and setting POSIX.1e capabilities (compat-libcap1-1.10-1.i686.rpm)
- Linux-native asynchronous I/O access library (libaio-0.3.107-10.el6(i686))
- GCC version 4.4 shared support library (libgcc-4.4.5-6. el6 (i686))
- GUN Standard C++ Library (libstdc++-4.4.5-6. el6 (i686))
- glibc-2.12-1.80.el6.i686.rpm
- nss-softokn-freebl-3.12.9-11.el6.i686.rpm

1. Insert the installation disk of Red Hat Linux 6.0 or above to the CD-ROM drive.
2. Enter the **System** > **Administration** > **Add/Remove Software** window.
3. Select **All Packages**, and then select and install the packages mentioned above in the software package list on the right.

Installation and configuration procedure

1. Establish global SSH key trust relationships with the SSH key deployment tool:
   a. Enter the **tools** directory on the IMC installation disk, copy file **vnm-plug-linux.zip** to a local disk drive, and decompress the file.
   b. Run the **install.sh** script in the decompressed file folder and enter **1** when you see the following menu:
   ```
   [root@daemon8930 vnm-plug-linux]# ./install.sh
   [1] Deploy SSH Key for KVM.
   [2] Install the vnm linux agent.
   [3] Exit the install program.
   Please enter your choice(1|2|3):
   ```
   c. Enter **1** when you see the SSH key deploy type menu:
   ```
   Please choose the ssh key deploy type:
   [1] Deploy SSH Key for new agent.
   [2] Deploy SSH Key for new added KVM.
   [3] Deploy SSH Key for agent maintenance.
   Please enter your choice(1|2|3):
   ```
   d. Enter **y** when you see the following message:
   ```
   Please add the target KVM to the ssh-key-tool/conf/host.txt(y/n):
   ```
   e. Enter the username and the password of the KVM server in the following format.
   ```
   ip:10.153.146.12 user:root passwd:imcimc
   ```
   In the previous character string, **root** and **imcimc** are the username and password of the KVM server, respectively. Edit these fields and add more commands according to the KVM server settings.
   f. Save the **host.txt** file with the **:wq** command.
   An execution result message appears.
2. Install the VNM Linux agent:
   a. On the VNM Linux agent installation interface, enter **2**.
   ```
   Deploy SSH Key for KVM.
   Install the vnm linux agent.
   Exit the install program.
   Please enter your choice(1|2|3):
   ```
   b. Enter the IP address of the master server. The default setting is **localhost**.
   ```
   Please enter the IMC Master Server IP Address(Default:localhost):
   ```
   c. Check whether or not the installation is successful by entering **ps –ef | grep imcvnmagent**.
   When the agent is successfully installed, you can see the **imcvnmagent** process is running.
3. Add SSH key trust for new KVM servers:
   Perform this step when new KVM servers connect to the network, so they can establish SSH key trust relationships with the agent, with every existing KVM server, and among themselves.

a. Run the **install.sh** script in the VNM Linux agent installation file folder and enter **1** when you see the following menu:

```
[root@daemon8930 vnm-plug-linux]# ./install.sh
[1] Deploy SSH Key for KVM.
[2] Install the vnm linux agent.
[3] Exit the install program.
Please enter your choice(1|2|3):
```

b. Enter **2** when you see the SSH key deploy type menu:

```
Please choose the ssh key deploy type:
[1] Deploy SSH Key for new agent.
[2] Deploy SSH Key for new added KVM.
[3] Deploy SSH Key for agent maintenance.
Please enter your choice(1|2|3):
```

c. Enter **y** when you see the following message:

```
Please enter the existed KVM to the ssh-key-tool/conf/host.txt(y/n):
```

d. Enter the username and the password of each new KVM server in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

In the previous character string, **root** and **imcimc** are the username and password of the KVM server, respectively. Edit these fields and add more commands according to the KVM server settings.

e. Save the **host.txt** file with the **:wq** command.

f. Enter **y** when you see the following message:

```
Please add the target KVM to the ssh-key-tool/conf/new_host.txt(y/n):
```

g. Enter the username and the password of each new KVM server in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

h. Save the **new_host.txt** file with the **:wq** command.

The SSH key trust relationships are successfully deployed for the new KVM server.

i. Restart the vnm-plug service in the system services.

4. Maintain SSH key trust relationships:

a. Run the **install.sh** script in the VNM Linux agent installation file folder and enter **1** when you see the following menu:

```
[root@daemon8930 vnm-plug-linux]# ./install.sh
[1] Deploy SSH Key for KVM.
[2] Install the vnm linux agent.
[3] Exit the install program.
Please enter your choice(1|2|3):
```

b. Enter **3** when you see the SSH key deploy type menu:

```
Please choose the ssh key deploy type:
[1] Deploy SSH Key for new agent.
[2] Deploy SSH Key for new added KVM.
[3] Deploy SSH Key for agent maintenance.
Please enter your choice(1|2|3):
```

c. Enter **y** when you see the following message:

```
Please enter the existed KVM to the ssh-key-tool/conf/host.txt(y/n):
```

d. Enter the username and the password of the KVM server to be modified in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

In the previous character string, **root** and **imcimc** are the username and password of the KVM server, respectively. Edit these fields according to the KVM server settings.

e. Save the **host.txt** file with the **:wq** command.

f. Enter **y** when you see the following message:

```
Please add the target KVM to the ssh-key-tool/conf/new_host.txt(y/n):
```

g. Enter the username and the password of each new KVM server in the following format.

```
ip:10.153.146.12 user:root passwd:imcimc
```

h. Save the **new_host.txt** file with the **:wq** command.

i. Restart the vnm-plug service in the system services.

Installing Android clients

Mobile clients (such as smart phones) can access IMC resources to manage and monitor IMC. This edition of IMC supports the access of mobile devices running an Android operating system.

A mobile device must meet the following requirements before it can access IMC:

- The device is installed with the operating system of Android 2.1 update1 or a later version.
- The screen resolution is HVGA(480*320) or WVGA(800*480).
- The mobile device can communicate with the IMC server (through wireless connection, for example).

To install an Android client:

1. Access the website **http://imc-addr:port/imc/noAuth/imc.apk** by using the embedded browser of the mobile device to automatically download the client installation program.

   a. **imc-addr** is the IP address of the IMC server, and **port** is the HTTP port number (8080 by default) set when IMC was deployed for the first time.

2. Install the program as prompted.

   When the message **Programs from unknown sources are not allowed to install** appears during installation, locate to **Settings > Applications** and select **Unknown source**.

To log in to IMC:

1. Open the client program.
2. Enter the IMC server address, login name, and password.

   The IMC server address is in the format of **http://imc-addr:port**, where **imc-addr** is the IP address of the IMC server and **port** is the HTTP port number (8080 by default). Do not add **/imc** to the end of the address. To use a secure connection, enter the address in the format of **https://imc-addr:port** (the port number defaults to 8443). When HTTPS does not use the default port number when IMC was deployed for the first time, enter the specified port number.

   The login name must be an existing login name, which has the privilege to access **IMC Platform > Resource Manager > Mobile Client Access** in IMC.

3. Select **Save password** or **Auto Login** as needed.

   When you select **Save password**, you do not need to enter the password for the next logins. When you select **Auto Login**, you do no need to enter the login name and password for the next logins.

4. Click **Login** to log in to the IMC server.

You can use the Android client to implement the following functions:

- View information about faulty devices and interfaces, and query specific devices.
- View device alarms.
- Inform real-time alarms.
- Test device reachability by using ping or traceroute.
- View custom views and device views.
- Use an Android browser to access IMC to perform configuration and management operations.
- Play IMC videos.

NOTE:

When RADIUS authentication or LDAP authentication is used or when you change the login password, you must first log in to the IMC from a PC successfully before you can use a mobile client to log in to IMC.

Installing LLDP agent plug-ins

When the VNM component is deployed, you must install an LLDP agent for topology calculation.

An LLDP agent contains the following packages: lldp-agent-redhat.zip, lldp-agent-ubuntu.zip, and lldp-agent-windows.zip. The first two packages are installed on a KVM server and the last package is installed on a Microsoft Hyper-V server. The installation procedure for lldp-agent-redhat is similar to that for llap-agent-ubuntu, and the following sections describe the installation procedure for lldp-agent-redhat.

Before the LLDP agent installation, copy the three packages to the target server and decompress the packages. If a Windows server is used, copy the lldp-agent-windows.zip file to a non-system disk.

IMPORTANT:

Do not delete the folder where the decompressed installation packages reside after completing the LLDP agent installation.

Installing an LLDP Linux agent

LLDP Linux agent plug-ins apply only to 64-bit Linux, including Redhat 5.5, Ubuntu 11.0, and their later versions.

To install and configure an LLDP Linux agent:

1. Set executable permission to the **install.sh** script and run the script in the LLDP Linux agent installation file folder.

   The LLDP Linux agent is installed.

2. Configure the LLDP Linux agent.

   The configuration file **lldpagent.conf** is located in the **conf** directory of the LLDP Linux agent installation file folder.

   LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP. To enable an LLDP agent to support CDP:

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

      ```
      vi lldpagent.conf
      ```

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

You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds. To change the setting, delete the pound sign (#) from the string **#INTERVAL=300** and change the value.

3. Restart the lldp-agent service.

```
service lldp-agent restart
```

Installing an LLDP Windows agent

LLDP Windows agent plug-ins 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 file folder.

   The LLDP Windows agent is installed.

2. Configure the LLDP Windows agent.

   The configuration file **lldpagent.conf** is located in the **conf** directory of the LLDP Windows agent installation file folder.

   LLDP agent plug-ins support either LLDP or CDP, but not both at the same time. By default, the plug-ins support LLDP.

   To enable an LLDP agent to support CDP:

   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**.

   You can set the interval at which LLDP or CDP packets are sent. The default setting is 300 seconds.

   To change the setting, delete the pound sign (#) from the string **#INTERVAL=300** and change the value.

   c. Restart the lldp-agent service.

7 Logging in to IMC

IMC does not provide separate client software for access. HP recommends that you access the IMC system using the following Web browsers:

- Internet Explorer 9 or 10
- Firefox 20 or later
- Chrome 26 or later

Access methods

Before you log in to IMC, make sure the Web service ports of IMC (8080 for HTTP and 8443 for HTTPS) are open in the firewall settings on the server installed with the IMC Platform.

To log in to IMC:

1. Enter the IMC login page using one of the following methods:

   Through HTTP:

   a. Input **http://192.168.4.44:8080/imc** in the address bar of your browser and press **Enter**. **192.168.4.44** is the IP address of the master server, and **8080** is the HTTP port set the first time the IMC platform subcomponents were deployed.

   b. The IMC login page appears. You can enable the verification code feature on the IMC login page. For more information, see *HP IMC Getting Started Guide*.

   Through HTTPS

   a. Enter **https://192.168.4.44:8443/imc** in the address bar of your browser and press **Enter.** **192.168.4.44** is the IP address of the master server, and **8443** is the HTTPS port set the first time the IMC platform subcomponents were deployed.

   b. A security certificate message appears. For more information, see *HP IMC Getting Started Guide*.

   c. Confirm the message and the IMC login page appears.

2. Enter the username and password and click **Login**.

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

   To enhance security, change the superuser password after login.

   - When the UAM user self-service component is deployed, access the IMC self-service center by entering either of the following addresses in the address bar of the browser:

     http://192.168.4.66:8080

     http://192.168.4.66:8080/selfservice

     192.168.4.66 is the IP address of the server where the UAM user self-service is deployed and **8080** is the HTTP port number set the first time the IMC platform subcomponents were deployed.

   - When the SOM service desk is deployed, access the service desk by entering **http://192.168.4.22:8080/servicedesk** in the address bar of the browser.

192.168.4.22 is the IP address of the server where the SOM service desk is deployed and **8080** is the HTTP port number set the first time the IMC platform subcomponents were deployed.

If you cannot access IMC using the Web browsers, check your hardware and browser configuration.

Table 9 Hardware and browser requirements

OS	Hardware	Browser version	Browser setting requirements
Windows	• CPU: 2.0 GHz or higher • Memory: 2 GB or higher • Hard Disk: 20 GB or higher • CD-ROM: 48 X or higher • Network Adapter: 100 Mbps or higher • Sound card: Required.	IE 9 or 10 Firefox 20 or later Chrome 26 or later	• Turn off the pop-up blocker. • Enable Cookies in Internet Explorer. • Add the IMC site to the trusted sites. • The recommended resolution width is 1280.

Displaying a user agreement

You can display a user agreement on the IMC login page to inform operators of the rights and obligations for 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 master server, access the **\client\conf** directory (**/client/conf** on Linux) in the IMC installation path.
2. Open the **commonCfg.properties** file in WordPad or vi.
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**.
6. Save the **terms.html** file to the **\client\web\apps\imc** directory (**/client/web/apps/imc** on Linux) in the IMC installation path.

Re-enter the IMC login page. A **User agreement** link appears under the username and password area. Operators can click the link to view terms of the user agreement. The **Login** button is grayed out unless **I accept the terms in the user agreement** is selected.

8 Upgrading, backing up, or removing IMC

The following information describes how to upgrade IMC components, using upgrading IMC Platform patches as an example.

After installing the IMC Platform and components, when you want to upgrade the IMC Platform, first make the following preparations:

- Components require IMC V5.0 or a later version. For the compatibility matrix, see the readme file.
- For data safety, HP recommends that you back up the database and the entire IMC installation path because it is not done during upgrade.
- Download the upgrade packages for all listed components before you upgrade the IMC Platform.

Backing up IMC

You can back up the IMC installation directory and database files.

To back up the IMC installation directory, execute the **backup.bat** script that is located in the IMC installation package. If IMC uses a local database, the **backup.bat** script also backs up the database files.

To backup files of a remote database, use **Dbman** in the Intelligent Deployment Monitoring Agent. Dbman cannot back up the IMC installation directory.

Because IMC uses a local database and is deployed in centralized mode, you could back up IMC by executing the **backup.bat** script on the IMC server. If IMC is deployed in stateful failover mode, back up IMC by executing the **backup.bat** script only on the servers that are online.

1. Log in to the operating system as an **Administrator**.
2. Run the **install\backup.bat** script in the downloaded installation package. The **Backup IMC** window appears, as shown in Figure 61.

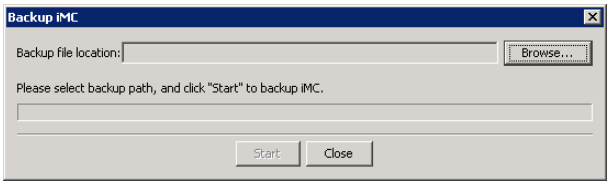
CAUTION:

- To back up IMC in Windows Server 2003 or Windows Server 2003 R2, you must log in as an administrator and back up IMC.
- To back up IMC in Windows Server 2008 or Windows Server 2008 R2, you must first right-click the **backup.bat** script and select **Run as Administrator** from the shortcut menu, or modify the **User Account Control Settings** and restart the server. After backing up IMC, you can restore the related settings as needed.
- To modify the user account control settings, select **Start** > **Control Panel** > **System and Security**, click **Change User Account Control Settings** in the **Action Center**, and set the **Choose when to be notified about changes to you computer** to **Never notify** in the **User Account Control Settings** window.

To back up IMC on Linux, you must start the IMC installation wizard by running the **backup.sh** script in the install directory of the IMC installation package as a root user.

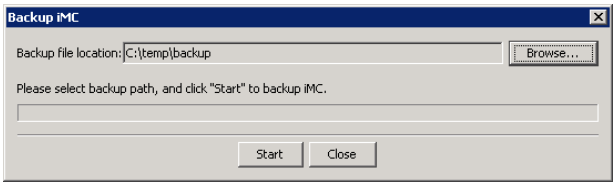
When the installation file is obtained via FTP, you must first authorize the **install.sh** script by executing **chmod –R 775 install.sh** in the directory of the script.

Figure 61 Backing up IMC



3. Check the size of the backup files and make sure the disk for saving the files has enough memory. Insufficient memory may cause backup failure.
4. Click **Browse** to customize the location for saving the backup files.

Figure 62 Choosing the backup file location



5. Click **Start** to start backing up IMC.

   After the backup is complete, the backup file directory generates a package **IMC.zip**, which contains the complete backup files under the IMC installation path. In the backup directory also is a folder named **db**, which contains the database backup data of all components.

Upgrading IMC

CAUTION:

- Make sure you have compatible upgrade packages for all deployed IMC components. Otherwise, IMC becomes invalid after upgrade.
- To upgrade IMC from version 3.x to version 5.x, re-log in to the registration website and obtain a new activation file.
- Do not upgrade IMC by running the **install\install.bat** script in the IMC installation path.

To upgrade an IMC component, ensure that the IMC Platform has been installed, and the components on which the component you want to upgrade depends have been installed and upgraded. Before you upgrade a service component that is related to the Report Management subcomponent, upgrade the Report Management subcomponent to a version compatible with the service component. Otherwise, the report function might be abnormal.

The following example describes how to upgrade the IMC Platform.

1. Use one of the following ways to start upgrade:
   - On the **Installation Completed** window, as shown in Figure 41, select **Install Other Components**, and click **Finish**.
   - After you have installed and deployed the IMC Platform, click **Start** > **All Programs** > **HP Intelligent Management Center** > **HP Deployment Monitoring Agent** (or run the **dma.sh** script in /deploy of the IMC installation path on Linux), to start the Intelligent Deployment Monitoring Agent and click **Install new components** on the **Monitor** tab.

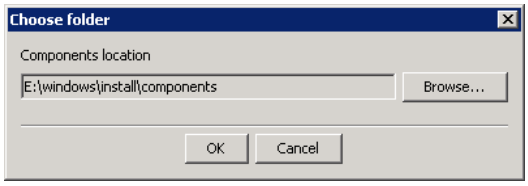
CAUTION:

- To upgrade IMC in Windows Server 2003 or Windows Server 2003 R2, log in as an administrator and upgrade IMC.
- To upgrade IMC in Windows Server 2008 or Windows Server 2008 R2, you must first select **Start** > **All Programs** > **HP Intelligent Management Center**, right-click **Deployment Monitoring Agent**, and select **Run as Administrator** from the shortcut menu to open the deployment monitoring agent, or modify the **User Account Control Settings** and restart the server. After upgrading IMC, you can restore the related settings as needed.
- To modify the user account control settings, select **Start** > **Control Panel** > **System and Security**, click **Change User Account Control Settings** in the **Action Center**, and set the **Choose when to be notified about changes to you computer** to **Never notify** in the **User Account Control Settings** window.

2. On the system tray of Windows, right-click the **Deployment Monitoring Agent** icon, and select **Install** from the menu.

   The **Choose folder** window appears.

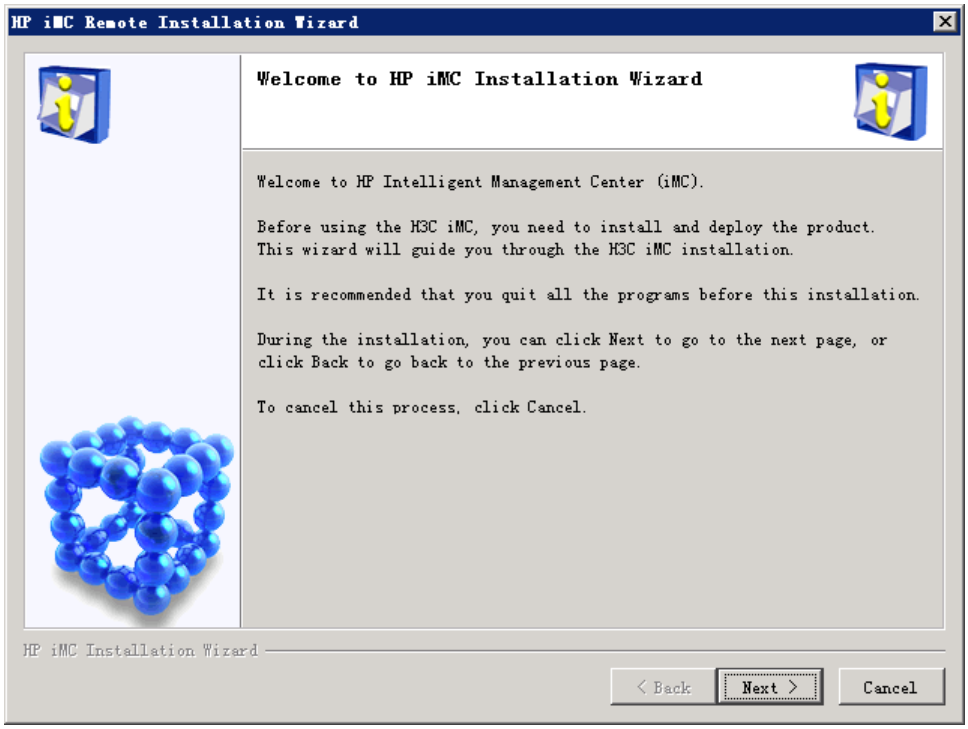
Figure 63 Choose folder



3. Click **Browse**, and select folder **install\components** in the upgrade files.
4. Click **OK**.

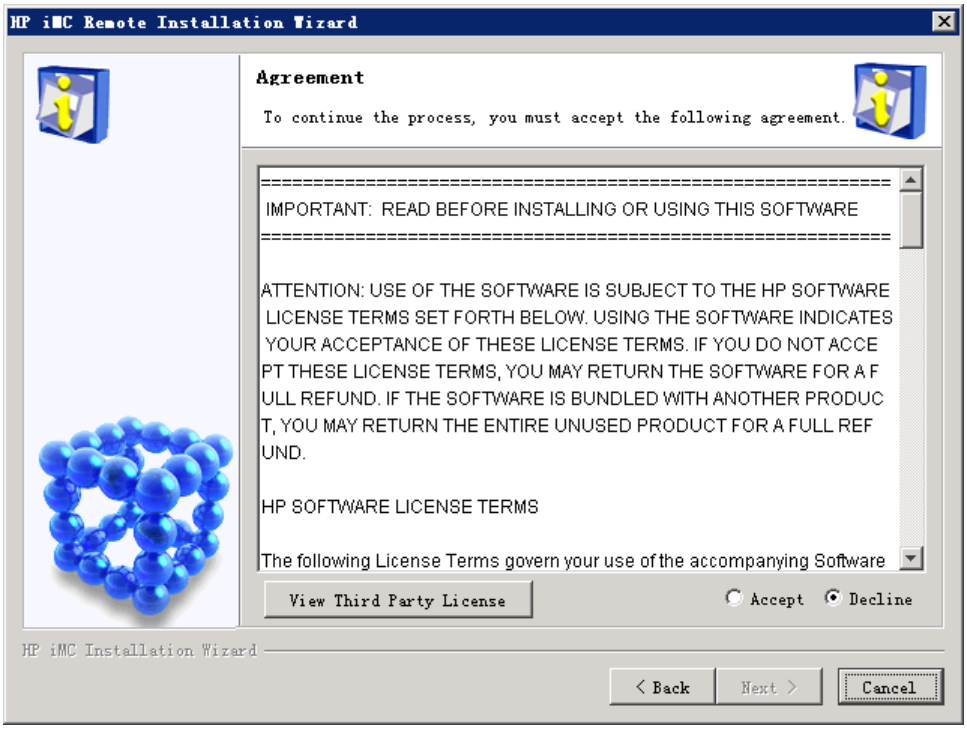
   The **Welcome to HP IMC Installation Wizard** window appears.

Figure 64 Welcome to HP IMC Installation Wizard



5. Click **Next**. The **Agreement** window appears.

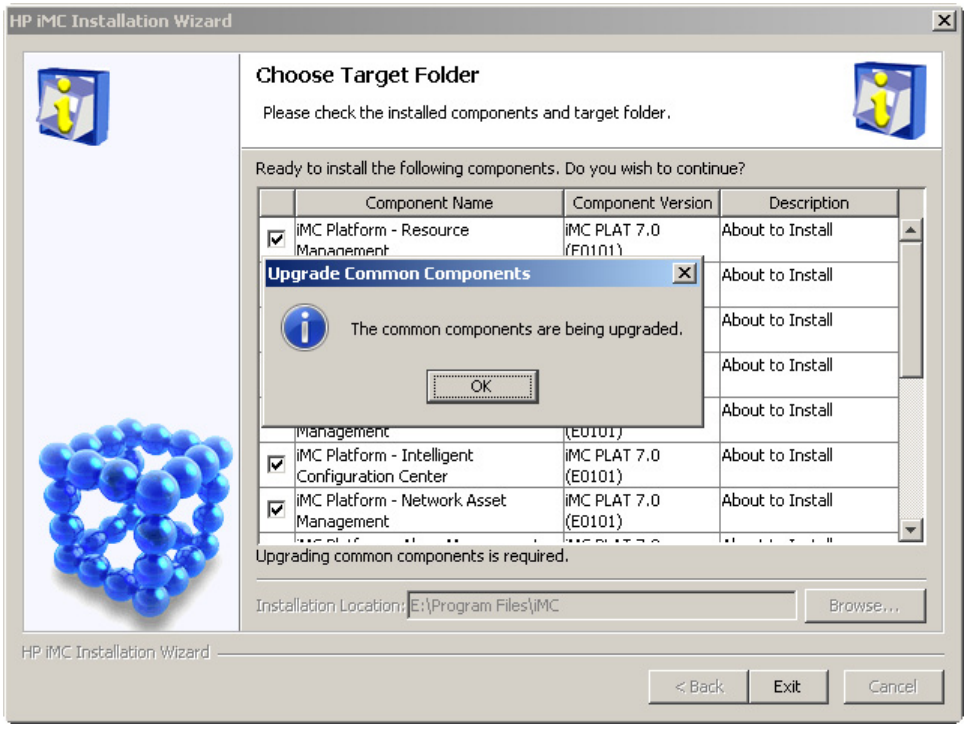
Figure 65 Agreement



6. Read the license agreement carefully, select **Accept**, and click **Next**.

   The **Upgrade Common Components** window appears.

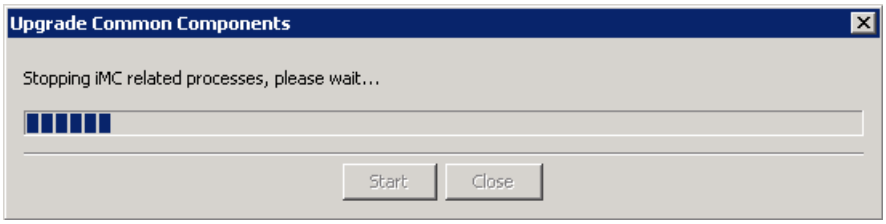
Figure 66 Upgrade Common Components



7. Click **OK**.

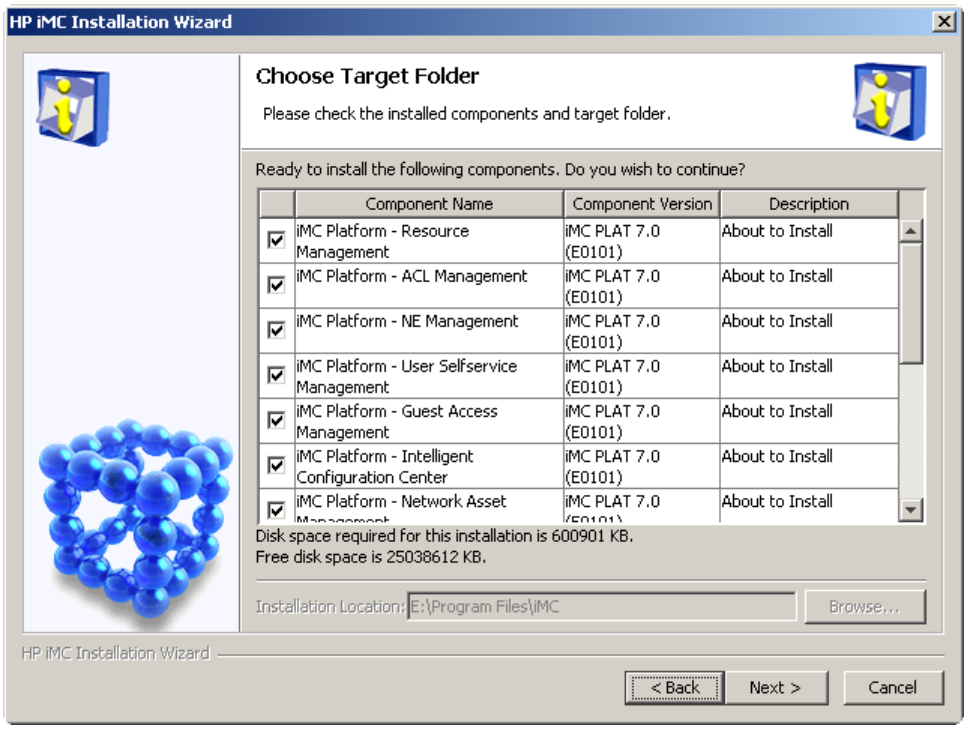
The system starts upgrading common components, as indicated by the **Upgrade Common Components** window.

Figure 67 Upgrade Common Components



After the common components are upgraded, the **Choose Target Folder** window appears.

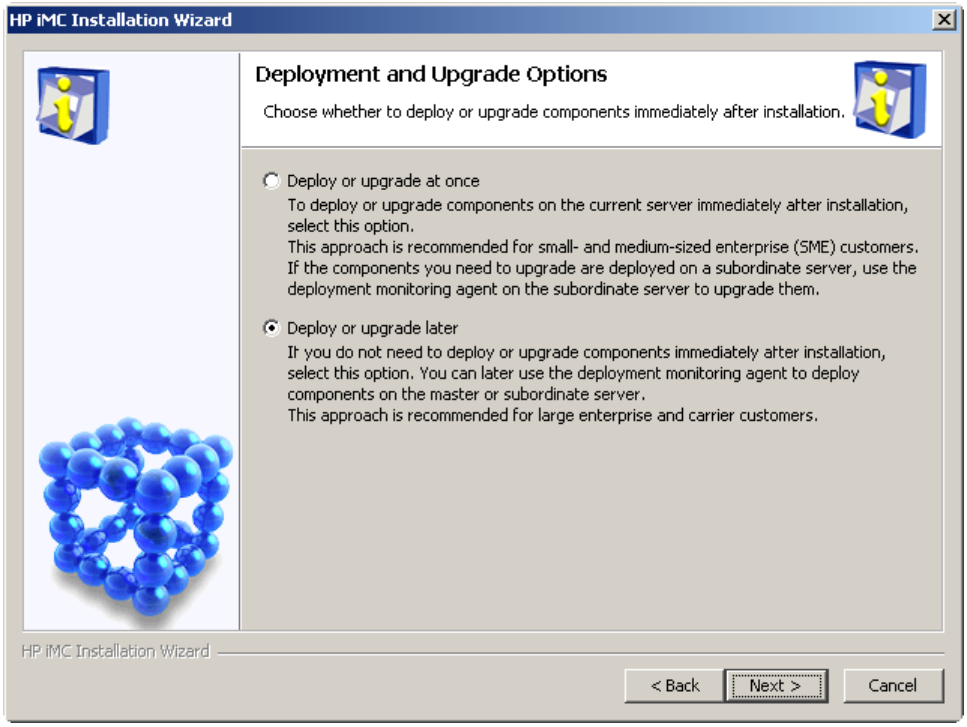
Figure 68 Choose Target Folder



The **Choose Target Folder** window displays the components to be upgraded. The system installs the upgrade files in the location where the IMC Platform is installed.

8. Check the information, click **Next**, and the **Deployment and Upgrade Options** window appears.

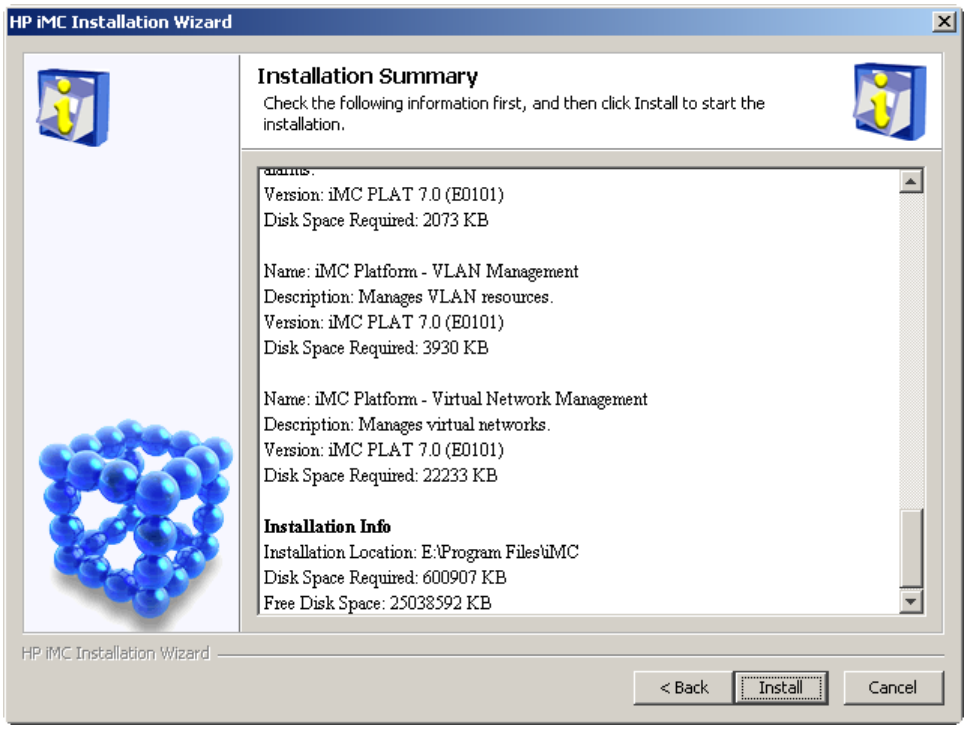
Figure 69 Deployment and Upgrade Options



9. Select a deployment and upgrade option as prompted by the window.

   In this example, select **Deploy or upgrade at once**, and click **Next**. The **Installation Summary** window appears.

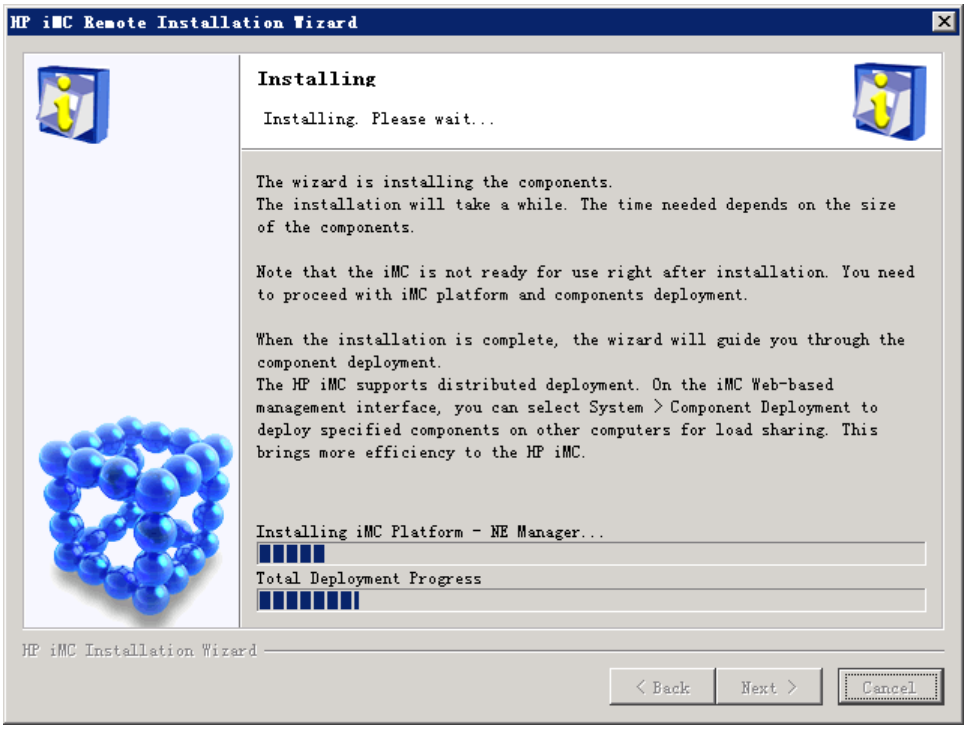
Figure 70 Installation Summary



10. Check the installation summary and click **Install**.

The **Installing** window appears.

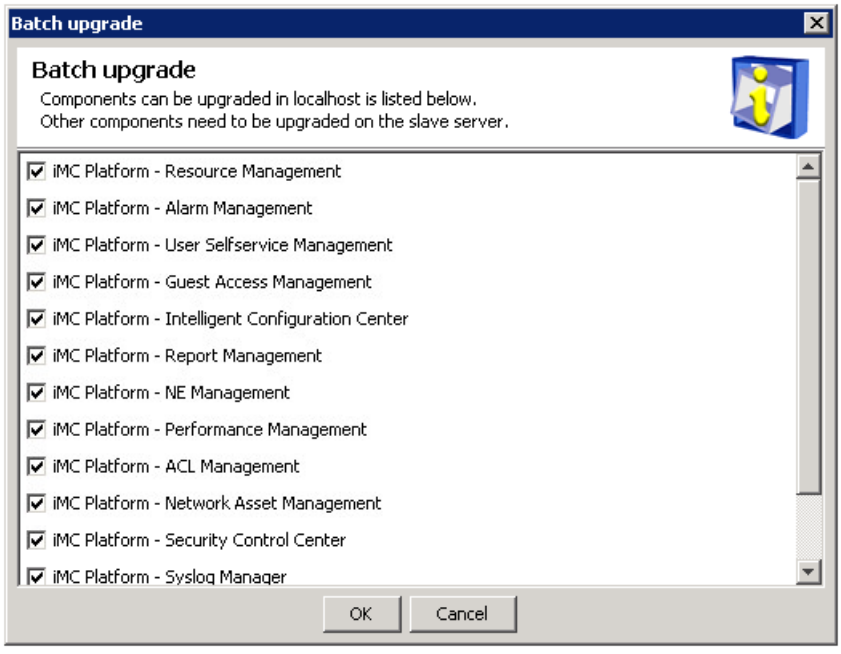
Figure 71 Installing



The installation wizard installs the components.

After the installation is finished, the **Batch upgrade** window appears.

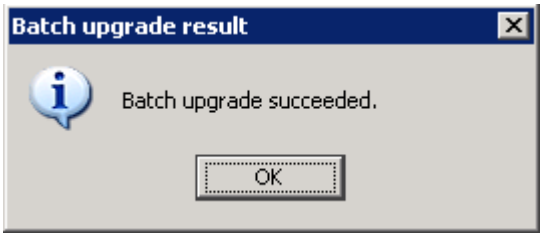
Figure 72 Batch upgrade



11. Select the components you want to upgrade and click **OK**.

    After the selected components are upgraded, the **Batch upgrade result** window appears.

Figure 73 Batch upgrade result



12. Click **OK**.

    If you have used Dbman for IMC auto backup or restoration before upgrade, the **Auto Backup and Restore Configuration** window appears.

13. Click **OK**.

    The automatic backup and restoration process starts. After that, you can launch IMC by clicking **Start IMC** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent.

    After the processes of all components are started normally, IMC is ready for use.

    When upgrading service components related to the Report Management module, you must also upgrade the Report Management module to the version compatible with these related service components, so that you can use the report function properly.

Restoring IMC

CAUTION:

In the Windows operating system, use WinRAR or 7-Zip to decompress the package, rather than the decompression tool included with the Windows system.

When an error occurs during the IMC upgrade, check the environment (for example, check whether the database is available) and upgrade IMC again. If the IMC upgrade still fails, follow these steps to restore IMC to the version before the upgrade:

1. Restore IMC database. See "Manual restore."
2. When the restoration is complete, stop the Intelligent Deployment Monitoring Agent and IMC service.
3. Manually delete all the files in the IMC installation path.
4. Decompress the **IMC.zip** package to the IMC installation path.
5. Restart the Intelligent Deployment Monitoring Agent and IMC service.

For IMC deployed in stateful failover mode, only restore IMC on the servers that are online.

Removing IMC

Removing IMC on Windows and Linux systems is similar. The following describes how to remove IMC from a Windows Server 2008 R2-based machine.

Removing an IMC component

Before removing an IMC component, remove any components that depend on it.

1. Launch the Intelligent Deployment Monitoring Agent on the IMC server.
2. On the **Monitor** tab, click **Stop IMC** to stop the IMC service.
3. On the **Deploy** tab, select **Undeploy the Component** from the right-click menu of the component that you want to undeploy.

   A dialog box appears, indicating that the component was successfully undeployed.
4. Click **OK**.
5. On the **Deploy** tab, select **Remove this Component** from the right-click menu of the component that you have undeployed.

   A dialog box appears, indicating that the component was successfully removed.
6. Click **OK**.

Removing all IMC components at one time

The following sections describe how to remove the IMC software deployed in centralized modes.

When reinstalling IMC, you must manually delete the folder named **IMCdata**, which is created on the IMC server upon installation of IMC when you have re-installed an SQL Server database after you uninstalled IMC.

When you fail to install or uninstall IMC, manually delete the IMC installation folder and the **IMC-Reserved** folder in the Windows installation directory (or delete this folder in the **/etc** directory on Linux operating systems). Otherwise, IMC cannot be reinstalled.

1. Launch the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop IMC** to stop the IMC service.
3. Launch the IMC uninstaller.
   - On windows, select **Start** > **All Programs** > **HP Intelligent Management Center** > **Uninstall HP Intelligent Management Center**.
   - On Linux, run the **uninstall.sh** script in **/deploy** of the IMC installation path.

   A window appears to guide you through the rest of the process.
4. Click **Uninstall**.
5. Click **Finish** when the **Uninstallation Completed** dialog box appears.
6. Delete the **IMC-Reserved** folder in the WINDOWS folder of the system disk (or delete the **IMC-Reserved** folder in the /etc/ directory on Linux).
7. Reboot the system.

9 Registering IMC and incremental node licenses

An unregistered IMC version delivers the same functions as that of a registered IMC, but can be used only for 60 days since the date on which the IMC service was first started. To unlock the time limitation or add extra nodes to IMC, the IMC licenses you have purchased must be registered and activated in the IMC Platform.

The IMC registrations on Windows and Linux systems are similar. The following describes how to register IMC on a Windows Server 2008 R2-based machine. Ensure you Register and Activate IMC before any additional node licenses.

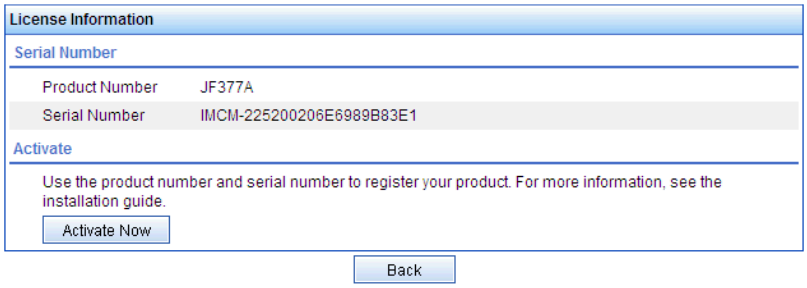
NOTE:

To transfer an existing license to a different Serial Number, contact HP Support.

Registering IMC

From the IMC login page click on the **Activate** link to enter the **License Information** page appears.

Figure 74 License Information



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

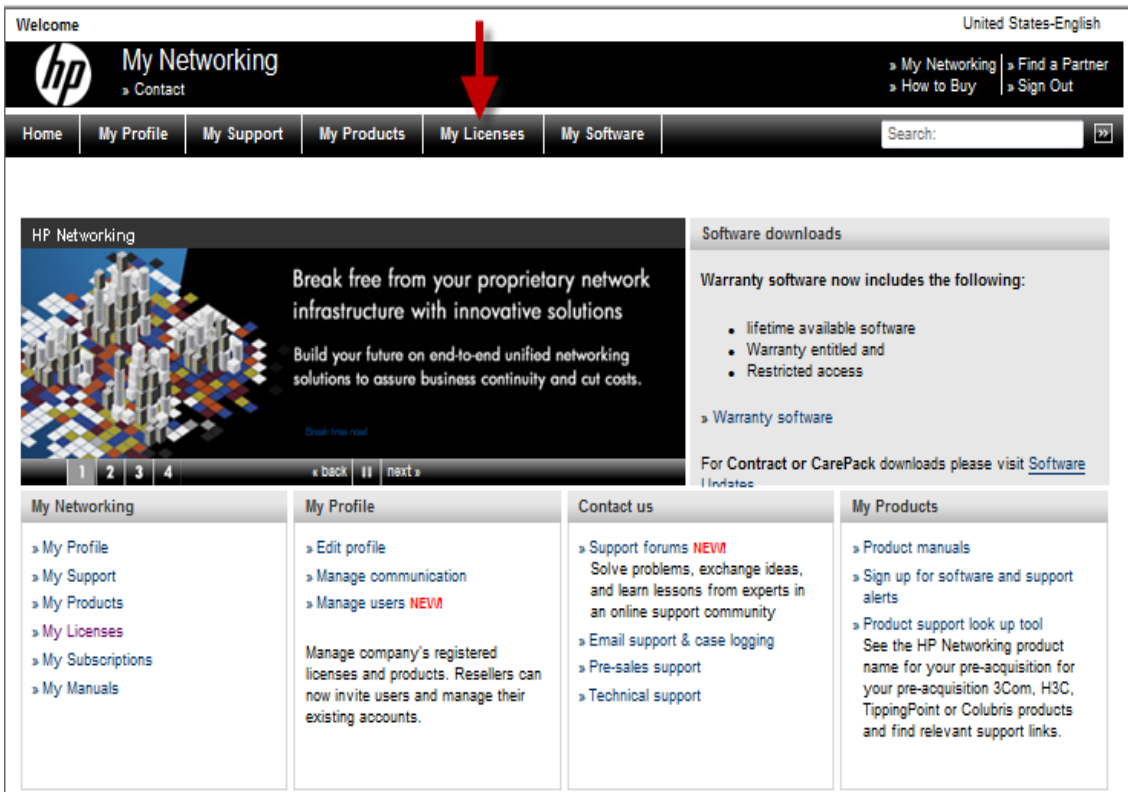
Registering first license

1. Go to the HP My Networking system website (http://hp.com/networking/mynetworking/), log in to My Networking portal, and the **HP Passport sign-in** page appears.

Figure 75 HP Passport sign-in

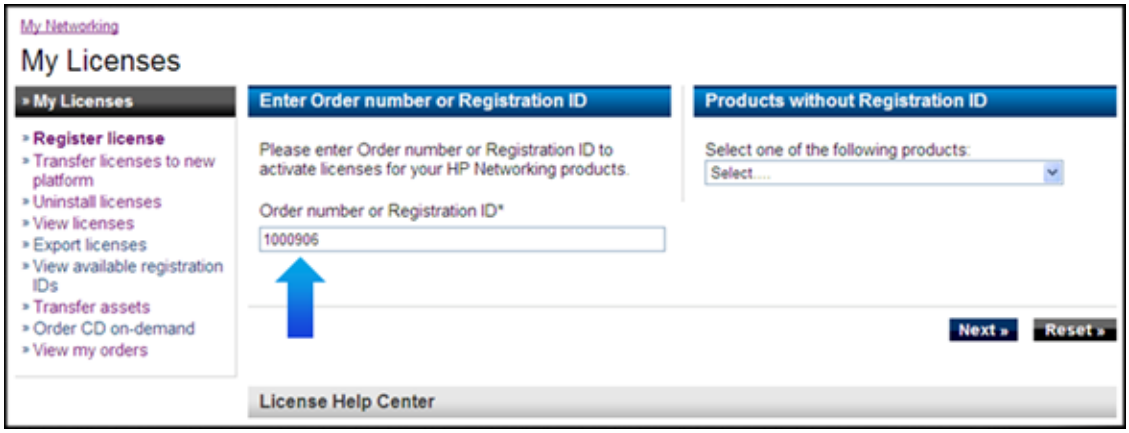
2. Enter the **User ID** and **Password** and click **Sign in**.
   The **Welcome** page appears.

Figure 76 Welcome page



3. Click the **My Licenses** tab from the tabular navigation system on the top.
   The **Enter Order number or Registration ID** page appears.

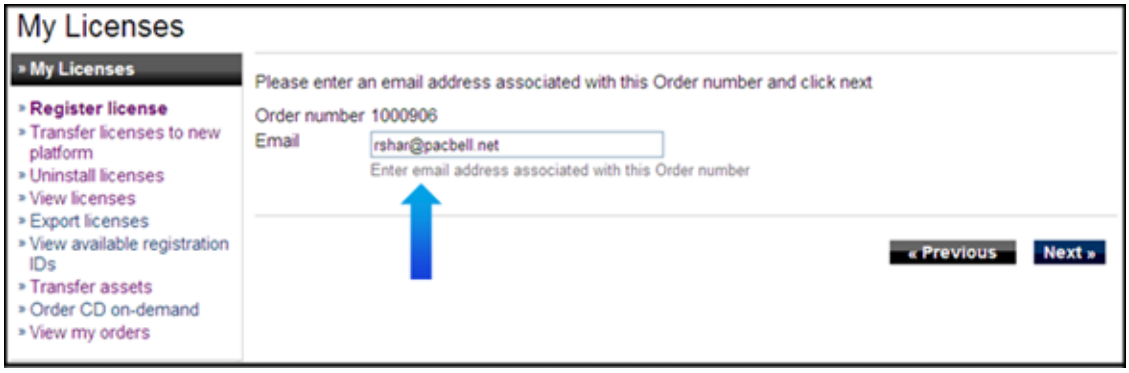
Figure 77 Enter Order number or Registration ID page



4. Enter the **Order number** or **Registration ID**, and click **Next**.

   The **Enter the email associated with Order number** page appears.

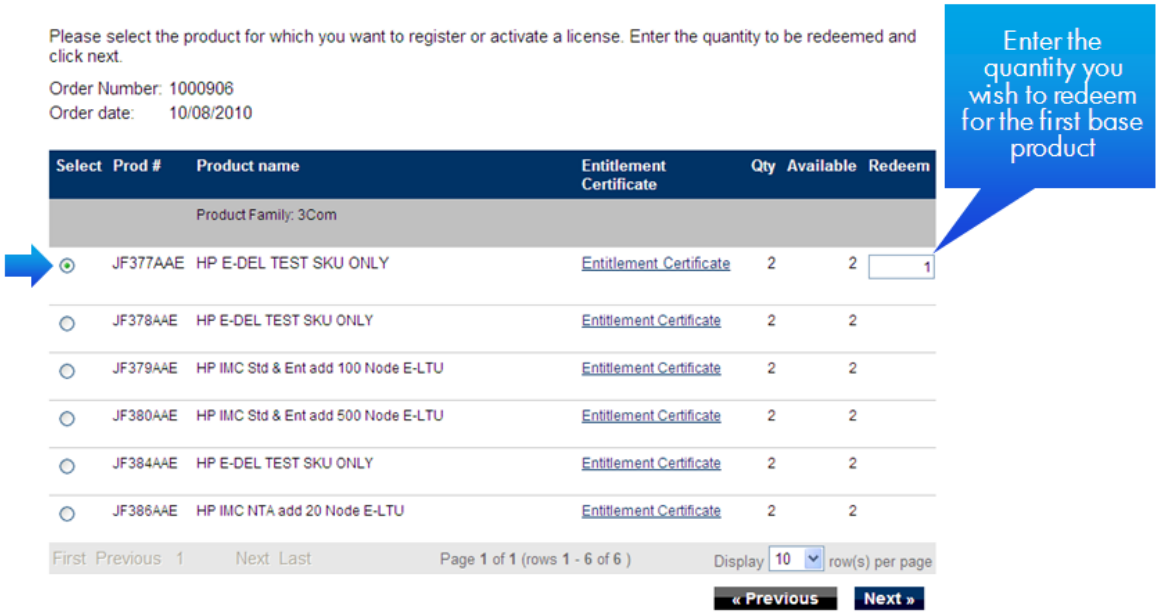
Figure 78 Enter the email associated with Order number page



5. Enter an email address associated with the **Order number** and click **Next**.

   The **Select the Product License** page appears.

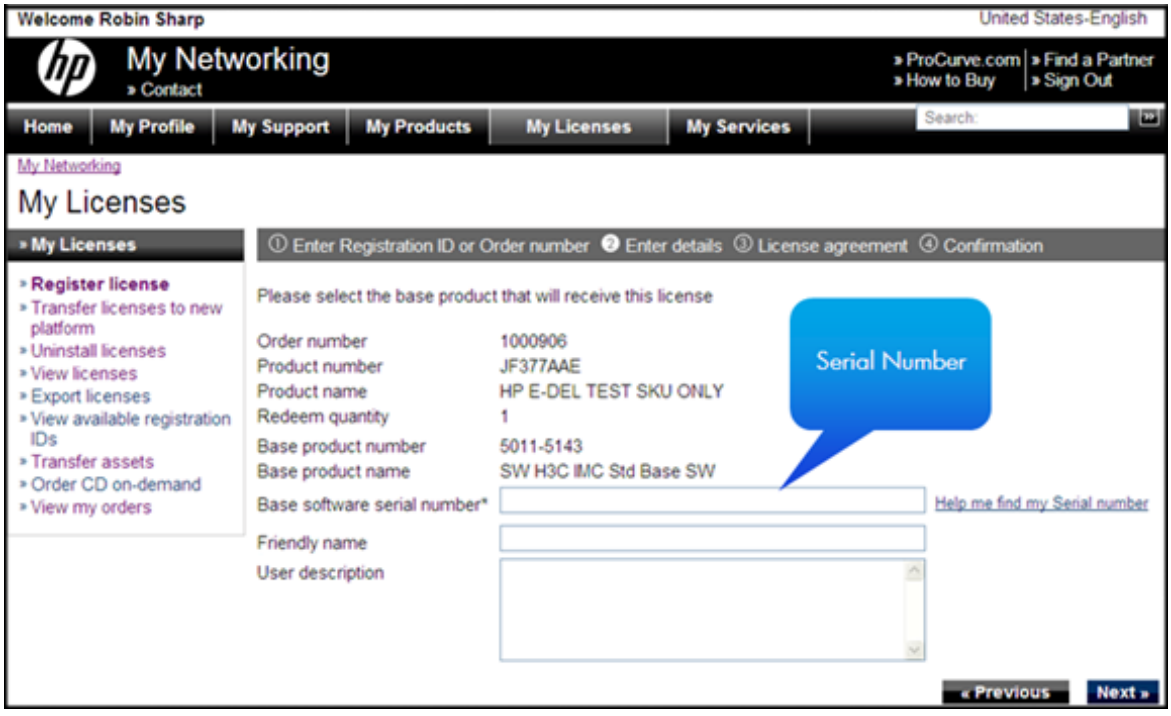
Figure 79 Select the Product License page



6. Select the product for which you want to register or activate a license.
7. Enter the quantity to be redeemed and click **Next**.

   The **Enter details** page appears.

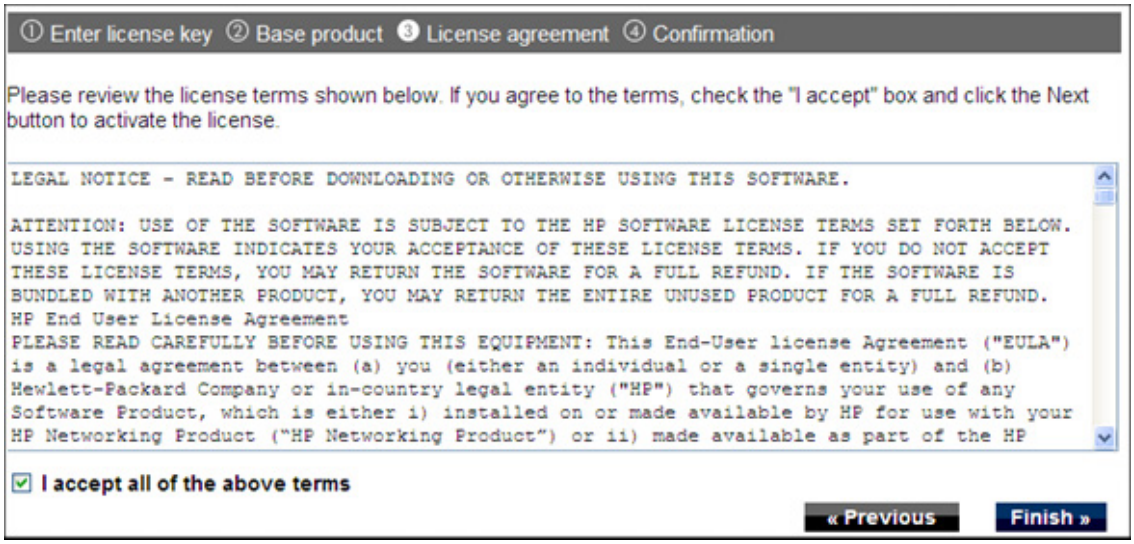
Figure 80 Enter details page



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

   The **License agreement** page appears.

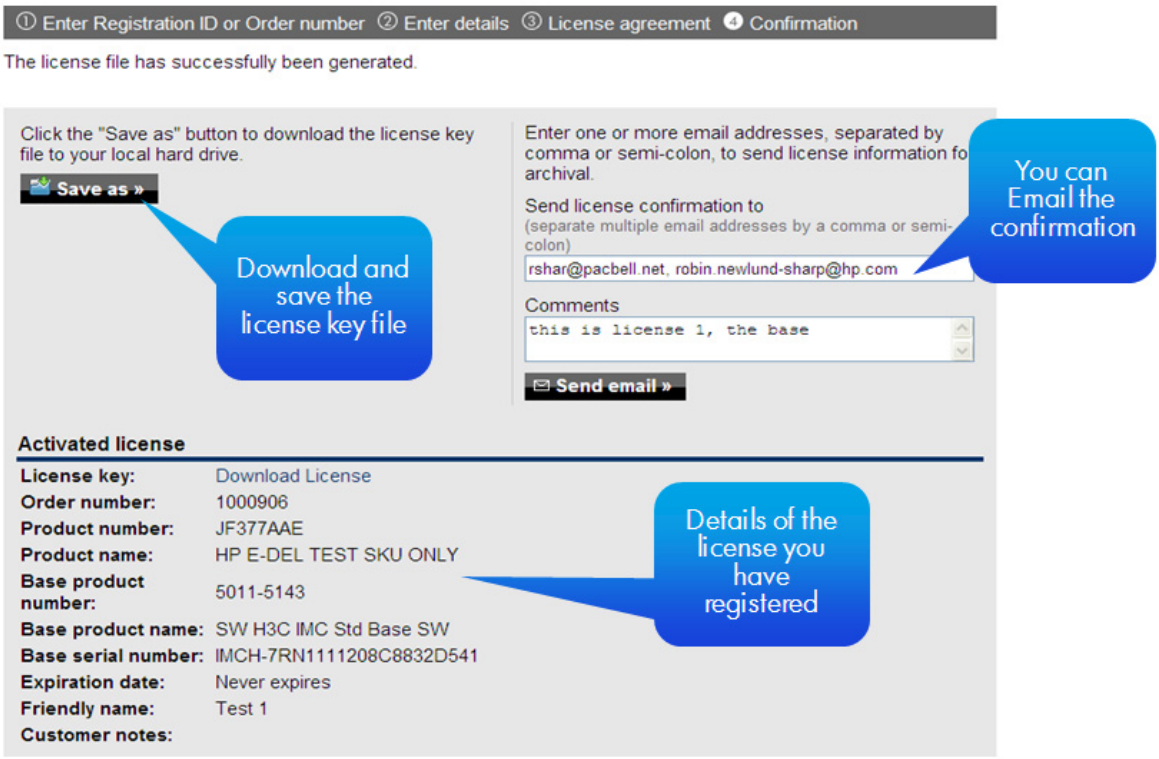
Figure 81 License agreement page



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

   The **Confirmation** page appears.

Figure 82 Confirmation page



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

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

11. When you need to email the confirmation, enter the **Send license confirmation to** and **Comments** and click **Send email** on this page. Also, you can view the details of the license you have registered.

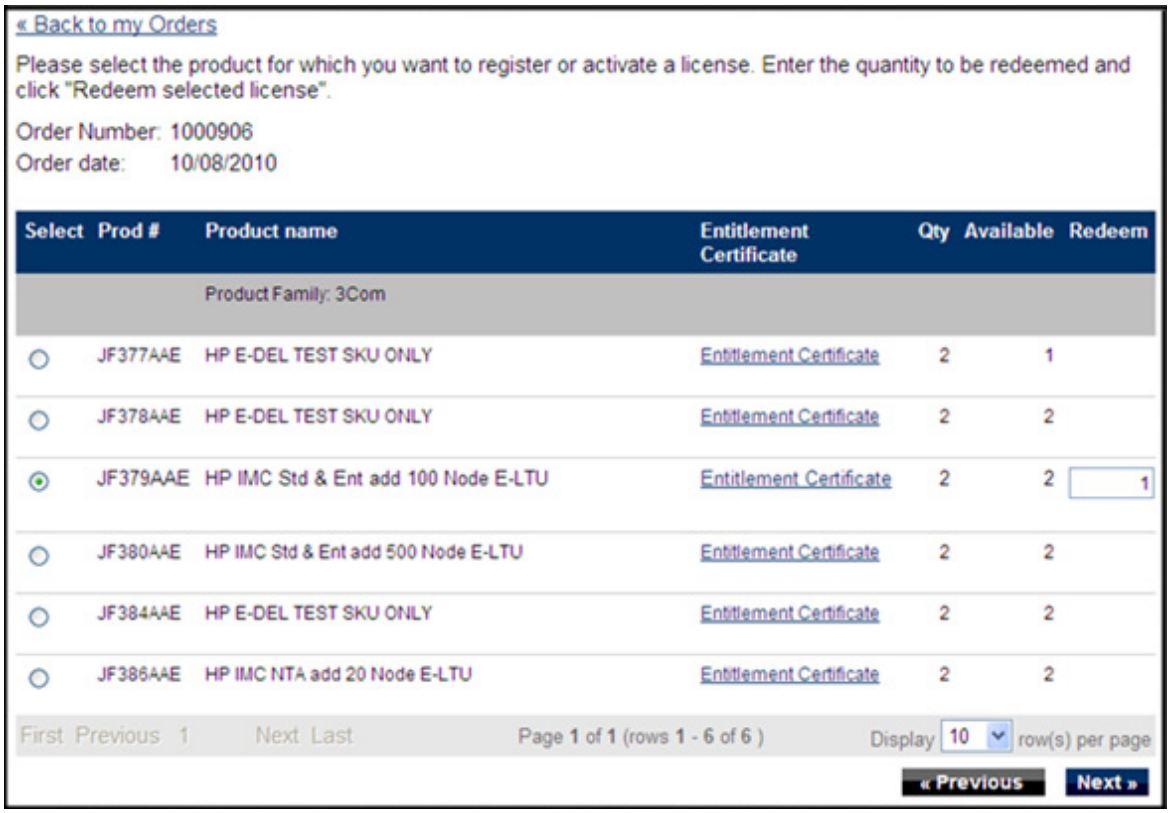
Registering incremental node licenses

Registering an Incremental Node License is similar to registering the first license. This 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.

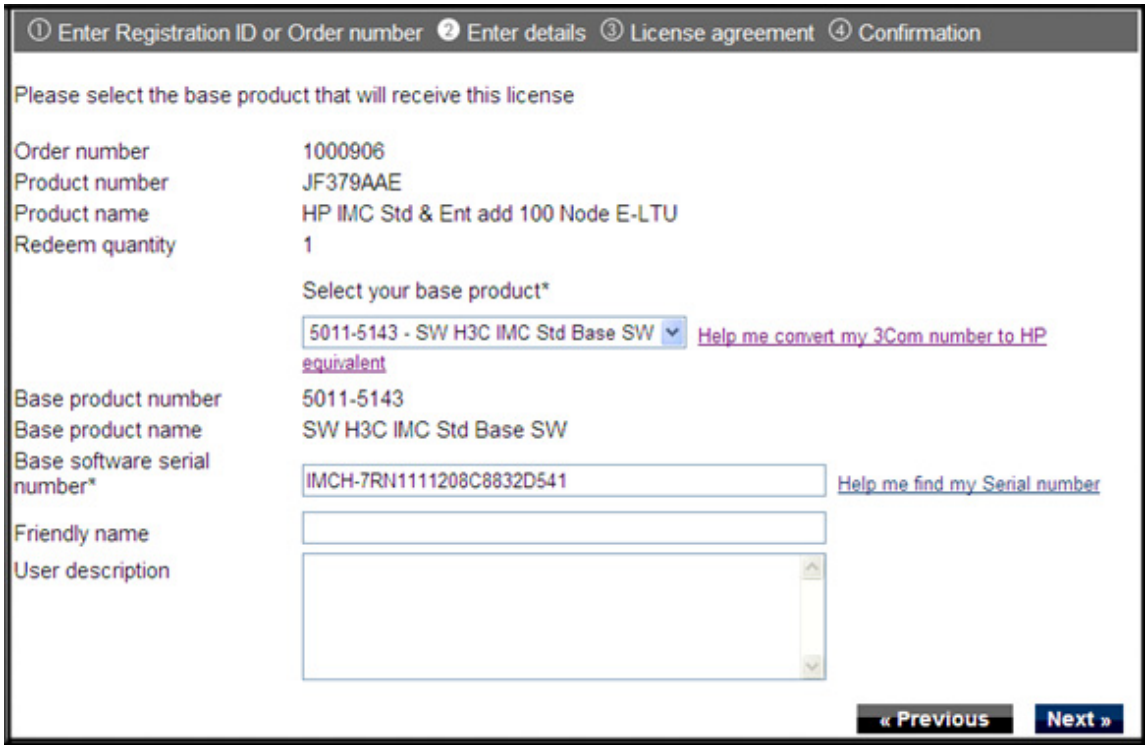
Figure 83 Select the Product License page



2. Click **Next**.

   The **Enter details** page appears.

Figure 84 Enter details page



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

   The **Confirmation** page appears (see Figure 82).

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

   You need to remember the location and file name for the next step of Activating the License in IMC.

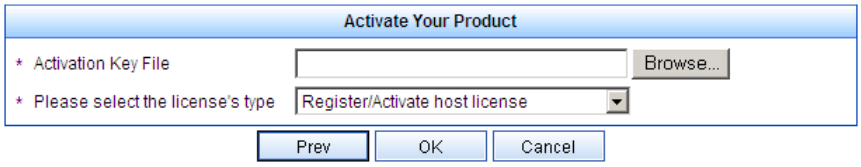
Activating IMC

To activate IMC:

1. Return to the **License Information** page (see Figure 74).
2. Select **Activate now.**

   The **Activate Your Product** page appears.

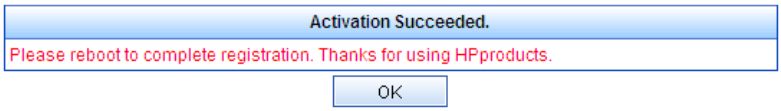
Figure 85 Activate Your Product



3. Select the license file in the format of .txt.
4. Select the license type, which can be **Register/Activate host license** or **Register/Activate back-up license**, as needed.
5. Click **OK**.

   The **Activations Succeeded** dialog appears.

Figure 86 Activation Succeeded



6. Reboot the system.

   Your IMC system has now been successfully Registered and Activated.

Upgrading to an IMC V7.0 license

Your existing eSupport account including your IMC licenses have been transferred to My Networking and a HP Passport account has been created with your eSupport user name.

The HP My Networking system address: http://hp.com/networking/mynetworking.

Your IMC license file has been updated in My Networking to support IMC V7.0.

You need to download your updated IMC license file from My Networking and reactivate your IMC V7.0.

To update your IMC license file from My Networking and reactivate your IMC V7.0:

1. Locate your IMC Serial Number:
   a. Follow the **Activate** link from the IMC login page to enter the **License Information** page and your IMC serial number appears.
   b. Select your IMC serial number, and copy and paste the serial from the IMC License information page to My Networking.
2. Reset your new HP Passport password so you can login to My Networking using your new HP Passport account:
   a. Go to the HP My Networking system website: http://hp.com/networking/mynetworking.
   b. Log in to My Networking portal, and the **HP Passport sign-in** page appears.

   Your eSupport user account has been transferred to My Networking and a HP Passport account has been created using your eSupport user name.
   c. Reset your HP Passport password before you can log in by following the **Forgot Password** link.
   d. Provide the email address of your eSupport account user to receive instructions on resetting your password.
   e. Follow the email instructions to click on the **Choose a new password** link.
   f. Enter your new HP Passport password and select your security questions and answers.

   Your HP Passport password is now reset, allowing you to log in to My Network using the HP Passport account with your eSupport user name and password.
3. Log in to My Networking
4. Click **Continue** in the Change HP Passport password page to log into My Networking.

   The **Welcome <username>** page appears.
5. Locate your IMC licenses
6. Click the **My Licenses** tab from the tabular navigation system on the top.

   The **Enter Order number or Registration ID** page appears.
7. Click on **View Licenses** from the **My Licenses** navigation.

8. Locate your IMC Platform license in the list of your licenses.

   When necessary copy and paste your IMC serial number into the search field and click **Search**.
9. Download the updated IMC license file
10. Click  corresponding to the IMC Platform license.

    The license information page appears.
11. Click the **Download License** link.
12. Choose to save the license file, and choose where to save the license file.

    Save the license file so that you can locate it again when you need it.

Updating your IMC V7.0 license file

1. Follow the Activate link on the IMC login page to enter the **License Information** page.
2. Click **Activate now.**

   The **Activate Your Product** page appears.
3. Browse to the location where you saved the license file and select it, and click **OK**.

   The **Activations Succeeded** dialog appears.
4. Select the license file which should be in .txt format.
5. Select the license type, which can be **Register/Activate host license** or **Register/Activate back-up license**, as needed.
6. Click **OK**.

   The **Activations Succeeded** dialog appears.

   Your IMC V7.0 is now fully licensed with the equivalent licenses you had previously.

10 Security and backup

Anti-virus software

To ensure the secure running of the IMC server, HP recommends that you install anti-virus software, and update the virus library.

Port settings

To ensure the steady running of the IMC server, HP recommends that you use a firewall to control the data sent to the IMC server cluster, that is, filter the non-service data sent to the IMC server. In this way, you can prevent abnormal attacks.

CAUTION:

- HP recommends that you use ACL configurations on a firewall rather than on a switch to control data packets. Otherwise, packet fragmentations are filtered.
- When you have installed firewall software on the IMC server, besides setting the ports listed in Table 10, set an IP address for the IMC server to ensure normal communication between them.

Table 10 and Table 11 list the port numbers used by IMC components.

Table 10 Port numbers used by the IMC PLAT

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	Port for the access to the IMC through HTTP	IMC server
TCP 8443, configurable	Port for the access to the IMC through HTTPS	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

Table 11 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

Default port number	Usage	Location
TCP 9099	JMX listening port for the NTA/UBA service	IMC server
UDP 18801, 18802, 18803	Communication ports between the NTA and UBA	IMC server

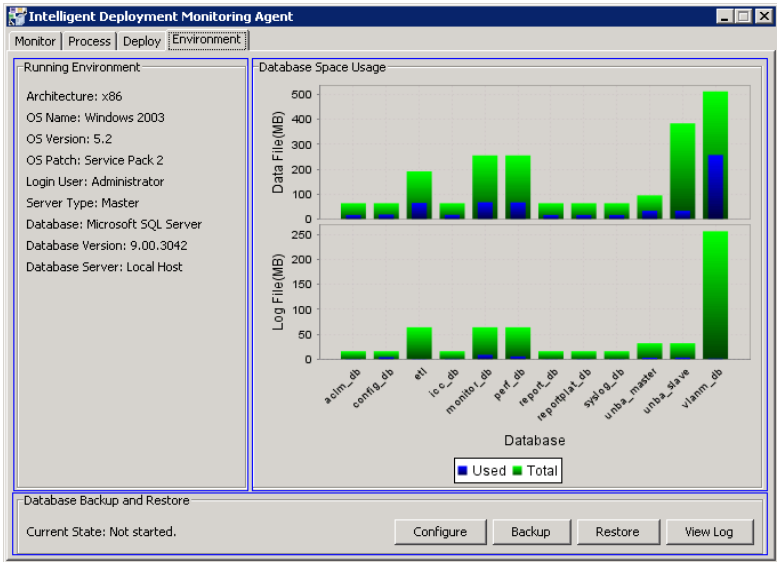
When a firewall resides between the probe and the IMC server, you need to configure an ACL on the firewall so that all the IP packets from the probe can be sent to the IMC server.

Basic database backup and restore operations

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 is integrated in the Intelligent Deployment Monitoring Agent.

Figure 87 Environment tab



The screen is broken into the following sections.

- The software and hardware information of the servers displays on the left of the **Environment** tab.
- The usage of the user database file and log file displays on the right.
- The Dbman database backup and restoration configuration displays at the bottom.

The Dbman database backup and restoration configuration includes the following options:

- **Configure**—Provides automatic backup and restoration function, which can back up and restore database files on a regular basis. You can also upload backup database files to an FTP server for storage. The automatic backup and restoration function is used mainly in stateless failover scenarios.
- **Backup**—Immediately backs up the database files of the current IMC server. This function is available only when the current IMC server uses a local database.
- **Restore**—Replace the current database files with the backup database files to restore the database to the specified time point. This function is available only when the current IMC server uses a local database.

- **View Log**—View the database backup and restoration log. The log size can be set by using the **Configure** function.

Manual backup

Manual backup allows you to manually back up IMC databases immediately. Make sure the target IMC system uses a local database, embedded or separate.

To perform a manual backup:

1. Start the Intelligent Deployment Monitoring Agent on the server.
2. Click the **Environment** tab.
3. Click **Backup**.

   The **Select database backup path** dialog box appears.
4. Select the backup file save path.
5. Click **OK**.

   Dbman starts to back up all databases used by the IMC system on the server to the specified path.

Manual restore

CAUTION:

When restoring databases of the IMC system, also restore databases of all components that have been deployed. If you restore only some of them, data loss might occur.

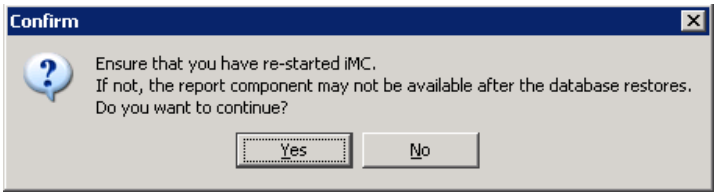
Manual restoration allows you to restore the IMC database files of a specified backup time point. Make sure IMC is started at least once after installation and the backup database files exist.

To perform a manual restoration:

1. Start the Intelligent Deployment Monitoring Agent on the server.
2. Click the **Environment** tab.
3. Click **Restore**.

   A confirmation dialog box appears.

Figure 88 Confirmation dialog box



4. Click **Yes**.
5. Select database files of all components and click **OK** in the popup dialog box.
6. Click **OK** in the popup dialog box.

   Dbman starts to restore the databases and displays a restoration success message after the restoration is complete.
7. Click **OK**. IMC will be automatically started.

NOTE:

During the restoration process, Dbman shuts down and restarts IMC and database.

Automatic backup

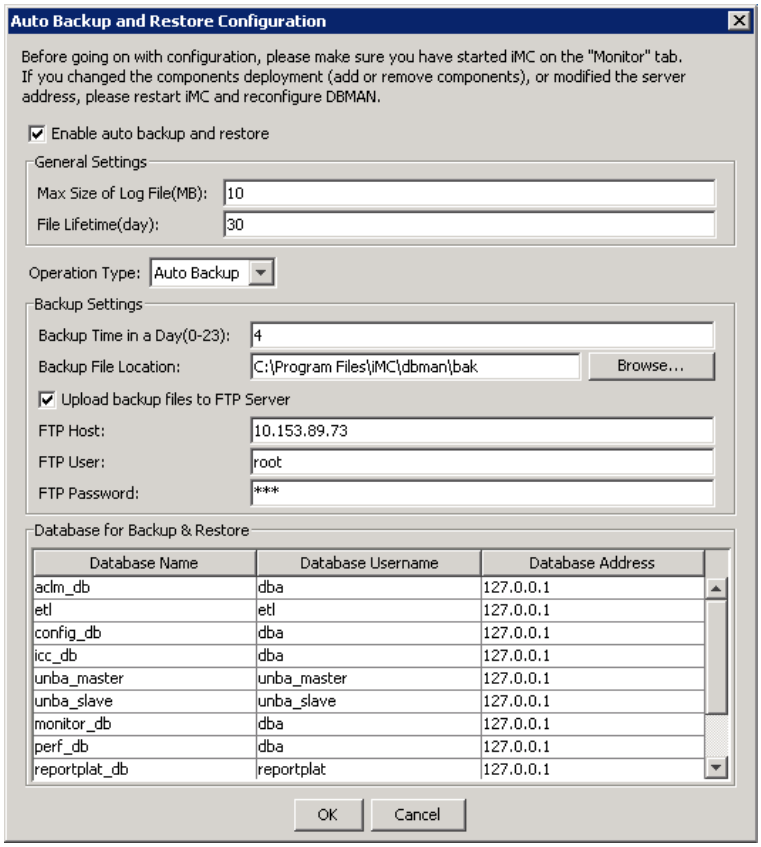
You can configure automatic database backup to periodically back up the IMC database files to the local database, and to upload the backup database files to the FTP server (Make sure FTP service is enabled on the server installed with IMC).

To configure automatic backup:

1. Start the Intelligent Deployment Monitoring Agent on the local server.
2. Click the **Environment** tab.
3. Click **Configure**.

   The **Auto Backup and Restore Configuration** dialog box appears.

Figure 89 Auto Backup and Restore Configuration



4. Enable automatic database backup and restoration and configure general parameters:
   - **Enable auto backup and restoration**—Enable or disable Dbman.
   - **Max Size of Log File**—Enter the maximum size of the log file for database backup and restoration, in MB. If the log file exceeds the maximum size, the system automatically creates a new log file. Log files are stored in the **IMC_install\dbman\log** directory.
   - **File Lifetime**—Enter how many days an automatic backup or restoration file can be kept. Expired files are automatically removed.

5. Configure the following automatic restoration parameters:
   - **Operation Type**—Select the operation to perform, automatic backup or automatic restoration. Select **Auto Backup** in this configuration.
   - **Backup Time in a Day**—Enter the hour at which the automatic backup operation starts every day.
   - **Backup File Location**—Enter or browse to the path where backup files are located. Make sure the path is located on a disk that has enough free space. Do not set the path to the operating system drive because the operating system cannot start normally when this drive is fully occupied.
   - **Upload backup files to FTP Server**—Select this option to specify an FTP server to store backup files.
   - **FTP Host**—Enter the IP address of the FTP server.
   - **FTP User**—Enter the FTP username. With a username specified, IMC automatically uploads the backup database files to the working directory of the user on the FTP server. Without a username, IMC uploads the backup database files to the root directory of the FTP server.
   - **FTP Password**—Enter the FTP user password.
6. Click **OK**.

   Dbman automatically backs up the IMC databases at the specified time and uploads the backup database files to the FTP server.

Automatic restore

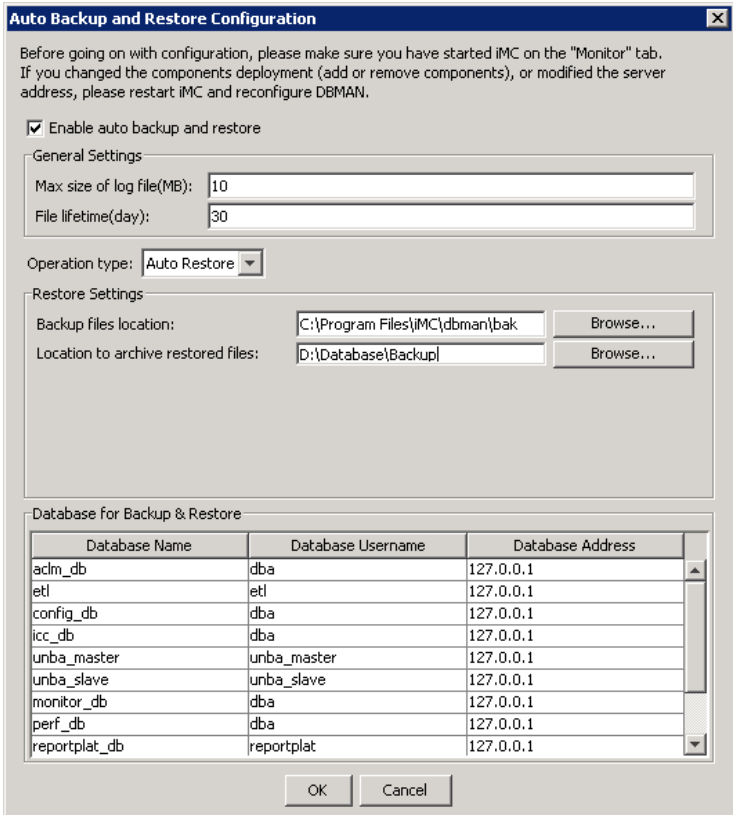
Automatic restoration applies to stateless failover scenarios to regularly restore IMC service database files on an IMC server or database server. You can configure automatic backup on the primary server and enable the FTP server function on the backup server. When new backup database files are uploaded from the primary server, the backup server immediately replaces existing database files with the new files to implement database restoration.

To configure automatic restoration:

1. Start the Intelligent Deployment Monitoring Agent on the local server.
2. Click the **Environment** tab.
3. Click **Configure**.

   The **Auto Backup and Restore Configuration** dialog box appears.

Figure 90 Auto Backup and Restore Configuration



4. Enable automatic database backup and restoration and configure general parameters:
   - **Enable auto backup and restoration**—Enable or disable Dbman.
   - **Max size of log file**—Enter the maximum size of the log file for database backup and restoration. If the log file exceeds the maximum size, the system automatically creates a new log file. Log files are stored in the **IMC_install\dbman\log** directory.
   - **File lifetime**—Enter how many days an automatic backup or restoration file can be kept. Expired files are automatically removed.
5. Configure the following automatic restoration parameters:
   - **Operation type**—Select the operation to perform, automatic backup or automatic restoration. Select **Auto Restore** in this configuration.
   - **Location to archive restored files**—Enter or browse to the path where the files to be restored are located. The path must be the same as the default working directory of the FTP user account that is specified for automatic backup. The backup server automatically restores the databases immediately after it receives the database backup files.
   - **Backup files location**—Enter or select a backup path to save database backup files after restoration.
6. Click **OK**.

Database backup and restore for a single IMC system

You can perform manual backup, automatic backup, and manual restoration for a single IMC system that uses one or more local databases.

This section describes how to back up and restore IMC databases locally.

The IMC Platform and all service components are deployed on the same server and use a local database.

To back up the local database of such a single IMC system, perform manual backup or configure automatic backup by using Dbman. For more information, see "Manual backup" or "Automatic backup."

To restore the local database for such a single IMC system, perform manual restoration. For more information, see "Manual restore."

Database backup and restore in IMC stateless failover

In a stateless failover scenario, the primary and backup servers use their respective local databases. The primary server automatically backs up and uploads database files to the backup server. When the primary server fails, the backup server automatically starts up and provides service.

Before you configure database backup in a stateful failover scenario, make sure that:

- The primary and backup servers use the same operating system, IMC version and patches, and database type and version.
- FTP server is configured on all backup servers.

This section describes how to back up and restore IMC databases for IMC stateless failover scenario in centralized deployment scenarios.

IMC is deployed in centralized mode on two servers. The license type is selected as primary server license on one server, and as backup server license on another server.

NOTE:

To implement database backup to the backup server for IMC deployed in centralized mode, the IMC components of the master server and the backup server must be deployed in the same way.

Database backup

IMC servers in stateless failover support automatic database backup, and do not support manual backup. With automatic backup configured, the primary server periodically backs up the IMC database files and uploads them to the backup server. For more information, see "Automatic backup."

Database restoration

IMC servers in stateless failover support both automatic database restoration and manual database restoration. HP recommends using automatic database restoration. For more information, see "Manual restore" or "Automatic restore."

In special cases, you might perform manual database restoration. To do that, make sure the database files of all IMC components are uploaded to the backup server for restoration. Otherwise, data loss will occur. For more information about manually restoring the database, see "Manual restore."

Configuration guidelines

- When a component of the IMC system, such as NTA, has a large amount of data, do not configure backup and restoration for such data when configuring Dbman. To disable Dbman from backing up the database, create a file with extension .skip (for example, nta.skip) in the **dbman\etc** folder of the database server of the component, and write the following to the file:

  ```
  dbName=nta_db (for SQL Server/MySQL)
  dbUserName=IMC_nta (for Oracle)
  ```

  After you save the .skip file, Dbman automatically reads the file and does not back up the database in the file.
- To add more configurations in the backup and restoration configuration file besides the properties configured with Dbman in the Automatic Backup and Restoration window, write the configurations to be added to file **dbman_addons.conf** at the **\dbman\etc** directory in the installation path. After you save the file, IMC automatically executes the configurations you added.

  For example, write the following before or after database restoration:

  ```
  BeforeSQLScript_monitor_db_IMC_monitor = D:\1.bat
  AfterSQLScript_monitor_db_IMC_monitor = D:\2.bat
  ```
- In an IMC stateless failover system, a backup license for the iAR report/table customization function provides read-only access. To synchronize the report/table template of the master system to the backup system, you must advertise that template on the backup system by using the trial version and register the backup system.

11 FAQ

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

To install the Java running environment, install JDK or JRE and configure JDK or JRE for Firefox. JDK is taken for example in the following part.

1. Download JDK

Address: http://www.oracle.com/technetwork/java/javase/downloads/index.html

Make sure the correct version is downloaded. For example: you must download jdk-6u12-linux-i586-rpm.bin for x86-based Linux.

2. Install JDK

Upload the installation file jdk-6u12-linux-i586-rpm.bin to the server. Suppose the installation file is saved in directory /tmp, execute the following commands:

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

After executing the commands above, press the **Space** bar to view the copyright information, and then enter **yes** to finish the JDK installation.

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

3. 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 executing the commands above, you can run /var/local/firefox/firefox to access IMC.

In Linux, the current system time in IMC (such as the login time and operation log record time) is different from that on the server, and the difference may be several hours. How to solve the problem?

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

After IMC is installed in the Windows Server 2003 64-bit edition, the IMC background processes cannot be started. How to solve the problem?

Before installing IMC in Windows Server 2003 64-bit OS, you must first install the WindowsServer2003-KB942288-v4-x64.exe patch. Otherwise, part of IMC processes cannot start after installation and deployment.

To solve this problem, stop IMC, install the patch mentioned above, and manually execute **IMC installation path\deploy\components\server\vcredist.exe**.

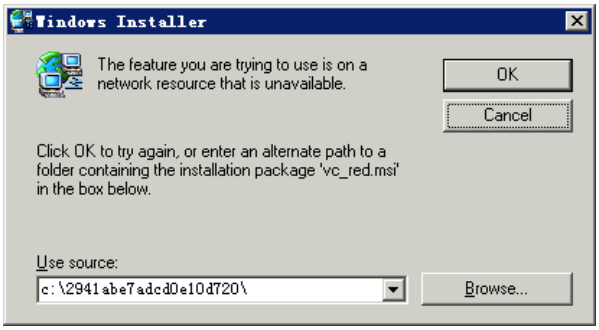
During the component deployment process, an error message "Deployment is stopped with error. For details, see the log." appears, and "Execute database script error!" is displayed in the system log. Then check the specified log file according to the prompt information, and only the error information that the object dbo.qv.id already exists is displayed. How do I solve the problem?

Log in to the Query Analyzer of SQL Server as an **sa** user and execute the following commands:

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

Deploy the component again.

When installing IMC on a PC running Windows Server 2008 R2, the system indicates the Windows Installer cannot be installed, as shown in the following figure. How do I solve this problem?



On the **Windows Installer** dialog box, click **Browse**. On the dialog box for selecting a file, search any folder whose name contains digits and letters **abcdef** in the root directory, select file **vc_red.msi** in the folder, and click **OK**. Then, you can continue the installation.

In Linux, how can I solve the problem that the JavaService is closed when Xwindows is closed?

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

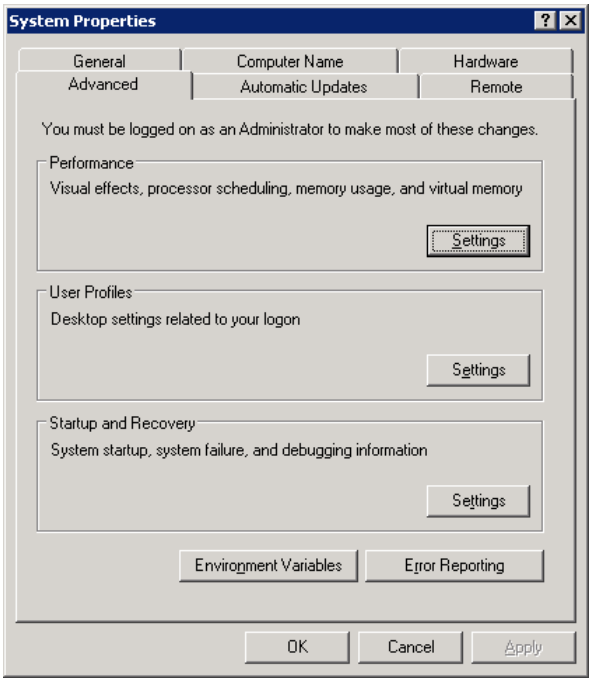
On Windows, IMC service processes cannot be started or stopped after IMC runs for a certain period of time. How to solve the problem?

This problem is caused by insufficient virtual memory. Set the virtual memory to the system managed size on the server.

Follow these steps to set the virtual memory to the system managed size:

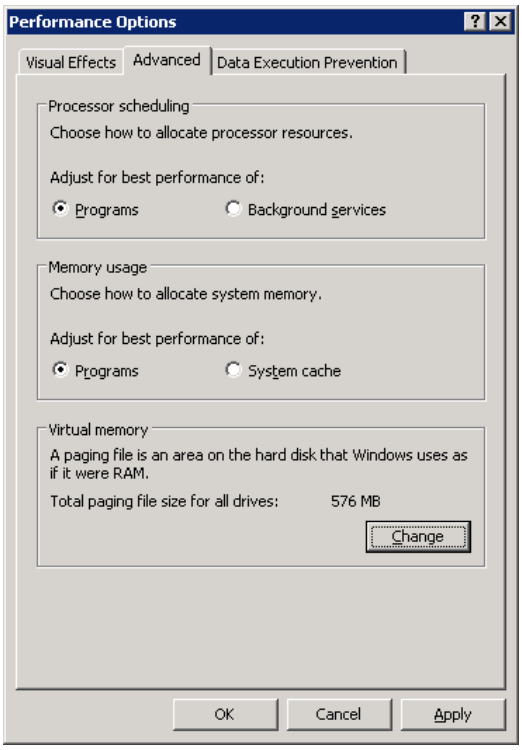
1. On the server, open the **Control Panel** window, and click the **System** icon. The **System Properties** dialog box appears.

Figure 91 System properties



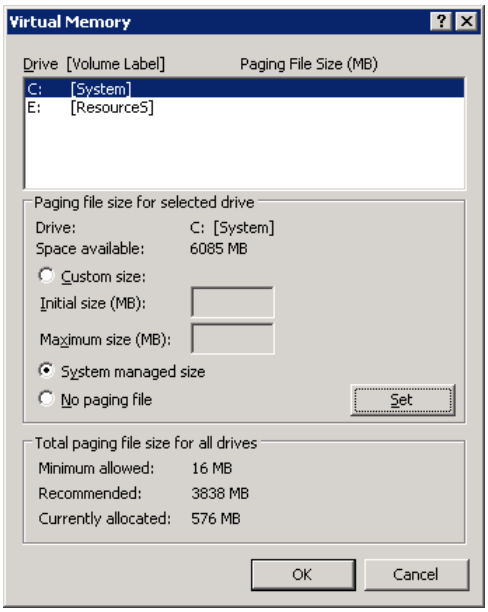
2. Select the **Advanced** tab, and click **Settings** in the **Performance** area. The **Performance Options** dialog box appears.

Figure 92 Performance options



3. On the **Performance Options** dialog box, select the **Advanced** tab, and click **Change** in the **Virtual memory** area. The **Virtual Memory** dialog box appears.

Figure 93 Virtual memory



4. Select the **System managed size** option, click **Set**, and click **OK**.

After an error occurs in deployment or upgrade of a component, the component remains to be in Deploying or Upgrading state in the IMC Intelligent Deployment Monitoring Agent on the master server. How to solve the problem?

IMC does not actively refresh the component states. To view the latest state of the component:

1. Stop the IMC Intelligent Deployment Monitoring Agent and quit the program.
2. Restart the H3C IMC server service.
3. Open and start the IMC Intelligent Deployment Monitoring Agent on the master or subordinate server.

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (when applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP A-Series Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking

- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com

Conventions

The following information describes the conventions used in this documentation set.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING!	Indicates that the failure to follow directions could result in bodily harm or death.
CAUTION	Indicates that failure to follow directions could result in damage to equipment or data.
IMPORTANT	Provides clarifying information or specific instructions.
NOTE	Provides additional information.
TIP	Provides helpful hints and shortcuts.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index