# INTELBRAS

# INC Deployment Guide for Remote Database

Intelbras S.A
**http://www.intelbras.com**

# Overview

The following information describes how to deploy INC in distributed mode and to use a remote database. This deployment scheme scales to networks of 200 to 10000 devices.

# INC components

INC includes the INC platform and service components.

## INC platform

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

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

## Service components

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

INC includes the following service components:

- **Endpoint Intelligent Access (EIA)**—Provides policy-based Authentication, Authorization, and Accounting (AAA) services. EIA software extends management to wired, wireless, and remote network users, and enables the integration of network device, user, guest, and terminal management on a single unified platform. Provides basic AAA functions for network devices or IT users for network device management security. EIA can assign users with different privileges, monitor login and command execution operations, and simplify user management.
- **Wireless Service Manager (WSM)**—Provides unified management of wired and wireless networks, adding network management functions into existing wired network management systems. WSM software offers wireless LAN (WLAN) device configuration, topology, performance monitoring, RF heat mapping, and WLAN service reports.

# INC editions

The following editions of INC are available:

- Professional
- Standard
- SNS

To deploy INC in distributed mode and to use a remote database, you must use the INC Professional or Standard edition.

**Table 1 Differences between INC editions**

| Item | SNS | Standard | Professional |
|---|---|---|---|
| Number of nodes | 40 | Extensible | Extensible |
| Hierarchical Network Management | Not supported | Lower-level NMS only | Supported |
| Distributed deployment | Not supported | Supported | Supported |
| Operating system | Windows | Windows | Windows |
| Embedded database | Supported | Supported only on Windows | Not supported |
| Remote database | Supported | Supported | Supported |

For information about installing a remote database for INC on Windows, see the following documents:

- *SQL Server 2012 Installation and Configuration Guide*
- *SQL Server 2014 Installation and Configuration Guide*
- *SQL Server 2016 Installation and Configuration Guide*
- *SQL Server 2017 Installation and Configuration Guide*
- *SQL Server 2019 Installation and Configuration Guide*
- *SQL Server 2022 Installation and Configuration Guide*
- *MySQL 5.5 Installation and Configuration Guide (for Windows)*
- *MySQL 5.6 Installation and Configuration Guide (for Windows)*
- *MySQL 5.7 Installation and Configuration Guide (for Windows)*
- *MySQL 8.0 Installation and Configuration Guide (for Windows)*

# Installation and deployment

In distributed deployment, the conductor server is the management center of INC. It interacts with member servers to implement network management. A member server is responsible for specific tasks, for example, network analysis for NTA and portal for EIA.

To improve server performance, INC uses the "Install + Deploy" model.

- **Install**—Copies the INC installation packages to the server and loads them to the Intelligent Deployment Monitoring Agent.
- **Deploy**—Decompresses the installation packages and runs deployment scripts on the server.

The INC components are operational only after they are deployed. In distributed deployment, all INC components are installed on the conductor server and deployed on the conductor server or a member server as needed. The conductor server provides centralized Web services.

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

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

# Deployment restrictions and guidelines

To deploy INC in distributed mode, follow these restrictions and guidelines:

- The conductor and member servers must use the same operating system.
- You can use SQL Server and MySQL databases for Windows.
- When you use Oracle, make sure all databases used by the conductor and member servers have different network service names.
- The following subcomponents must be deployed on the conductor server:
  - Resource Management
  - NE Management
  - Report Management
  - Network Asset Management
  - Security Control Center

  For more information about the deployment for other subcomponents, see Table 9. For more information about the deployment for other service components, see Table 10.
- If the INC Intelligent Deployment Monitoring Agent is already installed on member servers, uninstall it before you deploy INC components in distributed mode. For more information about how to uninstall the Intelligent Deployment Monitoring Agent, see "Uninstalling ."

# Obtaining INC installation and deployment methods

You can use the following methods to obtain the INC installation and deployment procedure:

- View the video case on Intelbras website.
- Read this document.

  This document describes information about installing and deploying INC on Windows Server 2012 R2.

The INC software is included in the DVD delivered with the product.

# Preparing for installation

## Hardware requirements

The tables in this section use the following terminology:

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

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

  **Table 2 Performance instances**

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

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

  To set the Java heap size for INC:On Windows, run the **setmem.bat** *heap size* script in the **\client\bin** directory of the INC installation path.

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

To improve 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 a minimum of 256 MB.
- When the number of collection units is from 200 K to 300 K, install two or more disks and a RAID card with a cache of a minimum of 512 MB.
- When the number of collection units is 300 K to 400 K, install four or more disks and a RAID card with a cache of a minimum of 1 GB.
- Install three disks in RAID 5, and four or more disks in RAID 0+1.

Optimal hardware requirements vary with scale, other management factors, and are specific to each installation. Please consult INTELBRAS Support, or your local account teams for exact requirements.

If service components are added to the INC platform, be sure to read the release notes of each component. When multiple components are deployed, the resources must be combined. Suppose the required CPU resource, memory resource, and disk resource of a component are A(num), B(num), and C(num), respectively. When multiple components are deployed, the required hardware resources are as follows

- CPU=A0+A1+A2+A3
- Memory=B0+B1+B2+B3
- Disk=C0+C1+C2+C3

# Hardware requirements of the INC platform

**Table 3 Hardware requirements for a 64-bit Windows operating system**

| Management scale | | | System minimum requirements | | | | |
|---|---|---|---|---|---|---|---|
| **Nodes** | **Collection units** | **Online operators** | **CPU (2.5GHz or above)** | **Server memory** | **Java heap size** | **Disk space for installation** | **Disk space for data storage** |
| 0 to 200 | 0 to 5 K | 20 | 2 cores | 12 GB | 4 GB | 100 GB | 100 GB |
| 0 to 200 | 5 K to 50 K | 10 | 2 cores | 12 GB | 4 GB | 100 GB | 200 GB |
| 200 to 1 K | 0 to 10 K | 30 | 4 cores | 16 GB | 4 GB | 100 GB | 100 GB |
| 200 to 1 K | 10 K to 100 K | 10 | 4 cores | 16 GB | 4 GB | 100 GB | 200 GB |
| 1 K to 2 K | 0 to 20 K | 30 | 6 cores | 24 GB | 8 GB | 150 GB | 100 GB |
| 1 K to 2 K | 20 K to 200 K | 10 | 6 cores | 24 GB | 8 GB | 150 GB | 200 GB |
| 2 K to 5 K | 0 to 30 K | 40 | 8 cores | 32 GB | 12 GB | 200 GB | 120 GB |
| 2 K to 5 K | 30 K to 300 K | 20 | 8 cores | 32 GB | 12 GB | 200 GB | 250 GB |
| 5 K to 10 K | 0 to 40 K | 50 | 16 cores | 48 GB | 16 GB | 200 GB | 150 GB |
| 5 K to 10 K | 40 K to 400 K | 20 | 16 cores | 48 GB | 16 GB | 200 GB | 300 GB |
| 10 K to 15 K | 0 to 40 K | 50 | 24 cores | 64 GB | 24 GB | 200 GB | 200 GB |
| 10 K to 15 K | 40 K to 400 K | 20 | 24 cores | 64 GB | 24 GB | 200 GB | 600 GB |

# Hardware requirements of the EIA component

### EIA

You can deploy the portal component on multiple servers in distributed mode. When there are high requirements for portal access, as a best practice, deploy the portal component in distributed mode. When you deploy the portal component in distributed mode, as a best practice, support more users on a dedicated portal server. A dedicated portal server must have at least a configuration that is one level lower than the current configuration.

If the number of managed access users is above 5k and self-service center is needed, you must deploy self-service center in distributed mode. A dedicated self-service center must have at least a configuration that is one level lower than the current configuration.

The following deployment scheme is given based on some reasonable assumptions. More specifically:

- In the following tables, the 802.1X access method represents any access method that does not need the collaboration of EIA, except portal access.
- The CPU requirements of EIA specified here are requirements for Intel CPUs. The requirements for Kunpeng and Feiteng ARM CPUs must be twice the requirements for Intel CPUs.

**Table 4 64-bit Windows**

| Management scale | | | | | | System minimum requirements | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Managed access users** | **Online operators** | **Access method** | **Authentication method** | **Online users** | **Concurrent online users** | **CPU (2.0GHz or above)** | **Memory** | **Java heap size** | **Disk size for installing INC** | **Disk size for running INC** | **Maximum IOPS of running disks** |
| <= 20K | 5 | 802.1X | PAP/CHAP/EAP-MD5 | 10000 | 100 | 4-core CPU | 16G | 4G | 150GB | 100GB | 300 (as a best practice, configure a RAID controller with the cache higher than 192M) |
| | | | EAP-PEAP/TLS/TTLS | 3000 | 10 | | | | | | |
| | | Portal | PAP/CHAP | 6000 | 50 | | | | | | |
| | | | EAP-PEAP/TLS/TTLS | 3000 | 10 | | | | | | |
| <= 100K | 10 | 802.1X | PAP/CHAP/EAP-MD5 | 50000 | 200 | 8-core CPU | 32G | 8G | 300GB | 150GB | 600 (as a best practice, configure a RAID controller with the cache higher than 256M) |
| | | | EAP-PEAP/TLS/TTLS | 15000 | 20 | | | | | | |
| | | Portal | PAP/CHAP | 20000 | 150 | | | | | | |
| | | | EAP-PEAP/TLS/TTLS | 15000 | 20 | | | | | | |
| <= 50 | 15 | 802.1X | PAP/CHAP/EAP-MD5 | 100000 | 500 | 16-core CPU | 64G | 12G | 600GB | 300GB | 1000 (as a |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0<br>K | | | EAP-PEAP<br>/TLS/TTLS | 30000 | 50 | | | | | | best<br>practic<br>e,<br>configu<br>re a<br>RAID<br>controll<br>er with<br>the<br>cache<br>higher<br>than<br>1G) |
| | | Portal | PAP/CHAP | 40000 | 300 | | | | | | |
| | | | EAP-PEAP<br>/TLS/TTLS | 20000 | 40 | | | | | | |

# Hardware requirements of the WSM component

When the number of collection units is 0 to 5k, no or few performance monitors are enabled.

**Table 5 64-bit Windows**

| **Management scale** | | | **System minimum requirements** | | | | |
|---|---|---|---|---|---|---|---|
| **Nodes** | **Collection units** | **Online operators** | **CPU (2.5GHz or above)** | **Memory** | **Java heap size** | **Disk size for installing INC** | **Disk size for running INC** |
| Fit APs: 0 to 500 | 0 to 50K | 10 | 2-core CPU | 4G | 1G | 3GB | 60GB |
| Fit APs: 500 to 1000 | 16K to 90K | 10 | 4-core CPU | 8G | 4G | 3GB | 100GB |
| Fit APs: 1000 to 3000 | 32K to 150K | 10 | 6-core CPU | 16G | 6G | 4GB | 200GB |
| Fit APs: 3000 to 5000 | 100K to 250K | 10 | 8-core CPU | 24G | 8G | 5GB | 250GB |
| Enterprise network: fit APs: 5000 to 10000 | 160K to 400K | 10 | 12-core CPU | 32G | 12G | 7GB | 300GB |
| Service provider: Fit APs: 5000 to 8000 | | | | | | | |

# Software requirements

**Table 6 Software requirements**

| **Item** | **Requirement** | **Remarks** |
|---|---|---|
| **Windows** | | |
| Operating system | Windows Server 2012 (64-bit) | KB2836988 |
| | Windows Server 2012 R2 (64-bit) | N/A |

| | | |
|---|---|---|
| | Windows Server 2016 (64-bit) | N/A |
| | Windows Server 2019 (64-bit) | N/A |
| | Windows Server 2022 (64-bit) | N/A |
| Database | SQL Server 2012 Enterprise | Service Pack 4 |
| | SQL Server 2014 Enterprise | Service Pack 3 |
| | SQL Server 2016 Enterprise | Service Pack 3 |
| | SQL Server 2017 Enterprise | N/A |
| | SQL Server 2019 Enterprise | N/A |
| | SQL Server 2022 Enterprise | N/A |
| | SQL Server 2017 Express | Used as the embedded database for SNS and standard editions only. |

# VM requirements

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

When installed on a virtual machine, INC supports the following virtual platforms:

- VMware:
  - VMware ESXi 5.5
  - VMware ESXi 6.0
  - VMware ESXi 6.5
  - VMware ESXi 6.7
  - VMware ESXi 7.0
- CAS:
  - CAS 2.0
  - CAS 3.0
  - CAS 5.0
- Hyper-V:
  - Hyper-V 2008 R2
  - Hyper-V 2012
  - Hyper-V 2012 R2

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

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

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

# Preparing the installation environment

To ensure the correct installation and operation of INC, make sure no other network management products are installed on the same server as INC.

Do not install INC in an IPv6 environment. However, INC allows users to manage IPv6 devices.

# Uninstalling previous versions of INC

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

After you uninstall INC:On Windows, delete the **INC-Reserved** folder from the **WINDOWS** folder of the system disk.

# Checking ports and firewalls

Make sure the INC Web service ports and database listening ports are open in the firewall. Table 7 lists the default INC Web service ports and database listening ports.

**Table 7 INC port requirements**

| Server | Usage: protocol/default port | Direction |
|---|---|---|
| Web | HTTP: TCP/8080<br>HTTPS: TCP/8443 | Browser to INC |
| Database | SQL Server database: TCP/1433<br>Oracle database: TCP/1521<br>MySQL database: TCP/3306 | INC and components to the database |

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

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

# Checking the database configuration

INC data can be stored on a remote database server. In distributed deployments, the data of all INC servers is typically stored on the same remote database server.

To use a SQL database server:

- Install a SQL Server client that has the same version as the database.
- Create a folder to store INC data files on the SQL server. You are required to provide the folder to save INC data on the remote database during INC deployment.
- As a best practice, use the account **LocalSystem** for the SQL Server service on the database server. This enables the database superuser used for installing INC to have read and write access to all disks on the database server. To use another account, you must grant the account read and write access to the database file folder. For more information, see *SQL Server 2012/2014/2016/2017 Installation Guide*.

To use an Oracle database:

- Install an Oracle client that has the same version as the database.
- Create a network service name and set the network service name to be the IP address of the database server.

Before installing INC, first install the database server, and then configure the database services to automatically start with the operating system.

For example, to use a SQL Server database for INC, install the database before INC installation and set the startup type of the **SQL Server** and **SQL Server Agent** services to **Automatic**.

To view the startup type of the database services, click **Start,** and then select **Administrative Tools** > **Services**.

# Checking the installation environment (optional)

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

To check the installation environment:

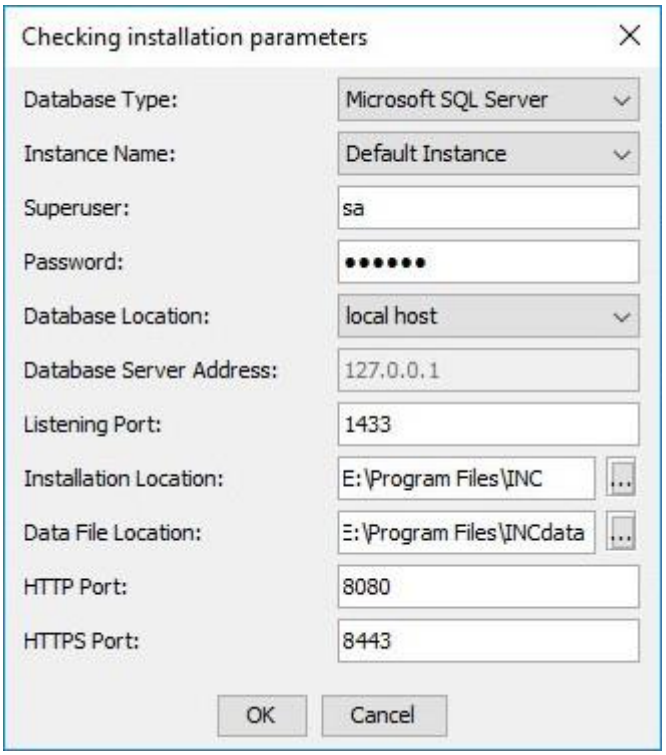
1. Copy the envcheck tool (**envcheck.bat** for Windows) from the **tools** folder to the **install** folder of the INC installation package.
2. Run the tool.

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

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

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

   **Figure 1 Checking installation parameters**



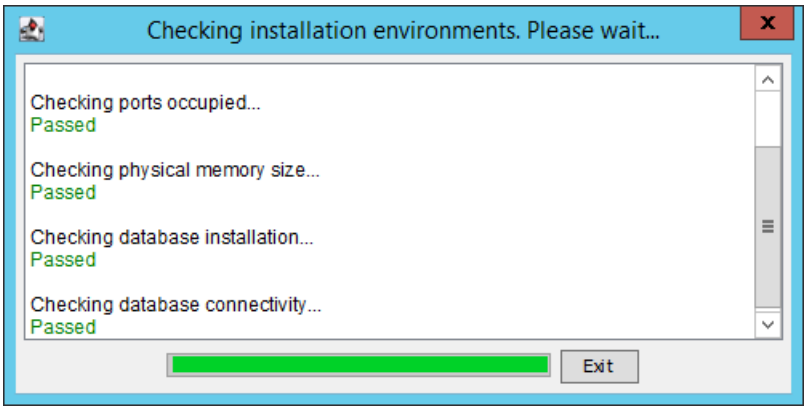

3. Configure the parameters for checking database connectivity:
   - **Database Type**—Select the database type. Options are **Microsoft SQL Server**, **MySQL**, and **Oracle**. The default is **Microsoft SQL Server**.
   - **Instance Name**—To connect to the default instance of the database, select **Default Instance**. To connect to a named instance, select **Other Instance**, and then enter the instance name.
   - **Superuser**—Enter the database superuser name. The default is **sa**.
   - **Password**—Enter the password of the superuser.
   - **Database Location**—Select **other server** from the list.
   - **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.
   - **Listening Port**—Enter the listening port of the database server. The default is **1433**.

- **Installation Location**—Specify the local directory for storing the INC installation package.
- **Data File Location**—Specify the local directory for storing the data files.
- **HTTP Port**—Enter the HTTP port number for the INC Web server. The default is 8080.
- **HTTPS Port**—Enter the HTTPS port number for the INC Web server. The default is 8443.

4. Click **OK**.

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

   **Figure 2 Check results**




5. Click **Exit**.

Fix any failed check items according to the check results.

# Superuser account

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

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

To perform the following tasks, you must update the password in INC if the password of the superuser account is changed after INC deployment:

- View database information on the **Environment** tab.
- Deploy new components.
- Update existing components.

To update the database user password in INC:

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

   The **Change Password** button is displayed only when the Intelligent Deployment Monitoring Agent detects an incorrect database user password.
3. Enter the new database password, and then click **OK**, as shown in Figure 3.

**Figure 3 Changing the superuser password**

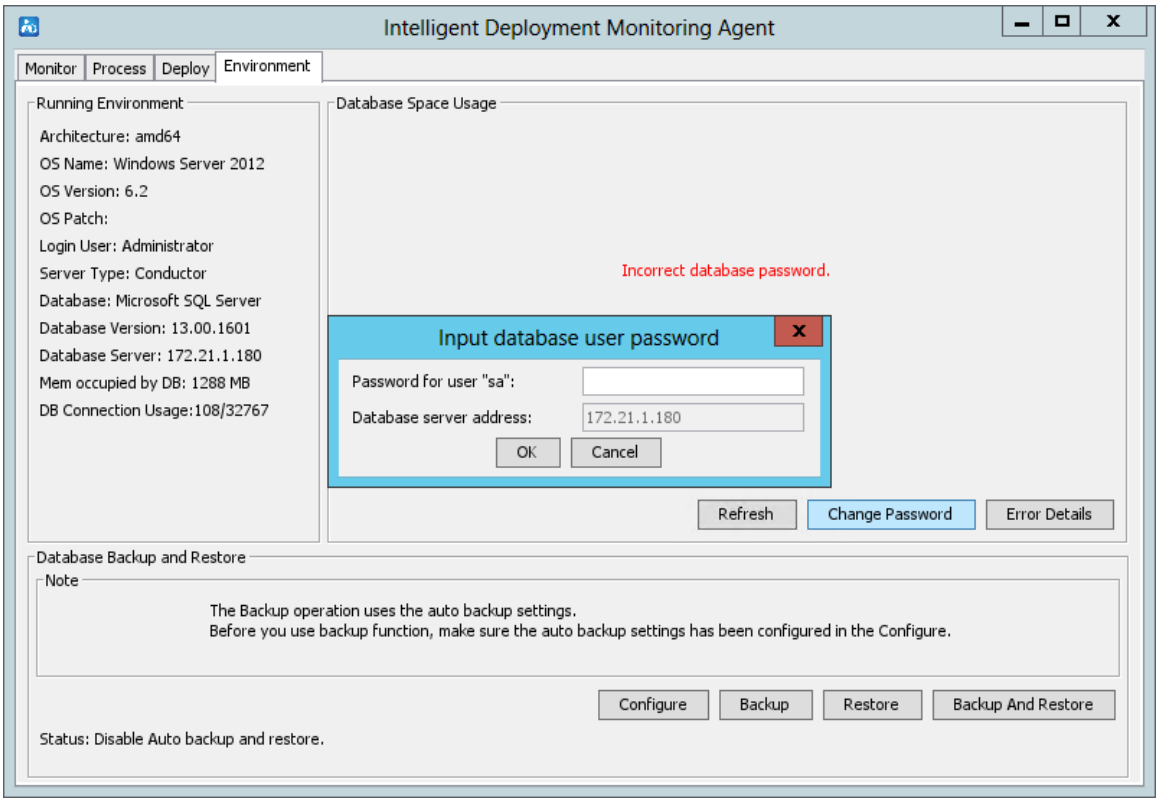



Table 8 lists the default superuser accounts.

**Table 8 Database superuser accounts**

| Database | Superuser |
|---|---|
| SQL Server | sa |
| Oracle | • system<br>• sys |
| MySQL | root |

# Setting the system time

Follow these guidelines when you set the system time:

- Do not enable seasonal time adjustments such as daylight savings time.
- Before installing INC, verify that the system time, date, and time zone settings on the server are correct.

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

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

# Installing and deploying the INC platform

You must install the database before installing INC. This example uses the SQL server 2012 database. For information about how to install the database, see *SQL Server 2012 Installation and Configuration Guide*.

Table 9 lists the INC platform subcomponents and the optional servers.

**Table 9 INC platform subcomponents and deployment requirements**

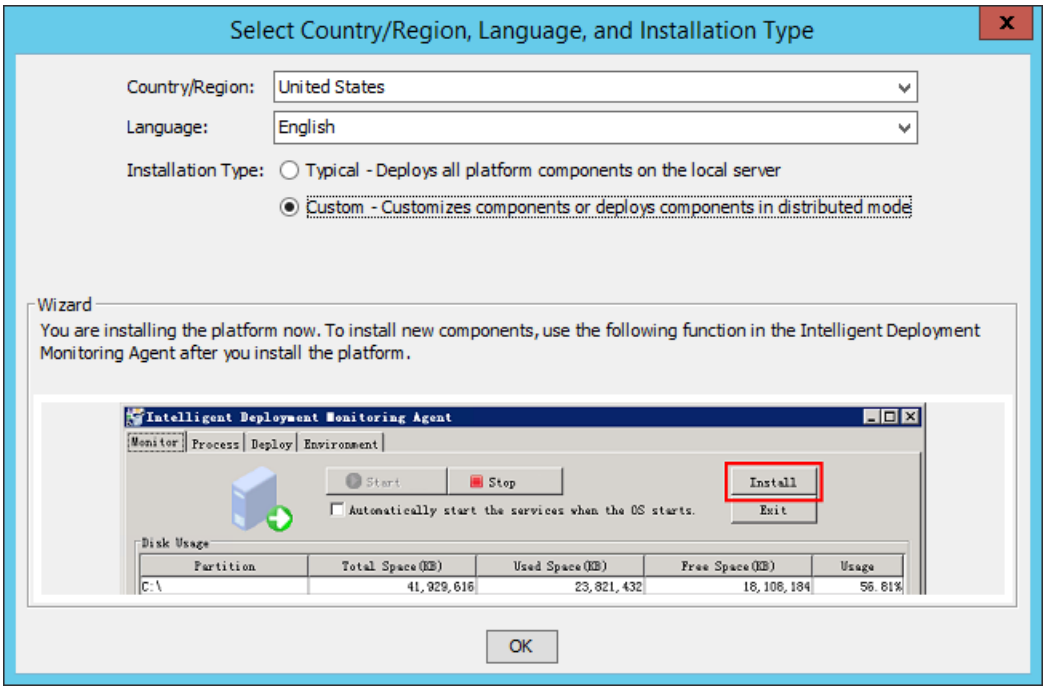
| Component | Subcomponents | Optional server |
|---|---|---|
| INC platform | Resource Management | Conductor |
| | Alarm Management | Conductor or member |
| | Guest Access Management | Conductor or member |
| | Performance Management | Conductor or member |
| | Network Asset Management | Conductor or member |
| | ACL Management | Conductor |
| | Intelligent Configuration Center | Conductor |
| | NE Management | Conductor or member |
| | Report Management | Conductor or member |
| | General Search Service Management | Conductor |
| | Security Control Center | Conductor |
| | Syslog Management | Conductor or member |
| | VLAN Management | Conductor or member |
| | User Selfservice Management | Conductor or member |
| | WeChat Server | Conductor or member |

# Selecting the installation type

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

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

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




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

   INC supports typical and custom installations.

   - **Typical**—Installs and deploys all platform subcomponents on the local host without manual intervention.
   - **Custom**—Allows you to select desired platform subcomponents to install and deploy on the conductor server. After the installation completes, you must manually deploy the platform subcomponents. A custom installation is required to start a distributed deployment.

4. Click **OK**.

When you install or upgrade INC, restart the INC server if a socket issue exists in the INC installation environment. If no socket issue exists, you do not need to restart the INC server.

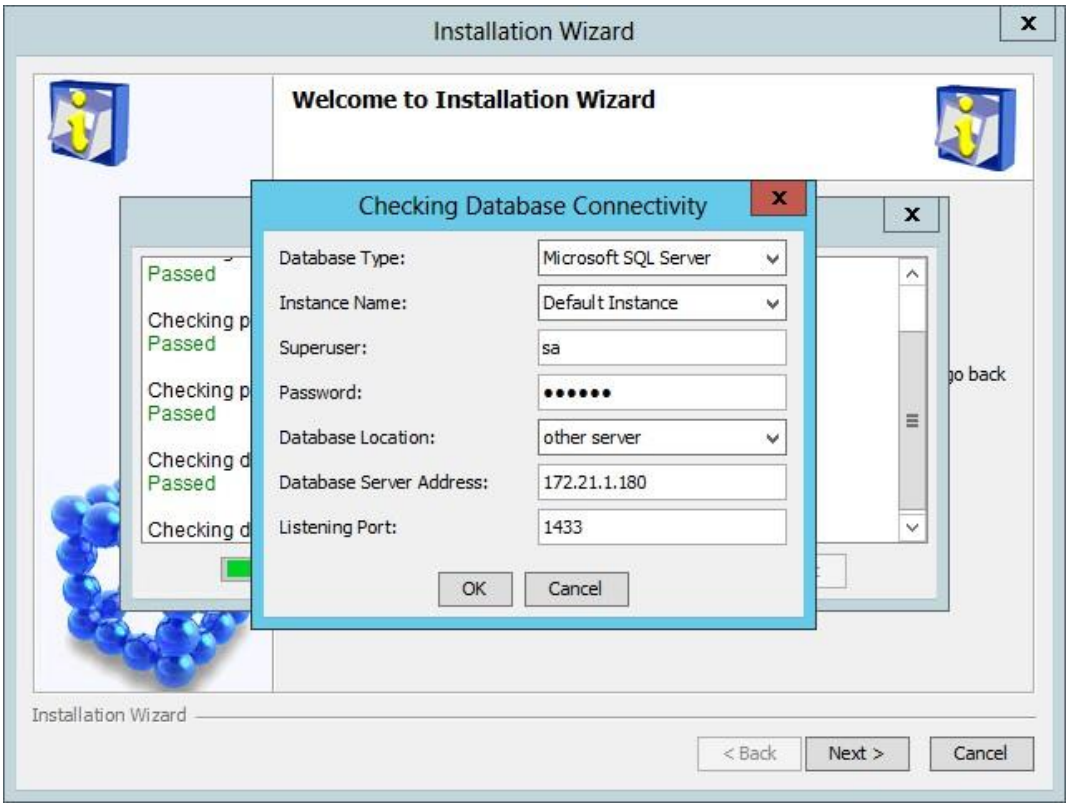
The installation packages of the following components are located in the **tools\components** directory: ACL, EUPLAT, GAM, RestPlugin, VLAN, and WeChat. Before you install and deploy the INC platform, copy the installation packages of the components you want to install to the **install\components** directory.

# Installing the INC platform

1. In the **Select Country/Region, Language, and Installation Type** dialog box, select the **Custom** installation type, and then click **OK**.

   The **Checking Database Connectivity** dialog box opens, as shown in Figure 5.

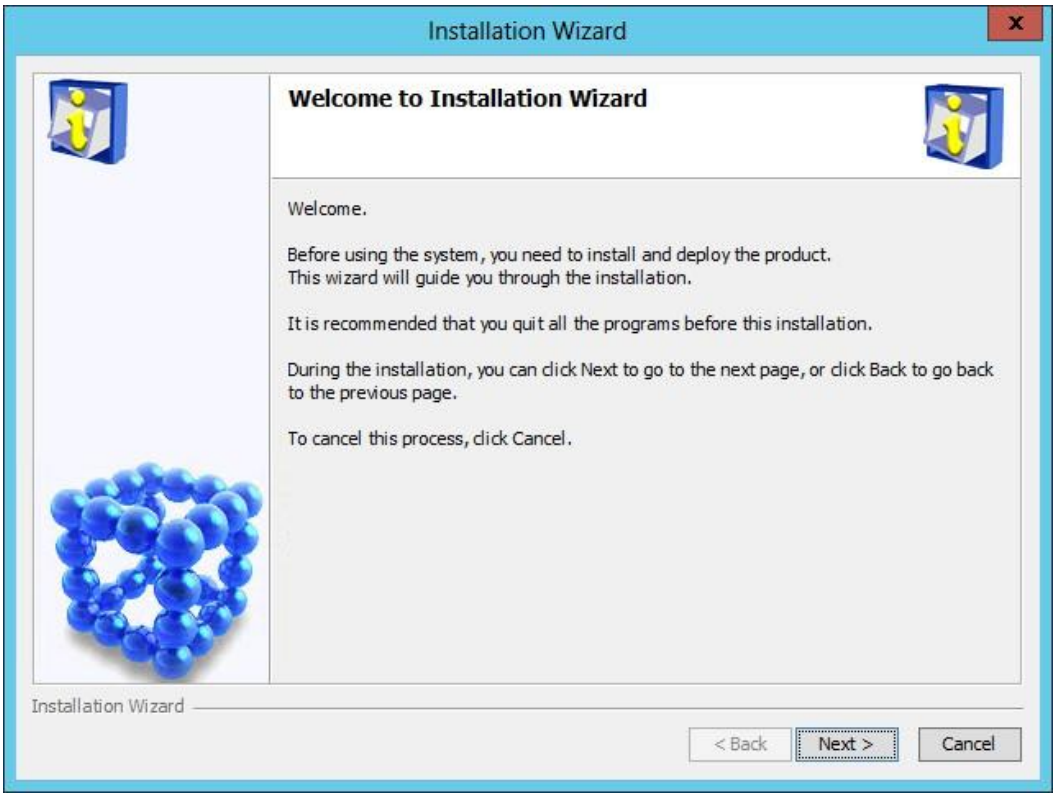
**Figure 5 Checking Database Connectivity**




2. Configure the parameters as needed. For descriptions about the parameters, see "Checking the installation environment."
3. Click **OK**.

   After the checks are passed, the INC installation wizard opens, as shown in Figure 6.

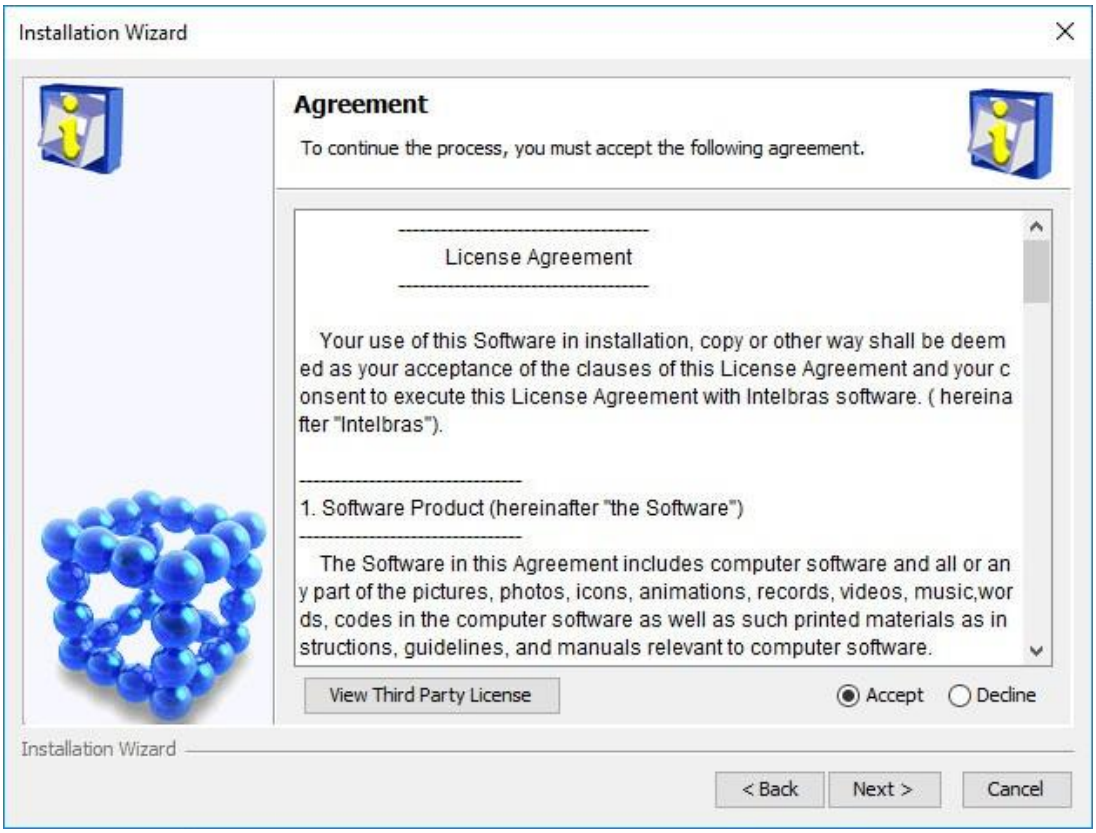
**Figure 6 INC installation wizard**




4. Click **Next**.

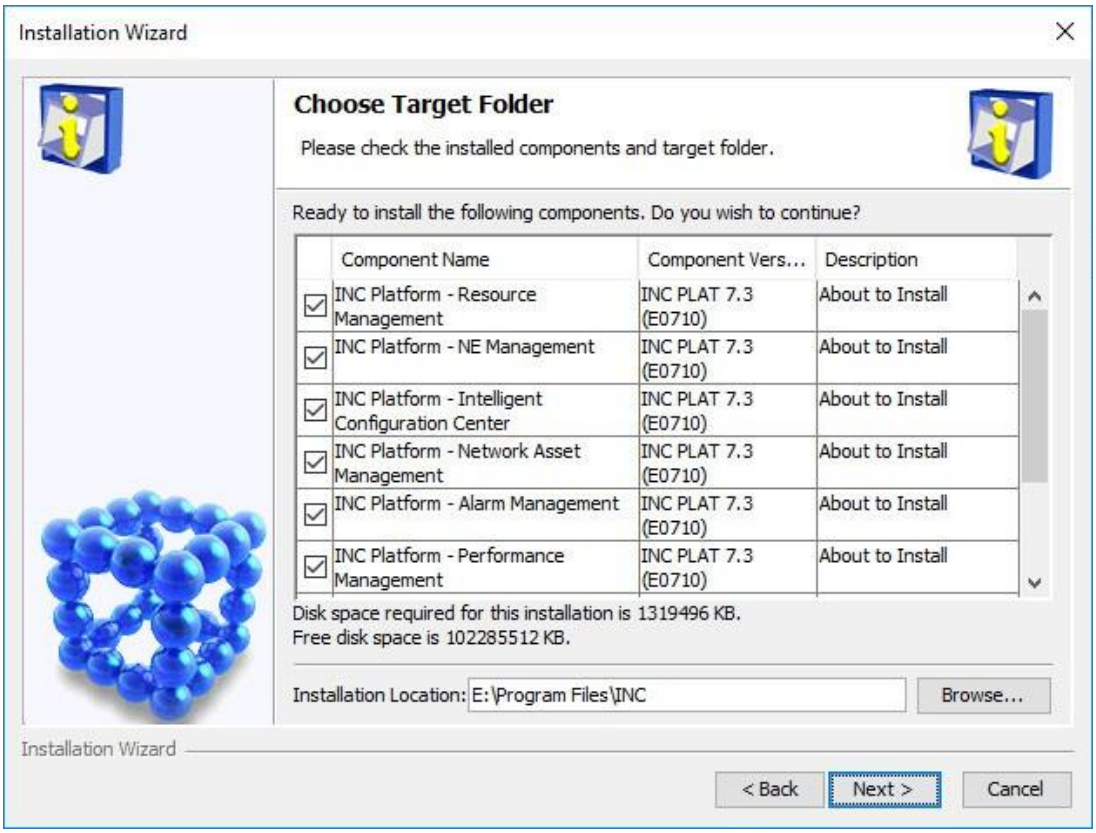
   The **Agreement** page opens, as shown in Figure 7.

**Figure 7 Agreement page**




**5.** Read the license agreement, select **Accept**, and then click **Next**.
The **Choose Target Folder** page opens, as shown in Figure 8.

**Figure 8 Choose Target Folder page**




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

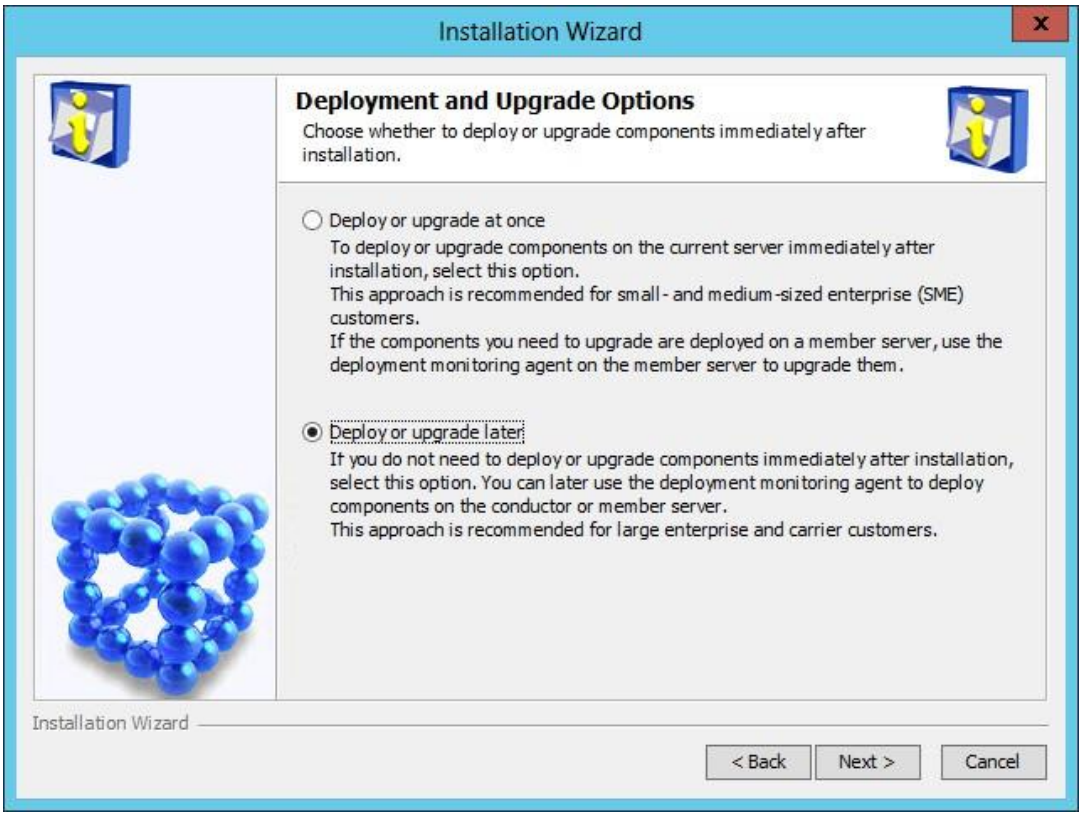
   The installation program examines whether the specified installation path contains files. If the path contains files, a message is displayed. Click **OK** to delete the files.

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

7. Click **Next**.

   The **Deployment and Upgrade Options** page opens, as shown in Figure 9.

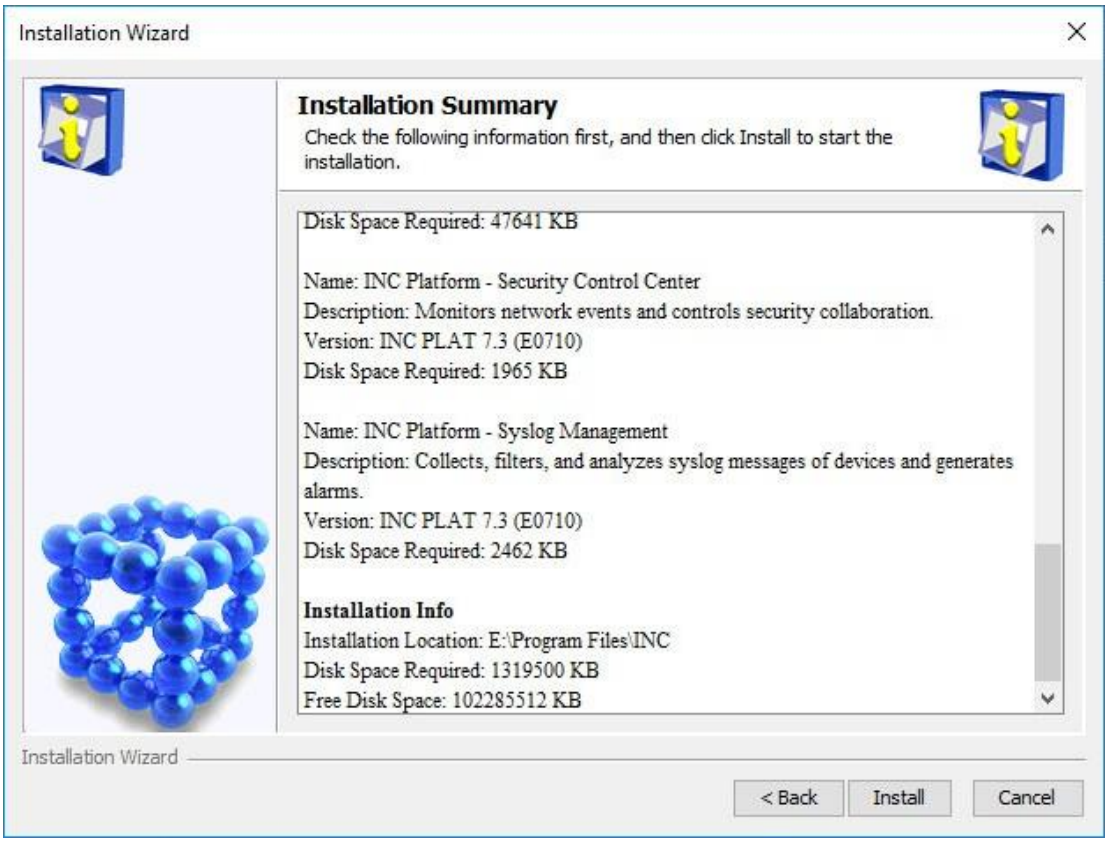
**Figure 9 Deployment and Upgrade Options page**




8. Select **Deploy or upgrade at once** or **Deploy or upgrade later**. In this example, select **Deploy or upgrade later**.
9. Click **Next**.

   The **Installation Summary** page opens, as shown in Figure 10.

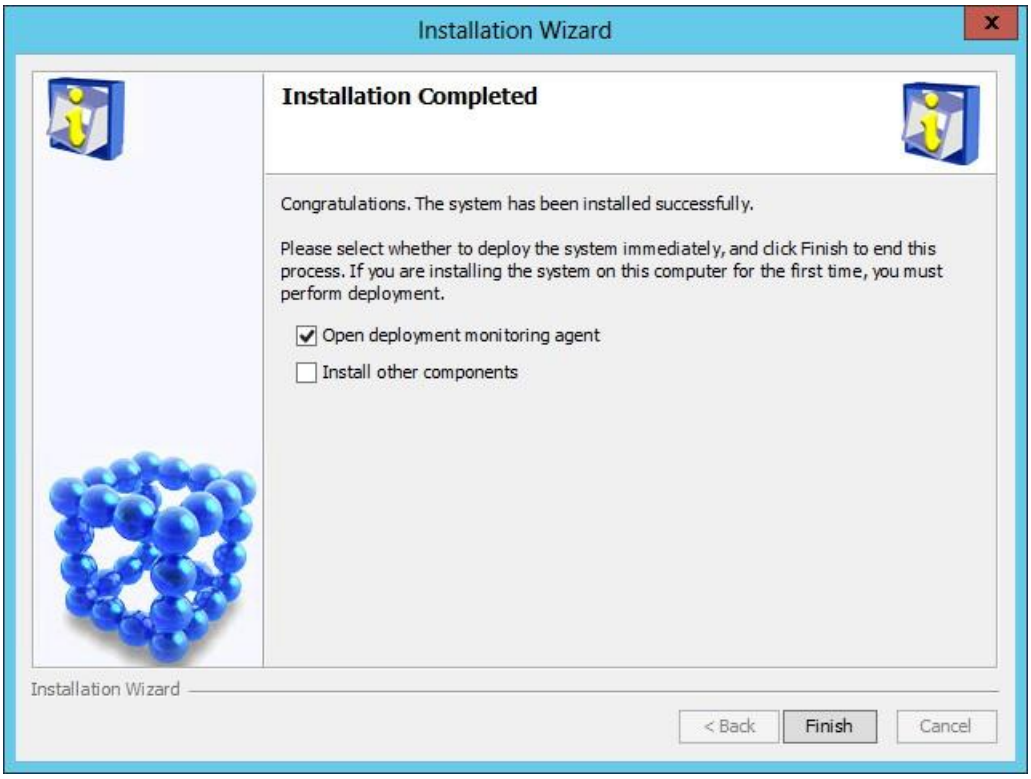
**Figure 10 Installation Summary page**




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

After the installation is complete, the **Installation Completed** page opens, as shown in Figure 11.

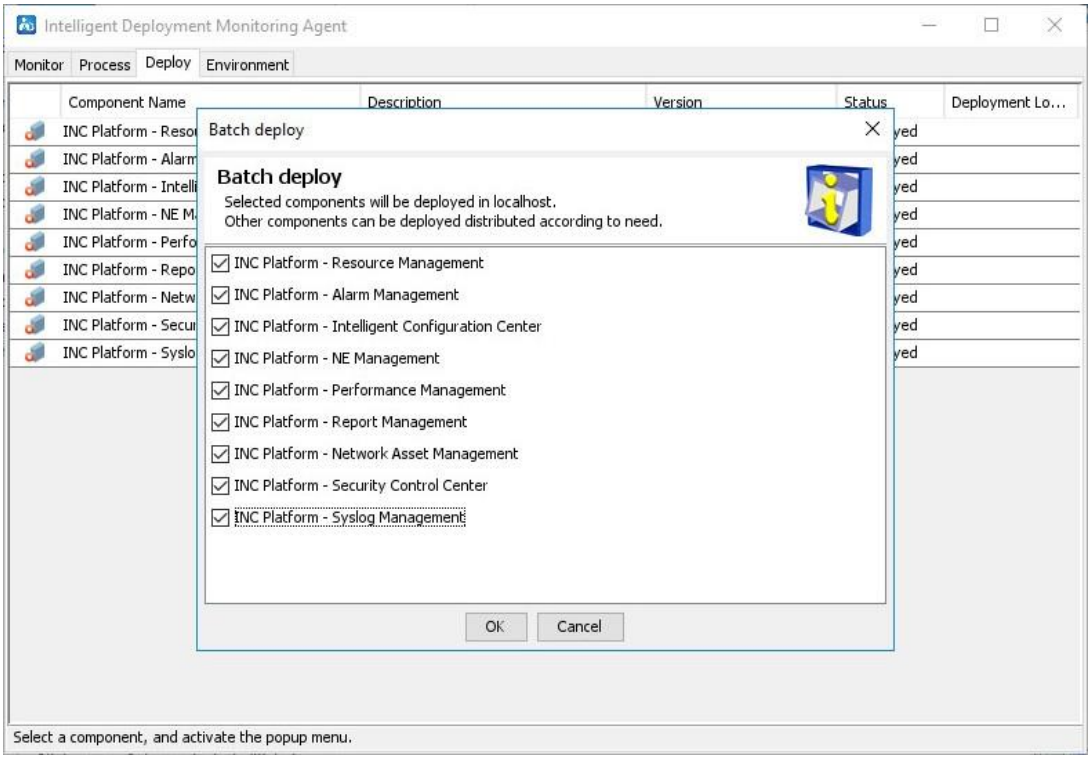
**Figure 11 Installation Completed page**




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

The system automatically starts the Intelligent Deployment Monitoring Agent and displays the **Batch deploy** dialog box, as shown in Figure 12.

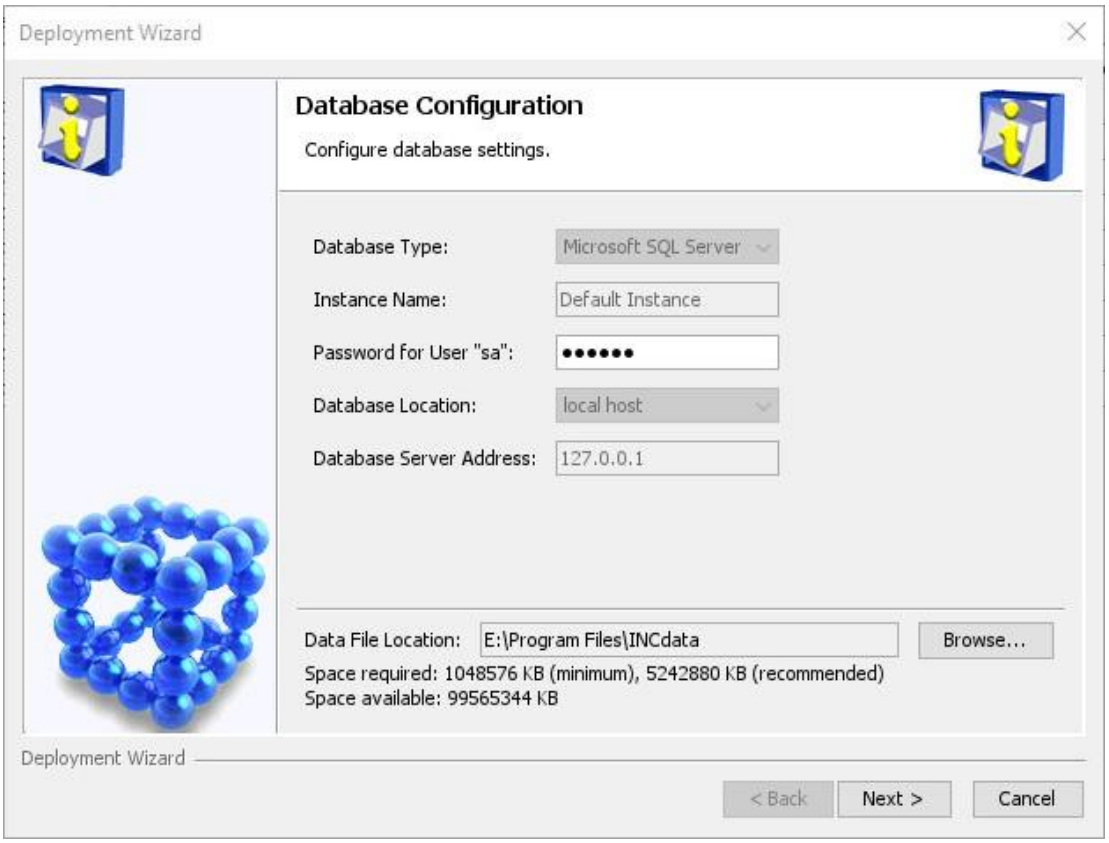
**Figure 12 Batch deploy dialog box**



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

    The **Database Configuration** page opens, as shown in Figure 13.

    **Figure 13 Database Configuration page**



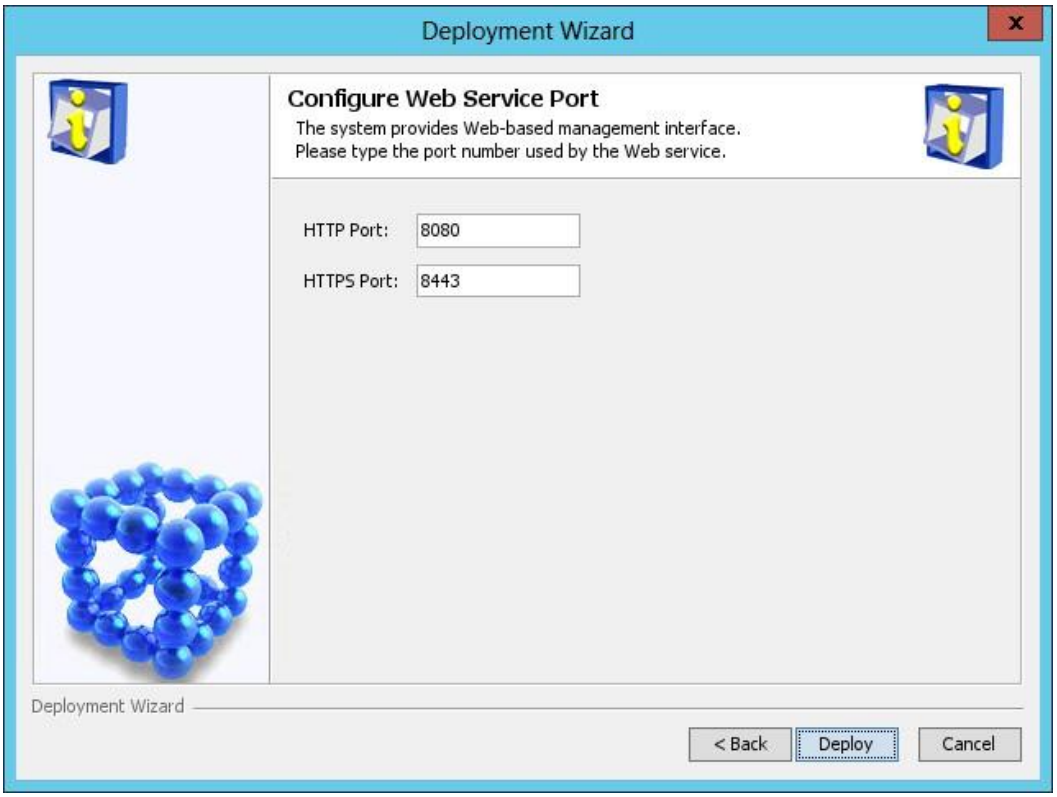

13. Enter the password of the superuser.
14. Set the data file location.

    You must first create a folder to save data files on the database server.

    Make sure the specified data file location is on a readable and uncompressed disk drive and does not include any files.
15. Click **Next**, and then click **OK** in the confirmation dialog box that opens.

    The **Configure Web Service Port** page opens, as shown in Figure 14.

**Figure 14 Configure Web Service Port page**



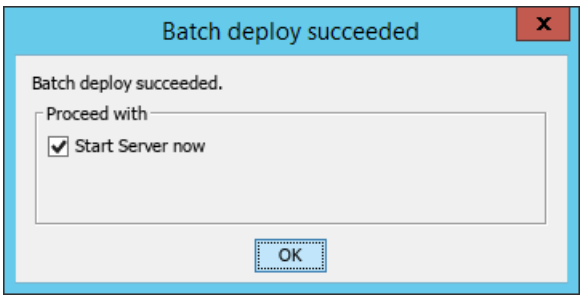

16. Enter the HTTP and HTTPS port numbers. This example uses the default port numbers 8080 and 8443.

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

17. Click **Deploy**.

    After the deployment is complete, the **Batch deploy succeeded** dialog box opens, as shown in Figure 15.

**Figure 15 Batch deploy succeeded dialog box**




18. Click **OK**.

# Deploying INC on a member server

Before you deploy INC subcomponents on a member server for the first time, install the Intelligent Deployment Monitoring Agent on the member server.

Make sure you have started INC on the conductor server.

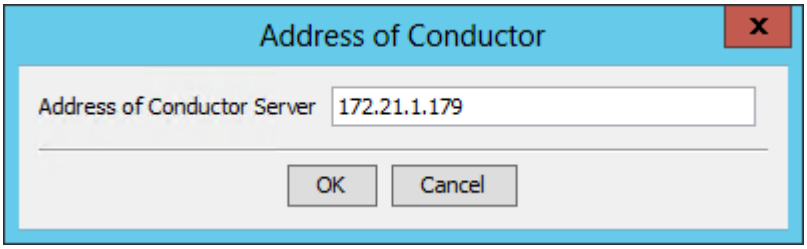
# Starting the remote installation wizard

To start the remote installation wizard.

1. On the member server, right-click the **installslave.bat** script in the install directory of the installation package and select **Run as Administrator**.

   The **Address of Conductor** page opens, as shown in Figure 16.

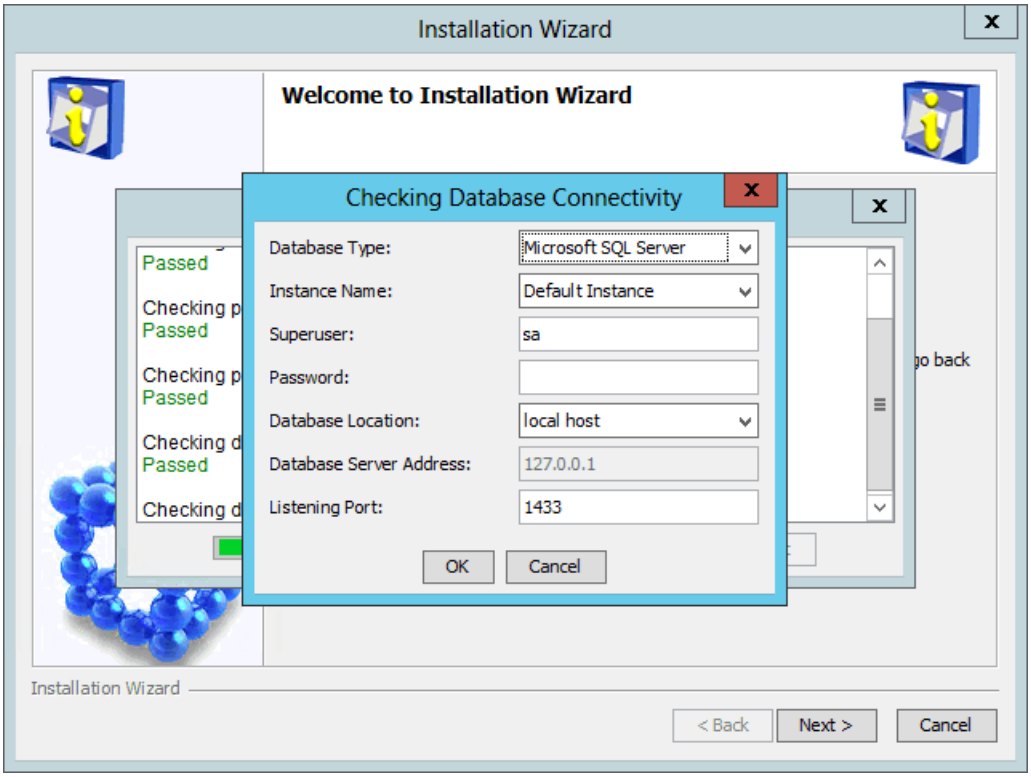
   **Figure 16 Address of Conductor**




2. Enter the IP address of the conductor server, and then click **OK**.

   The **Checking Database Connectivity** dialog box opens, as shown in Figure 17.

   **Figure 17 Checking Database Connectivity**




3. Configure the parameters as needed. For descriptions about the parameters, see "Checking the installation environment."
4. Click **OK** to start checking the database connectivity.

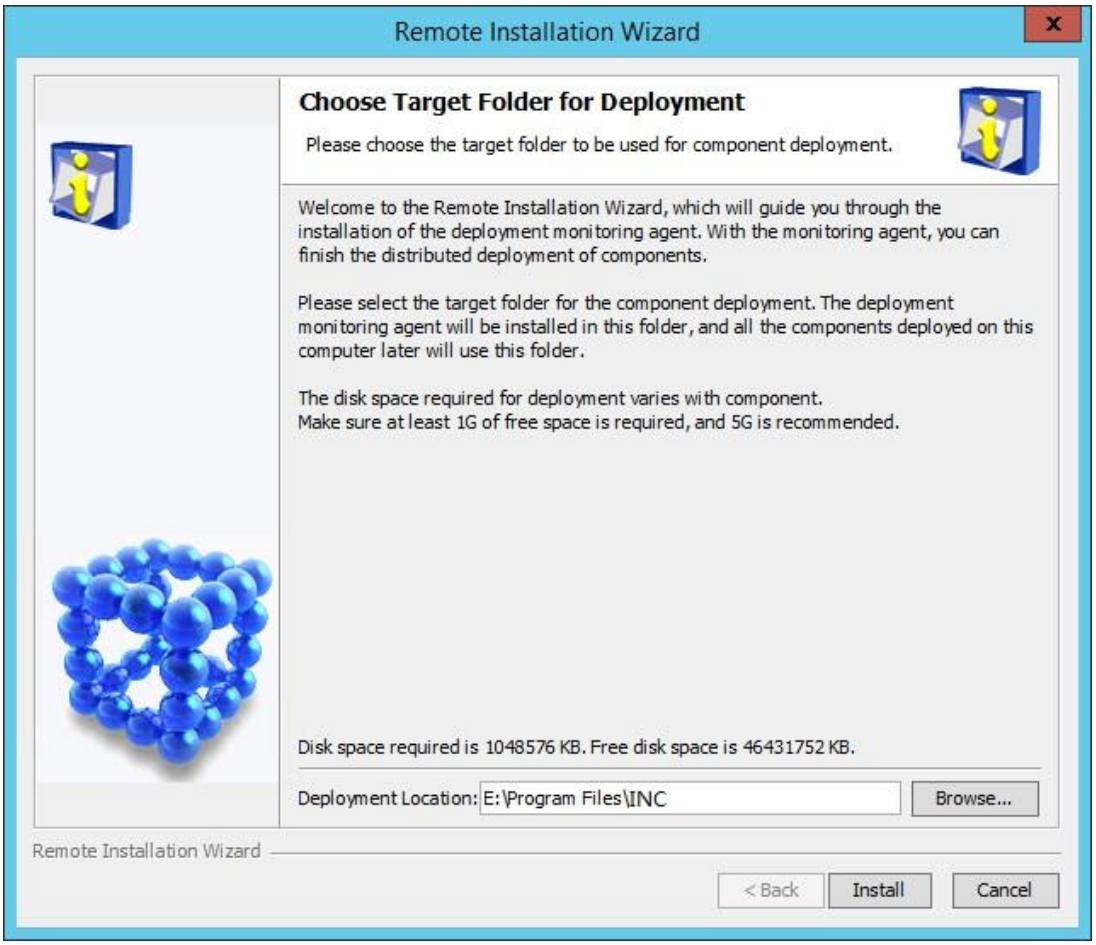
   After the installation environment check is passed, the **Remote Installation Wizard** opens, which means that you have successfully started the remote installation wizard.

1. On the **Choose Target Folder for Deployment** dialog box shown in Figure 18, specify the deployment location for the Intelligent Deployment Monitoring Agent.

   The default deployment location is the **\Program Files\INC** directory of the disk with the maximum free space on Windows. This example uses **E:\Program Files\INC**.

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

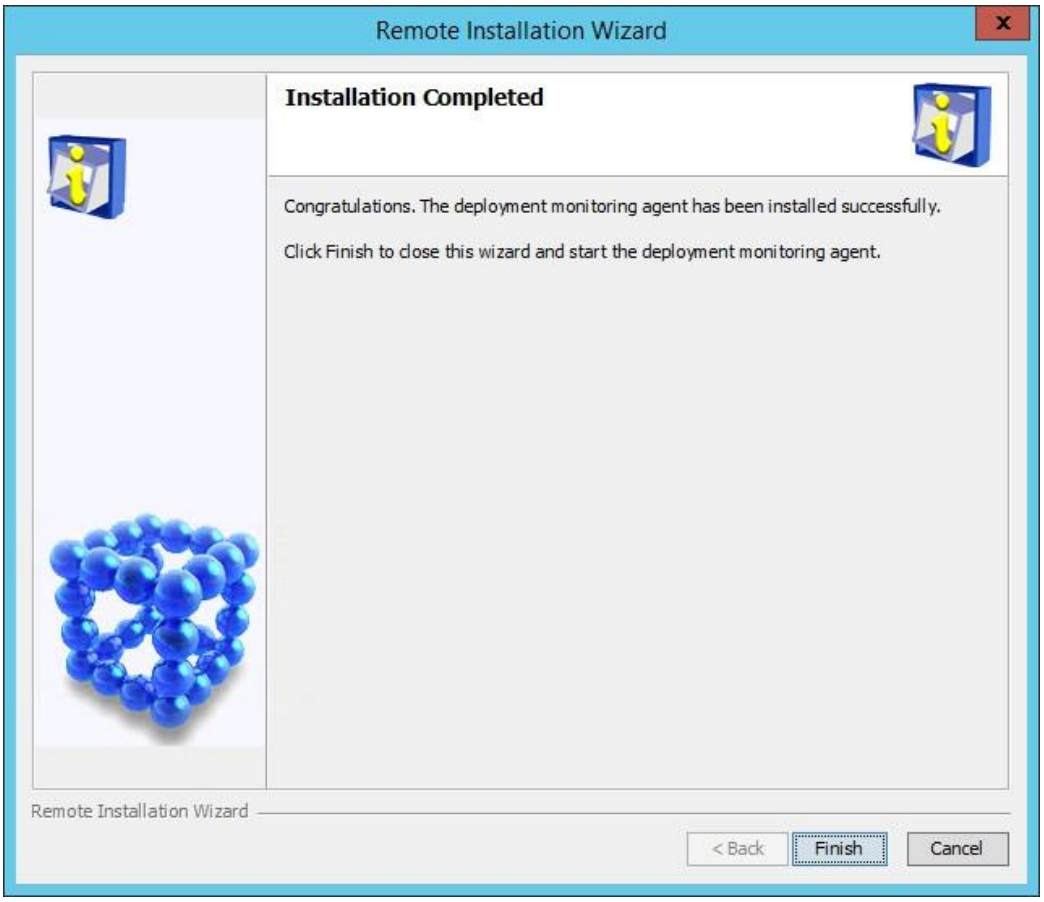
   **Figure 18 Choose Target Folder for Deployment**




2. Click **Install**.

   The system starts to download files. After the download, the **Installation Completed** dialog box opens, as shown in Figure 19.

**Figure 19 Installation Completed**




3. Click **Finish**.

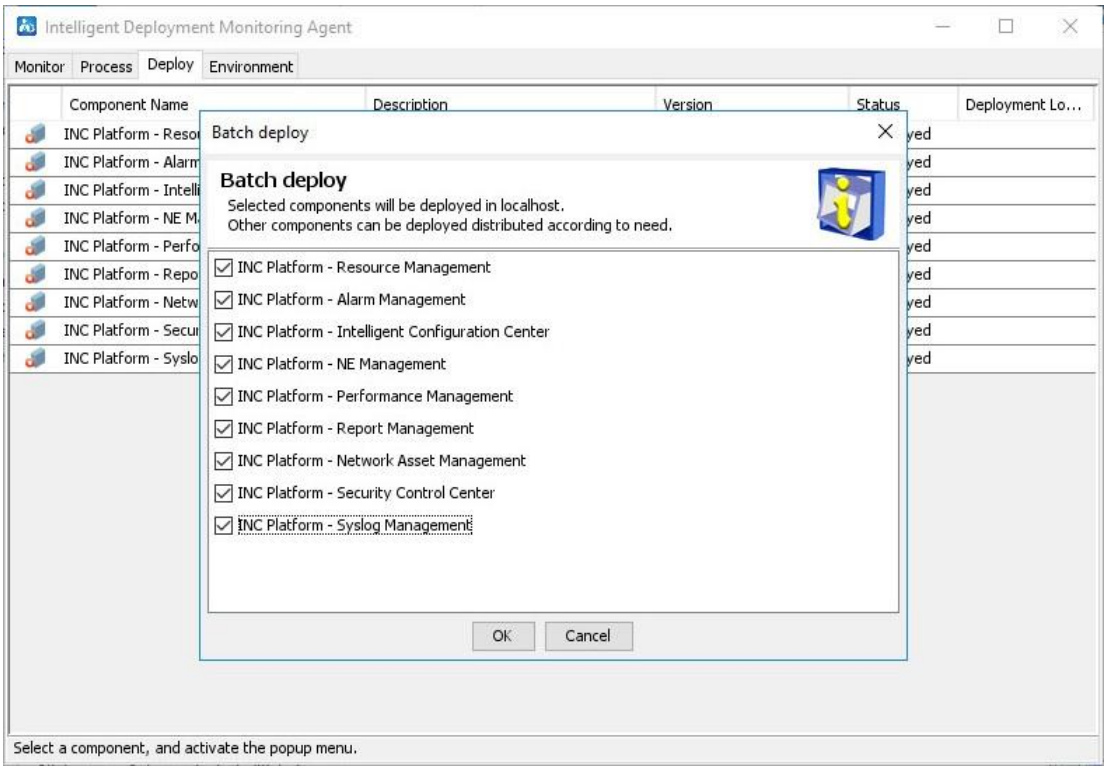
# Deploying the INC platform subcomponents

1. Click the **Deploy** tab.

   The **Deploy** tab displays information about all INC components that have been installed.
2. Right-click a platform subcomponent that has not been deployed, and then select **Batch Deploy** from the shortcut menu.

   The **Batch deploy** dialog box opens.

**Figure 20 Batch deploy**



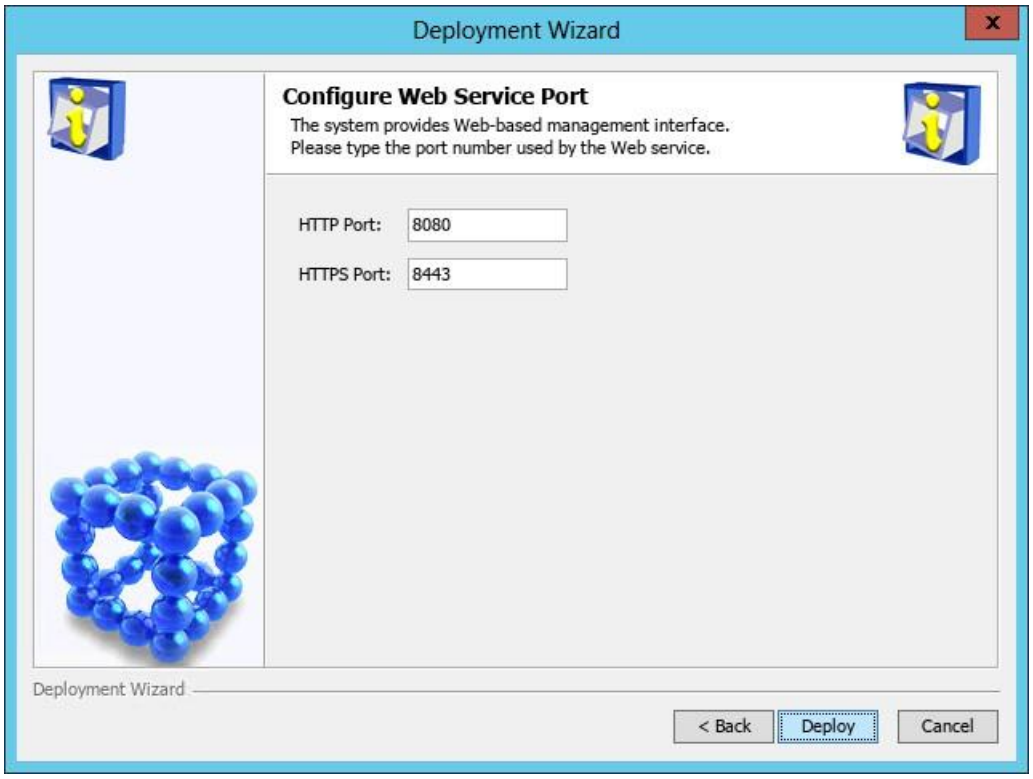

3. Select the subcomponents you want to deploy, and then click **OK**.

   The system starts downloading the files.

4. Perform the following tasks after the download is complete:

   a. On the **Configure Web Service Port** page, set **HTTP Port** (**8080** by default) and **HTTPS Port** (**8443** by default) as needed.

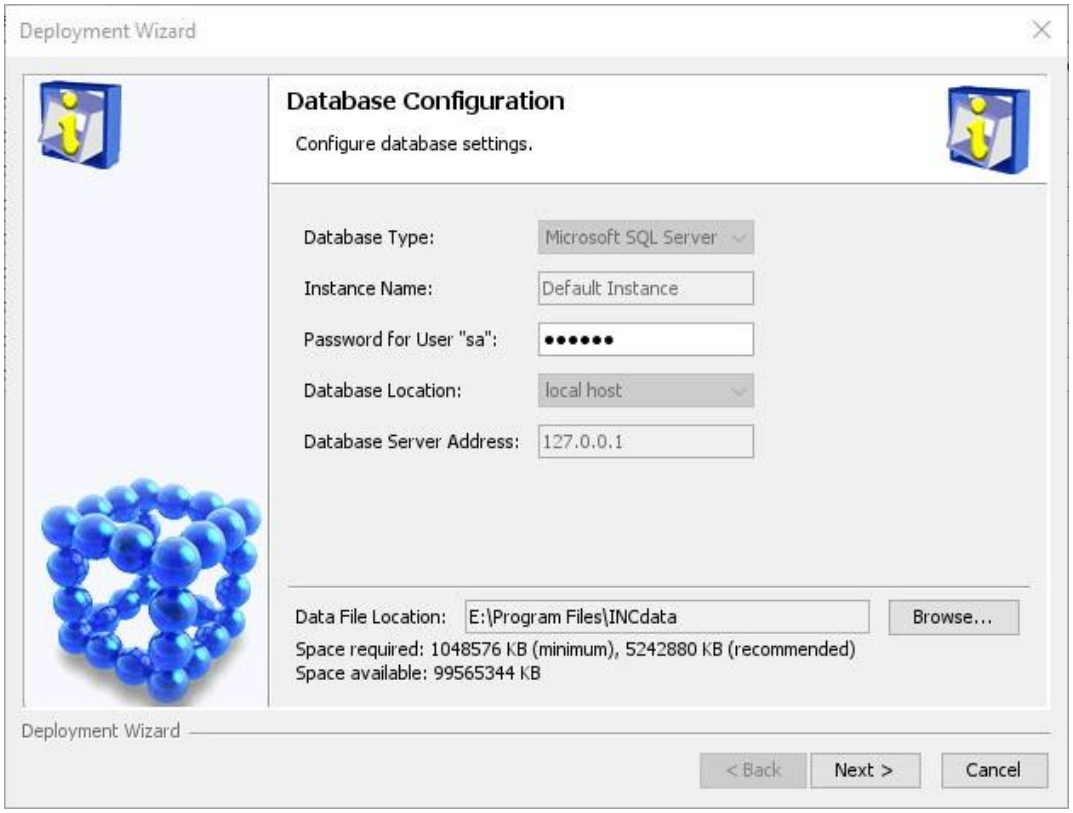
**Figure 21 Configure Web Service Port**




**a.** On the **Database Configuration** page, perform the following tasks:

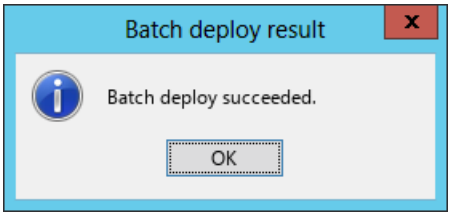
- Enter the password for the user **sa** for the current database, which is the superuser name specified during INC installation.
- Specify the data file location on the database server. The default location is the **\Program Files\INCdata** directory of the disk with the maximum free space on Windows. This example uses **E:\Program Files\INCdata**.

**Figure 22 Database Configuration**




5. Click **Deploy** to start the deployment.
   After the deployment is finished, the **Batch deploy result** dialog box opens.

   **Figure 23 Batch deploy result**




6. Click **OK**.

# Managing INC by using the Intelligent Deployment Monitoring Agent

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

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

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

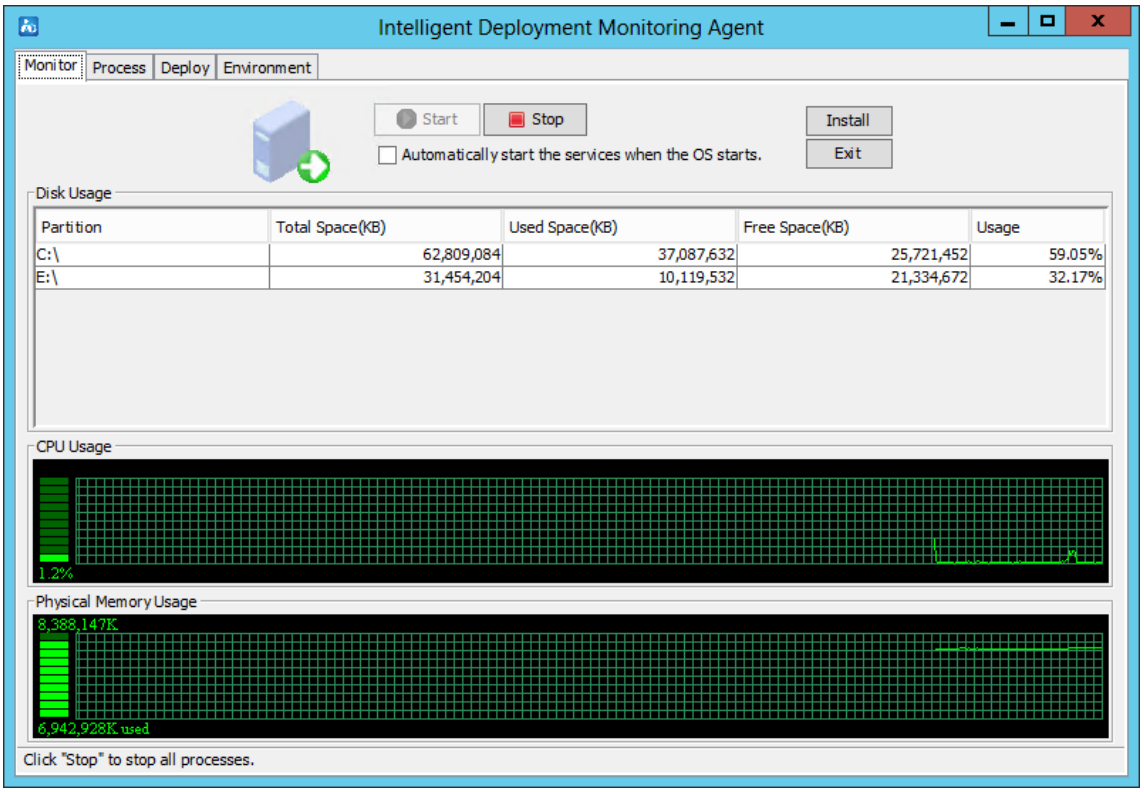
## Starting the Intelligent Deployment Monitoring Agent

To start the Intelligent Deployment Monitoring Agent, click **Start**, access the all applications page, and then select **INC** > **Deployment Monitoring Agent**.

As shown in Figure 24, the agent contains the following tabs: **Monitor**, **Process**, **Deploy**, and **Environment**. By default, the **Monitor** tab is displayed.

The following information describes the functionality of each tab.

**Figure 24 Intelligent Deployment Monitoring Agent**



# Monitor tab

As shown in Figure 25, the **Monitor** tab displays the performance information for the INC server, including the disk, CPU, and physical memory usage information.

The tab also provides the following options:

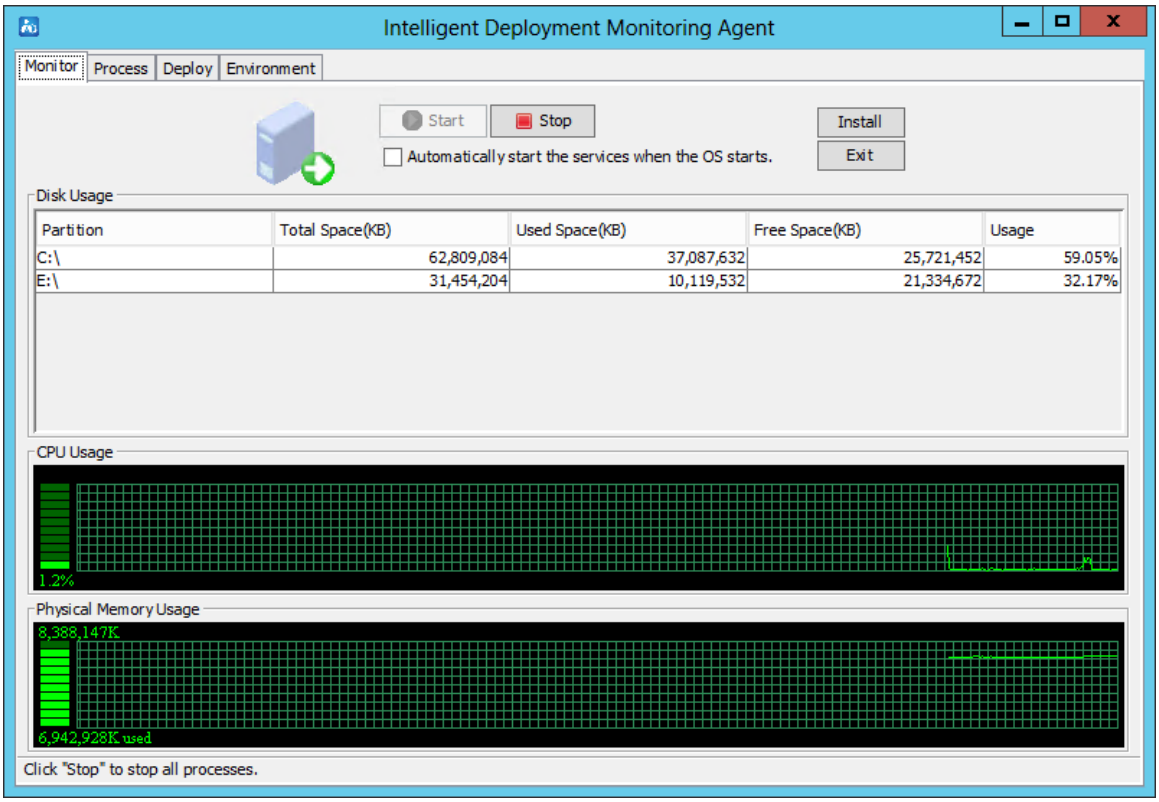
- **Start**—Click this button to start INC. This button is available when INC is stopped.

**IMPORTANT:**

For correct operation, the **Intelligent Management Server**service must start with an account that has read/write permissions on the INC installation folder. By default, the **Intelligent Management Server** service starts with the **Local System** account.

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

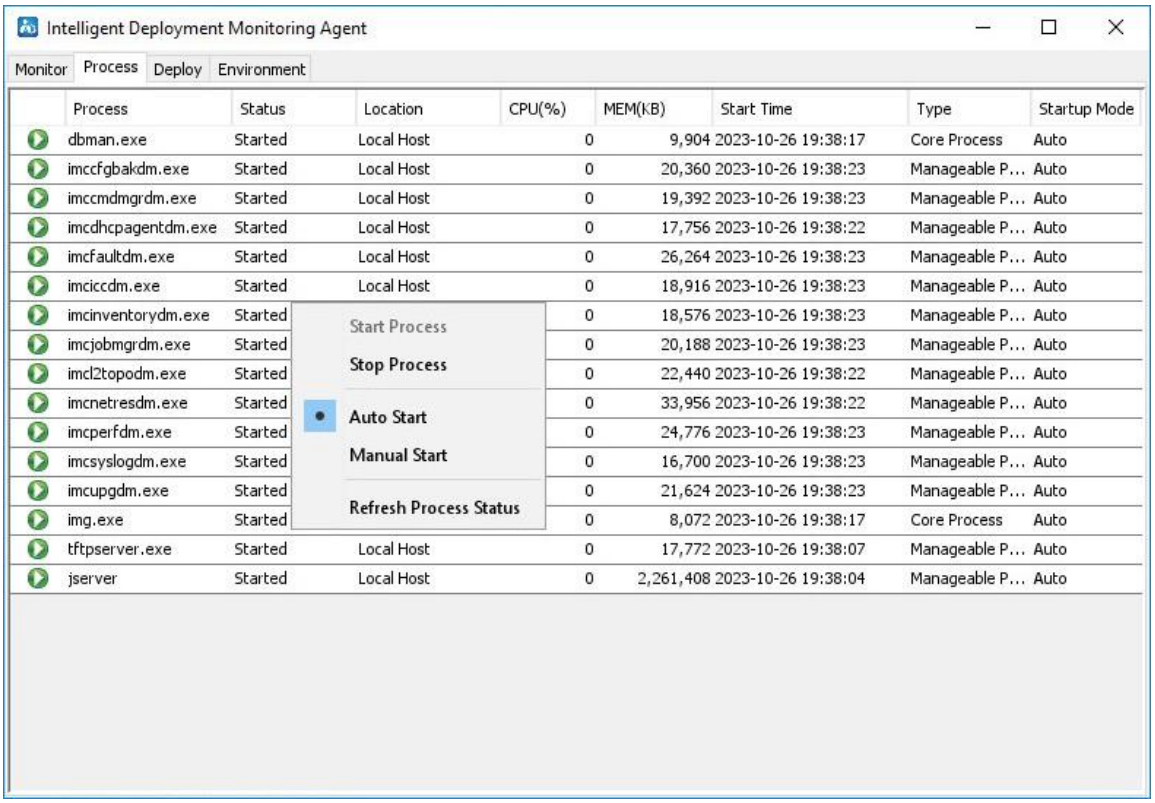
**Figure 25 Monitor tab of the Intelligent Deployment Monitoring Agent**




# Process tab

As shown in Figure 26, the **Process** tab displays INC process information.

**Figure 26 Process tab of the Intelligent Deployment Monitoring Agent**



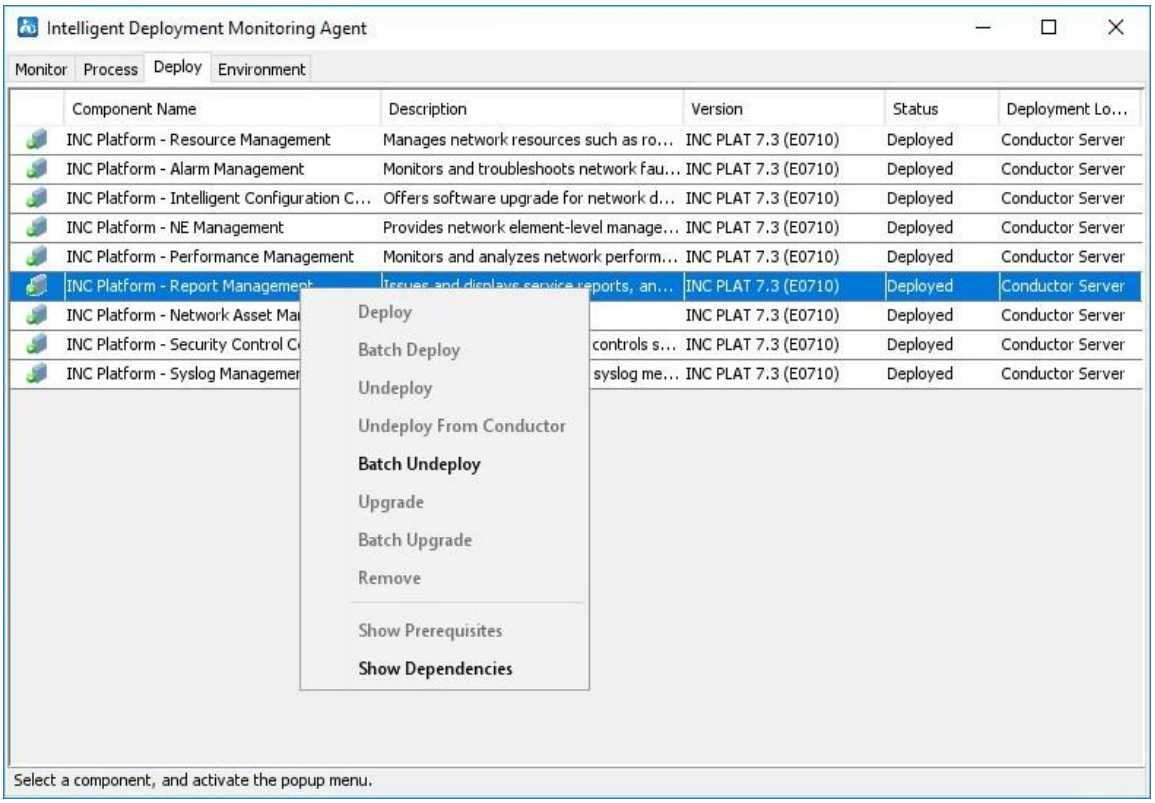

The right-click menu of a manageable process provides the following options:

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

# Deploy tab

As shown in Figure 27, the **Deploy** tab displays information about all deployed components.

**Figure 27 Deploy tab of the Intelligent Deployment Monitoring Agent**




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

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

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

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

  This option is available only when the selected component is in **Deployed** state.
- **Undeploy From Conductor**—Select this option to delete component deployment information from the conductor server.

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

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

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

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

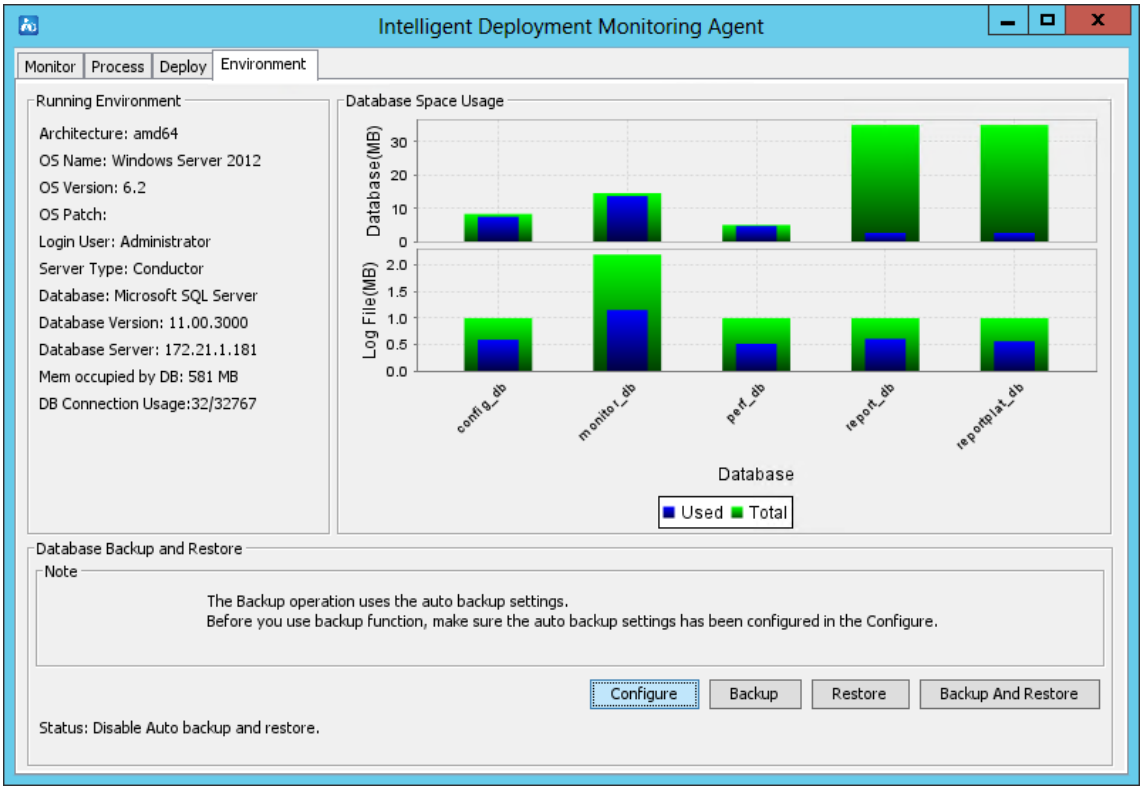
# Environment tab

As shown in Figure 28, the **Environment** tab displays the software, hardware, and database information for the current INC server.

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

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

**Figure 28 Environment tab of the Intelligent Deployment Monitoring Agent**



# Installing and deploying INC service components

The following information describes how to install and deploy the service components.

Table 10 lists all service components and subcomponents in INC.

**Table 10 Service components and subcomponents**

| Component | | Subcomponent | Optional server |
|---|---|---|---|
| Endpoint Intelligent Access | User Access Manager | Intelligent Strategy Proxy | Conductor or member |
| | | User Access Management | Conductor or member |
| | | User Access Management Sub Server | Member |
| | | Portal Server | Conductor or member |
| | | EIP Server | Conductor or member |
| | | EIP Sub Server | Member |
| | | Policy Server | Conductor or member |
| | | Policy Proxy Server | Conductor or member |
| | | User SelfService | Conductor or member |
| | | Third-Party Page Publish Server | Conductor or member |
| | TACACS+ Authentication Manager | TACACS+ Authentication Manager | Conductor or member |
| Wireless Service Manager | | Wireless Service Manager | Conductor or member |
| | | Wireless Intrusion Prevention System | Conductor or member |
| | | Wireless Location Manager | Conductor or member |
| | | Wireless Location Engine | Conductor or member |

All the service components can be installed in the same way, but their deployment procedure might differ. Based on the deployment procedure, the service components can be classified into several categories, as shown in Table 11.

**Table 11 Service components classified by deployment procedure**

| Example component | Similar components |
|---|---|
| EIA | N/A |

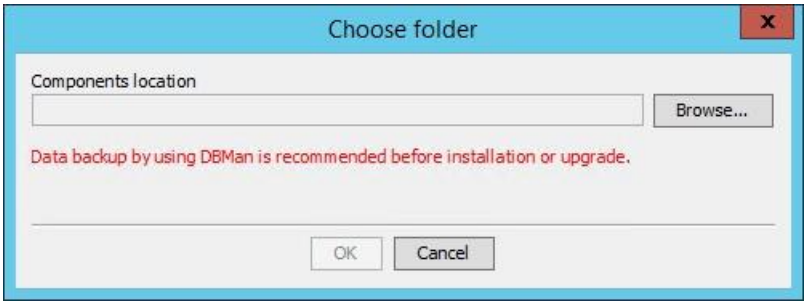
The following information describes how to install and deploy EIA.

# Installing and deploying INC EIA

## Installing INC EIA

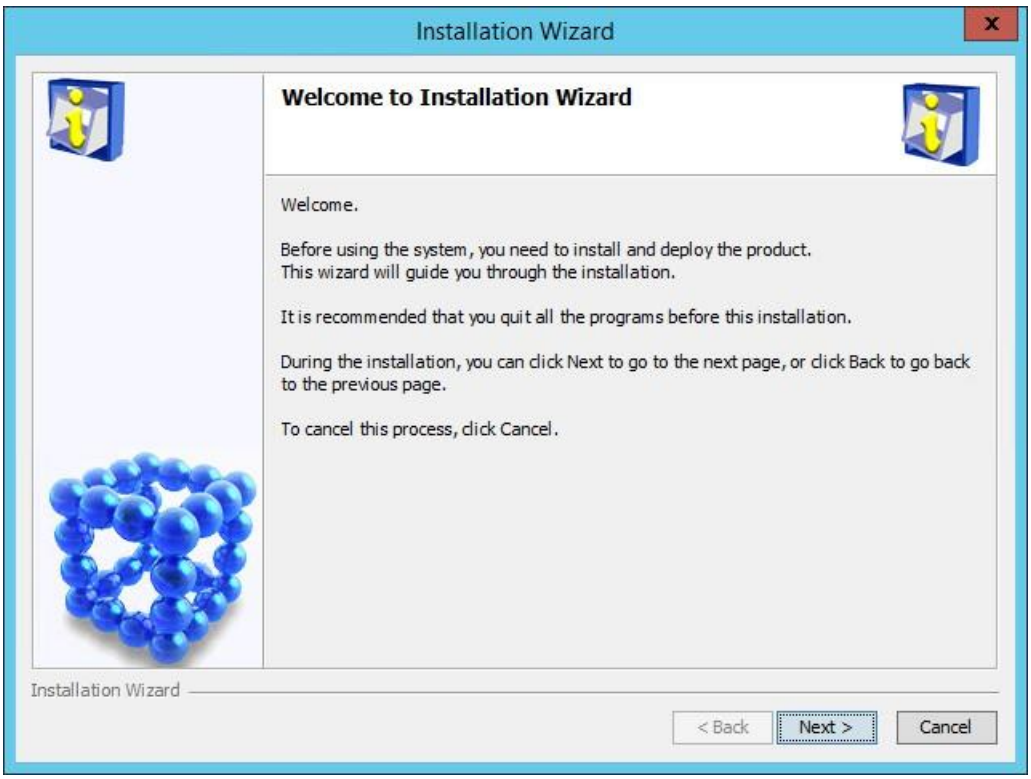
1. Start the Intelligent Deployment Monitoring Agent, and then click **Install** on the **Monitor** tab.
   The **Choose folder** dialog box opens, as shown in Figure 29.

   **Figure 29 Choose folder dialog box**



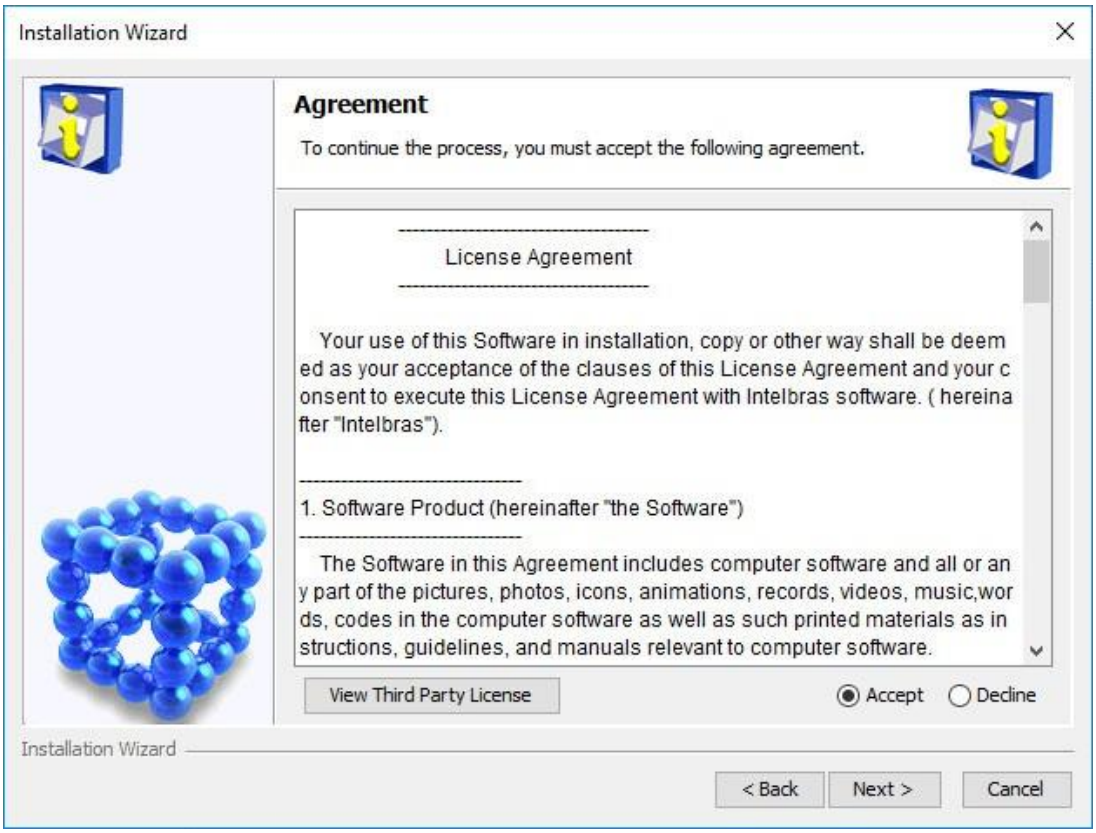

2. Click **Browse**, and then select the **install\components** folder in the EIA installation package.
3. Click **OK**.
   The INC installation wizard opens, as shown in Figure 30.

   **Figure 30 INC installation wizard**




4. Click **Next**.
   The **Agreement** page opens, as shown in Figure 31.

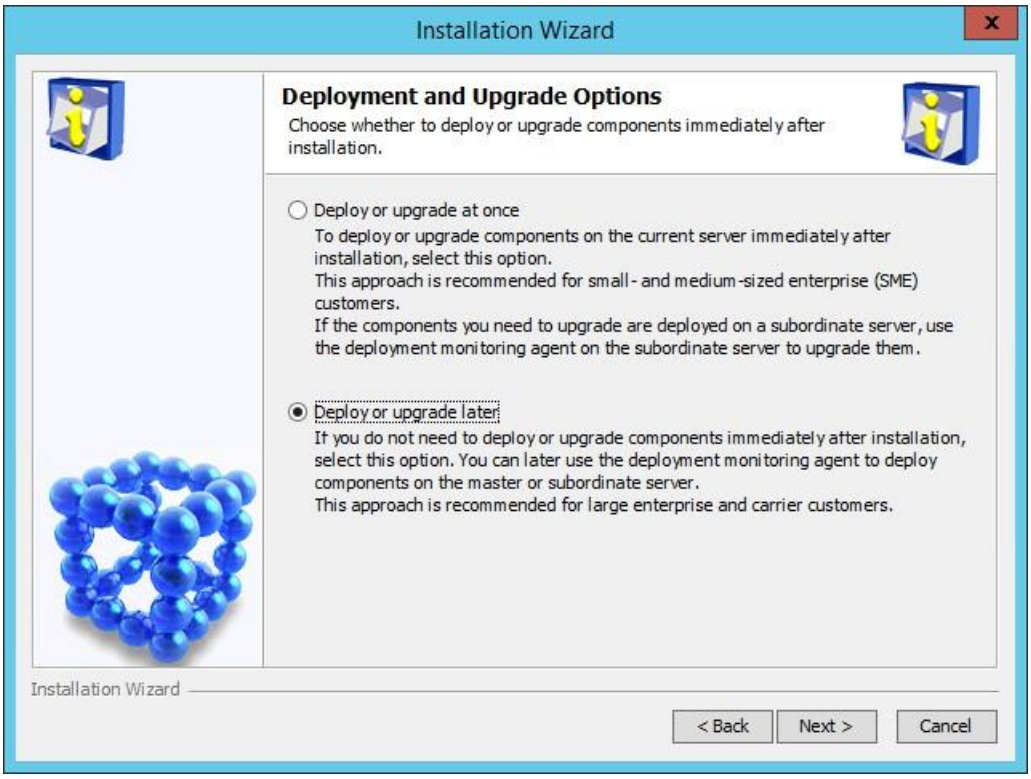
**Figure 31 Agreement page**




5. Read the license agreement and third-party license and select **Accept**.
6. Click **Next**.
7. Select the EIA subcomponents you want to install in the component list.
8. Click **Next**.

   The **Deployment and Upgrade Options** page opens, as shown in Figure 32.

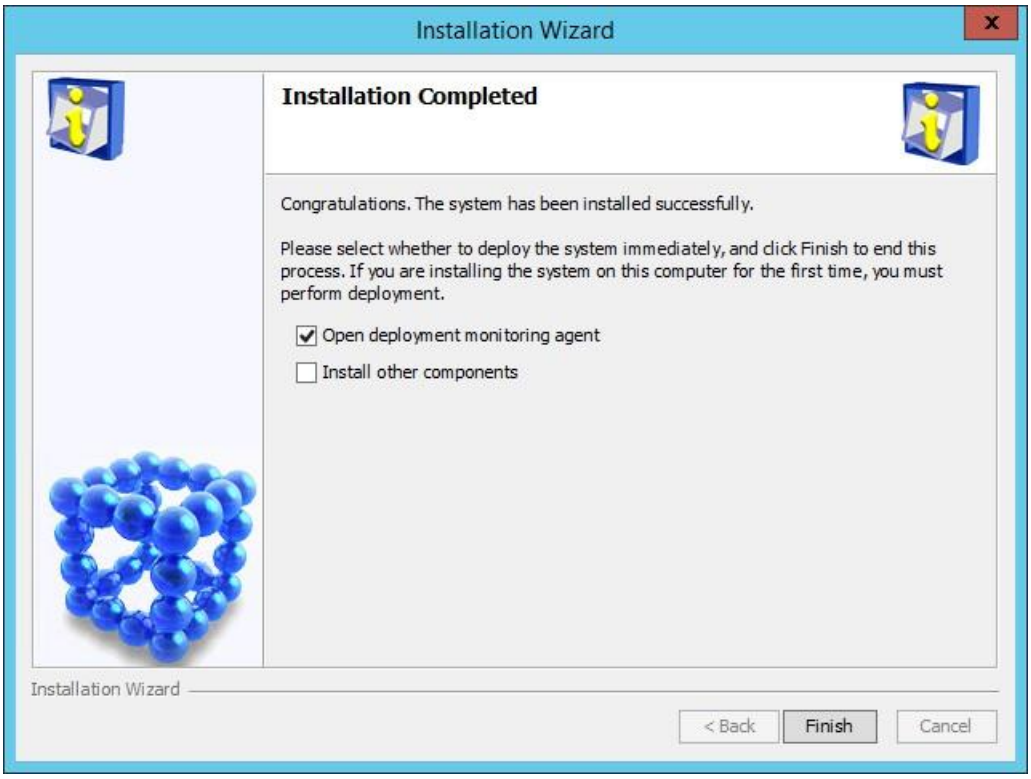
**Figure 32 Deployment and Upgrade Options page**




9. Select **Deploy or upgrade later**.
10. Click **Next**.
11. Verify the installation information, and then click **Install**.

    After the installation is complete, the **Installation Completed** page opens, as shown in Figure 33.

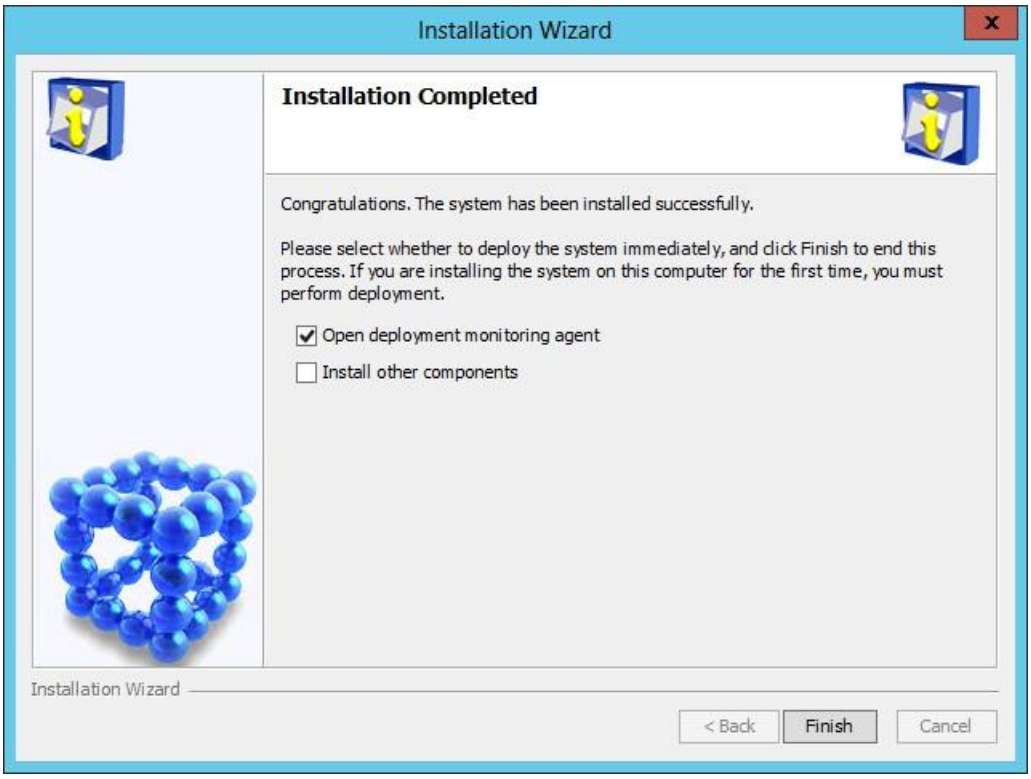
**Figure 33 Installation Completed page**




# Deploying EIA on the conductor server

1. On the **Installation Completed** page shown in Figure 34, select **Open deployment monitoring agent** and click **Finish**.

**Figure 34 Installation Completed page**




The **Batch deploy** dialog box opens.

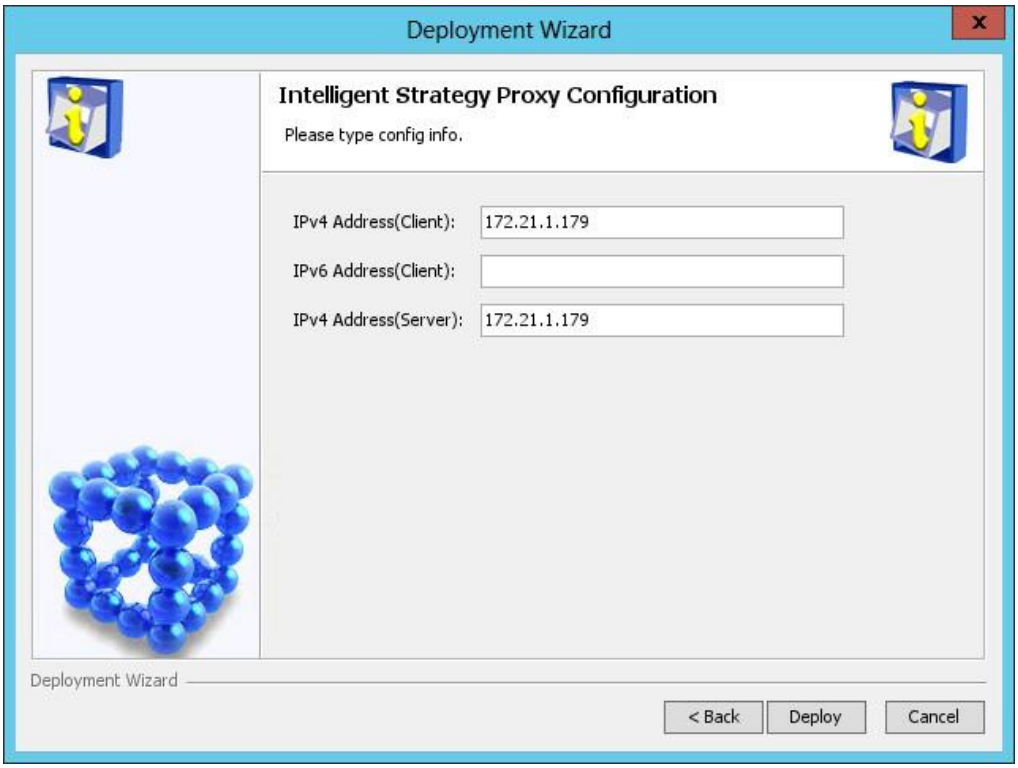
2. Select the EIA subcomponents you want to deploy, and then click **OK**.

   In this example, select all the EIA subcomponents except EIP Sub Server and Third-Party Page Publish Server.

   The EIP Sub Server subcomponent can be deployed only on member servers in distributed deployment.

   The INC deployment wizard starts and displays the **Intelligent Strategy Proxy Configuration** page, as shown in Figure 35.

**Figure 35 Intelligent Strategy Proxy Server Configuration page**

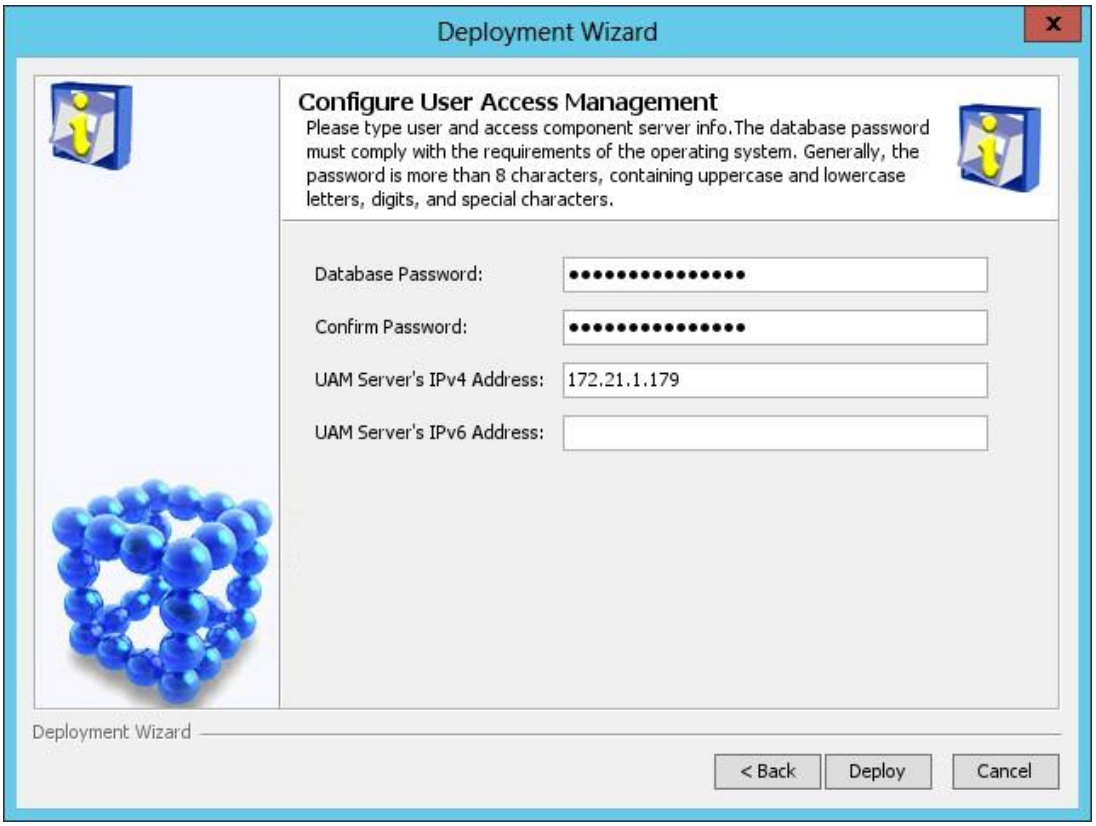



3. Configure the following parameters:
   - **IPv4 Address(Client)**—Enter the IP address of the Intelligent Strategy Proxy component. By default, this field is automatically populated with the IP address of the local host.
   - **IPv4 Address(Server)**—Enter the IP address of the User Access Management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

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

   The **Configure User Access Management** page opens, as shown in Figure 36.

**Figure 36 Configure User Access Management page**

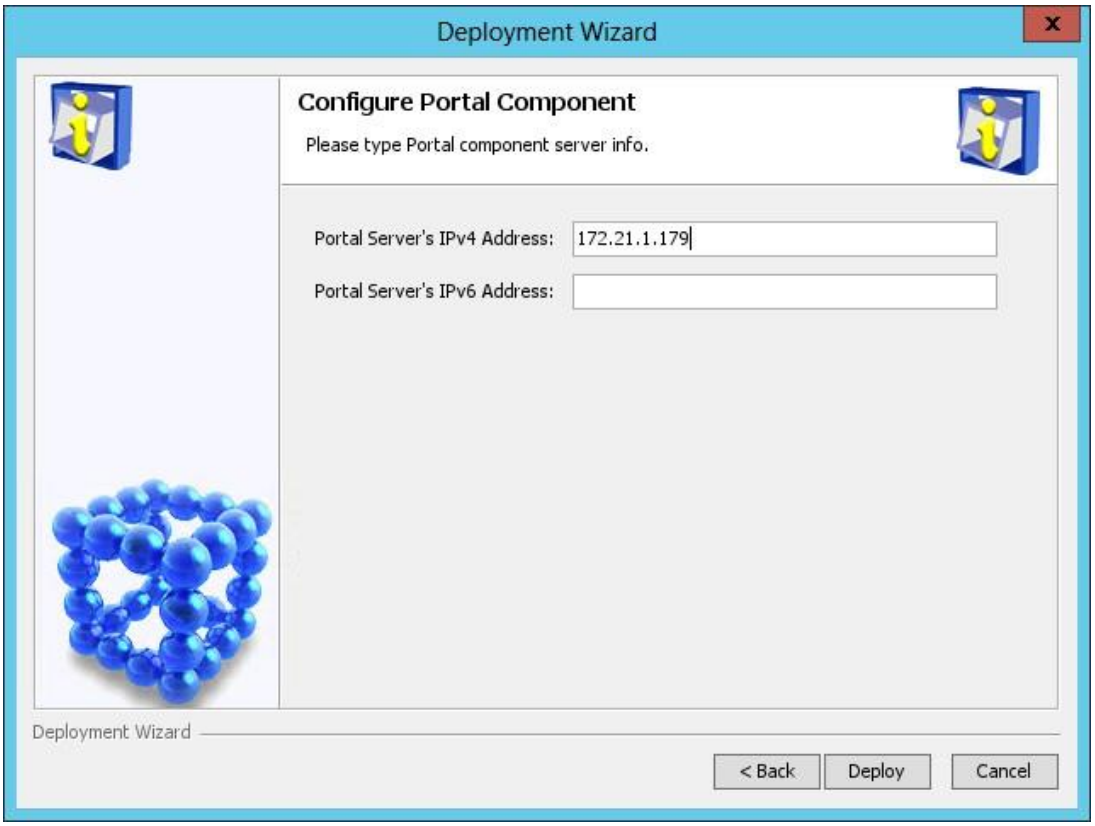



5. Configure the following parameters:
   - **Database Password/Confirm Password**—These fields are automatically populated with the password of the database superuser **sa** specified during INC platform installation.

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

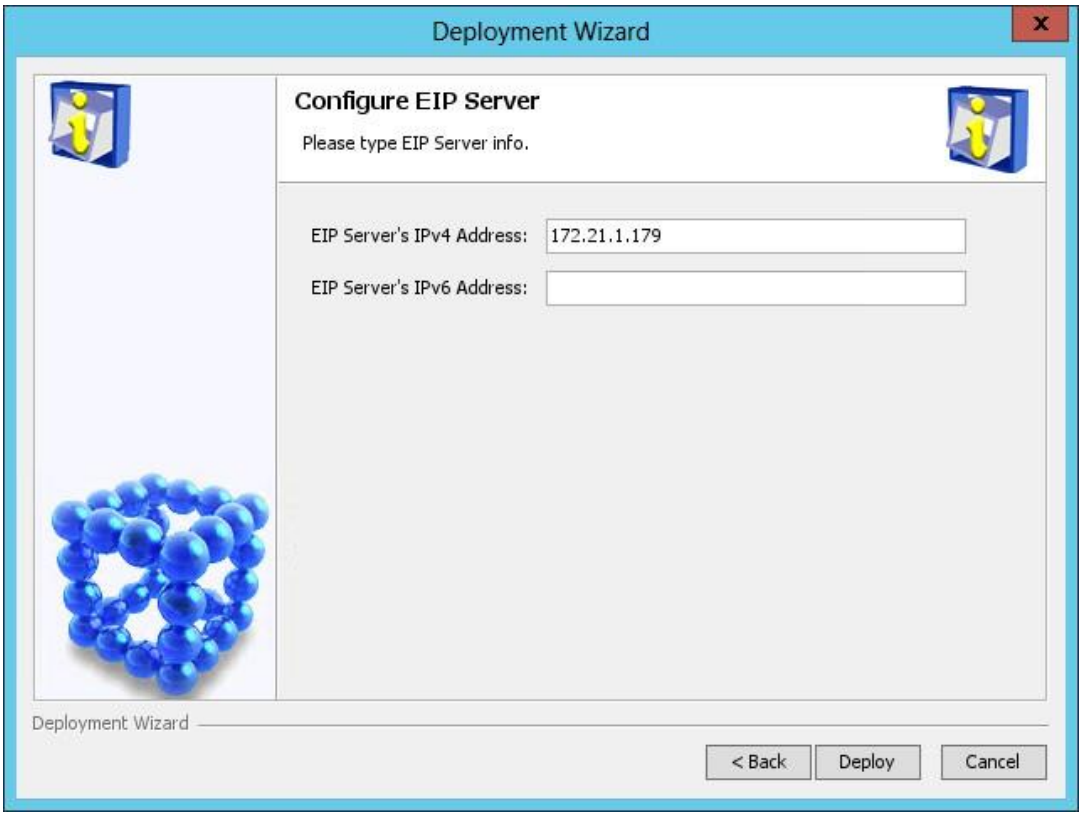
   The **Configure Portal Component** page opens, as shown in Figure 37.

**Figure 37 Configure Portal Component page**



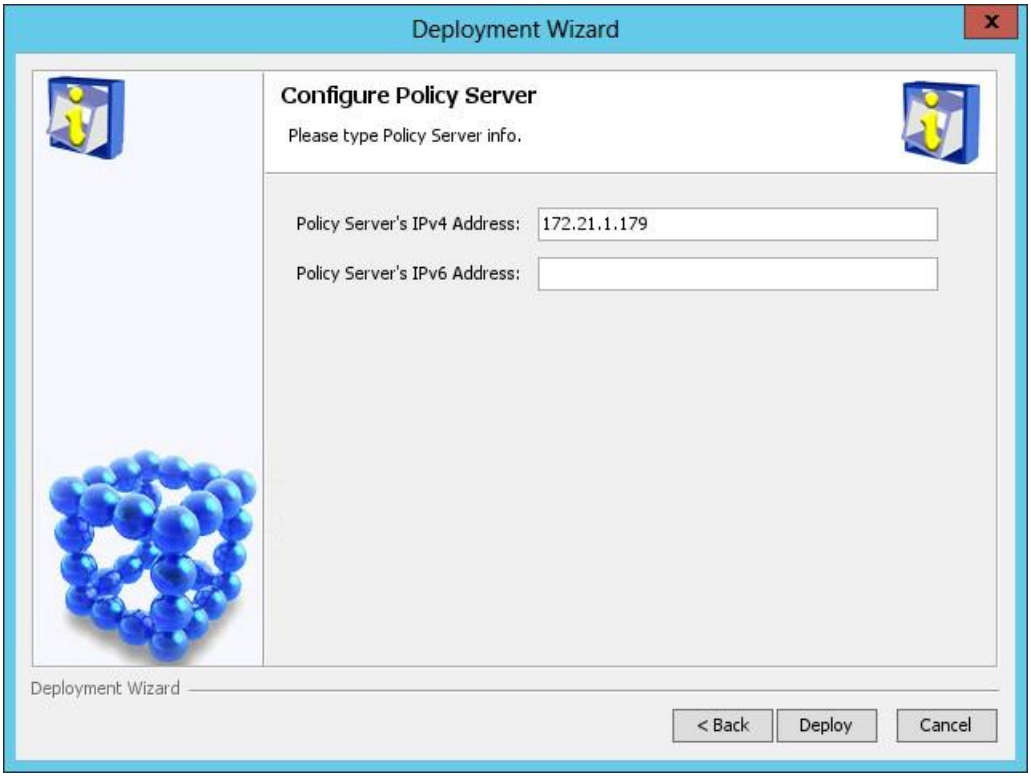

7. Use the default settings, and then click **Deploy**.
   The **Configure EIP Server** page opens, as shown in Figure 38.

**Figure 38 Configure EIP Server page**




8. Use the default settings, and then click **Deploy**.
   The **Configure Policy Server** page opens, as shown in Figure 39.

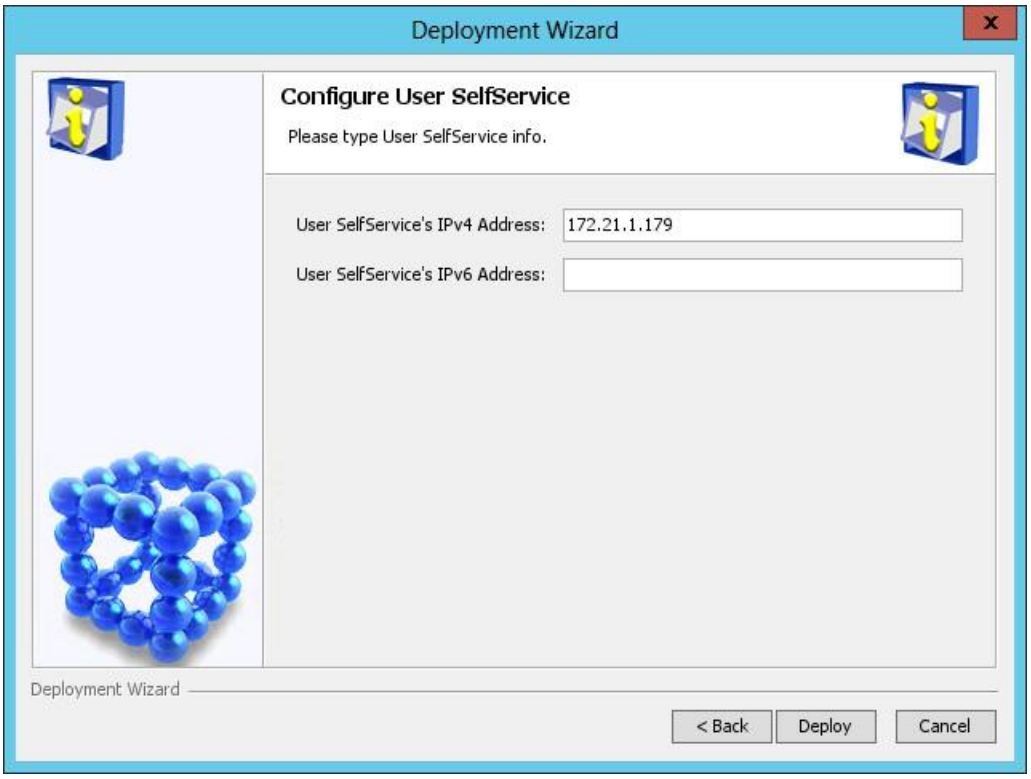
**Figure 39 Configure Policy Server page**



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

The **Configure User SelfService** page opens, as shown in Figure 40.

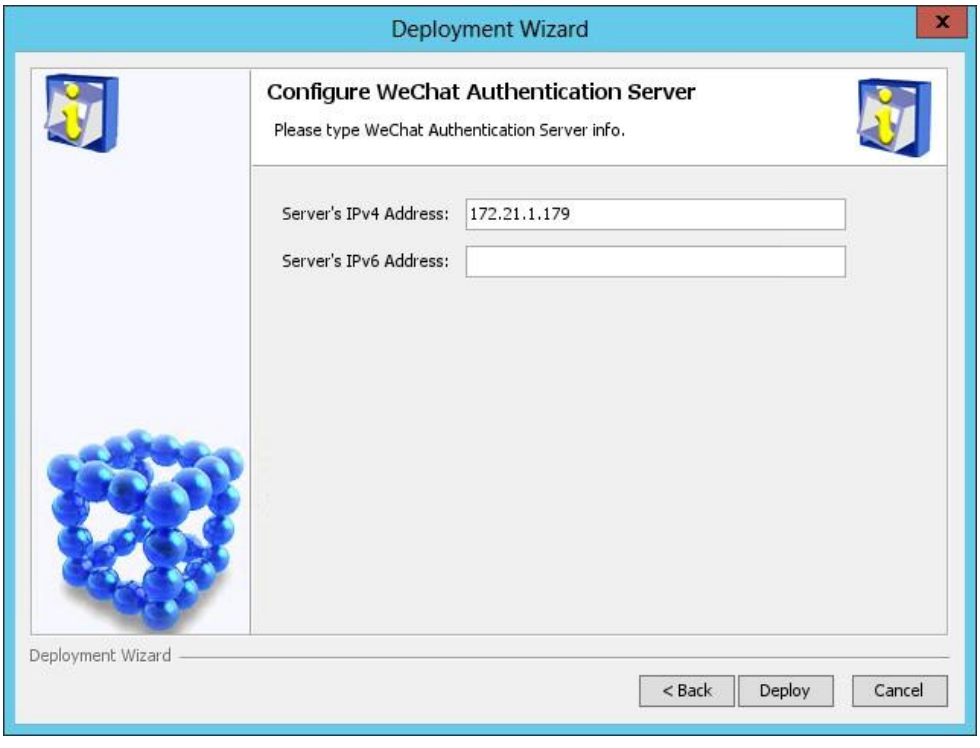
**Figure 40 Configure User SelfService page**




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

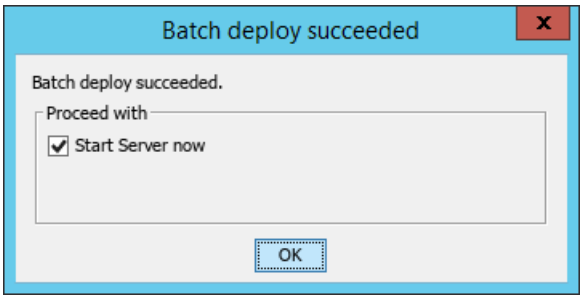
The **Configure WeChat Authentication Server** page opens, as shown in Figure 41.

**Figure 41 Configure WeChat Authentication Server page**



11. Use the default settings, and then click **Deploy**.
    All the selected EIA subcomponents are deployed.
    The **Batch deploy succeeded** dialog box opens, as shown in Figure 42.

    **Figure 42 Batch deploy succeeded dialog box**

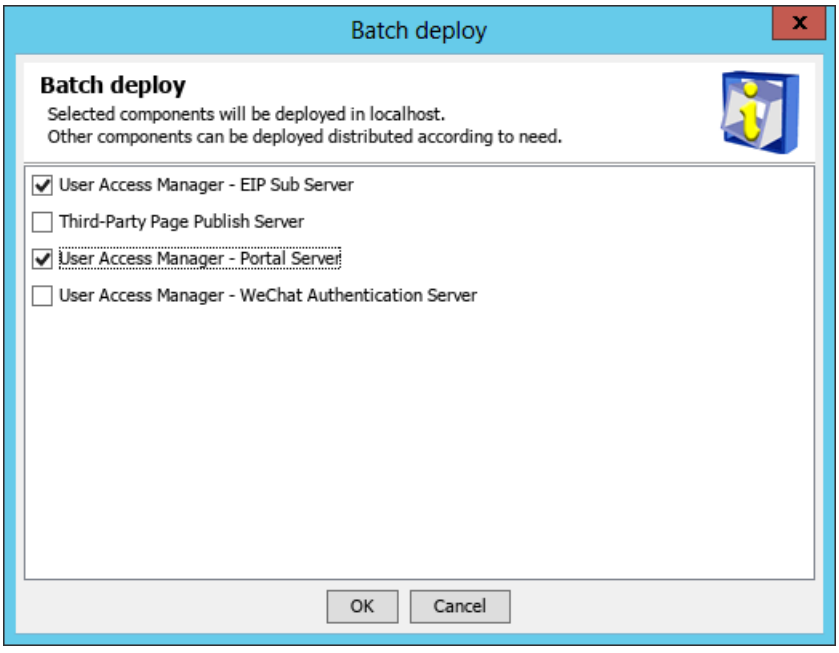



12. Configure **Start Server now** as needed, and then click **OK**.

# Deploying EIA on a member server

1. In the Intelligent Deployment Monitoring Agent, click the **Deploy** tab.
   The **Deploy** tab displays information about all INC components that have been installed.
2. Right-click a component that is not deployed, and then select **Batch Deploy** from the shortcut menu.
   The **Batch deploy** dialog box opens, as shown in Figure 43.

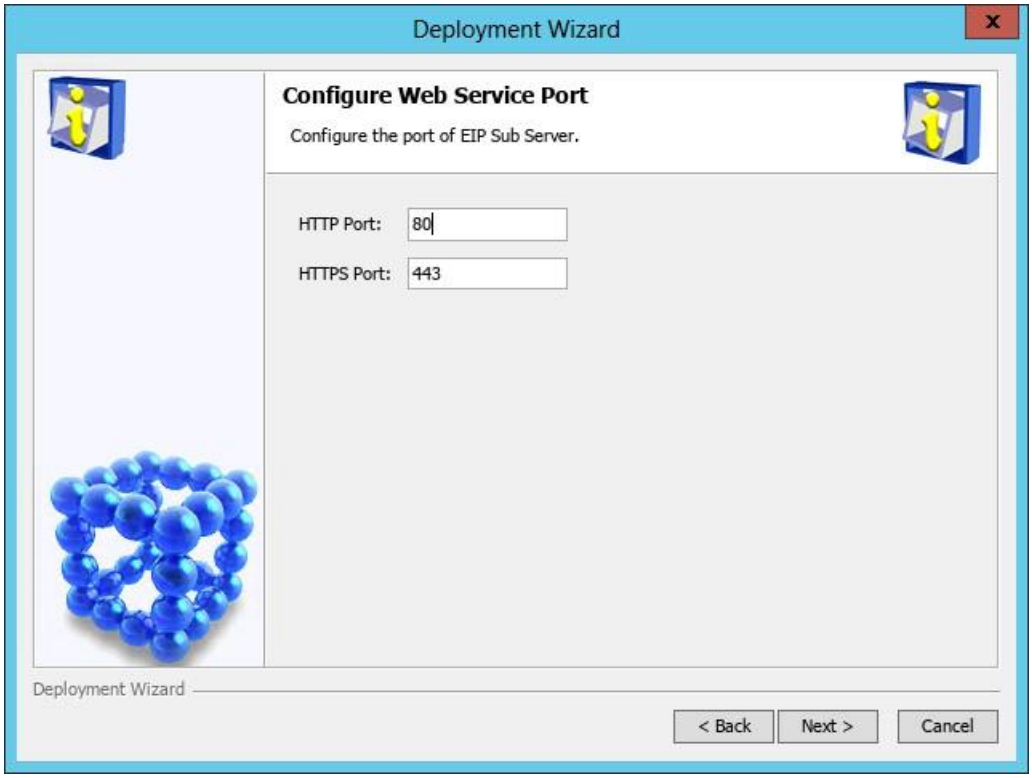
   **Figure 43 Batch deploy dialog box**




3. Select the EIA subcomponents you want to deploy.
   In this example, select Portal Server and EIP Sub Server.
4. Click **OK**.
   The system starts to deploy the selected EIA subcomponents.

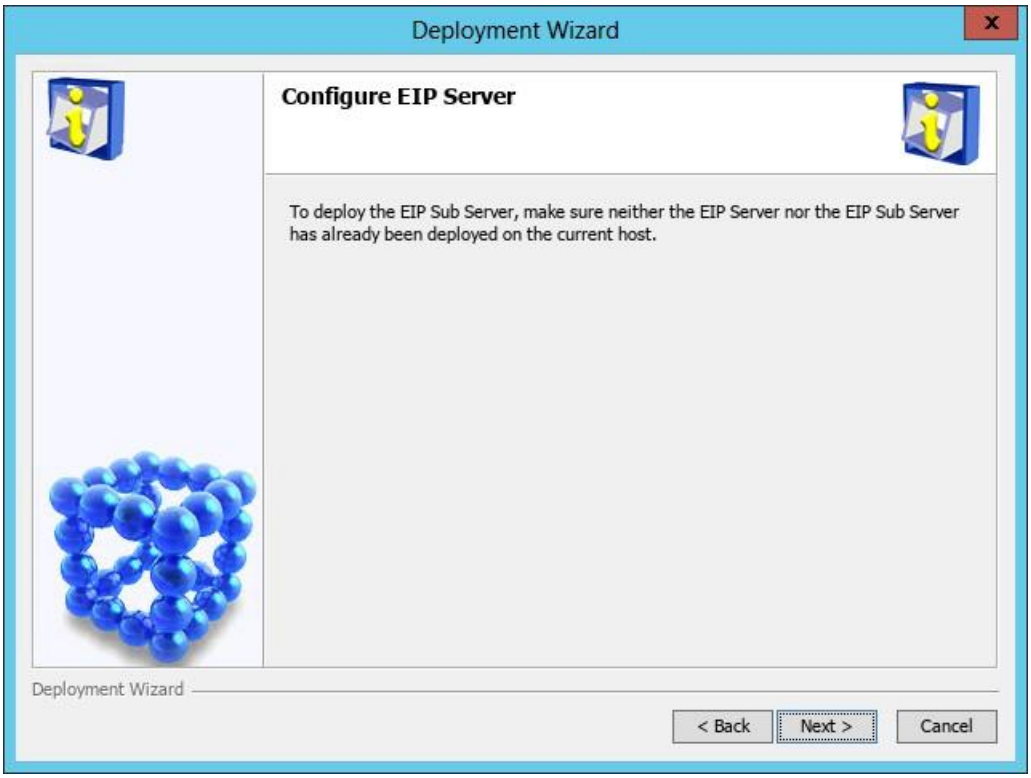
During the deployment progress, the **Configure Web Service Port** page, as shown in Figure 44.

**Figure 44 Configure Web Service Port page**




5. Configure the HTTP port and HTTPS port, and then click **Next**.
   The **Configure EIP server** page opens, as shown in Figure 45.

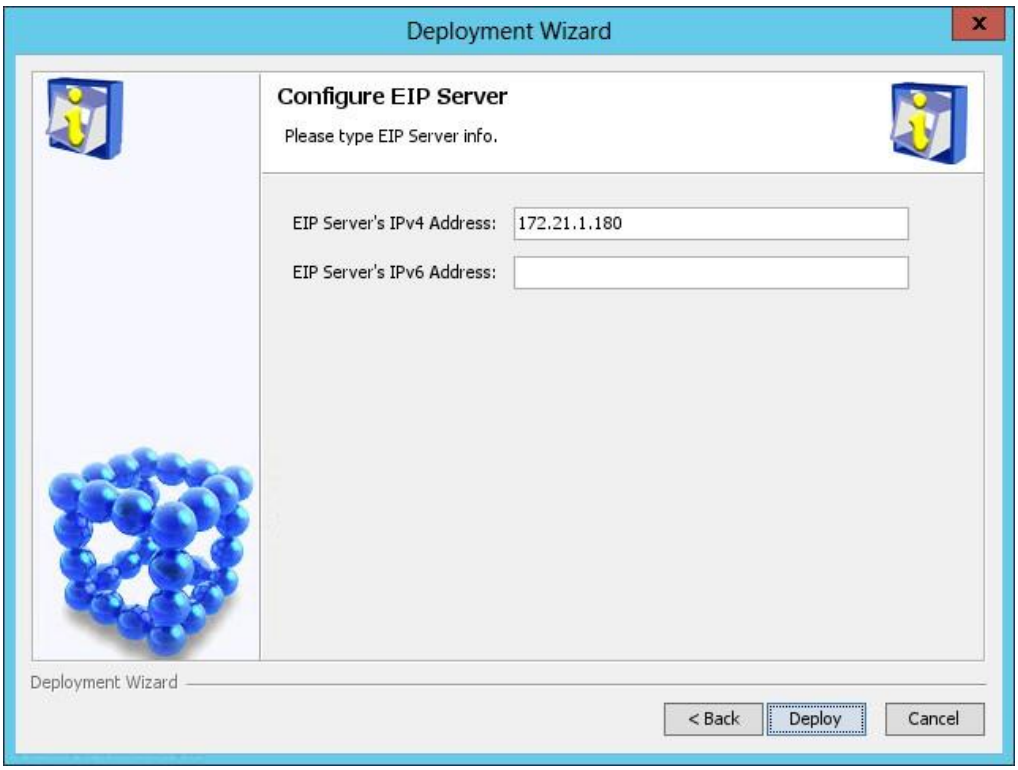
**Figure 45 Configure EIP Server page**




**6.** Verify that the EIP server and the member server have been locally deployed, and then click **Next**.

The **Configure EIP Server** page opens, as shown in Figure 46.

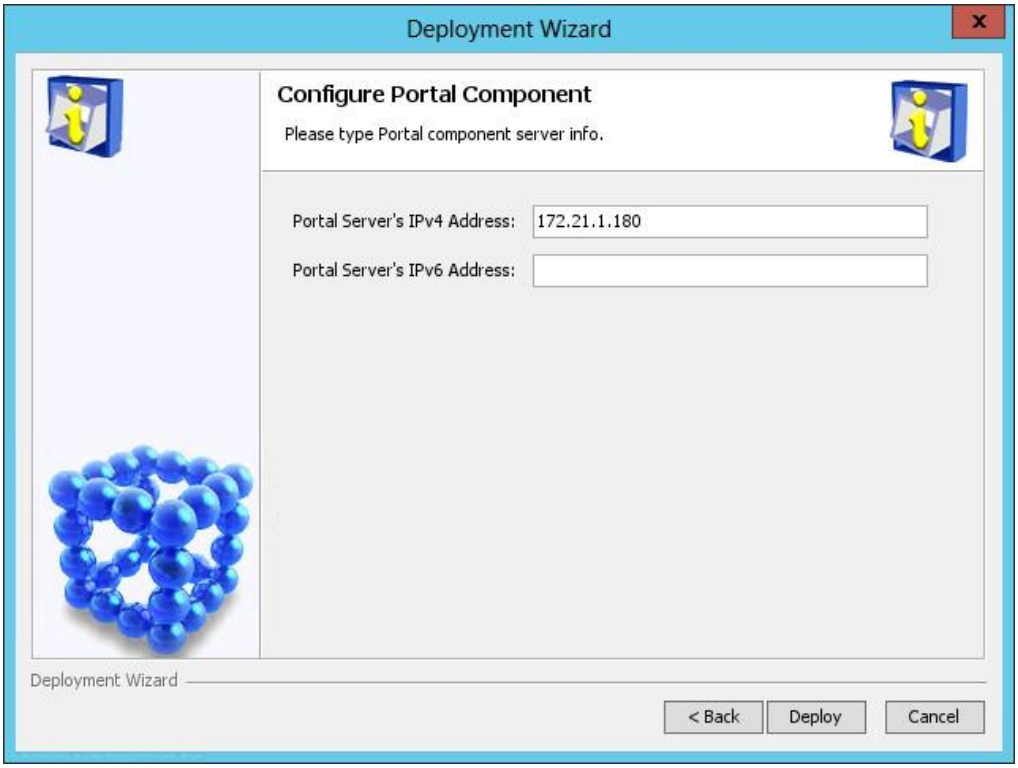
**Figure 46 Configure EIP Server page**



7. Enter the IP address of the EIP Sub Server component in the **EIP Server's IPv4 Address** field. By default, this field is automatically populated with the IP address of the local host.
8. Click **Deploy**.

   The **Configure Portal Component** page opens, as shown in Figure 47.

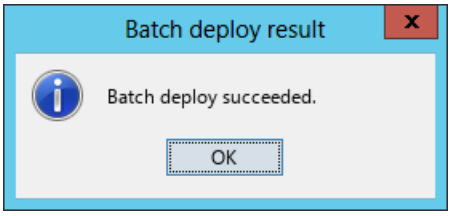
   **Figure 47 Configure Portal Component page**




9. Enter the IP address of the host where portal server is to be deployed in the **Portal Server's IPv4 Address** field. By default, this field is automatically populated with the IP address of the local host.

   After the deployment is complete, the batch deploy result dialog box opens, as shown in Figure 48.

   **Figure 48 Batch deploy result dialog box**




10. Click **OK**.

# Installing plug-ins

## Installing DHCP plug-ins

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

# Restrictions and guidelines

For INC to obtain endpoint names from a DHCP server correctly, the following requirements must be met:

- The DHCP server must exist, and it is the only DHCP server that has the DHCP plug-in installed and is reachable from the INC server.
- The **DHCP Server** service and **INC DHCP Plug** service are enabled on the DHCP server.
- The DHCP server is added to INC and its configuration is synchronized to INC.
- The **IMGAddress** value in file **server\imf\server\conf\imf.cfg** on the DHCP server is set correctly.

By default, INC does not obtain reserved or allocated IP addresses from the DHCP server. To enable INC to obtain such addresses, perform the following tasks:

1. On the DHCP server, set the value of **GetDHCPAllocAndReservedIpInfoFlag** to 1 in file **server\imf\server\conf\ dhcp_agent.cfg**.
2. Restart the **INC DHCP Plug** service on the DHCP server.
3. On the INC server, synchronize the DHCP server configuration to INC.

# Installing a DHCP plug-in on an MS DHCP server

1. On the conductor server, edit the **qvdm.conf** file to enable INC to obtain endpoint names or FQDNs from DHCP servers:
   a. In the**\server\conf** directory of the INC installation path, use Notepad to open the **qvdm.conf** file.
   b. Add the following line to the file:
      ```
      l2topoPCNameDhcpSwitch=1
      ```
   c. Save and close the file.
   d. Restart INC in the Intelligent Deployment Monitoring Agent.
2. On the MS DHCP server, edit the **imf.cfg** file so that the DHCP server can communicate with INC:
   a. Transfer the plug-in installation package **dhcp-plug-windows.zip** from the **\windows\tools** directory of the INC installation package on the INC server to the MS DHCP server.
   b. Decompress the installation package.
   c. Use Notepad to open the **imf.cfg** file in the **\dhcp-plug-windows\server\imf\server\conf** directory.
   d. Edit the **imf.cfg** file:
      - Set the value of **IMGAddress** to the IP address of the conductor server.
      - Set the value of **IMGPort** to the IMG port number, which is 8800 by default.
   e. Save and close the file.
3. Run the **install.bat** script in the **dhcp-plug-windows** directory.

   After the installation is complete, a new service **INC DHCP Plug** is added to the system services.
4. Start the **INC DHCP Plug** service:
   a. Click **Start**, and then select **Administrative Tools** > **Component Services**.
   b. On the **Component Services** page, select **Services (Local)** from the navigation tree.
   c. On the **Services (Local)** list, right-click the **INC DHCP Plug** service, and then select **Start**.

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

**IMPORTANT:**

Do not delete the directory where the plug-in installation package **dhcp-plug-windows.zip** is decompressed because the DHCP plug-in will not be uninstalled completely.

# Installing LLDP plug-ins

If topology calculation fails for displaying connection to servers, install an LLDP plug-in.

An LLDP plug-in contains the following packages:

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

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

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

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

**IMPORTANT:**

Do not delete the folder where the decompressed installation packages are located after LLDP agent installation because DHCP plug-ins will not be uninstalled completely.

# 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 path.

   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 path.

   The LLDP Windows agent supports both LLDP and CDP. You can enable either of them, but not both. By default, the agent supports LLDP.

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

   a. Open the **lldpagent.conf** file in the **\Program Files\lldpAgent** directory on the Windows system disk.

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

   c. Delete the pound sign (#) from the string **#INTERVAL=300**, and then set the interval as needed.

      The default setting is 300 seconds.

   d. Save and close the file.
3. Restart the **lldp-agent** service.

# Accessing INC

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

# Hardware, software, and browser requirements

Table 12 lists the hardware, software, and browser requirements for accessing INC.

**Table 12 Requirements for accessing INC from a PC**

| OS | Hardware and software | Browser version | Browser setting requirements |
|---|---|---|---|
| Windows | • Recommended resolution: 1280 pixels in width.<br>• JRE 1.7.0_update76 or later is installed. | • IE 10 or 11.<br>• Firefox 50 or later.<br>• Chrome 44 or later. | • Turn off the popup blocker.<br>• Enable Cookies.<br>• Add INC as a trusted site. |

# Accessing INC from a PC

## Accessing INC

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

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

   The INC login page opens.
2. Enter the username and password, and then click **Login**.

   The default username for the INC super administrator is **admin**. The default password is **admin**. The default password is **Pwd@12345**.

**IMPORTANT:**

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

## Accessing the EIA self-service center

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

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

In the URL, *ip-address* is the IP address of the conductor server and *port* is the HTTP port number used by INC.

# Accessing INC from a mobile device

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

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

   The INC login page opens.
3. Enter the username and the password in the **Operator** and **Password** fields.

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

   The PC version of INC requires complex operations and provides all functions. The mobile version of INC allows you to perform the following operations:
   - View information about faulty devices and interfaces.
   - Query devices.
   - View device alarms.
   - Receive real-time alarms.
   - Test device reachability by using a **ping** or **tracert** command.
   - View custom views and device views.
5. Click **Login**.

# Securing INC

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

- Change the password of the INC superuser **admin** immediately after the first login.
- Tie the administrative accounts to a central AAA server via LDAP or RADIUS.
- Retain one administrative account (not named **admin**) with a local password to recover from loss of access to the AAA server.
- Enable the verification code feature on the INC login page. For more information, see *INC Getting Started Guide*.

# Displaying a user agreement

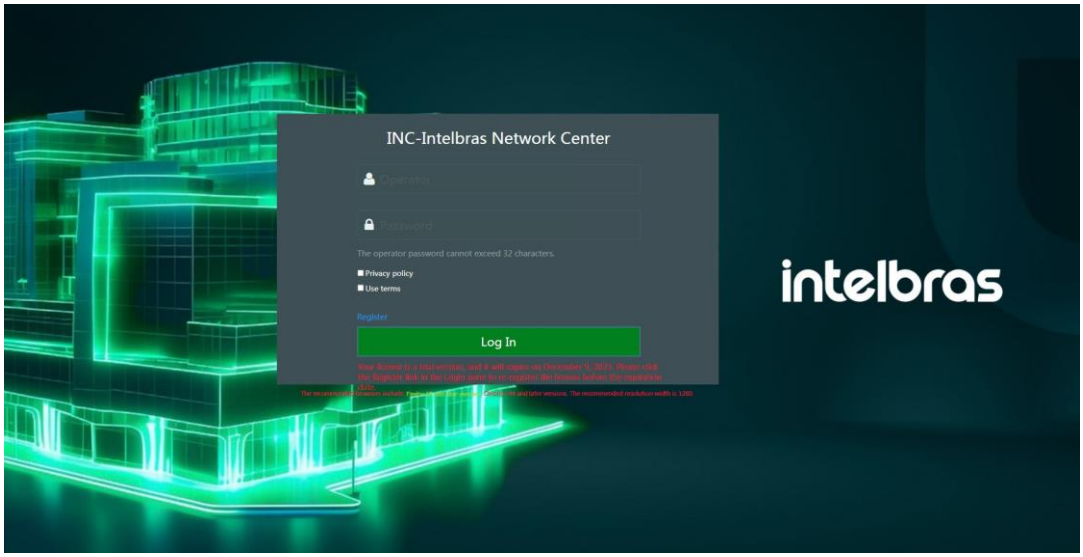
A user agreement on the INC login page informs operators of the rights and obligations for INC login. To log in to INC, operators must accept terms of the user agreement.

To display a user agreement on the INC login page:

1. On the conductor server, enter the **\client\conf** directory of the INC installation path.
2. Use Notepad to open the **commonCfg.properties** file.
3. Change the value of the **enableTerms** parameter to **true**.
4. Save and close the **commonCfg.properties** file.
5. Prepare a user agreement in HTML format named **terms.html**.
6. Save the **terms.html** file to the **\client\web\apps\imc** directory of the INC installation path on the conductor server.
7. Display the INC login page.

A **User agreement** link is displayed. Operators can click the link to view the terms of the user agreement.

**Figure 49 Viewing the user agreement on the login page**



# Upgrading INC

The following information describes how to upgrade INC components, using the INC platform as an example.

# Preparing for the upgrade

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

- Obtain the upgrade packages for the INC platform and all the deployed service components. After the INC platform upgrade, you must upgrade all the service components.
- Back up the INC installation directory and database files. If the upgrade fails, you can use the backup files to restore INC.

  To back up the INC installation directory and database files:

  **a.** Use **DBMan** in the Intelligent Deployment Monitoring Agent to back up the database files. For more information, see manual backup described in "Backing up and restoring the database."

  **b.** Stop all INC processes, and then manually copy the INC installation directory to a specific path.

# Upgrading INC

**CAUTION:**

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

You can use one of the following methods to upgrade components that are installed in the **tools\components** directory:

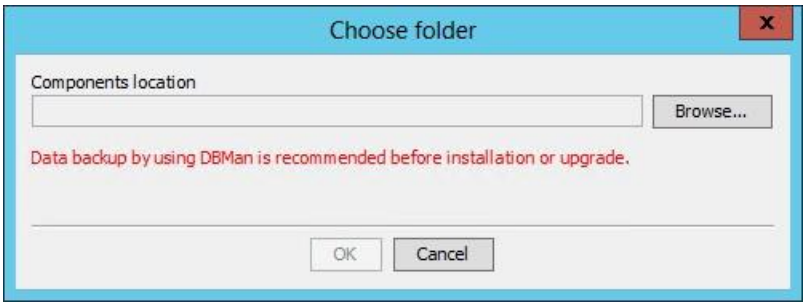
- Copy files of the following components from the **tools\components** directory to the INC installation directory **install\components**: ACL, EUPLAT, GAM, RestPlugin, VLAN, and WeChat. These components are upgraded when you upgrade the INC platform.
- Click **Install** in the **Monitor** tab of the Intelligent Deployment Monitoring Agent and select to upgrade components in the **tools\components** directory.

## Upgrading the INC platform

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

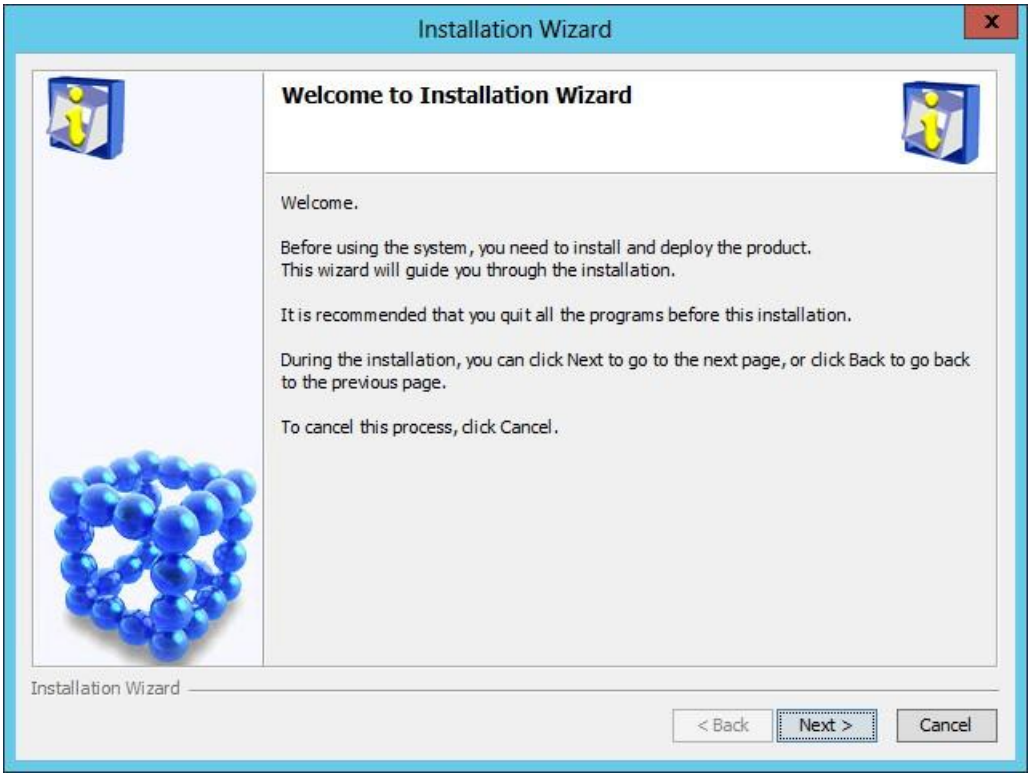
The **Choose folder** dialog box opens, as shown in Figure 50.

**Figure 50 Choose folder dialog box**



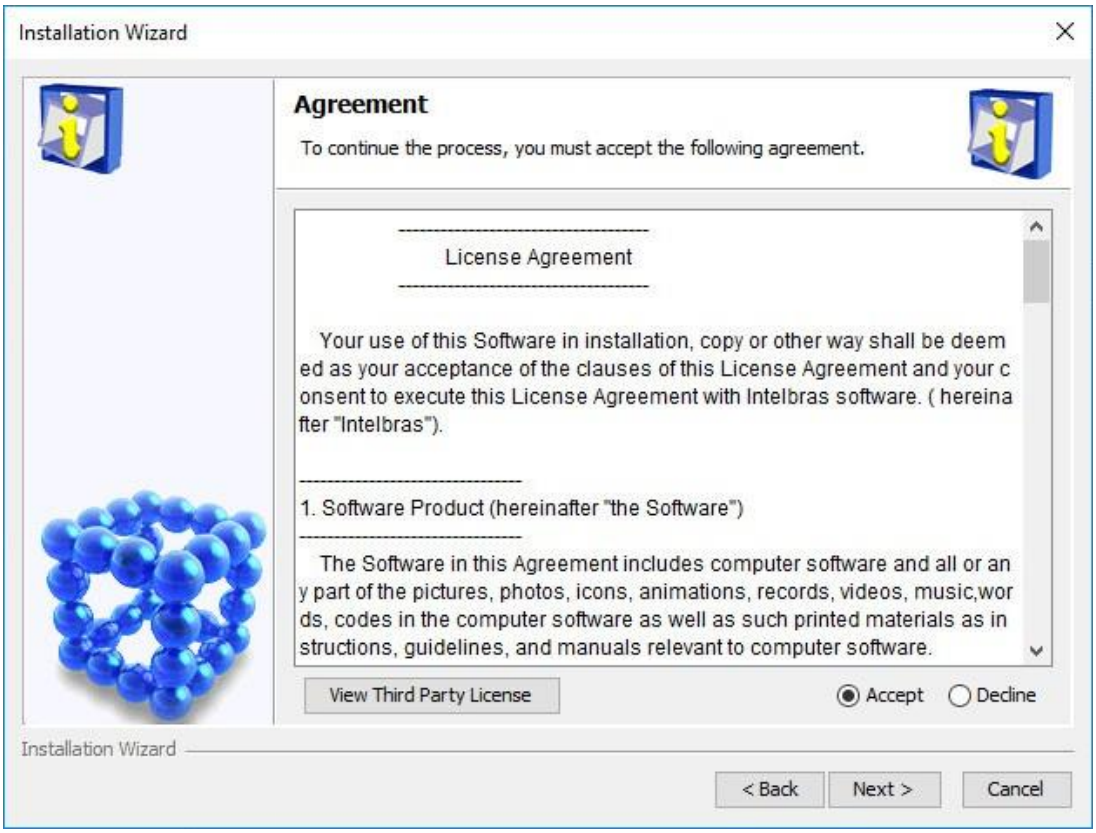

2. Click **Browse**, and then select the **\install\components** directory in the upgrade package.
3. Click **OK**.
   The INC installation wizard opens, as shown in Figure 51.

**Figure 51 INC installation wizard**




4. Click **Next**.
   The **Agreement** page opens, as shown in Figure 52.

**Figure 52 Agreement page**



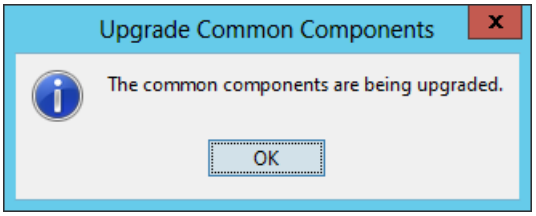

5. Read the license agreement, select **Accept**, and then click **Next**.

   The **Upgrade Common Components** dialog box opens, as shown in Figure 53.

**NOTE:**

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

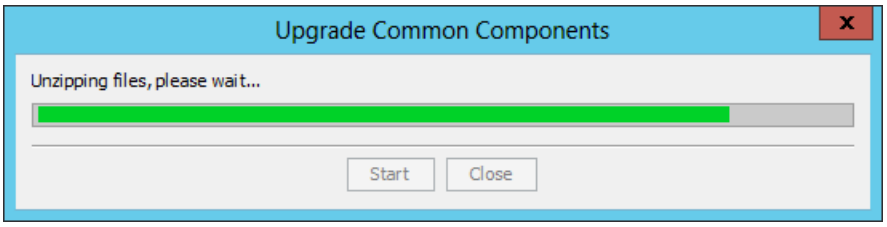
**Figure 53 Upgrade Common Components dialog box**




6. Click **OK**.

   The system automatically upgrades common components and displays the upgrade progress, as shown in Figure 54.

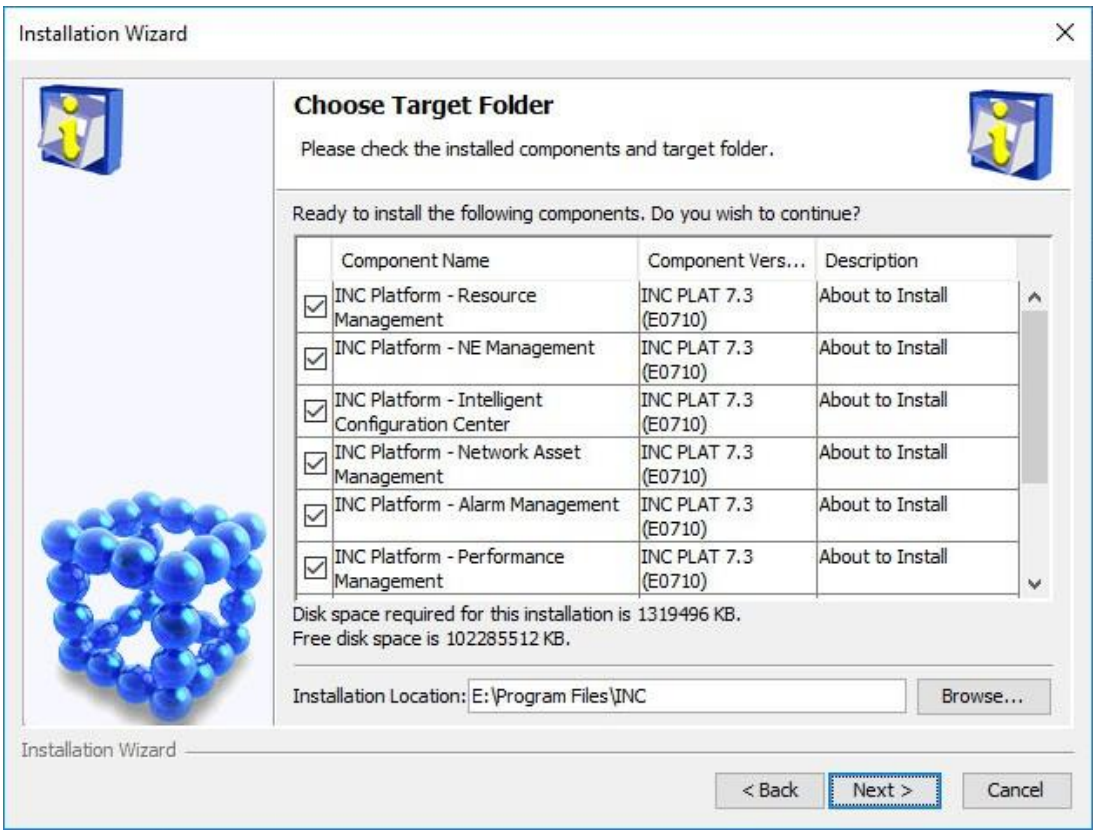
**Figure 54 Upgrading common components**




After the common components are upgraded, the **Choose Target Folder** page opens, as shown in Figure 55.

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

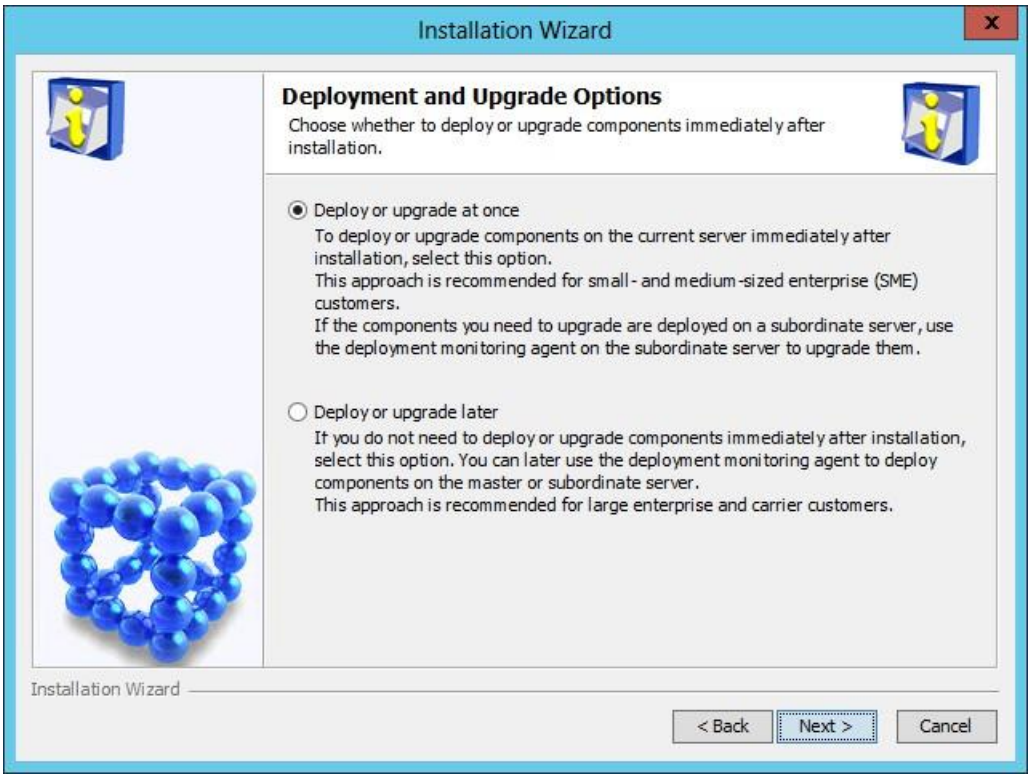
**Figure 55 Choose Target Folder page**




7. Verify the information, and then click **Next**.

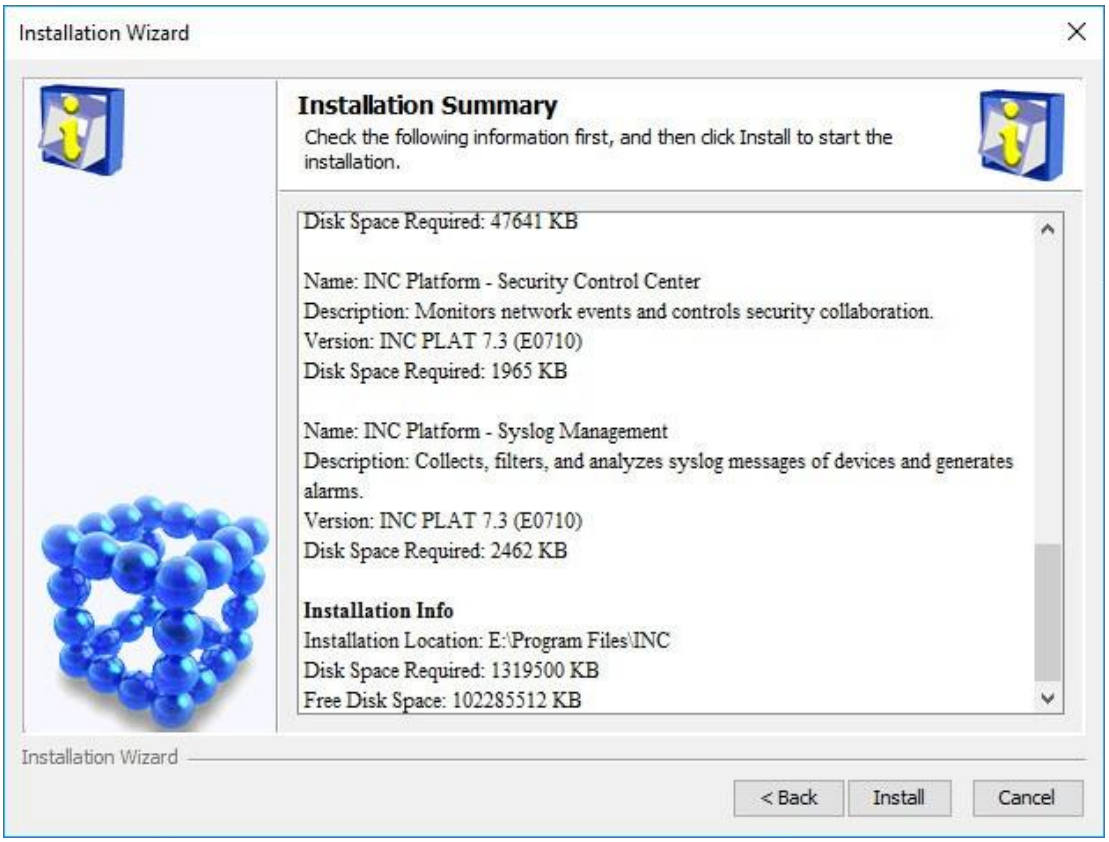
   The **Deployment and Upgrade Options** page opens, as shown in Figure 56.

**Figure 56 Deployment and Upgrade Options page**




8. Select **Deploy or upgrade at once**, and then click **Next**.
   The **Installation Summary** page opens, as shown in Figure 57.

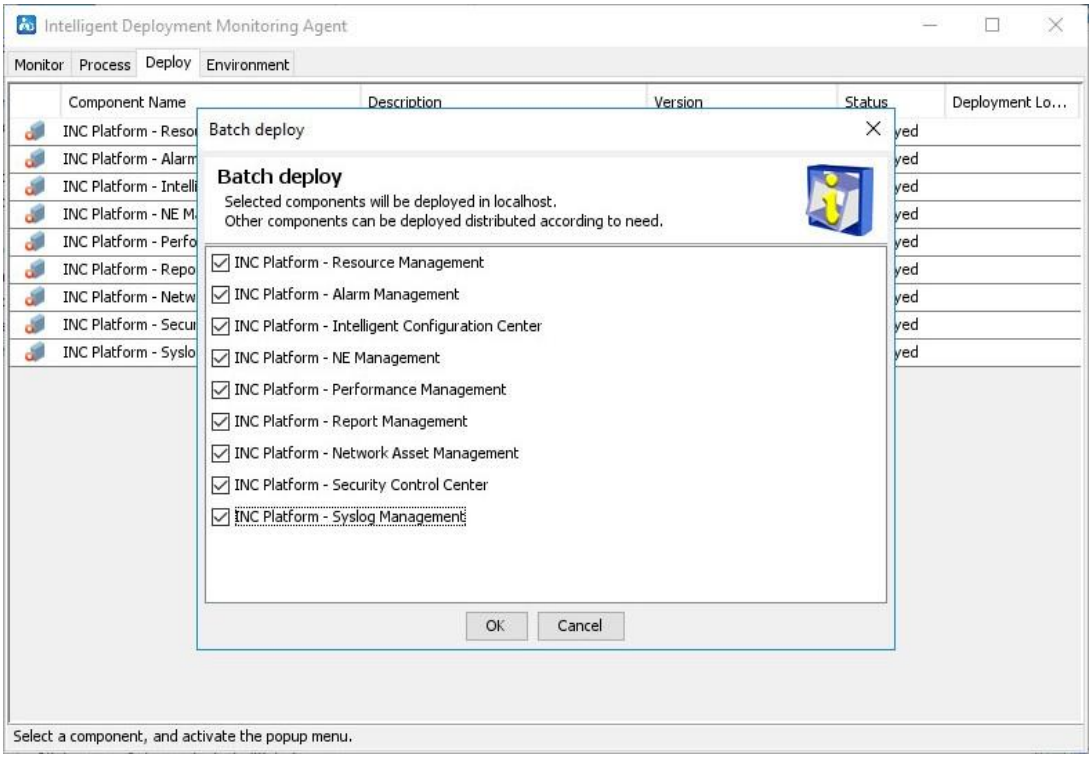
**Figure 57 Installation Summary page**




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

After the installation is complete, the **Batch upgrade** dialog box opens, as shown in Figure 58.

**Figure 58 Batch upgrade dialog box**



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

    After the upgrade is complete, the **Batch upgrade result** dialog box shown in Figure 59 or Figure 60 opens. The dialog box content varies depending on whether auto backup and restoration settings have been configured in DBMan before the upgrade.

**Figure 59 Batch upgrade result without auto backup and restoration**

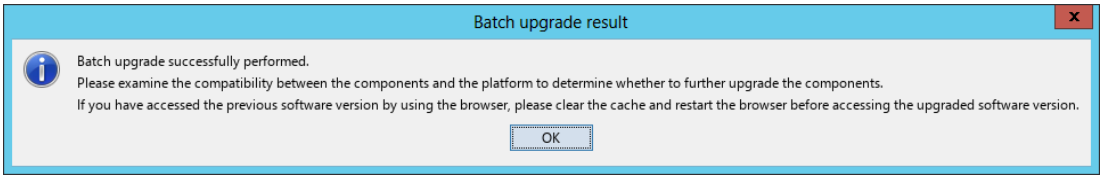
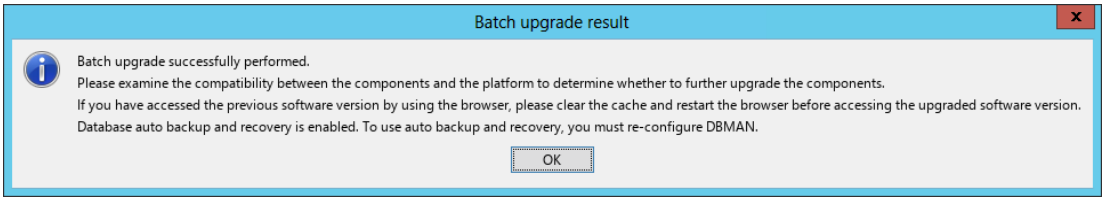


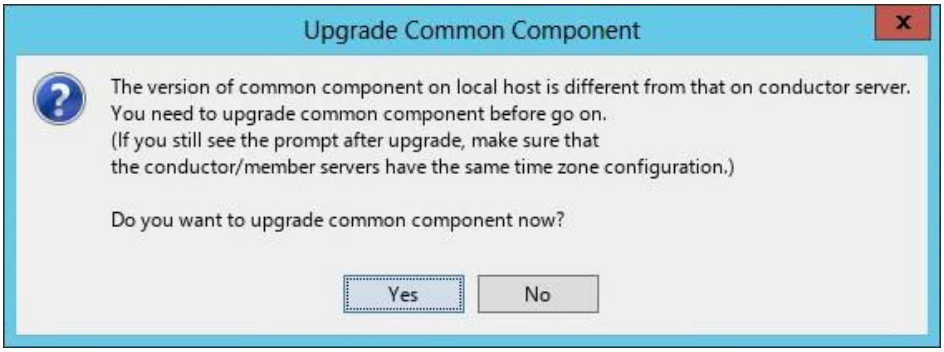

**Figure 60 Batch upgrade result with auto backup and restoration**




11. Click **OK**.
12. If the **Auto Backup and Restore Settings** dialog box opens, configure the auto backup and restoration settings and click **OK**.

    After the components on the conductor server are upgraded, the member server detects that the component version is different from the component version on the conductor server. The **Upgrade Common Component** page is displayed on the member server, as shown in Figure 61.

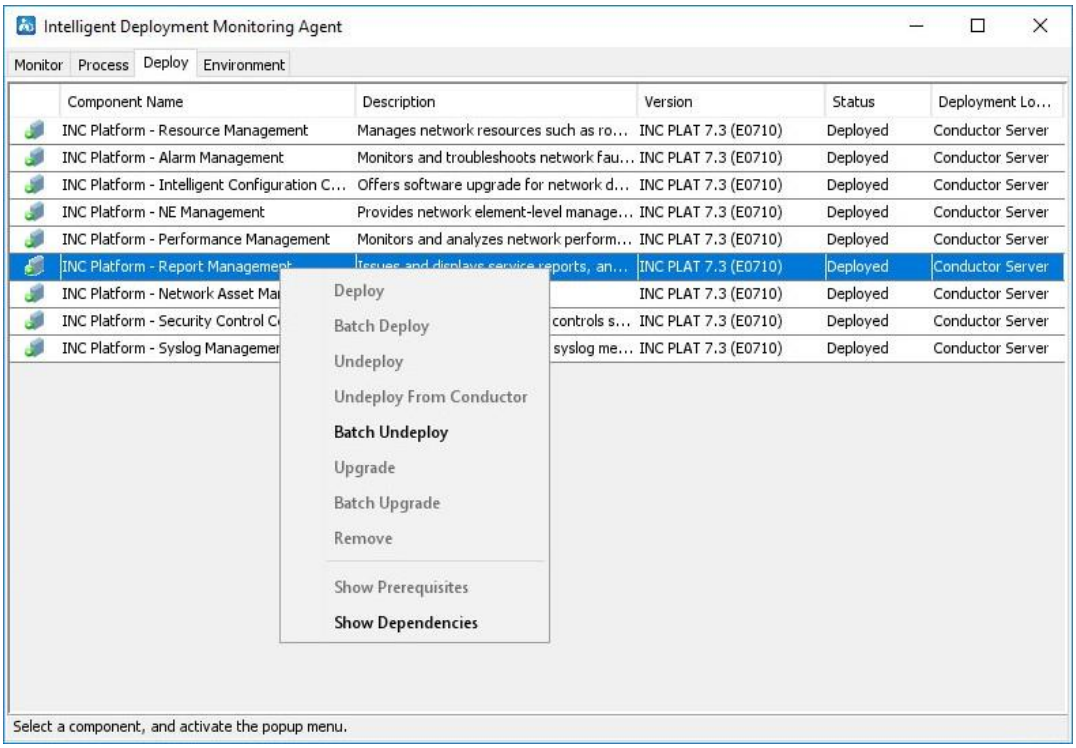
**Figure 61 Upgrade Common Component page**




13. Click **Yes**.

    The system downloads files.
14. On the **Deploy** tab of the Intelligent Deployment Monitoring Agent, right-click a component, and then select **Batch Upgrade**.

**Figure 62 Selecting batch upgrade**




15. Select components to be upgraded, and then click **OK**.

    The system upgrades the components. After the upgrade is complete, the upgrade result page opens.
16. Click **OK**.
17. On the conductor server, click **Start** on the **Monitor** tab of the Intelligent Deployment Monitoring Agent to start INC.

# Restoring INC

If the INC upgrade still fails, restore INC to the version before the upgrade:

1. Restore the INC database. For more information, see manual restoration described in "Backing up and restoring the database."
2. After the restoration is complete, stop INC in the Intelligent Deployment Monitoring Agent.
3. Close the Intelligent Deployment Monitoring Agent.
4. Stop the Intelligent Management Server service in the server manager.
5. In the INC installation directory, back up log files necessary for upgrade failure analysis, and then delete all the files in the directory.
6. Copy the backup INC installation directory to the INC installation path.
7. Start the Intelligent Management Server service in the server manager.
8. Start INC in the Intelligent Deployment Monitoring Agent.

For INC running in stateful failover mode, restore INC only on the active server in the failover system.

# Uninstalling INC

The following information describes how to uninstall INC on Windows Server 2012 R2.

To reinstall INC, complete the following tasks before reinstallation:

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

## Uninstalling an INC component

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

To uninstall an INC component:

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

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

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

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

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

## Uninstalling all INC components at one time

First uninstall the components deployed on member servers, and then uninstall the components deployed on the conductor server.

### Uninstalling the INC components from each member server

1. Open the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop**.
3. On Windows, click **Start**, access the all applications page, and then select **INC** > **Deployment Monitoring Agent**.

   An uninstall wizard opens.
4. Click **Uninstall**.
5. Click **Yes** in the confirmation dialog boxes that open.

   The Intelligent Deployment Monitoring Agent uninstalls all components. After the uninstallation is complete, the **Uninstallation Completed** dialog box opens.

6. Clear the OS reboot option, and then click **OK**.
7. Delete the **INC-Reserved** folder in the **WINDOWS** folder.
8. Reboot the operating system.

# Uninstalling the INC components from the conductor server

1. Start the Intelligent Deployment Monitoring Agent.
2. On the **Monitor** tab, click **Stop**.
3. On Windows, click **Start**, access the all applications page, and then select **INC** > **Uninstall**.

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

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

   The Intelligent Deployment Monitoring Agent uninstalls all components. After the uninstallation is complete, the **Uninstallation Completed** dialog box opens.
6. Clear the OS reboot option, and then click **OK**.
7. Delete the **INC-Reserved** folder in the **WINDOWS** folder.
8. Reboot the operating system.

# Registering INC

An unregistered INC version provides the same functions as those of a registered version, but it can be used for only 45 days since the date the service was first started. Register INC to unlock the time limitation.

For more information about requesting and installing the INC licenses, see *Intelbras INCcensing Guide*.

# Security settings

## Port settings

As a best practice, use a firewall to protect the INC server cluster by filtering the non-service data sent to the cluster. If the firewall is installed on the conductor server or member servers, open the IP addresses of the member servers or the conductor server in the firewall to ensure correct communication between them.

**NOTE:**

- As a best practice to avoid legitimate packet fragments being filtered, do not use ACLs on switches to filter data packets destined for the INC server cluster.
- NTA/UBA typically uses probes for log collection. When a firewall is deployed between the probes and INC, configure ACLs on the firewall to allow IP packets sent by the probes to INC.

Make sure the ports used by the INC components (listed in Table 13 and Table 14) are not blocked by the firewall.

**Table 13 Port numbers used by the INC platform**

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

**Table 14 Port numbers used by the INC NTA/UBA**

| Default port number | Usage | Location |
|---|---|---|
| UDP 9020, 9021, 6343 | Port for the INC server to receive logs | INC server |
| TCP 8051 | Listening port used to monitor the command for stopping the NTA/UBA service | INC server |
| TCP 9099 | JMX listening port for the NTA/UBA service | INC server |
| UDP 18801, 18802, 18803 | Communication ports between the NTA and UBA | INC server |

# Backing up and restoring the database

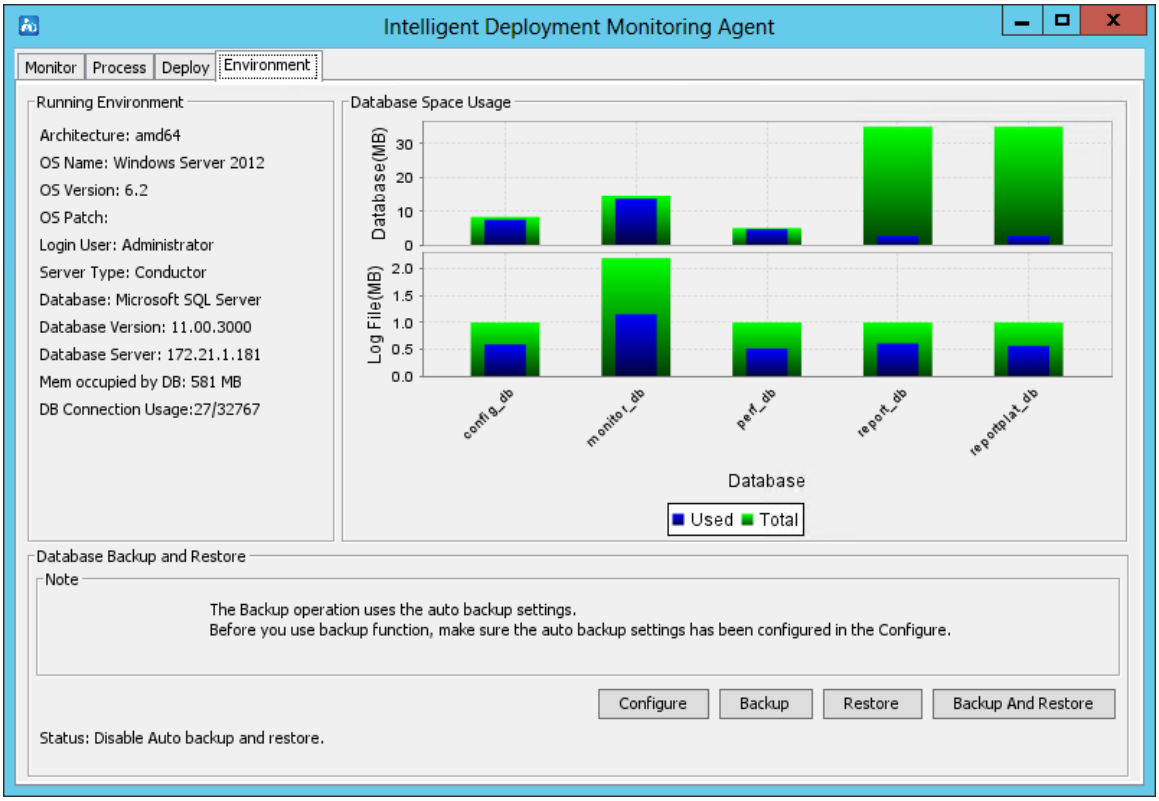
**IMPORTANT:**

In distributed deployment, DBMan is available only on the conductor server.

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

DBMan supports both manual and automatic database backup and restoration. It is integrated in the **Environment** tab of the Intelligent Deployment Monitoring Agent, as shown in Figure 63.

**Figure 63 Environment tab**




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

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

- **Backup And Restore**—Immediately backs up the database on the primary server to the backup server and performs automatic restoration. This option is applicable to stateless failover scenarios.

# Configuration restrictions and guidelines

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

- To ensure correct operation, do not back up and restore INC databases between different operating systems.
- In automatic backup configuration, use the **Upload to Backup System** option to back up database files to a backup INC system or an FTP server.
- The **Upload to Backup System** option requires one of the following conditions:
  - The **Conductor Server IP of Backup System** is specified for database backup.
  - An FTP server is configured in the **dbman_ftp.conf** file in the **\dbman\etc** directory of the INC installation path. For example:

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

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

  ```
  BeforeSQLScript_monitor_db_IMC_monitor = D:\1.bat
  AfterSQLScript_monitor_db_IMC_monitor = D:\2.bat
  ```
- After Oracle database restoration is complete, make sure the tablespace name is the same as that before restoration.

# Installing DBMan on the database server

By default, DBMan is not installed on the remote database server. Before database backup and restoration, install DBMan on the database server.

DBMan can be installed automatically when you install the Intelligent Deployment Monitoring Agent.

To start the remote installation wizard for installing the Intelligent Deployment Monitoring Agent, see "Starting the remote installation wizard."

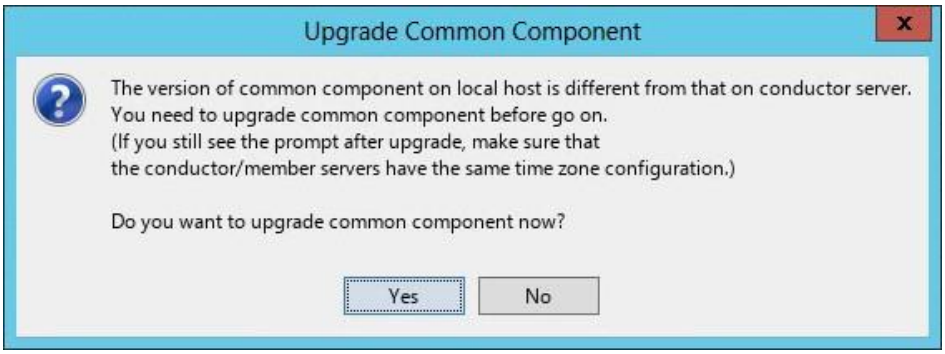
To install the Intelligent Deployment Monitoring Agent after the wizard has been started, see "Installing the Intelligent Deployment Monitoring Agent."

After installation, DBMan will be started when you start the server.

# Upgrading DBMan

When you upgrade INC, the **Upgrade Common Component** dialog box opens, as shown in Figure 64. Click **Yes** to upgrade common components including DBMan.

**Figure 64 Upgrade Common Component**




# Backing up and restoring databases for a single INC system

## Backing up databases

A single INC system supports both manual and automatic backup:

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

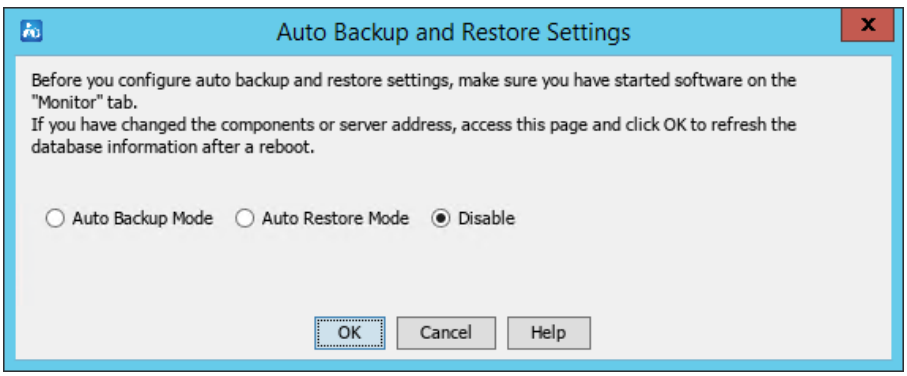
### Manual backup

1. On the **Environment** tab, click **Backup**.
   A confirmation dialog box opens.
2. Click **Yes**.
   The **Select database backup path** dialog box opens.
3. Specify a local path to save the backed up data files.
   Make sure the specified path has enough space.
4. Click **OK**.

### Automatic backup

1. On the **Environment** tab, click **Configure**.
2. In the confirmation dialog box that opens, click **OK**.
   The **Auto Backup and Restore Settings** dialog box opens, as shown in Figure 65.

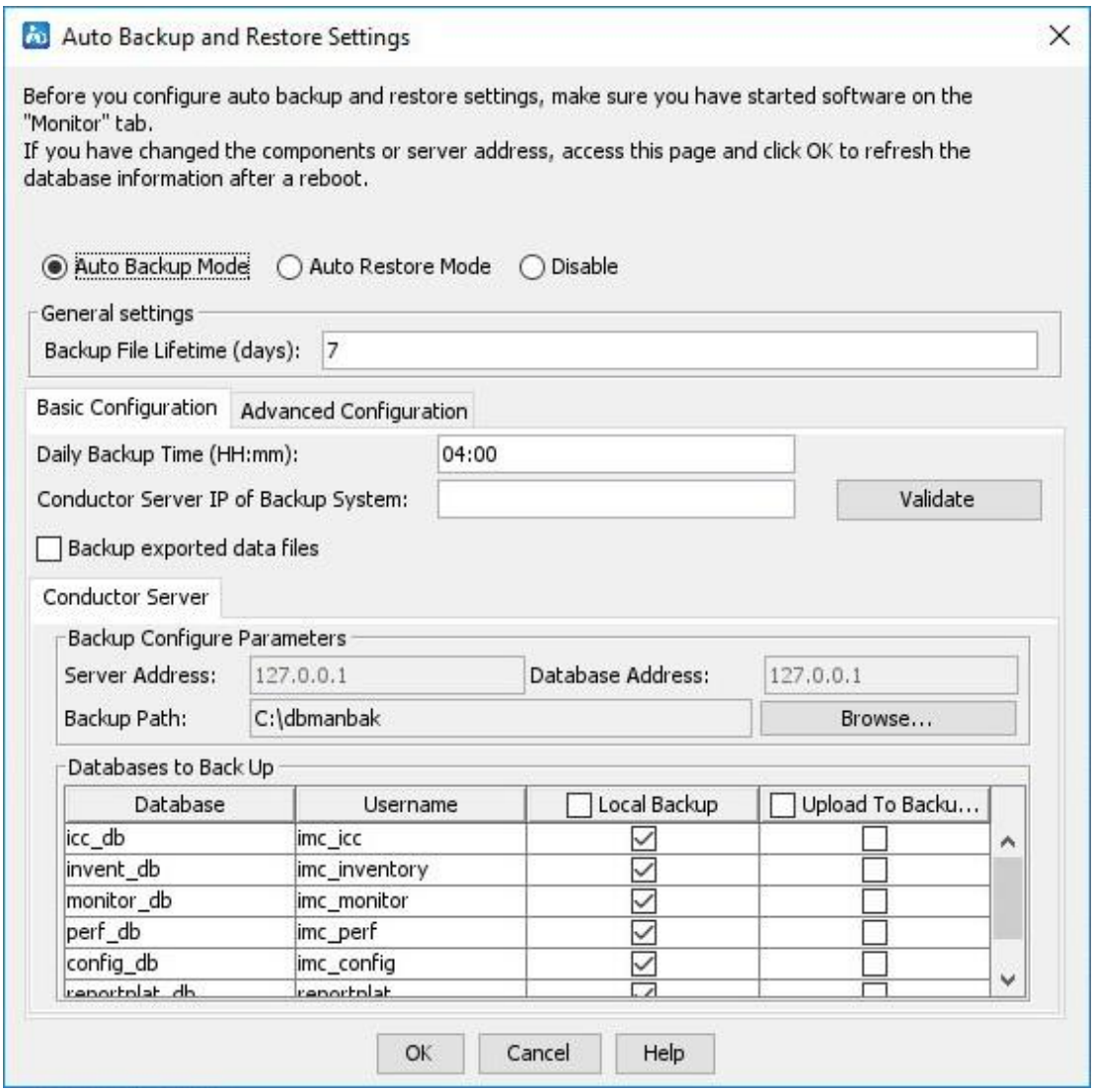
   **Figure 65 Auto Backup and Restore Settings**



3. Read information in the **Auto Backup and Restore Settings** dialog box, select **Auto Backup Mode**, and click **OK**.

   The page for configuring auto backup settings opens, as shown in Figure 66.

   **Figure 66 Configuring auto backup settings**




4. In the **General settings** area, configure the **Backup File Lifetime (days)** parameter:
   - **Backup File Lifetime (days)**—Enter how many days a backup file can be kept. Expired files are automatically deleted. By **default**, the backup file lifetime is 7 days.
5. On the **Basic Configuration** tab, and then configure the following parameters:
   - **Daily backup time (HH:mm)**—Enter the time at which the automatic backup operation starts every day. By default, the daily backup time is 04:00.
   - **Conductor Server IP of Backup System**—This parameter is applicable to database backup in stateless failover scenarios. To upload the database files to the conductor server of backup system, specify the conductor server IP address in this field. Make sure automatic restoration is enabled for the backup system. To verify the component and version consistency between the primary INC system and the backup INC system, click **Validate**.
   - **Backup exported data files**—Select this parameter to back up exported data files.
6. Click the **Conductor Server** tab and configure the following parameters:

- **Backup Path**—Enter or browse to the path where the backup database files are stored.
- **Database Backup Path**—Specify the path where the backup database files are stored on the database server.
- **Local Backup**—Select the databases to back up locally on the conductor server. By default, all databases are selected.
- **Upload To Backup System**—Select the databases to upload to an FTP server or the conductor server of a backup system. By default, no database is selected. When you select **Upload To Backup System** for a database, the **Local Backup** option is forcibly selected for the database. To configure the FTP server, see "Configuration restrictions and guidelines."

7. Click each **Member Server** tab and configure the following parameters:

**TIP:**

In distributed deployment, each member INC server has a separate **Member Server** tab in DBMan.

- **Backup Path**—Enter or browse to the path where the backup INC files are stored.
- **Database Backup Path**—Enter or browse to the path where the backup database files are stored.
- **Local Backup**—Select the databases to back up locally on the member server. By default, all databases are selected.
- **Upload To Backup System**—Select the databases to upload to an FTP server or the conductor server of a backup system. By default, no database is selected. When you select **Upload To Backup System** for a database, the **Local Back Up** option is forcibly selected for the database. To configure the FTP server, see "Configuration restrictions and guidelines."

8. Click the **Advanced Configuration** tab and configure the following parameters:
   - **Delete local files after upload even if upload fails**—Specify whether to delete local backup files after they are uploaded.
   - **Transfer backup files of Member Servers to the conductor server**—Specify whether to upload local backup files from member servers to the conductor server.
9. Click **OK**.

# Restoring databases

A single INC system supports only manual restoration of the databases.

Manual restoration immediately replaces all database files with the backup database files. It supports the following types:

- **Locally Restore**—Applicable to scenarios where all backup files are saved on the conductor server.
- **Remotely Restore**—Applicable to scenarios where backup files are saved on the conductor and member servers.

As a best practice, restore database files for the INC platform and service components together. If you restore only some of the database files, data loss or inconsistency might occur.

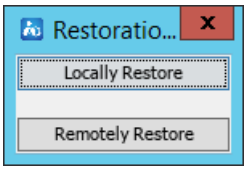
Make sure INC has been started at least once after installation before you restore the INC databases.

To perform a manual restoration:

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

   The **Restoration Type** dialog box opens, as shown in Figure 67.

**Figure 67 Restoration Type dialog box**



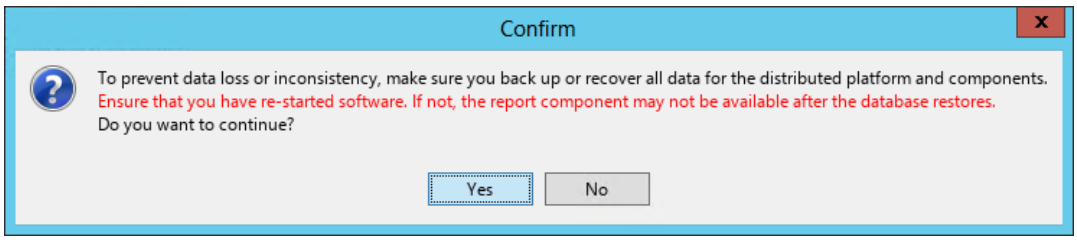

2. Perform one of the following operations:

   If all backup files are saved on the conductor server:

   a. Click **Locally Restore**.

      The **Confirm** dialog box opens, as shown in Figure 68.

      **Figure 68 Confirming the operation**

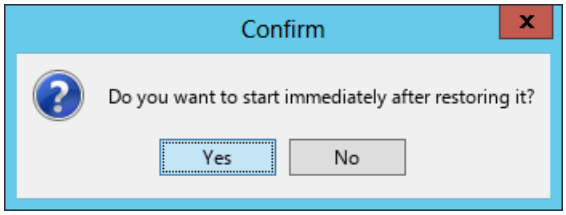
   a. Click **Yes**.

      The **Select the data file to be restored** dialog box opens.

   b. Select database files to be restored, and then click **OK**.

      A confirmation dialog box opens.

      **Figure 69 Confirmation dialog box**

   c. Click **Yes**.

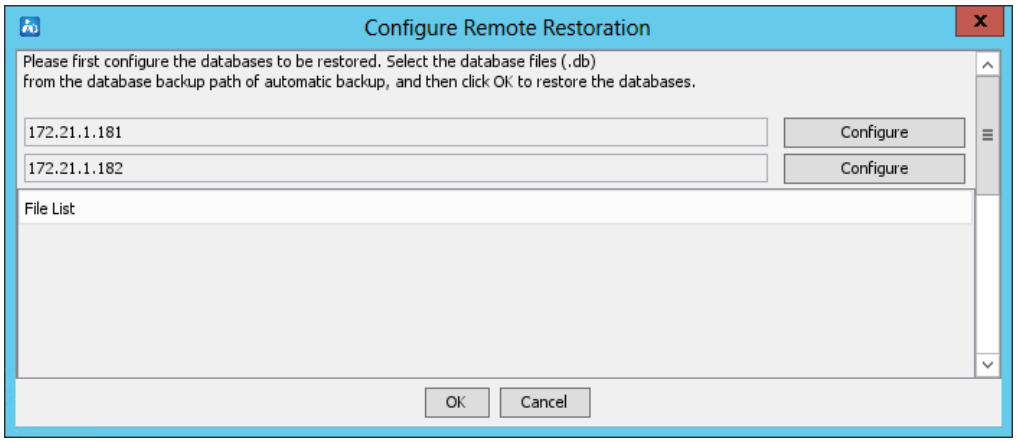
      The system starts restoring the database files.

   If backup files are saved on the conductor and member servers:

   a. Click **Remotely Restore**.

      The **Configure Remote Restoration** dialog box opens.

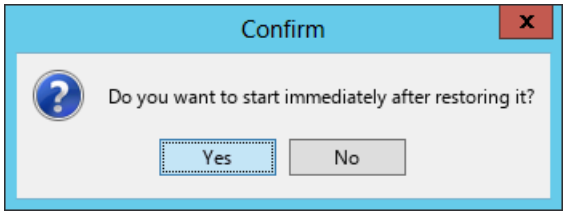
**Figure 70 Configure Remote Restoration dialog box**




**b.** Click **Configure** to select the database files to be restored on the conductor and member servers, and then click **OK**.

A confirmation dialog box opens.

**Figure 71 Confirmation dialog box**




**c.** Click **Yes**.

The system starts restoring the database files.

After the local or remote restoration is complete, the system displays a restoration success message.

**3.** Click **OK**.

The INC service will be automatically started.

**NOTE:**

- Before remote restoration, you must configure automatic backup and restoration parameters. Then DBMan can automatically locate running configuration files and database files.
- During the restoration process, DBMan shuts down and restarts INC and the database service.

# Backing up and restoring databases in stateless failover scenarios

A typical stateless failover scenario includes a primary INC system and a backup INC system:

- The primary INC system is deployed in distributed mode and uses a remote database.
- The backup INC system is deployed in centralized or distributed mode.

For stateless failover, configure automatic backup on the primary server and configure automatic restoration on the backup server. During automatic backup and restoration, DBMan on the primary server performs the following operations:

**1.** Periodically or immediately backs up database files.

2. Uploads the backed up database files to the backup server.
3. Instructs the backup server to restore the received database files.

**NOTE:**

In a stateless failover scenario, you can perform any of the operations in the **Auto Backup and Restore Settings** dialog box to back up data:

- Clear the option **Delete local files after upload even if upload fails** in the automatic backup configuration on the primary server.
- Set a path in **Backup Files Location** fields in the automatic restoration configuration on the backup server.

# Backing up databases

In a stateless failover scenario, you can configure automatic backup on the primary server.

Before the configuration, make sure the following settings are the same on the primary server and the backup server:

- OS
- Database type and version
- INC version and patches

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

# Restoring databases

In a stateless failover scenario, you can configure automatic restoration on the backup server. After receiving the backed up database files from the primary server, the backup server automatically restores the database files locally.

This example describes the automatic restoration settings for a failover INC system that is deployed in distributed mode and uses a remote database.

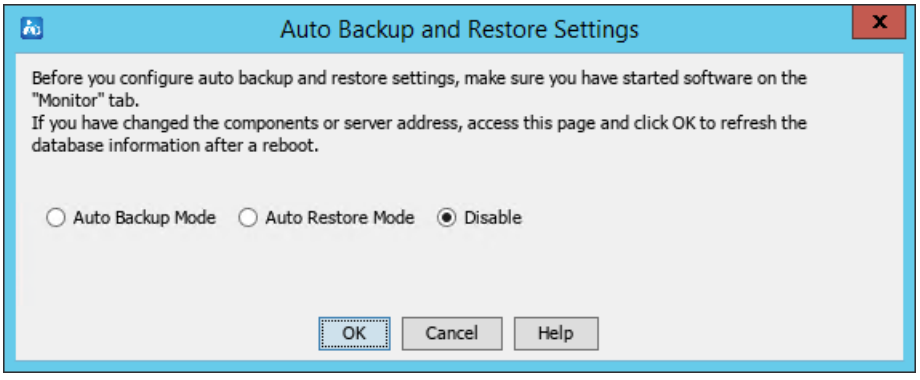
To configure automatic restoration:

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

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

   The **Auto Backup and Restore Settings** dialog box opens, as shown in Figure 72.

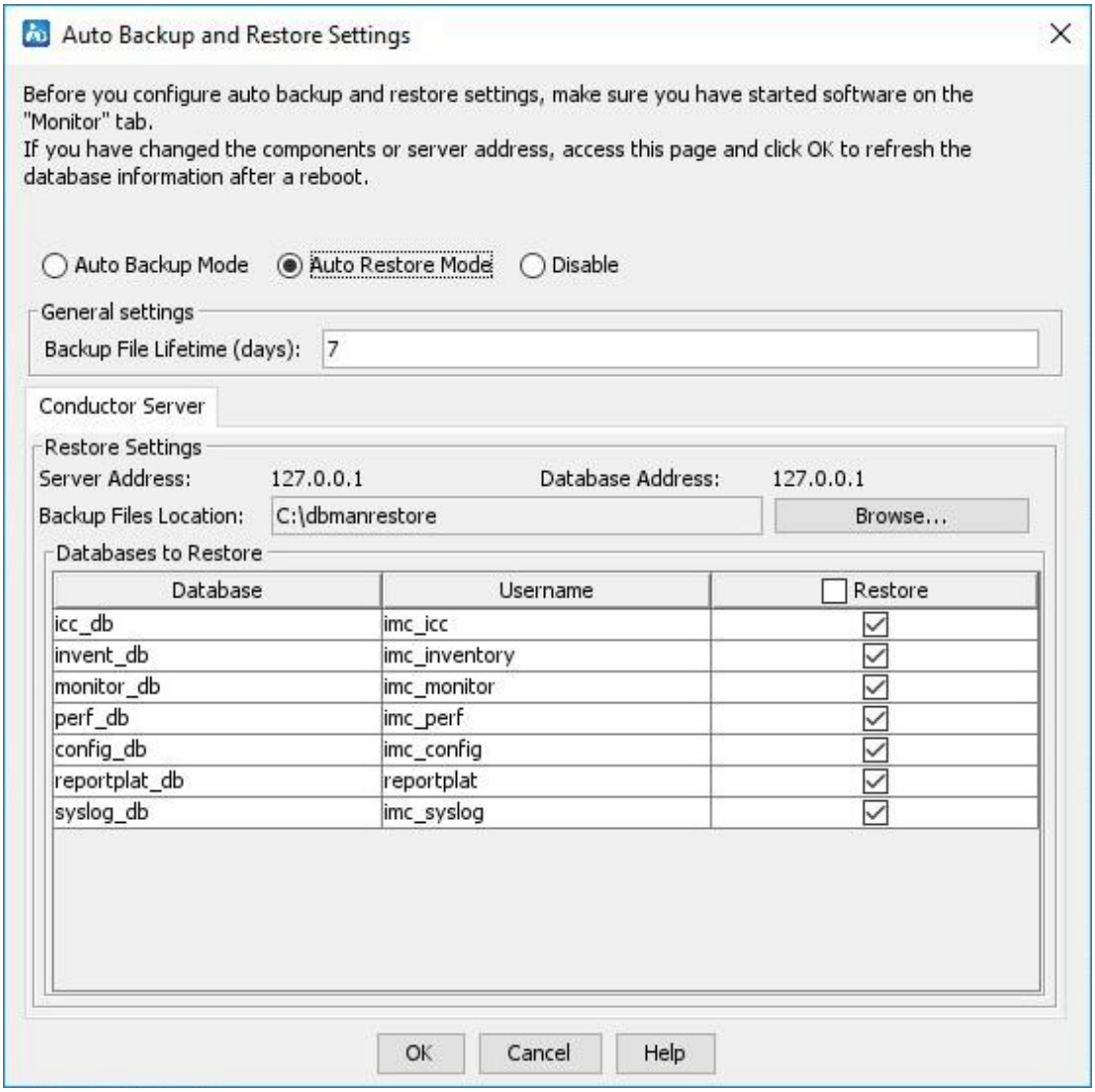
   **Figure 72 Auto Backup and Restore Settings dialog box**




3. Read information in the **Auto Backup and Restore Settings** dialog box, select **Auto Restore Mode**, and then click **OK**.

The page for configuring automatic restoration settings opens, as shown in Figure 73.

**Figure 73 Configuring auto restoration settings**




4. Click the **Conductor Server** tab and configure the following parameters:
   - **Backup Files Location**—Enter or browse to the path where the uploaded backup INC files are stored on the conductor server.
   - **Backup Files Location of Database**—Enter or browse to the path where the uploaded backup database files are stored on the conductor server.
   - **Restore**—Select databases to restore. By default, all databases are selected.
5. Click each **Member Server** tab and configure the following parameters:
   - **Backup Files Location**—Enter or browse to the path where the uploaded backup INC files are stored on a member server.
   - **Backup Files Location of Database**—Enter or browse to the path where the uploaded backup database files are stored on a member server.
   - **Restore**—Select databases to restore. By default, all databases are selected.
6. Click **OK**.

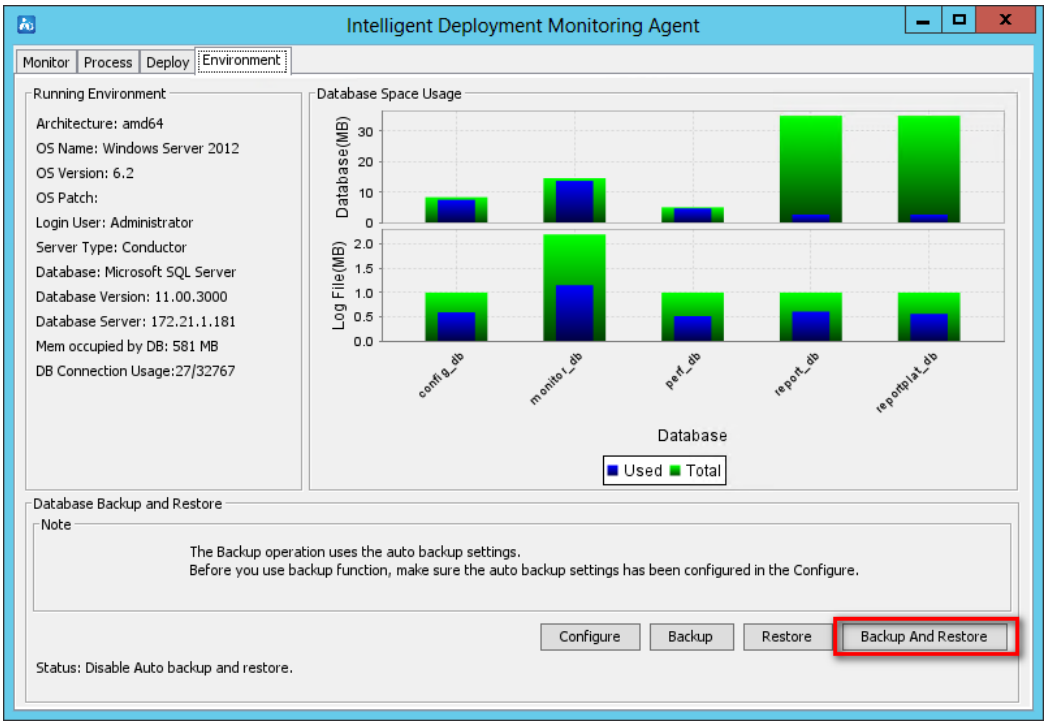
# Backing up and restoring databases

In a stateless failover scenario, use this option to back up the database on the primary server to the backup server and configure automatic restoration on the backup server.

To configure backup and restoration:

1. Configure automatic backup on the primary server in the same way you configure database backup in a single INC system. For more information, see "Automatic backup."
2. Configure automatic restoration on the backup server. For more information, see "Restoring databases."
3. Click **Backup and Restore** on the **Environment** tab in the Intelligent Deployment Monitoring Agent, as shown in Figure 74.

**Figure 74 Configuring backup and restoration**



# FAQ

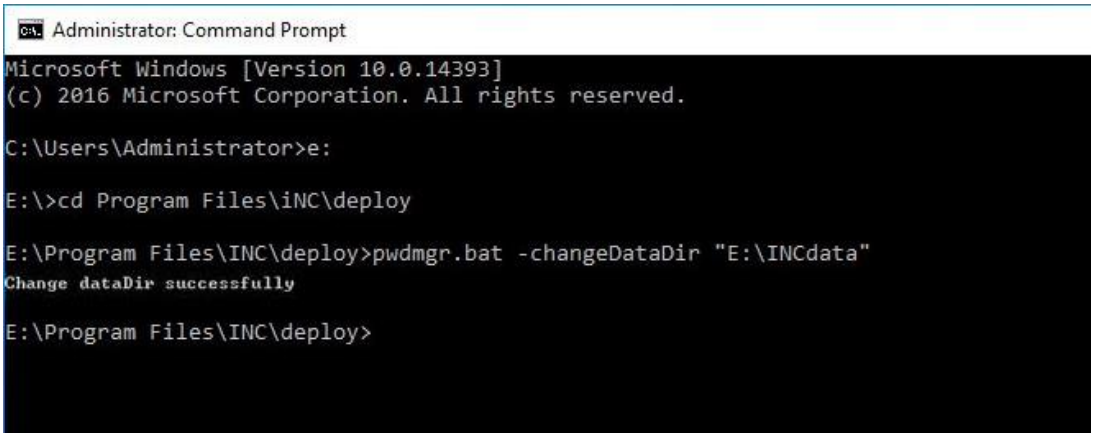
### After INC installation is complete, how do I change the database file storage path?

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

   ```
   pwdmgr.bat –changeDataDir "E:\INCdata"
   ```

   Figure 75 shows that the storage path has been successfully modified.

   **Figure 75 Modifying the database file storage path**

4. Start the INC service.

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

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

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

2. Redeploy the component that failed to be deployed.

### On Windows, INC service processes cannot be started or stopped after INC runs for a period of time. How can I resolve this issue?

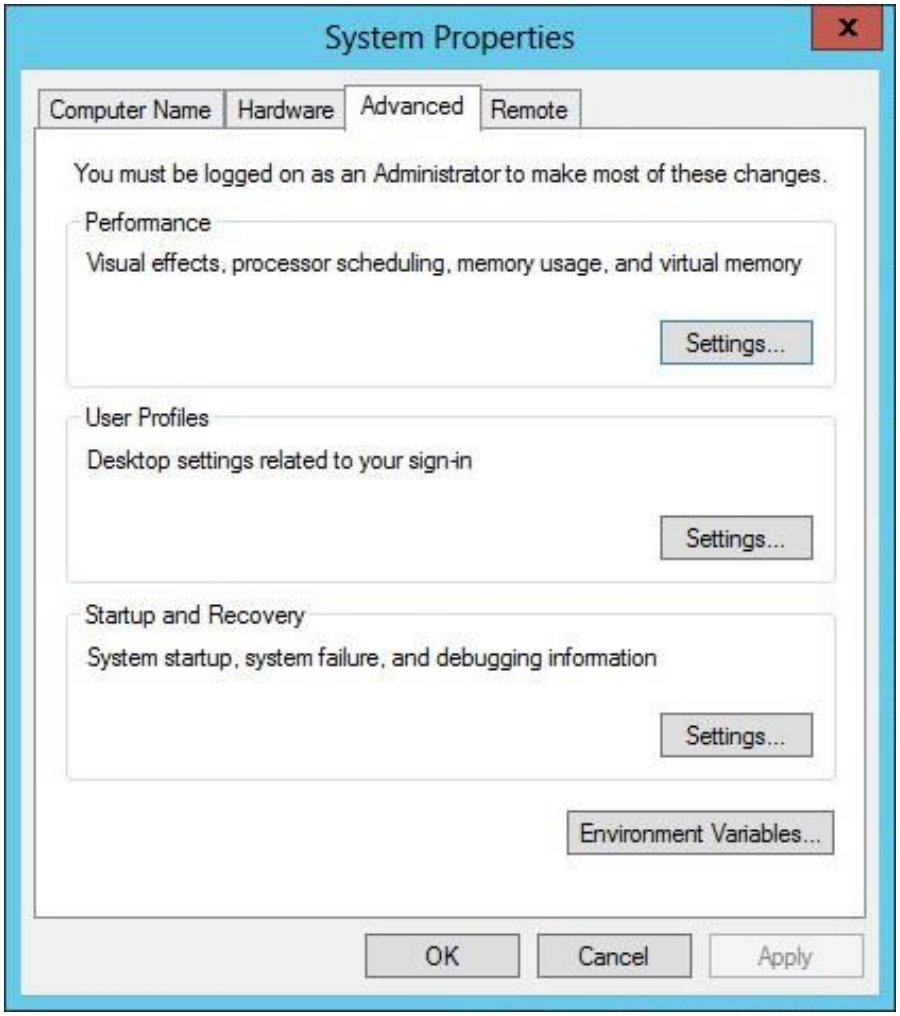
This issue is caused by insufficient virtual memory.

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

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

   The **System Properties** dialog box opens, as shown in Figure 76.

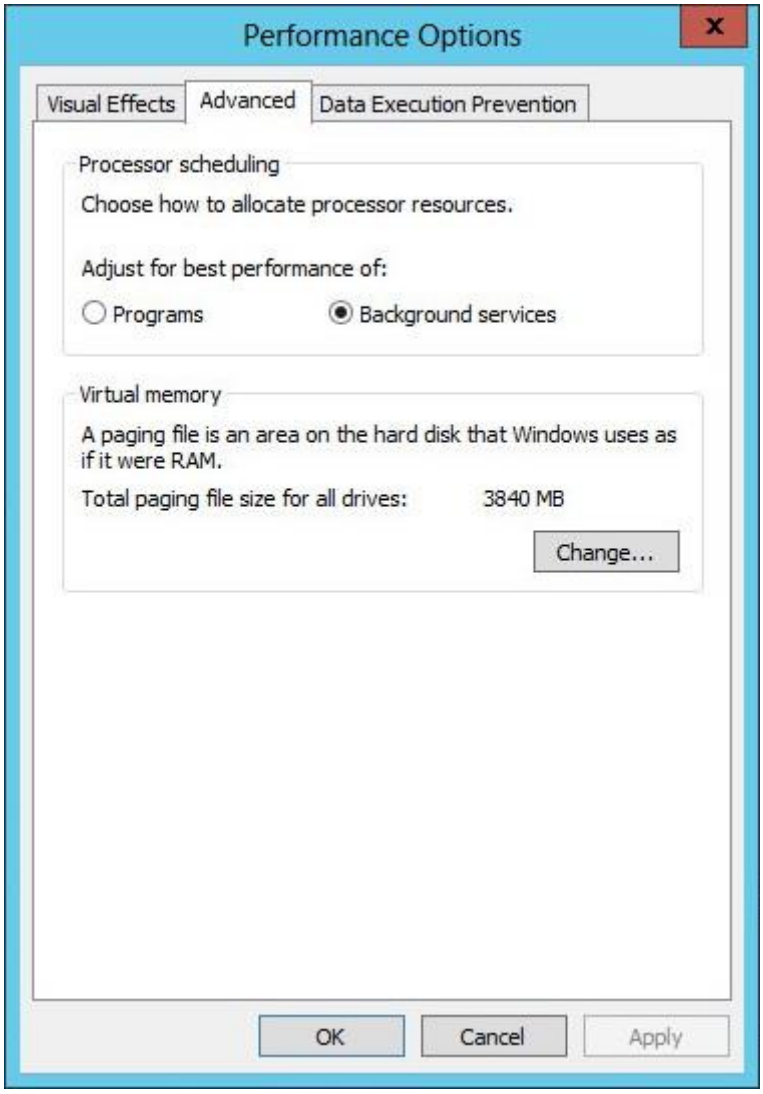
**Figure 76 System Properties dialog box**




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

   The **Performance Options** dialog box opens, as shown in Figure 77.

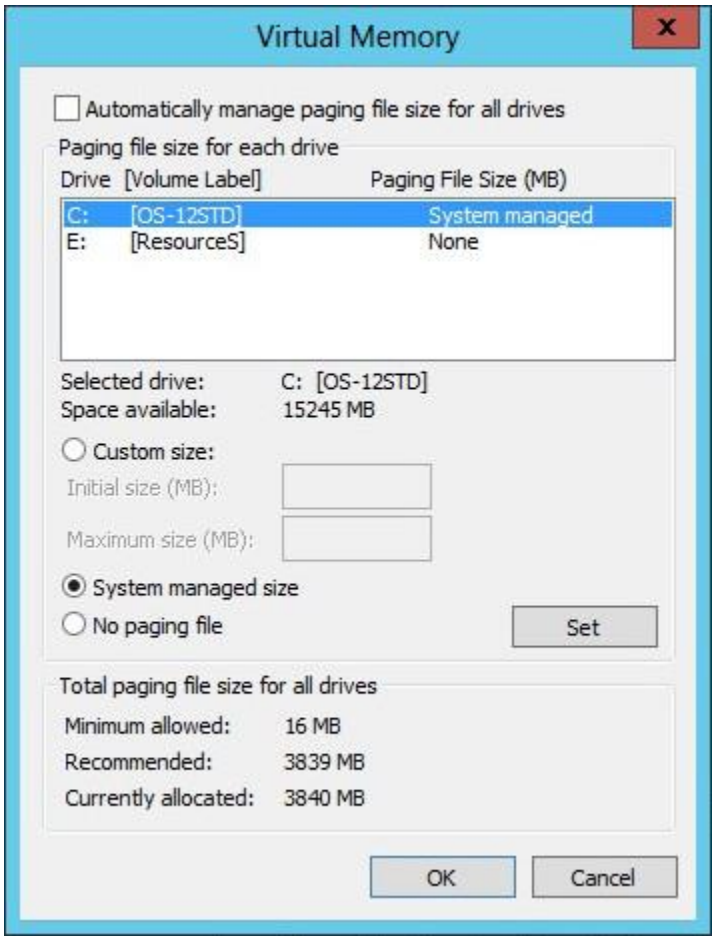
**Figure 77 Performance Options dialog box**




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

   The **Virtual Memory** dialog box opens, as shown in Figure 78.

**Figure 78 Virtual Memory dialog box**




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

## License verification fails after the Windows operating system reboots. How can I resolve this issue?

The license file contains only one MAC address if the license is requested after NIC teaming. After the operating system reboots, license verification fails because the MAC address of the NIC team has changed.

To resolve this issue, assign a static MAC address to the NIC team, as shown in Figure 79.

**Figure 79 Assigning a static MAC address to the NIC team**