IMC

iNode Intelligent Client v7.2 (E0407)

Table of Contents

What's New in this Release

The following lists all features released after iNode PC 7.0 (E0101). iNode PC 7.2 (E0407) can be upgraded from any previous versions.

Features released in iNode PC 7.2 (E0407)

- **Windows operating systems**

1. The DAM feature is supported on Centerm thin clients. Make sure NIC MAC is selected as the desktop asset fingerprint on the DAM Options tab in the Advanced Customization window of the iNode management center.
2. Supports iNode client update at the next user login. This feature must work with iMC UAM 7.2 (E0407) or later.
3. Support for negotiation of EAP authentication type, PEAP authentication subtype setting, and negotiation of PEAP authentication subtype.

Features released in iNode PC 7.2 (E0405)

None

Features released in iNode PC 7.2 (E0404)

- **Windows operating systems**

1. The SSL VPN client can be integrated into the dissolvable client and supports Web authentication.
2. IPsec VPN supports the dial-up connection by using a 3G network card.

3. Using the Calling Number attribute through the L2TP connection to report the client MAC address to the LNS.
4. Size optimization and improvement for the iNode installation package.
5. The msi installation packages can be uninstalled at the CLI.

Features released in iNode PC 7.2 (E0403)

- **Windows operating systems**

1. Customizing the iNode icon on the main page and the desktop iNode icons.
2. Customizing copyright information for the iNode client.
3. EAP-TLS authentication supports the CNG certificate. (Select Windows Server 2008 Enterprise as the Windows server version for the certificate template copied from a certificate that is issued by a Windows Server 2008 certificate server.)

Features released in iNode PC 7.2 (E0402)

- **Windows operating systems**

1. L2TP/ IPsec VPN access.
2. Grace days for patch noncompliance that specifies how many days the user can access the network when the PC passes all security check items except the patch check. During the grace days, the system performs the patch check every time the user comes online until the PC passes the patch check. If the user cannot pass the patch check after the grace days, the system isolates the user. This feature must work with iMC EAD 7.2 (E0402) or later versions.
3. Asset periodic reporting by DAM. This feature must work with iMC EAD 7.2 (E0402) or later versions.
4. Logical combination of AND and OR for items in a PC software control group. This feature must work with iMC EAD 7.2 (E0402) or later versions.

Features released in iNode PC 7.2 (E0401)

- **Windows operating systems**

1. The iNode client uses the customized portal redirect IP to trigger a redirect request. If the portal redirect IP is not customized in the iNode management center, the iNode client uses the predefined redirect IP to send the redirect request.

Features released in iNode PC 7.1 (E0313)

- **Windows operating systems**

1. Allows you to select whether to display the client authentication status window.

Features released in iNode PC 7.1 (E0312)

- **Windows operating systems**

1. Supports Windows 10.

Features released in iNode PC 7.1 (E0311)

- **Windows operating systems**

1. Disabling nonstandard storage devices, such as cell phones in DAM. This feature must work with iMC EAD 7.1 (E0301P07) or later versions.
2. Disabling the guest account of Windows. This feature must work with iMC EAD 7.1 (E0301P07) or later versions.
3. Checking whether the data execution prevention feature is enabled. This feature must work with iMC EAD 7.1 (E0301P07) or later versions.
4. Selecting the asset model during asset registration by using the DAM client. This feature must work with iMC EAD 7.1 (E0301P07) or later versions.

Features released in iNode PC 7.1 (E0310)

- **Windows operating systems**

1. Using a smart card for certificate authentication. The user is forced to log off when the smart card is removed.

Features released in iNode PC 7.1 (E0309)

- **Windows operating systems**

1. Supports the CLI mode, which allows a third-party vendor to perform 802.1X, portal, or SSL VPN authentication by calling commands.
2. Supports Trend Anti-virus network edition client 11.0.

Features released in iNode PC 7.1 (E0308)

- **Windows operating systems**

1. Supports MACsec (only for Windows). To use this function, the iNode client must work with H3C S10510 (temporary test version) and H3C S7506E (temporary test version) switches.
2. Certificate authentication supports using the Subject Alternative Name-UPN or Subject Alternative Name-DNS attribute as the access user account. Supports the Subject Alternative Name-UPN and Subject Alternative Name-DNS attributes when you customize Generate username from a certificate attribute.
3. Views the IP addresses and MAC addresses of all NICs of the host where the iNode client is located.

Features released in iNode PC 7.1 (E0307)

- **Windows operating systems**

1. The Hide the installation complete page option was added. When this option is selected, the installation program hides the installation complete page that provides OS restart options at the end of a silent installation or upgrade. For correct operation of the iNode client, make sure you restart the operating system after the iNode client installation is complete.
2. The Scan All Info option was added to the asset details page in iMC EAD. When a registered DAM client comes online, use this option to have the DAM client immediately report all asset information to iMC EAD. This option is available in iMC EAD 7.1 (E0301P04) and later versions.

Features released in iNode PC 7.1 (E0306)

- **Windows operating systems**

1. Added support for verifying the dynamic SMS password for a portal user whose authentication password is set to Account Password + Dynamic Password. This feature is available in IMC UAM 7.1 (E0302P08) and later versions.

Features released in iNode PC 7.1 (E0305)

- **Windows operating systems**

1. Added support for customizing .msi installation packages. The installation package is used by Windows domain controllers to deploy software to users or user PCs. On 64-bit Windows systems, the software can only be deployed to user PCs.
2. A MAC authentication connection can be preconfigured for the iNode client in the iNode management center.
3. DAM supports asset registration reminders. The **Grace Days for Unregistered Assets** parameter was added to the asset registration check configuration area of the EAD security policy. The parameter determines the number of days the system allows an unregistered asset to pass the security check and sends a daily reminder for asset registration. To use this feature, the iNode client must work with IMC EAD 7.1 (E0301P03) or later versions.
4. The iNode client supports using the **Subject-User ID** certificate attribute as the username for certification authentication. In the iNode management center, the **Subject-User ID** attribute was added to the list of certificate attributes that can be used to generate the username for certification authentication.
5. The **Minimize shortcut toolbar after startup** option was added. The option can be customized for the iNode client in the **General Options** tab of the iNode management center. By default, the option is not selected.

Features released in iNode PC 7.1 (E0304)

- **Windows operating systems**

1. Supports SSL VPN access.

2. Permitting user access only to the SSIDs on the SSID whitelist. Operators can configure the SSID whitelist in IMC UAM. This feature must work with IMC UAM 7.1 (E0302H01) or a later version.
3. Checks weak OS passwords based on the Windows group policy. iNode must work with IMC EAD 7.1 (E0301P02) or later.

- **Linux operating systems**

1. Supports running on a 64-bit version of Linux. To provide the client anti-crack function, iNode must work with IMC UAM 7.1 (E0302P06) or later.

Features released in iNode PC 7.0 (E0113)

- **MAC OS operating systems**

1. Supports MAC OS 10.10.

Features released in iNode PC 7.0 (E0112)

- **Windows operating systems**

1. The last login username can be hidden from the unified authentication page on Windows 7 or later versions. By default, the last login username is displayed. This option can be customized in the iNode management center.

Features released in iNode PC 7.0 (E0110)

- **Windows operating systems**

1. Customizing iNode single sign-on to perform an OS login before network authentication. The iNode management center provides a "Log into the OS without waiting for the authentication result" option to perform an OS login before network authentication during single sign-on. This function requires the PC to be connected to an AD server without passing network authentication.

Features released in iNode PC 7.0 (E0109)

- **Windows operating systems**

1. Supports Rising 24.00.16.46.
2. Supports Kaspersky 14.0.0.4651.
3. Supports Bitdefender 2012 15.0.40.172896763. iNode must work with IMC EAD 7.1 (E0301) or later.

Features released in iNode PC 7.0 (E0108)

- **Windows operating systems**

1. The logo, title, and prompt message for unified authentication on Windows 7 can be customized in the iNode Management Center.

2. When Internet access control is enabled, iNode supports the RADIUS failopen function for 802.1X access.
3. iNode supports certificate authentication for 802.1X and portal access by using a FEITIAN CA certificate. iNode must work with IMC UAM 7.0 (E0203P04) or later.

Features released in iNode PC 7.0 (E0107)

- **Windows operating systems**

1. The client supports password strength check during or after the security check as required by the security policy configured in EAD. The client is only granted limited access permissions before it completes the password strength check. This feature requires IMC EAD 7.0 (E0202P01) or later versions.
2. If the iNode PC client detects a version mismatch between the DAM client at startup, it displays a message to prompt the user to fix the problem.
3. The anti-proxy detection feature supports detecting the use of Cheetah free WiFi2.0.
4. When you use the iNode PC client running on Windows 7 for unified authentication, the login page no longer displays the domain name used for last successful login in abbreviated form. Instead, the complete domain name is displayed.

Features released in iNode PC 7.0 (E0106)

- **Windows operating systems**

1. The client supports up to 16 connections of the same access type.

- **Linux operating systems**

1. 802.1X authentication connections in the Linux/Mac OS client support multicast packets.

Features released in iNode PC 7.0 (E0105)

- **Windows operating systems**

1. Working with UAM to prohibit network access through a VM. This feature requires IMC UAM 7.0 (E0201) or later versions.
2. Working with EAD to provide offline audit for Internet access control. The operator can configure an IP address for the iNode client to ping when none of the client connections is active. All successful pings are recorded. When the iNode client is used for network access, it immediately reports the ping records to EAD for audit. This feature requires IMC EAD 7.0 (E0201) or later versions.
3. Working with EAD to check the status of Windows system restore feature. This feature requires IMC EAD 7.0 (E0201) or later versions.
4. Working with DAM to provide desktop asset approval. This feature requires the administrator to examine the asset information sent from the client. The

asset is registered with DAM only when the asset information is approved. This feature requires IMC EAD 7.0 (E0201) or later versions.
5. The Auto reconnect retries after network failure and Keep IP when disconnected options are supported by wireless access connections.
6. Working with UAM to report violations when the access policy uses Kick Out as the action for violation. This feature requires IMC UAM 7.0 (E0201) or later versions.
7. Supports Windows 8.1.

Features released in iNode PC 7.0 (E0103)

- **Windows operating systems**

1. On Windows Vista or above versions of Windows, the iNode client automatically uses the domain that the computer joins for unified authentication if the user does not specify any domain name.
2. Surface Pro is supported.

Features released in iNode PC 7.0 (E0102)

- **Windows operating systems**

1. Working with UAM to implement configuration upgrade of the iNode client. This feature requires IMC UAM 7.0 (E0102) or later versions.
2. Forcing 802.1X users to use the domain configured in the iNode management center for authentication.
3. Immediately upgrade when the user goes online. If the iNode client upgrade mode is set to Immediate Upgrade in the iNode management center, the iNode client is upgraded immediately when the user goes online.
4. Ping mode offline ACL configuration. You can configure EAD to apply different ACLs to the iNode client based on the ping results of specific IP addresses. This feature requires IMC UAM 7.0 (E0102) or later versions.
5. Logging user off for automatic repair of driver errors. This feature can be configured in the iNode management center and is disabled by default.
6. Using the subjectuid certificate attribute as the access account in certificate authentication. The iNode management center supports the subjectuid attribute for the Generate username from a certificate attribute feature.
7. Supports CLI. Devices of third-party vendors can initiate authentication through the CLI of the iNode client. This feature is available only on Windows hosts.
8. Wireless 3G adapters can be used for EAD and portal authentication after VPN dial-up.
9. Supports PEAP-GTC authentication.
10. Supports single sign on for 802.1X PEAP authentication.
11. Working with DAM to inform endpoint users of disabled peripheral devices.
12. Supports Kaspersky Endpoint Security 10.

Features released in iNode PC 7.0 (E0101)

- **Windows operating systems**

1. Automatic reconnection to the wireless network when the network failure is removed.

[Table of Contents]

Problems Fixed in this Release

iNode PC 7.2 (E0407) fixes the following problems, including all bugs fixed after iNode PC 7.0 (E0101).

Resolved Problems in iNode PC 7.2 (E0407)

1. After SSL VPN authentication is passed, the iNode client might fail to obtain a private IP address for the virtual NIC and cannot access the Intranet network.
2. On Mac OS, the iNode client is disconnected shortly after it comes online because UAM attempts to deliver a client message that includes more than 256 characters.
3. Changing the system time on Windows affects portal authentication. Portal users will be automatically disconnected after a time period.
4. A user might need to perform L2TP/IPsec VPN dial-up twice for network access when the iNode client uses the default action of Deny for Internet access control.
5. Text strings in VPN connection basic settings for L2TP/IPsec VPN dial-up connections are not displayed clearly and completely when DPI is set to 150% for the OS of the PC.
6. The security vulnerabilities CVE-2016-0800 are fixed.
7. The security vulnerabilities CVE-2015-3195 are fixed.
8. The security vulnerabilities CVE-2015-3196 are fixed.

Resolved Problems in iNode PC 7.2 (E0405)

1. When a user performs SSL VPN certificate authentication in the iNode client, the system displays the following message: Failed to query ssl vpn parameters, please check your network configuration or contact the administrator.
2. The LWF drive might still exist in the Windows 10 system after the iNode client with the Internet access control function is uninstalled from the system.
3. When an account is added to AD and is used in the iNode client for 802.1X unified authentication, the system displays the following message: There are currently no logon servers available to service the logon request.

Resolved Problems in iNode PC 7.2 (E0404)

1. If only the **Password and certificate** verification mode is selected in SSL VPN options during client customization, the client does not display the certificate selection field in the SSL VPN connection properties window.

2. When you collect debug logs by clicking **Collect** on the **Settings** tab of the **Management Plat** window, the **Authentication** tab of the NIC properties window does not appear.

Resolved Problems in iNode PC 7.2 (E0403)

1. The Internet access control feature might operate incorrectly on the iNode client after restart of the PC to complete repairing of the iNode client that supports Internet access control and ACL features.
2. If the OS has gone into hibernation, the client might fail to come online after the OS is woken up. You must restart the operating system or the iNode Service.
3. The iNode client requires 60 seconds to start up after the computer desktop has been displayed when Auto authN after startup, unified authentication, and machine authentication are enabled for connections on the iNode client.
4. Enable machine authentication for 802.1X connections on the iNode client. When the operating system is shutting down, it displays that netsh.exe runs incorrectly.
5. The Auto authN after startup option is selected for a portal connection on the iNode client. A user comes online after automatic authentication through portal at startup, and then goes offline. Then, another user comes online. If you point to the online user string in the online connection window, the user name in the tooltip is not the online user name.

Resolved Problems in iNode PC 7.2 (E0402)

1. When the **Save username and password** option is selected, a user passes unified 802.1X authentication and PEAP certificate authentication to come online as Account A. After the operating system restarts, the user cannot pass unified authentication as Account B, because the client automatically uploads information about Account A for authentication.
2. In Windows XP environment, a new 802.1X online user cannot pass authentication after being reauthenticated in the online user list in UAM. During authentication, the iNode client always displays the message of **Connecting** and no authentication progress message appears in the system tray. The user cannot come online even by manually reconnecting to the network.
3. uring 802.1X access, the secure status in the iNode client sometimes becomes **Unchecked** a few minutes after the user comes online.

Resolved Problems in iNode PC 7.2 (E0401)

1. A user comes online by passing 802.1X authentication and portal authentication with the same account. When UAM delivers an instant message to the online user and initiates reauthentication of the user, the iNode client stops working.
2. The iNode Mac OS client does not display the newly added USB network card in the Select NIC list of the 802.1X connection property window.

Resolved Problems in iNode PC 7.1 (E0313)

1. When the Minimize the window after startup option is selected in the Management Plat dialog box, and the Auto authN after startup option is selected in the connection properties, the iNode client sometimes does not minimize its window after the system is restarted.
2. If the disk serial number consists of only the digits of 0 to 9, the DAM client or other disk serial number reading tools failed to obtain the disk serial number.
3. On the 802.1X Options tab in the Advanced Customization window of the iNode management center, select Selected by Default and clear Allow Users to Modify for the Auto authN after startup option, and then create an 802.1X connection. The running iNode client failed to automatically perform 802.1X authentication at the Windows startup.
4. X509_cmp_time does not properly check the length of the ASN1_TIME string and can read a few bytes out of bounds. In addition, X509_cmp_time accepts an arbitrary number of fractional seconds in the time string. An attacker can use this to craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS on applications that verify certificates or CRLs.
5. The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.
6. If a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket then a race condition can occur potentially leading to a double free of the ticket data.
7. When verifying a signedData message the CMS code can enter an infinite loop if presented with an unknown hash function OID. This can be used to perform denial of service against any system which verifies signedData messages using the CMS code.

Resolved Problems in iNode PC 7.1 (E0312)

None

Resolved Problems in iNode PC 7.1 (E0311)

1. When an iNode client installation file named **iNode.exe** exists in the root directory of drive C, the following message appears repeatedly after installation or upgrade of an iNode client supporting DAM: A previous instance is still running. Please try it later.
2. When the trend antivirus software 10.6.5372 is installed on the PC and the antivirus software check policy is configured on the iMC EAD server, the iNode client is logged off a few seconds after the iNode client comes online.
3. When a guest VLAN is configured and the iNode client uses an 802.1X connection to access the network, the iNode client sometimes updates the IP address incorrectly.

Resolved Problems in iNode PC 7.1 (E0310)

1. The Lock Internet access ability option is selected and the default filter action is selected as Deny during the iNode client customization. The user comes

online by using a portal connection and the Automatic reconnect after network is restored option is selected in the connection properties. When the network recovers from a heartbeat timeout, the client does not automatically reconnect to the network.
2. After the iNode PC client is upgraded from version 7.0 or earlier to version 7.1 (E0304) or later, the client cannot save the user name and password.
3. Use the iNode client to perform unified authentication in Windows 7. When the user presses Ctrl + Alt + Delete to unlock the screen, the authentic Windows logon screen does not appear. The user must press Enter to show the logon screen.

Resolved Problems in iNode PC 7.1 (E0309)

1. When the Auto authN after startup option is selected for portal authentication, the iNodePortal.exe process exits abnormally on PCs after the user restarts the operating system or fixes the iNode client.
2. The iNode client is customized with client ACL, Internet access control, or MACsec. The operating system might crash when copying large files from the network.
3. When the iNode client is customized with client ACL, Internet access control, or MACsec, security check cannot be performed after the user passes 802.1X or portal authentication in the iNode client.

Resolved Problems in iNode PC 7.1 (E0308)

None

Resolved Problems in iNode PC 7.1 (E0307)

1. An online iNode PC client cannot be upgraded by using the client upgrade task configured in iMC UAM.to upgrade the iNode PC client from iNode PC 7.1 (E0306) to a later version.

Resolved Problems in iNode PC 7.1 (E0306)

1. Denial of Service attack might be launched and cause a server memory leak by exploiting security vulnerabilities CVE-2014-3572, CVE-2015-0204, and CVE-2015-0205.
2. A PC installed with multiple hard disks is registered with the DAM server and comes online. When the PC is restarted, however, the DAM client displays a message that the PC must be reregistered.

Resolved Problems in iNode PC 7.1 (E0305)

1. The **ip-tunnel** command is configured with the **force-all** keyword in SSL VPN context view on the Comware V7 SSL VPN gateway. The policy server is enabled in IMC UAM. Sometimes the user cannot access the network by using the SSL VPN client that runs on Windows 7. The following error message is displayed:

Cannot communicate with EAD server, socket binding failed.

Resolved Problems in iNode PC 7.1 (E0304)

None

Resolved Problems in iNode PC 7.0 (E0113)

None

Resolved Problems in iNode PC 7.0 (E0112)

1. The Windows Event Viewer shows error 7016: The iNode Service service has reported an invalid current state 0.
2. Unified 802.1X authentication in the iNode client fails when users operate according to the following steps: Enable The following options in the iNode client: Do not actively go offline when the user logs off or turns off the computer,then logs on to Windows using the administrator account, immediately logs out.After that,uses the domain user account for unified authentication.

Resolved Problems in iNode PC 7.0 (E0110)

None

Resolved Problems in iNode PC 7.0 (E0109)

1. The security vulnerabilities are CVE-2014-0224 fixed.
2. Reboot the computer after unified authentication has been performed through iNode on Windows 7. At the next startup, the account name does not appear in the login window and must be manually specified again.

Resolved Problems in iNode PC 7.0 (E0108)

1. The security vulnerabilities CVE-2014-0198 are fixed.

Resolved Problems in iNode PC 7.0 (E0107)

None

Resolved Problems in iNode PC 7.0 (E0106)

None

Resolved Problems in iNode PC 7.0 (E0105)

None

Resolved Problems in iNode PC 7.0 (E0103)

1. In IMC EAD, a software control policy is configured to check a white list of software products that are permitted to be installed only. On 64-bit Windows, the security check result includes only 64-bit software, but it does not include 32-bit software.

Resolved Problems in iNode PC 7.0 (E0102)

1. The iNode client is enabled with the Internet access control and client offline ACL features. Configure an upgrade task to upgrade the iNode client to use a new configuration package with the Internet access control feature disabled. The offline ACLs still work on the iNode client after the iNode client is upgraded.

Resolved Problems in iNode PC 7.0 (E0101)

1. To remove the wireless function of the iNode client, install a customization upgrade package to the endpoint on which the iNode client is running with the wireless and SSID access control functions, After the iNode client is upgraded, the endpoint user cannot use the Windows built-in client to manage wireless connections.

[Table of Contents]

---

iNode Software Distribution Contents

The iNode software contains the following files and folders:

1. iNode\manual\readme_iNode_PC_7.2 (E0407).html-this file
2. iNode\Windows\iNode Management Center for Windows 7.2 (E0407) .exe-the iNode Management Center installation program
3. iNode\Linux\iNodeClient_Linux.tar.gz-the iNode PC installation packet for Linux
4. iNode\Linux\iNodeClient_Linux64.tar.gz-the iNode PC installation packet for Linux 64 bit
5. iNode\MacOS\iNodeClient_MacOS.tar.gz-the iNode PC installation packet for Mac OS

[Table of Contents]

Installation Prerequisites

PC Requirements

The following are the minimum hardware and software requirements for running iNode PC on a PC:

- Minimum hardware requirements
  - CPU: Speed ≥ 1.5G
  - Memory: 512MB or higher
  - HD: 20G or higher
  - 1*integrated 100MB NIC

- Operating system
  - Windows XP (SP2 or a higher patch version required)
  - Windows Server 2003 (SP2 or a higher patch version required)
  - Windows Vista (SP1 or a higher patch version required)
  - Windows 7 Home Basic
  - Windows 7 Home Premium
  - Windows 7 Professional
  - Windows 7 Enterprise
  - Windows 7 Ultimate
  - Windows 8 Professional
  - Windows 8 Enterprise
  - Windows 8.1 Professional
  - Windows 8.1 Enterprise

  - Windows 10 Enterprise
  - Red Hat Enterprise Linux ES 5.0 (32 bit)
  - Red Hat Enterprise Linux ES 6.1 (64 bit)
  - Red Hat Enterprise Linux ES 7.0 (64 bit)

  - Ubuntu 9.0.4 (32 bit)
  - Ubuntu 11.10 (32 bit)
  - Ubuntu 12.04 (32 bit)
  - Ubuntu 12.10 (32 bit)

  - Ubuntu 14.10 (64 bit)
  - CentOS 7.0 (64 bit)

  - Fedora 9.0 (32 bit)

  - Fedora 20 (64 bit)

  - MAC OS 10.5
  - MAC OS 10.6
  - MAC OS 10.7
  - MAC OS 10.8

  - MAC OS 10.9
  - MAC OS 10.10

[Table of Contents]

Port Usage

The following TCP/IP Ports are used.

Port	Usage
UDP 500,1701	Port of the iNode client for listening to L2TP and IPsec packets
UDP 9019	Port of the policy proxy server for listening to the packets sent from the iNode client
UDP 9029	Port of the DAM proxy for listening to the packets sent from the iNode client
TCP 9090	Port of the iNode management center for listening to the packets sent from the iNode client
UDP 10102	Default port of the iNode client for listening to the EAD packets from the policy proxy server (if the service port assignment fails, the port number automatically increments by one)
UDP 20202	Default port of the iNode client for listening to the packets from the DAM agent (if the service port assignment fails, the port number automatically increments by one)
UDP 50100	Port of the portal server for listening to the packets from the iNode PC 3.60-E6301 and earlier version clients
UDP 50200	Port of portal transfer for listening to the packets from the iNode client

[Table of Contents]

Typical Installation

- Installing the iNode Management Center

1. Log in to the Windows operating system as Administrator.
2. Double-click the setup package to start the InstallShield wizard. Click **Next**.
3. Select **I accept the terms of the license agreement**, and click **Next**.
4. Specify an installation folder and click **Next**. The default installation folder is "C:\Program Files\iNode\iNode Manager."
5. Click **Install** to start installing the iNode management center. The installation process takes a while. To change any settings before the installation, click **Back** to go to the previous pages.
6. After the installation completes, click **Finish** to close the InstallShield wizard.

- Installing the iNode Client on Windows Operating System

1. The network administrator uses the iNode management center to customize the iNode client setup package and distributes the package to end users. The following operation steps are all performed by an end user.
2. Log in to the Windows operating system as Administrator.
3. Double-click the setup package to launch the installation wizard. Click **Next**.
4. Select **I accept the terms of the license agreement**, and click **Next**.
5. Specify an installation folder and click **Next**. The default installation folder is "**C:\Program Files\iNode\iNode Client**." You can click **Change** to change the installation folder.
6. Click **Install** to start installing the iNode client. To change any settings before the installation, click **Back** to go to the previous pages.
7. If you install the iNode client on Windows Vista or Windows 7 operating system, the user account control gives a security prompt. Click **Yes** to proceed with the installation.
8. Select **Yes, I want to restart my computer now.** and click **Finish** to restart your computer immediately, or select **No, I will restart my computer later.** click **Finish**, and restart your computer later.

- Installing the iNode Client on Linux Operating System

  The supported Linux operating systems include Red Hat Enterprise Linux Server ES 5, Ubuntu 9.0.4, Ubuntu 11.10, Ubuntu 12.0.4 and Fedora 9.0.

1. Log in to the Linux operating system as a root user. Because Ubuntu does not support root users, log in to Ubuntu as Administrator.
2. Create the iNode installation folder **/home/iNode/** if this folder does not exist. Use the **cp iNodeClient_Linux.tar.gz /home/iNode/** command to replicate the installation file to **/home/iNode/**.
3. Enter the directory of the installation file, and use the **tar -zxvf iNodeClient_Linux.tar.gz** command to decompress the installation file to the folder **/home/iNode/iNodeClient/**.
4. In the **/home/iNode/iNodeClient/** directory, use the **./install.sh** command to install the Linux iNode. In Ubuntu, use the **sudo ./install.sh** command to install the Linux iNode. Before executing the **install.sh** command, make sure that the root user has the execution privilege. You can use the **chmod 755 install.sh** command to modify the execution privilege for the root user.
5. After installing the Linux iNode, use the **ps -e | grep A** command to determine whether **AuthenMngService** is enabled. If this service is enabled, you have successfully installed the Linux iNode.

- Installing the iNode Client on Mac OS Operating System

  The supported versions of Mac OS operating system include Mac OS 10.5, Mac OS 10.6, and Mac OS 10.

1. Log in to the Mac OS operating system as Administrator.
2. We recommend you to replicate the configuration file **iNodeClient_MacOS.tar.gz** to the personal directory of the login user.
3. Double-click the configuration file to decompress it.

4. Double-click **iNodeClient** to start the installation wizard. Click **Continue**.
5. Specify a volume. The iNode will be installed under the folder **/Applications/iNodeClient/** on the specified volume.
6. Click **Continue** to enter the **Installation Type** page. Click **Continue.**
7. Type your username and password, and click **OK**.
8. Confirm the installation settings, and click **Install**.
9. After the installation process, click **Resta**rt to restart the operating system to ensure normal operation of the iNode client.

[Table of Contents]

Upgrade Installation

This version is available for versions iNode PC 5.0 (E0101) or later.

Follow these instructions to upgrade iNode PC:

- Upgrading the iNode Management Center

1. Remove the iNode management center of the old version.
2. Install a new version.

- Upgrading the iNode Client

  Direct upgrade—Directly upgrades the iNode client on Windows, Linux, or Mac OS operating system

1. The network administrator uses the iNode management center to customize a new iNode client setup package and distributes the package to end users. The following operation steps are all performed by an end user.
2. Remove the iNode client of the old version.
3. Install the iNode client of the new version.

   Online upgrade method I—Uses the IMC UAM to upgrade the iNode client. This method is available on only Windows operating systems.

1. The network administrator uses the iNode management center to customize an iNode client upgrade package.
2. Configure client upgrade on the IMC UAM.
   - Log in to the IMC console, select the **Service** tab, and select **User Access Manger** > **Service Parameters** > **Client Upgrade Configuration** from the left navigation tree.
   - Click **Add** to enter the **Add Client Upgrade Task** page.
   - Type the task name.
   - Select an upgrade type. The available options include **Force** and **Optional**. If you select **Force**, the end users in the specified range must upgrade their clients. If you select **Optional**, the end users in the

specified range can determine whether to upgrade their client or keep their old versions.
    - Specify the download rate limit, which can limit the speed at which a single user downloads the upgrade package.
    - Click **Browse** next to **Client Upgrade File**, and specify the previously customized upgrade package.
    - Click **Add** next to **User Group**, and specify the user groups that require client upgrade.
    - Click OK.
3. When the iNode client of an old version gets online, if you have specified **Optional** as the upgrade type, the end user can determine to upgrade the client or not. If you have specified **Force** as the upgrade type, the end user must upgrade the client. After the upgrade, restart the client computer.

   Online upgrade method II—Uses the iNode management center to upgrade the iNode client. This method is available on only Windows operating systems.

1. Upgrade the iNode management center (see “Upgrading the iNode Management Center”).
2. Enable the upgrade function on the iNode management center.
3. When the iNode client of an old version gets online, the client automatically gets upgraded if the client can communicate with the iNode management center.

[Table of Contents]

Un-Installation

- Removing the iNode Management Center

1. Terminate the iNode management center.
2. From the **Start** menu, select **All Programs > iNode > iNode Management Center > Remove iNode Management Center** to open the page for removing the program.
3. Click **Yes** to confirm your operation.
4. After the uninstallation completes, click **Finish** to exit the program.

- Removing the iNode Client from Windows Operating System

1. From the **Start** menu, select **All Programs** > **iNode** > **iNode Intelligent Client** > **Repair or Uninstall iNode Intelligent Client** to open the page for repairing or removing the program.
2. Select **Remove** and click **Next**.
3. Click **Yes** to confirm your operation.

4. A dialog box appears, asking whether you want to save the connection information that you have configured. For reinstallation of the iNode client, we recommend you to select **Yes**.
5. Select **Yes, I want to restart my computer now.** and click **Finish** to restart your computer immediately, or select **No, I will restart my computer later.** click **Finish**, and restart your computer later.

- Removing the iNode Client from Linux Operating System

1. Log in to Linux operating system as a root user. Because Ubuntu does not support root users, log in to Ubuntu as Administrator.
2. Enter the installation folder of the Linux iNode.
3. Use the **./uninstall.sh** command to remove the Linux iNode. In Ubuntu, use the **sudo ./uninstall.sh** command to remove the Linux iNode.

- Removing the iNode Client from Mac OS Operating System

1. Log in to the Mac OS operating system as Administrator. The administrator privilege is required when you remove the Mac OS iNode.
2. Click the **Spotlight** icon on the upper right corner of the desktop and search for the terminal.
3. Enter the installation directory of the Mac OS iNode.
4. Execute the **./uninstall.sh** command to remove the Mac OS iNode. The administrator's password for logging in to the operating system is required during the uninstallation process.

[Table of Contents]

Known Problems

Installation/Upgrade/Patch

N/A

Other Problems

N/A

[Table of Contents]

Issued: Apr 2016