[2014-05-29]iNode PC 7.0 (E0108)版本发布

马光彬 2014-06-07 发表

iNode PC 7.0 (E0108)的版本发布

一 适用范围及配套说明

iNode PC 7.0 (E0108)版本正式发布，使用范围为国内和海外市场。

1、历史版本号

历史版本号如表1所示：

表1 历史版本号

版本号	基础版本号	发布日期	备注
iNode PC 7.0 (E0108)	iNode PC 7.0 (E0107)	2014-05-29	
iNode PC 7.0 (E0107)	iNode PC 7.0 (E0106)	2014-04-30	
iNode PC 7.0 (E0106)	iNode PC 7.0 (E0105)	2014-02-13	
iNode PC 7.0 (E0105)	iNode PC 7.0 (E0104)	2013-12-27	
iNode PC 7.0 (E0104)	iNode PC 7.0 (E0103)	2013-11-08	仅对H3C发布，仅支持Windows系统
iNode PC 7.0 (E0103)	iNode PC 7.0 (E0102)	2013-09-12	
iNode PC 7.0 (E0102)	iNode PC 7.0 (E0101)	2013-08-07	
iNode PC 7.0 (E0101)	iNode PC 5.2 (E0409)	2013-07-13	
iNode PC 5.2 (E0409)	iNode PC 5.2 (E0408)	2013-06-13	
iNode PC 5.2 (E0408)	iNode PC 5.2 (E0406)	2013-05-10	
iNode PC 5.2 (E0406)	iNode PC 5.2 (E0402)	2013-04-11	仅发布中文版。
iNode PC 5.2 (E0402)	iNode PC 5.2 (E0401)	2013-02-05	仅支持Windows中文版。
iNode PC 5.2 (E0401)	iNode PC 5.1 (E0308)	2013-01-17	
iNode PC 5.1 (E0308)	iNode PC 5.1 (E0307)	2012-10-31	仅支持Windows系统。 无线客户端受限研发确认的局点使用，无线网卡适配情况请参见配套表。
iNode PC 5.1 (E0307)	iNode PC 5.1 (E0304)	2012-10-16	无线客户端受限研发确认的局点使用，无线网卡适配情况请参见配套表。
iNode PC 5.1 (C0306)	iNode PC 5.1 (E0304)	2012-09-12	仅支持Windows中文版，本版本合入苏州中行802.1X断线重连需求，受限苏州中行使用。本版本不包含iNode PC 5.1 （C0305）版本合入的特性，需要使用iNode PC 5.1 （C0305）版本新特性的用户不能使用本版本。 无线客户端仅限售前测试，不能大规模部署使用。
iNode PC 5.1 (C0305)	iNode PC 5.1 (E0304)	2012-08-22	仅支持Windows中文版，本版本合入光大银行SSID访问控制需求，受限光大银行使用。 无线客户端仅限售前测试，不能大规模部署使用。
iNode PC 5.1 (E0304)	iNode PC 5.1 (E0303)	2012-06-12	无线客户端仅限售前测试，不能大规模部署使用。
iNode PC 5.1 (E0303)	iNode PC 5.1 (C0302)	2012-05-28	无线客户端仅限售前测试，不能大规模部署使用。
iNode PC 5.1 (C0302)	iNode PC 5.1 (E0301)	2012-05-10	仅支持中文版本，本版本主要解决中山大学通过仿冒PAP认证获取用户密码问题，该版本受限中山大学和有上述问题的局点使用。
iNode PC 5.1 (E0301)	iNode PC 5.0 (C0106)	2012-01-16	

版本号	基础版本号	发布日期	备注
iNode PC 5.0 (C0106)	iNode PC 5.0 (E0105)	2011-11-04	仅支持中文版本，仅限特定局点使用。
iNode PC 5.0 (E0105)	iNode PC 5.0 (C0104)	2011-08-31	
iNode PC 5.0 (C0104)	iNode PC 5.0 (E0103)	2011-08-16	仅支持中文版本，仅限特定局点小规模试用，不允许在生产环境下使用，请在试用前联系研发确认
iNode PC 5.0 (E0103)	iNode PC 5.0 (C0102)	2011-05-09	
iNode PC 5.0 (C0102)	iNode PC 5.0 (E0101)	2011-03-01	
iNode PC 5.0 (E0101)	首次发布	2011-01-26	

2、版本配套表

配套的设备和软件信息请参见版本说明书。

3、版本使用限制及注意事项

iNode管理中心版本使用限制及注意事项

本版本不支持在虚拟机上使用管理中心和定制客户端。

iNode智能客户端版本使用限制及注意事项

(1) VPN认证，需要将LNS设备上对应的虚模板接口的MTU设置为1200，否则会导致长度接近网卡MTU的报文无法正常收发。

(2) VPN客户端在连接上线前会复制当前路由表，等下线后会再复制回来，恢复为上线前的路由表。对于用户在VPN连接上线后修改的路由，即对于上线期间路由表的变化，客户端无法知道，因而在VPN连接断开后，VPN连接用户在上线期间增加或修改的路由将不会被保存。

(3) Windows Vista及以上版本操作系统中进行VPN认证时，必须配置NAT穿越和ESP模式，但实际组网中并不要求必须有NAT设备存在。

(4) 由于McAfee防病毒软件的原因，客户端中显示的McAfee的病毒库版本不准确。

(5) 由于在使用VPN证书认证时，设备不发送安全网关名字，所以这种情况下不支持对VPN对端安全网关名字进行验证。

(6) 由于管理中心和客户端有共享的类库，在同一台机器上同时安装，若卸载其中一个请重新安装另一个，以保证能正常使用。

(7) 请在定制的iNode客户端安装盘文件名中包含setup字符串，否则在Vista下运行安装盘可能会没有响应。

(8) 使用用802.1X + IPsec VPN认证同时访问iMC配置管理台的拓扑管理，极小概率出现802.1X和VPN连接都正常在线，网络却不通的情况，重新认证一次即可。

(9) Windows刷新桌面机制是在系统中创建了一块区域叫桌面图标缓存，桌面图标缓存就是用来保存已经建立的快捷方式图标，刷新桌面显示时就无需重新建立，只需从缓存中读取。由于这种机制存在一定的缺陷，如果重新安装客户端时定制附加图标与第一次定制的不同（即两次定制不同的客户端图标），第二次安装的客户端的显示图标可能会显示第一次安装的客户端图标，这个时候右键刷新电脑桌面都是不起作用的，只有重启“explorer.exe”才会刷新；重启“explorer.exe”的方法：在任务管理器中查找到“explorer.exe”进程，选择该进程点击右键选择“结束进程”即可，结束进程后，在任务管理器窗口点击“文件”菜单，然后点击“新建任务”，在弹出的窗口输入“explorer.exe”，然后点击“确定”按钮即可。

(10) 客户端升级到高版本后又回退到低版本，可能会出现界面中英文混杂，出现这种情况请卸载客户端同时删除客户端相关安装目录后重新安装客户端，建议尽量不要使用版本回退。

(11) 打印机监控特性受Windows API限制，对于通过使用共享打印机（如A安装打印机，然后共享出来，B通过A的共享打印机进行打印）打印的情况，客户端上报的登录用户名可能是登录A的用户名，也可能是登录B的用户名，但打印文档机器的IP地址是正确的，对于打印文档超过一份的情况（如打印三份），打印监控只上报一份，另外不支持IPP方式设置的打印监控，因此该特性受限发布，不推荐大面积使用。

(12) 由于Windows操作系统原因，DAM对于超线程的启用和关闭不是硬件的变更也会当做硬件资产变化上报DAM服务器，即无法区分超线程和真正的双CPU（型号一样的）的区别，另外，由于Windows无法区分某些设备是禁用还是真正从计算机上卸载，因此对于这些设备的禁用和启用，DAM会作为硬件变更上报给服务器。

(13) 客户端仅上传IPv6的全球单播地址，如果存在多个全球单播地址则只上传第一个。Windows 2000不支持IPv6功能。由于Windows XP下没有自带的DHCPv6 Client，在Windows XP下iNode的DHCPv6的IPv6地址刷新与释放操作不会起作用，IPv6地址的刷新和释放由第三方DHCPv6 Client完成。

(14) 客户端从iNode PC 3.60-E6202版本及后续版本修改了防破解及客户端版本号检测机制，需要特定的服务器版本配合，如果服务器上启用了“客户端防破解”（iMC UAM在“业务” - “接入业务” - “系统参数配置”中设置；CAMS在“系统管理” - “系统配置”

- “业务参数配置”中设置）和“仅限iNode客户端”特性（iMC在“业务” - “接入业务” - “服务配置管理”中设置；CAMS在“服务管理” - “服务配置”中设置），则请确认CAMS升级到2.10-F0211P14及之后版本，iMC UAM安装或升级到 3.60-B6202及之后版本，否则会由于兼容性问题导致终端用户认证出现问题。

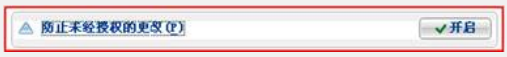
(15) EAD提供的手工补丁检查只支持Windows操作系统的补丁检查，不支持应用软件如Office、Execl等的补丁检查。

(16) 由于客户端安装时需要安装从网卡抓包、VPN虚拟网卡、客户端ACL等驱动，Windows操作系统限制安装驱动需要有管理员权限，因此普通用户权限（如Power User权限）不能正常安装客户端。

(17) 受防病毒软件不同版本实现机制的限制，有些防病毒软件不能正确检查病毒库版本，有些防病毒软件不能正确检查引擎版本，因此在服务器上的设置请参考“防病毒软件配套表”。

(18) iNode客户端域统一认证功能采用微软提供的GINA机制实现，该机制不允许多个厂商的GINA库同时被系统进程WinLogon.exe加载，因此在使用过程中可能会出现iNode客户端的GINA与其它厂商的GINA冲突的问题，典型的有与Think PAD系列笔记本的指纹识别系统冲突，此时可以取消客户端的域统一认证功能或不启用其它厂商使用GINA的系统，也可以联系其它厂商按照华三公司提供的《H3C iNode GINA与第三方GINA联动规范》对其系统进行开发。

(19) 由于趋势新版本防病毒软件对未经过微软徽标签名的程序控制更加严格，在安装、卸载iNode客户端时会非常慢（部分机器需要50分钟左右），即使等待正确安装完成，用户也不能正常上网，出现这种情况请在安装、卸载iNode客户端时在趋势防病毒软件中设置“防止未经授权的更改”功能关闭，安装完成后可以重新开启，如下图所示：



安装完成后将iNode Client.exe加入趋势防病毒软件的例外列表或将“防止未经授权的更改”功能关闭。

(20) 防病毒软件检查不支持金山毒霸5.0高级网络版（中小企业版），如果用户想检查金山毒霸，则需要将金山毒霸升级到6.0版本。

(21) 如果要更换定制的客户端图标，只能通过iMC UAM自动升级实现，不能通过定制间升级实现。

(22) 非认证网卡访问审计功能不支持IPsec+L2TP VPN连接，也不支持多个连接同时上线。

(23) 如果终端安全软件（如防病毒软件）自身设置了应用程序监控策略，则该安全软件会对所有进程（不仅限于该安全软件的进程）的行为进行监控，有可能导致iNode客户端不能正常运行，因此需要在该安全软件的监控策略中将iNode客户端的安装目录设置为例外，即iNode客户端安装目录下的所有文件都不受监控。

(24) Windows XP（SP3）及以上版本，使用802.1X认证，启用“运行后自动认证”选项，操作系统启动时进入桌面可能会比较慢。系统进入桌面的快慢与操作系统相关服务启动的速度有关，不同的机器情况可能不同，用户体验可能会有差异。

(25) 使用Linux/MacOS客户端做安全认证时，如果服务器下发的检查项客户端不支持，则客户端会忽略不处理，此时客户端不会下线也无法完成安全认证。因此，对于使用Linux/MacOS客户端的用户，请不要在EAD服务器的安全策略配置中配置客户端不支持的检查项，Linux/MacOS客户端支持的特性详见版本特性说明。

(26) 启用MAC认证时，客户端会将认证网卡的MAC地址作为用户名和密码进行身份认证，客户端上报的MAC地址格式为字母全部大写且没有分隔符，如000F1CD534EA。

(27) Windows Vista及以上版本操作系统下，终端PC共享目录检查功能仅支持检查使用“高级共享”方式共享的目录。

(28) iNode客户端支持的语言场景为：iMC英文+iNode英文，iMC非英文+iNode英文（服务器侧配置的下发消息只能是英文），iMC非英文+iNode对应服务器的语言。

(29) 纯英文环境的操作系统下，EAD可控软件检查功能不支持检查使用UNICODE编码的中文软件，DAM软件变更不支持上报使用UNICODE编码的中文软件。

(30) DAM客户端上报的硬盘、CPU等硬件信息是通过微软的WMI接口获取的，正确性完全依赖WMI接口的实现。

(31) 在Linux/MacOS系统下，对于没有提供卸载程序的软件，通过手工删除的方法无法将软件卸载干净，使用iNode作安全检查时，对于没有卸载干净的软件可能仍然会检查出已安装。

(32) 在Vista及以上版本的操作系统中使用定制了旧智能卡功能的iNode客户端，可能出现esafe_monitor.exe进程占用CPU偏高的情况，建议在上述操作系统中使用客户端不要定制旧智能卡功能。

(33) 纯英文环境的操作系统下，不支持中文防病毒软件的检查。

(34) 由于IE8自身问题，在Windows7系统下，使用客户端认证通过后，概率出现

不能弹出自动运行任务的页面，建议在上述操作系统中使用IE7或者IE9。
(35)　无线客户端仅支持与iMC UAM服务器配合作802.1X认证。
(36)　使用无线客户端接入不支持在设备上配置多种加密方式，例如在无线模板中同时配置aes和tkip加密方式。
(37)　在Windows Vista及以上版本系统下，使用iNode无线客户端作802.1X认证时，无线网卡的驱动版本必须与操作系统版本一致，即必须使用相应的Vista及以上版本的无线网卡驱动。
(38)　如果两个无线网络的SSID名称相同，iNode无线客户端只能显示其中的一个SSID。
(39)　Windows系统下，受用户权限限制，User用户登录后使用iNode客户端，切换语言菜单时需要点击两次才能生效。
(40)　Windows系统的图标缓存是针对每一个登录用户的，假设操作系统有两个帐号A、B，如果使用A帐号安装过老版本的iNode客户端卸载后，使用B帐号安装新版本的iNode客户端且新版本的客户端快捷图标有变化，则使用A帐号登录后看到iNode快捷图标还是老的。
(41)　使用iNode客户端进行802.1X认证，当流量较大的情况下受报文处理能力限制，可能出现802.1X握手报文丢包而导致用户下线，可以通过修改设备握手间隔和超时时间解决。建议将设备上802.1X心跳间隔时间设置为30秒或者更长时间，重试次数设置为6次或者更多次数。
(42)　某些终端安全软件（如卡巴斯基）有流量监控功能，使用客户端种子部署iNode客户端时，如果启用了流量监控功能，可能会导致iNode安装文件无法正常下载。建议在使用iNode客户端种子进行部署之前，先将终端安全软件退出。
(43)　可信移动介质管理功能不支持Windows2000操作系统。
(44)　可信移动介质管理客户端与注册中心不能安装在同一台机器上。
(45)　可信移动介质管理功能不支持小于8M的U盘。
(46)　使用可信移动介质管理客户端或者注册中心对移动存储介质进行操作的过程中，请不要插拔移动存储介质，以避免移动存储介质损坏或者数据丢失。
(47)　在Windows Vista及以上版本的操作系统中，加载可信移动介质时，操作系统会认为可信移动介质没有格式化而自动弹出格式化提示窗口，请忽略该提示，将格式化窗口关闭即可。
(48)　某些厂商的U盘，如Netac，如果U盘中有多个分区，Windows操作系统会将其识别成多个介质，因此可信移动介质管理注册中心也会将这种U盘识别成多个介质。
(49)　由于虚拟机存在时钟不稳定的情况，可能导致软件运行异常，因此不建议在虚拟机中使用iNode客户端。
(50)　由于iNode无线客户端与第三方无线客户端可能存在冲突，不要同时安装使用iNode无线客户端和第三方无线客户端。
(51)　IPv6组网环境下不支持动态VLAN切换。
(52)　如果禁用Symantec的Autoprotect功能和RTVScan功能，则iNode无法检查出Symantec软件已安装。
(53)　在个别PC机上安装或者升级iNode客户端，当安装VC2005分发包时，可能出现找不到vcredist.msi文件的提示，请联系我司用服获取工具修复。
(54)　使用3G上网卡作为认证网卡时不支持防内网外联、客户端ACL、URL访问控制、SSID访问控制、防代理检测功能。
(55)　虚拟机识别功能仅支持识别如下厂商的虚拟机：VMware、HyperV、KVM、Citrix。
(56)　我司H3C智能卡仅支持密钥长度为1024bit的证书，使用iNode管理中心将密钥长度不为1024bit的证书导入到智能卡后将无法正常认证

二 增减特性说明

iNode管理中心特性变更说明

新增特性：

Windows7系统单点登录窗口的图标、标题、登录提示信息可以在管理中心定制。

删除特性：

无。

修改特性：

无。

iNode智能客户端特性变更说明

新增特性：

（1）　iNode在启用防内网外联功能时支持802.1X逃生场景。

（2）　支持使用飞天诚信CA服务器签名的证书进行802.1X和Portal.证书认证。该特性需要与iMC UAM 7.0 (E0203P04)及之后的版本配套使用。

删除特性：

无。

修改特性：

无。

三 相对前一版本解决的问题

1、201405190254

[一般]问题现象：OpenSSL存在引用空指针的安全漏洞，使用iNode进行PEAP认证时可能出现后台异常退出的情况，该问题出现概率较低。

问题产生条件：使用iNode进行PEAP认证。

如要完整的了解该版本累计解决的软件BUG，请参看配套的《iNode PC 7.0 (E0108)版本说明书》。