



iNODE™ v1.9.5 release notes

Release Notes



iNODE™ Release series 1.9,
Published January 2021. Copyright 2001-2021 Dataways S.A.

Copyright

Copyright © 2021 Dataways S.A. This document is published and the foregoing notice is affixed to protect Dataways Communications S.A. in the event of inadvertent publication.

All rights reserved. No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Dataways S.A.

Trademarks

The Dataways name and logo and the iNODE™ Connectware name and logo are trademarks or registered trademarks in Greece and other countries. Linux is a registered trademark of Linus Torvalds. All other trademarks are properties of their respective holders.

TABLE OF CONTENTS

WHAT'S NEW IN V1.9.5	4
NEW FEATURES	4
MINOR NEW FEATURES:	6
ENHANCEMENTS	7
UPDATE NOTES	8
BUG FIXES	9
KNOWN PROBLEMS	12
HARDWARE SUPPORT	14
HARDWARE RECOMMENDATIONS	16
HOW TO INSTALL	18
UPGRADE FROM PREVIOUS VERSIONS	18
OLDER VERSIONS BACKUP FILES COMPATIBILITY	19
FAQ	20
FURTHER HELP	23

What's new in v1.9.5

This release contains several new features, bug fixes and enhancements. It is available to all existing and new customers with a valid support contract.

For more details you can view the online help or ask your Reseller.

New Features

The most notable features are described below.

- **Feature #1040 Mailbox migration Tool**
Mailbox Migration Tool is an IMAP transfer tool for transferring mailboxes between IMAP platforms. The purpose of this tool is to migrate existing IMAP mailboxes or to backup IMAP mailboxes from one system to another. It allows incremental and recursive IMAP transfers from one mailbox to another, between either known service providers or any IMAP compatible mail platform and your iNODE™ Mail server. When the current server is a source or a destination in the transfer task, no credentials are required. As an administrative task it can have full access to user mailboxes.
- **Feature #1971 E-Mail Logging feature**
A detailed log of all messages passing through the E-Mail Content Filtering service is now recorded. Each log entry represents a single email and contains the details of every aspect of the message: sender, date, subject and the list of recipients, along with the message content type as recognized by the E-Mail content filtering service and the antispam score (if antispam service is enabled).
The log gives a clear view of all emails passing through the system along with a view of all emails that are blocked. It replaces the old quarantine management interface, providing more information a lot faster. Existing Quarantine Management interface will be removed in future release.
- **Feature #2132 New mobile friendly webmail**
A new redesigned skin is now used in the webmail. The skin is responsive, automatically adjusting to mobile screen sizes, providing the best functionality and user experience on every device. The old skin is still available in the user preferences. Note that the new skin is now the default skin and will automatically be used when the webmail is accessed from a mobile device.
- **Feature #2141 Let's Encrypt certificates renewal automation support**
iNODE™ now supports the use of Let's Encrypt services. Let's Encrypt is a certificate authority run by Internet Security Research Group that provides X.509 certificates for TLS encryption at no charge. Most services give warnings and wait for client confirmation when self-signed certificates are

used, because they are not considered trusted. Let's Encrypt apart from being a trusted authority is also automatically renewing the certificates, so there is no need for user intervention and renewal administrative overhead. The service's settings are located at Configuration::System::Certificates Management::Let's encrypt.

The service offers an automated process designed to overcome manual creation, validation, signing, installation, and renewal of certificates.

NOTE-1: You can use the issued certificates in most services that require a certificate. The following system's services cannot use this type of certificates:

*DKIM signing: Let's encrypt certificates cannot be used for DKIM signing as they are automatically renewed and DKIM requires the public keys to be published via DNS.

*Proxy server: Proxy server requires a CA certificate in order to use it for generating dynamic certificates for proxied sites.

*VPN (OpenVPN client, OpenVPN server, IPsec): Let's encrypt certificates cannot be used for any type of authentication.

NOTE-2: It is required that port 80 (HTTP) of the system is accessible from the internet using the hostname specified for the certificate. The hostname corresponds to the Common Name (CN) of the certificate's subject. Port 80 is used to verify the certificate request.

- **Feature #2673 E-Mail content filtering reporting**

A new scheduled reporting feature has been added and the first available report comes with the E-Mail content filtering reporting feature. It is now possible to schedule a periodical report to be sent to a specific email. The report may contain statistics, full logs of all emails processed by the E-Mail content filtering service, or just the emails that have been blocked and lists of the top senders and recipients during the time specified for the report.

- **Feature #2690 E-mail Content Filtering now available with E-Mail service**

E-mail Content Filtering service from now on will always be available when the E-Mail service is licensed. Note that this does not include the E-Mail server antivirus or E-Mail server antispam modules which continue to be separate. Content filtering allows the use of filename filtering, blocking specific attachment types.

- **Feature #2734 New STUN/TURN service**

Traversal Using Relays around NAT (TURN) is a protocol that assists in traversal of network address translators (NAT) or firewalls for multimedia applications. TURN server's purpose is mainly to be used by the Collaboration Suite's Talk application. This service is available to users with File Server license and allows them to be connected to a Collaboration Suite's Talk Meeting from everywhere. A Talk Meeting is a rich multimedia and multi-participant sharing hub for online meetings by providing services like video conference, chat and Screen Sharing.

Enabling TURN server will automatically be used by Talk clients. It can also be used by other applications that require the use of a TURN server.

Minor new features:

- **Feature #2650 Introduce some fuzziness in scheduled tasks**
With the popularity of virtualisation increasing, it is quite often to have multiple systems on a single host. Scheduled tasks running on multiple VMs at the same time can cause the host system to have spikes of load at these times. In order to avoid this, a small fuzziness is introduced for tasks with predefined schedules that are not required to run at an exact time. This should reduce the load on the host server.
- **Feature #2670 Brute-Force protection on user's portal**
Brute-force Protection service now protects the user's portal against brute-force attacks.
- **Feature #2671 Groupware auto-logout settings**
It is now possible to specify the time period after which users are automatically logged out from the Webmail and the Collaboration Suite.
- **Feature #2683 OpenVPN user certificate automatic renewal**
When users get the OpenVPN configuration file from users' interface, user certificates can be issued automatically, if OpenVPN server is properly configured. However, when a user certificate expires, there was no way to renew it, unless you follow the full renewal cycle manually. Now, when the user certificate expires, the user can simply re-download the OpenVPN client configuration file and a renewed user certificate will be included in it. The old certificate is automatically revoked and a new certificate is issued in order to replace it.
- **Feature #2699 New DECK app in Collaboration Suite**
Deck is a kanban style organization tool integrated with the Collaboration Suite, aimed at personal planning and project organization for teams.
- **Feature #2702 Incremental FAX Backup/Restore from specific level**
Restoring an incremental FAX backup from specific level is now supported. This is especially useful to minimize the down-time in the case of migrating the system to new hardware.
- **Feature #2703 Search/filter box for real-time logs**
Realtime logs now contain a filtering capability allowing the administrator to specify a string that will be used to filter out irrelevant log entries.
- **Feature #2729 Epson Inkjet Printer Driver (EPSON-ESCPR) support**
The Epson Inkjet Printer Driver has been incorporated in this release. It supplies high quality printing with Seiko Epson Colour Ink Jet Printers.

Around 570 new printer drivers are included for a corresponding number of Epson printer models.

- **Feature #2762 Admin access to all user's data on Collaboration Suite**
It is now possible for specific admin users to have read-only access to all the content of all users in Collaboration Suite.
- **Feature #2731 Disk Statistics for storage pools**
Monitoring :: System :: Disk Statistics and System Dashboard now include I/O statistics and graphs for all storage pools that point to a block device.

Enhancements

The most notable enhancements are described below.

- **Enhancement #2750,2751 New login portal pages**
Login pages have been redesigned for iNODE™'s Management UI, User Portal, Collaboration Suite and GroupWARE.
- **Enhancement #2752 New iNODE™ Portal**
From now on a newly designed central iNODE™ UI Portal is available as a central hub, allowing users and admins to easily find iNODE™ Portals (iNODE™ Management UI, User Portal, GroupWARE, Collaboration Suite). This service is available to default http(s) ports and allows users or admins to choose proper portal.
- **Enhancement #2618 Webmail upgraded to latest release**
The webmail application has been upgraded to the latest available version.
- **Enhancement #2653 Collaboration Suite upgrade**
The Collaboration Suite platform has been upgraded to version 18.0.10.
- **Enhancement #2661 Bulk Content Delivery task deletion**
Content Delivery publisher, data courier and web courier task management pages now support bulk task deletion.
- **Enhancement #2666 Exclude Files capability for the File service antivirus**
In some cases, the file server antivirus module could cause issues when office files are directly edited on the file server, due to the way some temporary files are used by the applications. The File service antivirus can now be configured to avoid scanning of such files. The Exclude Temporary Office Files option can be set to YES to avoid these problems. Also, a custom list of file types that should be excluded from file server scanning can now be configured.

Update Notes

- **iNODE™ running as a virtual machines on Xen Hypervisor**

In case you run your iNODE™ system by hosting it on XEN hypervisors, you should check that you have enabled the extra swap size from the Management UI (Configuration :: System :: General Settings :: Swap Memory :: Extra Size). This is mandatory for live migrations to work properly. The correct extra swap size can be found for any system with the following table:

For RAM<2GB set Swap Extra Size to double the amount of RAM

For RAM between 2GB - 8GB set Swap Extra Size equal to the amount of RAM

For RAM between 8GB - 64GB set Swap Extra Size to half the amount of RAM

Note: Before changing extra swap size you need to check if your system disk has enough free disk space available.

- **Perform Auth-Backend changes during maintenance window**

Switching authentication back-ends should be done by the administrator in a proper maintenance window or in non-office hours for the following reasons:

- It will cause automatic logout of all users logged in Webmail, Collaboration Suite, Admin UI and User Portal.
- In systems with many users, it will take some minutes to finish, thus various services won't be ready to authenticate users.

- **GroupWARE skin automatically changing to new skin during upgrade**

iNODE™ v1.9.5 has a new modern skin for GroupWARE which is mobile friendly and it will be applied automatically to all users. If your users need to return to their familiar skin they can change this setting via their personal settings on GroupWARE.

Bug fixes

This release includes several bug fixes and patches of previous version 1.9.4.

The most notable bug fixes are described below:

- **Bug #2493 Enable/disable Address Book issue in Nextcloud Contacts**
In some cases, enabling or disabling an Address Book in Collaboration Suite Contacts, even if it appears to work, it actually fails as shown after a page refresh.
- **Bug #2660 File Sharepoints not accessible through Collaboration Suite when switching to A/D**
In some cases, switching the authentication backend to Active Directory would cause the file server sharepoints to appear inaccessible over Collaboration Suite.
- **Bug #2662 Brute-Force Protection issues**
In some cases, Brute-Force Protection may not work properly, causing delays at service start up and sometimes not responding to changes made to the configuration.
- **Bug #2672,2697 Dashboard not displaying properly in some cases**
The home page dashboard in Management UI was not displayed correctly. When the system's license had issues (expired or hardware changed) or in some cases where the wan interface is not properly set up (restored system backup).
- **Bug #2675 Webmail vacation filter not working**
Vacation filter may not work properly. The error would cause the stored sieve script to completely fail, causing any following rules after the failed vacation filter to be ignored.
- **Bug #2678 Sieve scripts referencing mailboxes with Greek characters do not work**
Sieve scripts (Webmail filters) generated using GroupWARE that had references to mailboxes with Greek characters (or any Unicode characters) did not work properly. The scripts would fail with error indicating that the mailbox specified was not found. The problem is now fixed but if any such scripts already exist in the system, they must be re-edited and fixed manually by their owner users. The problematic target mailbox may appear blank if the user omitted to correct the rules after upgrade.

- **Bug #2679 Restoring various backups from system ftp could fail with "unexpected error"**
Restoring various backups from files uploaded on system ftp (port 9221) could fail with "unexpected error".
- **Bug #2681 X-M2FUID header present in some emails**
In some cases, a header (X-M2FUID) would be present in messages containing the username of the authenticated user sending the email.
- **Bug #2691 Inverse network group firewall access rule not working properly**
When checking the inverse checkbox for a network group (meaning apply the firewall rule for any IP except the specified network group), the firewall rule would behave the opposite way, as if the checkbox was not checked.
- **Bug #2695 Number of active users warning**
In some cases, a warning is shown that the total number of active users would exceed the number of licensed active users in general system. This was not a problem but only a warning displayed that could just be ignored. Now, the warning will no longer be displayed.
- **Bug #2700 Brute-Force Protection service not blocking some SMTP authentication attempts**
Brute-Force Protection service would not block authentication attempts on port TCP/587. This has now been fixed.
- **Bug #2701 Webmail PGP keys missing from mail backup**
GroupWARE's public and private PGP keys, which are used to receive and send encrypted e-mails, were not included in the mail backup. This would cause the user to be unable to access previously encrypted emails on a new system, where mail was restored from a backup. Mail backup/restore now properly handles these files as well.
Compatibility note:
Webmail backup (part of Mail backup) generated on iNODE™ versions prior to 1.9.5 can be restored in iNODE™ v1.9.5 but webmail backup generated on iNODE™ v.1.9.5 cannot be restored in older iNODE™ versions (backward compatibility).
- **Bug #2704 IPsec issues with DH group 2 in proposals**
When DH group 2 (modp1024) is used in a custom IPsec proposal set, that proposal was ignored and could cause IPsec connectivity issues.
- **Bug #2705,2706 Antivirus/Antispam update may fail when set up with proxy authentication**
When the system is set up to use a proxy server with authentication, and the proxy password contains some special characters, antispam and antivirus may fail to update.

- **Bug #2708 IMAP archiving task fails with error "word too long"**
When archiving a mailbox that contains a large number of messages the task may fail with the above error message. The archiving task code has been improved to properly handle huge mailboxes.
- **Bug #2709 Quote character in CA certificate name causes issued certificates validation to fail**
A quote character in the CA certificate name would cause all issued certificates from the CA to fail validation.
- **Bug #2712 'Delete selected' functionality is not working properly in Log Maintenance pages**
In Log Maintenance pages when selecting multiple log months and clicking on 'Delete selected' would only delete one of the selected months.
- **Bug #2713 OpenVPN authentication failure after changing authentication back-end**
In some cases, changing the authentication backend has no effect on OpenVPN server, causing authentication failures.
- **Bug #2715 Collaboration Suite password change option not working**
Collaboration Suite settings provides a means of changing the user's password. This option does not work and although it reports an error, it also sends an email notification that says that the password was changed successfully which is misleading. The password changing option has been removed. The only way a user can change his own password is via User's Portal web interface in port 9237 HTTPS.
- **Bug #2716 ClamAV antivirus not updating in some cases**
ClamAV antivirus may not update properly when mail server antivirus and file server antivirus are both enabled.
- **Bug #2728 User Mailbox Size page was not showing mailboxes in other partitions**
User Mailbox Size page under Monitoring :: E-Mail Service :: Mailbox Server now includes a partition select control. The report displays the size of the storage pool occupied by each user mailbox. Note that some user mailboxes may have subfolders in different storage pools. These mailboxes will appear in multiple storage pool reports.
- **Bug #2737 Exporting certificates in p12 format may fail**
Exporting a certificate in p12 format may fail when the following conditions are both met: using a user account to log in to the administrative interface and the user's password contains some special characters (slash /). The p12 container is nevertheless successfully generated and can be manually downloaded using system ftp (port 9221).

Known Problems

Known problems in this release are:

- **Co-editing documents on file server using Collabora not available**

It is not possible for multiple users to simultaneously edit a document stored in a sharepoint of the file server which is visible on Collaboration Suite as an external folder (folder icon with an arrow over a frame). Co-editing is only available for documents on users' private folders, shared via Collaboration Suite (all other folders). When multiple users try changing the same document, a warning will notify the user that made the latest changes that the document has already changed on the server.
- **Content Delivery service authentications back-ends**

Content delivery service has no support for back-ends such as LDAP and Active-directory.
Only the local authentication back-end can be used from authentication mechanisms.
- **AVM Fritz!Card PCI Fax reception.**

We've noticed that there are reception only problems in cases where AVM Fritz!Card PCI board is used from the Fax Server. Such problems noticed only from some Fax machines (some Xerox models). These fax machines cannot sent fax to AVM Fritz!Card at all. On these cases the Fax Server will receive the message "Error no fax data was received" on real time log. We recommend using Active ISDN boards or external Fax/modems for production.
- **FAX service document preview problems**

Rarely in some cases may be not possible to preview a fax document. This problem may occur randomly with error "File does not begin with '%PDF-'" (Bug#256).
- **FAX service outgoing jobs with multiple pages**

Outgoing FAX jobs that contain more than one page cannot be previewed properly from the WEB-UI. Only the last page of the job is previewed.
- **Mail Statistics may be incorrect.**

There is a known problem on mail server statistics page where per sender or per recipient statistics may be incorrect. (BUG#268).
- **Some Real-time log lines may not appear.**

Rapid generation of log entries, may prevent some lines from being shown in real-time logs (Bug#303).
- **Shared Printer Drivers are not accessible by SMB Print Clients.**

Client printer drivers are not accessible by SMB clients as defined by iNODE™ v1.8.4 release notes.

- **Dialogic DIVA Server and AVM Fritz!Card PCI Fax conflicts.**
Do not use Dialogic Diva Server board together with AVM Fritz!Card PCI on the same system. They are conflicting on kernel CAPI stack.
- **Dialogic DIVA Server boards cannot be used for data connections.**
Due to Dialogic Diva Server boards driver changes you cannot use them for data calls yet.
- **XEN Live migration of virtual machines may fail**
Under uncertain circumstances, the VM would freeze after being landed in the target node. In that case you need to restart this VM.
- **User Management import/export incompatibilities**
User export and import files have been implemented using JSON format. Files exported from iNODE™ versions prior to 1.8.0 cannot be imported from iNODE™ versions after 1.8.0.

Hardware Support

iNODE™ is only compatible to run on 64-bit x86 CPU systems since version 1.9.0. Installing a fresh iNODE™ 1.9.x to a 32-bit machine, will fail.

iNODE™ v1.9.5 is supported to run on both BIOS and modern UEFI systems.

iNODE™ v1.9.5 Setup Tool can be run from Installation media and is working on both BIOS and EFI machines.

Hypervisor support

iNODE™ is able to run optimized and efficiently as a guest under Citrix XenServer, VMware ESXi, Microsoft Hyper-V 2012/2016 and QEMU/KVM hypervisors. Optimized drivers and management agents are automatically run on respective hypervisor environment.

In the tables below you can find recommended optimal settings and supported hypervisor Platform and features.

Virtual Machine Optimized Settings

Hypervisor	OS Type	Storage Controller	Network Controller	Optimized Console
RedHat KVM/QEMU	Linux 4.x/3.x	VirtIO SCSI/Virtio Block	VirtIO	UEFI
VMware ESXi 5.5, 6.0,6.5	Other Linux 2.6.x/3.x (64-bit)	Paravirtualized	VMXNET3	UEFI
MS HyperV 2012R2/16/19	-	GEN2/SCSI	GEN2/Network adapter	UEFI
Citrix XenServer 7.x	-	PVHVM	PVHVM	-

Virtual Machine Supported Features

Hypervisor	CPU Hotplug	Memory Balloon	Memory Hotplug	Disk Hotplug	Network Hotplug	Live Migration
RedHat KVM/QEMU	No	Yes	Yes	Yes (SCSI & VIRTIO)	Yes	Yes
VMware ESXi 5.5, 6.0,6.5	Yes (Add Only)	Yes	Yes (Add Only)	Yes	Yes	Yes
MS HyperV 2012R2/16/19	No	Yes	No	Yes	Yes	Yes
Citrix XenServer 7.x	No	Yes (PVHVM)	Yes	Yes	Yes	Yes

Hardware compatibility list

For a complete report of supported hardware please refer to the table below.

Processor Architecture	
CPU Type	X86_64 (Intel64 or AMD64) 64-bit CPU
SMP support	Yes
NUMA support	Yes
CPU technologies	Multi-core & Hyper threading support
Max CPUs	32
Memory	
Maximum RAM	2TB
ACPI	

Power Control	Power Button support
Batteries	Smart Battery System support
CPU/Thermal	CPU, Thermal zone support
Hardware support	
For a complete list of supported hardware including network interfaces, storage controllers and chipset please refer to the tables here .	

NOTE 1: Compaq's SMART2 IDA Controllers are not supported anymore.

NOTE 2: CCISS driver is removed but remains as an alias to HPSA for compatibility.

NOTE 3: MPT2SAS driver is removed but remains as an alias to MPT3SAS for compatibility.

NOTE 4: XEN PV mode is deprecated. Switch VMs to HVM mode for maximum performance.

Deprecated hardware

iNODE™ from version 1.9.x does not support the following deprecated hardware:

- Systems based on 32-bit x86 CPU
- ELSA Microlink
- Cyclades PC300
- Eicon Diva passive adapter
- Sangoma S514x PCI

Hardware Recommendations

The minimum and recommended hardware requirements to run iNODE™ v1.9.4 is shown on the following matrix.

	Minimum	Recommended
CPU	Single Core	Dual Core
RAM	768MB	4GB
CDROM	SATA/SCSI	SAS, USB
HARDSIDK	IDE/SATA 10GB	SATA 120GB
NIC	One 100BaseT	Two 1000BaseT

As a general guide for memory requirements on your system you can consult the following matrix:

	RAM requirements (MBytes)
Base System	380
DHCP Server	6
DNS Server	2 minimum – user defined cache
VPN Server – PPTP	2
each pptp connection	2,5
VPN Server – IPsec	11,5
VPN Server - L2TP	1,8
each L2TP connection	2
VPN Server - OpenVPN	25
each OpenVPN connection	2
VPN Client – PPTP	6
VPN Client – OpenVPN	4
Fax Server	10
each capi modem	2,8
each legacy modem	5
Email to fax service enabled	2
File Server	47
each CIFS client connection	9
Print Server	8
Publisher	2
each data courier connection	3
Data Courier task	6,5
Web Courier task	5,5
Mail Server	220
Replication process	25
each SMTP connection	3
each POP3 or IMAP4 connection	19
Webmail	78
Content filtering engine	80
SMTP proxy base	2

each SMTP proxy connection	2
POP3 proxy base	4
each POP3 proxy connection	4
each thread (default 3) w/o Antispam	22
each thread (default 3) with Antispam	41
ClamAV Engine	900
Collaboration Suite	512
per active user	25
Collabora Online	900
per active user	50
Proxy Server	25
Proxy RAM	user defined (20 default)
LDAP Server	130
LDAP cache	User defined (50 default)
LDAP replication	100
LDAP Proxy	35

How to install

iNODE™ v1.9.5 installation is a straight forward procedure with minimum skills required. The installation process will start after booting from the Installation media (CD, ISO or USB Boot). There are some questions about correct time/date and about hard disk preparation. The installation process will take about 15 minutes to complete. You can find more information in the iNODE™ Quick start Guide.

iNODE™ installation is bootable from USB storage devices. It currently works only with BIOS. UEFI is not supported. We suggest reading the article [here](#).

Upgrade from previous versions

ATTENTION: BEFORE PROCEEDING TO AN UPGRADE DO NOT FORGET TO TAKE A SYSTEM & DATA BACKUP ON THE RUNNING iNODE™ SYSTEM.

You can find iNODE™ v1.9.5 upgrade package from previous release v1.9.4 on the website. The system requirements are at least 768MB total physical RAM and 8GB free hard disk space. Otherwise proceed to upgrade your system disk or clean-up logs to free up disk space and upgrade RAM if needed before doing the software upgrade. Total upgrade time including reboot is about 5 minutes.

Note1: During update from 1.9.4 to 1.9.5, any patches released, that apply to version 1.9.4 are included in the 1.9.5 update package and are installed automatically. It is not required to manually install any intermediate patches.

Older versions backup files compatibility

ATTENTION: ALL BACKUP FILES ARE DESIGNED FOR DISASTER RECOVERY AND CAN BE USED FOR RESTORE PURPOSES. AFTER A RESTORE YOU WILL RECOVER THE FUNCTIONALITY TO THE LAST STATE JUST BEFORE THE BACKUP OPERATION. AS A GENERAL RULE YOU SHOULD NOT RESTORE ANY BACKUP FROM OLDER iNODE™ VERSIONS!

The Restore operations on iNODE™ v1.9.5 accepts backup files according to the following matrix:

Backup file	Version	Acceptance
System backup	1.9.5	Yes
System backup	1.x.x	No
File Backup* ¹	1.9.x, 1.8.x, 1.7.x, 1.6.x	Yes
File Backup	Other 1.x.x	No
Fax backup	1.9.x, 1.8.x, 1.7.x, 1.6.x, 1.5.x, 1.4.x, 1.3.x	Yes
Fax backup	Other 1.x.x	No
Fax archive	1.9.x, 1.8.x, 1.7.x, 1.6.x	Yes
Mail backup* ²	1.9.5	Yes
Mail backup* ³	1.9.x, 1.8.x, 1.7.x, 1.6.x, 1.5.x	Yes
Mail backup	Other 1.x.x	No

*¹ You cannot restore a File backup from release 1.9.1 or later to earlier versions before 1.9.1.

*² You cannot restore a GroupWARE backup contained in Mail backup from release 1.9.5 or later to earlier versions before 1.9.5.

*³ You cannot restore a backup from release 1.8.1 or later to earlier versions before 1.8.1.

FAQ

About Installation

Q: *What are the minimum hardware requirements in order to install iNODE™?*

A: Please see on Hardware Recommendations section above

Q: *Do I need to have Linux skills in order to install iNODE™?*

A: Not at all. iNODE™ is a software package for novice administrators. You need to boot from the Installation media. So, you need to set the appropriate PC BIOS booting sequence. After boot up there are only a few simple questions about system clock and hard disk preparation.

Q: *Can I have iNODE™ and other Operating System co-resident on the same PC?*

A: No. iNODE™ will use all system resources during normal operation. If you need to install it for demo purposes into your mobile PC you can install it as a virtual machine by using known virtual PC environments.

Q: *Can I use Installation media to upgrade from an existing earlier iNODE™ release?*

A: No. By using Installation media a fresh installation will be applied to the installed system. If you need to retain your previous settings you need to perform the upgrade via iNODE™ web interface or you should configure them manually.

Q: *Will my settings remain intact during upgrade from an existing earlier iNODE™ release?*

A: Yes. Your current settings and operating data will be retained.

Q: *Is it possible to install iNODE™ on a RAID system or a SCSI hard disk?*

A: Yes. iNODE™ supports installation on IDE P-ATA, SATA/SATAII or SCSI, SAS, RAID, SAN disk storage. You should check your storage system against the Hardware Support section above. New storage drivers are constantly added. Please contact technical support for assistance on using an unsupported storage driver; such drivers are usually validated and officially included in later software updates. Software RAID Controller (common embedded RAID controllers) is not currently supported.

Q: *Is it possible to make a copy of the iNODE™'s hard disk?*

A: No. iNODE™'s hard disk cannot be copied to another hard disk. The only way is to reinstall it via Installation media. We do not recommend installations via disk cloning. Always use the standard installation procedure.

Q: *I have the installation media. Can I install it and use it for trial purposes?*

A: The iNODE™'s installation media is the same whether you have purchased the iNODE™ system or you are installing it for trial or demo purposes. Once installed and configured through the startup wizard the system will operate for 30 days. If you decide to purchase the system then you need to purchase a license via your local reseller.

Q: *My network interface has failed. Can I replace it?*

A: Yes. Once the new network interface has been replaced you will have to contact your reseller and ask for an activation key.

Q: *I have installed iNODE™ as a virtual Machine and I need to install Optimized drivers (vmttools, xentools) in order to run optimized. How I can proceed?*

A: iNODE™ automatically installs optimized drivers during setup. By running iNODE™ it uses optimized drivers and is designed to run optimally on all known hypervisor environments.

Q: *Can I install iNODE™ on ESXi or HyperV or KVM virtualization environments?*

A: Yes. iNODE™ has been tested to run on these environments and you can install it on them as guest by booting from installation media. All appropriate optimized drivers and memory ballooning support will be used without any additional action.

General Questions

Q: *How can I obtain an Installation media?*

A: You can download the ISO image via Download section of the web site (http://www.inode.gr/support_downloads.php).

Q: *What is included in the iNODE™ support contract?*

A: It includes all software updates and support through the reseller that iNODE™ was purchased from.

Q: *I have problems with the installation procedure. Where can I get help?*

A: All support services are offered through the reseller network which is certified from the manufacturer. Through the certified reseller you can get all the assistance you might need. In case there is a major problem the reseller can contact the manufacturer and together they can give a solution to your problem.

Q: *Am I able to download the sources of OSS used by iNODE™?*

A: Yes. You can download all OSS used on iNODE™ from Download section of <http://www.inode.gr>.

Further Help

You can find comprehensive help content in each Web UI page with very detailed explanation of settings and options.

You can obtain further help and documentation on iNODE™ website <http://www.inode.gr> or by contacting to your Reseller directly.

If you have a valid support contract you can contact Dataways at:

Dataways S.A.

27, G. Scholis Ave. – GR57001 Thessaloniki – Greece

Tel. +30.2310 953953 Fax +30.2310 953963

Email: support@inode.gr



© 2021 Dataways Communications S.A.

27, Georgikis Scholis Ave. – GR57001 Thessaloniki – Greece
Tel. +30.2310 953953 Fax +30.2310 953963 – inode.gr

© 2021 Dataways S.A. All Rights Reserved

iNODE™ Connectware names and logo are registered trademarks of Dataways Communications S.A.

All other referenced trademarks and names belong to their respective owners.

Doc Rev1.2 - January 2021