

86456

VistaNET[®] 5.04 Release Notes

Version: 5.04
Release Date: June 2014
Type of Release: Production Release

Lentronics Multiplexers

JungleMUX SONET Multiplexers,
TN1U and TN1Ue SDH Multiplexers,
T1MX, E1MX and E1MXe Multiplexers



Copyright © GE Multilin 2013, All Rights Reserved

The copyright of this document is the property of GE Multilin. This document must not be copied, reprinted or reproduced in any material form, either wholly or in part, without the written consent of GE Multilin.

GE Multilin reserves the right to make changes and modifications to any part of this document without notice.

GE Multilin is not responsible for any damages or losses incurred as a result of out-of-date or incorrect information contained in this document.



TABLE OF CONTENTS

Table of Contents	2
Release Summary.....	4
Product/Component	4
Requirements.....	4
Release Details	5
New Features	5
Activation	5
Encryption	6
System Selection	6
User Authentication	7
Administrating Users.....	7
Enabling Remote Users	9
Domain Selection	10
SNMP Physical Entity and Traffic.....	10
SNMP Trap Control on Individual PCs	11
Heartbleed Bug fixed: Trac #1050	11
CDAX E1 Ring-Mode Support	12
Important Remarks:	13
Software Upgrade Procedure.....	18
Required software before upgrade.....	18
Upgrading from VistaNET version 2.25 or lower.....	18
Upgrading from VistaNET version 3.xx.....	19
Steps to upgrade VistaNET from 3.xx to 4.05.....	19
Installing VistaNET version 5.00 or Upgrading from VistaNET version 4.xx	20
Steps to INSTALL VISTANET 5.0x or upgrade VistaNET from 4.xx	20
Upgrading IPSU	21
Licensing and Activating VistaNET 5.0x.....	22
LICENSE FILE (*.lic)	22
LICENSING VistaNET	23
ACTIVATION PIN	24
ACTIVATING VistaNET	25
Replacing an Administrator account	28
Expiration of License or Activation PIN	29
Limitations.....	31



Non-VistaNET issues.....	32
Known Deficiencies	33
Fixed Deficiencies.....	37
Fixed Deficiencies - VERIFYING.....	38



RELEASE SUMMARY

PRODUCT/COMPONENT

- VistaNET version 5.04.14553

REQUIREMENTS

VistaNET version 5.04 requires the following components to be installed:

- Microsoft .NET Framework 4

VistaNET version 5.04 may be installed on to any of the following operating systems

- Windows 7 OS (recommended)
- Windows XP Service Pack 3 (for Windows XP OS)¹
- Windows Server 2008 and Windows Vista are also supported²

¹ Windows XP (not tested with any version released after 2011)

² For install procedure please contact Customer Support or refer to Windows Server 2008 or Windows Vista / Windows 7 OS installation sections in this document.



RELEASE DETAILS

NEW FEATURES

VistaNET 5.04 contains additional security features that further improve control associated with user access to Lentrionics Multiplexers. Active Directory (AD) is now fully integrated with VistaNET to authenticate users against this common and centralized directory structure. Alternatively, Local Windows™ Accounts can be used to authenticate user if AD is not employed. User credentials are no longer stored within the VistaNET database, only their Microsoft SID (security ID).

SNMP entity and traffic MIB's are now supported within VistaNET version 5.04. This optional component license (B86456-21 Traffic Manager) can be applied in nodal quantities within VistaNET to capture physical entities (units and unit ports) and all traffic carried between entities. Currently, this support is available for SONET and T1 Multiplexers.

A number of incremental improvements and bug fixes are also contained in this release of VistaNET.

The relevant system features present in previous software release include:

ACTIVATION

VistaNET 5.00 and above supports a new XML-based license format. The new licenses are digitally signed and have an expiry date. Moreover, two-factor activation is required in order to validate the new license and activate the software. In order to use VistaNET 5.00, 5.02 or 5.04, VistaNET administrators need to:

- Request a new license file
- Obtain a PIN associated paired to the license file

Once VistaNET is started, users are prompted to synchronize with the new license file (.lic). If users are upgrading from VistaNET 4.xx and if the license is valid (i.e. has not expired), the contents of the existing database are encrypted and available for use within VistaNET 5.04. The software however must still be activated with a second security factor (PIN). As users attempt to login, they will be prompted to enter the activation PIN. The PIN is provided by GE to a primary VistaNET administrator, to allow this individual to activate the software.

Distribution of the License file is recommended, but the PIN should remain private. Remote users (non-administrators) will be asked to synchronize their VistaNET service with an instance that has been previously activated. Remote VistaNET instances will be activated through synchronization (via encrypted communications).



ENCRYPTION

VistaNET version 5.00 and above encrypts all Inter-VistaNET NMS & Control data (for improved integrity and privacy).

What is encrypted?

- VistaNET Database (HC16Engine.db3)
- Peer-to-peer communication (port 8644)
- Data communication (port 8633)
- SNMP (version 3)

VistaNET is now included with security certificates located in the following folder “%ProgramFiles%\GE\VistaNET\SSL\Certs”.

Like all digital certificates, they will expire. GE has set this date to 2015, at which time the certificates would need to be refreshed, typically via the installation of a newer version of VistaNET.

What’s not encrypted?

- The communications between VistaNET and the Service Unit serial ports (craft interface ports) and any 86434-93 XPort paddleboards are not encrypted. GE’s new Cyber Secured Service Unit (available now) provides encryption between VistaNET and Lentrionics Multiplexers.

SYSTEM SELECTION

VistaNET 5.02 and 5.04 has eliminated the “System” selection (formally located in the *Administration and Startup Options*). GE’s new license file now contains the customers ‘System’ selection, either SONET/T1 or SDH/E1.

All labels displayed in the System Tree and with each unit GUI are controlled by this system setting.



The new system features now available in VistaNET 5.04 include:

USER AUTHENTICATION

VistaNET 5.04 now employs Microsoft Active Directory and Windows™ Local Accounts to authenticate users. All users currently stored in the VistaNET database will be deleted after migrating to VistaNET 5.04. A VistaNET administrator must 'pick' users from either an AD server, or locally from a pre-defined Windows™ local account. Users added from AD must now login to VistaNET with their network credentials, which are often the same login credentials used to log into their Windows Operating system.

IMPORTANT NOTE: All users currently stored in the VistaNET database will be deleted after migrating to VistaNET 5.04. User credential will no longer be stored in the VistaNET database.

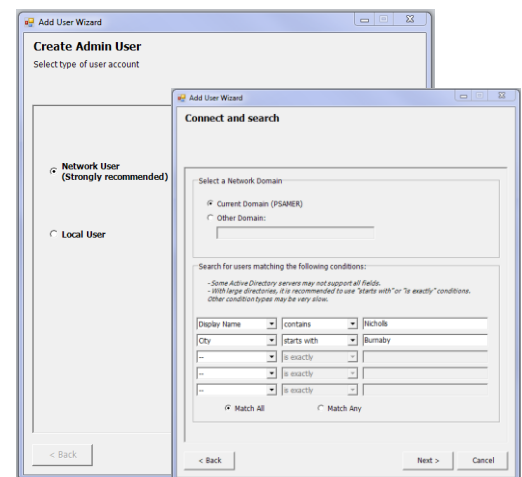
ADMINISTRATING USERS

After installing VistaNET 5.04 for the first time or upgraded to VistaNET 5.04, administrators will be prompted to create an administrator account with one picked from a Network or a Windows Local Account. For new installations of VistaNET, administrators will login with 'administrator' as the username and use the 'PIN' for the password. For customers upgrading VistaNET, administrators will login with their previous administrative account credentials.

An 'Add User Wizard' is included to help administrators add users. After selecting the source from which a user will be added, "Network" or "Local", the wizard then helps narrow the search criteria when picking from large network domains. A list of users that match the defined search parameters will be available for selection. After selection, a new administrator account is added into the VistaNET database, and locked to prevent accidental deletion. Adding a second administrative account would permit editing or deletion of the first. Non-administrative user accounts are added the same way, but a GROUP (other than administrator) must be defined.


Each user account stored in VistaNET contains a 'Display name' and a 'Security ID' value. This Microsoft generated value is uniquely assigned to each user based on their assigned username and domain. This SID is used to securely identify users. A user belonging to different domains would be assigned a different SID, and hence would require a VistaNET account to access each domain controller.

For users not contained in Active Directory service would require a Windows Local Account to access VistaNET. Please contact your IT administrator to help set one up. The VistaNET administrator will then require specific Windows account information to create this local user account, which can be extracted automatically by VistaNET.

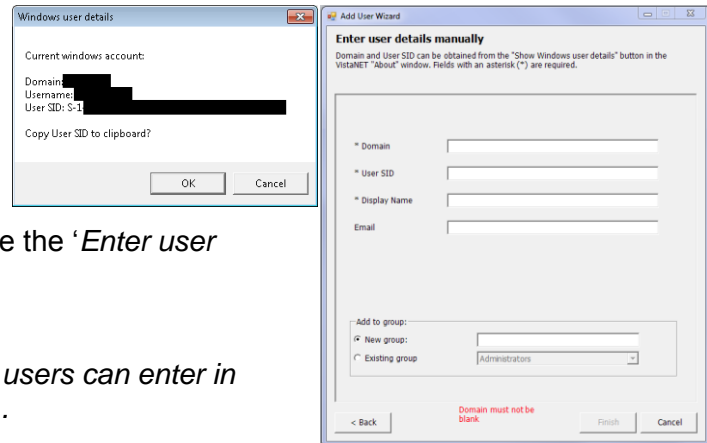




Administrating Local Users

To add a local VistaNET, an administrator will need to know that users domain and SID. Typically, administrators will need to ask the remote user for this information. From the PC where the local user will be logging into VistaNET, have the user login to their Windows account via their Windows Local Account credentials. Then have that local user VistaNET, and  select the information icon.

Have that user locate then select the “*Show Windows user details...*” button. After pressing this button, the necessary Windows user details are copied to the clipboard which can be emailed off to the VistaNET administrator. Administrator can now complete the ‘*Enter user details manually*’ for remote user account.



Note: Alternatively, from a command prompt, users can enter in “whoami /user” to obtain the same information.

Typically, adding/editing or deleting user accounts (either network or local) are performed from a central location. This allows the resulting account changes to be distributed via VistaNET synchronization to all remote VistaNET instances. To ensure synchronization is effective to remote users, Administrators must securely communicate the following to all remote users

- An IP address or host name of the centralized VistaNET service where the user accounts are stored
- User’s login instructions
 - If Active Directory: Domain name and reuse of users AD login credentials
 - If Local Windows Account: Host PC name, and reuse of users Window Local Account login credentials

Note: If firewalls are employed between central and remote VistaNET instances, please refer to the firewall section contained within these release notes.

Note: To avoid service interruptions, administrators should work with their IT departments when migration to a new domain is required. Users that are migrating to a new network domain will require a new VistaNET account linked to that domain (a new SID is needed to help authenticate users within VistaNET).

Note: All users, Networked or Local Windows accounts require a valid user password. The password field cannot be kept blank.




ENABLING REMOTE USERS

Remote VistaNET users upgrading to VistaNET 5.04 will not be able to use their previous usernames and passwords to login to VistaNET after the upgrade is complete. Depending on the new user type defined for each individual, remote users will login to VistaNET either by their company assigned network credentials (authenticated by active directory) or their windows local account credentials (authenticated by Windows™. These new user accounts must first be added into VistaNET by the VistaNET administrator.

Typically, adding the new user accounts is performed on a centralized 24/7 instance of VistaNET, and distributed to all remote users via Synchronization. In addition to communicating the type of user account defined for each user, administrators must also provide the IP address or host name of the PC where the new remote user accounts are stored. Synchronization of the data must occur to distribute the access control list to remote users.

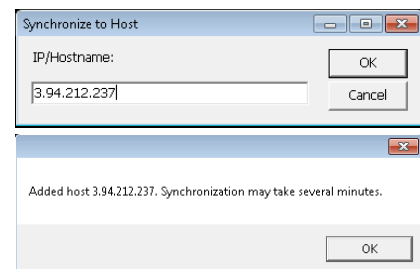
Note: VistaNET does not store user credentials, but does contain a list of 'Display names' and 'Security Identifiers' (SID). Either Microsoft's Active Directory or the local Windows Operating System will authenticate users against their supplied username and passwords.

After installing or upgrading to VistaNET 5.04, remote users can now quickly synchronize to a targeted 24/7 VistaNET service containing remote user account listings and SID's through a new "Synchronize to Host" prompt.

Remote users should press the login icon  and select "No" to "Is this the first VistaNET PC to be upgraded". This action will both activate remote VistaNET instances, and synchronize an active control list (ACL).

After a few moments, remote users can now login to VistaNET.

The IP address used to synchronize to Host will be automatically added to the list of unicast IP addresses, contained in the *Administration and Startup Options*, which VistaNET uses periodically (and upon startup) to connect with 24/7 VistaNET instances.



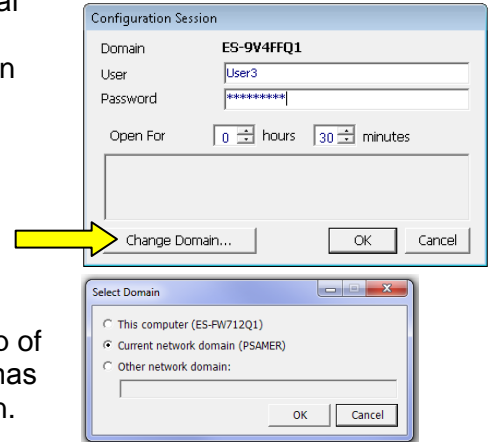


DOMAIN SELECTION

VistaNET 5.04 authenticates users against Networked or Local Windows accounts. These accounts are aligned with Microsoft's active directory or within Windows Local Accounts. VistaNET needs to know which domain the user is attempting to authenticate against. The user login prompt has been modified in this release of the software to allow users to toggle between

- Network domain preconfigured on their PC
- Local Host name of their PC
- Another domain that can be manually defined by the user

The selected Domain is presented to the user in bold text at the top of the Configuration Session dialog box. A 'Change Domain' button has been added to this same dialog box to change the selected domain.

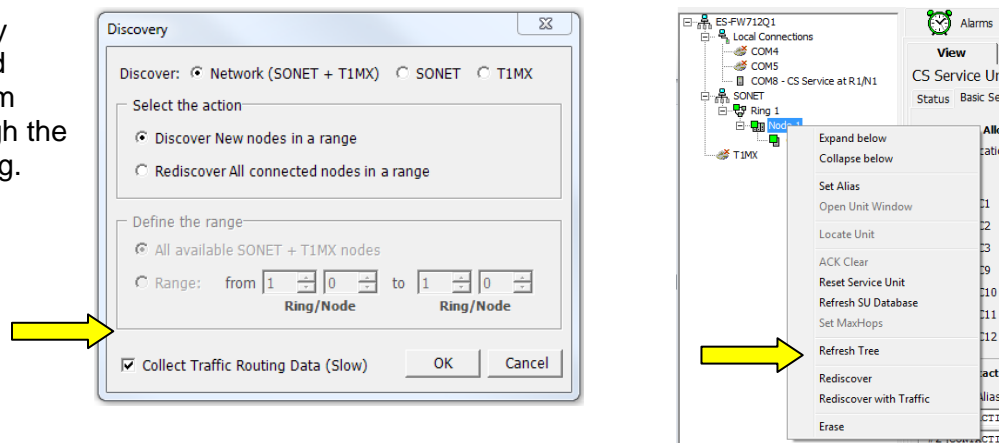


SNMP PHYSICAL ENTITY AND TRAFFIC

VistaNET 5.04 is now capable of supporting an 'Extended Discovery' (currently for SONET and T1 networks) in addition to the Unit-based discovery available up to this point. An Extended Discovery additionally captures each units' physical properties (units and ports are referred to as Entities) and the traffic that passes over and between physical entities. The extended discovery results are stored in SNMP tables, to enable SNMP-based managers to visualize the JMUX network, including inter nodal topology and intra shelf connections.

The extended discovery feature operates on a per-nodal license, controlled through VistaNET's traffic manager license (86456-21). One Traffic Manager License will allow the extended discovery of one JMUX node. Rediscovering a node with extended discovery enabled overwrites the previously stored data within the SNMP table for that node only.

The extended discovery checkbox and extended discovery via the system tree is controlled through the traffic manager licensing.





The following MIBs are required by SNMP-managers to represent Lentronics Multiplexer Entities and Traffic via an SNMP manager

1. LENTRONICS-VN-MIB, This document contains definitions for the objects for managing the VistaNET service.
2. LENTRONICS-ROOT-MIB, Contains the root OID definitions for GE LENTRONICS line of telecommunications equipment.
3. LENTRONICSMIB, The MIB describing the LENTRONICS Agent.
4. LENTRONICS-ENTITY-MIB, This MIB document contains definitions for the objects related to physical and logical entities such as traffic information.
5. LENTRONICS-PRODUCT-MIB, This MIB document contains definitions of the system object ids for LENTRONICS products.
6. ENTITY, ORGANIZATION "IETF ENTMIB Working Group, The MIB module for representing multiple logical entities supported by a single SNMP agent.
7. ENTITYSTATEMIB, ORGANIZATION "IETF Entity MIB Working Group", This MIB defines a state extension to the ENTITY MIB.
8. ENTITYSTATE-TCMIB, "IETF Entity MIB Working Group", This MIB defines state textual conventions.

SNMP TRAP CONTROL ON INDIVIDUAL PCS

VistaNET 5.04 now allows SNMP traps to be enabled or disabled on individual computers.

WARNING: This option is disabled after installation. Please make sure you manually enable this option on 24/7 PCs.

HEARTBLEED BUG FIXED: TRAC #1050

The Heartbleed bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs). This issue is fixed in VistaNET 5.04

A patch is also available for customer running VistaNET 5.00 or 5.02 and cannot upgrade to VistaNET 5.04 right away. Please contact the LENTRONICS technical services team for instructions on how to apply this patch.



CDAX E1 RING-MODE SUPPORT

The VistaNET version 5.04 implements GUI modifications for B86486-21 CDAX unit firmware v2.01 that adds support for E1MX/E1MXe ring topologies. Notable changes were made in the Main tab (PDH Mode and Timing Mode fields) and Cross-Connect tab (applicable only when PDH Mode is set to E1 Ring Master or E1 Ring Normal). Minor modifications were also made in the appearance of E1 tab's Timing Priority fields for Ports Q and P when the unit is operating in E1 Ring Master or E1 Ring Normal mode. Note that the GUI appearance for B86486-21 CDAX unit versions <2.00 has not changed.

T1Port Info									
Slot	TU#	Status	Near End			Far End		Test Bytes	
			CV	BER	Alarm @	CV	BER	XMT	RCV
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-

Clear CV Clear CV

Drop Port Info				
	Port S	Port R	Port Q	Port P
Mode	Share Drop	-	E1	E1
Status	Channel Test	-	OK	OK
Output	On-line	-	On-line	On-line
Priority	-	-	-	-
Force Off-line	-	-	-	-
Switch on RDI	-	-	-	-

Mode		Timing		Unit Monitor	
Operation	Awake	Mode	Internal	Unit Status	OK
PDH	E1 Ring Master	Source	Internal	Paddleboard	86486-61/-71
Unit Location				VCKO Voltage	1.59 V
Rack	1	Shelf	1	Temperature	35 °C
Group	2	Node	1		

***End of New Features

**IMPORTANT REMARKS:****MANAGEMENT OF THE VISTANET SERVICES**

The VistaNetService.exe has to be stopped / restarted whenever:

- A new passport/license file has been synchronized.
- There were changes in Administrative & Startup Options.
- Whenever prompted to restart VistaNET.
- When removing/upgrading VistaNET.

VistaNET.exe will start VistaNetService.exe but it will not stop it on exit. On the other hand VistaNetService.exe will close VistaNET.exe when stopped.

VistaNetService.exe has default startup option set to Manual. The PC administrators may choose to change this to Automatic (recommended for 24/7 PC used to manage the Lentronics Multiplexer system).

If a VistaNET service fails to start or if the service fails to install, reboot the computer and attempt the request again.

If VistaNetServices fails to stop from Services snap-in, at least one of the following two procedures should be able to stop it. Please use these as a last resort, since you may lose data when abruptly killing the service. A restart of the PC is then recommended.

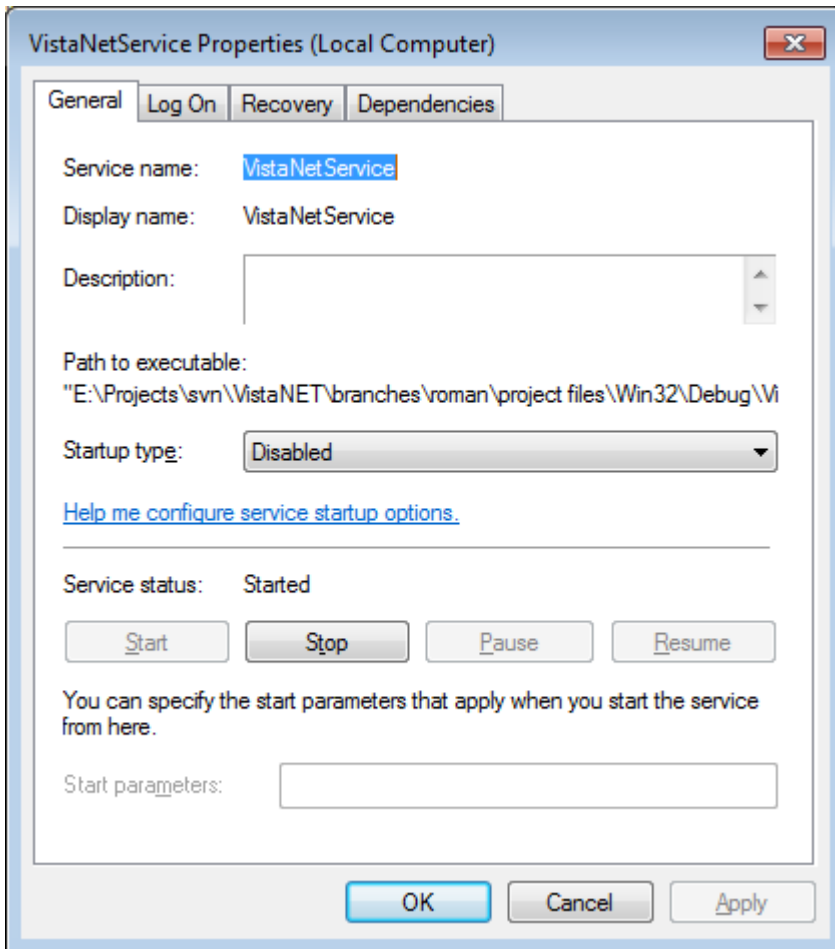
1. End VistaNetService process, which runs as SYSTEM user, from the Task Manager (running as Administrator on W7, make sure to Show processes from all users).

Image Name	PID	User Name	CPU	CPU Time	Working Set (Memory)	Memory (Private Working Set)	Page Faults	Handles	Threads	USE
wmpnetwk.exe	3636	NETWORK SERVICE	00	0:00:09	5,444 K	2,640 K	41,919	272	9	
WmPrvSE.exe	4424	LOCAL SERVICE	00	0:00:00	5,080 K	1,640 K	1,465	123	8	
winlogon.exe	572	SYSTEM	00	0:00:00	1,464 K	600 K	5,456	130	3	
wininit.exe	444	SYSTEM	00	0:00:00	160 K	112 K	1,280	79	3	
vmware-vmx.exe	5856	Roman	00	0:30:26	261,352 K	11,108 K	873,928	440	9	
vmware-tray.exe	3148	Roman	00	0:00:01	1,016 K	516 K	39,829	286	6	
vmware-authd.exe	1980	SYSTEM	00	0:02:49	1,576 K	868 K	6,674	242	7	
vmware.exe	692	Roman	00	0:00:08	3,288 K	2,064 K	45,747	371	7	
vmnetdhcp.exe	2028	SYSTEM	00	0:00:00	564 K	192 K	1,489	45	3	
vmnat.exe	1948	SYSTEM	00	0:00:00	588 K	212 K	1,414	67	5	
VistaNetService.exe	4584	SYSTEM	00	0:11:55	68,396 K	45,284 K	63,702	503	44	
VistaNET.exe	1828	Roman	00	0:03:29	125,592 K	92,396 K	909,228	575	13	2,
taskmgr.exe	5092	Roman	00	0:00:21	10,516 K	2,240 K	3,091	129	5	
taskhost.exe	2492	Roman	00	0:00:02	3,004 K	1,136 K	8,933	208	8	

Processes: 59 CPU Usage: 0% Physical Memory: 74%



2. Disable the service from Services MMC plug-in (change Manual or Automatic Startup Type option to Disabled), and reboot the computer.





WINDOWS FIREWALL

If used, the first time that VistaNetService is started, a Windows Firewall message may be generated. Ensure that the 'Private Networks' checkbox is checked and press 'Allow Access'. Active Services will now be allowed through the Windows Firewall.

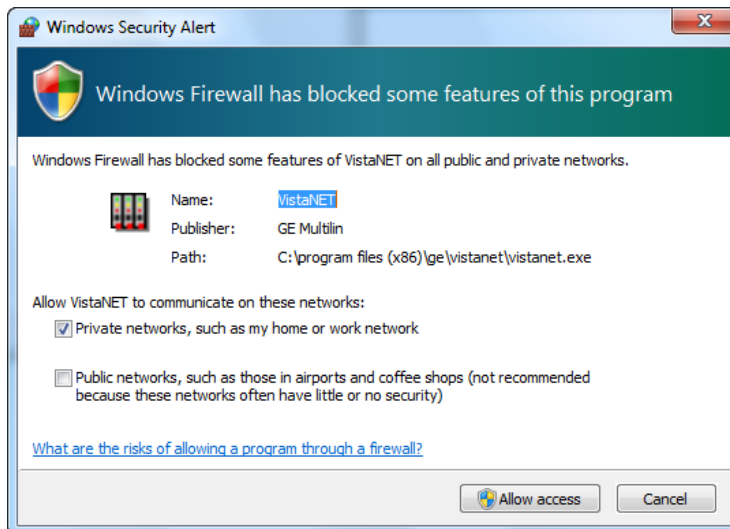


Figure: Windows Firewall

WINDOWS SERVER 2008 FIREWALL

Unlike the Windows 7 firewall setting, which prompts the user to allow VistaNetService through the firewall, in Windows Server 2008 an inbound firewall rule must explicitly be set. By default, all applications are blocked by the firewall. An inbound rule must be created to open the firewall for the specified application.

Open the Server Manager and navigate to the 'Configuration – Windows Firewall with Advanced Security – Inbound Rules'.

In the Actions panel, select 'New Rule'. This will walk the user through creating a new rule using a new rule wizard.

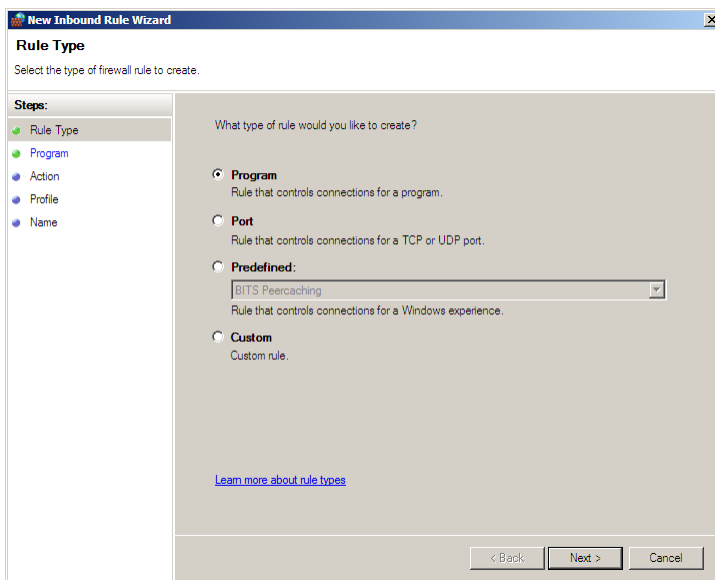


Figure: 2008 Server New Inbound Rule Wizard – Step #1 – Rule Type

Select the 'Program' option. This will allow all IP ports that are used by VistaNetService to be passed through the firewall. Press the 'Next' button.

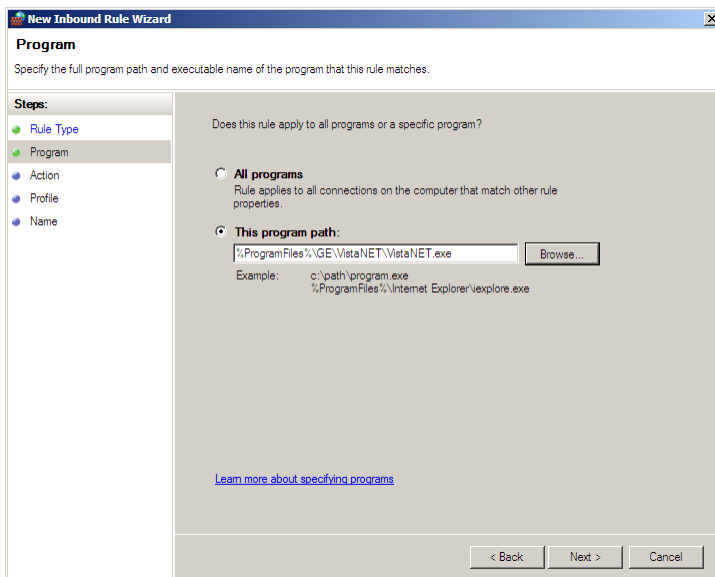


Figure: Program Path

Using the 'Browse' button navigate to the 'C:\Program Files\GE\VistaNET\VistaNetService.exe' application (32-bit) or 'C:\Program Files (x86)\GE\VistaNET\VistaNET.exe' (64-bit). Press the 'Next' button.

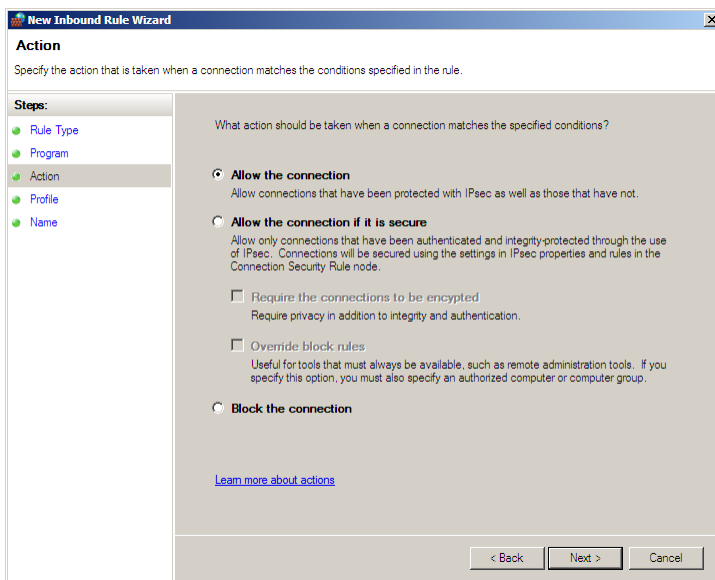


Figure: Action

Select the 'Allow the connection' option to allow the VistaNetService ports through the firewall. Press the 'Next' button.

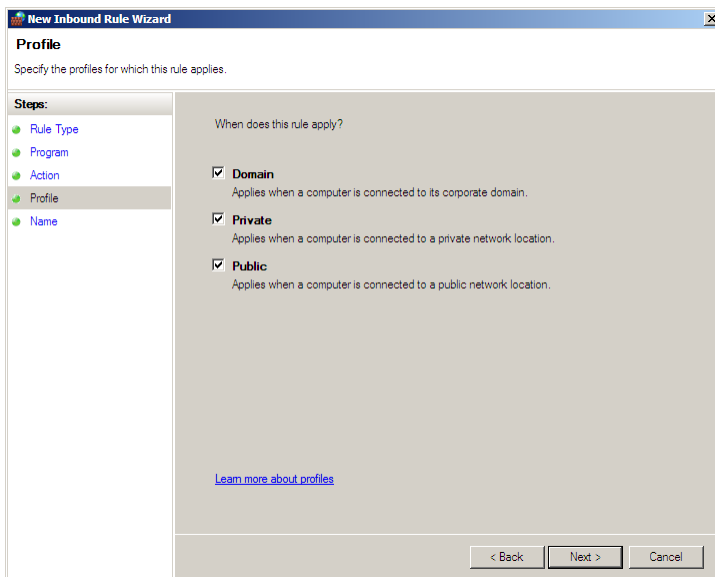


Figure: Profile

Determine on which networks the rule will apply. This rule must be applied to allow connections to any VistaNetService session used on the network.

Press the 'Next' button. The user will be requested to give the rule a name (typically VistaNET).

Press the 'Next' button to complete the rule.

The firewall rule will now apply to all users of the Windows 2008 Server. There will not be a requirement to change rules for other users (such as Standard users).



SOFTWARE UPGRADE PROCEDURE

This section focuses on upgrading your PC with VistaNET 5.04 Software.

REQUIRED SOFTWARE BEFORE UPGRADE

VistaNET version 5.04 requires the following components to be installed:

- Microsoft .NET Framework 4

UPGRADING FROM VISTANET VERSION 2.25 OR LOWER

- If you are upgrading from VistaNET versions 2.25 and below, you must uninstall the old version using **Add/Remove Programs** before installing VistaNET version 5.0x.
 - **Uninstall** is required due to the change in the installer software used.
- You must upgrade the H7Engine.dat with VistaNET4.xx before VistaNET version 5.0x will be installed, since running it will not update the H7Engine.dat file to a new format. As a result of this new install, you will not be able to revert to any previous versions of VistaNET unless you also revert to the saved version of the H7Engine.dat file by manually copying it in the corresponding VistaNET file folder.

RECOMMENDATION: GE recommends that the old database files (H7engine.dat) be removed from the program files directory after a backup is securely saved.

- After installing VistaNET version 5.0x, you must rediscover the existing network in order to populate the database with required data. This discovery is required for the nodes containing CDAX cards, to properly obtain and store CDAX Left/Right information. Also, the discovery is needed in order to obtain and store the units' Serial Number, and data used to properly refresh the tree view of your network.
- After installing VistaNET version 5.0x and connecting various VNI/VSA computers in your management network, you must let it run for at least one hour before performing any tasks. This approach will allow VistaNET to resynchronize all the JMUX/TN1U network data between the networked VistaNET computers.
- VistaNET 5.0x will not start properly if in earlier VistaNET versions you had the modem connection name or telephone number containing an ampersand (&). In this case please make sure that there are no '&' characters in the modem name(s) or numbers before installing.



UPGRADING FROM VISTANET VERSION 3.XX

If you are upgrading from VistaNET versions 3.xx, uninstalling the previous version is NOT required, but you are required to upgrade your database with VistaNET 4.xx before proceeding with the installation of VistaNET version 5.0x.

STEPS TO UPGRADE VISTANET FROM 3.XX TO 4.05

- Stop any previous versions of VistaNET
- Using Windows Explorer, go to the “C:\Program Files\GE\VistaNET\H7Engine” folder and make a backup copy of the H7Engine.dat file.
- Using a Web-browser, open <http://www.JMUX.com>
- Click on the *Existing Customers Login* button.
This is a protected site, a username and password is required
- Select the ‘*Software*’ web link
- Select ‘*VistaNET Software Download*’
- Download the *VistaNETsetup_405.msi* file to the PC’s hard drive
- Run the *VistaNETsetup_405.msi* file
- Follow the Install Shield installation instructions
- Repeat on all PC’s running VistaNET

Note: There is no need to start VistaNET 4.05. Proceed to upgrade to VistaNET 5.0x.



INSTALLING VISTANET VERSION 5.00 OR UPGRADING FROM VISTANET VERSION 4.XX

If you are upgrading from VistaNET versions 4.xx, uninstalling the previous version is NOT required.

STEPS TO INSTALL VISTANET 5.0X OR UPGRADE VISTANET FROM 4.XX

For new installation of VistaNET version 5.0x or when upgrading from VistaNET version 4.xx:

- If you are upgrading from VistaNET 2.xx or 3.xx, please read above for additional upgrade instructions
- Stop any previous versions of VistaNET (GUI and Service) before performing this upgrade
- Using Windows Explorer, go to the “C:\Program Files\GE\VistaNET\H7Engine” folder and make a backup copy of the H7Engine.db3 file. If you are upgrading from version 4.00, the location of the database is in “%APPDATA%\GE\VistaNET\H7Engine”.
- Using a Web-browser, open <http://www.JMUX.com>
- Click on the *Existing Customers Login* button.
This is a protected site, a username and password is required
- Select the ‘*Software*’ web link
- Select ‘*VistaNET Software Download*’
- Download the *VistaNETsetup_50x.msi* file to the PC’s hard drive

NOTES and RECOMMENDATIONS

1. **NOTE 1:** The new database (*.db3 file) employed within VistaNET 5.0x is additionally encrypted during the upgrade. Ensure a copy of the original (version 4.xx) db3 file is retained before the upgrade is performed
2. **NOTE 2:** All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade.
 - Run the *VistaNETsetup_50x.msi* file
 - Follow the Install Shield installation instructions
 - License and Activate the VistaNET software
 - see *License File* and *Licensing VistaNET*, and *Activation PIN* and *Activating VistaNET*
 - Repeat on all PC’s running VistaNET
3. **RECOMMENDATION:** GE recommends that the old database files (H7engine.dat and H7engine.db3) be removed (from “C:\Program Files\GE\VistaNET\H7Engine” and “APPDATA\GE\VistaNET\H7Engine” directory’s respectively) after a backup is securely saved.

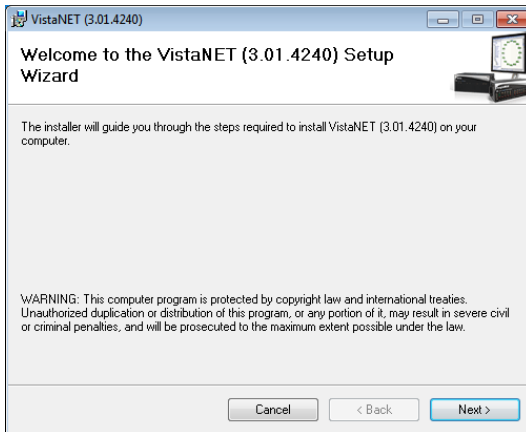


Figure: Welcome Screen

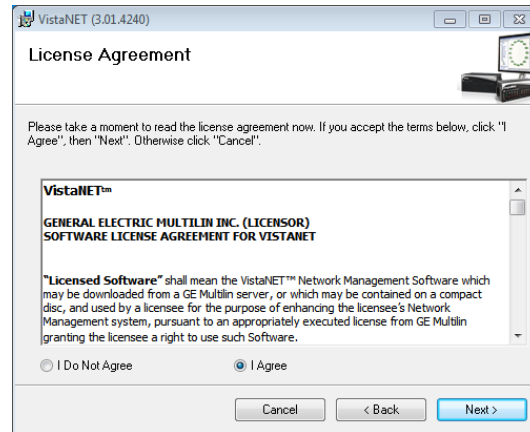


Figure: License Agreement

INSTALLATION NOTES

1. If a Windows generated User Account Control warning is seen, select 'Allow'. The installation will then complete.
2. VistaNET will be installed in the C:\Program Files\GE\VistaNET folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET folder (64-bit).

UPGRADING IPSU

VistaNET 5.04 is not supported for IPSU's. GE recommends the use of 86456-51 vSNMP (a VistaNET SNMP license) where SNMP functionality is required for Lentrionics Multiplexers), and/or the new B86434-11 Cyber Secured Service Unit (for IP connectivity to Lentrionics Multiplexers).



LICENSING AND ACTIVATING VISTANET 5.0X**LICENSE FILE (*.LIC)**

The VistaNET license file used to activate and control licensed features has been changed for VistaNET version 5.0x. A new license file (issued by GE Digital Energy) will facilitate improved security for VistaNET administrators and users in the following ways:

1. VistaNET activation requires two security factors, a license file (*.lic) and activation PIN.
2. Previous copies of the VistaNET passport (company_name.psr, .dat or .db3 files) will not successfully activate VistaNET version 5.0x.
3. The new license file contains no default username or password. Distribution of this license file is recommended and will successfully start VistaNET, but prevents equipment configuration because it contains no users or user privileges.
 - a. An Activation PIN is required to add users and privileges (typically performed on a 24/7 VistaNET service by the VistaNET administrator).
 - b. Successful synchronization to a VistaNET service containing users and user privileges is another acceptable method of activating remote VistaNET instances.
4. The license file is digitally signed, and as such, authentication is verifiable.
5. The license file also contains an expiry date (36 months by default, but configurable from 1 month to 60 months), preventing activation of VistaNET with the underlying base code, and preventing normal VistaNET operation. This will ensure that uncontrolled copies of the license file are (in time) rendered inoperable.
6. An activation PIN used to activate VistaNET expires after a defined period, preventing activation of VistaNET with the license file (3 months by default, but configurable from 1 month to 60 months).

A representative (VistaNET administrator) from each organization will need to register for a new VistaNET License file. This file is in an XML format following this naming convention "company_name.lic".

Obtaining a .LIC file: Each VistaNET administrators should register for the license file by visiting the Lentrionics Multiplexer website <http://www.JMUX.com> (recommended)

- Click on the Existing Customers Login button. This is a protected site, a username and password is required
- Select the 'Software' web link
- Select 'VistaNET Passport Registration Form'
- Complete and submit the registration form
 - Please specify desired PIN and LICENSE file expiration dates.

Alternatively, contact our customer support team at VistaNET@GE.com



GE Lentronics will create the license file (company_name.lic). A notification will be e-mailed to each VistaNET administrator indicating the passport location and integration instructions. A second factor, a security PIN, required to fully activate VistaNET version 5.0x, will be independently supplied to each primary VistaNET administrator.

Distribute the LICENSE file:

This license file can be safely distributed (recommended) to all VistaNET users that require VistaNET version 5.0x.

See 'Licensing VistaNET' below for more details on activating VistaNET.

LICENSING VISTANET

VistaNET is licensed to a company using the new license file ("company_name.lic"). After installation of VistaNET is complete, running VistaNET will prompt each user for a license file. Start VistaNET, then Browse for and Synchronize to the supplied license file.

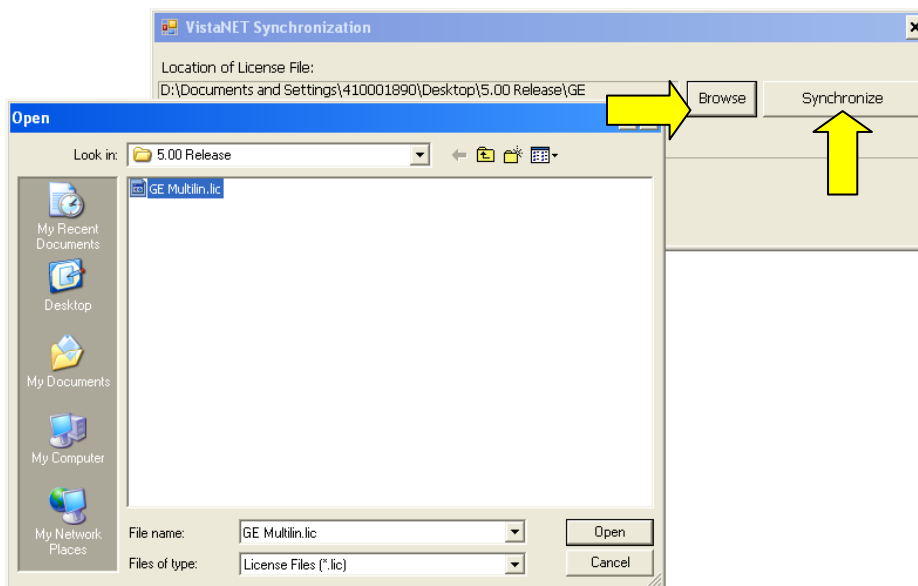


Figure: Open license file

Figure: Synchronization

After synchronization is successful, an encrypted (secure) database file (.db3) will be created and stored on C:\Program Files\GE\VistaNET\H7engine\ folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET\H7engine folder (64-bit).

VistaNET can now be successfully started; however, VistaNET 5.0x is not fully operational. No equipment configuration is permitted until a second security factory is applied.



This second security factor can be applied in one of three ways

1. Activation PIN
 - Reserved to VistaNET Administrators
2. Synchronization with an activated version of VistaNET
 - Recommended for general VistaNET users
3. Supply remote VistaNET instances with a secure db3 file
 - Recommended for remote VistaNET users without network access to a centralized VistaNET service. Windows™ administrative privileges are required.

ACTIVATION PIN

VistaNET version 5.0x requires two factors before the product is successfully activated and ready for use. The license file is the 1st factor, generated by GE and sent to a designated VistaNET administrator, then distributed internally within each organization, while the 2nd factor, an activation PIN, is also required.

While VistaNET appears to be operable without this second security factor, any attempt to configure equipment will prompt the user for this PIN.

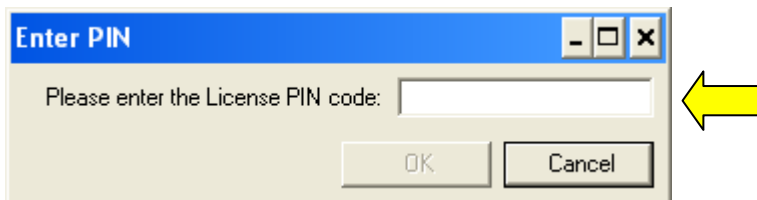


Figure: Enter Activation PIN

This activation PIN is married to the supplied license file (paired keys). Both factors are needed to successfully license and activate VistaNET 5.0x. Additionally, the license file and activation PIN are both designed to expire, protecting companies who lose control of their security keys.

RECOMMENDATION: GE strongly recommends that the activation PIN be protected, and NOT distributed.



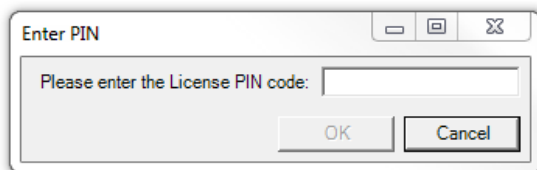
ACTIVATING VISTANET

Activating VistaNET 5.0x can be achieved in one of three ways,

1. Apply an Activation PIN (reserved for VistaNET Administrators)
2. Synchronization VistaNET with a previously activated version of VistaNET 5.0x (recommended for general VistaNET users)
3. Supply remote VistaNET instances with a secure db3 file.

1. Activation via a PIN

A VistaNET administrator who has been supplied with both security keys, can pair the license file and activation PIN to activate VistaNET 5.0x. Essentially, the pairing will permit this administrator to create an administrative user within the software. This action is performed typically once by the VistaNET administrator on a centralized 24/7 PC where the primary VistaNET service runs. The newly created administrative account has a default user name of '*administrator*' and password equal to the *activation pin*. VistaNET 5.04 will then prompt the administrator to replace this account with one picked from Active Directory or from a Windows Local Account. This step must be performed before the software activation process is successful.






2. Activation via SYNCHRONIZATION

Remote VistaNET instances may also be activated by an administrator using the activation PIN (as described above); however, this would require an administrator to apply the pin locally on every VistaNET PC. A more convenient method is recommended. Remote VistaNET instances can instead synchronization to a centralized 24/7 VistaNET instance, previously activated by the administrator.

In this case, instruct each remote user to

- Install VistaNET (provide a link to the downloaded VistaNET 5.0x installation executable),
- License VistaNET (provide a link to the company-wide license file)
- Instruct each user to press the login icon  and select “No” to “*Is this the first VistaNET PC to be upgraded?*”. This action will both activate remote VistaNET instances, and synchronize an active control list (ACL).



Configuring this IP/Hostname of a centralized VistaNET service (and/or Backup service) is an allowed setting without an activation pin. Once the remote VistaNET service connects with the centralized service, the 2nd security factor will be learned, along with the complete list of usernames, and associated access control credentials.

Please note. *The communications link between VistaNET 5.0x services is completely encrypted, mitigating man-in-the-middle attacks.*

Remote instances of VistaNET 5.0x are now fully operational.



3. Activation via secure .db3

Remote VistaNET instances may be optionally activated by supplying users with a copy of a secure .db3 file. This activation method is not typical, but suitable none-the-less when a remote user cannot synchronize with a centralized 24/7 VistaNET instance.

In this case, instruct each remote user to

- *Install* VistaNET (provide a link to the downloaded VistaNET 5.0x installation executable),
- *Instruct* each user to save a secure .db3 file into C:\Program Files\GE\VistaNET\H7engine\ folder (32-bit) or the C:\Program Files(x86)\GE\VistaNET\H7engine folder (64-bit).

Note: Providing users with this secure (encrypted) .db3 file provides them with an exact copy from the source database. Saving this file into the specified location will require Windows™ administrative privileges by the user logged into this remote PC.

Remote instances of VistaNET 5.0x are now fully operational.

LICENSING AND ACTIVATION NOTES

1. The database (*.db3 file) is additionally encrypted during the upgrade to version 5.0x. Ensure a copy of the original (version 4.xx) db3 file is retained before the upgrade is performed.
2. All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade.
3. GE strongly recommends that the VistaNET administrator protect the activation pin.
4. After the license file has expired, VistaNET will not be able to synchronize with its local license file (synchronization error). A new VistaNET license file is required from GE Digital Energy. See "Obtaining a .LIC file"



REPLACING AN ADMINISTRATOR ACCOUNT

Starting with VistaNET 5.04, all user accounts are picked from Active Directory or from a Windows Local Account. Forgetting a username / password will therefore impact a user's ability to login to their PC's Windows user account.

Occasionally an administrator needs to be replaced. If no other users had been assigned administrator group privileges, then the encrypted VistaNET database and associated users access control list cannot be modified. The administrator will need to contact GE for a new *.lic file and activation pin.

The administrator should follow these steps to regain access control

1. Contact GE Customer Service (VistaNET@ge.com) or 604-421-8610 to request a renewal of the VistaNET passport
 - a. Note: GE will send the renewed License file and Activation PIN only to the original VistaNET administrator. If requested recipient is different, GE will insist that this request be made in writing, and approved by a manager.
2. From a centrally connected VistaNET service (VNET_24/7), shut down the VistaNET application (GUI and Service).
3. Locate a remote VistaNET PC (VNET_remote) that's able to connect over IP to the production / operational VistaNET PC from step 2 above.
4. From the VNET_remote PC, open Windows Explorer, locate then rename the local database (i.e. from H7engine.db3 to H7enginedb3.old)
 - a. Start VistaNET
 - b. VistaNET will ask for a new license file. Browse for then synchronize to the new license file supplied by GE
 - c. Press the "Key" Icon (from VistaNET's top-level icons) and enter the Activation PIN
 - d. Pick a new administrator from Active Directory or from a Windows Local Account
 - e. Connect this remote VistaNET PC onto the production / operational network and enter the IP address of a known VistaNET service.

Note: *Synchronization of the two services will take place. The new "administrator" created in step 4d will be added to the active control list, and available from both sessions.*

5. Consider creating administrative designates.



EXPIRATION OF LICENSE OR ACTIVATION PIN

After a prescribed period of time, each companies LICENSE file and ACTIVATION PIN will EXPIRE. By default, the license file expiration is set to 36 months, while the activation PIN default expiration is 3 months.

A company may specify the expiration duration when GE creates these security factors. In both cases, the security key expiration can be set between 1 and 60 months.

The impact of expiring license and PIN differs.

1. EXPIRED LICENSE FILE

When a license file expires, activation of VistaNET via the license file is no longer permitted. Additionally, existing instances of VistaNET will require a new license file before it continues to operate normally.

A user or administrators should apply for a new license file well in advance of the license file expiry date. Please refer to *License File > Obtaining a new license* for instructions on requesting a new license file.

2. EXPIRED PIN

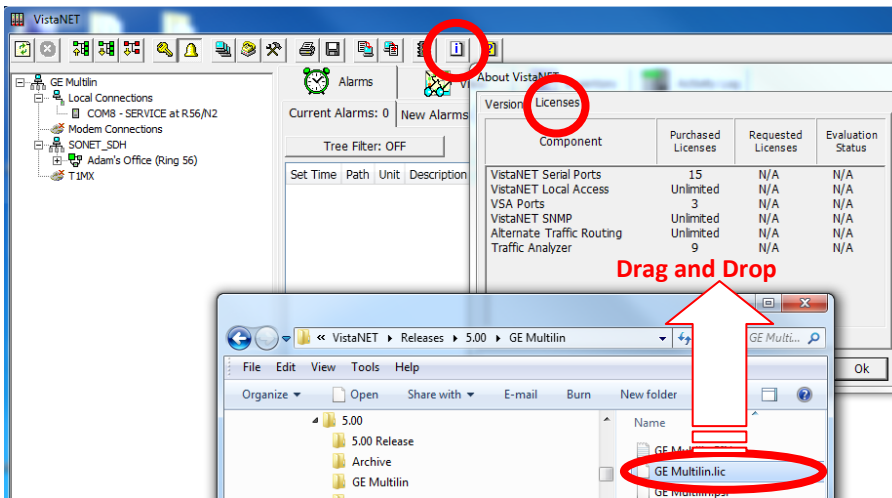
When the activation PIN expires, administrators will not be able to activate the VistaNET software via the first activation method described herein.

However, the activation PIN is typically needed just once, during the initial activation of VistaNET 5.00. The VistaNET administration team can administer users and user privileges via a valid VistaNET administrative login.

A new pin is only typically needed if an administrator loses their access password. See '*Forgot your administrative account credentials?*

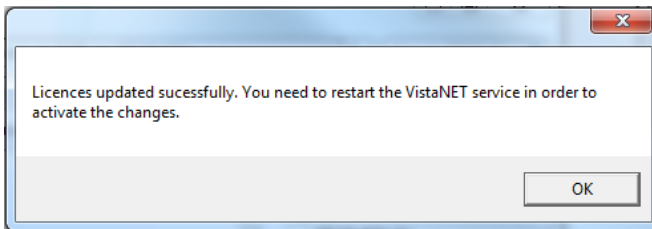
3. REPLACING AN EXPIRED LICENSE FILE

If a license file has expired, VistaNET will prompt the user to Synchronize with a valid license file. Users must request a new license file from GE, and then drag the new license file into the VistaNET Licenses tab. Please refer to *License File > Obtaining a new license* for instructions on requesting a new license file.

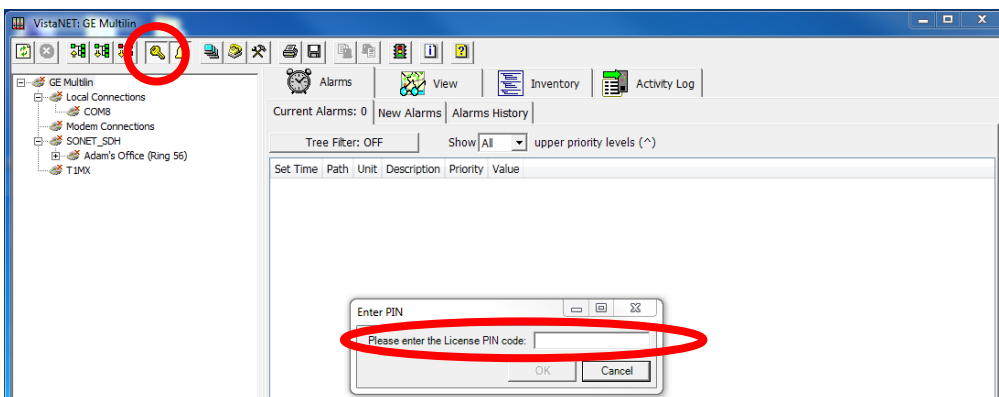


Drag the new license file into the VistaNET Licenses tab.

If the license file is valid, users will be asked to restart the VistaNET service in order to activate the changes.



After restarting the VistaNET service and the VistaNET GUI, the new license file has been successfully integrated, but will require a second security factor to activate it. VistaNET will appear inactive and completely disconnected from the equipment hardware until activation is complete.



Entering the activation pin is one of three methods described above (see *Activating VistaNET*). The primary VistaNET administrator will receive a corresponding activation PIN to enable the first instance of this new license file.



LIMITATIONS

The following is a list of known limitations related to VistaNET 5.00. A workaround was provided where applicable. Please note that these items are listed in conjunction to our tracking system ticket number.

- In VNI/VSA networks, restart VistaNET anytime the IP address of the VSA machine changes (for example, from 127.0.0.1 to the external address). Failure to do so may cause some nodes to appear as if they are visible, even if they are not, due to the node controllers for the port not being updated properly in the database. *Workaround:* Restart VistaNET after the IP address changes [ticket #269].
- After upgrading to VistaNET 3.01 and newer, it can be observed that right button in the unit view does not get selected for the pair of units. *Workaround:* Rediscover the node containing the unit. The discovery will update unit side information in the database and resolve the issue [ticket #383].
- It is not allowed to have XPort connection and Craft Interface connection to the same Service unit. If attempted, VistaNET will become unresponsive and the results might be unpredictable [ticket #322]. *Workaround:* First, remove J10 and J11 jumpers on XPort paddleboard to open serial connection to XPort, before connecting to Craft Interface. Then, replace jumpers upon CI disconnect to resume Service Unit to XPort communications.
- When using the Craft Interface to connect to units, it may be observed that Serial Number is not updated properly in the Unit Info box. If serial connection from one unit is quickly switched to another unit with similar unit type and unit option (for example, CDAX option 01) the serial number of the first one will still be shown in the Unit Info box. *Workaround:* When working the units of the same type and option, wait for the COM connection to drop before connecting to another unit or connect to a different unit type first (for example, Service unit) [ticket #293].
- When Rack/Shelf/Slot information changes through local unit configuration, the unit configuration for this unit through NMS will fail if the unit is not rediscovered to apply local changes. *Workaround:* Rediscover the unit every time its Rack/Shelf/Slot information was changed through local configuration [ticket #381].
- In a JIFshare, after physically adding a new DS-0 unit or clearing the DS-0 channel table, allow a couple minutes before initiating discovery on the node this JIFshare belongs to. The JIFshare requires some time to obtain DS-0 unit information required for discovery. If discovery is performed too fast, JIFshare may return incorrect discovery results: presents non-existing units or misses existing units. *Workaround:* If first discovery is incorrect, do rediscover to correct the issue. Or, wait for up to 1 minute before initiating discovery after making changes to JIFshare DS-0 channel table [ticket #23, #321, #345].
- For Windows 2000 users, after upgrading to VistaNET 3.01 and newer, it may be observed that the tree is empty and all previously discovered inventory, by older version of VistaNET, is missing. *Workaround:* Rediscover the entire network. Note that all aliases will be preserved and rediscovery is needed only once after upgrade [ticket #386].
- Rebooting an IPSU without a LAN connection, allowing it to finish discovery and then applying the LAN connection causes the IPSU to not obtain an IP address in DHCP mode. *Workaround:* Reboot IPSU after applying LAN connection [ticket #825].
- If ntp server time is changed abruptly, IPSU needs to be restarted [ticket #826].



NON-VISTANET ISSUES

On occasions, issues that appear to be VistaNET problems are in fact limitations associated with individual units. In some cases, the limitation may be solved with future unit firmware updates. To help users differentiate between unit firmware and VistaNET issues, the following is a list of known unit limitations that have been reported as VistaNET problems.

- 4W unit cannot copy/paste between unit firmware version 2.07 and 2.05. The paste option is reported to be not shown
Response: Copy/paste was removed by design. Significant unit firmware changes made to version 2.06 prevent copy/paste of data between units running these firmware versions
- VistaNET Map view is not clearing alarms and test indications after the L/R optics units are disabled (unchecked) from the Service Unit's GUI
Response: The Service Unit continues to respond to optical issues (alarms and tests) even after the optics units have been disabled.
- The CV count in the OC-3 Error tab does not clear the (section CV) count when Clear counter is selected to be "CV". [*ticket#418*]
- The VistaNET map (Ring view) shows unexpected alarms on the L/R optics units when AIS-L(T) and AIS-P(R) are enabled [*ticket#339*]
- Optics units that support SFP transceivers equipped with 'colored' xWDM options shall report their wavelength [*ticket#618*]

**KNOWN DEFICIENCIES**

The following is a list of known deficiencies related to this VistaNET release. The [ticket number] reflected in the GE Lentrionics deficiency tracking system precedes each deficiency. Note that these deficiencies are worked upon based on a schedule that permits the release of new and awaited features in parallel with improved and correct functionality of the VistaNET NMS system.

Ticket	Summary	Component
<u>#111</u>	<u>VNET-871: OC-XX: JIF Port tabs->Multiple JIFshares in one JIFport/slot assignment</u>	OpticUnits
<u>#161</u>	<u>Sometimes Configure and Cancel Buttons do not get enabled when a configuration is desired [Workaround: Restart or just close and re-open VistaNET and re-select the unit]</u>	Other
<u>#306</u>	<u>Modem Lockout jumper is not functional [Workaround: None]</u>	Security
<u>#425</u>	<u>J-Sync shows incorrect ssm information in some cases</u>	GUI
<u>#426</u>	<u>Occasionally an alarm status in the main tab of OC-3 is not properly refreshed</u>	GUI
<u>#483</u>	<u>STM-16: Discovered node not accurately shown when asymmetrical configurations exist on the node.</u>	Discovery
<u>#500</u>	<u>When selecting a COM port item in local connections, the "open unit window" option opens an empty GUI</u>	GUI
<u>#522</u>	<u>In T1MX Spur, Multiple T1MX trees painted when the group value at L0 is changed</u>	T1MX/E1MX
<u>#523</u>	<u>CDAXs that have their group and node number changed are not accessible anymore</u>	T1MX/E1MX
<u>#524</u>	<u>Discovery fails Intermittently after one or more nodes deleted from the discovered ring</u>	Discovery
<u>#526</u>	<u>T1MX discovery incorrectly show L0 CDAX that doesn't support T1 Spur</u>	Discovery
<u>#533</u>	<u>Audible alarm button is non functional</u>	Alarms
<u>#538</u>	<u>Ring and node number for level 0 CDAX still shows on the unit after it is relocated</u>	T1MX/E1MX
<u>#539</u>	<u>The new setting of a moved CDAX from level 0 to a level N location still accessibel from L0 icon</u>	GUI
<u>#545</u>	<u>In T1MX, the Data unit path identifier at Level 0 does not meet the requirement</u>	T1MX/E1MX
<u>#549</u>	<u>Aliases are not shown in the alarm engine "Unit path" field</u>	Alarms
<u>#578</u>	<u>Inconsistent alarm information on tree view</u>	GUI
<u>#579</u>	<u>Tree does not paint correct information on JIF-Share under OC-12</u>	GUI
<u>#583</u>	<u>VistaNET freezes during configuration when unit changes rack shelf slot info</u>	DataAccess



<u>#598</u>	<u>STM-16: Connecting TU12-structured TUG-3s to Bulk TUG-3 slots on CBW ports</u>	GUI
<u>#640</u>	<u>SRP - Alias for DS0 circuit in alarm history</u>	Alarms
<u>#691</u>	<u>Multiple unit user controls are displayed on top of each other when clicking around on the tree quickly</u>	GUI
<u>#697</u>	<u>Date drop down and "next" (>>) button are not updated when VistaNET is running for more than 1 day</u>	GUI
<u>#705</u>	<u>Order of units in Inventory XML file does not reflect the parent/child relationship of the network</u>	GUI
<u>#716</u>	<u>Nodes controlled by IPSU are not released during firmware upgrade using the Craft Interface</u>	IPSU
<u>#717</u>	<u>VistaNET Local IP display in Status Tab Does Not Update With A Change in IP address</u>	GUI
<u>#730</u>	<u>IPSU GUI: Disable fields associated with new IPSU when connected to old IPSU</u>	GUI
<u>#779</u>	<u>VistaNET does not show correct option numbers for certain TN1U/TN1Ue units</u>	GUI
<u>#780</u>	<u>4W VF Unit Loopback field not coloured in blue</u>	GUI
<u>#785</u>	<u>Dead JIF-DS1 causes bogus DS0 alarm and VT test</u>	GUI
<u>#791</u>	<u>A 4W single channel unit sometimes is displayed with left and right sides</u>	Discovery
<u>#796</u>	<u>Terminal Window does not get displayed after Modem has connected</u>	DataAccess
<u>#799</u>	<u>CDAX T1 port LOS alarm is displayed when alarm is disabled and multiple alarms exist</u>	DataAccess
<u>#803</u>	<u>Yellow text box on L0 CDAX does not appear if the unit is set as G0N0</u>	GUI
<u>#813</u>	<u>IPSU sometimes does not reset correctly when issued RESET command from VistaNET</u>	GUI
<u>#815</u>	<u>Simultaneous and differing configurations to the same JIFPort slot can corrupt optical units and hang VistaNET displays</u>	GUI
<u>#820</u>	<u>Menu bar dialog box has inconsistent behaviour</u>	GUI
<u>#821</u>	<u>Passport file company name too long for IPSU "Company Name" field</u>	GUI
<u>#827</u>	<u>VistaNET sometimes displays an exception when selecting the unit of an alarm</u>	GUI
<u>#832</u>	<u>Wrong error message for Serial-over-IP link to NMX unit</u>	GUI
<u>#833</u>	<u>VSA license checkbox is N/A to Serial-over-IP links to NMX unit</u>	GUI
<u>#839</u>	<u>Strong Arm IPSU shows wrong Processor Info</u>	GUI
<u>#846</u>	<u>Unknown publisher, VistaNET code is not signed</u>	GUI
<u>#850</u>	<u>Traffic Manager does not display E100 under OC-3</u>	GUI
<u>#852</u>	<u>VistaNET 4.00 Performance</u>	GUI
<u>#870</u>	<u>OC48 Sometimes displays "VT" in the CBW cross connect</u>	GUI
<u>#872</u>	<u>VistaNET show invalid argument during discovery</u>	GUI
<u>#885</u>	<u>CDAX reset returns (expected?) exception with hresult = 0x80591099</u>	GUI



<u>#897</u>	<u>VistaNET 4.06: IPSU GUI: Software Licensing frame always reports as IPSU0406</u>	GUI
<u>#901</u>	<u>Cannot shutdown VistaNET gracefully per services.msc method</u>	GUI
<u>#913</u>	<u>Memory Growth for VistaNET.exe GUI will cause a crash</u>	GUI
<u>#923</u>	<u>Synchronized VistaNET PC services only forward alarms from the locally monitored network and not from synchronized services, even though synchronized alarms are in the alarm engine</u>	VSNMP
<u>#926</u>	<u>Unplug CI cable while discovering a network will cause VistaNetService crash</u>	Discovery
<u>#927</u>	<u>VistaNET does not check in the background if a unit has been put to sleep.</u>	DataAccess
<u>#938</u>	<u>Alias disappearing on G703 circuits</u>	GUI
<u>#940</u>	<u>Potential race condition when attempting to add Redirected Serial over IP connections</u>	GUI
<u>#948</u>	<u>Video IO alarm not displayed in the tree</u>	GUI
<u>#950</u>	<u>Bogus NMS alarms when simultaneous Alarm, Alert (and Test) are reported from DSO level unit</u>	GUI
<u>#954</u>	<u>VistaNET should display a more meaningful error message instead of DISP E TYPMISMATCH when the company id does not match</u>	GUI
<u>#955</u>	<u>Engine ID setting on IPSU is not available.</u>	VSNMP
<u>#956</u>	<u>Nx64F is shown as Nx64 in the SNMP entry</u>	VSNMP
<u>#959</u>	<u>Expired License + PIN number license file can be made to work again by changing the time and date on the local PC</u>	Security
<u>#962</u>	<u>Unit view doesn't appear when connected to CI although unit is detected and displayed in tree</u>	GUI
<u>#965</u>	<u>Extended loss of LAN and VistaNET shutdown on PC results in IPSU not being able to synchronize when everything is restored</u>	Synchronization
<u>#967</u>	<u>Inconsistency when adding Group Name between the Users and Groups Tab of the Administration & Startup Options window</u>	GUI
<u>#970</u>	<u>Treeview not loading after improper server shutdown</u>	GUI
<u>#977</u>	<u>Alarm engine description incorrect for STS level alarms</u>	GUI
<u>#978</u>	<u>VNI client not shutting synchronization when another VNI client service is shutdown</u>	GUI
<u>#980</u>	<u>VistaNET synced with another *.lic file on network</u>	GUI
<u>#984</u>	<u>Ring Icon shows erroneous JMUX alarm status for non-existent side of linear system in System/Network Map View</u>	DataAccess
<u>#1004</u>	<u>Cannot enter CBW-Tie Table information for tied nodes on System Map View</u>	DataAccess
<u>#1021</u>	<u>Restart of VistaNET service required when PC comes back from standby or hibernation</u>	Other
<u>#1023</u>	<u>STM-16 Unit Fibre View does not display Unit and FOT Temperatures</u>	GUI
<u>#1024</u>	<u>STM-16: NMS Location cannot be properly set</u>	GUI



<u>#1025</u>	<u>STM-16: Individual VC-4 loopbacks available when AUG-4 is set for VC-4-4c mode</u>	GUI
<u>#1026</u>	<u>System Tree Labels incorrect (shows SONET & T1MX for SDH .lic file)</u>	GUI
<u>#1027</u>	<u>Multiple CBW Tie Links can be entered in Network Map View</u>	GUI
<u>#1034</u>	<u>CDAX Spur links are not present in Traffic table</u>	Discovery
<u>#1035</u>	<u>Incorrect links between VM40 units in the SNMP traffic table</u>	Discovery
<u>#1036</u>	<u>The number of traffic licenses is not checked when creating the SNMP traffic table entries.</u>	VSNMP
<u>#1038</u>	<u>Modem connections are displayed on the Local Connections tree</u>	Discovery
<u>#1042</u>	<u>IPSU Problem with VistaNET 5.xx</u>	IPSU
<u>#1043</u>	<u>Service locks up when trying to shut down while modem is connected</u>	DataAccess
<u>#1047</u>	<u>Node View does not update when status changes</u>	GUI
<u>#1054</u>	<u>JIF-E1 is not represented in SNMP traffic table</u>	Discovery
<u>#1055</u>	<u>Active Directory sometimes times out when attempting search by employee ID</u>	Security
<u>#1057</u>	<u>Removing a JVT TIE in map view</u>	GUI
<u>#1059</u>	<u>"Open Unit Window" shows invalid data when the CI connection is changed to different unit</u>	GUI
<u>#1060</u>	<u>DTT-RCV (86442-01) shows an invalid channel number in the tree and path elements</u>	GUI
<u>#1062</u>	<u>Tree shows unit as dead instead of in alarm when one or more but not all VTs/Channels are dead</u>	DataAccess
<u>#1063</u>	<u>right unit in connected CDAX pair shows as serial number for first 5 minutes after power cycling node</u>	DataAccess
<u>#1064</u>	<u>Contact I/O woken up from sleep mode displays "Invalid" channel</u>	GUI
<u>#1065</u>	<u>86485-02 JIF-Share Channel Unit Information table</u>	GUI



FIXED DEFICIENCIES

The following deficiencies were identified corrected and validated prior to this release at GE Lentrionics. They are listed here as a reference to your reported earlier problems and also as a record of the shared knowledge base with the VistaNET user base:

Ticket	Summary	Component
<u>#995</u>	<u>E1 CDAX: incorrect help messages for some fields</u>	GUI
<u>#996</u>	<u>E1 CDAX issues</u>	GUI
<u>#997</u>	<u>E1 CDAX: Hairpin-PTM GUI problem</u>	GUI
<u>#998</u>	<u>E1 CDAX GUI change for E1/optic alarm</u>	GUI
<u>#999</u>	<u>E1 CDAX: Hairpin menu should show 30 channels for E1 ports</u>	GUI
<u>#1001</u>	<u>JIF-Share: Switch on RDI is not a test condition</u>	GUI
<u>#1003</u>	<u>Add a yellow highlight when the mouse moves over the boxes to add SPE's to the CBW</u>	GUI
<u>#1005</u>	<u>CDAX-E1: correction to the paddleboard option</u>	GUI
<u>#1006</u>	<u>VistaNET 5.01.13647: Cannot start VistaNET GUI</u>	GUI
<u>#1009</u>	<u>STM-1: Add FF SFP option type (5.02)</u>	GUI
<u>#1010</u>	<u>STM-1 option 51: disable ATR for fw 1.3 or less (5.02)</u>	GUI
<u>#1012</u>	<u>CDAX T1: Invalid cross-connect between Share and Optic port modes</u>	GUI
<u>#1015</u>	<u>E1 CDAX GUI Issue</u>	GUI
<u>#1016</u>	<u>JIF-Share 86485-02 Slot CV Count Mapping</u>	GUI
<u>#1017</u>	<u>JIF-Share 86485-02 DS0 Channels tab flashing red</u>	GUI
<u>#1018</u>	<u>Ether-1000: "Contains Ether-100" checkbox is greyed out</u>	GUI
<u>#1019</u>	<u>86485-02 JIFShare Channel Unit Information Cannot Load</u>	GUI
<u>#1022</u>	<u>Discovery View does not offer any options to discover E1MX nodes</u>	GUI
<u>#1028</u>	<u>TUG3 Unit Control does not display</u>	GUI
<u>#1029</u>	<u>Hairpin does not work with CDAX optical port</u>	GUI
<u>#1030</u>	<u>"Discover" button does not become enabled when connecting to a T1/E1 spur</u>	DataAccess
<u>#1037</u>	<u>"Network" discovery sometimes skips T1 nodes on a new system.</u>	Discovery
<u>#1039</u>	<u>Cannot do local log into VistaNET on computer that has no password</u>	Security
<u>#1041</u>	<u>The currently selected unit changes when moving the CI cable to another unit</u>	GUI
<u>#1044</u>	<u>Unit Control becomes unusable after 10 minute timeout with configuration change</u>	GUI
<u>#1046</u>	<u>Cannot access sleeping CDAX unit</u>	DataAccess
<u>#1048</u>	<u>Progress bar for discovery does not always get displayed correctly and flickers during discovery</u>	GUI
<u>#1049</u>	<u>GUI does not switch properly when craft interface cable is moved to a different unit</u>	GUI



#1050	<u>VistaNET needs to apply OpenSSL 1.0.1g patch to remove Heartbleed bug vulnerability</u>	Security
#1052	<u>Copy & Paste does not work as expected (observed on STM-4 unit)</u>	GUI
#1053	<u>"Reset Service Unit" and "Refresh SU Database" commands are not working</u>	GUI

FIXED DEFICIENCIES - VERIFYING

The following deficiencies were identified corrected prior to this release at GE Lentrionics but validation of the issue continues. These issues remain open. They are listed here as a reference to your reported earlier problems and also as a record of the shared knowledge base with the VistaNET user base:

<u>Ticket</u>	<u>Summary</u>	<u>Component</u>
#736	<u>GigE: SDH terminology</u>	GUI
#776	<u>Rename STM-1 label to Aggregate</u>	GUI
#806	<u>JIF-DS1/Quad-DS1: VistaNET would not let put JVT-S in service</u>	GUI
#936	<u>Change prioritization of Contact I/O unit status alarms</u>	GUI
#958	<u>Activation and Operation with Expired .lic file and Activation PIN</u>	Security
#968	<u>86439-21/31 (E1) GUI does not correctly configure the Shelf Number in the Unit Location Frame</u>	GUI
#982	<u>Ether-1000 QVLAN Filtering</u>	GUI
#983	<u>Ether-1000 Line Setup - TDM Topology</u>	GUI
#988	<u>SPE-JIF 02 is missing JifPort=4 info in the Jif Port fields (and xml values)</u>	GUI
#1000	<u>Jif-Share 02: missed items in new JIF Share VistaNet</u>	GUI
#1002	<u>Improper STS-1 alarm prioritization & description in Alarm engine</u>	GUI
#1007	<u>CSSU: Implement Contact Input Alerts functionality</u>	GUI
#1008	<u>CSSU: Add Unit Mode field to the Status tab</u>	GUI
#1011	<u>E1000: In VLANs tab, cannot allow ingress of tagged frames for Q-Access ports</u>	GUI
#1013	<u>CDAX: incorrectly shows SFP info when unit is in sleep mode.</u>	GUI
#1014	<u>86432-41/-51 GUI does not show current with DD multimode SFP</u>	GUI
#1040	<u>Cannot access L0 elements from standalone network when SONET/SDH inventory is present</u>	DataAccess
#1045	<u>Strange exception when discovering a range that has a start node of zero and a non-zero end node</u>	GUI
#1056	<u>Newly provisioned CMUX unit CBUS ports are not selectable in CMUX's "Show TU-11" via NMS</u>	GUI