

86456

VistaNET[®] 5.08 Release Notes

Version: 5.08
Release Date: April 2016
Type of Release: Production Release

Lentronics Multiplexers

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



Copyright © GE Multilin 2016, 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GE Multilin is not responsible for any damages or losses incurred as a result of out-of-date or incorrect information contained in this document.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
 - 24/7 VistaNET PC..... 5
 - Certificates Handling 7
 - UNIT Configuration Backup And Traffic Analyzer..... 8
 - DTT (B86441-42) Unit GUI..... 11
 - 4W VF E&M (B86444-08 / B86444-28) Unit GUI..... 12
 - SNMP Support 13
 - Activity Log 14
 - License and Certificates Expiration Notification 15
- Important Remarks 17
 - Management of the VistaNET Services 17
 - Firewall..... 19
 - Windows Firewall..... 19
 - Windows Server 2008 Firewall..... 19
- Software Upgrade Procedure..... 22
 - Required software before upgrade..... 22
 - Upgrading from VistaNET version 2.25 or lower..... 22
 - Upgrading from VistaNET version 3.xx..... 22
 - Steps to upgrade VistaNET from 3.xx to 4.05..... 22
 - Installing VistaNET version 5.08 or Upgrading from VistaNET version 4.xx 23
 - Steps to INSTALL VISTANET 5.08 or upgrade VistaNET from 4.xx 23
 - Upgrading IPSU..... 24
- Licensing and Activating VistaNET 5.0x..... 25
 - License File (*.lic) 25
 - Licensing VistaNET..... 27
 - Activation PIN..... 28
 - Activating VistaNET 28
 - Activation via a PIN 28
 - Activation via Synchronization 29



Activation via secure .db3	30
Licensing and Activation Notes	30
Replacing an Administrator Account.....	30
Expiration of License or Activation PIN	31
Impact of expiration	31
Replacing an ExpiRed License File or Add a new License	32
User Authentication	33
Administrating Users.....	33
Domain Selection	36
Limitations.....	37
Non-VistaNET issues.....	39
Known Deficiencies	40
Fixed Deficiencies	44
Fixed Deficiencies - VERIFYING.....	45



RELEASE SUMMARY

PRODUCT/COMPONENT

- VistaNET version 5.08.16316

REQUIREMENTS

VistaNET version 5.08 requires the following components to be installed:

- Microsoft .NET Framework 4

VistaNET version 5.08 may be installed on to any of the following operating systems

- Windows 7 OS (recommended)
- Windows 8 OS
- Windows 10 OS as non-24/7 VistaNET PC
- Windows Server 2008
- Windows Server 2012 as non-24/7 VistaNET PC

Note: Windows XP Service Pack 3 and Windows Vista are NOT Supported.



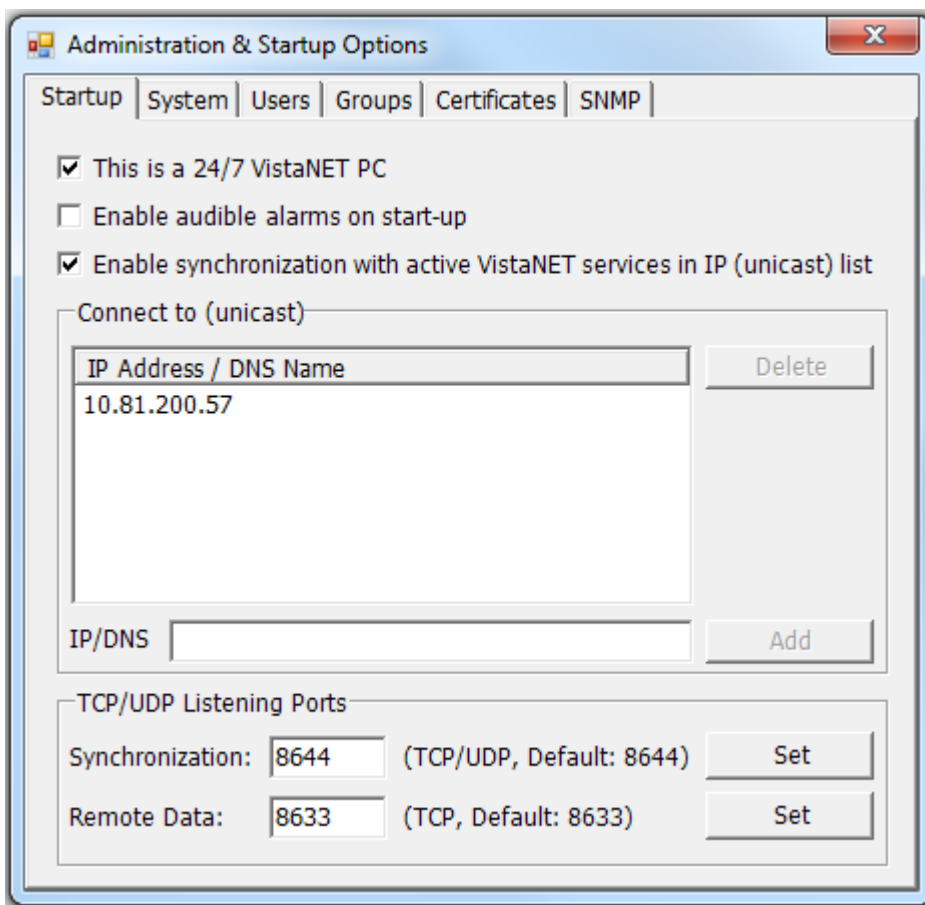
RELEASE DETAILS

NEW FEATURES

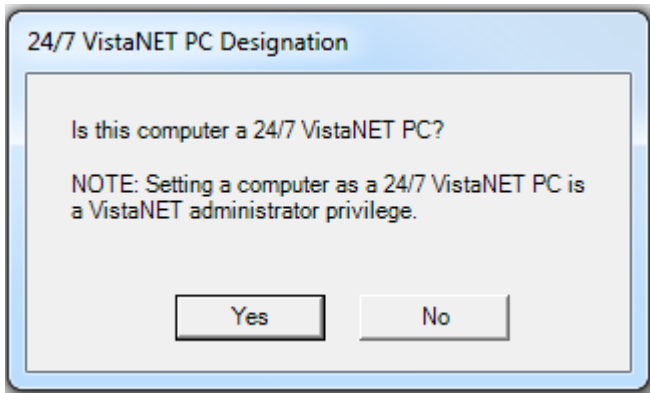
The new system features present in this software release version are:

24/7 VISTANET PC

The 24/7 VistaNET PC designation is added to VistaNET 5.08, replacing the “Disable Local Connections & Synchronization on VistaNET GUI Shutdown” checkbox in the Administration & Startup Options dialog.



On the first run, VistaNET 5.08 (or higher) will ask if the PC will be designated as a 24/7 VistaNET PC. This option can be changed at any time from the Startup tab.



A PC designated as a 24/7 VistaNET PC will not release the COM ports when VistaNET GUI shuts down. There are additional restrictions imposed on a 24/7 VistaNET PC, where modifying these configurations will require VistaNET administrator:

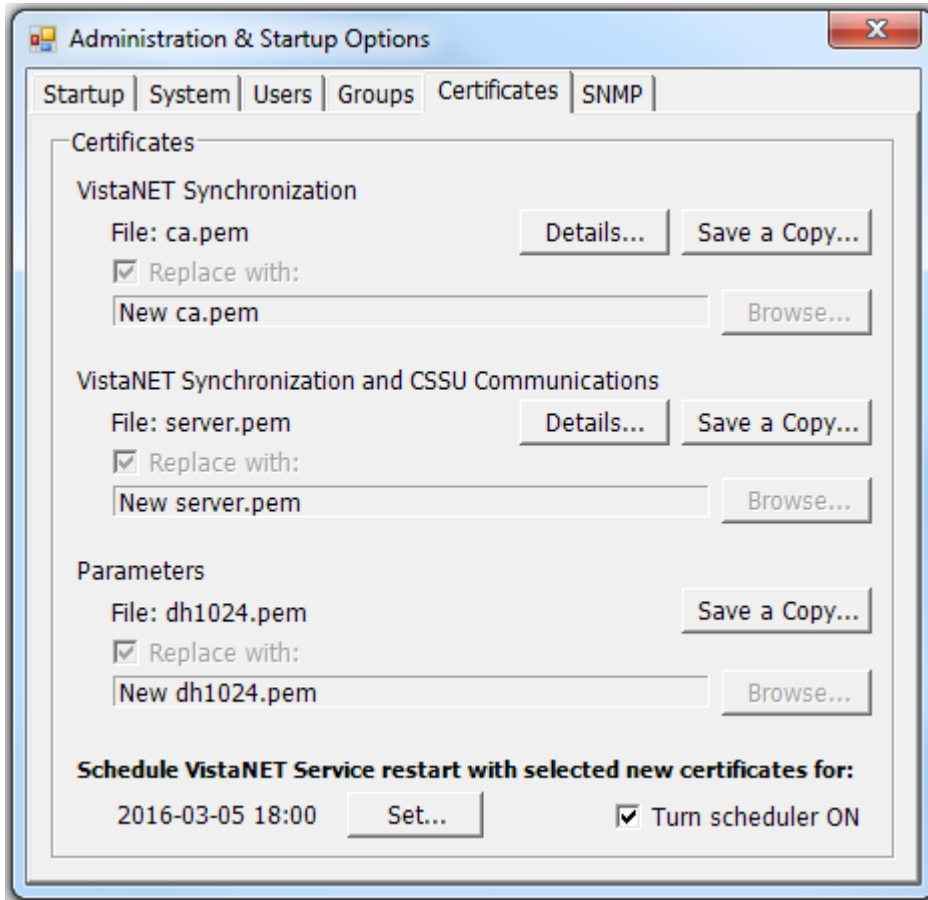
- Administration & Startup Options dialog
 - Startup tab:
 - “This is a 24/7 VistaNET PC” checkbox.
 - “Enable synchronization with active VistaNET services in IP (unicast) list” checkbox.
 - “TCP/UDP Listening Ports”.
 - Certificates tab:
 - “Replace with:” checkbox.
 - “Set...” button.
 - SNMP tab:
 - All configurations.
- Serial Connections dialog: any changes (add, delete, edit) in this dialog will require VistaNET administrator password when the Apply, Dial or Hang Up button is clicked.



CERTIFICATES HANDLING


The new Certificates tab in Administration & Startup Options dialog provides a way to save the currently used certificates, and to replace them.

When multiple instances of VistaNET are used, replacing the certificate files has to be performed to each and every PC where VistaNET is used. Because replacing certificate requires VistaNetService to be restarted, the process across all PC can be scheduled to take place at a convenient time to minimize the disruption.





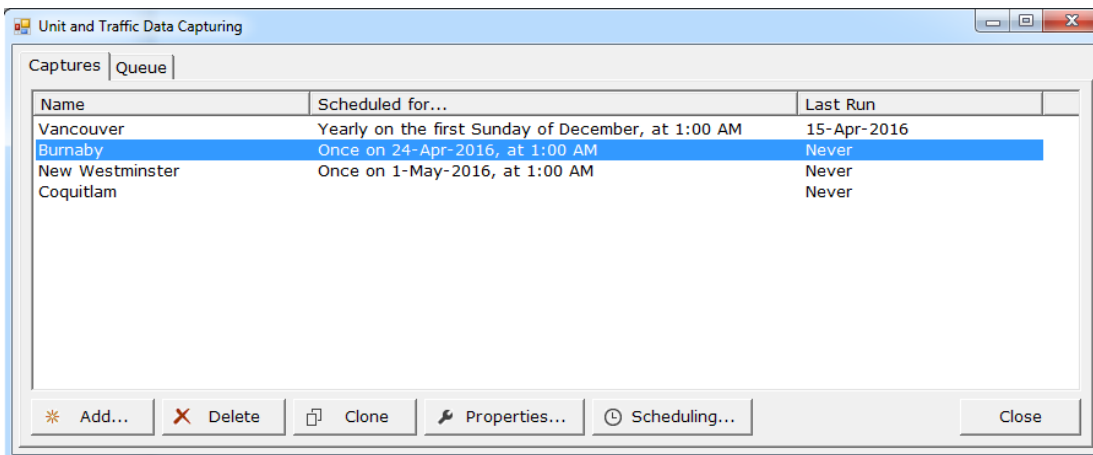
UNIT CONFIGURATION BACKUP AND TRAFFIC ANALYZER

VistaNET 5.08 adds a new feature to create backup of multiple unit's configuration (.vux file). The feature can be accessed by clicking on the camera icon () from the system icon toolbar.

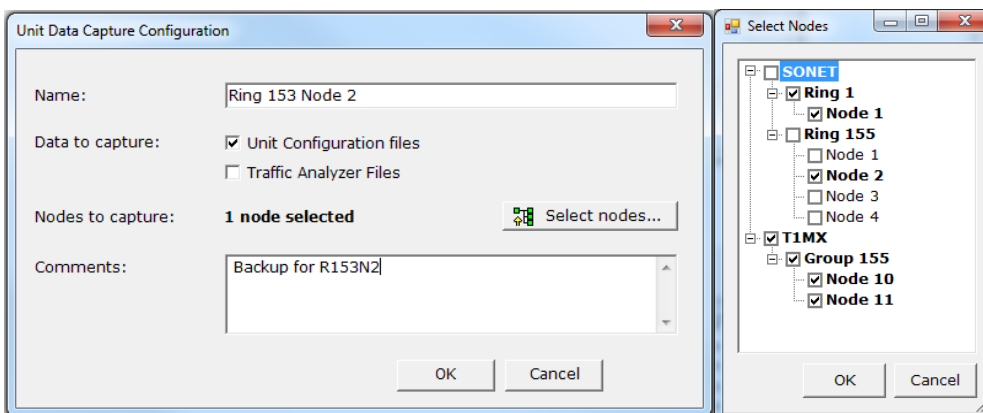


The camera icon combines Traffic Analyzer and Nodal Configuration Backup into one dialog.

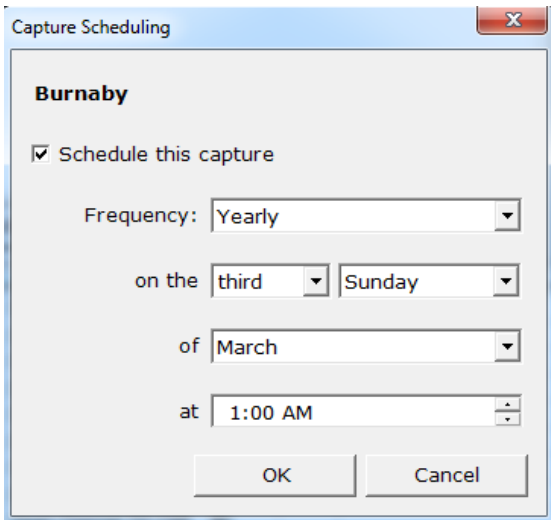
To perform a backup or traffic analyzer, create a “capture” by clicking on the camera icon and hit the Add button. A capture defines the configuration such as whether it covers the whole or selected network, rings, or nodes, and when the capture will be run.



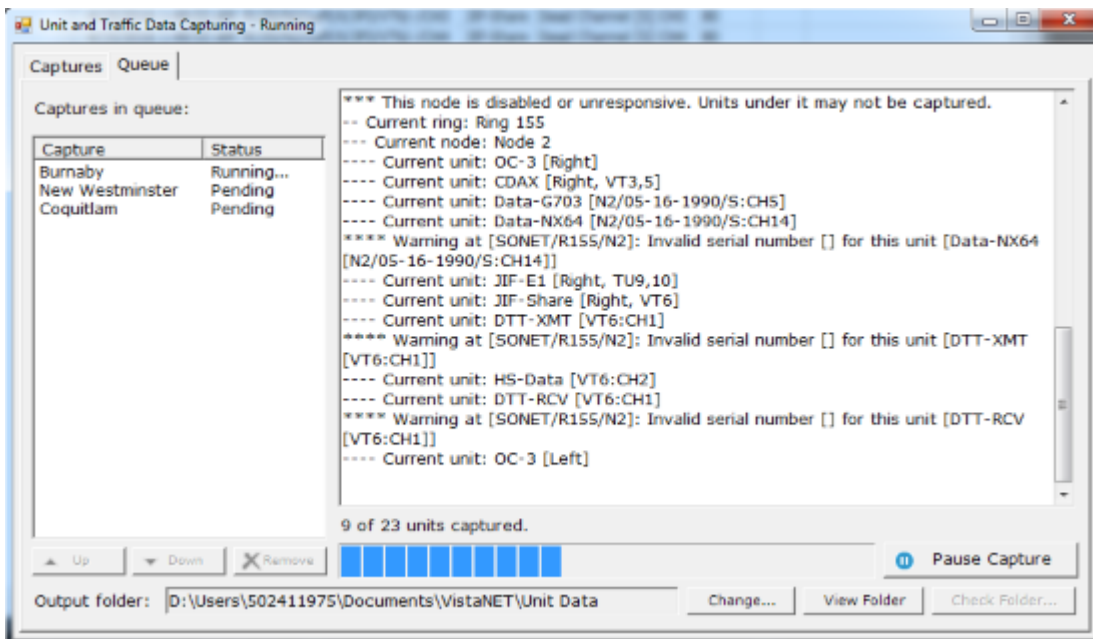
After specifying the capture name, and selecting what type of data to capture (unit configuration or traffic analyzer), select the network/rings/nodes to capture.



To run a capture immediately, right click on the capture name and select “Run”. To schedule a capture, click on the “Scheduling...” button.



While a capture is running, progress will be displayed and a summary will be provided at the end. A detailed report is available and saved in the specified output folder.



Multiple captures can be queued, and a pause/resume button allows for captures to be paused until a more convenient time.

A “Check Folder” button allows the user to check if there are any units that have not yet been backed up.



LICENCING

The Unit & Traffic Data Capturing feature is bundled into the Traffic Analyzer license.

Traffic Analyzer is licensed on a per-node basis. You will require one license for every node you wish to back-up. Please contact your VistaNET sales representative for more information on obtaining this license.

If you have insufficient licenses to cover your entire network, nodes will be licensed in the following order:

- Lowest ring/group number, then
- Network (SONET/SDH before T1MX/E1MX), then
- Lowest node number.

IMPORTANT NOTES

- Captured data is stored only on the local computer. It is not synchronized over the VistaNET network. For this reason, it is recommended to capture the entire network on the 24/7 VistaNET computer, so you have a centralized storage of unit data. If network access to these files is desired, an admin could either share this folder over the network, or set up a task to synchronize these files to some other network location.
- The Unit & Traffic Data Capturing window cannot see undiscovered nodes. You must first discover all nodes you wish to capture.



DTT (B86441-42) UNIT GUI

GE's release of a new Direct Transfer Trip unit (B86441-42) is now available for Lentrionics Multiplexers. The new unit replaces all legacy DTT transmit units (B86441-xx) and DTT receive units (B86442-xx). Both units are shipping with release 1.00e firmware supporting the following features

- 2 full duplex commands channels per DTT unit (each consuming a single 64kb/s channel)
- Each Transmit and Receive command channel supports both a main and auxiliary interface for improved dependability
- Units occupy two shelf-slots on a CBUS
- 3 keying loop voltages supported, 48VDC, 130VDC or 250VDC
- Adjustable spurious trip immunity, 1ms increment to 20ms
- BC96 address circuit addressing that ensures end-to-end circuit and continuous integrity monitoring for high dependability and security
- Unit 'sleep mode' of operation to minimize the impact of enabling a misconfigured unit.
- A series of new DTT paddleboard (86441-93, -95, -97) are available for each of the supported keying loop voltages 48VDC, 130VDC and 250VDC respectfully [JMUX/TN1U/T1MX & E1MX].
- A series of new DTT paddleboard (86441-73, -75, -77) will be available Q3 2016 for each of the supported keying loop voltages 48VDC, 130VDC and 250VDC respectfully [TN1Ue & E1MXe].
- Form-C alarm relay for unit and per loop Form-C relay for port monitoring
- Supports test monitoring for end-to-end and local circuit monitoring through the optional DTT test panel
- Two firmware images, active and standby

The new DTT units can interoperate with legacy versions of the DTT cards and DTT test panels. For example, a DTT XMT unit at node A can establish a DTT circuit with a new DTT Tx/Rx unit at node B. Similarly, a new DTT Tx/Rx unit at node A can establish a DTT circuit with a legacy DTT Rcv unit at node B. Additionally, a CBUS can also accommodate both legacy and new DTT units as long as unique 64kb/s channels are assigned.



4W VF E&M (B86444-08 / B86444-28) UNIT GUI

GE's release of a new single channel 4W unit (B86444-08) and quad channel 4W VF unit (B86444-28) is now available for Lenronics Multiplexers. The single channel 4WVF unit replaces all legacy single channel VF units (B86444-04/05/14/15) while the quad channel 4WVF unit replaces GE's legacy dual channel unit (B86444-26). Both units are shipping with release 1.00e firmware supporting the following features

- 1 or 4-port 4WVF circuits both support Type I-V E&M, however external battery connections required for select signaling types.
- Transmission Only (TO) mode is supported when no E&M signaling conditions are established to the unit paddleboards
- Single channel unit is compatible with legacy paddleboard (86444-90 & -91 for TN1U/JMUX/E1MX and T1MX product lines; 86444-72 for TN1Ue/E1MXe product lines)
- Ch 1-2 ports of the Quad channel unit is compatible with legacy paddleboards also
- Custom signaling pattern available allowing BITS A, B, C, D that carrying VF signaling (On/Off hook) to be controlled
- Transmit levels -17.5 to +6.5 dBm
- Receive levels -11.0 to +13.0 dBm
- Built-in 1kHz test tone generator
- Configurable u-law / A-law PCM coding
- Local and Line Loopbacks for "circuit" testing
- BC96 address circuit addressing that ensures end-to-end circuit alignment
- Unit 'sleep mode' of operation to minimize the impact of enabling a misconfigured unit.
- Two firmware images, active and standby
- A new Quad-channel paddleboard is also available (86444-96 for the TN1U/JMUX/E1MX and T1MX product lines; 86444-78 for the TN1Ue & E1MXe product lines)

The new single-channel and quad-channel units can interoperate with legacy versions of the 4WVF cards. Additionally, a CBUS can accommodate both legacy and new 4WVF units as long as unique 64kb/s channels are assigned. Each new 4WVF card occupies a single shelf slot.



SNMP SUPPORT

With the release of DTT (B86441-42) and 4W VF E&M (B86444-08 / B86444-28) units, the MIB files for channel unit data-points have been updated to support these new units:

- LENTRONICS-JMUXTN1U-CHANNEL-TC
- LENTRONICS-JMUXTN1U-CHANNEL

These files can be downloaded from www.jmux.com.



ACTIVITY LOG

VistaNET 5.08 provides more activity logging information. The following events are now being logged into the Activity Log:

1. Viewing, saving and replacing certificates,
2. Adding, editing and deleting serial connections,
3. Modifying Startup configuration under Startup tab of Administration and Startup Options,
4. Modifying SNMP configuration under SNMP tab of Administration and Startup Options,

In addition, the Activity Log Filter has been expanded to include new categories:

- Certificate,
- Admin Config

Alarms View Inventory Activity Log

<< Show History Showing 0 of 28 entries (Network) From Mar 22 14 days << >>

Tree Filter: ON

Include following categories

- Startup
- Log In/Out
- Unit Config
- Discovery
- Erase
- Unit Reset
- User Config
- Certificate
- Admin Config

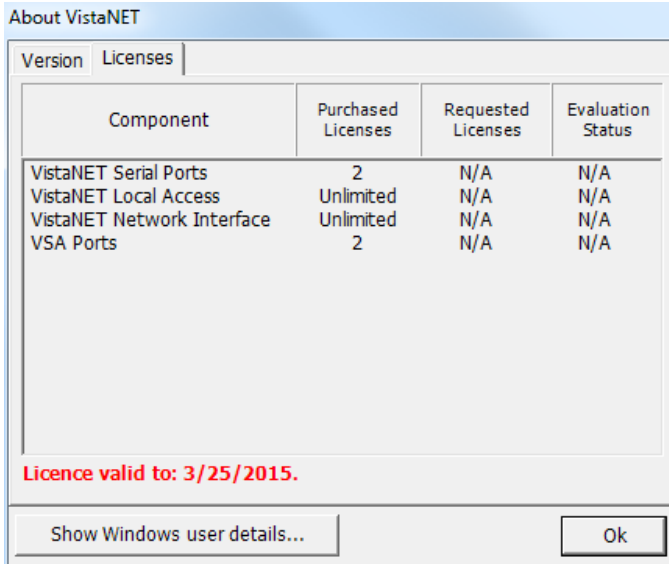
Text Searches (partial matches accepted)

- User
- Unit CDAX
- Description
- Details

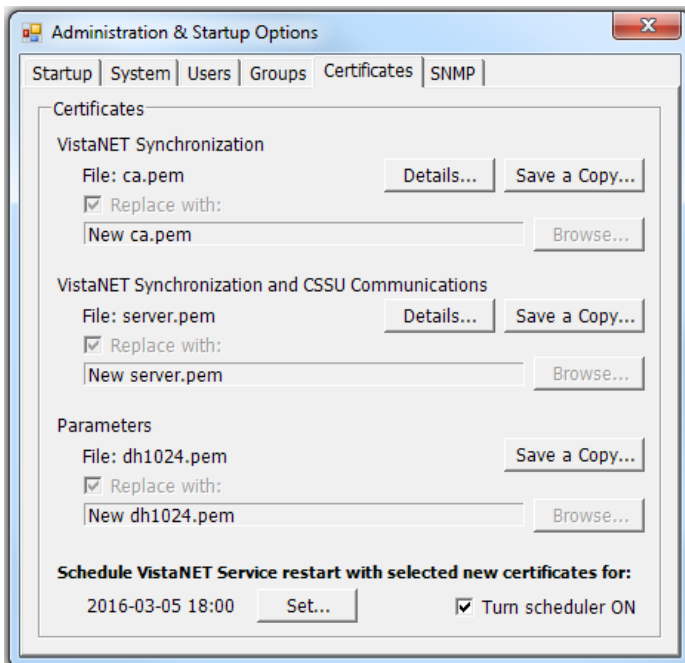


LICENSE AND CERTIFICATES EXPIRATION NOTIFICATION

VistaNET notifies users when the digital certificate associated with the License file is about to expire. Each license file will expire within a 36 month period after it has been created. Each organization will need to contact GE and request a new license file. Users can also see the expiry date through the About dialog box (accessed through the 'Information' icon)

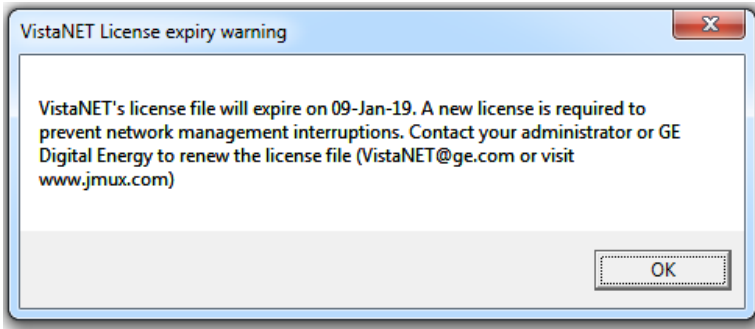


VistaNET also notifies users when the X.509 certificate is about to expire. The certificate's expiry date can be verified by opening the Administration & Startup Options dialog box (🔧 icon), selecting the Certificates tab, and clicking on the Details... button.





VistaNET will provide one warning every 24 hours when there is 14 - 60 days remaining, and one warning every six hours when there is less than 14 days remaining.





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 Lentrionics 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.

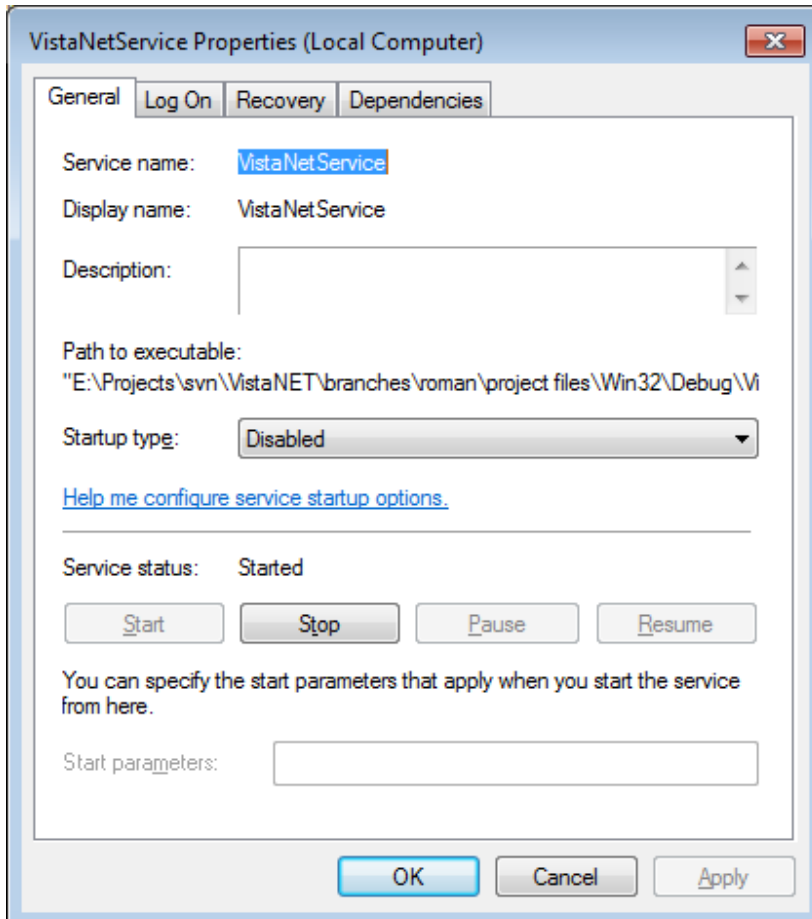
1. End VistaNetService process, which runs as SYSTEM user, from the Task Manager (running as Administrator on W7, make sure to Show processes from all users).

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	
WmiPrvSE.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.





FIREWALL

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.

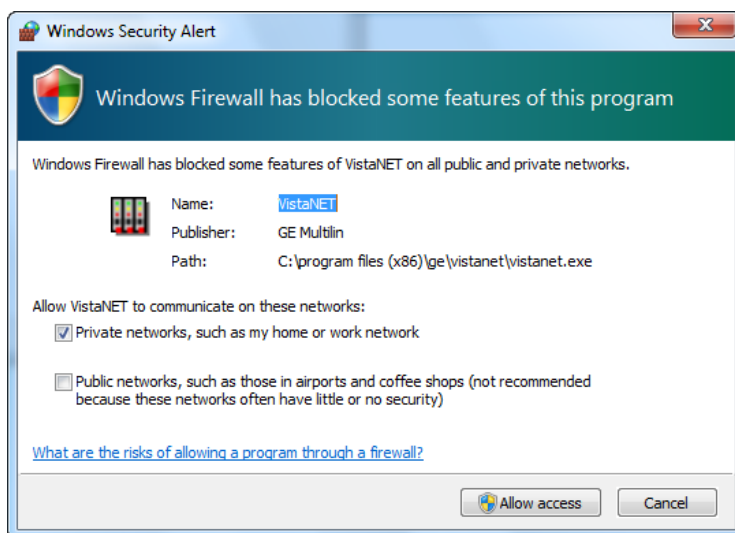


Figure: Windows Firewall

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.

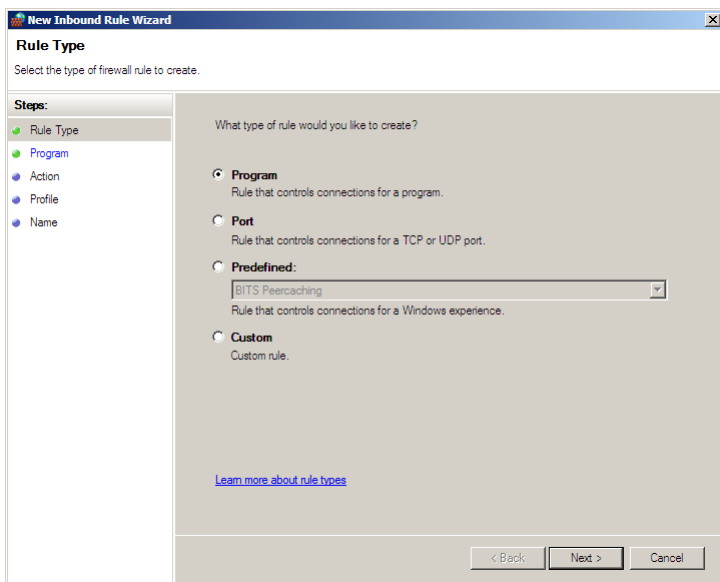


Figure: 2008 Server New Inbound Rule Wizard – Step #1 – Rule Type

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.

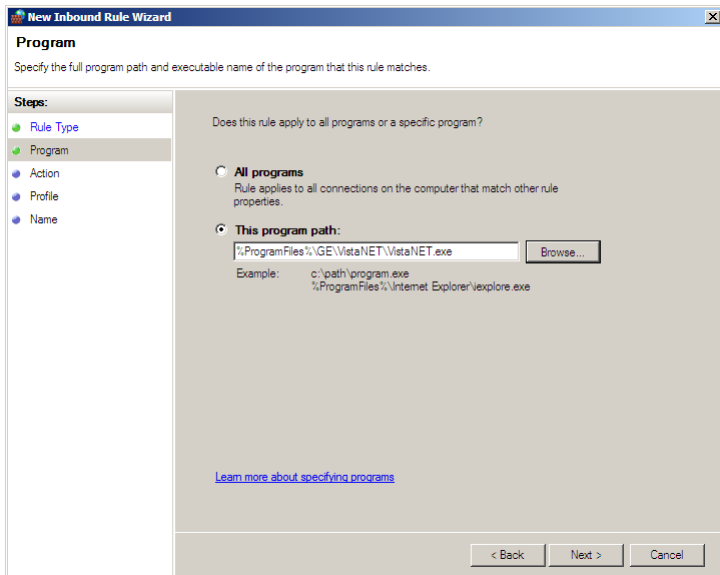


Figure: Program Path

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.

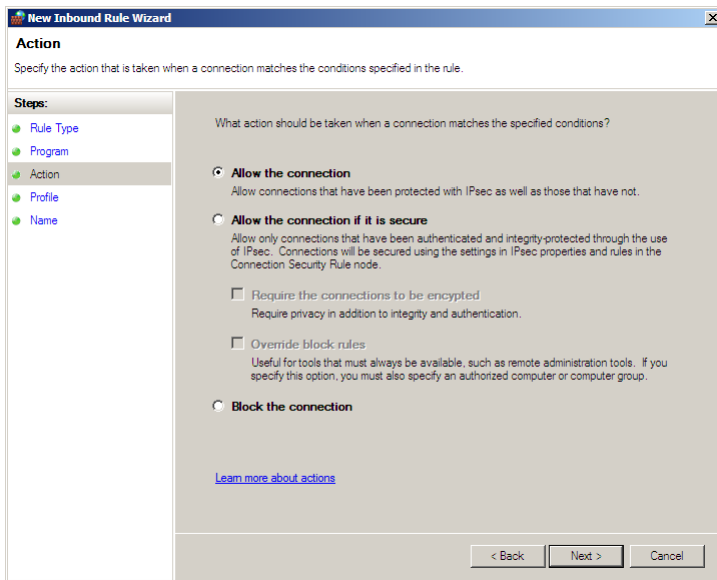


Figure: Action

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

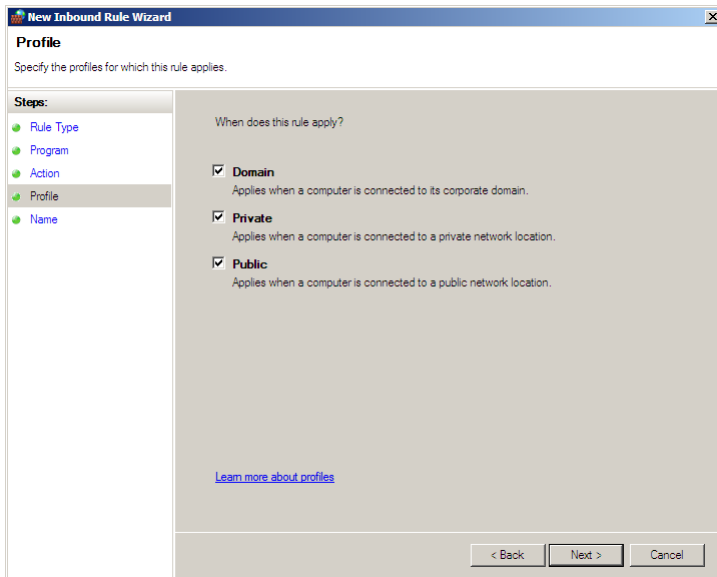


Figure: Profile

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 5.08 Software.

REQUIRED SOFTWARE BEFORE UPGRADE

VistaNET version 5.08 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 5.08.
 - **Uninstall** is required due to the change in the installer software used.
- You must upgrade the H7Engine.dat with VistaNET4.xx before VistaNET version 5.08 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 5.08, 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 5.08 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 5.08 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 5.08.

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 5.08.

INSTALLING VISTANET VERSION 5.08 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 5.08 OR UPGRADE VISTANET FROM 4.XX

For new installation of VistaNET version 5.08 or when upgrading from VistaNET version 5.00, 5.02 or 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 *VistaNET_508_16316.msi* file to the PC's hard drive

NOTES and RECOMMENDATIONS

1. **NOTE 1:** After installing VistaNET version 5.08, you must rediscover the existing network in order to populate the database with required data. This discovery is required for all nodes due to significant changes with SNMP-based Entity, Traffic and Performance MIBs.
2. **NOTE 2:** All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade.



- Run the *VistaNET_508_16316.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.

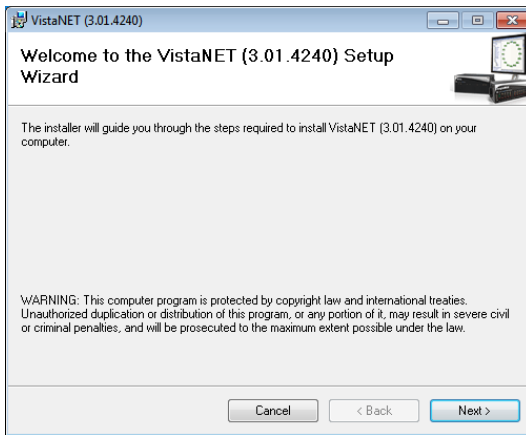


Figure: Welcome Screen

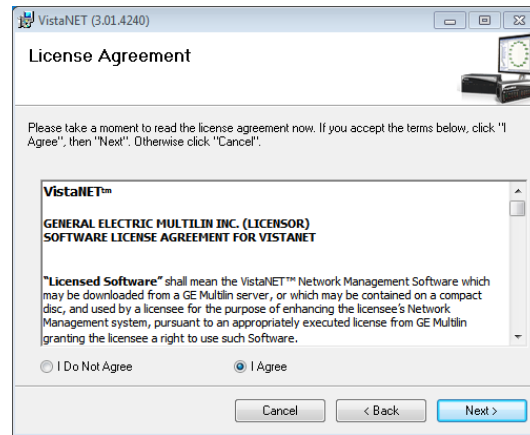


Figure: License Agreement

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 5.08 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 5.08

LICENSE FILE (*.LIC)

The VistaNET license file used to activate and control licensed features has been changed for VistaNET version 5.08. 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 5.08.
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 administrator should register for the license file by visiting the Lentrionics Multiplexer website.

- Visit <http://www.gegridsolutions.com/communications/Multiplexers.asp>
- Enter your username and password to log on to the site
- Select the "I agree" button for the Terms of Use
- Select the "Software" web link
- Select "VistaNET License Registration form" (<http://www.gegridsolutions.com/Communications/Lentrionics/passport/register.asp>)
- Complete and submit the registration form
- Please specify desired PIN and LICENSE file expiration dates between **1 & 36 months**



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



GE Lentrionics 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 factory, a security PIN, required to fully activate VistaNET version 5.08, 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 5.08.

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.

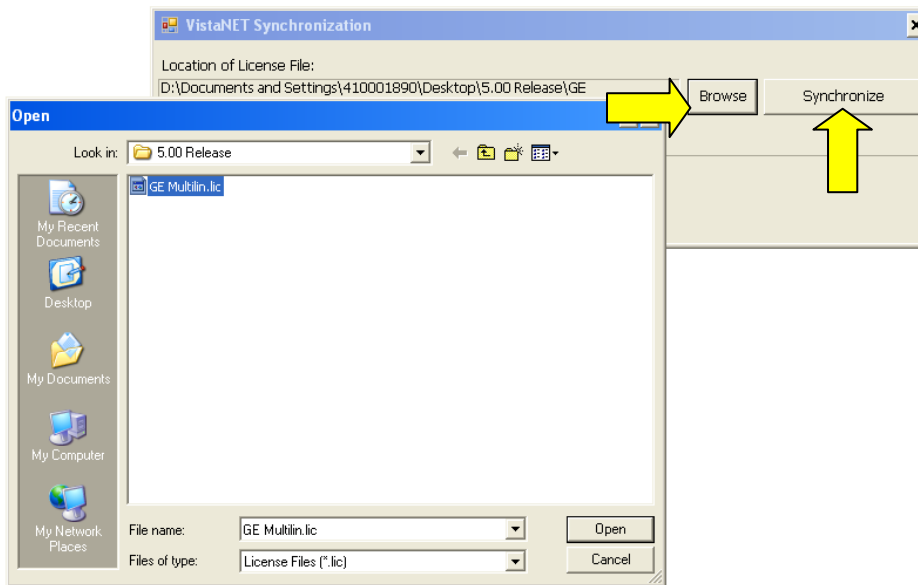


Figure: Open license file

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 5.08 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 5.08 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.

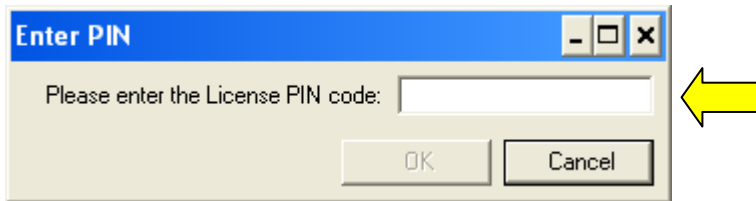


Figure: Enter Activation PIN

This activation PIN is married to the supplied license file (paired keys). Both factors are needed to successfully license and activate VistaNET 5.08. 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

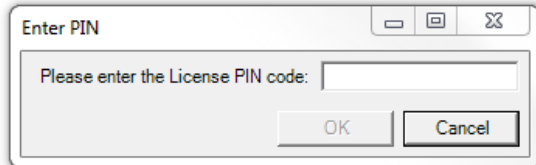
Activating VistaNET 5.08 can be achieved in one of three ways,

1. Apply an Activation PIN (reserved for VistaNET Administrators)
2. Synchronization VistaNET with a previously activated version of VistaNET 5.08 (recommended for general VistaNET users)
3. Supply remote VistaNET instances with a secure db3 file.

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 5.08. 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 5.08 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.



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 5.08 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 5.08 services is completely encrypted, mitigating man-in-the-middle attacks.*

Remote instances of VistaNET 5.08 are now fully operational.



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 5.08 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 5.08 are now fully operational.

LICENSING AND ACTIVATION NOTES

1. The database (*.db3 file) is additionally encrypted during the upgrade to version 5.08. 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 from VistaNET version 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 company's 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.

IMPACT OF EXPIRATION

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.

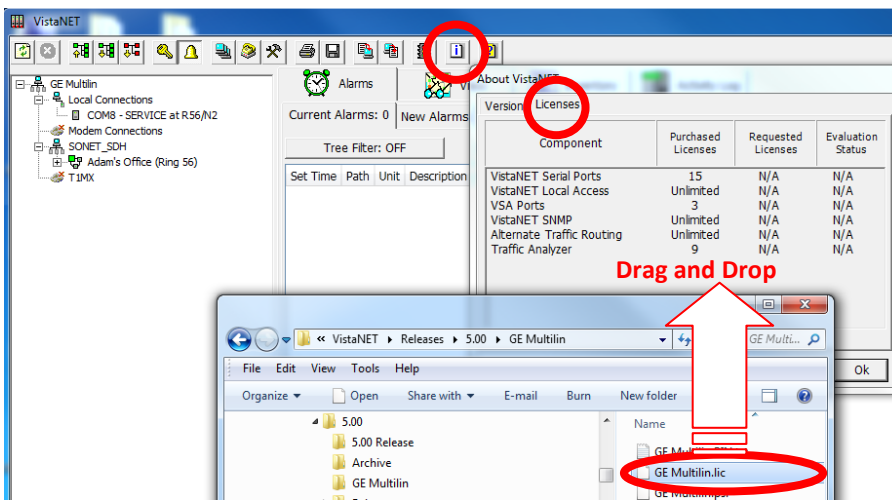


However, the activation PIN is typically needed just once, during the initial activation of VistaNET 5.00. The VistaNET administration team can administer users and user privileges via a valid VistaNET administrative login.

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

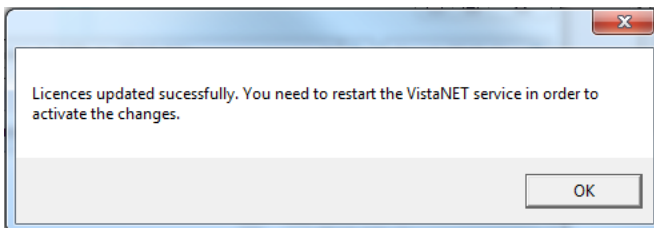
REPLACING AN EXPIRED LICENSE FILE OR ADD A NEW LICENSE

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.



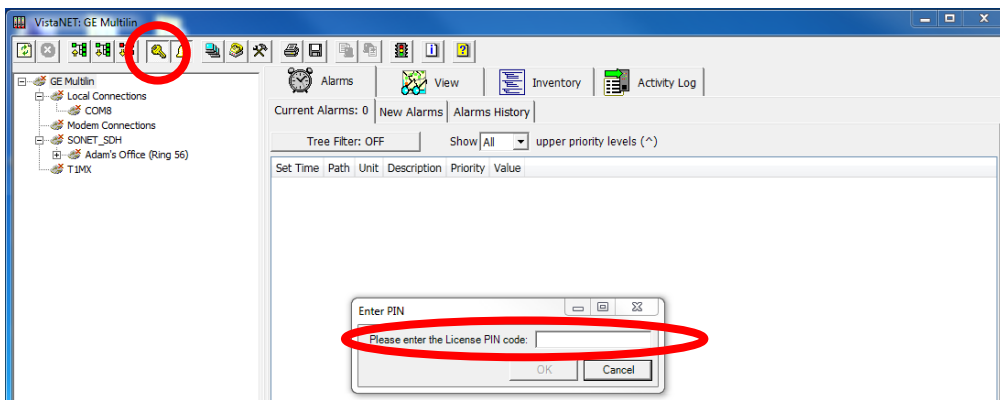
Drag the new license file into the VistaNET Licenses tab.

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.

This is the same process a customer would follow if a new license feature has been purchased. GE will deliver this new license via the .LIC file. Users need to drag this license file over the VistaNET licenses tab to integrate the new license.



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.

USER AUTHENTICATION

Starting from version 5.04, VistaNET employs Microsoft Active Directory (AD) and Windows™ Local Accounts to authenticate users. All users previously stored in the VistaNET database will be disabled after migrating to VistaNET 5.04 or higher versions. These disabled accounts are still visible to the user with the “Show Obsolete Accounts” checkbox. A VistaNET administrator must select 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.

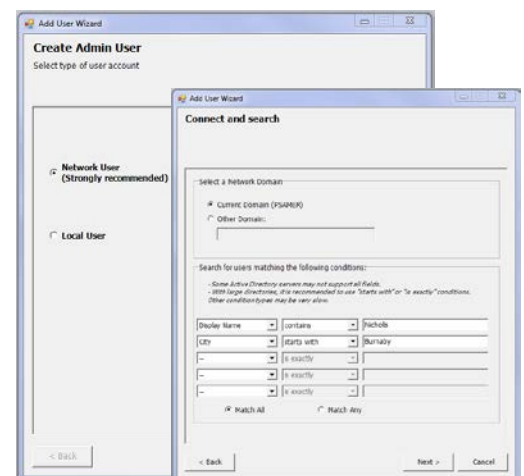
IMPORTANT NOTE: All users stored in the VistaNET database before VistaNET version 5.04 will be deleted after migrating to VistaNET 5.04 or higher. User credential will no longer be stored in the VistaNET database.

ADMINISTRATING USERS

After installing VistaNET 5.04 (or higher) for the first time or upgrading from VistaNET 5.03 (or lower), administrators will be prompted to create an administrator account with one picked from a Network or a Windows Local Account:

1. for new installations of VistaNET, administrators will login with ‘administrator’ as the username and use the ‘PIN’ for the password.
2. 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' (SID) 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 VistaNET 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.

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
 - For Active Directory: Domain name and reuse of users AD login credentials
 - For 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).*

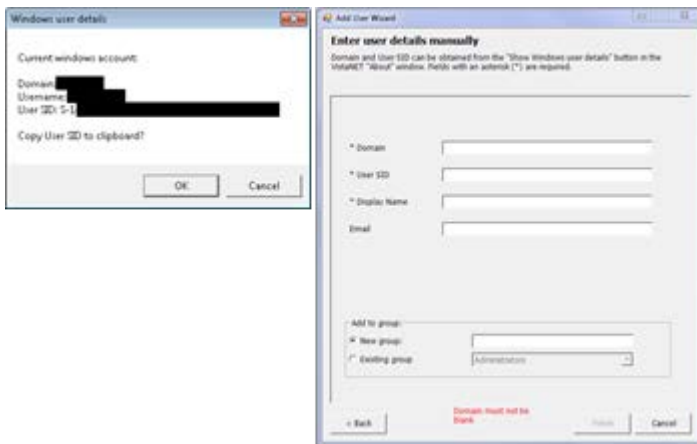
Note: *All users, with Network or Local Windows accounts, require a valid user password. The password field cannot be kept blank.*

ADMINISTRATING LOCAL USERS

To add a local VistaNET user account, an administrator will need to know the user's domain and SID.

To locate this information, administrator will need to ask a user to perform the following actions from the PC where the local user will be logging into VistaNET:

1. login to user's Windows account via their Windows Local Account credentials
2. select the information icon  in VistaNET, running on user's PC
3. 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 complete the 'Enter user details manually' for remote user account when user's domain and SID are provided.

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

ENABLING REMOTE USERS


Remote VistaNET users upgrading from VistaNET 5.03 or lower versions 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.

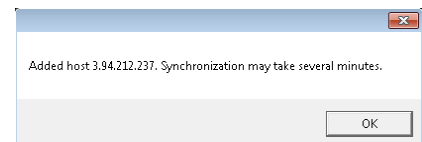
Typically, adding the new user accounts is performed on a centralized 24/7 instance of VistaNET, and distributed to all remote users via Synchronization. In addition to communicating the type of user account defined for each user, administrators must also provide the IP address or host name of the PC 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 or higher version, remote users can quickly synchronize to a targeted 24/7 VistaNET service containing remote user account listings and SIDs 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.

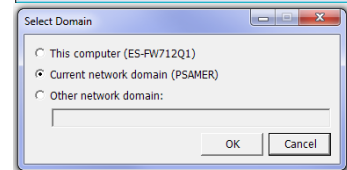
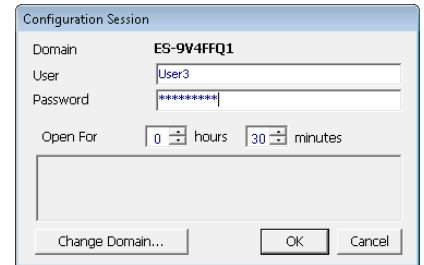


DOMAIN SELECTION

VistaNET 5.04 (or higher) authenticates users against Network 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 to allow users to toggle between:

- Network domain preconfigured on their PC,
- Local Host name of their PC, or
- 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.





LIMITATIONS

The following is a list of known limitations related to VistaNET 5.08. 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].



-
- During AD upgrade process, if user selects to enter an IP/host to synchronize to, VistaNET says "synchronization may take several minutes", but then immediately closes. The VistaNetService is actually continuing the synchronization in the background [ticket #1170].
 - On Windows 8, Windows 10, Windows Server 2008 and Windows Server 2012, selecting a license file from network drive will fail.

Workaround: Copy the license file to the local drive [ticket #1187].

- When used as 24/7 VistaNET PC, Windows 10 and Windows Server 2012 may fail synchronization process.

Workaround: Use recommended Windows 7 OS for 24/7 instances of VistaNET.



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
#111	VNET-871: OC-XX: JIF Port tabs->Multiple JIFshares in one JIFport/slot assignment	OpticUnits
#161	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]	Other
#306	Modem Lockout jumper is not functional [Workaround: None]	Security
#425	J-Sync shows incorrect ssm information in some cases	GUI
#426	Occasionally an alarm status in the main tab of OC-3 is not properly refreshed	GUI
#483	STM-16: Discovered node not accurately shown when asymmetrical configurations exist on the node.	Discovery
#500	When selecting a COM port item in local connections, the "open unit window" option opens an empty GUI	GUI
#522	In T1MX Spur, Multiple T1MX trees painted when the group value at L0 is changed	T1MX/E1MX
#523	CDAXs that have their group and node number changed are not accessible anymore	T1MX/E1MX
#524	Discovery fails Intermittently after one or more nodes deleted from the discovered ring	Discovery
#526	T1MX discovery incorrectly show L0 CDAX that doesn't support T1 Spur	Discovery
#533	Audible alarm button is non functional	Alarms
#538	Ring and node number for level 0 CDAX still shows on the unit after it is relocated	T1MX/E1MX
#539	The new setting of a moved CDAX from level 0 to a level N location still accessible from L0 icon	GUI
#545	In T1MX, the Data unit path identifier at Level 0 does not meet the requirement	T1MX/E1MX
#549	Aliases are not shown in the alarm engine "Unit path" field	Alarms
#578	Inconsistent alarm information on tree view	GUI
#579	Tree does not paint correct information on JIF-Share under OC-12	GUI
#583	VistaNET freezes during configuration when unit changes rack shelf slot info	DataAccess
#598	STM-16: Connecting TU12-structured TUG-3s to Bulk TUG-3 slots on CBW ports	GUI
#640	SRP - Alias for DS0 circuit in alarm history	Alarms
#691	Multiple unit user controls are displayed on top of each other when clicking around on the tree quickly	GUI
#697	Date drop down and "next" (>>) button are not updated when VistaNET is running for more than 1 day	GUI
#705	Order of units in Inventory XML file does not reflect the parent/child relationship	GUI



Ticket	Summary	Component
	of the network	
#716	Nodes controlled by IPSU are not released during firmware upgrade using the Craft Interface	IPSU
#717	VistaNET Local IP display in Status Tab Does Not Update With A Change in IP address	GUI
#730	IPSU GUI: Disable fields associated with new IPSU when connected to old IPSU	GUI
#779	VistaNET does not show correct option numbers for certain TN1U/TN1Ue units	GUI
#780	4W VF Unit Loopback field not colored in blue	GUI
#785	Dead JIF-DS1 causes bogus DS0 alarm and VT test	GUI
#791	A 4W single channel unit sometimes is displayed with left and right sides	Discovery
#796	Terminal Window does not get displayed after Modem has connected	DataAccess
#799	CDAX T1 port LOS alarm is displayed when alarm is disabled and multiple alarms exist	DataAccess
#803	Yellow text box on L0 CDAX does not appear if the unit is set as G0N0	GUI
#813	IPSU sometimes does not reset correctly when issued RESET command from VistaNET	GUI
#815	Simultaneous and differing configurations to the same JIFPort slot can corrupt optical units and hang VistaNET displays	GUI
#820	Menu bar dialog box has inconsistent behavior	GUI
#827	VistaNET sometimes displays an exception when selecting the unit of an alarm	GUI
#832	Wrong error message for Serial-over-IP link to NMX unit	GUI
#833	VSA license checkbox is N/A to Serial-over-IP links to NMX unit	GUI
#839	Strong Arm IPSU shows wrong Processor Info	GUI
#846	Unknown publisher, VistaNET code is not signed	GUI
#850	Traffic Manager does not display E100 under OC-3	GUI
#852	VistaNET 4.00 Performance	GUI
#870	OC48 Sometimes displays "VT" in the CBW cross connect	GUI
#872	VistaNET show invalid argument during discovery	GUI
#885	CDAX reset returns (expected?) exception with hresult = 0x80591099	GUI
#897	VistaNET 4.06: IPSU GUI: Software Licensing frame always reports as IPSU0406	GUI
#901	Cannot shutdown VistaNET gracefully per services.msc method	GUI
#923	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	VSNMP
#926	Unplug CI cable while discovering a network will cause VistaNetService crash	Discovery
#927	VistaNET does not check in the background if a unit has been put to sleep.	DataAccess
#938	Alias disappearing on G703 circuits	GUI
#940	Potential race condition when attempting to add Redirected Serial over IP connections	GUI
#950	Bogus NMS alarms when simultaneous Alarm, Alert (and Test) are reported from DS0 level unit	GUI



Ticket	Summary	Component
#954	VistaNET should display a more meaningful error message instead of DISP_E_TYPEMISMATCH when the company id does not match	GUI
#956	Nx64F is shown as Nx64 in the SNMP entry	VSNMP
#959	Expired License + PIN number license file can be made to work again by changing the time and date on the local PC	Security
#962	Unit view doesn't appear when connected to CI although unit is detected and displayed in tree	GUI
#967	Inconsistency when adding Group Name between the Users and Groups Tab of the Administration & Startup Options window	GUI
#970	Tree view not loading after improper server shutdown	GUI
#977	Alarm engine description incorrect for STS level alarms	GUI
#978	VNI client not shutting synchronization when another VNI client service is shutdown	GUI
#980	VistaNET synced with another *.lic file on network	GUI
#984	Ring Icon shows erroneous JMUX alarm status for non-existent side of linear system in System/Network Map View	DataAccess
#1021	Restart of VistaNET service required when PC comes back from standby or hibernation	Other
#1023	STM-16 Unit Fibre View does not display Unit and FOT Temperatures	GUI
#1024	STM-16: NMS Location cannot be properly set	GUI
#1025	STM-16: Individual VC-4 loopbacks available when AUG-4 is set for VC-4-4c mode	GUI
#1026	System Tree Labels incorrect (shows SONET & T1MX for SDH .lic file)	GUI
#1027	Multiple CBW Tie Links can be entered in Network Map View	GUI
#1034	CDAX Spur links are not present in Traffic table	Discovery
#1038	Modem connections are displayed on the Local Connections tree	Discovery
#1043	Service locks up when trying to shut down while modem is connected	DataAccess
#1047	Node View does not update when status changes	GUI
#1049	GUI does not switch properly when craft interface cable is moved to a different unit	GUI
#1055	Active Directory sometimes times out when attempting search by employee ID	Security
#1057	Removing a JVT TIE in map view	GUI
#1059	"Open Unit Window" shows invalid data when the CI connection is changed to different unit	GUI
#1062	Tree shows unit as dead instead of in alarm when one or more but not all VTs/Channels are dead	DataAccess
#1063	right unit in connected CDAX pair shows as serial number for first 5 minutes after power cycling node	DataAccess
#1064	Contact I/O woken up from sleep mode displays "Invalid" channel	GUI
#1066	Orderwire unit configuration issue	GUI
#1067	External Sync Units must appear above aggregate units in System Tree	GUI
#1068	Any remote change in CDAX CC tab for a T1/Optic port sets its 'Alarm Enable' to enabled	GUI



Ticket	Summary	Component
#1069	Clearing red fields on the Node Icon upon reestablishing communication to its Service Unit	GUI
#1071	VistaNET 5.04 Log In Problem	GUI
#1073	Invalid IP Address '127.0.0.1' gets stuck in database	DataAccess
#1078	The "Locate Unit" menu option does not display "in T1MX" or "in SONET"	GUI
#1079	"Grey Box" in status bar does not display 3D relief	GUI
#1087	VistaNET believes that it is still connected to a USB to RS232 Converter when the USB to RS232 Converter is disconnected from the USB Port	GUI
#1088	VistaNET Current Alarms count is erroneous when VSA'ed and there is time difference between the VistaNETs.	GUI
#1097	Active Services May Not Display Peer IP	GUI
#1100	Inconsistent Inventory Counts for CDAXes in SONET and T1MX Spurs	GUI
#1103	Tie Info Tab on the TIE unit GUI does not refresh	GUI
#1104	TIE Unit Bad Tie Cable Alarm does not show on the tree view	GUI
#1105	Serial Connection Drop-off	GUI
#1116	JIF-Share/CMUX/CDAX Channel Force Offline feature should be designated 'RS' rather than 'RW'	JIF/TIFUnits
#1125	Node-to-node connectivity in Map View does not match info in entPhysicalTable	VSNMP
#1130	Update tie table when Node/Ring # is changed in Edit Tie Connections view	GUI
#1131	Allow for creating tie connections from the same node to multiple rings	GUI
#1149	Issue with VistaNET login when AD password is changed	GUI
#1158	86485-21 CMUX on show TU 11 tab (V1, V2 values are not at correct position	GUI
#1170	VistaNET closes after entering host to synchronize to during AD Upgrade	GUI
#1173	Synchronization between VistaNET will replace local users	Synchronization
#1187	On newer operating systems, adding licence from network drive fails	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
#1083	Setting all channels to "Thru" and then attempting to change a single channel back does not work on JIF-Share-02/CMUX-22	GUI
#1102	Local connection to a CSSU continually drops out and takes a very long time to stabilize.	GUI
#1108	"Launch VistaNET" checkbox not working in installer	GUI
#1113	Data-Nx64F: Mistakenly exposed Transmit and Expected Circuit Addresses	GUI
#1114	E1 CDAX: problem pasting the hairpins on the E1 port	GUI
#1118	OC-48 GUI Exception when toggling between right and left units if backup tab was selected	GUI
#1119	Ether-1000: Doesn't allow configuring SPE Slots by non-admin users in High Security Mode	GUI
#1120	Upgrading from VistaNET 5.02 or earlier to 5.04 or 5.06 may remove some DS0 alias	GUI
#1121	CDAX: Clear Channel Tables button is not visible for older firmware	GUI
#1122	Wrong filter selection logic in VistaNET Activity Log	GUI
#1126	JIF-Share 02: Cannot configure Left priority for port P under DS0 Channels tab	GUI
#1133	Problems & inconsistencies with displaying serial numbers in Add/Edit Tie Table Views	GUI
#1145	VistaNET TN1U Tie Unit Show TU12 Tab	GUI
#1146	CSSU: Switching CSSU's mode of operation remotely	GUI
#1152	Node status is not reflected on the tree after CSSU reboot	GUI
#1174	NX64, NX64F, & G.703 Unit GUI Allows Configuration of Circuit Address Parameters When Locally Connected	GUI

**FIXED DEFICIENCIES - VERIFYING**

The following deficiencies were identified and corrected prior to this release at GE Lenronics 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:

Ticket	Summary	Component
#1060	DTT-RCV (86442-01) shows an invalid channel number in the tree and path elements	GUI
#1070	86486-21 E1CDAX Ring GUI Support	GUI
#1074	Save Unit Data to File on Unit with Multiple Channels or VTs sometimes fails if not all elements are configured	DataAccess
#1084	T1/E1 Unit does not display alarms under certain conditions	Alarms
#1096	VistaNET GUI Does Not Exit Gracefully when VistaNET Service Stops	GUI
#1106	Cannot Remotely Configure NMS Channel at Level 0 T1/ E1 CDAX	GUI