86456

VistaNET® 5.12 Release Notes

Version:	5.12.17059
Release Date:	May 2019
Type of Release:	Maintenance Release

Lentronics Multiplexers

JungleMUX SONET Multiplexers,

TN1U and TN1Ue SDH Multiplexers,

T1MX, E1MX and E1MXe Multiplexers

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GE Multilin is not responsible for any damages or losses incurred as a result of out-of-date or incorrect information contained in this document.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

RELEASE SUMMARY

PRODUCT/COMPONENT

- VistaNET version 5.12.17059 (replacing version 5.12.17028, released March 2019)
- No new functionality added to 5.12.17059, only fixes RZVLE-91, -99 and -100 (refer to ‘Fixed deficiencies)

REQUIREMENTS

VistaNET version 5.12 requires the following components to be installed:

- Microsoft .NET Framework 4

VistaNET version 5.12 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.

In order to install or upgrade VistaNET, the installer requires to be run with Windows administrator privilege.

RELEASE DETAILS

NEW FEATURES 5.12.17028

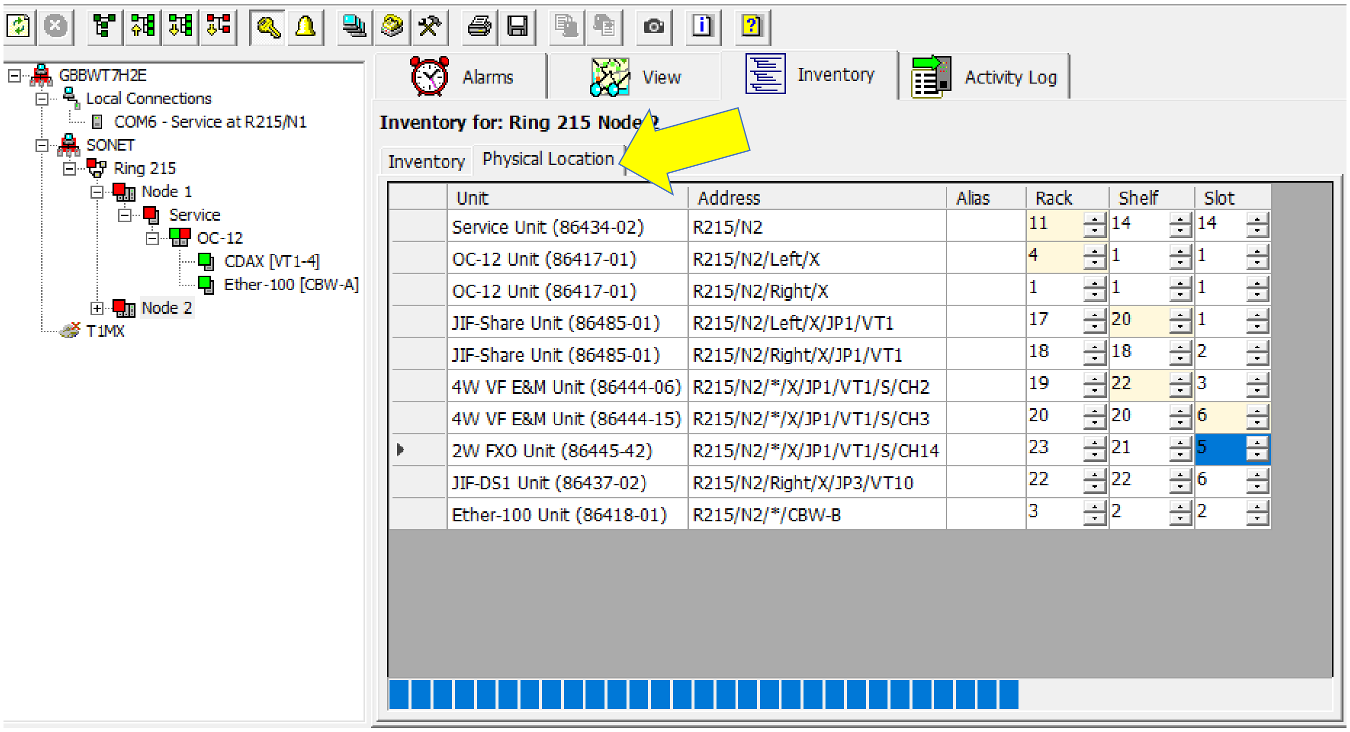
The new system features present in this software release version are:

BULK RACK/SHELF/SLOT CONFIGURATION

Configurations of each units Rack, Shelf, and Slot fields are important parameters when modeling the JungleMUX/TN1U and T1/E1 Multiplexers within an external Manager of Managers (MoM). Partner products like MegaSys's Telenium MoM allow users to visualize the physical arrangement of cards within a node to assist operational staff in network planning, circuit commissioning and lifecycle management of these assets. With correctly configured RSS, the Multiplexers themselves become the record of trust, feeding information to MegaSys Telenium through an automated approach that introduces simplicity to much of the reporting and maintenance tasks previously manually performed.

Prior to the release of this RSS configurator, VistaNET users had to visit each remote site and configure these parameters locally. Now, configuring these parameters over an NMS channel from a remote location is possible.

Additionally, Bulk RSS configurator is available as a licensed feature (p/n 86456-32), eliminating the repetitive nature of programing RSS one card at a time and enabling an entire system of RSS parameters to be configured in one shot.

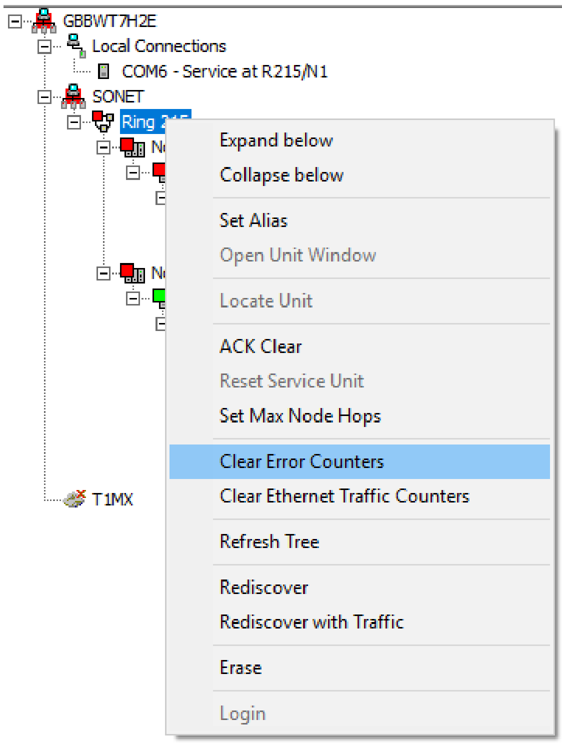


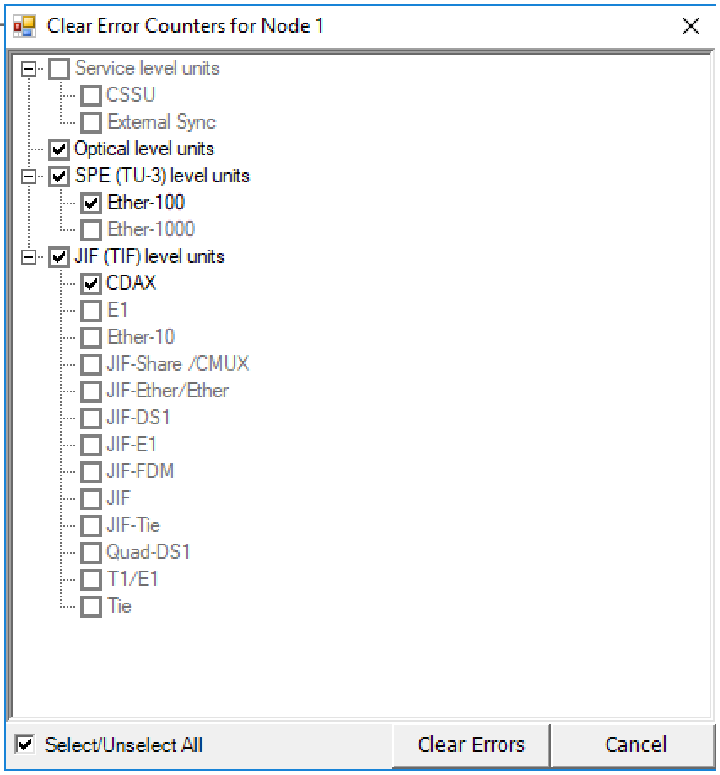
Inventory for: Ring 215 Node 2

Unit	Address	Alias	Rack	Shelf	Slot
Service Unit (86434-02)	R215/N2		11	14	14
OC-12 Unit (86417-01)	R215/N2/Left/X		4	1	1
OC-12 Unit (86417-01)	R215/N2/Right/X		1	1	1
JIF-Share Unit (86485-01)	R215/N2/Left/X/JP1/VT1		17	20	1
JIF-Share Unit (86485-01)	R215/N2/Right/X/JP1/VT1		18	18	2
4W VF E&M Unit (86444-06)	R215/N2/*/X/JP1/VT1/S/CH2		19	22	3
4W VF E&M Unit (86444-15)	R215/N2/*/X/JP1/VT1/S/CH3		20	20	6
2W FXO Unit (86445-42)	R215/N2/*/X/JP1/VT1/S/CH14		23	21	5
JIF-DS1 Unit (86437-02)	R215/N2/Right/X/JP3/VT10		22	22	6
Ether-100 Unit (86418-01)	R215/N2/*/CBW-B		3	2	2

CLEAR ERROR COUNTERS

Clear Error Counters is a licensed VistaNET feature (p/n 86456-31) that allows users to remotely clear CV counters across a wide range of nodes and across different equipment categories. Until the release of this feature, users were only able to Clear Error Counters on a unit by unit basis.




Clear Error Counters for Node 1

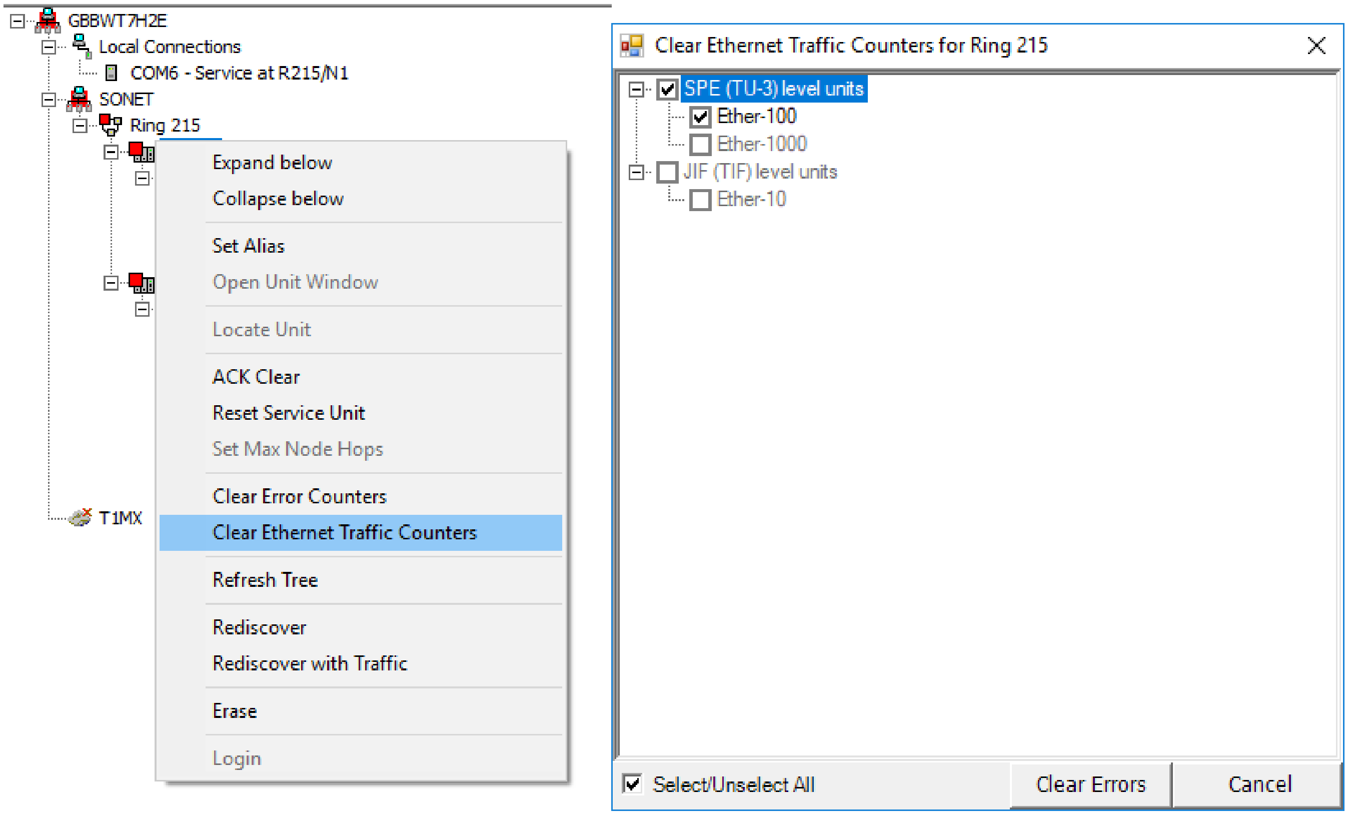
- ☐ Service level units
  - ☐ CSSU
  - ☐ External Sync
- ☑ Optical level units
- ☑ SPE (TU-3) level units
  - ☑ Ether-100
  - ☐ Ether-1000
- ☑ JIF (TIF) level units
  - ☑ CDAX
  - ☐ E1
  - ☐ Ether-10
  - ☐ JIF-Share /CMUX
  - ☐ JIF-Ether/Ether
  - ☐ JIF-DS1
  - ☐ JIF-E1
  - ☐ JIF-FDM
  - ☐ JIF
  - ☐ JIF-Tie
  - ☐ Quad-DS1
  - ☐ T1/E1
  - ☐ Tie

☑ Select/Unselect All

Now, with Clear Error Counters licensed, users can clear all CV across all Optics, SPE/TUG-3, JIF/TIF level cards within defined ranges (Rings or within a Node).

CLEAR ETHERNET TRAFFIC COUNTERS

For Ether-100/1000 units, clearing Traffic counters is also now available and included within the right-to-use licensing for clearing error counters (p/n 86456-31). Select between clearing Error counters or Clearing Ethernet Traffic counters from VistaNET's navigation tree at the ring or node level.



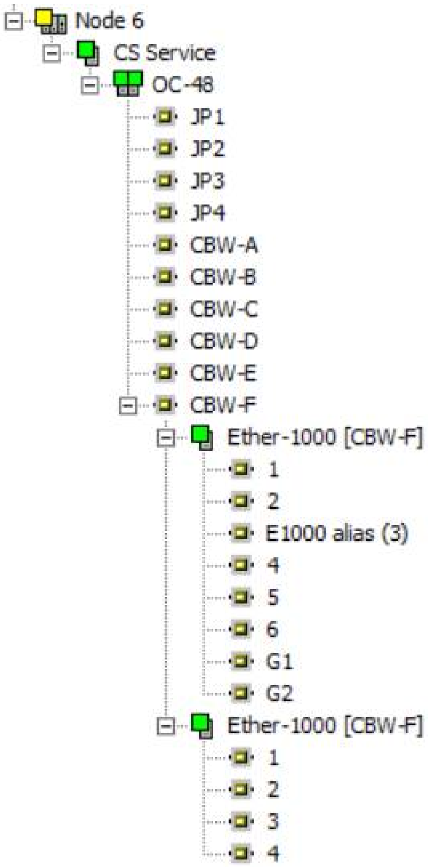
The implications on efficiency and overall costs savings are immediately obvious. Users can clear all the error counts within a single ring in one configuration step or reset all the counters within each of their Ether-100/1000 units without clearing counters within the T1/E1 units.

SETTING ETHER-1000 PORT ALIASES

Ether-1000 units' switch ports are now exposed within the VistaNET navigation tree, and users have the option to set an individual port alias. Alias works the same as Unit, Node or Ring aliasing, by right mouse clicking on an Ether-1000 port and selecting the Alias function.

All aliased parts are synchronized with all other connected VistaNET instances.

The illustration below shows the navigation pane in "Traffic" mode. Users can select "Show units and traffic" (formally "Show units and ports") in the VistaNET toolbar.



```
Node 6
  CS Service
    OC-48
      JP1
      JP2
      JP3
      JP4
      CBW-A
      CBW-B
      CBW-C
      CBW-D
      CBW-E
      CBW-F
        Ether-1000 [CBW-F]
          1
          2
          E1000 alias (3)
          4
          5
          6
          G1
          G2
        Ether-1000 [CBW-F]
          1
          2
          3
          4
```

Associated with this changes, Ether-1000 paddleboards are now discovered while ports formally labelled G1 and G2 (GigE port 1 and 2) have been relabeled to ports 7 and 8.

Port aliasing is supported on single or cascaded Ether-1000 units.

IMPORTANT REMARKS

MANAGEMENT OF THE VISTANET SERVICES

The VistaNetService.exe must 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.

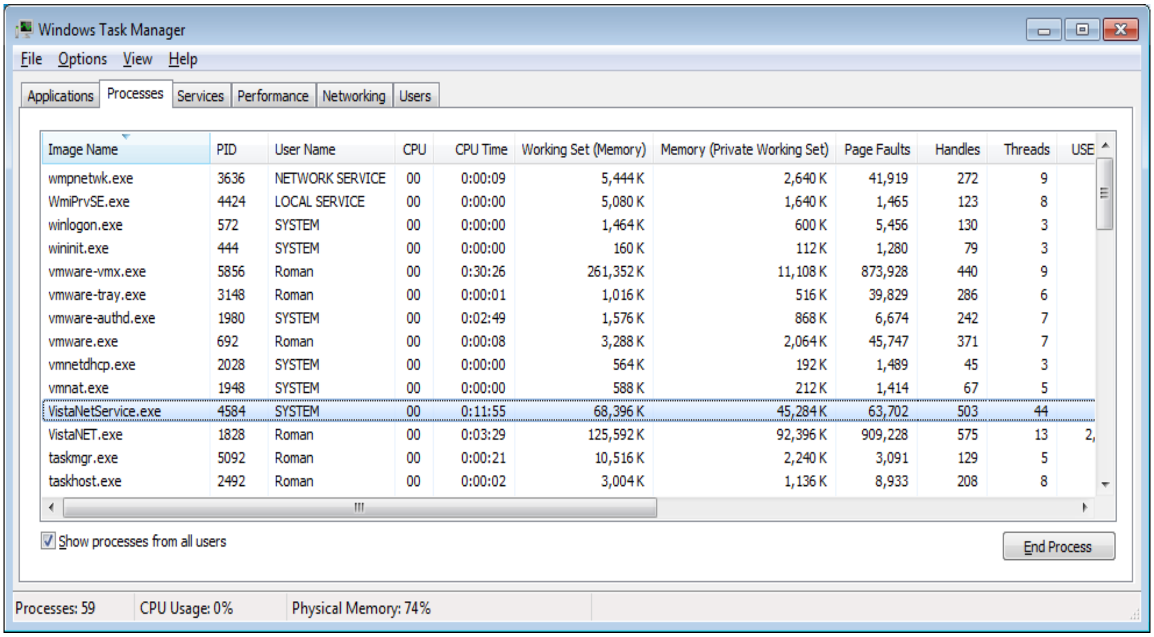
VistaNET.exe will start VistaNetService.exe but it will not stop it on exit. On the other hand, VistaNetService.exe will close VistaNET.exe when stopped.

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).



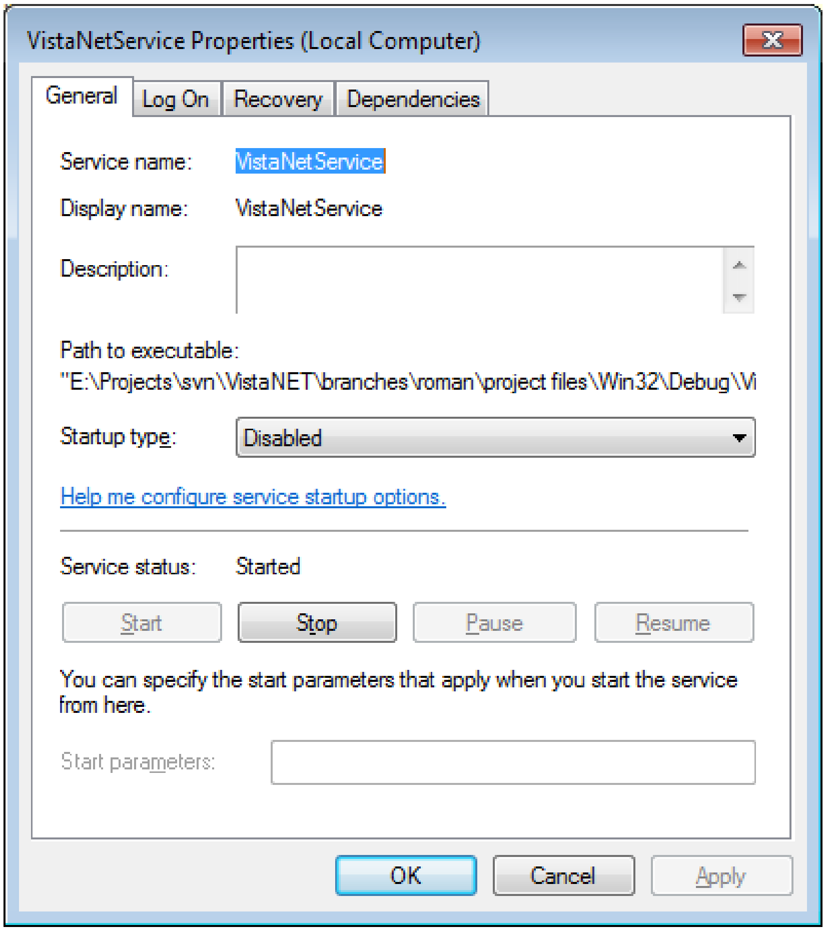
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

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	

☑ Show processes from all users

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.



VistaNetService Properties (Local Computer)

Service name: VistaNetService

Display name: VistaNetService

Description:

Path to executable:
"E:\Projects\svn\VistaNET\branches\roman\project files\Win32\Debug\Vi

Startup type: Disabled

Help me configure service startup options.

Service status: Started

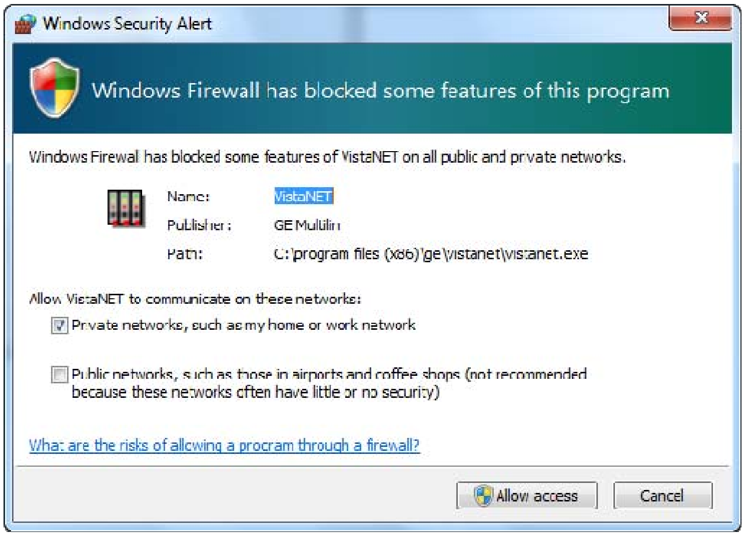
You can specify the start parameters that apply when you start the service from here.

Start parameters:

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.



Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked some features of VistaNET on all public and private networks.

Name: VistaNET
Publisher: GE Multilin
Path: C:\program files (x86)\ge\vistanet\vistanet.exe

Allow VistaNET to communicate on these networks:

☑ Private networks, such as my home or work network

□ Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security)

What are the risks of allowing a program through a firewall?

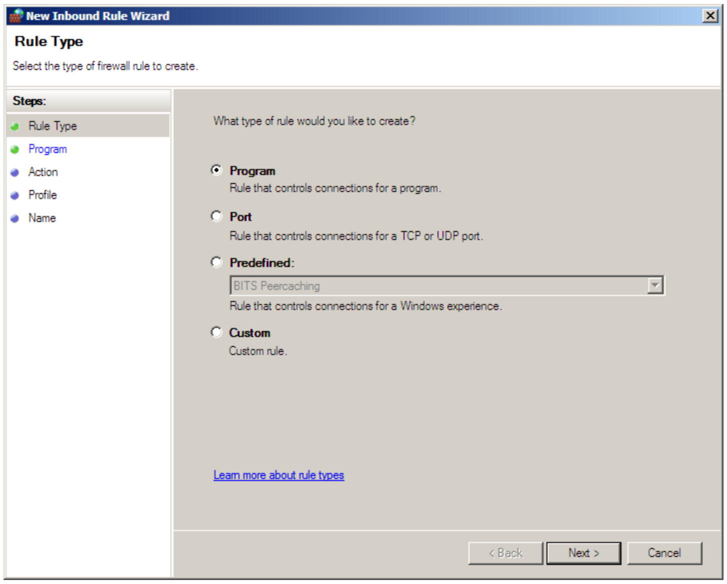
Figure: Windows Firewall

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.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

● Program
Rule that controls connections for a program.

○ Port
Rule that controls connections for a TCP or UDP port.

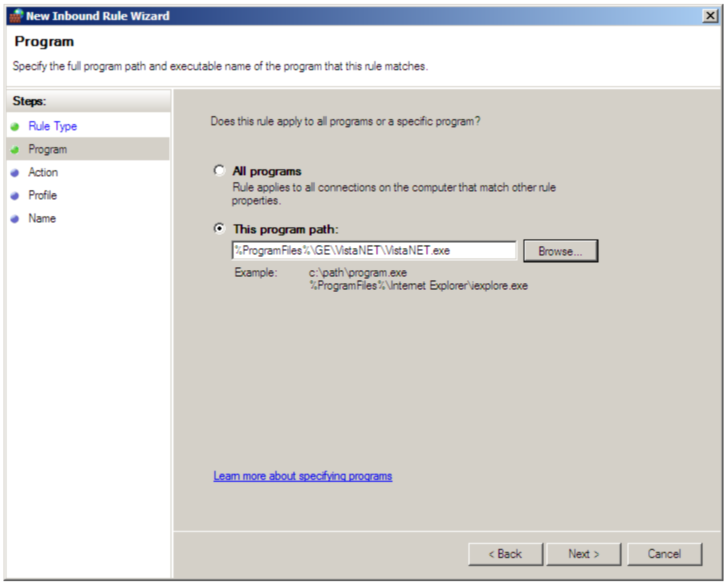
○ Predefined:
BITS Peercaching
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

Learn more about rule types

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.



New Inbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

○ All programs
Rule applies to all connections on the computer that match other rule properties.

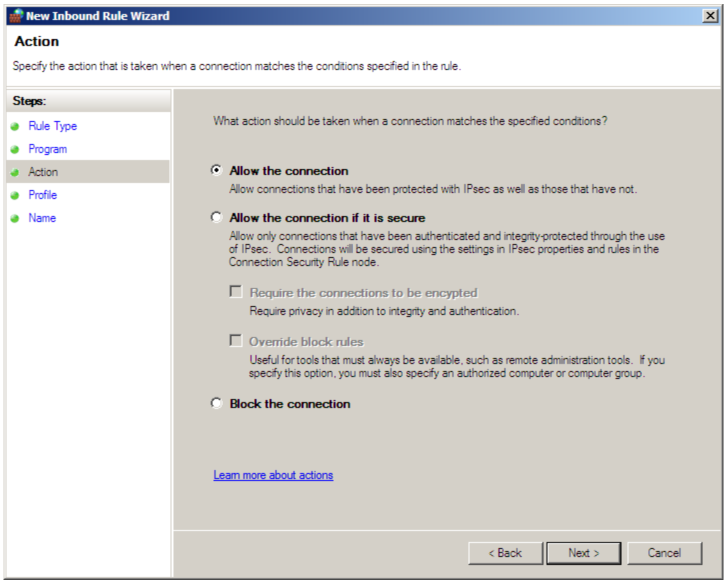
● This program path:
%ProgramFiles%\GE\VistaNET\VistaNET.exe

Example: c:\path\program.exe
%ProgramFiles%\Internet Explorer\iexplore.exe

Learn more about specifying programs

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.



New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

○ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

□ Require the connections to be encrypted
Require privacy in addition to integrity and authentication.

□ Override block rules
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

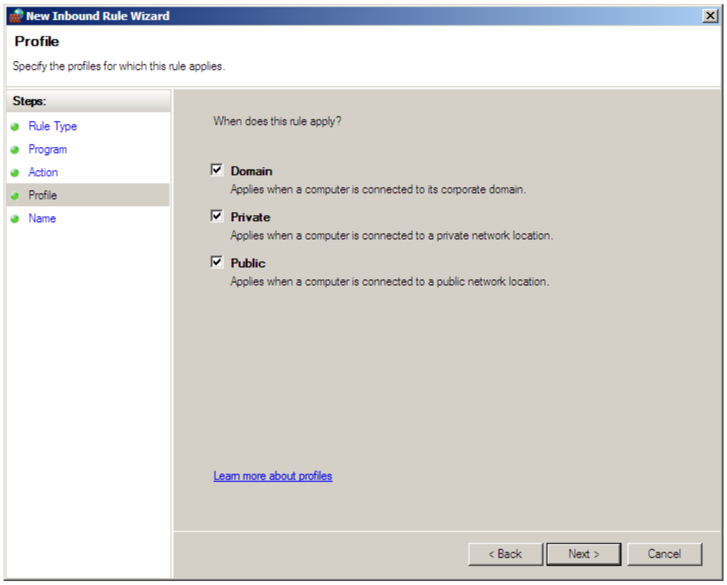
○ **Block the connection**

Learn more about actions

< Back | Next > | Cancel

Figure: Action

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



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Program
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Learn more about profiles

< Back | Next > | Cancel

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 5.12 Software.

REQUIRED SOFTWARE BEFORE UPGRADE

VistaNET version 5.12 requires the following components to be installed:

- Microsoft .NET Framework 4
- Customers who have previously installed release 5.12.17028 should upgrade to version 5.12.17059, but closing the VistaNET GUI and Service and running the installation file.
- Customers who have not upgraded to VistaNET 5.12 shall upgrade immediately to version 5.12.17059.

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 5.12.
    - **Uninstall** is required due to the change in the installer software used.
- <u>You must upgrade the H7Engine.dat with VistaNET4.xx before VistaNET version 5.12 will be installed</u>, 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 5.12, 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 5.12 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 5.12 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 5.12.

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 5.12.

INSTALLING VISTANET VERSION 5.12 OR UPGRADING FROM VISTANET VERSION 4.XX

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

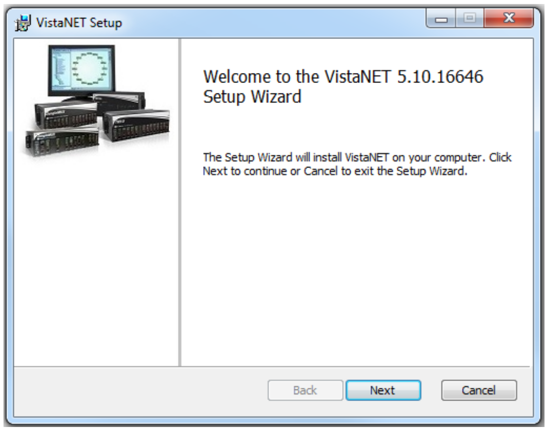
STEPS TO INSTALL VISTANET 5.12 OR UPGRADE VISTANET FROM 4.XX

For new installation of VistaNET version 5.12 or when upgrading from VistaNET version 5.00 - 5.10 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_510_16646.msi* file to the PC’s hard drive

NOTES and RECOMMENDATIONS

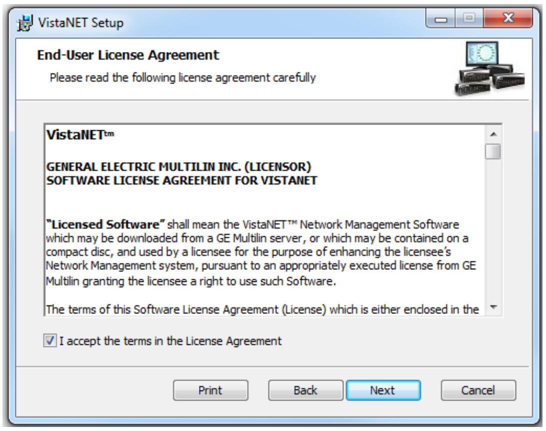
1. **NOTE 1:** After installing VistaNET version 5.12, you must rediscover the existing network in order to populate the database with required data. This discovery is required for all nodes due to significant changes with SNMP-based Entity, Traffic and Performance MIBs.
2. **NOTE 2:** All of the information contained in the .db3 file prior to the upgrade will be available after the upgrade.
   - Run the *VistaNET_511_XXXXX.msi* file
   - Follow the installer's 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.



Welcome to the VistaNET 5.10.16646 Setup Wizard

The Setup Wizard will install VistaNET on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Figure: Welcome Screen



End-User License Agreement

Please read the following license agreement carefully

VistaNETtm

GENERAL ELECTRIC MULTILIN INC. (LICENSOR)
SOFTWARE LICENSE AGREEMENT FOR VISTANET

"Licensed Software" shall mean the VistaNET™ Network Management Software which may be downloaded from a GE Multilin server, or which may be contained on a compact disc, and used by a licensee for the purpose of enhancing the licensee's Network Management system, pursuant to an appropriately executed license from GE Multilin granting the licensee a right to use such Software.

The terms of this Software License Agreement (License) which is either enclosed in the

☑ I accept the terms in the License Agreement

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

LICENSING AND ACTIVATING VISTANET 5.12

LICENSE FILE (*.LIC)

The VistaNET license file used to activate and control licensed features has been changed for VistaNET version 5.xx. 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.xx.
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 Lentronics 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/Lentronics/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 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 factory, a security PIN, required to fully activate VistaNET version 5.12, will be independently supplied to each primary VistaNET administrator.

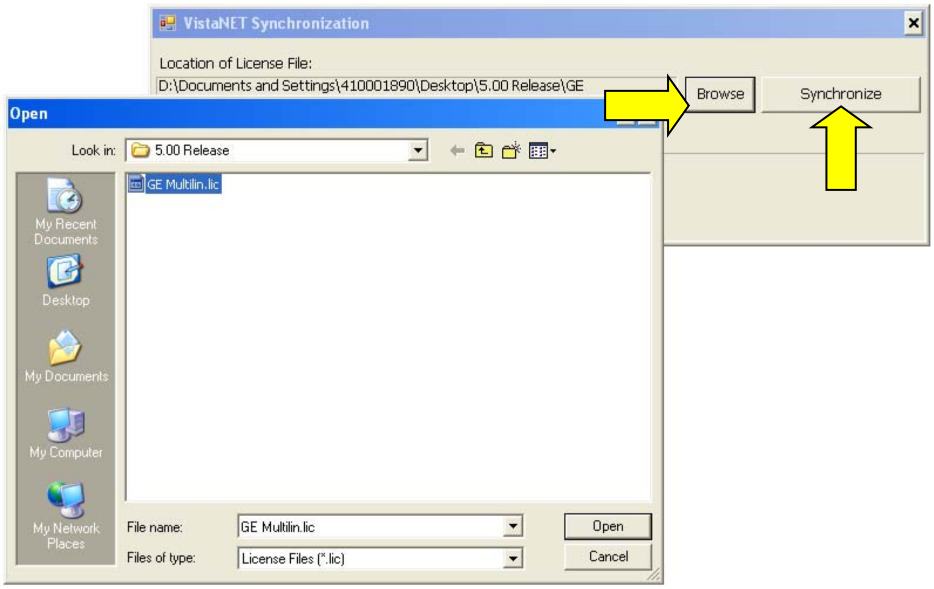
<u>Distribute the LICENSE file:</u>

This license file can be safely distributed (recommended) to all VistaNET users that require VistaNET version 5.12.

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.



VistaNET Synchronization

Location of License File: D:\Documents and Settings\410001890\Desktop\5.00 Release\GE

Open

Look in: 5.00 Release

GE Multilin.lic

File name: GE Multilin.lic

Files of type: License Files (*.lic)

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; <u>however</u>, VistaNET 5.12 is <u>not fully operational</u>. 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 5.12 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.

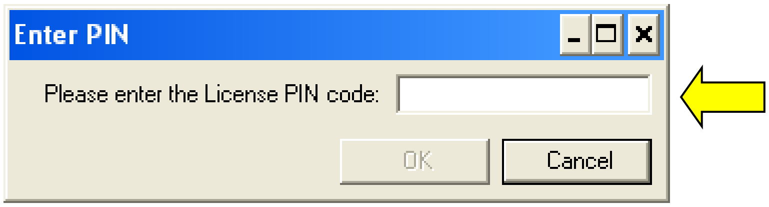


Figure: Enter Activation PIN

This activation PIN is married to the supplied license file (paired keys). Both factors are needed to successfully license and activate VistaNET 5.12. 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.

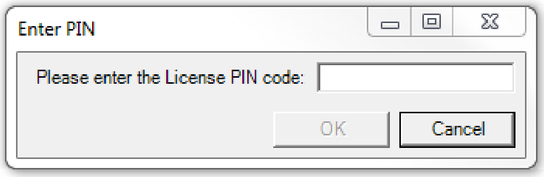
ACTIVATING VISTANET

Activating VistaNET 5.12 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 5.12 (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 5.12. 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 5.12 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.



Enter PIN

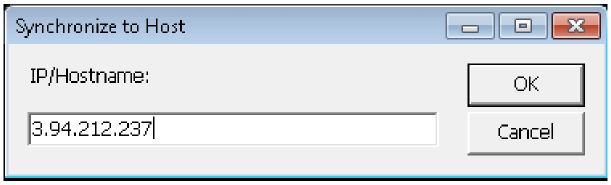
Please enter the License PIN code:

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 5.12 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).



Synchronize to Host

IP/Hostname: 3.94.212.237

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

Remote instances of VistaNET 5.12 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 5.12 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 5.12 are now fully operational.

LICENSING AND ACTIVATION NOTES

1. The database (*.db3 file) is additionally encrypted during the upgrade to version 5.12. 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

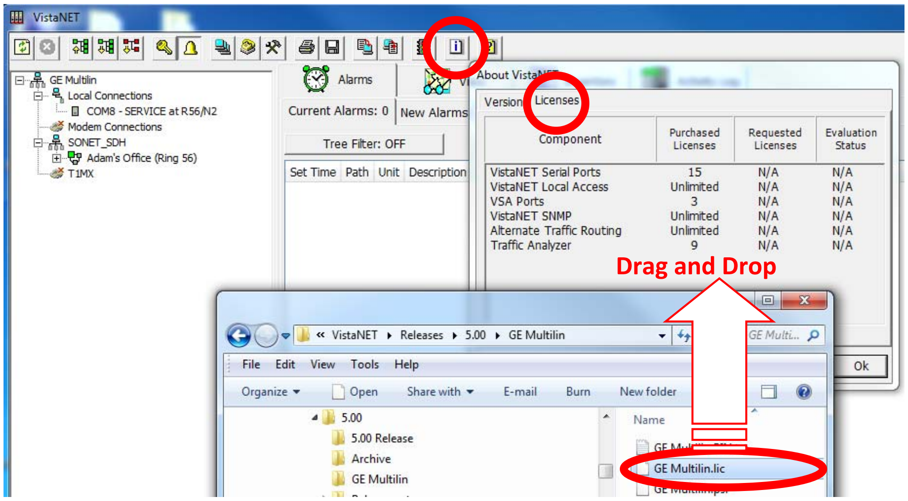
When the activation PIN expires, administrators will not be able to activate the VistaNET software via the first activation method described herein.

However, the activation PIN is typically needed just once, during the initial activation of VistaNET 5.12. 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.

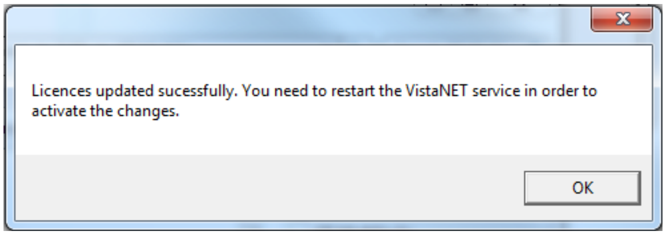


Component	Purchased Licenses	Requested Licenses	Evaluation Status
VistaNET Serial Ports	15	N/A	N/A
VistaNET Local Access	Unlimited	N/A	N/A
VSA Ports	3	N/A	N/A
VistaNET SNMP	Unlimited	N/A	N/A
Alternate Traffic Routing	Unlimited	N/A	N/A
Traffic Analyzer	9	N/A	N/A

Drag and Drop

Drag the new license file into the VistaNET Licenses tab.

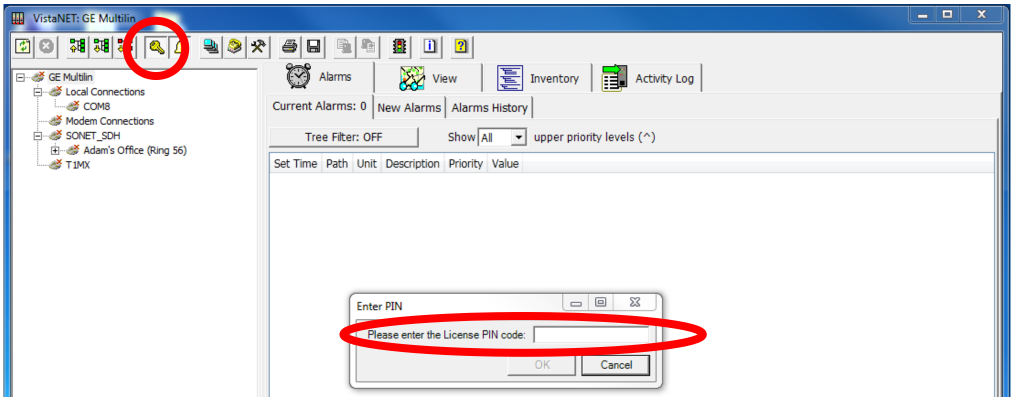
If the license file is valid, users will be asked to restart the VistaNET service in order to activate the changes.



Licences updated sucessfully. You need 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.



Enter PIN

Please enter the License PIN code:

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.

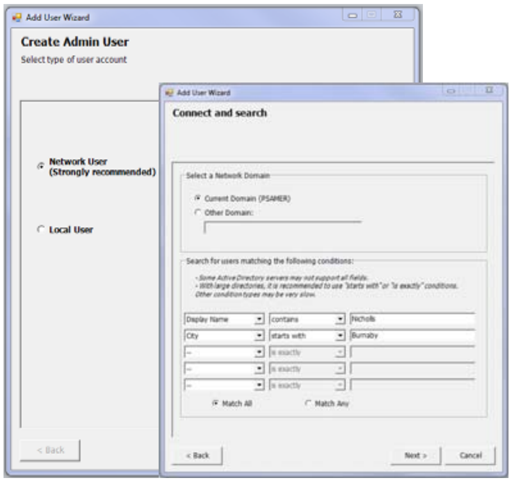
IMPORTANT NOTE: *All users stored in the VistaNET database before VistaNET version 5.04 will be deleted after migrating to VistaNET 5.04 or higher. User credential will no longer be stored in the VistaNET database.*

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



Create Admin User
Select type of user account

● Network User (Strongly recommended)
○ Local User

Connect and search

Select a Network Domain
● Current Domain (PSAMER)
○ Other Domain:

Search for users matching the following conditions:
- Some Active Directory servers may not support all fields.
- With large directories, it is recommended to use "starts with" or "is exactly" conditions. Other condition types may be very slow.

Display Name	contains	Nicholls
City	starts with	Burnaby
--	is exactly	
--	is exactly	
--	is exactly	

● Match All ○ Match Any

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).*

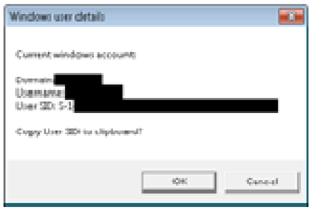
Note: *All users, with Network or Local Windows accounts, require a valid user password. The password field cannot be kept blank.*

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 ℹ 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.

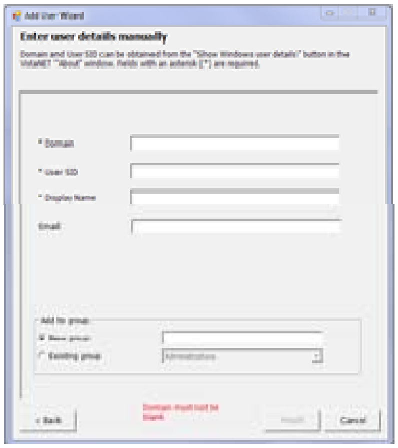


Window user details

Current windows account:

Domain: [redacted]
Username: [redacted]
User SID: S-1[redacted]

Copy User SID to clipboard?



Add User Wizard

Enter user details manually

Domain and User SID can be obtained from the "Show Windows user details" button in the VistaNET "About" window. Fields with an asterisk (*) are required.

* Domain
* User SID
* Display Name
Email

Add to group:
● New group
○ Existing group Administrators

Domain must not be blank

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.*

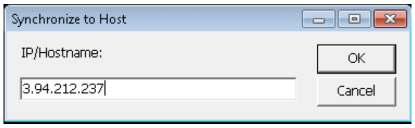
ENABLING REMOTE USERS

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.*

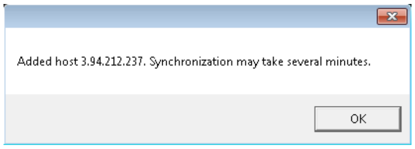
After installing or upgrading to VistaNET 5.04 or higher version, remote users can quickly synchronize to a targeted 24/7 VistaNET service containing remote user account listings and SIDs through a new "Synchronize to Host" prompt.



Synchronize to Host

IP/Hostname: 3.94.212.237

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).



Added host 3.94.212.237. Synchronization may take several minutes.

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

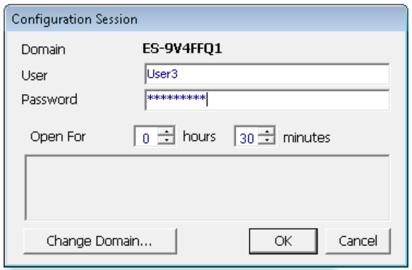
The IP address used to synchronize to Host will be automatically added to the list of unicast IP addresses, contained in the *Administration and Startup Options*, which VistaNET uses periodically (and upon startup) to connect with 24/7 VistaNET instances.

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

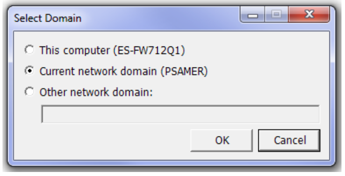
The selected Domain is presented to the user in bold text at the top of the Configuration Session dialog box. A '*Change Domain*' button has been added to this same dialog box to change the selected domain.



Configuration Session

Domain **ES-9V4FFQ1**
User User3
Password *********

Open For 0 hours 30 minutes



Select Domain

○ This computer (ES-FW712Q1)
● Current network domain (PSAMER)
○ Other network domain:

LIMITATIONS

The following is a list of known limitations related to VistaNET 5.12. 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 DCHP 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 Lentronics 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

FIXED DEFICIENCIES

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

Ticket	Summary				Component
Key	Summary	Issue Type	Status	Priority	Resolution
RZBLE-3	Add Ether-1000 ports to the tree and allow to set aliases.	Improvement	Closed	Critical	Fixed
RZBLE-5	Store port aliases in the database.	Task	Closed	Major	Fixed
RZBLE-11	Add Eth-100 ports to the tree	Improvement	Closed	Normal	Fixed
RZBLE-12	24/7 Designation dialog appearance with large fonts	Improvement	Closed	Normal	Fixed
RZBLE-19	Change tooltip for button.	Improvement	Closed	Normal	Fixed
RZBLE-41	Fix Connection Properties Dialog	Improvement	Closed	Normal	Fixed
RZBLE-44	Fix connections list dialog	Improvement	Closed	Normal	Fixed
RZBLE-50	Show path for right Ether-100/1000	Improvement	Closed	Normal	Fixed
RZBLE-51	Increase VistaNET login session to > 10hrs for 24/7 computers	Improvement	Closed	Normal	Fixed
RZBLE-52	Support network configuration of Rack, Shelf, Slot	Improvement	Closed	Normal	Fixed
RZBLE-53	Provide ability for Bulk Rack/Shelf/Slot configuration (plus new license support in separate ticket)	Improvement	Closed	Normal	Fixed
RZBLE-54	Provide license support for Bulk RSS functionality	Improvement	Closed	Normal	Fixed
RZBLE-55	Clear Error Counters /Clear Ethernet Traffic Counters feature	Improvement	Closed	Normal	Fixed
RZBLE-72	Write shortcut modification description.	Task	Closed	Normal	Fixed
RZBLE-74	Certificate expiration date	Bug	Closed	Normal	Fixed

RZBLE-76	VistaNET 5.12.16991 Certain text is no longer displayed correctly for different units under Windows 7	Improvement	Closed	Normal	Fixed
RZBLE-78	VistaNET 5.12.16991 shows version 5.10 help file - needs to be updated to 5.12	Task	Closed	Normal	Fixed
RZBLE-80	Unhandled Exception at GetShortPathElements	Bug	Closed	Major	Fixed
RZBLE-82	"Clear Errors" | "Cancel" buttons and "Select/Unselect All" checkbox are missing from the "Clear Error Counters for <Node | Ring>" dialog box when lower resolution monitor display settings are used	Improvement	Closed	Normal	Fixed
RZBLE-84	Ether-1000 Line Setup - TDM Topology	Bug	Closed	Critical	Fixed
RZBLE-85	Ether-1000 QVLAN Filtering	Bug	Closed	Critical	Fixed
RZBLE-86	UCF fails with long aliases	Bug	Closed	Minor	Fixed
RZBLE-87	Editing Group permission does not save the changes	Bug	Closed	Normal	Fixed
RZBLE-91	Another user login problem in Windows 10	Bug	Closed	Normal	Fixed
RZBLE-99	Universal clear counters feature does not clear any counters.	Bug	Closed	Normal	Fixed
RZBLE-100	Subscriptions stay active when unit view is disabled due to timeout.	Improvement	Closed	Normal	Fixed

FIXED DEFICIENCIES - VERIFYING

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

None.