Contents

1. Purpose of this document

This document describes the security and configuration settings which have to be applied to a PROGNOST® system. If not otherwise specified, the default settings from Microsoft are applied.

2. Responsibility

Responsible for this document is:
Olaf Berens, PROGNOST Systems GmbH, olaf.berens@prognost.com

Request for changes can be addressed to
R&D, PROGNOST Systems GmbH, christian.koers@prognost.com

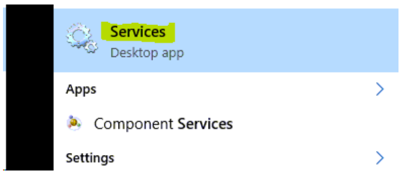
3. How to stop the PROGNOST® Services

Prior to a system shutdown, maintenance or reboot, the PROGNOST services should be stopped manually.

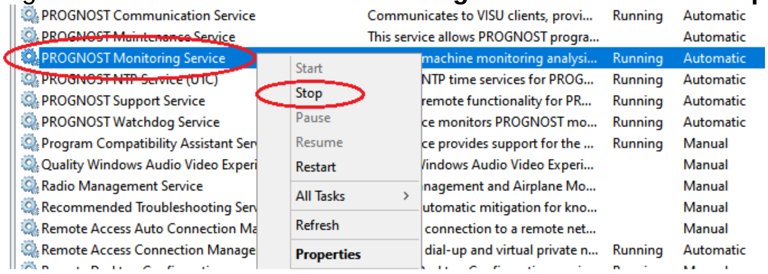
If you follow these steps it is guaranteed that all trend, ring and database files are stored to disk correctly. By quitting the applications in this order your compressor(s) will NOT shut down, but Trend and Ring buffer data are NO LONGER WRITTEN TO DISK. The order is important and should always be followed.

1. To close the PROGNOST Monitoring Service click **Start**, type **Services** and select **Services**

   Alternative:
   Start->Run->Services.msc <ENTER>



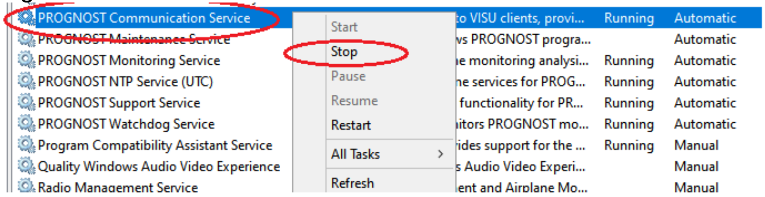
2. Right-click the **PROGNOST Monitoring Service** and select **Stop**



PROGNOST Communication Service	Communicates to VISU clients, provi...	Running	Automatic
~~PROGNOST Maintenance Service~~	This service allows PROGNOST progra...		Automatic
PROGNOST Monitoring Service	machine monitoring analysi...	Running	Automatic
~~PROGNOST NTP Service (UTC)~~	NTP time services for PROG...	Running	Automatic
PROGNOST Support Service	remote functionality for PR...	Running	Automatic
PROGNOST Watchdog Service	ce monitors PROGNOST mo...	Running	Automatic
Program Compatibility Assistant Ser	ce provides support for the ...	Running	Manual
Quality Windows Audio Video Experi	/indows Audio Video Experi...		Manual
Radio Management Service	nagement and Airplane Mo...		Manual
Recommended Troubleshooting Serv	utomatic mitigation for kno...		Manual
Remote Access Auto Connection Ma	connection to a remote net...		Manual
Remote Access Connection Manage	dial-up and virtual private n...	Running	Automatic

Remark: This process takes up to one minute.

3. Right-click the **PROGNOST Communication Service** and select **Stop**



PROGNOST Communication Service	o VISU clients, provi...	Running	Automatic
~~PROGNOST Maintenance Service~~	vs PROGNOST progra...		Automatic
PROGNOST Monitoring Service	e monitoring analysi...	Running	Automatic
PROGNOST NTP Service (UTC)	e services for PROG...	Running	Automatic
PROGNOST Support Service	functionality for PR...	Running	Automatic
PROGNOST Watchdog Service	itors PROGNOST mo...	Running	Automatic
Program Compatibility Assistant Service	ides support for the ...	Running	Manual
Quality Windows Audio Video Experience	s Audio Video Experi...		Manual
Radio Management Service	ent and Airplane Mo...		Manual

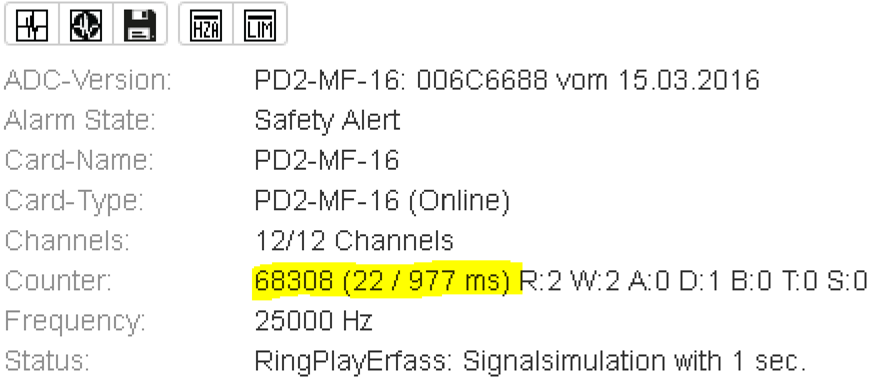
Remark: This process takes up to one minute.

If you follow these steps it is guaranteed that all trend, ring and database files are stored to disk correctly. By quitting the services in this order your compressor(s) will **NOT** shut down, but Trend and Ringbuffer data are NO LONGER WRITTEN TO DISK.

4. System shutdown and reboot

1. Quit all PROGNOST applications as described in Chapter 3
2. To shut down or reboot Windows click on Start->Shutdown
3. After Reboot: Please check that “**PROGNOST Communication Service**” and “**PROGNOST Monitoring Service**” are up and running after system reboot to ensure proper machine safety monitoring. (see chapter 3 for details)
4. Start the Monitoring Dashboard and check if the “Transient counter” is incrementing at least every 5 seconds. This guarantees the correct operation of the complete system and ensures the safety protection of your machine(s).

Example:



ADC-Version:	PD2-MF-16: 006C6688 vom 15.03.2016
Alarm State:	Safety Alert
Card-Name:	PD2-MF-16
Card-Type:	PD2-MF-16 (Online)
Channels:	12/12 Channels
Counter:	68308 (22 / 977 ms) R:2 W:2 A:0 D:1 B:0 T:0 S:0
Frequency:	25000 Hz
Status:	RingPlayErfass: Signalsimulation with 1 sec.

5. Operating system „Windows 10 IoT Enterprise (LTSB)“

In 2018 the default operating system for PROGNOST computers changed from
Windows Embedded Standard 7 to **Windows 10 IoT Enterprise (LTSB)** (english only).

Why does PROGNOST use **Windows 10 IoT Enterprise** for their industrial PC´s?

1. Windows 10 IoT Enterprise offers state of the art security options like secureboot and defender and is configured to fit perfectly to the industrial PC´s hardware components. Windows 10 IOT Enterprise extended support is available until 2029
2. Updates and Patches can easily be installed by using the Cumulative Security Updates from Microsoft.

The PROGNOST VISU Client application is always compatible to the most recent Windows operating systems. (as of 04/2023 this is Windows 11 and Windows Server 2022)

6. Networking

In case a PROGNOST® system is connected to the customers network (Business LAN, DMZ and/or Process LAN), the local IT has to assign a fixed IP address, a Subnet Mask and a default Gateway. Optional a DNS Server and/or SMTP Server can be configured. The PROGNOST® system could optionally be added to the customer's domain (controller). Windows Firewall is activated for incoming AND outgoing traffic on all network interfaces. An optional hardware based Firewall **PROGNOST NetGuard** is also available to protect the PROGNOST Units as well as your network infrastructure.

7. Service pack

All PROGNOST® computers have the most recent Service Packs installed on delivery.

8. Security patches

The most recent Microsoft Security Patches are installed with the shipment of a PROGNOST® system. From that moment on, the customer is responsible to install the patches on its own.
Manual patching via cumulative monthly Updates or automated patching via WSUS is possible.

(PROGNOST offers regular updates and patches as a part of the Service Contract, please ask)

Please also read important information regarding the PROGNOST security philosophy at:
http://www.prognost.com/security/security_e.pdf

9. Approved patches

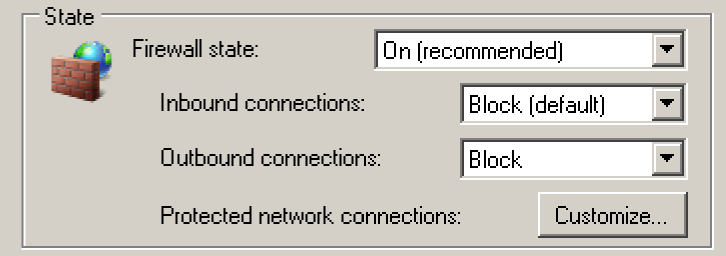
PROGNOST maintained a list of approved MS patches for several years without any single influence to the PROGNOST applications and services.

Now we changed our philosophy to no longer approve single patches. We established a complex automated testing environment which always and constantly runs on the latest patch level. Any problem would now be detected within a few hours from availability at Microsoft. We advise customers to wait one month after Microsoft released Updates/Patches. This will give PROGNOST and Microsoft a period of one month to test and verify. This also enables us to inform our customers about an incompatible patch in time. Please provide contact details for this.

10. Windows firewall

The built in Windows Firewall has to be activated on all PROGNOST® systems which are connected the customers network.

Incoming and **Outgoing** connection MUST be set to **Block:**



State
Firewall state: On (recommended)
Inbound connections: Block (default)
Outbound connections: Block
Protected network connections: Customize...

The following TCP/UDP ports are set on shipment as a default and shall not be changed.
(ICMP v4 is allowed per default but may be disabled upon customer request)

TCP-Ports		UDP-Ports	
25	(E)SMTP (Alarm Email)	7	WOL (optional)
123	NTP (Time Sync)	53	DNS (optional)
443	SILver 2 Status / Dashboard	67/68	DHCP (optional)
502/503	MODBUS	123	NTP (Time Sync)
700	PROGNOST Database Access	5005	NetCmd-Service
3333	Online, Trend, Ringbuffer, DCS data	8010-8015	SILver 2 Datastream
3337	Machine Tree Status Data		
3341	SILver 2 Status Data		
3400/3480	Service Dashboard		
3800	Service and Support Tool		

This table is valid for all industrial computers delivered by PROGNOST
Please refer also to the architectural overview.

The PROGNOST Firewall scripts are located within the desktop folder “Firewall”:
a) _EnableFirewall.cmd (generic rules)
b) _CustomerFirewallRules.cmd (your own specific an optional rules, please change only here)

11. TCP/IP Ports used by VISU Client Software

The following ports are used by the PROGNOST VISU Software product where PROGNOST VISU is the TCP Client and the Communication Unit (within cabinet) is the TCP Server:

TCP-Ports		IP-Protocol	
3341	SILver 2 status information	6	TCP
3333	Configuration Data, Online, Trend, Ringbuffer, DCS values	6	TCP
3337	Machine Status (tree of traffic lights)	6	TCP

This table is valid for all VISU installations at Site (Business LAN, Process LAN or DMZ)
Please refer also to the architectural overview.

12. TCP/IP Ports used by PROGNOST Service Department

In addition to the above TCP/IP Ports used by VISU, the following ports are also used by the PROGNOST Service Department when supporting via VPN, WTS, Citrix, etc.:

TCP-Ports	IP-Protocol

3389	RDP Remote Desktop Client (Option)	6	TCP
3800	Service and Support Tool for System Adjustment and Troubleshooting	6	TCP
5005	Emergency and Recovery Tool (optional)	17	UDP

This table is valid for Remote Access to the PROGNOST Communication Unit (if allowed and available)
Please refer also to the architectural overview.

13. Flow of Information (TCP Port 3333, permanent connection)

1) VISU Client connects to the Communication Unit (SYN)
2) Communication Unit sends Acknowledge (SYN, ACK)
3) VISU Client sends encrypted username and password to Communication Unit (PSH,ACK)
4) Communication Unit sends Acknowledge (PSH, ACK) on success
5) Communication Unit ends connection (FIN, ACK) on failure or timeout
6) VISU Client sends request (Online, Trend, DCS data, etc.) to Communication Unit (PSH,ACK)
7) Communication Unit replies including data (PSH, ACK)
8) Communication continues as described at 6) and 7) for the complete session
9) VISU Client requests session close (FIN,ACK)
10) Communication Unit closes session and replies (ACK)

Please refer also to the architectural overview.

14. Flow of Information (TCP Port 3337, permanent connection)

1) VISU Client connects to the Communication Unit (SYN)
2) Communication Unit sends Acknowledge (SYN, ACK)
3) VISU Client sends encrypted username and password to Communication Unit (PSH,ACK)
4) Communication Unit sends Acknowledge (PSH, ACK) on success
5) Communication Unit ends connection (FIN, ACK) on failure or timeout
6) Communication Unit sends Machine Tree Status Information periodically once per minute or immediately on Status change event.
7) VISU Client send acknowledge (PSH, ACK)
8) Communication continues as described at 6) and 7) for the complete session
9) VISU Client requests session close (FIN,ACK)
10) Communication Unit closes session and replies (ACK)

Please refer also to the architectural overview.

15. Flow of Information (TCP Port 3341, on demand connection)

1) VISU Client connects to the Communication Unit (SYN)
2) Communication Unit sends Acknowledge (SYN, ACK)
3) VISU Client sends encrypted username and password to Communication Unit (PSH,ACK)
4) Communication Unit sends Acknowledge (PSH, ACK) on success
5) Communication Unit ends connection (FIN, ACK) on failure or timeout
6) VISU Client sends request for SILver 2 status data to Communication Unit (PSH,ACK)
7) Communication Unit reads status data from SILver via Monitoring Unit replies including data (PSH, ACK)
8) VISU Client requests session close (FIN,ACK)
9) Communication Unit closes session and replies (ACK)

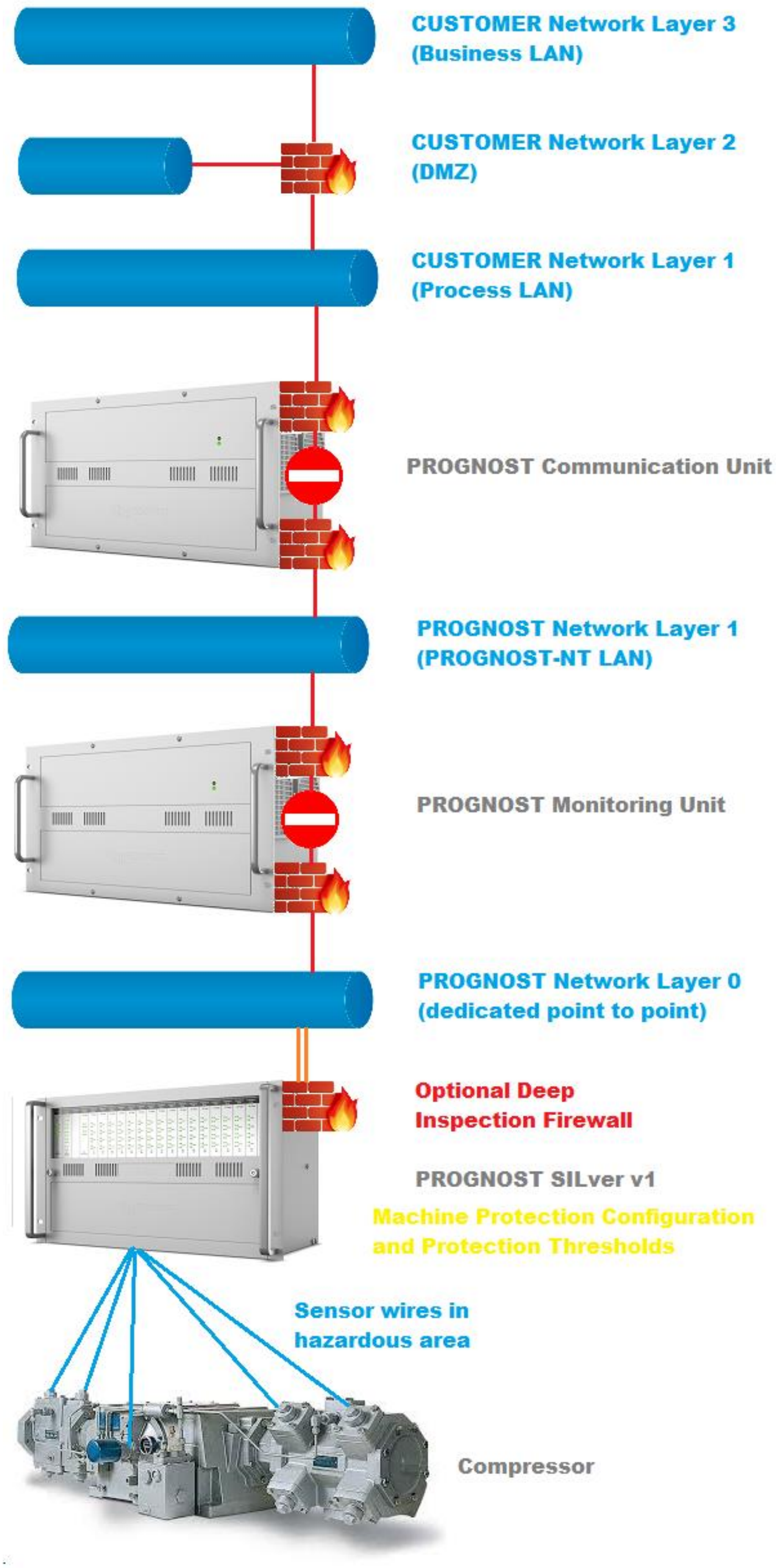
Please refer also to the architectural overview.

16. Securing the Machine Protection Configuration

The Machine Protection Configuration is stored in an internal flash memory chip within the SILver rack. The PROGNOST network architecture ensures a high isolation grade from the customers LAN: (see Image below)

- All Network Cards have Firewall Protection ON
- All Units do not allow any IP forwarding
- No routing active/possible between the PROGNOST network layers
- All PROGNOST Units do have strict password policy active
- Configuration of Safety Settings requires a secret SILver password held by customer (no backdoors for PROGNOST staff or OEM)
- Configuration of Safety Settings requires a dedicated Laptop connected directly to the SILver Rack
- Credentials for remote access to Monitoring Unit could be held by customer, (no backdoors for PROGNOST staff or OEM)
- SILver 2 requires a key switch, username and password to change Safety Configuration
- SILver 1 and 2 Safety Configuration changes can be secured by an optional Firewall having deep packet inspection capability. (e.g. PROGNSOT NetGuard)
  Configuration protocol/requirements/details available on request

Machine Protection is executed just and only within the SILver rack and is independent of any network interruptions or errors. Even loss of any or all PROGNOST unit(s) or network components does not influence the SILver Machine Protection.



CUSTOMER Network Layer 3
(Business LAN)
CUSTOMER Network Layer 2
(DMZ)
CUSTOMER Network Layer 1
(Process LAN)
PROGNOST Communication Unit
PROGNOST Network Layer 1
(PROGNOST-NT LAN)
PROGNOST Monitoring Unit
PROGNOST Network Layer 0
(dedicated point to point)
Optional Deep
Inspection Firewall
PROGNOST SILver v1
Machine Protection Configuration
and Protection Thresholds
Sensor wires in
hazardous area
Compressor

17. USB protection

All PROGNOST Units contain a protection mechanism to prevent from:

- Booting via USB Flash Drives and/or USB Disk drives
- Copying data from and to USB Flash Drives and/or USB Disk drives
- USB Storage Driver Recovery

18. Antivirus solutions

PROGNOST does not offer an antivirus solution by default because most of our customers have a central/corporate antivirus solution in place already or is not necessary, as all critical ports are closed and related windows services are disabled. Please see also: http://www.prognost.com/security/security_e.pdf
PROGNOST software is not compatible to all antivirus solutions. Due to the fact that PROGNOST writes high speed ring and trend data at a rate of up to 5 Megabytes per second, any available antivirus solution will produce a CPU overload condition at this throughput. Therefore the antivirus software has to be configured in such a manner that the high speed signal data streams are excluded from the antivirus scan. This is not a security risk because the related files contain just signal and trend data. There is no executable to be excluded on most antivirus solutions.

Please find a list of tested and approved antivirus solutions for use on PROGNOST in the following chapter. Other products have to be tested and approved by PROGNOST to avoid unwanted influences or interruptions during the data acquisition. PROGNOST is not responsible for any issues related to foreign antivirus products. Please ask for the compatibility of your product.

18.1. Antivirus Exceptions

At least one of the following exceptions should be configured in your Antivirus solution to maintain a performant but secure PROGNOST-NT

18.1.1. Option a) Exception by FOLDER:

-	D:\MONITORING\TREND	(incl. subdirectories)
-	D:\MONITORING\RING	(incl. subdirectories)
-	D:\MONITORING\ONLINE	(incl. subdirectories)
-	D:\MONITORING\LOGS	(incl. subdirectories)
-	D:\KOMMSERV\LOGS	(incl. subdirectories)
-	D:\DATABASE	(incl. subdirectories)

18.1.2. Option b) Exception by process

- Erfass32.exe
- Kommserv.exe

18.1.3. Option c) Exception by file extension:

-	log	(regular ASCII log files)
-	rng	(pure data ringbuffer files)
-	hdf5	(pure data trend files)
-	btr	(BTRIEVE database files)
-	ntdb	(SQLITE database files)
-	ntdb-wal	(SQLITE Write Ahead Log)
-	onl	(pure data online files)

To restrict the available paths for Viruses the “Client for Microsoft Networks” and “File and Printer Sharing for Microsoft Networks” should be deactivated for all network adapters connected to the customer’s network (Business LAN and/or Process LAN).

18.2. Antivirus compatibility list

18.2.1. Approved antivirus solutions (alphabetical order)

Product	Exclusions / Notes
AVIRA AntiVir	PROGNOST processes (EXE-Files) have to be excluded
AVG Business Ed.	
eTrust	PROGNOST directory RING, TREND and ONLINE has to be excluded
Grisoft AVG	Default file extension list has to be used
G DATA Security	PROGNOST processes (EXE-Files) have to be added to the "Exclusions" (Process)
McAfee VirusScan	PROGNOST Directory RING, TREND and ONLINE has to be excluded
McAfee VirusScan	Several PROGNOST directories have to be excluded (see list below) All PROGNOST applications should be specified as "Low Risc Process" which then should not be scanned by the OnAccessScanner In addition the Buffer Overflow Protection must be DISABLED. Otherwise we get very HIGH CPU load within the TrendWriter
McAfee Internet Security	PROGNOST Directory RING, TREND and ONLINE has to be excluded
Norton Antivirus	PROGNOST directory RING, TREND and ONLINE has to be excluded
Symantec Endpoint Protection	V11: PROGNOST processes (EXE-Files) have to be added to the "TrueScan Proactive Scan Exception List"
Symantec Endpoint Protection	V12: PROGNOST processes (EXE-Files) have to be added. (Exceptions>Windows Exceptions>Application to Monitor) or extensions" (log,rng,hdf5,ntdb,ntdb-wal,onl) have to be excluded.
Symantec Endpoint Protection	V13 and above: PROGNOST pure data file extensions must be added to "Security Risk Exception->Extensions" (log,rng,hdf5,ntdb,ntdb-wal,onl)
Trend Micro OfficeScan	PROGNOST directory RING, TREND and ONLINE has to be excluded
Trend Micro SafeLock	Patching Windows / PROGNOST-NT requires special steps within Trend Micro Safe Lock

Other products have to be tested and approved by PROGNOST to avoid unwanted influences or interruptions during the data acquisition. PROGNOST is not responsible for any issues related to foreign antivirus products. Please ask for the compatibility of your product.

18.2.2. Incompatible antivirus solutions

Product	Version	Exclusions / Notes
Norton Antivirus	2005	CPU load to high, no Safety analysis possible
McAffee VirusScan	Enterprise 8.7(i)	CPU load to high, unless "Buffer Overflow Protection" is DISABLED

19. Backup solutions

Due to the fact that PROGNOST writes high speed ring and trend data at a rate of up to 5 Megabytes per second, most available backup solution may produce a CPU overload condition at this throughput. To avoid this, the backup software has to be configured in such a manner that the high speed signal data streams are not interrupted. This could be achieved e.g. by lowering the process priority of the backup software. The operating system files are located on the HDD drive C: (first partition), while all PROGNOST data files are located on the HDD drive D: (second partition). The operating system files do not change during regular operation, therefore they do not need to be backed up often. The PROGNOST data files change continuously, which cannot be stopped without stopping the machine protection. But PROGNOST has developed a specific data storage concept to allow backup during regular operation.
Just the following files will fail to back up:

- D:\MONITORING\RING\xxxxx_actual.rng
- D:\MONITORING\RING\xxxxx_pls_actual.rng

Both files contain just temporary live data and are not needed for a complete restore.

The following Backup solutions have been tested:

- **Acronis Backup and Recovery V10** have been verified as a compatible solution.
- **Microsoft Windows NtBackup** launched in Low Process Priority Mode
- **SEP Sesam 4.x** has been verified as a compatible solution.

If you wish to use other backup solutions that are not listed please contact your PROGNOST product representative.

20. Windows services

20.1. Deactivated services (or set to “manual”)

The following services are “deactivated” or set to “manual” to avoid unwanted influences or interruptions during the data acquisition process.

- Themes
- Print Spooler (manual)
- Telnet Server
- Help and Support
- Wireless Zero Connection
- Shell Hardware Detection
- Fast User Switching
- Indexing
- Print Spooler
- Remote Registry
- Routing and Remote access (manual)
- RPC (Remote Procedure Call) (manual)
- Terminal Services (except remote desktop is required)
- Messenger
- SNMP
- Distributed Link Tracking Client
- Webclient
- Windows Audio
- Windows Time
- **Workstation** (manual)
- **Server** (manual)
- NETBIOS
- DHCP (manual)
- DNS (manual)
- All Gaming Services (XBOX)
- All WLAN Services
- All autoconfiguring Services
- Auto Time Zone Updater

20.2. Network drive access (MAPROGxx and APLPROGxx)

As the Windows Workstation Service is set to “manual” per default, it is not possible to access network drives from a PROGNOST PC. For temporary access there is a batch file on the desktop available which is named “Start Sharing”. This batch file starts the DHCP-, DNS- and Workstation-Service. Afterwards it is possible to access network resources if you own the required username and password for the network resource. You also should always start the other batch file “Stop Sharing” after you are finished with your temporary work on the network.

Remark: Even if you start the Server Service, it will never possible to reach the PROGNOST PC from the network side, because the TCP/UDP ports for the Server-Service are always closed.

21. Time synchronization

PROGNOST has a build in TIME synchronization system, which supports the following standards:

The **Time Protocol** is a network protocol in the Internet Protocol Suite defined in 1983 in RFC 868.
Its purpose is to provide a site-independent, machine readable date and time. The Time Protocol may be implemented over the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).

The **Network Time Protocol (NTP),** is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. NTP provides Coordinated Universal Time (UTC) including scheduled leap second adjustments. The protocol uses the User Datagram Protocol (UDP) on port number 123

The PROGNOST Communication Unit automatically synchronizes the TIME to all connected Monitoring Units. In addition PROGNOST offers TIME synchronization to VISU client PC´s.

Please provide the IP address of your NTP/TIME Server and allow the NTP/TIME protocol (TCP port 123/37) to pass through any firewall in between.

22. Remote control

22.1. Remote control software installed and used by PROGNOST

Each PROGNOST® Industrial Computer has a Remote Control Software installed to enable PROGNOST to give support in abnormal situations. In addition to that, the remote control software is used to modify the system and machine configuration per customer needs. Remote Desktop is disabled as default but could be enabled on customer needs.

22.2. List of approved remote control software products

- ServiceServer (WinVNC, optimized by PROGNOST)
- Teamviewer >v4
- LogMeIn
- Symantec pcAnywhere v9, v10, v11, v12
- STAC ReachOut v6 (no longer in production)

Other products have to be tested and approved by PROGNOST to avoid unwanted influences or interruptions during the data acquisition. PROGNOST is not responsible for any issues related to foreign remote control products. Please ask for the compatibility of your product.

22.3. List of incompatible remote control software products

The following remote control software products have been tested by PROGNOST and are classified to be NOT compatible to PROGNOST® systems due to system overload, I/O blocking, etc.:

- Dameware v4.x v5.x, v6.x
- RealVNC
- UltraVNC
- TeamViewer v4
- PCDUO v8.x (now NetSupport Manager v9.x)