varian

Varian Cybersecurity

Administration Reference Guide

P1055890-003-C

OCTOBER 2024

Legal Information

Publication ID

P1055890-003-C

Publication Title

Varian Cybersecurity Administration Reference Guide

Abstract

This document provides reference information on the Varian policy regarding installation of third-party products on or with Varian products, reference information on data backup processes and guidance for Varian system-specific backups, general security recommendations on ransomware and on securing customer-purchased Varian products, and clarification on the function, purpose, and intent of the MICAP configuration for the following Varian products:

- Treatment Delivery Systems
- Infrastructure running customer-purchased Varian products
- Customer-hosted Software Solutions
- Varian-managed Services and Software as a Service Offerings

This publication is the English-language original.

Notice

Information in this publication is subject to change without notice and does not represent a commitment on the part of Varian.

Copyright

© 2022-2024 Varian Medical Systems, Inc. All rights reserved. Published in Switzerland.
No part of this publication may be reproduced, translated, or transmitted without the express written permission of Varian Medical Systems, Inc.

Trademarks

VARIAN, ARIA, ARIA CORE, BRAVOS, CALYPSO, CLINAC, DOSELAB, ECLIPSE, EDGE, ETHOS, GAMMAMED, HALCYON, MOBIUS3D, NOONA, ON-BOARD IMAGER, PROBEAM, SMARTCONNECT, TRUEBEAM and VITALBEAM are trademarks of Varian Medical Systems, Inc., pending or registered with U.S. Pat. & Tm. Off. All other trademarks are the property of their respective owners.

Contact Varian Customer Support / Report Incidents

For customer support, go to www.MyVarian.com and select **Contact Us**. Use MyVarian to report incidents. If you do not have access to MyVarian, contact your local representative or call +41-41-749-8844.
Any serious incident that has occurred while using the device should be reported to the manufacturer and the competent authority of the Member State in which the user or patient is established.

WHO

ICD-O codes and terms used by permission of WHO, from:

- International Classification of Diseases for Oncology, Third Edition.

ICD-10 codes and terms used by permission of WHO, from:

- International Statistical Classification of Diseases and Related Health Problems, Tenth Revision (ICD-10).

Medical Device

MD

CE 2797

⚠ CAUTION: US Federal law restricts this device to sale by or on the order of a physician.

FDA 21 CFR 820 Quality System Regulations (cGMPs)

Varian Medical Systems, Oncology Systems products are designed and manufactured in accordance with the requirements specified within this federal regulation.

International Organization for Standardization ISO 13485

Varian Medical Systems, Oncology Systems products are designed and manufactured in accordance with the requirements specified within the ISO 13485 quality standard.

ISO 13485 REGISTERED

IEC 62083

This product is IEC 62083 compliant.

EU REACH SVHC Disclosure

The link to the current EU REACH SVHC disclosure statement can be found at http://www.varian.com/us/corporate/legal/reach.html

Legal Manufacturer

Varian Medical Systems, Inc.
3100 Hansen Way
Palo Alto, CA 94304
United States of America

Authorized Representative / Importer in the EU

EC REP

Varian Medical Systems Nederland B.V.
Kokermolen 2
3994 DH Houten
The Netherlands

Table of Contents

Varian Cybersecurity Administration Reference Guide 8
- Introduction 8
- Cybersecurity Checklist 8
- Visual Cues 14
- Definitions 14

Varian Anti-Virus Software Policy 17
- Affected Products 17
- General Anti-Virus Software Policy 17
- Treatment Delivery Systems 17
- Non-Treatment Delivery Systems 17
- Treatment Delivery System Policies 18
- Non-Treatment Delivery System Policies 22
  - Exclusions from Real-Time Scanning 23
  - Real-Time Scanning 27
- Best Practices and Recommendations 29
  - Internet and USB Drives 29
  - Microsoft Operating System Security Updates 29
  - Citrix Endpoint Security and Anti-Virus Best Practices 29

Third-Party Hardware or Software Installation with Varian Products Policy 31
- Affected Products 31
- Installing Third-Party Hardware and Software with Varian Products 31
- Policy for Third-Party Hardware and Software Installation 32
  - Category 1 Products and Policy 32
  - Category 2 Products and Policy 33
  - Category 3 Products and Policy 34
  - Category 4 Products and Policy 36
  - Operating System Policy 37

Database Access Policy 40
- Affected Products 40
- Varian Database Access Policy 40
  - Database Access Rules 40
  - Responsibilities 40

Microsoft (MS) SQL Server as Pertains to Varian Medical Systems Software 42
- Affected Products 42
- Varian Use of MS SQL 42

Varian Responsibilities 42
Customer Responsibilities and Prohibitions 42
Determining the Type and Number of MS SQL Licenses 44
Determining the Edition and Version of MS SQL 45
Running the Varian System Database on a Virtual Server 45
Number of Instances of Installed MS SQL SOFTWARE 45
Replacing the Backup and Database Maintenance Software with Customer Solutions 46
Removing or Disabling Accounts 46
Adding DBA Group Accounts to MS SQL 46
Password Change Policy 47

Backup Guidelines 48
Affected Products 48
Scope 48
Backup Responsibility 48
Backup Solutions 48
Arcserve 49
Other Third-Party Backup Solutions 49
Data Backup Overview and Guidelines 49
ARIA / AURA Database Server 50
ARIA Web (Platform) Server 51
ARIA Image Server 51
DCF Core Installed on a Server 51
Eclipse Clients 51
Eclipse Standalone System 52
Citrix Environment 52
ARIA Connect 52
VelocityGRID Server 52
Backup Frequency 54
Data Backup Exceptions 54
Mobius3D 54
IDENTIFY 55
Backup and Maintenance Tool 56
ARIA 13.X and Earlier 56
ARIA 15.X and Later 57
Restoration and Recovery of Data 58

Mission Critical Application Protection (MICAP) 59
Affected Products 59
Mission Critical Application Protection (MICAP) 59
Classification of Varian Workstations 60

End Point Device Management ... 60
Additional Benefits of MICAP ... 61
MICAP Installations ... 61
MICAP Device ... 62
Customer Security Posture and the MICAP Device ... 66
MICAP Maintenance and Reliability ... 66
MICAP Management Services ... 66
MICAP Sphere ... 67

Securing Varian Products from Ransomware ... 68

Introduction ... 68
Customer Responsibility ... 69
Prepare, Prevent, Respond to the Unexpected ... 69
Prepare ... 69
Prevent ... 70
Respond ... 71
Vulnerability Management ... 72

Varian Digital Certificate Use Policy ... 73

Affected Products ... 73
Varian Digital Certificate Use Policy ... 73
Digital Certificate Use Rules ... 73
Use of Custom Digital Certificates ... 73

SmartConnect Access Control Manager ... 75

Introduction ... 75
Network Access Setup ... 75
Users, Profiles, and Roles ... 77
Confirm Users ... 77
Create a Security Profile ... 78
Create a Role ... 79
Policies, Permission, Access Rights, and Filters ... 80
Create Passthrough Filter ... 82
Apply Passthrough Filter to a Policy ... 83
Create a Maintenance Window for Remote Service ... 84
Add Assets, Group Assets and Create Notification to Approve Access Request ... 88
Approve Pending Requests for Access ... 90
Monitor and End a Remote Session ... 90
Audit Log Information ... 90
Export the Audit Log ... 91
Change the Time Period for a Log Record to Be Displayed in the UI ... 91
Sign In ... 93

Get Quick Help 93

Index 94

Varian Cybersecurity Administration Reference Guide

Introduction

Cyberattacks can enter the network and invade treatment delivery systems and radiation therapy treatment software. This may result in compromised system performance, data loss, data breach, treatment interruptions and outage, and misadministration. It is important to have an information security program that considers the evolving external landscape as new security threats and vulnerabilities are introduced. The program should enable your organization to prepare, prevent, and respond to and recover from a cyberattack.

Varian is committed to keeping your site and your patients defended from cybersecurity threats and attacks. This guide is intended as a helpful reference on Varian policies and use of its treatment delivery software and hardware products.

Review the Cybersecurity Checklist that follows. Then take concrete steps to protect your site, data, and patients as described in this guide.

Cybersecurity Checklist

Table 1 Cybersecurity Checklist for Varian Treatment Delivery Systems

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT	Which firewall is installed between your network and treatment delivery systems?	Check your firewall protection. The Mission-Critical Application Protection (MICAP) firewall is critical for protecting your treatment delivery systems from cyberattacks. For systems predating MICAP, options are available. Contact Varian Customer Support to install and configure the MICAP firewall.	Ensure that your delivery systems are running on the most recently validated MICAP device, firmware, and configuration by contacting Varian Customer Support. Review Mission Critical Application Protection (MICAP) on page 59.

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT	Does your MICAP firewall have the most recent Varian-validated updates to address new vulnerabilities that continually arise?	Contact Varian Customer Support for help with configuring and updating your MICAP firewall.	Rely only on Varian expertise to properly configure your MICAP firewall. Unauthorized and do-it-yourself changes expose your systems to cybersecurity threats and may compromise system performance.
IT	Are your treatment delivery system workstations running the recently Varian-validated Microsoft Operating System?	Coordinate with Varian to Upgrade to the most recently Varian-validated Microsoft Operating System on your workstations to avoid downtime should your system become inoperable. Develop a plan to upgrade Windows workstations with Varian Customer Support.	Ensure that your delivery systems are running on the most recently validated operating systems.
IT, Clinical staff	How are users using treatment delivery workstations? Are they browsing the Internet or checking email? Internet browsing and checking email often introduce malicious software and viruses that compromise performance, cause data loss, and interrupt treatment.	Implement the latest MICAP device and configuration to prevent browsing the Internet and checking email. Develop a plan to upgrade your MICAP device and configuration with Varian Customer Support.	Set and enforce policies banning use of delivery system workstations for activities other than treatment.

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT, Clinical staff	Are users inserting USB drives into the workstations? Using a corrupted USB drive can compromise the cybersecurity of your system.	If available, upgrade to the latest product release that includes Advanced Removable Media Control feature that restricts the use of USB drives. Scan all removable drives on workstations unconnected to the delivery system to help keep workstations free of malware.	Set and enforce policies that permit only approved business use of USB drives and ban unscanned USB drives. Set and enforce policies that only devices with USB hardening can be deployed in your network.
IT	Is any third-party hardware or software that has not been validated by Varian installed behind the MICAP firewall?	Use an independent workstation not connected to the treatment delivery system for third-party hardware or software that is necessary for your clinical workflow, for example, QA Matrix.	Keep third-party hardware and independent computers separate from your treatment delivery system and the MICAP firewall to block inroads for cyberattacks.
IT	Does your backup policy include system administration activity and maintenance data backup for the treatment delivery systems?	Contact Varian Customer Support for help with backing up system, administration, and maintenance data on the treatment delivery systems.	Review Backup Guidelines on page 48. Rely on Varian expertise to properly back up your system as needed.
IT	Is your IT hardware or infrastructure protected by physical security?	Implement physical access control e.g. physical lock to the building, rooms and cabinet where IT infrastructure is stored.	Ensure your organization and IT infrastructure have a disaster recovery plan that includes physical access control.

Table 2 Cybersecurity Checklist for Varian Software

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT	Is your Microsoft SQL Server on the latest Varian-validated version? Review Microsoft (MS) SQL Server as Pertains to Varian Medical Systems Software on page 42.	Coordinate with Varian to install the latest validated Microsoft SQL Server service pack, Cumulative Update (CU) or General Distribution Release (GDR) version. Refer to Knowledge Article 000042700 on MyVarian.com.	Only apply Microsoft SQL service packs, CUs and GDRs that have been reviewed and validated by Varian. This enhances your treatment delivery system uptime and clinical availability.
IT	Do you patch servers and workstations regularly according to the Varian policy statement?	Implement a patch management program within your organization. Review Third-Party Hardware or Software Installation with Varian Products Policy on page 31.	Varian recommends applying latest OS patches as released to Varian Software workstations. Review Operating System Policy on page 37.
IT, Clinical staff	Have you identified key personnel within your organization to be responsible for reviewing update summaries on MyVarian.com?	Register key personnel to carry out your organization’s cybersecurity policies on MyVarian.com.	Assign someone on the team to regularly review update summaries, important notices, and news posted on MyVarian.com.
IT	What is your plan to maintain data integrity and availability in case servers fail or become corrupted?	Implement an infrastructure redundancy plan to protect against failure of primary servers and infrastructure.	Regularly test the standby replacement for production servers and infrastructure to verify they are available if needed. This testing ensures continuity of operations with minimal downtime.
IT	Is your anti-virus software up to date? Robust anti-virus software is a base level requirement for enterprise software.	Varian has policies for installation and configuration of anti-virus software. Review Varian Anti-Virus Software Policy on page 17.	Set policies that comply with the Varian Anti-Virus Policy, described in Varian Anti-Virus Software Policy on page 17.

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT, Clinical staff	Are you prepared for loss of data in case of a natural disaster, system failure, cyberattack, or data corruption?	Have a backup system in place to regularly copy data to secure hardened on-site or off-site locations to enable complete restoration in the event of a disaster. Review Backup Guidelines on page 48. Ensure you have a business recovery plan. Ensure you create a cyberattack response checklist and regularly review and update it.	Develop a plan to constantly monitor your backups and keep them up to date. Backup plans position you to resume treating patients with minimal disruption to care. Periodically test and restore critical data to ensure their integrity. Review Backup Guidelines on page 48.
IT, Clinical staff	Are you protected from power events that can render systems inoperative in case of surges, loss of power, or brown outs?	Confirm that all critical servers and workstations are protected from power-related events. Install qualified surge protection and battery backup devices on all critical servers and workstations.	Regularly monitor whether workstations and servers remain protected against power-related events.
IT	Do you have a segmented network with a firewall between your network and Varian Software products?	Install a firewall between your network and the infrastructure hosting the Varian software products (a firewall for infrastructure outside MICAP) . This is one way to limit/ prevent the propagation of malware within the network.	Ensure that your infrastructure hosting the Varian Software product has a firewall with a policy that only gives access to known traffic. Review Customer Security Posture and the MICAP Device on page 66.
IT	Does your workstation and/or servers hosting the Varian Software product allow all .exe files to run?	Use application allowlisting software to only allow authorized executables and block execution of malicious software (e.g. Ransomware) or greyware (e.g.Adware).	Set an Access Control Policy for your workstation and/or servers using an application allowlisting software.

Your Role	1: Review Your Procedures	2: Prepare for the Unexpected	3: Set a Protection Policy
IT	Do you perform vulnerability scans on your non-treatment delivery system or Varian Software product workstations?	Perform regularly scheduled scans during non-treatment hours to identify systems that are missing security patches, which could expose service and software vulnerabilities. Review Third-Party Hardware or Software Installation with Varian Products Policy on page 31.	Set a vulnerability scan policy for your workstation. Review Varian Anti-Virus Software Policy on page 17. Refer to “Exclusions from Real Time Scanning” and “Real Time Scanning” sections in Non-Treatment Delivery System Policies on page 22.
IT, Clinical Staff	Do you have SmartConnect Access Control Manager installed and configured?	Ensure you have assigned approvers and administrators for Access Control Manager. If not, ensure passthrough filters are configured for trusted users or set access rights to **Always Allow**. Review SmartConnect Access Control Manager on page 75.	Configure the SmartConnect Access Control Manager to align with your security policy. Review SmartConnect Access Control Manager on page 75.
IT, Clinical Staff	Are you practicing good password hygiene?	Practice password hygiene by ensuring staff members, vendors and 3rd party personnel use complex passwords between accounts, do not use commonly used passwords or passwords containing identifiable words, and do not reuse passwords. Ensure accounts are disabled when they are no longer needed.	Work with your IT department to ensure your passwords meet cisa.gov complexity requirements for interactive and non-interactive accounts.
IT	Do you disable accounts (e.g. Privileged accounts, admin accounts etc) that are not in use?	Perform regularly scheduled review of accounts to identify accounts that are not in use by staff members, vendors, 3rd party personnel and systems.	Ensure your security policy is updated to include a statement to disable accounts that are not in use.

Visual Cues

This publication uses the following visual cues to help you find information:

WARNING: A warning describes actions or conditions that can result in serious injury or death.

CAUTION: A caution describes hazardous actions or conditions that can result in minor or moderate injury.

NOTICE: A notice describes actions or conditions that can result in damage to equipment or loss of data.

Note: A note describes information that may pertain to only some conditions, readers, or sites.

Tip: A tip describes useful but optional information such as a shortcut, reminder, or suggestion, to help get optimal performance from the equipment or software.

Definitions

Table 3 Terms and Definitions

Term	Definition
Real-time scanning	Real-time scanning, also referred to as *Auto Protect* is built into most anti-virus packages. Files typically must meet one or more of the following conditions to be scanned: ● On access: files are scanned on any access. ● On read: files are scanned only on read access. ● On write or any file modification: files are scanned only on write. ● On execute: files are scanned when code is executed.
Non-treatment delivery device	Devices that are not directly responsible for delivery of radiation.
Treatment delivery device	Any device or workstation that either delivers, assists in the delivery of, or is used to facilitate the delivery of radiation whether it is for diagnostic or treatment purposes.
Allowlisting software	Identifies entities that are accepted, approved, or recognized.
AD	Active Directory
NAS	Network Attached Storage
SAN	Storage Area Network
FAS	Framework Agent Server

Term	Definition
DCF	Distributed Calculation Framework
DAS	Direct Attached Storage
4DITC	4D Integrated Treatment Console Workstation
Clinac	Varian Linear Accelerator
CNID	Clinac Network Interface Device (legacy term for MICAP device)
CBCT	Cone-Beam Computerized Tomography
CU	Cumulative Update
DES	Data Encryption Standard
DHCP	Dynamic Host Communication Protocol
DMZ	Demilitarized zone
DNS	Domain Name System
EDR/XDR	“Endpoint Detection and Response” and “Extended Detection and Response” (agent) software. EDR/XDR solutions help to detect and block threats on the endpoints based on network traffic, system and user activity monitoring by identifying potentially malicious activities (considering typical tactics, techniques and procedures used by threat actors).
GDR	General Distribution Release
HIPS	Host Intrusion Prevention Software Host Intrusion Prevention Software scans inbound and outbound data packets for malicious content. This scanning can have a negative impact on system performance and is not recommended.
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LinacVI	Linear Accelerator Verification Interface
MICAP	Mission Critical Application Protection
MLC	Multi-Leaf Collimator
NAT	Network Address Translation
NTP	Network Time Protocol
OBI	On-Board Imager

Term	Definition
OSP	Oncology Systems Platform
PV AI	PortalVision Advanced Imaging
RGSC	Respiratory Gating for Scanners
RPM	Real-time Position Management
SIEM	Security Information and Event Management
SP	Service Pack
SSH	Secure Shell
Threat actor	Malicious person or group with the intent to tamper with or exploit IT/OT systems with the objective of impacting the system's operation (availability) or to gaining unauthorized access to networks/systems/data. Unauthorized access may for example consist of accessing a system directly (through exploiting a vulnerability) or through a malware that has managed to infect the system.
UI	User Interface
URL	Uniform Resource Locator (WWW address)
VSP	Varian Service Portal (formerly OSP)
VTN	Varian Treatment Network
XML	Extensible Markup Language

Varian Anti-Virus Software Policy

Affected Products

The Varian Anti-Virus Software Policy is applicable to all Varian Products.

The Varian Anti-Virus Software Policy is applicable to both malware and greyware.

General Anti-Virus Software Policy

Varian does not provide anti-virus, anti-spyware, anti-malware, Host Intrusion Prevention Software (HIPS) software or EDR/XDR with its devices and software products. (Varian does not recommend HIPS, which scans inbound and outbound data packets for malicious content. This scanning can negatively impact system performance and is not recommended.)

The information in this document should be used as a guide on installing and configuring host-based protection software.

When host-based protection software (includes vulnerability scanners, anti-virus, anti-spyware, anti-malware, anti-spyware, anti-greyware, HIPS, EDR/XDR) is installed on a device that is crucial to the operation of the Varian suite of products, Varian recommends that it is configured in accordance with the information in this chapter. Varian policy depends on whether software is used for treatment delivery devices or for non-treatment delivery applications.

Treatment Delivery Systems

A treatment delivery system or device is any device or workstation that either delivers, assists in the delivery of, or is used to facilitate the delivery of radiation whether for diagnostic or treatment.

It is **NOT** permitted to install anti-virus or anti-malware or anti-greyware software or EDR/XDR on computers that are part of a treatment delivery system.

These computer devices use processes that rely heavily on time-sensitive data transfers. Interruptions or delays may interrupt service or cause malfunctions in the affected device or connected devices.

Scans by additional software such as anti-virus, anti-spyware, anti-malware, or HIPS may impact the devices and yield unexpected results.

Refer to Treatment Delivery System Policies on page 18 for additional information on specific systems.

Non-Treatment Delivery Systems

A non-treatment delivery system is a device or devices not directly responsible for delivery of radiation.

Varian highly recommends installing anti-virus and anti-malware software on computers that are not part of the treatment delivery system.

Follow the guidance as stated in Non-Treatment Delivery System Policies on page 22.

Treatment Delivery System Policies

Varian prohibits external protection software (including EDR/XDR) types on devices classified as treatment delivery system computers or workstations. The following table lists the treatment delivery systems covered by this policy, their affected devices, mitigation provided by the product’s Varian Security Framework, and the specific policy.

Table 4 General Treatment Delivery System Policies

Applicable Devices	Varian Security Framework	Policy for external protection software types
4D Integrated Treatment Console (4DITC). On-Board Imager (OBI) Workstation. Cone Beam CT (CBCT) Reconstruction Computer. Real-time Position Management (RPM) Gating Computer. In-Room Monitor Workstations. RPM Workstation. Acuity system Workstation. Clinac Console Computer. Visual Coaching Device (VCD). MLC Workstation. Varian Treatment Workstation. Respiratory Gating for Scanners (RGSC) Workstation. Bravos afterloader system -Treatment Console. Bravos Service Workstation. GammaMed afterloader -Treatment Console. VariSource iX HDR afterloader -Treatment Console. DICOM Worklist – On workstation behind MICAP DICOM Worklist – On Varian System Server (ARIA Database Server) or Image Server, not behind MICAP	MICAP Firewall is required and a component on newer versions of Varian Treatment Delivery Systems. On older versions, Varian strongly recommends having any Treatment Delivery System computers or workstations behind MICAP firewall. The 4DITC v13 MR4 release enhances cybersecurity with a new 4DITC workstation image. Microsoft AppLocker application is included in the image. Microsoft Applocker creates a list of permitted executable programs and blocks operation of zero day and known malware. The release also implements USB hardening to prevent unauthorized use of USB drives and deny them read/write access to the operating system. Other devices such as keyboards, mice, barcode readers are still permitted. For more information, see: ● *4D Integrated Treatment Console (4DITC) v13.0 MR4* Security Update Customer Notification (EOS-00024) on www.MyVarian.com. ● *4D Integrated Treatment Console 13.0 MR4 Customer Release Note* (P1050417) on www.MyVarian.com.	No external protection software types are supported on devices classified as treatment delivery system computers or workstations.

Table 5 TrueBeam and Related Systems Policies

Treatment Delivery Systems	Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
TrueBeam system, TrueBeam STx system, VitalBeam system, Edge radiosurgery system; Ethos radiotherapy system; Halcyon system.	Treatment Workstation. Reconstruction Workstation. In-Room Monitor Workstation. Services Workstation. OSM1 and OSM2 Workstations (Ethos only).	The TrueBeam system deploys these mitigations: ● MICAP, incoming ports are closed. ● MICAP outgoing port 80, 443 TCP connections are only allowed based on an allowlist. ● Varian user shell prevents access to Windows. ● Varian user shell prevents the USB autorun function.	No external protection software types are recommended or supported on devices classified as treatment delivery system workstations.

Table 6 ProBeam System Policies

Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
Proton Treatment Console Workstation. Reconstruction Workstation. Main Control Room Console Workstations. Motion Control System Servers. ProBeam Facility Servers.	ProBeam deploys these mitigations: ● MICAP, all undefined incoming and outgoing connections are blocked ● Application allowlisting on all user consoles to only allow known software (Microsoft AppLocker). ● Systems hardened based on Industry and Regulatory guidelines ● Disabled USB autorun functionality	No external protection software types are supported on devices classified as ProBeam treatment delivery system computers, workstations, or servers.

Table 7 Calypso Extracranial Tracking System Policies

Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
Calypso Tracking Station. Calypso Console PC (in room).	When Calypso extracranial tracking is installed with a Varian Treatment Delivery System, it is installed behind MICAP.	No external protection software types are recommended on devices classified as Calypso treatment delivery system computers or workstations.

Table 8 OSMS (Vision RT) Systems Policies

Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
All products and computers running Vision RT software.	Not applicable.	Contact Varian support if you have questions. ● Sophos anti-virus software is installed and licensed on the workstation during manufacturing. To use an alternative security product, consult with your Vision RT sales or support representative. ● Windows Firewall is enabled during manufacturing. If an alternative firewall is used, then the following exceptions must exist: ● `F:\Vision RT\Common\DICOM\VRTServer.exe` ● Port 104 – inbound, TCP & UDP Additional wide-area connections (WAN) are used to facilitate other services, which benefit Vision RT products. These WAN connections are defined in WAN Connections. To take advantage of the services may require defining these exceptions in a site-wide firewall.

Table 9 Brachytherapy HDR Systems Policies

Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
Bravos Treatment Console. Bravos Service Workstation. GammaMed iX Treatment Console. VariSource iX Treatment Console. Worklist Workstation.	Brachytherapy HDR systems deploy these mitigations: ● MICAP, incoming ports are closed (Port number 106 or 50500 TCP open for inbound DICOM). ● Varian user shell prevents access to the operating system and runs anti-executable, allowlisting software.	No external protection software types are supported on devices classified as Brachytherapy HDR treatment delivery system computers or workstations. **Note:** Brachytherapy HDR treatment console for Bravos, GammaMed iX, and VariSource iX systems, monitor treatments in real time.

Table 10 IDENTIFY Policies

Applicable Devices	Varian Security Framework	Policy for External Protection Software Types
IDENTIFY Room Workstation. IDENTIFY Central Server.	The following mitigation can currently be deployed with the IDENTIFY system: ● On IDENTIFY 2.2 and 2.3: MICAP, incoming and outgoing open ports can be found in MICAP Device, Table 36 List of TCP Ports for IDENTIFY on page 65.	No external protection software types are supported on devices classified as IDENTIFY servers or workstations.
IDENTIFY Windows Planning Tool	On IDENTIFY 2.3: No MICAP is installed between the IDENTIFY Windows Planning Tool and the customer network. The customer is allowed to install their own firewall per incoming and outgoing open ports that can be found in MICAP Device, Table 36 List of TCP Ports for IDENTIFY on page 65.	Varian does not provide anti-virus, anti-spyware, anti-malware or HIPS software with its devices and software products. It is the customer's choice to provide, install, and configure host-based protection software or not. It is the customer's choice to apply Windows operation system updates from Microsoft, either through the Windows Updater or manually via the Windows System Administration, at their discretion.

Non-Treatment Delivery System Policies

Varian highly recommends installing anti-virus and anti-malware software on computers that are not part of the treatment delivery system.

It is recommended to refrain from continuous or real-time scanning of some directories and folders as identified in Exclusions from Real-Time Scanning.

Anti-virus software typically requires frequent updates to remain current against new viruses. It is the customer's responsibility to purchase anti-virus software and maintain associated anti-virus update files.

Perform anti-virus full scan checks only when the affected system is not being used clinically. A false positive anti-virus call-out during intended clinical operation could jeopardize the product operation, patient care, and warranty support.

For more information on real-time scanning, refer to Real-Time Scanning on page 27.

Also, refer to Third-Party Hardware or Software Installation with Varian Products Policy on page 31.

Policies for non-treatment delivery system software and devices apply to these products:

- Server class computers
- Eclipse treatment planning system client workstations
- BrachyVision treatment planning system client workstations

- BrachyVision standalone workstations
- Standard ARIA workstations
- ARIA Unified Reporting Application (AURA) System
- InSightive analytics
- Vitesse
- VariSeed
- ARIA Connect System
- Velocity Server Systems
- Varian Exchange
- One or more FAS (Framework Agent Server) Servers with the Distributed Calculation Framework (DCF) Core installed on them
- Mobius3D
- Visual Coaching Device (VCD)
- DICOM Worklist - On ARIA Client (not behind MICAP)

Exclusions from Real-Time Scanning

Exclusions from Real-Time Scanning for Non-Product Specific List of Folders

Varian recommends refraining from continuous or real-time scanning of the directories listed below on any device where Varian software is running, regardless of whether the device where these directories reside is provided by Varian or not.

The directories and shares are:

- `[Drive]:\Program Files\Varian`
- `[Drive]:\Program Files (x86)\Varian`
- `[Drive]:\VMSOS`
- `C:\Program Files\Acronis`
- VA_DATA$
- VA_ROOT$
- DCF$
- Any directories where DICOM files are stored and used by ARIA applications. For example, CT sets coming in from various modalities, and so on.

Note: [Drive]:\ refers to the primary drive that the indicated directories and / or shares reside on.

All subdirectories under these main directories are included in the exclusion by design.

These directories and their sub-directories contain data or executables that Varian products use in day-to-day operations; they may also contain data in the format of XML files, DICOM files, executables, WOX files, and many other common or proprietary formats, which any anti-virus software may identify as false positives.

Exclusions from Real-Time Scanning for Microsoft SQL Server Database System

Microsoft SQL Server recommends additional exclusions to ensure performance and reliability of the data stored within the database management system.

For more information, see the Knowledgebase Article (KB) from Microsoft,
How to choose antivirus software to run on computers that are running SQL Server.

The directories and shares are:

- [Drive]:\MSSQL directories that hold data in the MDF / LDF / NDF file extensions as well as backup data in the format of BAK and TRN file extensions.
- `[Drive]:\Program Files\Microsoft SQL Server\`
- `[Drive]:\Program Files (x86)\Microsoft SQL Server\`
- Any configured directory that holds TRACE files (.trc), if the server is configured to do so.
- Any configured directory that holds files with the SQLAUDIT file-name extension, if auditing is enabled on the SQL Server.

Exclusions from Real-Time Scanning for the Eclipse DCF Server

Exclude Vulnerability testing on Port 57555, 57567, 57570, 57571 and 57580.

Vulnerability scans performed against the Varian Eclipse DCF Server on Port 57555, 57567, 57570, 57571 and 57580 are known to cause the Varian DCF Distributor Windows service (`VCDDistributor.exe`) to stop or fail. The Windows Event log will record the failure of the service. However, there is no indication of this condition displayed in the user interface until the user is prevented from performing Dose Calculation. The Varian DCF Distributor service would need to be restarted manually on the DCF Server to restore normal treatment planning functionality. In some cases, the DCF agents of Eclipse calculation workstations and FAS may also need to be restarted manually to restore full DCF functionality.

Exclusions from Real-Time Scanning for Velocity Systems

Refer to the following table for directory exclusions from real-time scanning for the Velocity system and its components.

Note: Typical locations are examples, which may differ at your site. Contact Varian Customer Support for help in determining the correct locations.

In the table, N/A means that exclusions by anti-virus software do not apply.

Table 11 Exclusions from Real-Time Scanning for Velocity

Directory	Typical Location	VelocityGRID	VelocityAI
INI Folders (Velocity 3.2)	`%ProgramData%\Velocity Medical Solutions, LLC`	Exclude	Exclude
INI Folders (Velocity 4.0+)	`%ProgramData%\Varian`	Exclude	Exclude

Directory	Typical Location	VelocityGRID	VelocityAI

GRID Database	`C:\Velocity\Database`
	OR
	`D:\Velocity\Database`
		Exclude	N/A

GRID Executable (binary/bin) folder	`C:\Velocity\GRID`
	OR
	`D:\Velocity\GRID`
		Exclude	N/A

AI Workstation (binary/bin) folder	`C:\Velocity\Workstation`
	OR
	`D:\Velocity\Workstation`
		N/A	Exclude

AI Database	`C:\Velocity\Databases`
	OR
	`D:\Velocity\Databases`
		N/A	Exclude

DICOM Listener Folder	User defined	Exclude	Exclude

If Ophthalmic Tomography (OPT) DICOM listener service is running, it MUST be excluded from real-time scanning. Otherwise, this item does not apply.

Exclusions from Real-Time Scanning for InSightive Database Server

To improve server performance for the InSightive server class computer, exclude the following directories and shares:

- `[Drive]:\Program Files\Tableau` OR `[Drive]:\Program Files (x86)\Tableau`
- `[Drive]:\ProgramData\Tableau`

Note: The ProgramData folder is hidden by default. To view it, set the operating system to show hidden files and folders.

Exclusions from Real-Time Scanning for VariSeed and Vitesse

The following exclusions are optional and normally not required for proper system operation. The following lists directory exclusions from real-time scanning for VariSeed and Vitesse systems and components. In the table, N/A means that exclusions by anti-virus software do not apply.

Table 12 Exclusions from Real-Time Scanning for VariSeed and Vitesse

Directory	Default Location	VariSeed	Vitesse
Licensing	`C:\ProgramData\CrypKey\`	Exclude	Exclude
VariSeed Database	`C:\VariSeed 9\`	Exclude	N/A
VariSeed Executable (binary/bin) folder	`C:\Program Files (x86)\VariSeed 9\`	Exclude	N/A
Vitesse Database	`C:\Vitesse 4.0\`	N/A	Exclude
Vitesse Executable (binary/bin) folder	`C:\Program Files (x86)\Vitesse 4.0\`	N/A	Exclude

Exclusions from Real-Time Scanning for ARIA Connect Systems

Refer to the following table for directory exclusions from real-time scanning for the ARIA Connect system to ensure performance and reliability of the configuration data stored within Cloverleaf folder and ARIA Connect program directory.

Note: Typical locations are examples, which may differ at your site. Contact Varian Customer Support for help in determining the correct locations.

Table 13 Exclusions from Real-Time Scanning for ARIA Connect

Directory	Typical Location	ARIA Connect
ARIA Connect Cloverleaf Directory	`[Drive]:\Cloverleaf`	Exclude these directories, all subdirectories, and executables contained therein from real-time scanning of anti-virus software.
ARIA Connect Program Directory	`C:\Program Files (x86)\Varian\ARIA Connect`	

Exclusions from Real-Time Scanning for Mobius3D

Mobius3D requires that ClamAV is used as an anti-virus scanner. No other anti-virus scanner is validated to be used with Mobius3D. The virus scans are completed during nightly maintenance and detected threats are logged. When there is suspicion of a threat, Varian Customer Support will analyze ClamAV log files and repair the system as needed. If the server has access to the Internet with a DNS address configured, the system automatically downloads virus definition updates. ClamAV software updates and virus definition updates are included in Mobius3D software updates.

Exclusions from Real-Time Scanning for ARIA eDoc

The following exclusions are required for ARIA eDoc product operation. The following lists directory exclusions from real-time scanning for ARIA eDoc systems and components.

Table 14 Exclusions from Real-Time Scanning for ARIA eDoc

Directory	Typical Location	ARIA eDoc
ps2pdf.dll	C:\Program Files (x86)\Varian\ARIA IC\ARIAeDoc\FileServer\ps2pdf.dll	Exclude the postscript to PDF conversion DLL file (ps2pdf.dll) from real-time scanning of anti-virus software.

Real-Time Scanning

Many Varian software applications require constant feedback and communication from within the network architecture. Having anti-virus software and/or EDR/XDR configured to automatically run and update itself could interfere with this network communication. Non-treatment delivery devices should only have anti-virus and/or EDR/XDR full scan checks performed when the affected system is not being used clinically. Varian recommends that anti-virus and EDR/XDR software be configured in real-time with on-access and on-read file scanning enabled with exclusions for all non-treatment delivery devices that are involved in the operation of Varian software. The EDR/XDR can use longer than average baselining/profiling period in “Monitor Only” mode on non-treatment delivery devices only if the “Monitor Only” mode is designed to allow all traffic and shows block events as “would be blocked”. The “Monitor Only” feature differs by EDR/XDR and Varian has not validated any EDR/XDR solution.

Varian shall not be liable for any failure of Varian product to perform according to its specifications, nor for any cybersecurity incident or security breach that arises in conjunction with the use of an EDR/XDR “Monitor Only” feature on non-treatment delivery devices. The use of a EDR/XDR “Monitor Only” feature on non-treatment delivery devices voids any warranty, extended warranty, or service support obligation of Varian.

If a customer chooses to use the EDR/XDR “Monitor Only” feature on non-treatment delivery devices, the customer is not allowed to ask Varian personnel to assist, in any way, with the installation of the EDR/XDR “Monitor Only” feature.

Varian disclaims all responsibility or liability arising out of or related to the EDR/XDR “Monitor Only” feature, including, but not limited to, the following:

- Configuration, installation, or support of this EDR/XDR “Monitor Only” feature when used with non-treatment delivery devices.
- The impact of any scripts, reports, or procedures that are developed and distributed about this EDR/XDR “Monitor Only” feature.
- The security or use of any EDR/XDR “Monitor Only” feature with Varian products and/or services.
- Costs, licenses, and administrative functions related to the use of this EDR/XDR “Monitor Only” feature.

If a customer uses, directly or indirectly, an EDR/XDR “Monitor Only” feature on/in Varian non-treatment delivery devices, the customer agrees to indemnify and hold Varian harmless from any and all damages, liabilities, and costs (including attorneys’ fees, litigation expenses, and court costs) that Varian may incur in response to any third-party claim that involves a product, software, or service in which the customer used the EDR/XDR “Monitor only” on/in Varian non-treatment delivery devices.

A false positive anti-virus call-out (anomalies) during intended clinical operation could jeopardize the product operation, patient care, and warranty support. Anti-virus and EDR/XDR software typically requires frequent updates to remain current against new viruses. It is the customer's responsibility to purchase anti-virus and EDR/XDR software and maintain associated anti-virus and EDR/XDR update files.

Note: These real-time scanning recommendations exclude treatment delivery system devices. Also refer to Exclusions from Real-Time Scanning.

Real-Time Scanning Anomalies

Real-time scanning can produce anomalies, impact performance, and cause the non-treatment delivery device to crash.

Performance and Reliability Implications

Every file, when accessed by the system, is scanned by the anti-virus software increasing the time required to load the file by double or more.

The stream of DICOM image data will be scanned, resulting in possible errors due to timeouts and related events. This leads to overall performance degradation.

Possibility of False Positives

Some anti-virus software can erroneously decipher files it cannot “understand” to be viruses, worms (derivatives of viruses), or Trojans (mutations of viruses).

The anti-virus software quarantines the files causing the files to be inaccessible by Varian software. This can cause applications to crash. If possible, configure the anti-virus software to prompt the user whether the file should be quarantined.

Misinterpretation of Data

Some data passed over the network could be misinterpreted as “possibly malicious” scripts, which are halted pending user intervention.

This can negatively impact treatments since the system is waiting for that single script to be executed to perform normally.

Database Backup Routine Slowed or Stopped

Routine system database backups can drastically slow down when real-time scanning is performed.

An entire database backup routine could fail if a marginally suspicious file or script being run requires user intervention to proceed: typically, no users are present to intervene when this happens. This can leave the database server in an inconsistent state and thus unable to function properly during normal clinical operations.

Blocking of Ports by Anti-Virus Software

Some anti-virus software may block communication ports to prevent potential attacks from outside computers.

Varian recommends that ports not be directly blocked on any host device. This task is best performed by a Hardware Network Firewall device.

Consult Varian Customer Support for a list of ports needed for your software version.

Auto-Update Program for Anti-Virus Files

Anti-virus programs can use network bandwidth. If the anti-virus auto update utility is set to auto-update definition files during operational clinical hours on treatment delivery devices, these workstations and servers will experience slow-downs and could possibly crash. The application may crash or freeze when the CPU resources it needs are being utilized by the update utility.

Best Practices and Recommendations

Internet and USB Drives

Most Varian software is designed to operate on the most common versions of Microsoft Windows operating systems. Microsoft Windows-based workstations are often used to run other applications such as e-mail or word processing. These workstations are on a network and many of these workstations have internet connectivity. This environment is susceptible to the transmission of computer viruses via the internet.

By default, Microsoft Edge is included with the Microsoft Windows operating system software and is loaded onto every workstation.

Varian strongly discourages internet browsing and downloading files on the treatment delivery devices.

USB drives are transport vehicles for malicious software: they never should be used on treatment delivery devices without first being thoroughly scanned on a non-connected device. Varian recommends disabling USB ports or restricting USB ports if needed.

NOTICE: USB drives pose the highest risk factor for malware being able to propagate to/infect treatment delivery devices located behind MICAP firewalls!

Microsoft Operating System Security Updates

Varian recommends that users review these sites regularly for updated information.

- For Varian standalone software, refer to: Microsoft Operating System Security Update Recommendation for Varian Standalone Software, Operating System Policy on page 37, and Customer Responsibilities and Prohibitions on page 42.
- For treatment delivery systems, refer to Securing Varian Products from Ransomware on page 68, Operating System Policy on page 37, and Customer Responsibilities and Prohibitions on page 42.

Citrix Endpoint Security and Anti-Virus Best Practices

Varian recommends that the advice listed at the following site be implemented at site if Citrix is used to deliver applications, in particular the Antivirus Exclusions section:

https://docs.citrix.com/en-us/tech-zone/build/tech-papers/antivirus-best-practices.html

Varian recommends reviewing the content regularly for updated information.

Note: Any system or device not listed in the Varian Anti-Virus Software Policy section does not fall within the scope of the policy but may still be affected by recommendations contained within this document.

Third-Party Hardware or Software Installation with Varian Products Policy

Affected Products

The third-party hardware or software installation with Varian Products is applicable to all Varian products. In addition to this policy, refer to the product customer release notes for additional information.

Installing Third-Party Hardware and Software with Varian Products

The policy on installation of third-party hardware and software addresses all third-party applications installed on or used with any Varian hardware, software, or service, with the exception of anti-virus applications addressed in Varian Anti-Virus Software Policy on page 17.

The policy addresses three categories of products:

Category 1: Software products that have been tested with some third-party software (for example, Microsoft Word) and generic computer hardware for general compatibility for use with Varian products.

Category 2: Software products that have been tested with generic server hardware and specific third-party software.

Category 3 and Category 4: Products in this category contain both hardware and software provided by Varian. These have been tested with specific configurations of computer hardware and specific third-party software.

All Category 1 and 2 products were designed to maximize customer choices of brands, models, and vendors for hardware, networking, and system software where feasible. Although hardware platforms lend themselves to use with other third-party software and hardware, it is important that users understand the ramifications of such a decision.

Most products listed in categories 1 through 4 were designed for operations with a dedicated database server, and these will have best response times and performance if the database server and/or image file server remain dedicated to those products.

The servers used by products listed in the product category-specific tables (see section Policy for Third-Party Hardware and Software Installation) are not suited for file, print, or other types of services. Varian recommends that additional dedicated servers be used for these tasks.

Day-to-day operations outside the domain of Category 1 products can be served by third-party software such as desktop office, quality assurance, e-mail communication, and Internet access applications that were not validated by Varian Medical Systems, Inc. Installation of any third-party software not included in the products within Category 1, Category 2, Category 3 and Category 4 results in a configuration that has not been validated by Varian. Hence, Varian does not market or sell products for such use and makes no claims or warranty about the safety or efficacy of these third-party software not validated by Varian as part of the FDA-compliant Varian validation process or any other regulatory validation process, for use with Varian products.

Policy for Third-Party Hardware and Software Installation

Category 1 Products and Policy

Table 15 Third-Party Hardware and Software Installation for Category 1 Products

Category 1 - Products	Policy
ARIA Practice Management Clients ARIA Radiation Oncology Clients DICOM Worklist-On ARIA Client (not behind MICAP) Comprehensive Cancer Solution Clients ARIA Medical Oncology Clients InSightive Clients InSightive Desktop Application ProBeam Research User Interface ProBeam Eye Patient Manager Client Velocity GRID Client	Customers are not prohibited from loading third-party applications on the same workstations that operate Category 1 products nor from patching these workstations. General classes of server software such as backup or anti-virus may be used. Varian has not tested all third-party software. Some third-party productivity software was tested (for example, Microsoft Word) for general compatibility for use. It is the customer's responsibility to ensure that: ● Any general class of server software does not interfere with the operations of Category 1 products listed in this table (or their associated applications within a product family). ● Any generic workstation hardware for use with Category 1 applications meets the minimum or recommended specifications provided by Varian for specific versions of Varian products (Refer to www.MyVarian.com.) Varian has tested Category 1 products on generic workstation hardware for general compatibility for use. ● Patient data integrity is always maintained. ● Workstations operating Category 1 products are patched and updated.

Category 2 Products and Policy

Table 16 Third-Party Hardware and Software Installation for Category 2 Products

Category 2 - Products	Policy
Varian System Server (also called ARIA Database Server) ● MS SQL Database (depending on version of Varian software) ● Oncology Systems Platform (OSP) ● Shared Framework ● VAIS (Varian Authentication and Identification Services) ● DICOM Services ● RePortal ● DICOM Worklist - On Varian System Server (not behind MICAP) Image Server ● DICOM Worklist - On Image Server (not behind MICAP) High Availability & Rapid Recovery Protection (HARRP) Information Exchange Manager (IEM) / ARIA Connect Docs2EHR E-Prescribe XmediusFax Citrix Thin Client Server(s) ● Radiation Oncology ● Medical Oncology AURA InSightive Equicare Patient Portal Oncology Cancer Registry OncQT OncoView ProBeam Eye Treatment Database ● MS SQL Server ● Eye Database Services	General classes of server software such as backup or anti-virus may be used. However, Varian has not tested all third-party software. Refer to Non-Treatment Delivery System Policies on page 22 (in chapter Varian Anti-Virus Software Policy). Varian requires that the database integrity be maintained in the manner developed and implemented, and consistent with the cleared labeling. **Third-party software should not be loaded on database servers that might host or service any of the Category 2 products listed.** Refer to the product's manual or technical advisory for patch policy. It is the customer's responsibility to ensure that: ● Any generic server hardware for use with Category 2 products meets the minimum or recommended server specifications provided by Varian for specific versions of Varian products. (Refer to www.MyVarian.com.) Varian has tested Category 2 software products on generic server hardware. ● Third-party software and/or third-party server software does not interfere with Category 2 products listed in this section (or their associated applications within a product family).

Category 2 - Products	Policy
Eye Position Verification System Velocity ● GRID Server ● Standalone	

Category 3 Products and Policy

WARNING: Installation of any third-party software not authorized by Varian on any computer system servicing Category 3 products may result in injury to patients.

NOTICE: Installation of any third-party software not authorized by Varian on any computer system servicing Category 3 products may damage the equipment, cause loss of data, and / or jeopardize warranty support.

Table 17 Third-Party Hardware and Software Installation for Category 3 Products

Category 3 - Products	Policy
VariSeed Vitesse Varian HDR Treatment Console ● Bravos Treatment Console ● Bravos Service Workstation ● GammaMed iX Treatment Console ● VariSource iX Treatment Console ● DICOM Worklist - On Workstation behind MICAP Simulation ● Acuity 4D Integrated Treatment Console ● 4DITC ● Linac Verification Interface (LVI) TrueBeam, VitalBeam, Edge, TrueBeam STx, Halcyon, and Ethos radiotherapy system console ● Treatment Workstation ● Reconstructor Workstation ● Service Workstation ● In Room Monitor Workstation ● OSM1 and OSM2 Workstations (Ethos only) ProBeam ● Proton Treatment Console Workstation ● Reconstructor Workstation ● ProBeam Facility Servers ● Main Control Room Console Workstations ● Motion Control System Servers OBI systems CBCT Mobius3D Varian Treatment (VTx) (also called Non-Varian Treatment (NVT)) ● Treatment Console ● Linac Verification Interface (LVI)	● The customer is prohibited from installing any third-party application (except validated anti-virus software as identified by the labeling, for example, Customer Release Notes) on any workstation or server hosting Category 3 products. ● The customer is prohibited from patching servers or workstations operating Category 3 products behind MICAP. For workstations or servers operating Category 3 products outside MICAP, refer to the product's manual or technical advisory for patch policy. These computers require live interfaces with medical devices used for patient planning, treatment delivery, and simulation, and they are considered critical elements to patient care.

Category 3 - Products	Policy
Patient Positioning Management - Calypso (HCL) - Respiratory Gating - Respiratory Gating for Scanners (HGS) - IDENTIFY (Room Workstation and Central Server)	

Category 4 Products and Policy

WARNING: Installation of any third-party software not authorized by Varian on any computer system servicing Category 4 products may result in injury to patients. Refer to customer release notes, product security whitepaper and/or manuals for authorized third-party software.

NOTICE: Installation of any third-party software not authorized by Varian on any computer system servicing Category 4 products may damage the equipment, cause loss of data, and/or jeopardize warranty support.

Table 18 Third-Party Hardware and Software Installation for Category 4 Products

Category 4 - Products	Policy
Eclipse treatment planning system - Eclipse Calculation Workstations - Eclipse Non-Calculation Workstations BrachyVision treatment planning system - BrachyVision Client Workstation - BrachyVision Standalone Workstation FAS (Framework Agent Server)	- The customer is prohibited from installing any unauthorized third-party application on any workstation or server hosting Category 4 products. - The device driver updates of Category 4 products should not be applied. All device driver updates must be validated. The most sensitive device driver is the GPU. The customer can patch only the OS of servers or workstations operating Category 4 products. Some OS update may come with device driver updates, only the OS update should be applied and not the device driver update. Refer to the Category 4 product's manual, instruction for use or product labeling documents for more patch policy information. These computers require live interfaces with medical devices used for patient planning, treatment delivery, and simulation, and they are considered critical elements to patient care.

Operating System Policy

⚠ WARNING: Updates and/or upgrades to the operating system (OS) that require a version and OS build change should not be performed on Varian systems without Varian validation. All operating systems behind the MICAP firewall should not be updated without Varian validation.

The table below provides a guide for updating an operating system within the same version and “OS build number”. “✓” indicates that OS and device drivers of the same version and same “OS build number” can be updated. This includes Cumulative Updates (CU) and General Distribution Release (GDR) within the same OS version and “OS build number”. Microsoft Service Pack (SP) should not be applied without Varian validation.

“O” indicates that only the OS within the same version and “OS build number” can be updated. This includes CUs and GDR within a specific OS version and “OS build number”. However, all device drivers should not be updated without Varian validation. Device driver updates should not be performed when the CUs and GDR are applied within the specific OS version and “OS build number”. Microsoft Service Pack should not be applied without Varian validation. For example, a system using Windows 10 Enterprise LTSC 1809 OS build number 17763 should only apply CUs and GDR for OS build number 17763. In this example, the device driver for OS build number 17763 should not be updated.

“I” indicates that only the OS and device drivers of the same version and “OS build number” can be updated. This includes CUs and GDR within the same OS version and “OS build number”. Microsoft Service Pack should not be applied without Varian validation. The Citrix Workspace Application version or Citrix XenApp Server of the same build can be updated. Upgrades to a different Citrix build are not allowed without Varian validation. Varian validates its software with supported Citrix build versions on a specific Windows Version and “OS build number”.

Review the specific Varian product version release notes and technical specification guide for the validated OS version and OS build number.

Table 19 Operating System Update Guide

	Operating System	**Security Updates**
ARIA Thick-Client Workstation	Microsoft Windows XX Version XXXX	✓
Citrix Thin-Client	Citrix Workspace App XXXX - Citrix Receiver version on MS Windows XX Version XXXX	I
Eclipse Calculation Workstation	MS Windows XX Ultimate MS Windows XX Enterprise LTSB XXXX MS Windows XX Enterprise LTSC XXXX	O

	Operating System	Security Updates
Eclipse Non-Calculation Workstation	MS Windows XX Ultimate LTSB XXXX MS Windows XX Enterprise LTSB XXXX MS Windows XX Enterprise LTSC XXXX	O
Database Server (except Combo)	Microsoft Windows Server XXXX	✓
Database Server (Combo only)	Microsoft Windows Server XXXX	✓
Data Warehouse (“DW”) Server (AURA Server)	Microsoft Windows Server XXXX	✓
Platform Server (Standalone)	Microsoft Windows Server XXXX	✓
Platform Server (Combo)	Microsoft Windows Server XXXX	✓
File Server	Microsoft Windows Server XXXX	✓
Platform & File Server	Microsoft Windows Server XXXX	✓
DICOM Server (not behind MICAP)	Microsoft Windows Server XXXX	✓
DCF Server (Core)	Microsoft Windows Server XXXX	✓
FAS (Framework Agent Server) Server	Microsoft Windows Server XXXX	O
T-Box Server (test)	Microsoft Windows Server XXXX	✓
Interface Server – Information Exchange Manager (IEM)	Microsoft Windows Server XXXX	✓
Interface Server – ARIA Connect	Microsoft Windows Server XXXX	✓
Citrix XenApp Server Specifications for Radiation Oncology Client Application Virtualization	Microsoft Windows Server XXXX	I
Citrix XenApp Server Specifications for Medical Oncology Client Application Virtualization	Microsoft Windows Server XXXX	I
ARIA CORE MOBILE Server	Microsoft Windows Server XXXX	✓
Insightive Server	Microsoft Windows Server XXXX	✓
Always On availability groups for SQL Server Enterprise	Microsoft Windows Server XXXX	✓
Velocity Standalone Workstation	Microsoft Windows XX Version XXXX	✓

	Operating System	Security Updates
VelocityGRID Server	Microsoft Windows Server XXXX	✓
VelocityGRID Client	Microsoft Windows XX Version XXXX	✓
VelocityGRID Server Virtualization	Microsoft Windows Server XXXX	✓
VelocityGRID Client Application Virtualization	Microsoft Windows Server XXXX	✓

Database Access Policy

Affected Products

This Database Access policy applies to Eclipse, BrachyVision, ARIA Oncology Information System (OIS) for Medical Oncology (MO), ARIA OIS for Radiation Oncology (RO), InSightive, and ARIA CORE Mobile (previously called Varian Mobile) App software and applications. Not Applicable to Velocity as it uses an embedded PostgreSQL which is not accessible outside the Velocity Application. The Velocity database is not accessible over the network and is only accessed in-memory internally by Velocity software.

Varian Database Access Policy

All Varian software systems are based on client server architectures that allow many other systems to query the related database or databases. Any client application that accesses the database must do so responsibly. Failure to follow certain rules may give rise to severe performance impacts on the system and, in the worst case, loss of critical data.

Database Access Rules

Varian requires that all client applications follow these rules:

1. Any application inserting or updating data in any Varian database server or system must use the ARIA Connect API or similar Varian approved linking programs or APIs. Failure to do so may invalidate referential integrity of data within the database and cause loss of data.
2. For any client application accessing any Varian database, a dedicated account has to be created with the minimal set of required privileges (e.g. restricted to use tables, limited to read-only).
3. Before using an SQL query to query a database, users must first test the SQL query to ensure that it does not lock tables and impact database performance. Varian recommends testing all new queries outside normal operating hours or against an ARIA Reports server.

Failure to follow these rules would cause use of the product to fall outside the scope of the 510(k) clearance, regulated industry standard testing, and the cleared labeling for the device. Such unauthorized use could jeopardize patient care, clinical operations, and warranty support.

Responsibilities

Varian is not responsible for the following:

- Configuration, installation, or support of any data access software such as Open Database Connectivity (ODBC) or ActiveX Data Objects (ADO) drivers.
- Providing logging information of client application data access to Varian Database (e.g. HIPAA mandated logging for accessing data containing PHI). The customer is responsible for keeping track and logging when their application is accessing Varian Database.
- The impact of any scripts, reports, or procedures that are developed and distributed in the user community.
- The security or use of any third-party application that is accessing a Varian database.

Customers are not prohibited from running any report. However, we do not recommend customers run queries against production database. The read and write access should be via published API, reports and queries against the AUR. It is the user’s responsibility to ensure that any reports and applications run do not interfere with the operation of any Varian database and applications.

Microsoft (MS) SQL Server as Pertains to Varian Medical Systems Software

Affected Products

Varian uses MS SQL as the third-party database software to support Eclipse and Varian OIS (ARIA OIS for RO and MO). This information is applicable to these Varian products.

Varian Use of MS SQL

Varian has an Independent Software Vendor (ISV) license agreement with Microsoft, which restricts the MS SQL licenses supplied by Varian for use with Varian software.

An ISV license is a Microsoft License that software developers such as Varian can use to package MS SQL with their software. The license restricts the MS SQL software to be used only with provided Varian software and cannot be used with any other third-party products.

Varian uses MS SQL Standard edition, which is allowed to be moved from one server to another only once in any 90-day period.

Varian Responsibilities

Varian personnel are responsible for the initial installation of the SQL Server software.

Varian will maintain the MS SQL Software Assurance provided that a Varian customer maintains an SSA (Software Support Agreement) on the Varian System Database. Doing this ensures that the MS SQL software is covered under Microsoft’s Software Assurance.

Varian is not responsible for the database if the customer modifies any part of the system. The database is part of an FDA-regulated medical device, and altering it invalidates the product’s clearance. Varian strongly recommends that customers, before modifying any part of the system, document the changes to allow for proper customer troubleshooting and maintenance if needed.

Varian is not responsible for the customer's misuse of the administrative accounts. Varian is not responsible for any impact on the system or patient treatments due to delays in servicing the system if the customer changes account passwords.

Other responsibilities and restrictions are described within the specific topics.

Customer Responsibilities and Prohibitions

It is the customer’s responsibility (or that of their IT department) to keep the Operating System used by SQL Server patched with all critical updates and patches as released from Microsoft. For anti-virus software and related queries, refer to the following sections:

- Non-Treatment Delivery Systems on page 17
- Non-Treatment Delivery System Policies on page 22
- Category 2 Products and Policy on page 33

Administrative accounts provide unlimited access to the database. Misuse of these accounts can seriously impact the system. The customer is responsible to use its administrative accounts responsibly and safeguard these accounts from unauthorized use or misuse.

It is NOT permissible to apply any blanket MS SQL service packs, GDR updates and /or cumulative updates without prior authorization from Varian. The customer is responsible for getting authorization from Varian before applying any blanket service packs or updates.

Applying service packs, GDR updates and cumulative updates can jeopardize performance, usability, future updates, and serviceability. If software patches were inadvertently applied, it is the customer's responsibility to revert the state of the SQL Server to a valid installation base prior to any service work being done upon said server.

Note: Always ensure that valid and verified backups of the user databases exist before applying any form of software patches to the Microsoft SQL Server database engine.

The table below provides a guide for updating SQL Server within the same version and SQL build number. "X" indicates that SQL Server should not be updated regardless of Cumulative Updates (CU), General Distribution Release (GDR) or service pack versions.

Table 20 Microsoft SQL Server Update Guide

	Operating System	Security Updates
Database Server (except Combo)	Microsoft SQL Server XXXX	X
Database Server (Combo only)	Microsoft SQL Server XXXX	X
Data Warehouse ("DW") Server (AURA Server)	Microsoft SQL Server XXXX	X
T-Box Server (test)	Microsoft SQL Server XXXX	X

The customer may use third-party monitoring software provided the tools do not modify the running system (see Third-Party Hardware or Software Installation with Varian Products Policy on page 31). The customer is entirely responsible for any negative effects on system performance due to the use of any software installed on the server. If any performance impact and/or operational anomaly is detected when additional software is installed on the server, Varian will not be able to test/analyze what the root cause may be (due to lack of monitoring or identical test environment). Therefore the customer will have to take the responsibility for analyzing and determining the cause.

The customer is prohibited from doing the following, which will invalidate the warranty:

- Installing Varian System Database using the customer's current MS SQL installation. The MS SQL software is installed using a custom installer designed to support a proper installation of the Varian System Database. Varian does not support installation of the Varian System Database into an existing MS SQL farm or using customer supplied installation media.
- Updating or upgrading the Varian supplied software.

Only versions officially supported by Varian can be used, even if customers supply their own MS SQL license. The supplied Microsoft SQL database software manages data for use with devices that control treatment of patients on Radiation Therapy devices that can deliver potentially harmful doses of radiation. Varian tests its software against a specific version of Microsoft SQL database software and cannot guarantee the proper operation of its software with any version of MS SQL software that it has not tested. Customers must ensure that any automatic software update policies exclude the computer housing the Microsoft SQL Server Database and its engine.

Varian does not authorize or allow anyone but trained Varian personnel to update or upgrade the SQL Server engine on a system where clinical data resides. This includes (but is not explicitly limited to) service packs, optional updates, language packs, version upgrades, and core changes, among other updates.

- Using built-in MS SQL clustering / mirroring / replication.

  The database is part of an FDA Class II medical device and requires strict testing to ensure proper operation. Varian has not tested and does not support the use of the built-in clustering, mirroring, or replication features of Microsoft SQL at this time. This may change in the future if the technology is adopted as part of a validated release by Varian.

- Modifying Varian Databases, Tables, and Stored Procedures.

  Any change to the Varian schema is strictly prohibited.

  Altering the contents of databases immediately invalidates all implicit and explicit warranties with respect to system performance in accordance with Varian’s Standard Terms and Conditions of Sale. The database schema for any Varian-owned databases is proprietary, and cannot be modified in any form, either through addition or deletion of any objects contained within, including but not limited to logins, stored procedures, indices, tables, views, structures, and so on.

  Varian cannot, does not, and will not test or qualify any given software release with customer-specific changes in the database.

  If needed, customers can either create another database containing their own schema on the same database server (assuming liability for performance impacts, maintenance, backups, etc.) or do remote queries from another owned SQL Server that is distinct from the one that houses the Varian supplied databases. ARIA API is the preferred and recommended method to collect data from the ARIA database. SQL authentication is currently not supported.

  Contact Varian Customer Support before making any alteration to the Microsoft SQL Server.

Determining the Type and Number of MS SQL Licenses

Customers have either a combination of User & Device CAL (Client Access License) or CPU CAL (Central Processing Unit CAL) depending on the number of users of Varian products.

Products such as 4DITC, OBI, CBCT, and TrueBeam Console are always covered under a Device CAL regardless of whether Varian also supplies User or CPU CALs for other Varian software accessing the Varian System Database.

On request, Varian will provide a report of the number and type of MS SQL licenses that have been installed at a customer site. Requests should be submitted to the customer’s site Service Manager.

Determining the Edition and Version of MS SQL

As of May 2024, Varian supplies

- ARIA Versions 18.x - Microsoft SQL Server 2019 CU9
- ARIA Versions 17.x - Microsoft SQL Server 2019 CU9
- ARIA Versions 13.x, 15.x, and 16.x - Microsoft SQL Server 2014 Standard SP3 CU4
- ARIA Versions 13.x below 13.6 - Microsoft SQL Server 2012 Standard
- ARIA Version 11 - Microsoft SQL Server 2008 R2 Standard (Cumulative Update 8)

Although Varian supplies the above Microsoft SQL Server with the hardware system, check the knowledge article 000042700 on http://myvarian.com/ for any updates regarding the latest Varian validated version of MS SQL software.

Microsoft Audit

Varian reports to Microsoft the MS SQL licenses that it supplies and manages for use with Varian products. Thus, customers need to provide to the Microsoft auditor only the Varian ISV Royalty agreement number, 8573616, in their “exclusions list”. This information identifies for Microsoft that the MS SQL software used to support Varian software is covered under a specific ISV program and directs the auditor to follow up with Varian as needed.

Customer Enterprise Agreement with Microsoft

Customers with an enterprise agreement with Microsoft can use their own licenses and cover the MS SQL software under their own Enterprise licensing agreement. However, the customer then is entirely responsible to ensure that its license covers all use by the end users of the supplied MS SQL software with Varian software, including tracking and reporting to Microsoft in case of a Microsoft audit.

Running the Varian System Database on a Virtual Server

With some limitations, the customer may run the Varian System Database on a virtual server. Refer to the product technical specifications document for applicable limitations.

For MS SQL with CPU CAL-type licenses, customers must not enable hyper-threading, and the number of cores assigned to the running instance of MS SQL must equal or be less than the maximum number of cores in the physical server. In addition, for failover purposes the number of cores in the failover server must equal that on the production server.

Number of Instances of Installed MS SQL SOFTWARE

Microsoft allows any number of instances of the MS SQL software to be installed, but only one running instance may be active at any time. For failover capability, Varian customers may have one other “non-running-instance” installed provided that the MS SQL software on the secondary server is not active. In keeping with Microsoft licensing practices, the two instances may not be run at the same time except while recovering the production instance.

Replacing the Backup and Database Maintenance Software with Customer Solutions

The customer may remove current backup and database maintenance software and instead use the customer's solution.

However, removing the Varian supplied maintenance scripts and backup routines has these risks and consequences:

- The Varian supplied software is validated as part of an FDA regulated medical device. Changing the operating parameters adulterates the device.
- Varian cannot validate any customer designed scripts nor guarantee that they will operate properly.
- Varian may not be able to recover the database to its latest iteration if the customer uses customized backup or maintenance scripts to maintain the database and they fail.
- Varian may not be able to guarantee or improve on any performance issues caused by incorrect maintenance being performed on the server.
- Varian may not be able to guarantee integrity of the database if external maintenance is being performed on the database.

If the customer modifies any part of the system, Varian strongly recommends documenting the changes to allow for proper customer troubleshooting and maintenance if needed.

Removing or Disabling Accounts

For ARIA Versions 15.1 and later, with integration into the Active Directory environment, it is possible, and recommended, to disable any SQL Server specific accounts and use domain level accounts for all SQL Server related tasks.

Do not remove the SA account.

Varian recommends disabling the SQL Server Service Admin (SA) account.

ARIA Versions earlier than 15.1 require these accounts for Varian to maintain the system properly. See Password Change Policy on page 47 about changing passwords for certain accounts.

Adding DBA Group Accounts to MS SQL

Adding Database Administrator (DBA) group accounts is allowed. However, any changes to the system must be strictly tracked and controlled, because the database is part of a medical device.

Varian is not responsible for any harm, damage to the system, performance degradation, or improper functioning of the system caused by the existence or use of any DBA group accounts.

In the interest of serviceability, Varian strongly recommends adding a "Varian only" audited and controlled account to the DBA group granting Varian personnel access to use it as needed. Varian also recommends that when this account is not needed, that it be disabled; it should not be used for day-to-day tasks.

For security reasons, Varian personnel cannot assist in creation of system level administrative accounts (DBA accounts) on behalf of the customer or their IT. The affected groups must create, track, and maintain these accounts, regardless of elevation levels. Varian does not guarantee that these accounts will carry forward with major or minor updates; Varian reserves the right to disable or delete these accounts in cases of troubleshooting or recovery from intrusive breaches.

Password Change Policy

Only the password of accounts used to maintain and service the system may be changed, to include the Windows Domain Varian account, the serviceadmin account, and the SA account. However, changing the passwords may directly impact Varian's ability to service the system in a timely manner and could impact patient treatments. Varian is not responsible for any impact on the system or patient treatments if changing these account passwords delays servicing the system.

Due to the nature of computer security as well as the elevated status of the SA and / or serviceadmin accounts, these accounts need to be strictly controlled. However, these passwords are also needed for serviceability of the equipment.

If needed, the customer (or their IT representatives) can take ownership of said accounts, with knowledge that the ownership transfer is immediate and final. Thus, on ownership, the customer and their IT representatives take all liability for maintaining, auditing, and protecting said accounts.

Backup Guidelines

Affected Products

These guidelines apply to ARIA environments later than version 11, including ARIA OIS and Treatment Planning Systems data backup and restoration. Also included are backup guidelines for Mobius3D and IDENTIFY.

Scope

Guidelines describe:

- Relevant basic data backup information. Outside the scope of these guidelines is information on selecting or learning about specific hardware, software, technology, or backup solutions.
- Specific backup and recovery information and instructions.
- Mission critical data that must be backed up individually.

Intended audience is hospital and clinical administrators including IT personnel responsible for managing and maintaining OIS and Treatment Planning Systems. Personnel who manage these systems should consider this information when planning for implementing a disaster recovery solution or program.

Backup Responsibility

During product installation, Varian personnel are responsible for configuring required backups and verifying that they function correctly.

On customer acceptance of an installation, the customer’s respective IT personnel is solely responsible to proactively manage and maintain backup operations. It is critically important for long-term data safety and recovery purposes that this responsibility is not neglected. All SQL databases should be backed up and maintained on a regular basis.

⚠ CAUTION: Varian customers are solely responsible for the integrity and/or completeness of backed up data produced from a backup solution that they alone select and implement.

Backup Solutions

Ensuring that a given backup solution routinely performs, maintains, and provides pertinent and viable data backups is critical to the recovery of Varian Medical Systems OIS and/or Treatment Planning Systems when needed.

Arcserve

Arcserve is a purchasable backup solution that Varian offers and considers to meet its data backup requirements. During Varian installation of Arcserve, the Varian installation team will show customers how to perform specific backups during an Arcserve installation. However, note the following:

- Varian does not provide specific Arcserve training.
- Arcserve training is obtained via the contact page at https://www.arcserve.com/about/contact/.
- Arcserve documentation and information can be retrieved from the Arcserve Website and from the Arcserve Support page.

Other Third-Party Backup Solutions

Varian customers may independently implement a third-party backup solution of their choice. If they do, they are solely responsible for ensuring proactive maintenance of the solution selected so that viable backup data is available at any time to recover Varian OIS and/or Treatment Planning Systems.

When selecting a third-party backup solution, be sure to assess long-term archiving, data capacity requirements, performance characteristics, reliability, support availability, and scalability.

Data Backup Overview and Guidelines

Varian recommends that customers do the following:

- Immediately back up data that consist of irreplaceable information such as patient databases, diagnostic images, and so on.
- Incorporate redundancy in the backup strategy such that backups are also stored in a backup system or network or both separate from the primary system and network. For example, if a customer uses the Arcserve Backup solution, at least one data tape cartridge should be stored weekly (or daily if possible) in a premise distance from the Treatment Planning Room or the Data Center.
- Regularly back up any files that change frequently.
- Periodically back up the entire system in case of a catastrophic disaster.
- Include in periodic backups system files that contain specific user information for customized settings and passwords.
- Back up available software for which the original physical media is no longer available.
- The backup of the databases and the backup of the file repositories should be conducted simultaneously. Not doing it simultaneously may cause data integrity issues where the data stored in files is different from the information that the database is expecting.
- Ensure adequate security of backed up files as they contain sensitive information. Encrypt all backups that contain or may contain sensitive data (e.g. database, patient data, entire system backups) on a file level to protect against potential mass data breach due to backup data exfiltration.
- Ensure the availability of the created backups by storing a copy of the backups offline or by using an immutable storage solution (deleting all available backups is a prime objective for threat actors especially in the ransomware domain).

- Provide disk/file system level encryption in all cases when data is either temporarily or permanently stored on dedicated physical disk(s) (e.g. local disks or local NAS) that are not protected against physical access.

Storage solutions and/or devices such as Storage Area Network (SAN), Advanced Technology Attached (ATA), and Direct Attached Storage (DAS) may not be available to accommodate the backup size of the increasing critical data present in a Varian Radiation Oncology environment.

Most backup software provides the option to back up all drive data, just the files that have changed since the last backup, or only individually selected files.

For mission critical data that must be backed up individually, review the sections that follow. Note the following when reviewing as the location of data to back up may vary:

- Give immediate priority to completing backups involving pertinent database, patient, and user data such as those described in ARIA / AURA Database Server on page 50 and ARIA Image Server on page 51 as an example.
- Not all information in the sections that follow may apply to a given Varian customer's Radiation Oncology environment. Evaluate these sections and include those that are relevant to backup procedures.
- Paths described in the "Typical Path" column apply to ARIA v11.x and later unless otherwise noted.
- Target data to back up may exist on the same or different servers. For example, a single server may provide both web and image server roles (combo server). Ensure that all servers in the production environment and the data that resides on each are assessed to complete required backups.
- Target data to back up may exist as multiple instances. For example, there may be multiple instances of a VA_DATA$ folder located across multiple separate disk drives and servers.

If the configuration files of DICOM worklist service got corrupted and/or the DICOM worklist services are not able to function, the service field engineer does the following:

- Create new DICOM worklist services using the DICOM worklist tool.
- Re-install DICOM worklist if needed.

ARIA / AURA Database Server

Stop the database engine (that is, all related database services) before attempting to back up database files. Failure to do so before a backup is started may result in corrupt backup data. For information on the local backup of the database using the Varian provided tool, refer to Backup and Maintenance Tool on page 56.

Table 21 ARIA / AURA Database Server

Data Description	Typical Path
MSSQL	`[Drive]:\MSSQL`
MSSQL logs	`[Drive]:\MSSQL\LOG`
MSSQL backups	`[Drive]:\MSSQL\BACKUP`
variansystem / varianenm logs	`[Drive]:\ (variansystem and varianenm logs)`

ARIA Web (Platform) Server

Table 22 ARIA Web (Platform) Server

Data Description	Typical Path
VMSOS	`[Drive]:\VMSOS`

VA_ROOT$	`[Drive]:\Program Files\Varian`
	`[Drive]:\Program Files (x86)\Varian`

ARIA Image Server

Paths to pertinent data on the ARIA Image server may exist on either Varian Database or Web server.

Table 23 ARIA Image Server

Data Description	Typical Path
VA_DATA$	`[Drive]:\Varian\Data`
VA_Transfer$	`[Drive]:\Varian\Transfer`

Varian	`[Drive]:\Program Files\Varian`
	`D:\varian` or `[Drive]:\varian`

DCF Core Installed on a Server

The table below applies when DCF Core is installed on either a DCF Core Server, FAS Server, Image Server or a Combo Server.

Table 24 DCF Core Installed on a Server

Data Description	Typical Path
DCF$	`[Drive]:\VMSOS\DCF`
DCF$ (On DCF Core Server for ARIA v18x and later)	`[Drive]:\DCF`

Eclipse Clients

Data backup of Eclipse clients is discretionary. The table provided here is a general backup assessment. Evaluate clients that may have backup-worthy data such as local DICOM filters and back up accordingly.

Table 25 Eclipse Clients

Data Description	Typical Path
VMSOS	`[Drive]:\VMSOS`
Varian	`[Drive]:\Program Files\Varian`

Eclipse Standalone System

Table 26 Eclipse Standalone System

Data Description	Typical Path
C Drive	`C:\`
D Drive	`D:\`
E Drive	`E:\`

Citrix Environment

System critical files and folders in a Citrix environment are the same as those described for the Varian ARIA/AURA Database and ARIA Image servers (Table 21 ARIA / AURA Database Server on page 50, Table 23 ARIA Image Server on page 51). The difference is the addition listed in the Citrix Environment table here.

Table 27 Citrix Environment

Data Description	Typical Path
IMA DB	`[Drive]:\Temp`

ARIA Connect

Table 28 ARIA Connect

Data Description	Typical Path
ARIA Connect WS root	`C:\Program Files\Varian\Product-Line\WSF\13.06.0717.0\VMS.AC.WebServices`
ARIA Connect HL7 App root	`[Drive]:\Cloverleaf\cis6.1\integrator`
ARIA Connect Config	`[Drive]:\VMSOS\Config2\Shared\Systems\OSP8\Products\AriaConnect\AriaConnectService.wox`

VelocityGRID Server

Note the following regarding VelocityGRID server backups.

- Velocity data backups must be scheduled to be performed regularly. It is suggested to create periodic file system level snapshots using the Microsoft Volume Shadow Copy Service.

- All data and SQL information must derive from a single point in time when backing up or restoring Velocity data. Data loss or corruption will occur if files or SQL information are backed up or restored piecemeal or from differing points in time.

  Most commercial backup software support creating either file system, memory, or operating system level snapshots to ensure that database backups are consistent. This functionality is available in the Windows Backup software integrated into Microsoft Windows Server.
- To guarantee that a Velocity backup is produced at a single point in time, it is permissible to shut down the Velocity software by stopping the Windows Service before backup occurs.

  For VelocityAI Standalone Workstations, there is no additional service running that can modify the database when the client application is closed.

  For VelocityGRID server software, the Windows Service is generally named “VelocityGRID” or “VelocityGrid” along with a version number.
- Backups may be performed to any industry common device hardware and/or medium.
- Network file systems are acceptable for data backup only if long file names are supported.

Table 29 VelocityGRID Server

Data Description	Typical Path
INI Folders (Velocity 3.2)	`%ProgramData%\Velocity Medical Solutions, LLC`
INI Folders (Velocity 4.0+)	`%ProgramData%\ Varian`
Binaries	* `[Drive]:\Velocity\GRID`
SQL	* `[Drive]:\VelocityData\ServerTables`
Database(s)	* `[Drive]:\VelocityData\Databases`
DB1	* `[Drive]:\Velocity\Databases\VMS_CLINICAL`
DB2	* `[Drive]:\Velocity\Databases\VMS_ARCHIVE`
DICOM Listener	* `[Drive]:\VelocityData\DICOM_INBOX`

Table 30 Velocity Standalone Workstation (Windows)

Data Description	Typical Path
INI files	`[Drive]:\ProgramData\Velocity Medical Solutions, LLC`
Binaries	* `[Drive]:\Velocity\Workstation`
Database(s)	* `[Drive]:\VelocityData\Databases`
DB1	* `[Drive]:\Velocity\Databases\VMS_CLINICAL`
DB2	* `[Drive]:\Velocity\Databases\VMS_ARCHIVE`
DICOM Listener	* `[Drive]:\VelocityData\DICOM_INBOX`

Locations listed in tables Table 29 VelocityGRID Server and Table 30 Velocity Standalone Workstation (Windows) with a * (asterisk) are examples of typical Velocity folder locations. The application locations and data locations may reside under the same parent folder or may exist in separate folders or different volumes. Verify your Velocity folder names and locations, which may be unique. Contact Varian Customer Support if assistance is needed.

Backup Frequency

Following are the suggested backup frequencies for files that change often such as databases, patient files and folders, and system files:

Table 31 Backup Frequencies

Element	Suggested Backup Frequency
Users' data files	Daily on all files or only those that changed.
Entire system	Daily, otherwise perform weekly (recommended), biweekly, or monthly for all program files, data files, and the system registry.
System critical database logs	Hourly.

Note: Varian recommends retiring tapes after a year if they are used for daily backups.

Data Backup Exceptions

Mobius3D and IDENTIFY differ from other products’ backups.

Mobius3D

All backups of the Mobius3D server are handled by configuring an automatic backup to a network file share location of choice.

Table 32 Mobius3D Backup

Backup Location	Save to Network Drive.
Frequency	Automatic and Nightly. (Midnight by default. Contact Varian Customer Support to modify the nightly maintenance time.)
Contents	Configuration Information Database Information (Including PHI) **DICOM data is not included**

Encryption	Backup files are **not** encrypted.
Backup Restoration	Backup restoration **MUST only** be performed by Varian Customer Support. Backup restoration can only be performed when the source backup is from the exact same version of Mobius3D as the target server.

IDENTIFY

Varian customers are responsible for backups related to IDENTIFY Central Server. There are two different scenarios for a customer to create a backup depending on the IDENTIFY Central Server environment.

Physical IDENTIFY Central Server

Table 33 Physical Central Server Backup (IDENTIFY)

Backup Location	IDENTIFY external secure location.
Frequency	Daily or weekly.
Method	IDENTIFY 2.2 Creating and restoring a back-up is only possible by Varian Personnel. IDENTIFY 2.3 **Creating a back-up:** 1. Log in to the clinical OS user. 2. Open the IDENTIFY Backup tool. 3. Select the Backup Export Shared Folder 4. Create a Backup 5. DO NOT “restore from backup” after completion of backup creation. **Restoring a back-up:** Restoring a back-up is only possible by Varian Personnel.
Backup Contents	● Reports ● Settings ● User data ● Database ● Translations
Encryption	IDENTIFY 2.2 uses OpenPGP 1.x. IDENTIFY 2.3 uses OpenPGP 2.1.
Backup restoration	Restoration of the backup can only be performed by the Varian Customer Support.

Virtual IDENTIFY Central Server

Table 34 Virtual Central Server Backup (IDENTIFY)

Backup location	Secure location.
Frequency	Daily.
Method	Create a backup of the entire virtual machine.
Backup contents	Complete virtual environment.
Backup restoration	Restoration of the backup can only be performed by the customer.

Backup and Maintenance Tool

The Varian provided Backup and Maintenance Tool creates an automated series of SQL jobs to handle the backup and maintenance of Varian system critical databases.

This tool applies only to the ARIA SQL Databases mentioned in the following sections and is not intended to send the backed-up data off site; rather it only creates a backup set of the data locally.

The sections that follow provide an overview of what the Backup and Maintenance Tool does.

Note: The scheduled days and times of the backup jobs are customizable during the installation of the Varian Database Backup and Maintenance tool. The listed schedules are the installation defaults and intended only as a general guide.

ARIA 13.X and Earlier

1. A backup is performed on the variansystem and varianenm databases. This is scheduled to run Monday through Friday at 11:00 p.m., every week.
   a. Previous day's backup files are replaced / overwritten.
   b. The integrity of the variansystem database is checked.
   c. The variansystem database is backed up to the MSSQL directory.
   d. The integrity of the varianenm database is checked.
   e. The varianenm database is backed up to the MSSQL directory.
2. Maintenance as well as backups are performed. This is scheduled to run every Thursday at 11:00 p.m.
   a. All steps are run from section 4.1.1.
   b. Statistics are updated on the variansystem database after the integrity has been checked.
3. A transaction log backup is performed. This is scheduled to run every two hours Monday through Friday, between 8:00 a.m. and 6:01 p.m., every week.
   a. Previous transaction log backup files are replaced / overwritten.
   b. The variansystem transaction log is backed up to the MSSQL directory.

   c. The varianenm transaction log is backed up to the MSSQL directory.

4. System Databases are backed up and maintenance is performed. This is scheduled to run Monday through Friday at 11:00 p.m., every week.
   a. Previous days backup files are replaced / overwritten.
   b. Integrity is checked on the master, model, and msdb databases.
   c. Integrity is checked on the varianospdb.
   d. The master database is backed up to the MSSQL directory.
   e. The msdb database is backed up to the MSSQL directory.
   f. The model database is backed up to the MSSQL directory.
   g. The varianospdb database is backed up to the MSSQL directory.
5. History is purged. This is scheduled to run every day at 2:00 a.m.
   a. Verify that automation is enabled.
   b. History is purged in the msdb database.
   c. Phantom system health records are erased.

ARIA 15.X and Later

1. Backup and Maintenance are performed on all the databases on the server. The default schedule is to run Monday through Friday at 11:00 p.m., every week.
   a. Full integrity of all databases is checked.
   b. All databases are backed up to the MSSQL directory.
   c. If the current backup is successful, backup files older than 4 days are deleted.
   d. Indexes are rebuilt where PageCount is 1000 or more and Fragmentation is 20% or higher.
   e. All Index Statistics are updated.
   f. The job will stop 7 hours after it has started.
2. Backup and Maintenance are performed on all the databases on the server. The default schedule is to run Saturday at 11:00 p.m., every week.
   a. Full integrity of all databases is checked.
   b. All databases are backed up to the MSSQL directory.
   c. If the current backup is successful, backup files older than 4 days are deleted.
   d. All indexes are rebuilt.
   e. All Index Statistics are updated.
   f. The job will stop 8 hours after it has started.
3. A transaction log backup is performed. The default schedule is to run every two hours Monday through Friday, between 5:00 a.m. and 8:00 p.m., every week.
   a. The transaction logs are backed up to the MSSQL directory.
4. System databases are backed up and maintenance is performed. The default schedule is to run Monday through Friday at 11:00 p.m., every week.
   a. Previous days backup files are replaced / overwritten.
   b. Integrity is checked on the master, model, and msdb databases.

c. The master database is backed up to the MSSQL directory.

d. The msdb database is backed up to the MSSQL directory.

e. The model database is backed up to the MSSQL directory.

5. If database monitoring is active, its history is purged. The default schedule is to run every day at 2:00 a.m.

   a. Verify that automation is enabled.

   b. History is purged in the msdb database.

   c. Phantom system health records are erased.

   d. Previous transaction log backup files are replaced / overwritten.

   e. The variansystem transaction log is backed up to the MSSQL directory.

   f. The varianenm transaction log is backed up to the MSSQL directory.

6. System databases are backed up and maintenance is performed. The default schedule is to run Monday through Friday at 11:00 p.m., every week.

   a. Previous days backup files are replaced / overwritten.

   b. Integrity is checked on the master, model, and msdb databases.

   c. Integrity is checked on the varianospdb.

   d. The master database is backed up to the MSSQL directory.

   e. The msdb database is backed up to the MSSQL directory.

   f. The model database is backed up to the MSSQL directory.

   g. The varianospdb database is backed up to the MSSQL directory.

7. History is purged. The default schedule is to run every day at 2:00 a.m.

   a. Verify that automation is enabled.

   b. History is purged in the msdb database.

   c. Phantom system health records are erased.

Note: The scheduled days and times of the backup jobs are customizable during the installation of the Varian Database Backup and Maintenance Tool. The listed schedules are the installation defaults and intended only as a general guide.

Note: All SQL databases should be backed up and maintained on a regular basis.

Restoration and Recovery of Data

Setting the correct schedule is crucial to achieve the desired recovery point objective. The customer will need to take many things into consideration including frequency of snapshots, transaction log backups, database backup, VA_DATA backup etc. In the event of a system crash or other disaster, it will be necessary to restore and recover system critical data. For restoration of any system critical data related to Varian applications, contact Varian Customer Support. To ensure the integrity of the data recovery and integration back into a working system, it is required that Varian Customer Support (Varian Technical Help Desk team) facilitates the restoration of data.

Mission Critical Application Protection (MICAP)

Affected Products

The Varian products that use MICAP include TrueBeam, Non-Varian Treatment, RPM, 4DITC (OBI/PVAI), Varisoure, GammaMed, Bravos, Acuity, Halcyon, RGSC, IDENTIFY, Verification Console (Mevion, Sumitomo).

Mission Critical Application Protection (MICAP)

MICAP, also called Clinac Network Interface Device (CNID), is a security framework designed and implemented to assist in securing the Varian Treatment Network (VTN).

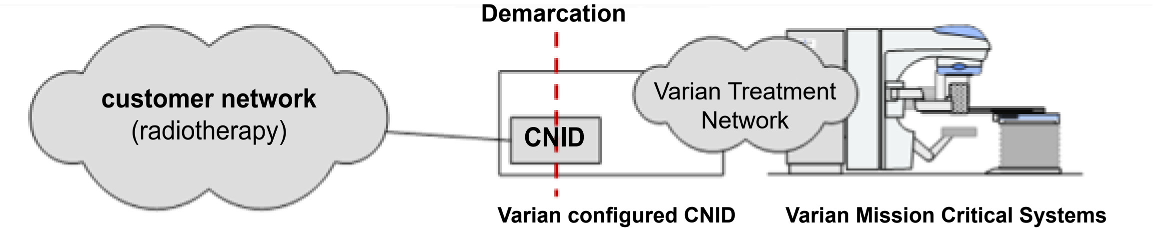


Figure 1 Network Diagram Illustrating Varian Treatment Network (VTN) Connection to a Customer Network (although Similar ProBeam Network Diagram is different).

NOTICE: Varian Mission Critical Applications directly affect both prescription and delivery of treatment protocols to patients. Varian software and workstations are classified as Medical Devices by the FDA. This classification requires that the Mission Critical Applications operate in the same software environment as they were validated.

Varian Treatment Network consists of Mission Critical Applications (MICAP) and workstations. The MICAP solution enhances the security of VTN by segmenting the VTN from the customer network. MICAP is implemented by integrating a MICAP device, currently a firewall, into the network framework of mission critical applications. This offers Varian mission critical applications a layer of perimeter protection enhancing network segmentation to and from customers' existing IT infrastructure.

The MICAP device isolates, controls, and routes traffic between the VTN and the customer network, mitigating both intentional and unintentional manipulation of Treatment Delivery Systems. The MICAP device is an integral part of the Varian mission critical applications and is a required component for qualified device operation.

MICAP has been and will continue to be implemented in a phased approach with the intent to evolve the security posture of Varian mission critical workstations into an abstracted component of medical devices. This includes limiting configuration to only the mission critical applications and controlled user experience settings, that is, hospital name, to ensure use is limited to medical device operation only. These changes are part of a continuing product development lifecycle intended to align with industry best practices.

Classification of Varian Workstations

Workstations running Varian applications can be classified into two groups, mission critical and non-critical.

Mission Critical Workstations

Mission critical devices directly affect prescription or delivery of treatment to a patient. These clinical workstations run Varian applications that must compute results within a defined response time and act in a quasi-real-time mode. Following is a sample list of devices classified as mission critical that may be inside the protected MICAP environment:

- Acuity Workstation
- 4DITC
- OBI / PortalVision Advanced Imaging (PVAI))
- Non-Varian Treatment
- IDENTIFY (In Room Workstation and IDENTIFY Central Server)
- Verification Console Workstation (Mevion, Sumitomo)
- TrueBeam Workstation
- Respiratory Gating System (includes RPM, RGSC)
- Halcyon Workstation
- Brachytherapy (VariSource, GammaMed, Bravos)
- ProBeam Workstation

Non-Critical Workstations

Non-critical workstations are unrestricted workstations that run Varian management applications used to edit or review patient data and images. These workstations are relatively bandwidth-insensitive. Examples of unrestricted applications include all VARiS applications , ARIA applications, Treatment Review (Image Review), RT Chart, and Eclipse SomaVision (SV). These workstations are managed, controlled, and maintained by the customer IT department.

End Point Device Management

Many customer IT departments ensure the integrity of Mission Critical Application devices by deploying, managing, and updating the end point device management software of their choice.

Varian clinical workstations hosting mission critical applications will experience a time delay when running anti-virus software and/or EDR/XDR software in a real-time mode. This time delay can negatively influence communication and device utilization and cause mission critical devices to behave unpredictably.

Varian software is installed on workstations that run the Microsoft Windows Operating System.

In addition to information in the Mission Critical Application section, compliance with the following is required for all mission critical products.

- Varian Anti-Virus Software Policy
- Third-Party Hardware or Software Installation with Varian Products Policy

Clinical devices need to focus all their resources on delivery technique. Anti-virus software and changes in MICAP configuration can consume resources needed by the mission critical application. This policy was developed in response to testing and observing how mission critical application behaviors are altered when subjected to real-time anti-virus scanning in a clinical environment.

On end point systems that have MICAP implemented, the firewall device, the firewall configuration designed by Varian, and the console are an integral part of the overall security framework for treatment delivery systems. These are all parts of the medical device and exist as inputs to the product development threat modeling processes. Neither the firewall, nor the treatment delivery system computers should be bypassed, modified, patched, or tampered with in any way, unless Varian has validated the configuration.

The MICAP strategy effectively balances Varian's stringent requirements for patient safety and risk management of mission critical applications and the needs of clinical infrastructure providers. In summary, MICAP demonstrates improvement in both the security and the stability of mission critical applications.

Additional Benefits of MICAP

MICAP provides the network level connectivity for various treatment delivery systems and is a required component for proper operation of the devices.

MICAP simplifies the network architecture within the hospital environment. Hospital IT administrators need to provide minimal information for the MICAP to function. These include a single hospital network Internet Protocol (IP) address, DNS addresses, domain names, and gateway address. MICAP has only one network cable drop to manage for each treatment delivery system. This results in simpler cabling and installation requirements for the treatment delivery system. Also, MICAP is single secured network point of presence, rather than an application-based package running on each of the clinical workstations within the Varian Treatment Network.

The MICAP device improves network security, reduces network congestion, and simplifies treatment area cabling. MICAP can eliminate interdependencies on Hospital IT services such as Domain Name Service and Dynamic Host Communication Protocol (DHCP).

Each treatment delivery system will have a required MICAP device forming a demarcation between the hospital LAN and the Varian Treatment Network.

MICAP Installations

A goal of Varian is to create a layer-secured network and system environment that will increase the reliability, performance, and security of the existing Varian products.

MICAP is mandatory for all new treatment delivery system installations. Treatment delivery system ancillary products, including RPM and Acuity, include a MICAP device / firewall as part of their approach to providing network connectivity and perimeter security. However, older installations may or may not have implemented the MICAP firewalls. Customers whose ancillary devices do not have a MICAP firewall device, and require additional security, may contact Varian to verify product eligibility for MICAP purchase and installation.

MICAP Device

A Varian configured MICAP device (currently a Juniper firewall) is part of the Varian treatment delivery system, which allows the Varian mission critical systems a connection to the customer network over a single network port. The MICAP device is designed to provide a demarcation point between the Varian Treatment Network (VTN) and the customer network.

The MICAP device permits data to be transferred between the Varian Treatment Network and the customer network and adds a layer of perimeter security. The MICAP device is configured for stateful operation. For each product that has MICAP implemented, Varian uses a standardized configuration which has been designed to support the product's network requirements. A typical configuration implements Network Address Translation (NAT), Port Forwarding, DNS proxy, Host Services protection, Network Time Protocol (NTP) Synchronization, URL allowlisting, access restrictions, system services to block all external services, un-trust screen support for zones, and gateway interfaces for the Varian Treatment Network. These features are subject to change in future releases.

The illustration represents a single linear accelerator. Multiple installations are common for a clinical environment. Each installation requires a separate MICAP. For ProBeam, refer to PB-CTR-00015 (*ProBeam Network Connectivity*) and PB360-CTR-00013 (*ProBeam 360 Network Connectivity*).

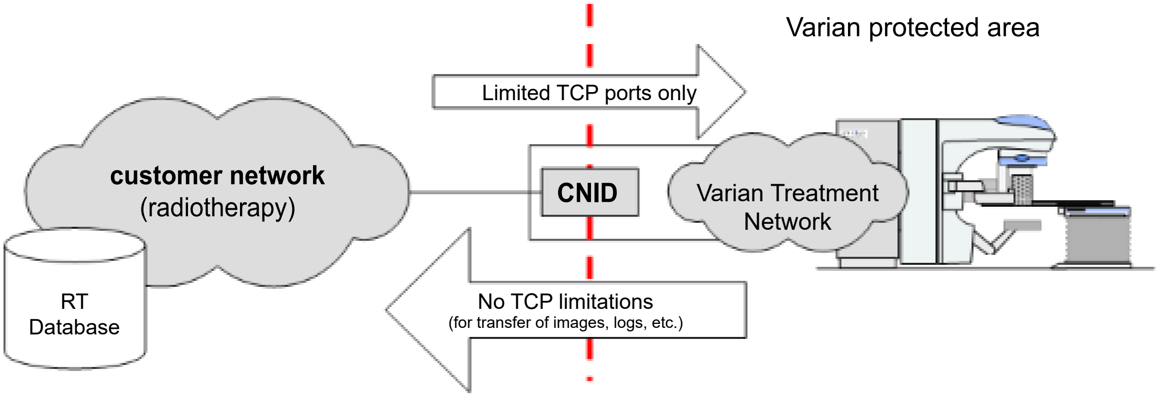


Figure 2 MICAP (CNID) Configuration

Outbound Traffic: Data traffic from the VTN is not limited to certain ports or destinations, except for URL allowlisting (permitting) of Varian recognized websites. Outbound ports are configured with no port timeout.

Inbound Traffic: Inbound ports are permitted to access the Varian Treatment Network, are forwarded to the appropriate product's IP address, and are configured with no port timeout.

Note: The port lists are based on the latest MICAP configuration for the device. The tables will be updated as new configurations are released and product port requirements change.

In the following table, **O** indicates an outbound port, **I** indicates an inbound port.

* Indicates the port may not be used in later product versions

Table 35 List of Transmission Control Protocol (TCP) Ports for All Products Except IDENTIFY and ProBeam

Acuity	Brachytherapy Consoles	C3 (4DITC)	Halcyon	TrueBeam	RGSC	RPM (CT only)	Varian Treatment	Verification Console MEVION	Verification Console SUMITOMO	Feature, Protocol	Ports
O*	O*	O*	O*	O*	O*		O*			Sybase	5000
O	O	O	O	O	O		O	O	O	SQL Server	1433-1435
O	O	O	O	O	O	O	O	O	O	OSP Web Access	55000
O	O	O	O	O	O		O	O	O	OSP Flexnet Licensing	55010
O	O	O	O	O	O	O	O	O	O	OSP Syslog	55020
O*	O*	O*			O*		O*	O*	O*	VMS License Service	57362
O		O	O*	O			O			Elekta Tx Queue	50020
O		O	O*	O			O			Elekta DICOM Out	104
I										Acuity Proxy Host	56780
I										MOS DICOM Daemon	51402

Acuity	Brachytherapy Consoles	C3 (4DITC)	Halcyon	TrueBeam	RGSC	RPM (CT only)	Varian Treatment	Verification Console MEVION	Verification Console SUMITOMO	Feature, Protocol	Ports
I		I	I	I			I	I	I	Treat DICOM Daemon	50500
	I									Brachy Console (DICOM)	50509
			I	I						Image DICOM Daemon	51500
I		I					I	I	I	Image DICOM Daemon	51101
I		I					I			Image DICOM Daemon PVAI	51102
I*		I	I*	I			I			Treatment ADI	56050
I*		I								Multiplicity	30564
					I					RGSC DICOM Daemon	51600
I										Treat DICOM Daemon iX	106
							I	I	I	MVDS	1234
								I		Mevion Inbound	4002

Acuity	Brachytherapy Consoles	C3 (4DITC)	Halcyon	TrueBeam	RGSC	RPM (CT only)	Varian Treatment	Verification Console MEVION	Verification Console SUMITOMO	Feature, Protocol	Ports
								I	I	Mevion/ Sumitomo Outbound 1	3002
								I	I	Mevion/ Sumitomo Outbound 2	3004
									I	Sumitomo Inbound	7002

In the following table, **O** indicates an outbound port, **I** indicates an inbound port.

Table 36 List of TCP Ports for IDENTIFY

IDENTIFY (Server)	IDENTIFY (IRW)	IDENTIFY Windows Planning Tool (WPT)	Feature, Protocol	Ports
O	O		SSH	22
I	O	O	ICS Daemon	8001
I	O		Auto Pat Select Daemon	10001
I	O		Rsyslog Daemon	514
I	O		Audisp Daemon	60
I	O		HL7 Inbound Daemon	10000
I			DICOM Inbound Daemon	11112
O			Samba Daemon	445
O	O		SmartConnect Proxied	17002
O			OIS HL7 MDM	19071 default or Customer Specified
O	O		SmartConnect	80
O	O		SmartConnect	443

Customer Security Posture and the MICAP Device

Varian realizes customers may have a security posture required by their IT or Information Security departments on how they manage cybersecurity risks and protect their enterprise's software and hardware, networks, services, and information.

If a customer chooses to control the traffic exiting MICAP, the customer can implement their own firewall on the customer network facing the MICAP device. Care must be exercised to allow the necessary ports and traffic for the treatment delivery system to operate as designed.

Varian recommends working with Varian Customer Support when configuring and deploying the customer’s firewall.

For a list of necessary ports that must be opened, see the SPM-SS-VVX (VVX = the applicable version of ARIA, for example SPM-SS-15X or SPM-SS-16X) on www.MyVarian.com. SPM-SS-VVX is the ARIA version System Preparation Manual.

MICAP Maintenance and Reliability

To improve and harden security across the product lines for treatment delivery systems, Varian Treatment Delivery Systems Engineering will assess vulnerabilities of the firewall firmware to ensure acceptability for use. Varian evaluates public and announced vulnerabilities per the National Vulnerability Database and will confirm with Juniper Security Advisories (JSA) to determine if the vulnerabilities reported are applicable to Varian treatment delivery systems. Applicability is based on specific model of device and the configuration settings.

Analysis is conducted quarterly and is documented for review. The Chief Information Security Office (CISO) and Product Security organization may drive a non-cadenced assessment based on criticality.

The vulnerability evaluation will drive decisions for firmware modification and changes to the Varian standard configuration. If a change is decided, Treatment Delivery Systems Engineering will determine the testing necessary for firewall hardware, firmware, configuration, as well as the integration with the product line. The firewall hardware, firmware and configuration testing have to be validated before it is released. Any changes to the MICAP device and/or MICAP device configuration must be validated by Varian.

For the MICAP device, mean time between failures (MTBF) is specified at 44 years. For ProBeam, the MICAP device has an MTBF of 27 years. The device is an enterprise device. It has a 1 Gbit/s auto-negotiated interface that connects to the customer network. The MICAP device is managed through an https or sshv2 interface. Varian has trained service personnel to support this device and has a supply chain to replace defective devices within a brief time. However, 24/7 maintenance cannot be done for the MICAP device. The MICAP device is specially configured by Varian, it is part of the Treatment Delivery Network.

MICAP Management Services

MICAP management services can be performed locally or remotely via MICAP Sphere.

MICAP Sphere

MICAP Sphere is a remote maintenance and support service for the MICAP device. It enables customers to quickly receive the most recent validated MICAP device configuration or firmware after it has been validated. It is an off-premise web portal managed and used by Varian to perform firmware updates, configuration management, and related service interventions. Access to the portal requires two-factor authentication and is limited to a small administration team. The customer device has to be onboarded to MICAP Sphere. Varian communicates when a new configuration and/or firmware has been validated and works with the customer to schedule a time period when an update or upgrade is to be performed.

When a MICAP firewall is onboarded to MICAP Sphere, it establishes an outgoing SSHv2 connection over port 4087 with the platform. It also streams syslog to the platform over various ports. MICAP firewalls require DNS resolution and communication with the following endpoints:

- skyent-ncd01.juniper.net
- skyent-ncd02.juniper.net
- logs.juniperskyenterprise.net

Securing Varian Products from Ransomware

Introduction

The purpose of this section is to be a helpful guide including general security recommendations on ransomware, including malware, infection, unauthorized access, and denial of service attacks, which may occur in the customer's controlled network and which may impact customer-purchased Varian products. The recommendations are for informational purposes only and should be used to secure infrastructure running customer purchased Varian products. The document includes recommendations on preparing, preventing, and responding to ransomware attacks.

For the purpose of this section, customer-purchased Varian products are grouped into three infrastructure categories:

- Treatment Delivery System
- Customer-hosted Software Solution
- Varian-managed Services and Software as a Service (SaaS) Offerings

Treatment Delivery Systems

Treatment Delivery Systems include linear accelerators, brachytherapy afterloaders, and other medical devices assisting in the treatment preparation and delivery behind the MICAP firewall or a Varian-validated firewall. Product examples in this category include: C-Series, OBI, Acuity, 4DITC, Calypso, RGSC, RPM, Halcyon, Ethos radiotherapy system, Ethos treatment planning, Ethos treatment management, IDENTIFY, TrueBeam, Edge, VitalBeam, VCD, VariSource iX with MICAP, GammaMed iX with MICAP, Bravos, ProBeam 360 proton therapy system, ProBeam, VTx.

Customer-Hosted Software Solutions

Customer-hosted Software Solutions include Varian software applications and services running on an IT infrastructure managed by the customer. Examples of these include DoseLab linac QA, Mobius3D, BrachyVision, VariSeed, Vitesse, RapidSphere, ARIA CORE Mobile (previously called Varian Mobile), RPM Data Converter, IDENTIFY Central Server, VariSource iX without MICAP, GammaMed iX without MICAP, and Varian Exchange.

Varian-Managed Services and Software as a Service Offerings

Varian-managed Services and Software as a Service Offerings include Varian Software and Service offerings running on infrastructure managed by Varian. SaaS offerings include Noona, Qumulate (Service Support Only), ePeerReview (Service Support Only), ARIA STM, ARIA CORE Mobile and Insightive Gen2. Varian-managed Services include hosting infrastructure and operational support for Varian software solutions. There are two types of Varian-managed Services:

- Varian Cloud Managed Services, where the infrastructure is not at a customer-provided location. These include FullScale Private Cloud and FullScale Infinity Cloud.
- FullScale On-Premise Solution, where the infrastructure is placed at a customer-provided location.

Examples of Varian Software that are available for either the customer-hosted solution or Varian-managed Services include: Ethos Treatment Planning (Varian Managed Services), Eclipse treatment planning system, ARIA OIS for RO, ARIA OIS for MO, ARIA RTM Client, ARIA Connect, Velocity, and InSightive.

Customer Responsibility

The customer and Varian are each responsible for their own information security programs. These programs must consider the evolving external landscape as new security threats and vulnerabilities are introduced.

Securing the customer's network, data (including data when decommissioning equipment), infrastructure, and connected device is the responsibility of the customer. When decommissioning equipment, it is the customer's responsibility to ensure the PHI information on their equipment has been secured or deleted before the equipment is removed from the customer site and/or handed over to a recycling company.

There are several resources that can be used to better understand and assess these risks and vulnerabilities, including:

- Health Information Sharing and Analysis Center: https://h-isac.org/
- US Cybersecurity & Infrastructure Security Agency: https://us-cert.cisa.gov/
- CISA Ransomware Page: https://www.cisa.gov/stopransomware
- NIST Guide for Conducting Risk Assessments: https://www.nist.gov/publications/guide-conducting-risk-assessments

Prepare, Prevent, Respond to the Unexpected

Prepare

Recommendations on preparing for a ransomware attack include:

1. Develop and implement security awareness training, policies, and processes:
    - Implement a cybersecurity and user awareness training program that includes guidance on how to identify and report suspicious activity.
    - Develop and maintain policy on suspicious e-mails for end users. Ensure suspicious e-mails are reported.
    - Implement spam filters at the e-mail gateways. Specialized spam filters can reduce the number of phishing e-mails that reach an address inbox.
    - Have a ransomware response checklist.
    - Inform employees of a threat and increased need to stay highly diligent during this time.
2. Back up data:
    - Ensure that you have regular robust and well protected backup (see Backup Guidelines on page 48).
    - Have a business continuity and disaster recovery policy and procedure for a response plan when a disaster occurs. Ensure that the business continuity and disaster recovery policy is up-to-date and readily available. Review the policy and test procedure once a year to ensure it achieves its recovery objectives.

Varian Role in Preparing for a Ransomware Attack

For the treatment delivery system (TDS), Varian is responsible for system, administration, and maintenance data backup if the customer has Elite or Essential service agreement on the treatment delivery system. For other service agreement types, at an additional cost, Varian can perform system, administration, and maintenance data backup services on the treatment delivery system.

For Varian-managed Services and SaaS offerings, Varian is responsible for data backup. Data is backed up a minimum of once a day. For Varian-managed Service, the recovery point objective (RPO) is 8 hours. The RPO is the maximum tolerable period in which data might be lost from an IT service due to a disaster. For SaaS offerings, data will be restored to the most current point where the data is not corrupted.

Prevent

Varian recommends the following actions to prevent a ransomware attack:

1. Network security:
   - Block known sites that provide known functionality to malware.
   - Monitor and block DNS queries for unexpected/malicious requests.
   - Monitor network traffic and set up alerting for unexpected/large/long data transfers (possibly indicating data exfiltration).
2. Network segmentation:
   - Install an additional firewall to inspect traffic from the treatment delivery environment.
   - Place servers in a separate network segment from the client workstations and limit both incoming and outgoing network connections to them.
   - Limit administrative access to servers on a network level to designated sources (e.g. dedicated management servers).
3. System hardening:
   - Disable/limit access to remote desktop solutions to limit lateral movements by threat actors.
   - Use application allowlisting software to allow only authorized executables, thus blocking execution of a malware or ransomware.
   - Disable or constrain scripting environments and macros.
   - Disable autorun for mounted media.
4. Vulnerability scanning:
   - Perform regularly scheduled scans during *non-treatment hours* to identify systems that are missing security patches and updates. Missing security patches or updates lead to exposed service and software vulnerabilities.
   - Refer to Third-Party Hardware or Software Installation with Varian Products Policy on page 31.
5. Patching:
   - Develop a cadence for applying patches during non-treatment hours.
   - Create a plan for testing and deploying security updates to systems and applications where applicable.

6. Anti-virus software:
   - Refer to Varian Anti-Virus Software Policy on page 17.

Varian Role in Preventing a Ransomware Attack

On the treatment delivery system, Varian does not permit the use of anti-virus/anti-malware or anti-spyware software or vulnerability scanning. This is because scans, interruptions, or delays from this software may cause service interruptions and/or malfunctions on the affected device, thus impacting the device and yielding unexpected results. Varian uses other solutions to guard against malicious executable files or malware such as the MICAP firewall, allowlisting, advanced media removal control (restricts the use of USB drives), hardening, and BIOS tampering protection. These features are included on validated Varian product releases.

Varian will continue to include security updates and features to product releases as needed. Varian reviews the need for security updates and determines if the update should be included on the next product release. Examples of security features that may be included in a release include updated operating systems, security patches, system hardening, application allowlisting, and updates to MICAP firewall.

For Treatment Delivery System, customer-hosted Software Solution, Varian-managed Services, it is the customer's responsibility to ensure that they are upgrading their devices and applications to the latest Varian-validated product release that includes security updates. The customer should request the update and pay for it if applicable. Varian will perform the upgrade work as needed. It is recommended for customers to have a service agreement with a service entitlement that provides these upgrades. For SaaS offerings, Varian will automatically and periodically push updates.

For Varian-managed Services and SaaS offerings, firewalls are used within the infrastructure architecture to prevent unwanted access. Real-time anti-virus scans, on-demand anti-virus scans, and vulnerability scans are done when applicable. In addition, regular patch updates are applied to infrastructures, operating systems and applications where additional Varian validation is not needed.

For customer-hosted Software Solution, the customer is responsible for preventing ransomware, malicious malware, spyware, trojan horse, or malicious executable files.

Respond

Recommendations on responding to a ransomware attack include:

1. Incident response:

   Detect, analyze and contain the incident are some steps to take during incident response. Evidence collection, evidence preservation and root cause analysis are some detect and analyze security recovery recommendations. Containment is critical to minimize damage and prevent ongoing risks to critical assets and data. For all countries, consider reporting the incident to your local law enforcement agency.

   There are several resources that can be used to better understand incident response procedures, including:

   - The SANS Institute, https://www.sans.org/reading-room/whitepapers/incident/paper/33901

- National Institute of Standards and Technology (NIST), https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

2. Recover and restore service:

   A security recovery is designed to stop, learn, and then correct a cyberattack event after an occurrence. The recovery response to a cyberattack should be quick and a lesson learned, or retrospective should be done after a correction is made. Evidence collection, evidence preservation and root cause analysis are some security recovery recommendations. For all countries, consider reporting the incident to your local law enforcement agency.

Varian Role in Recovering from a Ransomware Attack

For Varian-managed Services and SaaS offerings, Varian is responsible for the recovery of the hosted infrastructure. The target duration of time to restore service (recovery time objective (RTO)) is 14 days for Varian-managed Services. The customer is responsible for ensuring connectivity between the managed service infrastructure and that their network is enabled and working. The customer is also responsible for validating the integrity of the recovered system.

Security recovery is the responsibility of the customer on the Treatment Delivery System and customer-hosted Software Solution. After an incident occurs, Varian, at additional cost, will provide help as needed.

Vulnerability Management

Varian releases cybersecurity advisory on varian.com and on www.MyVarian.com. The customer should review these sites for updated cybersecurity information.

Varian Digital Certificate Use Policy

Affected Products

The Varian Digital Certificate Use Policy applies to all Varian products.

Varian Digital Certificate Use Policy

This Policy addresses all installations of digital certificates on/in any product designed and marketed by Varian, including hardware, software, or service components. This Policy does not relate to third-party products that may be sold by Varian in conjunction with a Varian system, for example, computer work stations, servers, monitors, etc. Varian verifies, validates, and documents different digital certificate formats that can be properly used with its products.

Note: Only digital certificates generated as part of the Varian documented installation or upgrade process may be used. A digital certificate that is not generated as part of Varian installation process is regarded as a “custom digital certificate.” Custom digital certificates are not verified and validated with Varian products and/or services and are not supported by Varian.

Digital Certificate Use Rules

By using any Varian products, customers agree that they will only use a digital certificate that is verified, validated, and deployed as part of Varian installation or upgrade process and will not use any custom digital certificate in its place.

Use of Custom Digital Certificates

Use of a custom digital certificate with a Varian product is not allowed and may affect the operability and interoperability of the product, software, or service provided. Use of a custom digital certificate will adulterate the Varian product. Adulteration of the Varian product constitutes a violation of the applicable medical device statutes and regulations. Varian product may not legally be used with a custom digital certificate.

Varian shall not be liable for any failure of Varian product to perform according to its specifications, nor for any cybersecurity incident or security breach that arises in conjunction with the use of a custom digital certificate. The use of a custom digital certificate voids any warranty, extended warranty, or service support obligation of Varian.

If a customer chooses to use a custom digital certificate, the customer is not allowed to ask Varian personnel to assist, in any way, with the installation of a custom digital certificate.

Varian disclaims all responsibility or liability arising out of or related to the custom digital certificate, including, but not limited to, the following:

- Configuration, installation, or support of this custom digital certificate when used with Varian products and/or services.
- The impact of any scripts, reports, or procedures that are developed and distributed about this custom digital certificate.

- The security or use of any custom digital certificate with Varian products and/or services.
- Costs, licenses, and administrative functions related to the use of this custom digital certificate.

If a customer uses, directly or indirectly, a custom digital certificate on/in a Varian product, software, or service, the customer agrees to indemnify and hold Varian harmless from any and all damages, liabilities, and costs (including attorneys' fees, litigation expenses, and court costs) that Varian may incur in response to any third-party claim that involves a product, software, or service in which/on the customer used a custom digital certificate.

SmartConnect Access Control Manager

Introduction

The SmartConnect Access Control Manager is a feature in SmartConnect that allows the customer to control, manage, and audit remote sessions on the devices Varian can access. The component or inventory of device used in SmartConnect Access Control Manager is Thingworx Policy Server. The Policy Server is a server-based application installed on the customer network that the customer should manage and maintain. For customers having a SmartConnect Access Control Manager, Varian recommends that the customer create and configure a separate and noncritical physical or virtual server. This server must have appropriate administrative controls that enable the customer to manage and control the remote connection criteria through SmartConnect.

Varian will lead installation and configuration efforts, which include defining connection security criteria. Varian will also provide any additional pertinent instructions. You can request SmartConnect Access Control Manager from your local District Service Manager.

Network Access Setup

The customer can set up one SmartConnect Access Control Manager to control access on one or multiple networks. The most suitable setup depends on the customer IT organization structure. For example, an organization having one IT team responsible for multiple networks may want to use one SmartConnect Access Control Manager to control many networks. Likewise, an organization having different IT teams responsible for different networks may want to use one SmartConnect Access Control Manager for each network. It is important that the chosen setup aligns to the security policy of your organization. Below are different examples of network access setups for SmartConnect Access Control Manager.

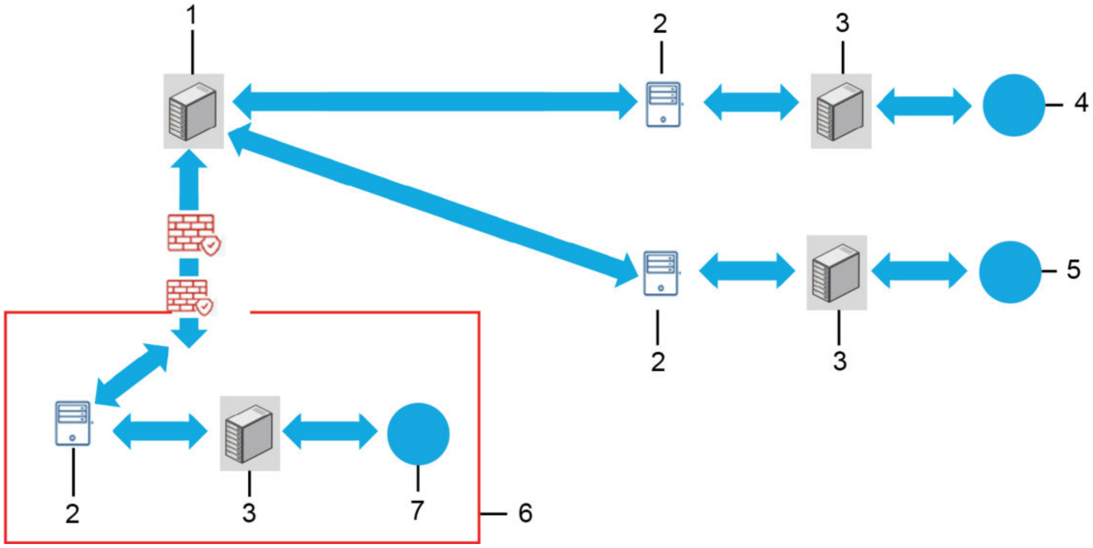


Figure 3 Setup 1 - One SmartConnect Access Control Manager Controlling One Network

1. SmartConnect Access Control Manager with connection to customer AD
2. SmartConnect Gateway
3. SmartConnect Agent
4. Info System
5. Aria
6. Behind MICAP
7. TrueBeam

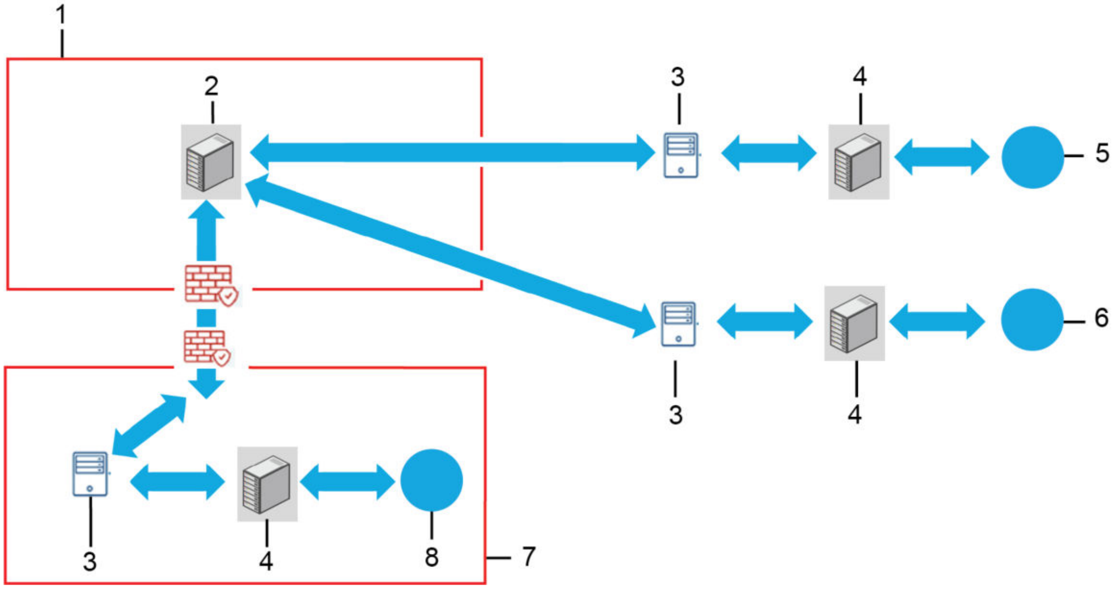


Figure 4 Setup 2 - One SmartConnect Access Control Manager in DMZ Controlling One Network

1. DMZ
2. SmartConnect Access Control Manager with connection to customer AD
3. SmartConnect Gateway
4. SmartConnect Agent
5. Info System
6. Aria
7. Behind MICAP
8. TrueBeam

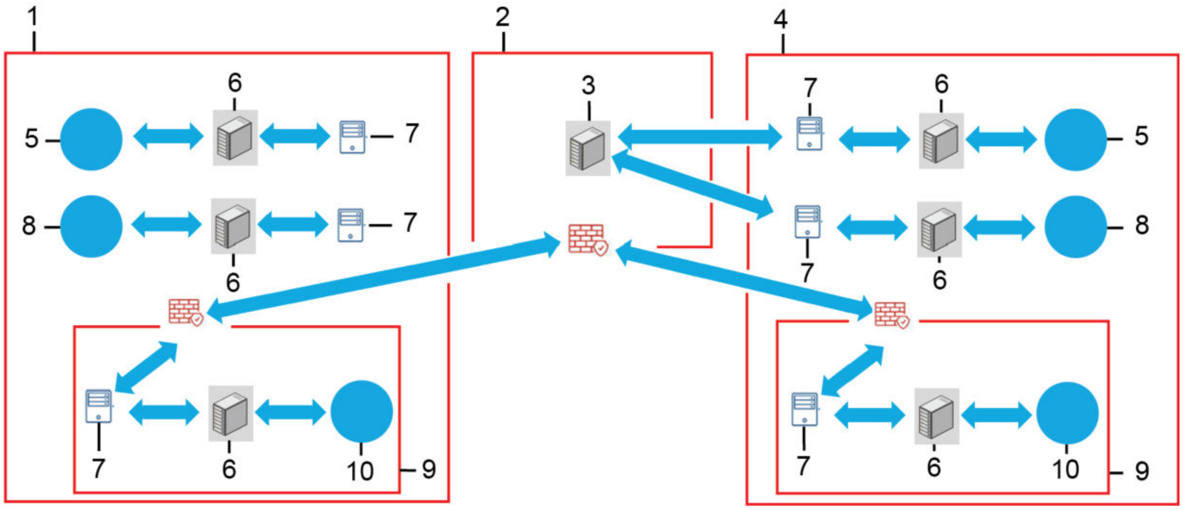


Figure 5 Setup 3 - One SmartConnect Access Control Manager Controlling Multiple Networks

1. Network 1
2. DMZ
3. SmartConnect Access Control Manager with connection to customer AD
4. Network 2
5. Info System
6. SmartConnect Agent
7. SmartConnect Gateway
8. Aria
9. Behind MICAP
10. TrueBeam

Users, Profiles, and Roles

Varian recommends setting up the SmartConnect Access Control Manager so that the customer can use their Active Directory (AD).

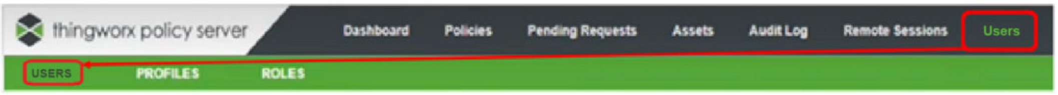
Note: After you set up all users, apply security profiles and roles to each user.

Confirm Users

Note: The **Users** page always includes a Policy Server installation account (for example, “VarianInstaller” or “Installer”). Only use this installation account to install the policy server software. Moreover, this installation account is not a generic account and cannot be used for asset access requests. Asset access requests from Varian personnel will be identified in audit logs by their respective Varian user IDs.

If you use AD, follow these steps:

1. Open the **thingworx policy server** dashboard.
2. Click **Users**.
3. Click the **USERS** tab.



4. Verify that you can see here all the users that have been added to the AD groups.

Create a Security Profile

Common security profiles include the following:

Admin Profile The user has all “Add/Edit” privileges, can view logs, and can end remote sessions.

Remote Asset Access Request Approver The user can approve pending requests for remote access and can end remote sessions.

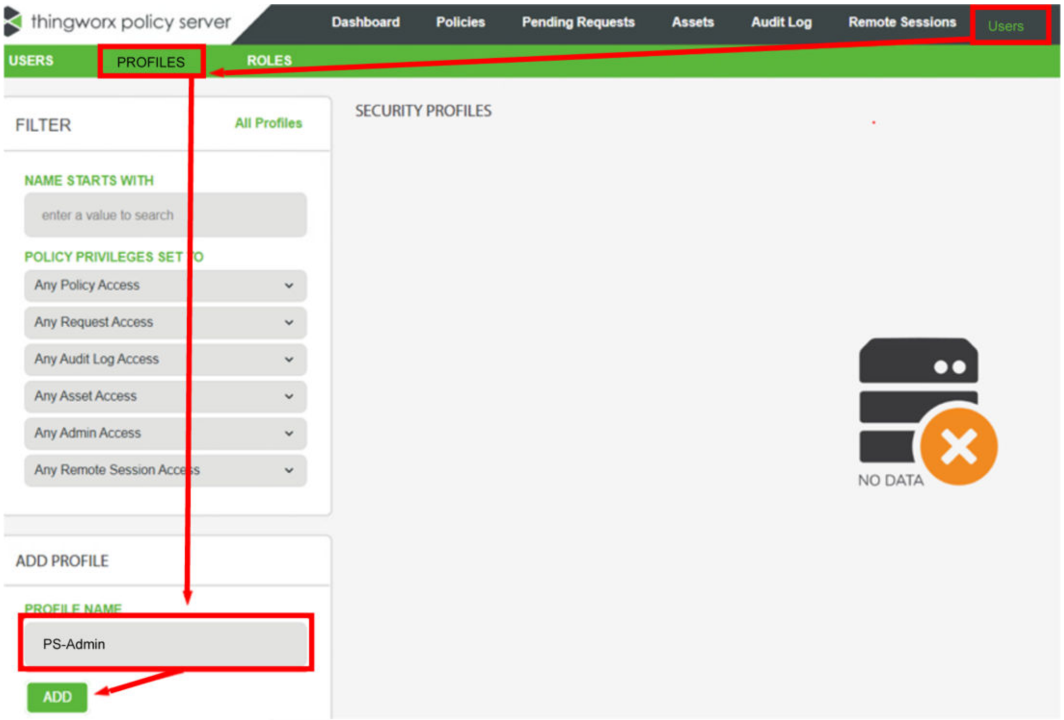
View Only The user has all “view only” privileges.

Log Profile The user can access audit logs only.

Asset Manager The user can add and edit assets.

From the **thingworx policy server** dashboard, follow these steps to create a security profile:

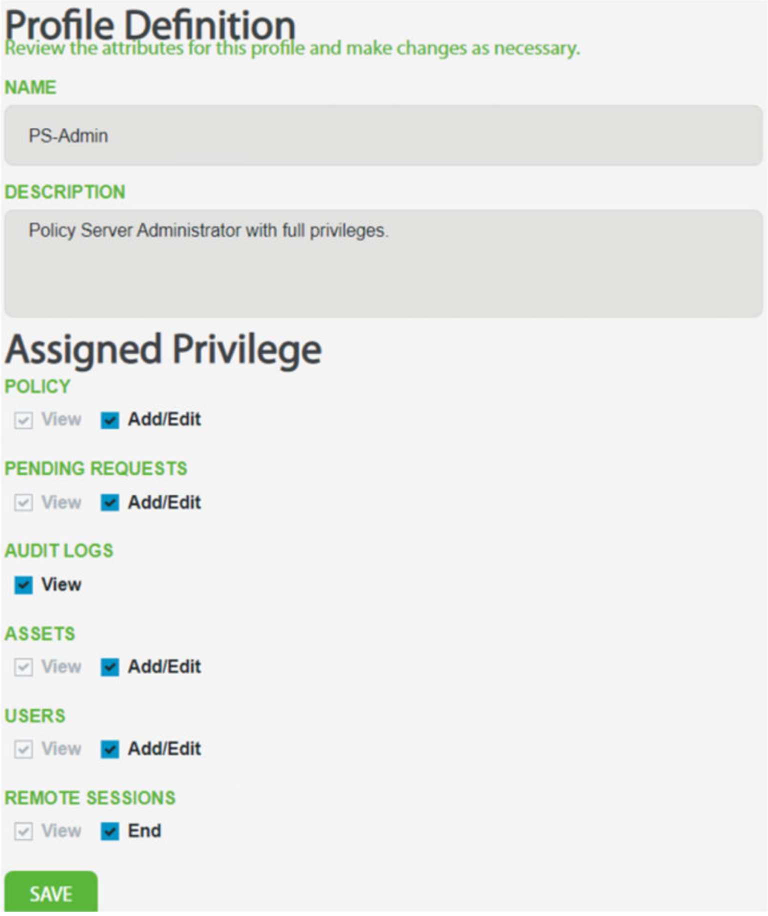
1. Click **Users**.
2. Click the **PROFILES** tab.
3. Enter a profile name.
4. Click **ADD**.



PROFILE NAME
PS-Admin

5. Enter a description for the profile.
6. Assign privileges.

7. Click **SAVE**.



Profile Definition

Review the attributes for this profile and make changes as necessary.

NAME

PS-Admin

DESCRIPTION

Policy Server Administrator with full privileges.

Assigned Privilege

POLICY

☑ View ☑ Add/Edit

PENDING REQUESTS

☑ View ☑ Add/Edit

AUDIT LOGS

☑ View

ASSETS

☑ View ☑ Add/Edit

USERS

☑ View ☑ Add/Edit

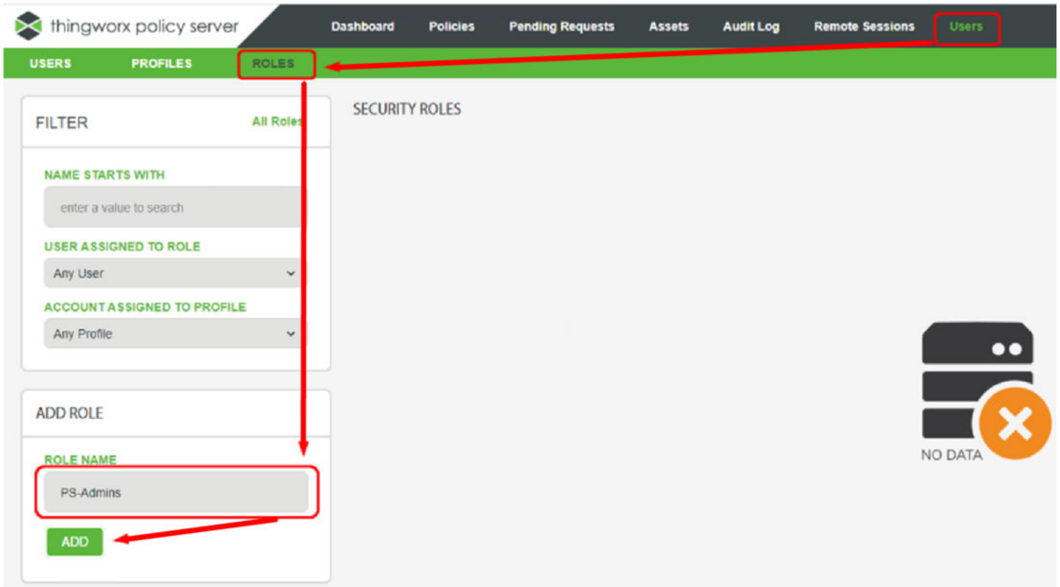
REMOTE SESSIONS

☑ View ☑ End

Create a Role

1. Click **Users**.
2. Click the **ROLES** tab.
3. Enter a role name.

4. Click **ADD**.



FILTER All Roles

NAME STARTS WITH: enter a value to search

USER ASSIGNED TO ROLE: Any User

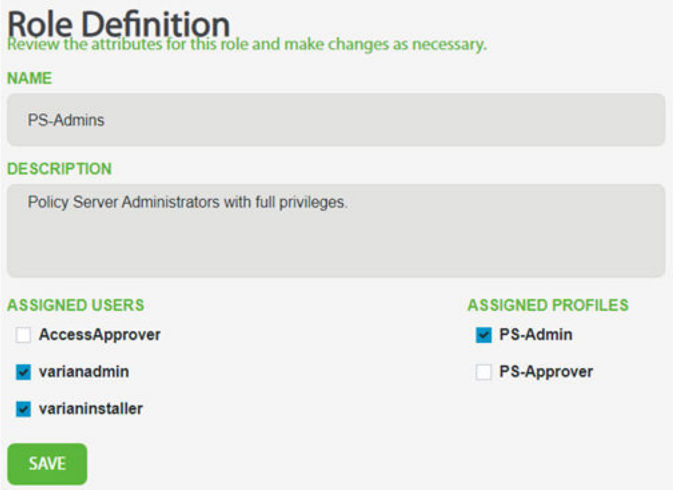
ACCOUNT ASSIGNED TO PROFILE: Any Profile

ADD ROLE

ROLE NAME: PS-Admins

ADD

5. Enter a description for the role.
6. Assign users and profiles.
7. Click **SAVE**.



Role Definition

Review the attributes for this role and make changes as necessary.

NAME: PS-Admins

DESCRIPTION: Policy Server Administrators with full privileges.

ASSIGNED USERS
- □ AccessApprover
- ☑ varianadmin
- ☑ varianinstaller

ASSIGNED PROFILES
- ☑ PS-Admin
- □ PS-Approver

SAVE

Policies, Permission, Access Rights, and Filters

A *policy* consists of a set of actions and the permissions for performing them.

A *permission* defines how an action is managed.

An *access right* determines who can remotely access SmartConnect Access Control Manager. After a permission is created, it can be assigned with access rights.

There are three access rights:

Always Allow Individuals and systems can always access a network remotely without asking for approval.

Ask For Approval Individuals and systems must ask for approval before accessing a network remotely.

Never Allow Individuals and systems cannot access a network remotely.

A *filter* is a set of restrictions for a permission. You can create different filters according to the use cases. For example, you can use a **passthrough filter** to create exceptions for trusted users and systems. This way they can always access the system remotely without asking for approval even if the access right is set to **Never Allow** or **Ask for Approval**. You can also use a filter to create a time window. For example, you can create a “Maintenance Window” to enable service technicians to perform work remotely only in the set time frame.

To benefit from all Varian remote services and support entitlements (remote software updates and upgrades, remote diagnosis and repair, remote assistance, remote training, remote proactive and predictive monitoring) while maintaining the customer control, Varian recommends the following access permission settings. For each **ACTION/GROUP NAME** item listed in the **Policies** page of the **thingworx policy server** dashboard, apply the permissions as per the following order.

1. Apply the **Never Allow** permission (✓👍✕) to all **ACTION/GROUP NAME** items.
2. Apply the **Always Allow** permission (✓👍✕) to the following **ACTION/GROUP NAME** items:
   - Alarms
   - Events
   - Execute
   - File Download
   - File Upload
   - Gateway Provisioning
   - Modify Ping Update Rate
   - Package
   - Restart Agent
   - Set Time
   - Stop Remote Application
   - Start Remote Application
3. Apply the **Ask for Approval** permission (✓👍✕) to the following **ACTION/GROUP NAME** items:
   - Start Remote Terminal

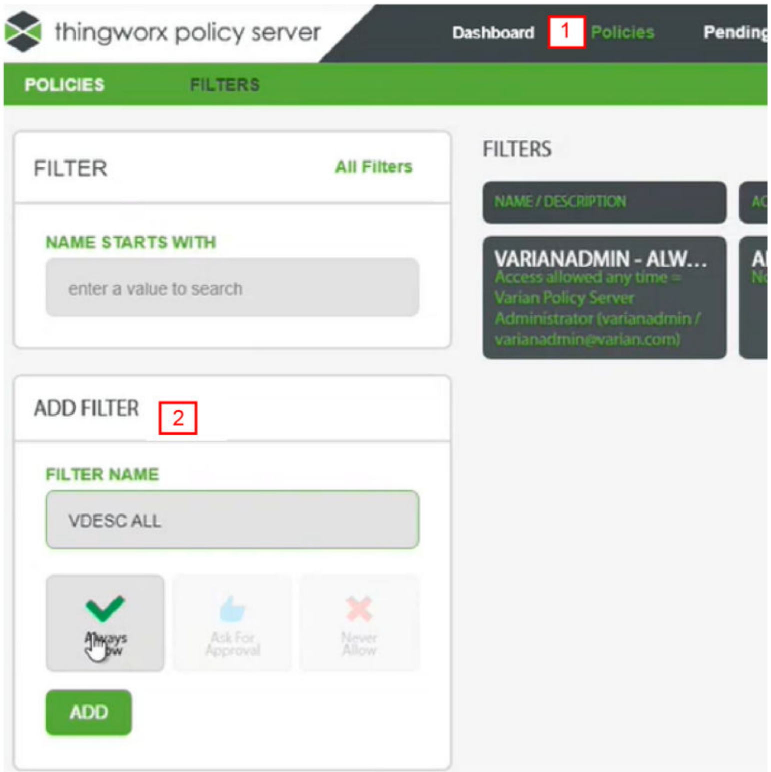
Note: If any **ACTION/GROUP NAME** policy is set to **Ask for Approval** (for example, Start Remote Terminal is set to **Ask for Approval**), ensure to create a passthrough filter for trusted users. For more information, refer to Create Passthrough Filter on page 82. Moreover, be sure to have an approval team available to approve **Ask for Approval** requests. If an approval team is not available, set the **ACTION/GROUP NAME** policy to **Always Allow** (for example, set Start Remote Terminal to **Always Allow**, if an approval team is not available and a passthrough filter was not created).

This configuration is applicable to both parent asset group (global asset group) and child asset group (hierarchy asset group). For more information, refer to Add Assets, Group Assets and Create Notification to Approve Access Request on page 88.

Create Passthrough Filter

You can use a passthrough filter to create exceptions for trusted users and systems such that they can always access the system remotely without asking for approval.

1. Click **Policies**.
2. Enter a filter name, for example, `VDESC ALL`.
3. Select the **Always Allow** access right.
4. Click **ADD**.



VARIANADMIN - ALW...
Access allowed any time = Varian Policy Server Administrator (varianadmin / varianadmin@varian.com)

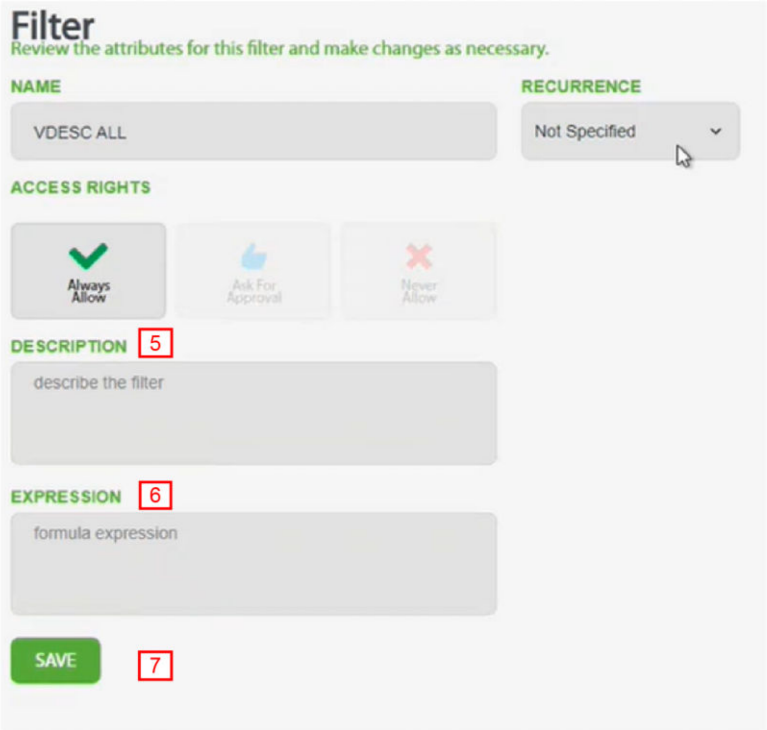
FILTER NAME: VDESC ALL

5. Enter a description for the filter, for example, `Access allowed any time = Varian Field Service Rep`.

6. Type the user ID in the **EXPRESSION** text box. Use the following format: Varian domain/ Windows login user name plus “@varian.com”, for example, `userid=varianadmin@varian.com`.

   Note: In the **EXPRESSION** text box, enter the user ID of the user that is granted the **Always Allow** access.

7. Click **SAVE**.



Filter

Review the attributes for this filter and make changes as necessary.

NAME: VDESC ALL

RECURRENCE: Not Specified

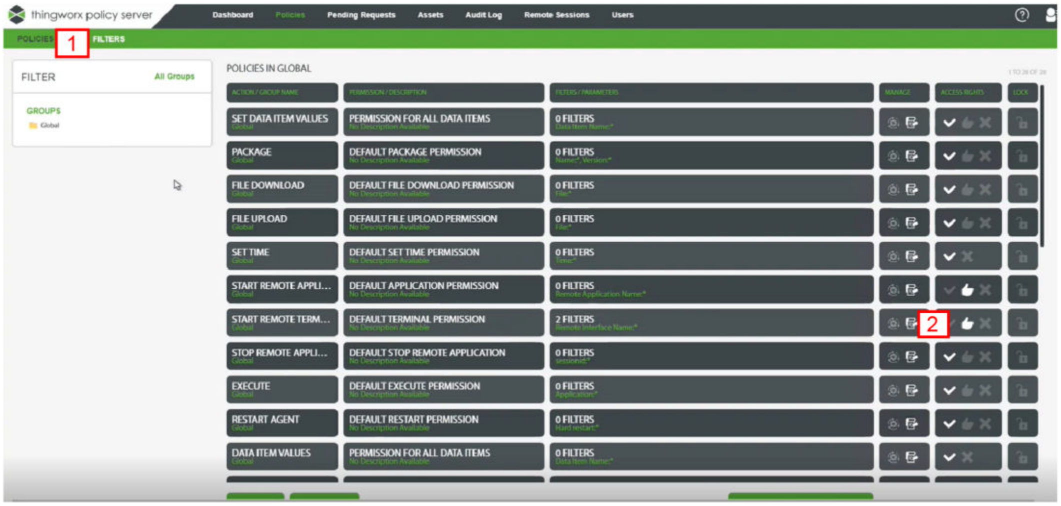
ACCESS RIGHTS

DESCRIPTION: describe the filter

EXPRESSION: formula expression

Apply Passthrough Filter to a Policy

1. Click the **POLICIES** tab.
2. Click on the manage symbol in **START REMOTE TERMINAL**.

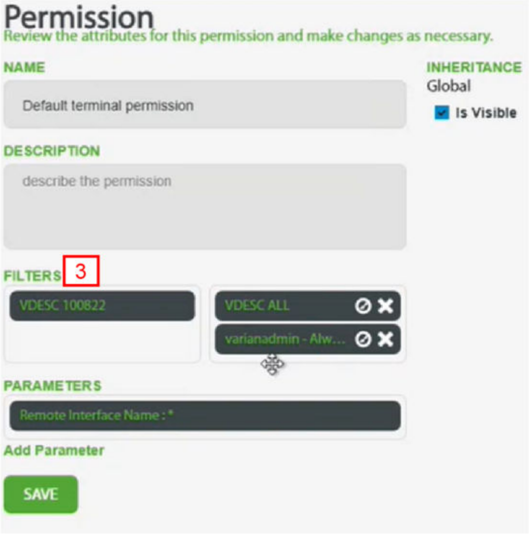


POLICIES IN GLOBAL

1 TO 28 OF 28

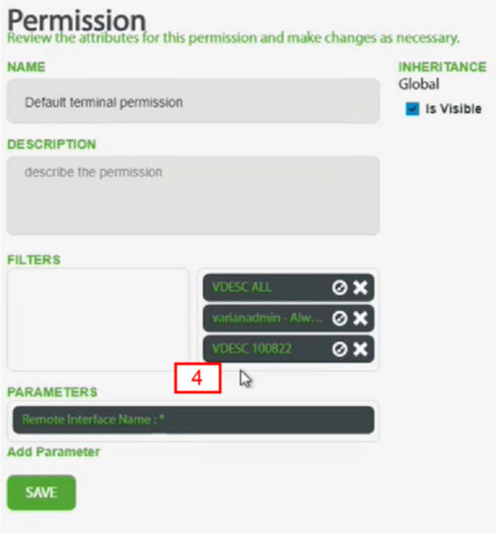
ACTION / GROUP NAME	PERMISSION / DESCRIPTION	FILTERS / PARAMETERS
SET DATA ITEM VALUES Global	PERMISSION FOR ALL DATA ITEMS No Description Available	0 FILTERS Data Item Name:*
PACKAGE Global	DEFAULT PACKAGE PERMISSION No Description Available	0 FILTERS Name:*, Version:*
FILE DOWNLOAD Global	DEFAULT FILE DOWNLOAD PERMISSION No Description Available	0 FILTERS File:*
FILE UPLOAD Global	DEFAULT FILE UPLOAD PERMISSION No Description Available	0 FILTERS File:*
SET TIME Global	DEFAULT SET TIME PERMISSION No Description Available	0 FILTERS Time:*
START REMOTE APPLI... Global	DEFAULT APPLICATION PERMISSION No Description Available	0 FILTERS Remote Application Name:*
START REMOTE TERM... Global	DEFAULT TERMINAL PERMISSION No Description Available	2 FILTERS Remote Interface Name:*
STOP REMOTE APPLI... Global	DEFAULT STOP REMOTE APPLICATION No Description Available	0 FILTERS sessionid:*
EXECUTE Global	DEFAULT EXECUTE PERMISSION No Description Available	0 FILTERS Application:*
RESTART AGENT Global	DEFAULT RESTART PERMISSION No Description Available	0 FILTERS Hard restart:*
DATA ITEM VALUES Global	PERMISSION FOR ALL DATA ITEMS No Description Available	0 FILTERS Data Item Name:*

3. Select the desired passthrough filter (for example, `VDESC ALL`) among the list of filters you will have in the first drop box of the **FILTERS** section.
4. Drop the selected filter in the second drop box on the right.



Permission
Review the attributes for this permission and make changes as necessary.

NAME: Default terminal permission
INHERITANCE: Global
☑ Is Visible
DESCRIPTION: describe the permission
FILTERS



Permission
Review the attributes for this permission and make changes as necessary.

NAME: Default terminal permission
INHERITANCE: Global
☑ Is Visible
DESCRIPTION: describe the permission
FILTERS

5. Click **SAVE**.

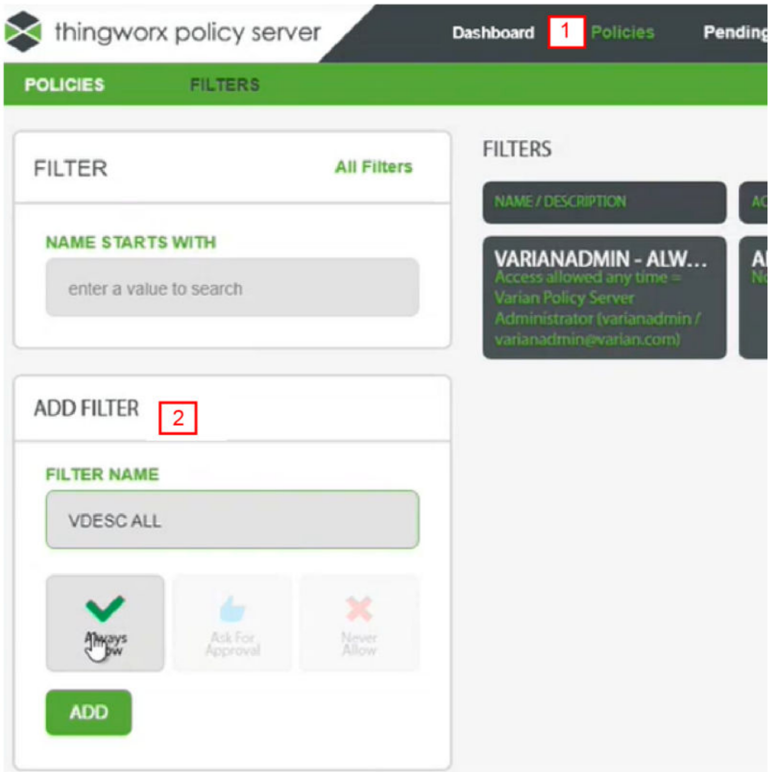
Create a Maintenance Window for Remote Service

Maintenance windows are useful for scheduled maintenance.

Create a maintenance window using a filter.

1. Click **Policies**.
2. Enter a filter name, for example, `VDESC ALL`.
3. Select the **Always Allow** access right.

4. Click **ADD**.



FILTER NAME

VDESC ALL

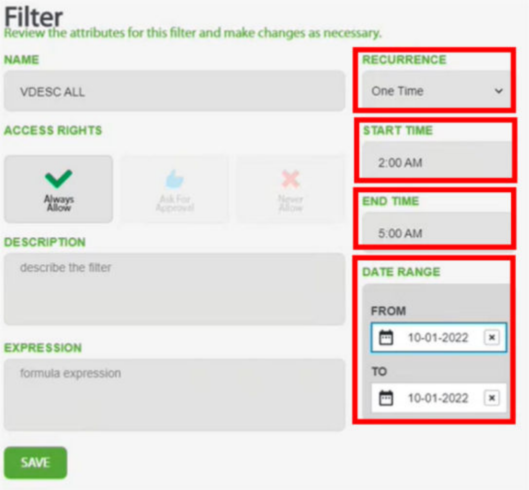
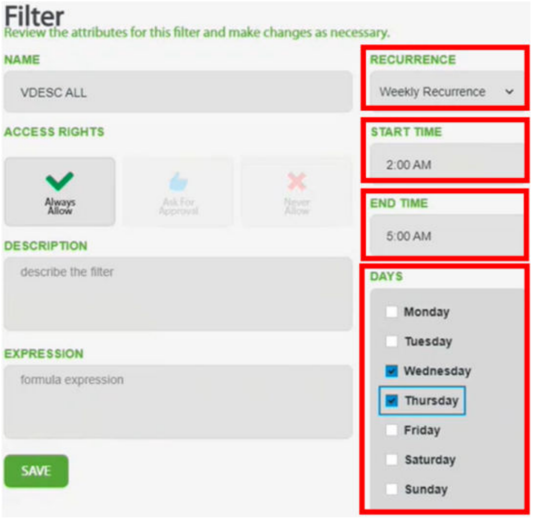
VARIANADMIN - ALW...
Access allowed any time = Varian Policy Server Administrator (varianadmin / varianadmin@varian.com)

5. Enter a description for the filter, for example, `Access allowed any time = Varian Field Service Rep`.
6. Leave the **EXPRESSION** text box blank.

   Note: Although blank, SmartConnect Access Control Manager automatically documents the user ID of any Service or Maintenance team member accessing the system during the maintenance window.

7. Select one of the following options from the **RECURRENCE** tab:

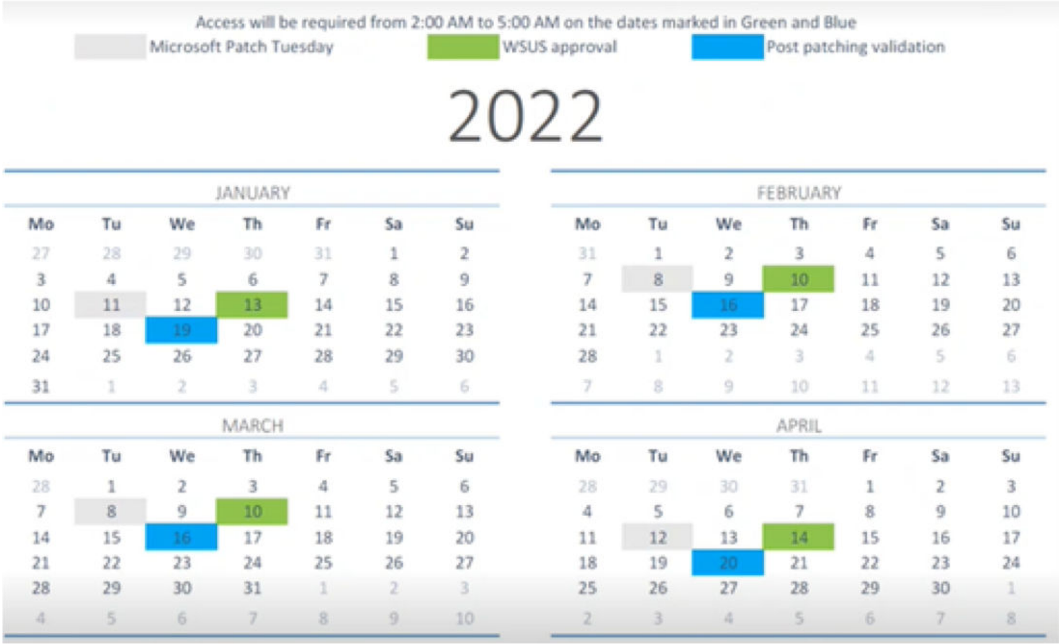
Option	**Description**
Not Specified	This option specifies no time period for access. If you previously added a Time Window and need to remove it, select this option.

Option	Description
One Time	This option allows a single time period for access, for example, Service or Maintenance access. Use this option to perform maintenance at multiple defined scheduled days. Select a start time, an end time, and the date range for the agreed maintenance.  Filter Review the attributes for this filter and make changes as necessary. NAME: VDESC ALL RECURRENCE: One Time ACCESS RIGHTS: Always Allow START TIME: 2:00 AM END TIME: 5:00 AM DESCRIPTION: describe the filter DATE RANGE FROM: 10-01-2022 TO: 10-01-2022 EXPRESSION: formula expression
Weekly Recurrence	This option allows access on specified days of the week, during specified hours. Use this option to perform maintenance weekly during a defined time slot. Select a start time, an end time, and the days for the agreed maintenance.  Filter Review the attributes for this filter and make changes as necessary. NAME: VDESC ALL RECURRENCE: Weekly Recurrence ACCESS RIGHTS: Always Allow START TIME: 2:00 AM END TIME: 5:00 AM DESCRIPTION: describe the filter EXPRESSION: formula expression DAYS ☐ Monday ☐ Tuesday ☑ Wednesday ☑ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Option	Description
Weekly Range	This recurring option allows access during a specified range of days of the week.

Note: The selected maintenance window should allow access during the agreed time slots.

For example, Varian may provide a patching calendar, requesting to access from 2 a.m. to 5 a.m. once every month, on Wednesday and Thursday. For each of these days, create a “One Time” filter and apply the filter to the “Start Remote Terminal” policy (see Apply Passthrough Filter to a Policy on page 83).



Access will be required from 2:00 AM to 5:00 AM on the dates marked in Green and Blue

⬜ Microsoft Patch Tuesday 🟩 WSUS approval 🟦 Post patching validation

2022

JANUARY

Mo	Tu	We	Th	Fr	Sa	Su
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

FEBRUARY

Mo	Tu	We	Th	Fr	Sa	Su
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

MARCH

Mo	Tu	We	Th	Fr	Sa	Su
28	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

APRIL

Mo	Tu	We	Th	Fr	Sa	Su
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

If Varian requires access for 24 days non-concurrently, the customer will need to create a total of 24 “One Time” filters (one for each requested day) and apply the filters to the “Start Remote Terminal” policy.

8. Click **SAVE**.

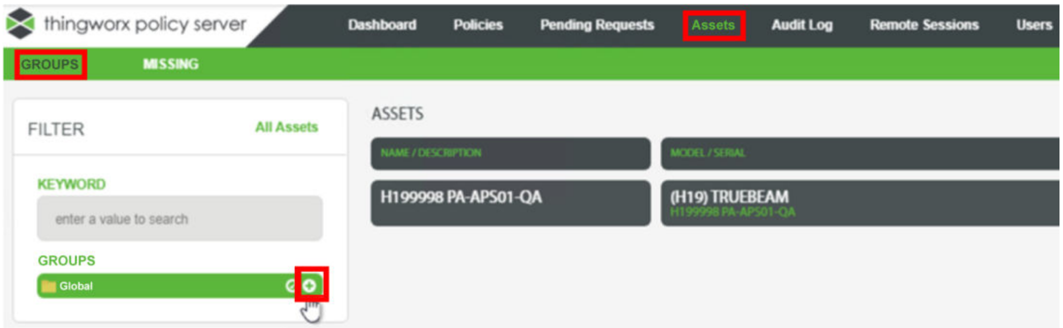
Add Assets, Group Assets and Create Notification to Approve Access Request

Note: To add assets, you will need Varian assistance.

The hierarchy of asset groups exists to support the inheritance of policies. By default, all automatically created asset groups inherit the policy of the Global asset group. To change this inheritance, you can create your own asset groups with a set of customized policies and move assets to these newly created groups. For example, TrueBeam machines and ProBeam machines can exist in two separate groups with different sets of policies such that each group can have different access controls (for example, different maintenance windows, approvers, passthrough filters).

You can add assets and create notifications by creating asset groups.

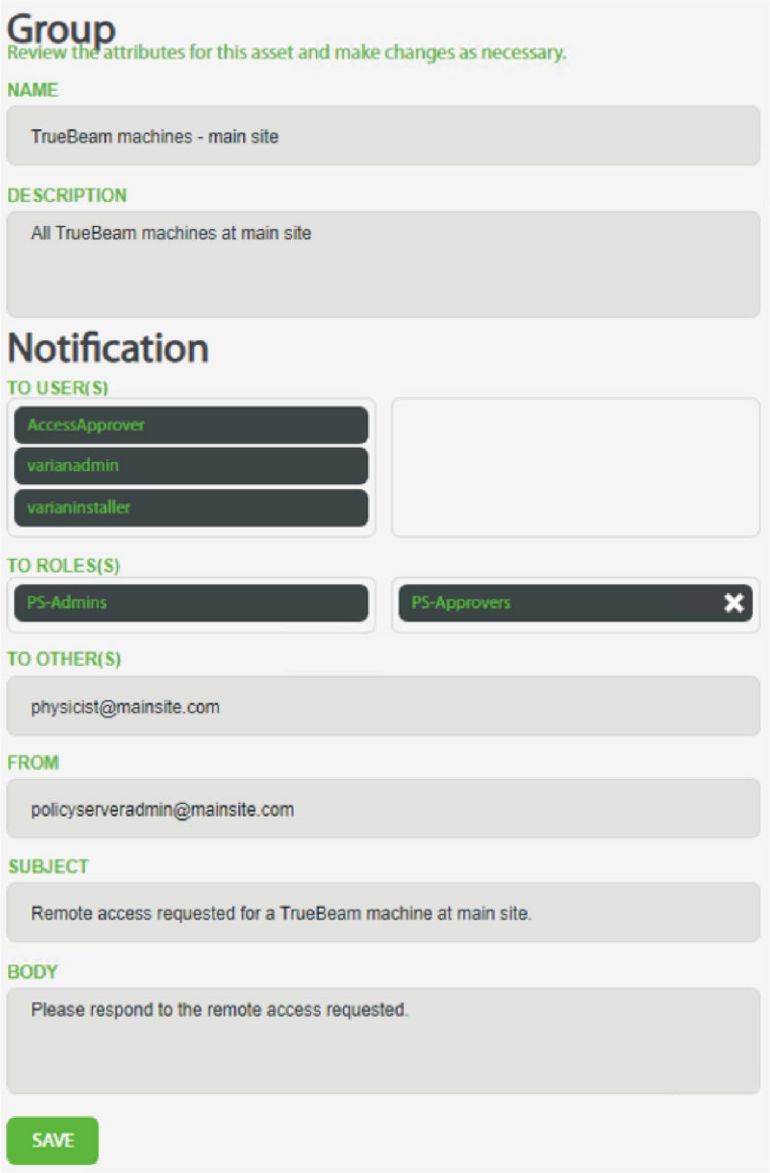
1. Contact Varian to add asset.
2. Group the assets by site, machine name, or customer-preferred name for the group.
3. Click **Assets**.
4. Click the **GROUPS** tab.
5. Click ⊕ next to the **Global** folder to add a subgroup.



NAME / DESCRIPTION	MODEL / SERIAL
H199998 PA-APS01-QA	(H19) TRUEBEAM H199998 PA-APS01-QA

6. Use the **TO USER(S)** or **TO ROLE(S)** tabs to move the users or roles to be notified to the drop box on the right.
7. Enter a name, a description, one or more recipient e-mail addresses in **TO OTHER(S)**, and the sender e-mail address in **FROM**.
8. Enter the subject and the body of the e-mail with all relevant notification information.

9. Click **SAVE**.



Group

Review the attributes for this asset and make changes as necessary.

NAME

TrueBeam machines - main site

DESCRIPTION

All TrueBeam machines at main site

Notification

TO USER(S)

AccessApprover

varianadmin

varianinstaller

TO ROLES(S)

PS-Admins

PS-Approvers ✕

TO OTHER(S)

physicist@mainsite.com

FROM

policyserveradmin@mainsite.com

SUBJECT

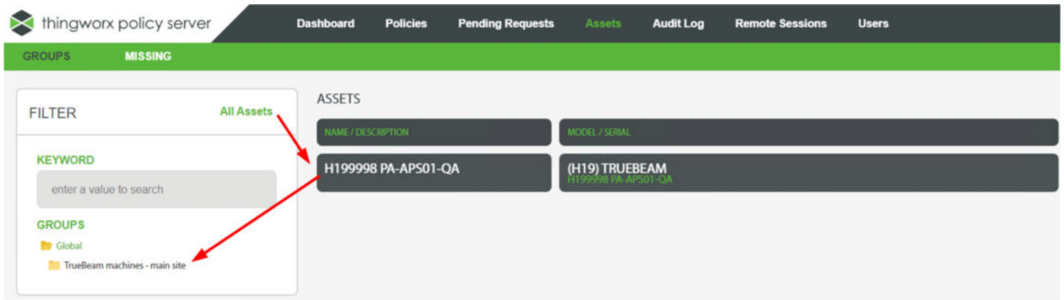
Remote access requested for a TrueBeam machine at main site.

BODY

Please respond to the remote access requested.

10. Click **All Assets**.

11. Drag and drop the desired asset (for example, “H199998 PA-APS01-QA”) to the desired group (for example, “TrueBeam machines - main site”) on the left.



ASSETS

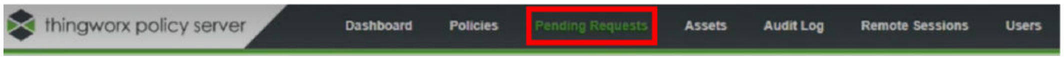
NAME / DESCRIPTION	MODEL / SERIAL
H199998 PA-APS01-QA	(H19) TRUEBEAM H199998 PA-APS01-QA

Approve Pending Requests for Access

If an access right is set to **Ask for Approval**, the SmartConnect Access Control receives a request for approval and sends an email notification to the assigned user.

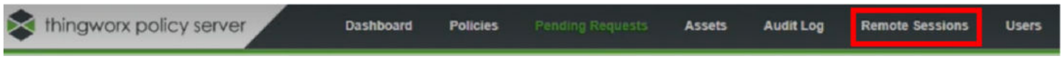
The user should follow the below instructions.

1. Click **Pending Requests** to see any pending accessing requests.
2. Approve or deny a pending request.



Monitor and End a Remote Session

1. Click **Remote Sessions** to view the status of all remote sessions.
2. End an in-progress remote session if necessary.



Audit Log Information

Note: The **Audit Log** tab shows all activity that SmartConnect Access Control Manager generates by recording in text. The **Audit Log** tab also shows the activity included in the XML messages provided by SmartConnect Agents.

An audit log shows the following information:

User The name of the user associated with the audited activity.

Date/Time The date and time that the action was generated or initiated.

Category The type of activity, for example, User Access (logins, logouts), Asset Communication (messages sent from/to SmartConnect Agents), Configuration (Asset tab), Remote Access (remote sessions), Administration (Users tab – create, modify, and delete profiles, roles, and users).

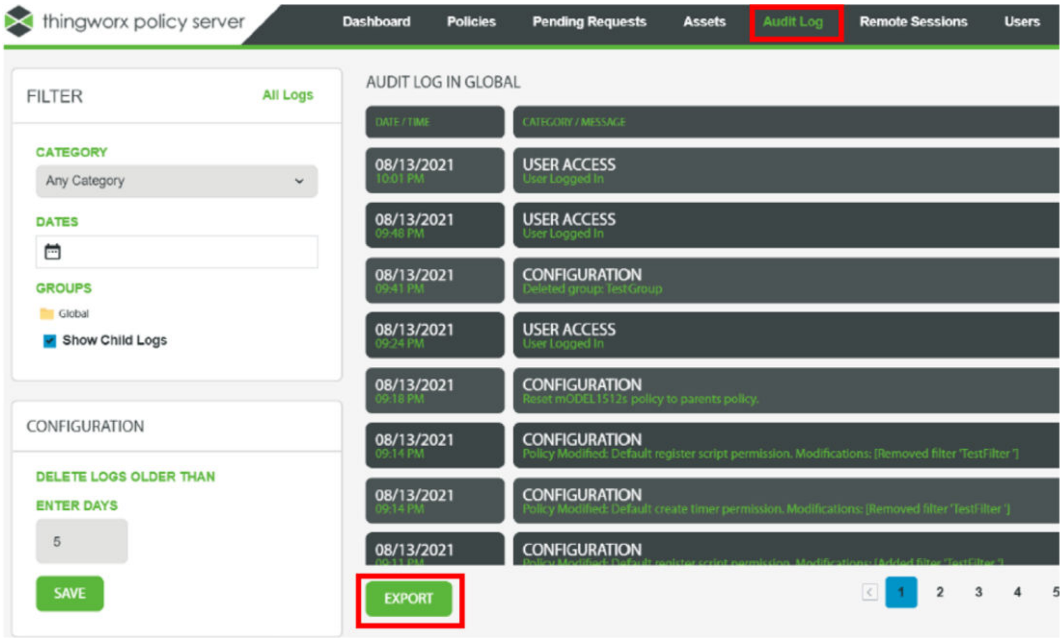
Message A detailed description of the activity.

Group If applicable, the name of the asset group related to the entry and saved on Policy Server.

Export the Audit Log

1. Click **Audit Log**.
2. Click **EXPORT** to export the audit log into .CSV format.

> **Note:** You can also export the audit log to a “Security Information and Event Management (SIEM)” system. Varian can assist you with SmartConnect Access Control Manager installation and configuration. The customer is responsible for configuring their SIEM, Syslog, or their environment to receive information from SmartConnect Access Control Manager.



CATEGORY: Any Category

DATES

GROUPS: Global

☑ Show Child Logs

CONFIGURATION

DELETE LOGS OLDER THAN

ENTER DAYS: 5

AUDIT LOG IN GLOBAL

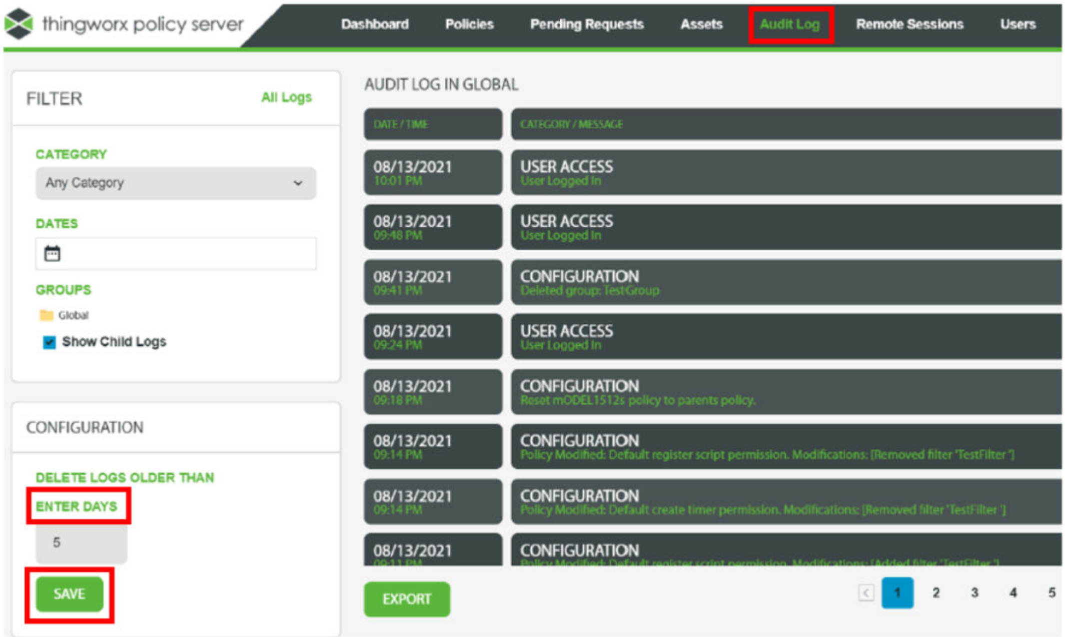
DATE / TIME	CATEGORY / MESSAGE
08/13/2021 10:01 PM	USER ACCESS User Logged In
08/13/2021 09:48 PM	USER ACCESS User Logged In
08/13/2021 09:41 PM	CONFIGURATION Deleted group: TestGroup
08/13/2021 09:24 PM	USER ACCESS User Logged In
08/13/2021 09:18 PM	CONFIGURATION Reset mODEL1512s policy to parents policy.
08/13/2021 09:14 PM	CONFIGURATION Policy Modified: Default register script permission. Modifications: [Removed filter 'TestFilter ']
08/13/2021 09:14 PM	CONFIGURATION Policy Modified: Default create timer permission. Modifications: [Removed filter 'TestFilter ']
08/13/2021 09:11 PM	CONFIGURATION Policy Modified: Default register script permission. Modifications: [Added filter 'TestFilter ']

Change the Time Period for a Log Record to Be Displayed in the UI

> **Note:** The default and minimum number of days a log record is displayed on the UI is 5 days. You cannot set a lower value and you must use an integer to specify the desired number of days. All log records are stored in a log folder.

Follow the instructions below to change the time period for a log record to be displayed in the UI.

1. Click **Audit Log**.
2. Click **ENTER DAYS** for logs to be displayed in the UI.
3. Click **SAVE**.



CATEGORY

Any Category

DATES

GROUPS

Global

☑ Show Child Logs

CONFIGURATION

DELETE LOGS OLDER THAN

ENTER DAYS

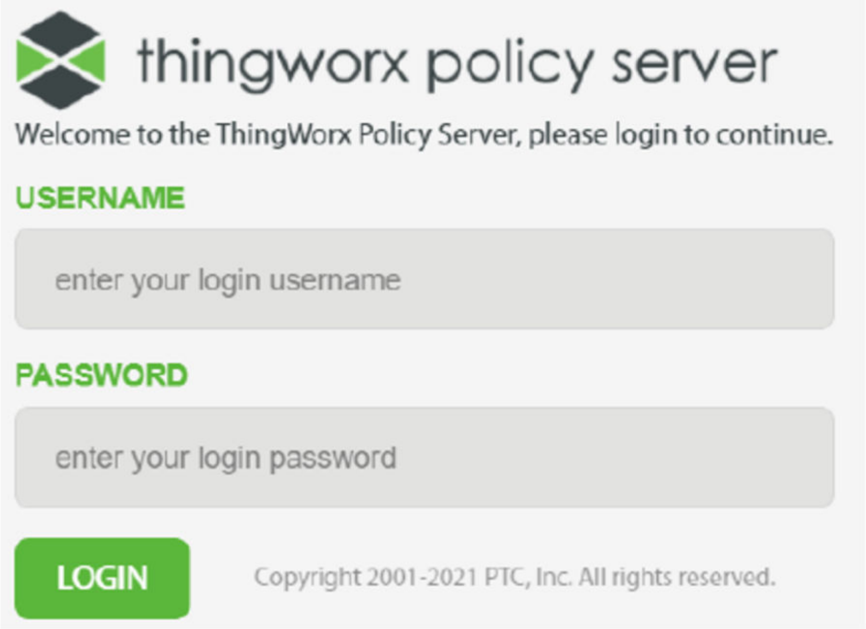
5

AUDIT LOG IN GLOBAL

DATE / TIME	CATEGORY / MESSAGE
08/13/2021 10:01 PM	USER ACCESS User Logged In
08/13/2021 09:48 PM	USER ACCESS User Logged In
08/13/2021 09:41 PM	CONFIGURATION Deleted group: TestGroup
08/13/2021 09:24 PM	USER ACCESS User Logged In
08/13/2021 09:18 PM	CONFIGURATION Reset mODEL1512s policy to parents policy.
08/13/2021 09:14 PM	CONFIGURATION Policy Modified: Default register script permission. Modifications: [Removed filter 'TestFilter ']
08/13/2021 09:14 PM	CONFIGURATION Policy Modified: Default create timer permission. Modifications: [Removed filter 'TestFilter ']
08/13/2021 09:11 PM	CONFIGURATION Policy Modified: Default register script permission. Modifications: [Added filter 'TestFilter ']

Sign In

1. Type the IP address and port number for thingworx policy server in the address bar of your browser.
   - If you are running the browser from the same machine where thingworx policy server is running, type localhost.
   - If you are using port 80, you do not need to type a port number. Type instead the number of the listening port you chose for thingworx policy server. The login page for the thingworx policy server application appears.



thingworx policy server

Welcome to the ThingWorx Policy Server, please login to continue.

USERNAME

enter your login username

PASSWORD

enter your login password

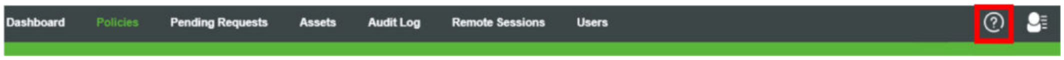
LOGIN

Copyright 2001-2021 PTC, Inc. All rights reserved.

2. Enter your credentials choosing one of the following options:
   - If you are an administrator user, type the username and password associated to the administrator saved in the LDAP directory server and added to the APSAdmins group.
   - If you are a user in Microsoft Active Directory, type the username and password you use to access Microsoft Active Directory.

Get Quick Help

1. Click the question mark button in the upper right corner of the screen to find additional information or help topics.



Index

4D Integrated Treatment Console (4DITC)
- anti-virus software policies 18
- TCP ports 62
- third-party hardware or software installation policy 34

A

abbreviations 14

access permissions 80

access requests
- approve 90

access rights 80

acronyms 14

Acuity system
- anti-virus software policies 18
- TCP ports 62
- third-party hardware or software installation policy 34

adding assets 88

adding system-level administration (DBA) accounts 46

Always Allow 80

anomalies from real-time anti-virus scanning 28

anti-virus software
- real-time scanning anomalies 28

anti-virus software policy 17
- ARIA Connect 26
- ARIA eDoc 26
- Citrix 29
- Eclipse DCF Server 24
- exclusions from continuous or real-time scanning 23–26
- InSightive database server 25
- Microsoft SQL database system 24
- Mobius3D 26
- non-treatment delivery system policies 22
- non-treatment delivery systems 17
- treatment delivery system policies 18
- treatment delivery systems 17
- VariSeed and Vitesse 25
- Velocity systems 24

applying passthrough filters to a policy 83

approve access requests 90

Arcserve backup solution 49

ARIA Connect
- anti-virus software policies 22
- backup guidelines 52
- exclusions from anti-virus scanning 26
- third-party hardware or software installation policy 33

ARIA Database Server
- backup guidelines 50
- third-party hardware or software installation policy 33

ARIA eDoc
- exclusions from anti-virus scanning 26

ARIA image server
- backup guidelines 51

ARIA Oncology Information System (OIS)
- database access policy 40

ARIA systems and workstations
- anti-virus software policies 22
- exclusions from anti-virus scanning 23
- third-party hardware or software installation policy 32
  - AURA 33

ARIA web (platform) server
- backup guidelines 51

Ask for Approval 80

Asset Manager 78

assets
- adding 88
- grouping 88

ATA (Advanced Technology Attached) 49

audit log
- Category 90
- Date/Time 90
- export 91
- Group 90
- Message 90
- time period for displaying log records 91
- User 90

auditing remote sessions 91

audits of Microsoft SQL 45

AURA (ARIA Unified Reporting Application)
- anti-virus software policies 22
- third-party hardware or software installation policy 33

AURA database server
- backup guidelines 50

B

backup and maintenance tool 56
  ARIA 13.X and earlier 56
  ARIA 15.X and later 57
backup frequency 54
backup guidelines 48, 49
  affected products 48
  ARIA / AURA database server 50
  ARIA Connect 52
  ARIA image server 51
  ARIA web (platform) server 51
  backup solutions 48
    Arcserve 49
    other third-party backup solutions 49
  Citrix environment 52
  DCF Core Installed on a Server 51
  Eclipse clients 51
  Eclipse standalone system 52
  exceptions 54
  IDENTIFY system 55
  Mobius3D 54
  VelocityGRID 52
backup responsibility 48
backup software
  replace with customer solutions 46
Brachytherapy
  anti-virus software policies 18
  TCP ports 62
BrachyVision treatment planning system
  anti-virus software policies 22
  database access policy 40
  third-party hardware or software installation policy 36
Bravos
  anti-virus software policies 18
  third-party hardware or software installation policy 34

C

Calypso
  anti-virus software policies 18
  third-party hardware or software installation policy 34
CBCT (Cone-Beam Computerized Tomography)
  see Cone Beam CT (CBCT)
change log record display period 91
change password for maintenance and servicing accounts 47
checklist on cybersecurity 8
Citrix
  backup guidelines 52
  third-party hardware or software installation policy 33
Citrix endpoint security 29
classification of Varian workstations 60
Clinac 14
  anti-virus software policies 18
CNID (Clinac Network Interface Device) 59
Combo Server
  backup guidelines 51
Comprehensive Cancer Solution Clients
  third-party hardware or software installation policy 32
Cone Beam CT (CBCT)
  anti-virus software policies 18
  third-party hardware or software installation policy 34
confirming users 77
creating maintenance windows 84
creating notifications 88
creating passthrough filters 82
creating roles 79
creating security profiles 78
CU (Cumulative Update) 14
custom digital certificates 73
customer enterprise agreement with Microsoft 45
customer security posture and MICAP 66
cybersecurity checklist 8

D

DAS (Direct Attached Storage) 49
database access policy 40
  access rules 40
  affected products 40
  responsibilities 40
database maintenance software
  replace with customer solutions 46
DBA (Database Administrator) accounts 46
DCF (Distributed Calculation Framework) 14
DCF Core Server
  backup guidelines 51
definitions 14
DES (Data Encryption Standard) 14

determining the edition and version of MS SQL 45
determining the type and number of MS SQL licenses 44
DHCP (Dynamic Host Communication Protocol) 61
DICOM Services
  third-party hardware or software installation policy 33
digital certificate use rules 73
digital certificates use policy 73
  affected products 73
disabling Microsoft SQL accounts 46
DNS (Domain Name System) 14
Docs2EHR
  third-party hardware or software installation policy 33
DoseLab 68

E

E-Prescribe
  third-party hardware or software installation policy 33
Eclipse treatment planning system
  anti-virus software policies 22
  backup guidelines
    clients 51
    standalone systems 52
  database access policy 40
  exclusions from anti-virus scanning 24
  third-party hardware or software installation policy 36
Edge radiosurgery system
  anti-virus software policies 18
  third-party hardware or software installation policy 34
edition of MS SQL 45
EDR (Endpoint Detection and Response) 14
end point device management 60
ending remote sessions 90
ePeerReview 68
Equicare Patient Portal
  third-party hardware or software installation policy 33
Ethos radiotherapy system
  anti-virus software policies 18
  third-party hardware or software installation policy 34
Ethos treatment management 68
Ethos treatment planning 68
exclusions from continuous or real-time anti-virus scanning 23
  ARIA Connect 26
  ARIA eDoc 26
  Citrix 29
  Eclipse DCF Server 24
  InSightive database server 25
  Microsoft SQL database system 24
  Mobius3D 26
  VariSeed and Vitesse 25
  Velocity systems 24
exporting Audit Log 91
Eye Position Verification System
  third-party hardware or software installation policy 33

F

FAS (Framework Agent Server)
  anti-virus software policies 22
  backup guidelines 51
  third-party hardware or software installation policy 36
FullScale 68

G

GammaMed
  anti-virus software policies 18
  third-party hardware or software installation policy 34
GDR (General Distribution Release) 14
grouping assets 88

H

Halcyon system
  anti-virus software policies 18
  TCP ports 62
  third-party hardware or software installation policy 34
High Availability & Rapid Recovery Protection (HARRP)
  third-party hardware or software installation policy 33
HIPS (Host Intrusion Prevention Software) 14

I

IDENTIFY system
- anti-virus software policies 18
- backup guidelines 55
- TCP ports 62
- third-party hardware or software installation policy 34

Image Server
- backup guidelines 51
- third-party hardware or software installation policy 33

In-Room Monitor Workstations
- anti-virus software policies 18

Information Exchange Manager (IEM)
- third-party hardware or software installation policy 33

InSightive
- anti-virus software policies 22
- database access policy 40
- third-party hardware or software installation policy 33

InSightive clients
- third-party hardware or software installation policy 32

InSightive database server
- exclusions from anti-virus scanning 25

InSightive desktop application
- third-party hardware or software installation policy 32

installing third-party hardware and software with Varian products 31
- category 1 products policy 32
- category 2 products policy 33
- category 3 products policy 34
- category 4 products policy 36
- operating system policy 37
- product categories 31

internet best practices 29

introduction 8

IP (Internet Protocol) 61

ISV (Independent Software Vendor) license agreement 42

L

Linac Verification Interface (LVI)
- third-party hardware or software installation policy 34

Log Profile 78

log record storage 91

M

maintenance windows
- creating 84

mean time between failures 66

MEVION Verification Console
- TCP ports 62

MICAP (Mission Critical Application Protection) 59
- affected products 59
- benefits 61
- customer security posture 66
- device configuration 62
- installations 61
- integrity 60
- maintenance 66
- remote management service 67
- requirements 61

MICAP management services 66

MICAP Sphere 67

Microsoft audits 45

Microsoft Hot-Fix Release memo 45

Microsoft operating system security 29

Microsoft SQL 42
- adding system-level administration (DBA) accounts 46
- affected products 42
- allowed number of installed software instances 45
- customer responsibilities and prohibitions 42
- determining the edition and version 45
- determining the type and number of licenses 44
- Microsoft audit 45
- Microsoft customer enterprise agreement 45
- password change policy 47
- removing or disabling accounts 46
- replacing the backup and database maintenance software with customer solutions 46
- running Varian System Database on a virtual server 45
- Varian responsibilities 42

Microsoft SQL database system
- exclusions from anti-virus scanning 24

mission critical workstations 60
MLC (Multi-Leaf Collimator) workstation
  anti-virus software policies 18
Mobius3D
  anti-virus software policies 22
  backup guidelines 54
  exclusions from anti-virus scanning 26
  third-party hardware or software installation policy 34
monitoring remote sessions 90
MS SQL
  see Microsoft SQL
MS SQL Database
  third-party hardware or software installation policy 33
MTBF (mean time between failures) 66

N

NAS (Network Attached Storage) 14
NAT (Network Address Translation) 62
Never Allow 80
non-critical workstations 60
non-treatment delivery systems
  anti-virus software policies 17, 22
Non-Varian Treatment (NVT)
  third-party hardware or software installation policy 34
noona 68
Not Specified 84
notifications
  creating 88
NTP (Network Time Protocol) 62
number of instances of installed Microsoft SQL software 45
number of MS SQL licenses 44

O

OIS (Oncology Information System)
  database access policy 40
On-Board Imager (OBI)
  anti-virus software policies 18
  third-party hardware or software installation policy 34
Oncolog Cancer Registry
  third-party hardware or software installation policy 33
Oncology Systems Platform (OSP)
  third-party hardware or software installation policy 33
OncoView
  third-party hardware or software installation policy 33
OncQT
  third-party hardware or software installation policy 33
One Time 84
OSMS systems
  anti-virus software policies 18

P

passthrough filters
  applying 83
  creating 82
password change policy 47
paths
  see typical paths
pending requests
  approve 90
performance issues due to real-time anti-virus scanning 28
preparing for ransomware attacks 69
  Varian responsibility 70
preventing ransomware attacks 70
  Varian responsibility 71
ProBeam
  anti-virus software policies 18
  third-party hardware or software installation policy 32, 34
ProBeam 360 proton therapy system 68
ProBeam Eye Treatment Database
  third-party hardware or software installation policy 33
prohibitions
  use of MS SQL 42
PVAI (PortalVision Advanced Imaging) 60

Q

quick help 93
Qumulate 68

R

ransomware 68
- customer responsibility 69
- prepare 69
- prevent 70
- respond 71

RapidSphere 68
real-time anti-virus scanning 14, 27
- anomalies 28

recovery of data 58
Remote Asset Access Request Approver 78
remote management for MICAP 67
remote sessions
- auditing 91
- ending 90
- monitoring 90

removing Microsoft SQL accounts 46
replacing the backup and database maintenance software with customer solutions 46
RePortal
- third-party hardware or software installation policy 33

requirements for MICAP functionality 61
Respiratory Gating
- third-party hardware or software installation policy 34

responding to ransomware attacks 71
- Varian responsibility 72

responsibilities
- backup 48
- database access 40
- ransomware 69–72
- use of MS SQL
  - customer 42
  - Varian 42

restoration of data 58
RGSC (Respiratory Gating for Scanners)
- anti-virus software policies 18
- TCP ports 62

roles
- creating 79

RPM (real-time position management)
- anti-virus software policies 18
- TCP ports 62

RPO (recovery point objective) 70
RTO (recovery time objective) 72
running Varian System Database on a virtual server 45

S

SaaS (Software as a Service) 68
SAN (Storage Area Network) 49
security profiles
- creating 78

server class computers
- anti-virus software policies 22

serviceadmin account
- change password 47

Shared Framework
- third-party hardware or software installation policy 33

signing in to Thingworx Policy Server 93
SmartConnect 75
SmartConnect Access Control Manager 75
- setup options 75

SP (Service Pack) 14
SQL Server Service Admin (SA) account
- change password 47

SSH (Secure Shell) 14
SUMITOMO Verification Console
- TCP ports 62

Sybase
- third-party hardware or software installation policy 33

system backup 54
system critical database logs backup 54
system security updates 29
- up-to-date Citrix information 29

T

TCP (Transmission Control Protocol)
- ports 62

terms 14
Thingworx Policy Server 75
- signing in 93

third-party backup solutions 49
- Arcserve 49

third-party hardware or software installation 31
- category 1 products policy 32
- category 2 products policy 33
- category 3 products policy 34
- category 4 products policy 36
- operating system policy 37
- product categories 31

treatment delivery systems
- anti-virus software policies 17, 18

TrueBeam STx system
- anti-virus software policies 18
- third-party hardware or software installation policy 34

TrueBeam system
- anti-virus software policies 18
- TCP ports 62
- third-party hardware or software installation policy 34

type of MS SQL licenses 44

typical paths
- ARIA / AURA database server data 50
- ARIA Connect data 52
- ARIA image server data 51
- ARIA web (platform) server data 51
- Citrix environment data 52
- Eclipse clients data 51
- Eclipse standalone system data 52
- FAS server data 51
- VelocityGRID data 52

U

updated information on Citrix security 29

updated information on Microsoft operating system security 29

updates of Microsoft SQL 45

USB drives best practices 29

user data files backup 54

users
- confirming 77

using own MS SQL licenses 45

V

VAIS (Varian Authentication and Identification Services)
- third-party hardware or software installation policy 33

Varian Database Access Policy 40
- affected products 40
- database access rules 40
- responsibilities 40

Varian Exchange
- anti-virus software policies 22

Varian HDR Treatment Console
- third-party hardware or software installation policy 34

Varian Mobile App
- database access policy 40

Varian Oncology Information System 42

Varian System Database
- run on a virtual server 45

Varian System Server
- third-party hardware or software installation policy 33

Varian Treatment (VTx)
- TCP ports 62
- third-party hardware or software installation policy 34

Varian Treatment Workstation
- anti-virus software policies 18

Varian use of Microsoft SQL 42
- customer responsibilities and prohibitions 42
- Varian responsibilities 42

VariSeed
- anti-virus software policies 22
- exclusions from anti-virus scanning 25
- third-party hardware or software installation policy 34

VariSource
- anti-virus software policies 18
- third-party hardware or software installation policy 34

Velocity standalone
- third-party hardware or software installation policy 33

Velocity systems
- anti-virus software policies 22
- exclusions from anti-virus scanning 24

VelocityAI 52

VelocityGRID
- backup guidelines 52
- third-party hardware or software installation policy 32, 33

version of MS SQL 45

View Only 78

Visual Coaching Device (VCD)
- anti-virus software policies 18, 22

visual cues 14

VitalBeam system
- anti-virus software policies 18
- third-party hardware or software installation policy 34

Vitesse
- anti-virus software policies 22

exclusions from anti-virus scanning 25
third-party hardware or software installation policy 34
VSP (Varian Service Portal) 14
VTN (Varian Treatment Network)
protection 59

W

Weekly Range 84
Weekly Recurrence 84
Windows Domain Varian account
change password 47
Worklist Workstation
anti-virus software policies 18
third-party hardware or software installation policy 34
workstations
classification 60

X

XDR (Extended Detection and Response) 14
XmediusFax
third-party hardware or software installation policy 33