



BackBox[®] E4.13 Virtual BackBox Installation

Abstract

This Virtual BackBox Installation document is for BackBox[®] E4.13

Published: July 2024



Legal Notice

© Copyright 2013, 2024 ETI-NET Inc. All rights reserved.

Confidential computer software. Valid license from ETI-NET Inc. required for possession, use or copying.

The information contained herein is subject to change without notice. The only warranties for ETI-NET- products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. ETI-NET shall not be liable for technical or editorial errors or omissions contained herein.

BackBox is registered trademark of ETI-NET Inc.

StoreOnce is a registered trademark of Hewlett Packard Development, L.P.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Tivoli

Storage Manager (TSM) is a registered trademark of IBM Corporation.

QTOS is a registered trademark of Quality Software Associates Inc.

All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

This document, as well as the software described in it, is furnished under a License Agreement or Non- Disclosure Agreement. The software may be used or copied only in accordance with the terms of said Agreement. Use of this manual constitutes acceptance of the terms of the Agreement. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another programming language, for any purpose without the written permission of ETI-NET Inc.

Copyright © 2013, 2024 ETI-NET Inc. All rights reserved.

Table of Contents

Introduction	4
Virtual Machine Requirements	5
BackBox Software	6
TCP/IP Connection	7
PowerShell Execution Policy	8
Install Additional Roles and Features	9
Complete the Server Preparation	11
Virtual Server Naming	11
System Settings	12
Remote Desktop	12
Remote Desktop Session Host Configuration	13
Windows Update	14
Advanced Sharing Settings	14
Firewall Settings	15
VTC Management Console	17
Domain Node	17
iSCSI Node	17
Install the Virtual Tape Controller Software	20
Customize Server Identity	23
License Request	23
Start Services	25
Connect Virtual Tape Device to Virtual NonStop System	27
Install BackBox UI Client	28
Atto HBA Target Mode in VMWare ESXi Passthrough Mode	29
Appendix	34

Introduction

This guide documents the preparation of the virtual Windows server(s) who will act as a Virtual Tape Controller for BackBox iSCSI environment. The virtual BackBox will only work with a virtual NonStop system.

Virtual Machine Requirements

The following minimum specifications are required to install and use a Virtual BackBox (vBB).




Atto Fiber card in passthrough mode is supported only with VMware ESXi. In this case, vBackBox must remain attached to this ESXi hypervisor host.

- 2 Cores (or 2 Core per physical Atto port assigned to the VM)
- 8 Gb of memory (add extra 4 Gb for each Atto port assigned to the VM up to 32 Gb)
- 250 Gb Hard Drive
- 2, 10 Gb Ethernet card (one for iSCSI and one to access the storage)
- Windows Server Standard 2022, 2019 or 2016 (English US).

BackBox Software

Get the latest released software version package and uploaded to the newly created virtual machine.

	The package for the virtual machine contains the same folders as for the normal BackBox.
---	--

Folder Installation Package Latest Released Version	Content
Guardian-E413-yyyyymmdd	Latest BackBox Guardian Software
UI-E4.13nn	Installer for the BackBox UI Client
VTC-E4.13nn	Installer for the VTC application
VTCserverScripts-yyyyymmdd	PowerShell installation scripts required for upgrade or new installation

TCP/IP Connection

Connect the TCP/IP cable to the appropriate Network adapter and configure TCP/IP according to the following Guidelines:

Guidelines

Assign a fixed TCP/IP address (do not use DHCP to obtain the address) according to customer's specification.

Make sure that the IP routing allows communications between the VTC and the NonStop server, between the VTC and the operator/installer workstation.

Make sure the server is registered into the DNS or the Host file, if you plan to use the host name to reach the VTC.

Virtual NonStop must have a second adapter configured on a storage CLIM. This adapter must be able to reach the public LAN on which the vBB is installed.

If ATTO Fiber HBA will be used in passthrough mode, you must configure the ESXi passthrough and assign physical port to the VM. Install the Atto driver prior to running PowerShell VTCServerPreparation.ps1 script. Refer to [Atto HBA Target Mode in VMWare ESXi Passthrough Mode](#) section for more details.

PowerShell Execution Policy

While logged as local administrator, start a PowerShell command window and type the following command to allow script execution:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope  
LocalMachine
```

- Answer Yes [Y]

Ensure the policy is in force:

```
Get-ExecutionPolicy -List
```

```
Scope                ExecutionPolicy -----  
MachinePolicy        Undefined  
UserPolicy            Undefined  
Process              Undefined  
CurrentUser          Undefined  
LocalMachine         RemoteSigned
```


Install Additional Roles and Features

Keep all default roles and features enabled by the Windows Server Standard edition (Desktop experience or Core installation) used for the operating system installation.

- The BackBox software requires an additional feature called Message Queuing Server (MSMQ-Server), that is automatically installed by the VTCServerPreparation.ps1 PowerShell script (in case it hasn't been already installed).

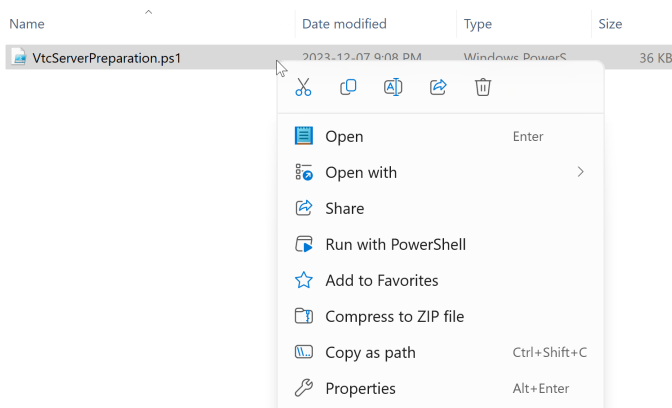


Before performing the VTC installation log in with the local Administrator account (Administrator user). Using such an account (with administrator privileges) may require an extra configuration step.



IMPORTANT: If you are using an account with Administrator privileges and not the local Administrator, start PowerShell command line using the Run as Administrator or pre-load macros before running scripts from a PowerShell command line: `Import-Module Server Manager`.

- In the same folder you uploaded the T0954V04^AAX SPR , locate the VTCServerScripts-yyyyymmdd folder, right-click on the file VtcServerPreparation.ps1 and click on Run with PowerShell (or launch the script from the opened PowerShell command line).



Some features may require server reboot. Re-execute this script until it shows that there are no more features to be installed.

```

Administrator: Windows PowerShell
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
Transcript started, output file is C:\Users\Administrator\Desktop\T0954V04^AAW\VTcserverScripts-20210420\ServerPreparati
on.log

Preparing Microsoft Windows Server 2022 Standard

VTC Server MS SChannel TLS configuration

Enable TLS 1.2
TLS 1.2 has been enabled (Server reboot required)
Configure .NET applications to use TLS 1.2
TLS 1.2 has been enabled for .NET applications (Server reboot required)
Disabled weak TLS protocols
TLS 1.0 has been disabled (Server reboot required)
TLS 1.1 has been disabled (Server reboot required)
Disable weak ciphers and algorithms
Protocol TLS_DHE_RSA_WITH_AES_256_CBC_SHA is currently disabled
Protocol TLS_DHE_RSA_WITH_AES_128_CBC_SHA is currently disabled
Protocol TLS_RSA_WITH_AES_256_GCM_SHA384 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_128_GCM_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_256_CBC_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_128_CBC_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_256_CBC_SHA has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_128_CBC_SHA has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_3DES_EDE_CBC_SHA has been disabled (Server reboot required)
Protocol TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 is currently disabled
Protocol TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 is currently disabled
Protocol TLS_DHE_DSS_WITH_AES_256_CBC_SHA is currently disabled
Protocol TLS_DHE_DSS_WITH_AES_128_CBC_SHA is currently disabled
Protocol TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA is currently disabled
Protocol TLS_RSA_WITH_RC4_128_SHA is currently disabled
Protocol TLS_RSA_WITH_RC4_128_MD5 is currently disabled
Protocol TLS_RSA_WITH_NULL_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_NULL_SHA has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_AES_256_GCM_SHA384 has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_AES_128_GCM_SHA256 has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_AES_256_CBC_SHA384 has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_AES_128_CBC_SHA256 has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_NULL_SHA384 has been disabled (Server reboot required)
Protocol TLS_PSK_WITH_NULL_SHA256 has been disabled (Server reboot required)
TLS/SSL Server Supports the use of Static key Ciphers has been disabled (Server reboot required)
TLS/SSL Server Supports the use of longer Diffie-Hellman ephemeral (DHE) key shares for TLS servers as been configured (S
erver reboot required)

Install MSNQP-Server Feature
Message Queuing Server already installed

System restart required to apply settings. Restart computer now?

Confirm
Are you sure you want to perform this action?
Performing the operation "Enable the local shutdown access rights and restart the computer." on target "localhost
(TECHWRITER)".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): _

```

- Reboot the system.

The server preparation script creates a specific log file in the script folder location: ServerPreparation.log. The transcript of each execution will be automatically logged into this file.

```

VTCserverScripts-20210420
File Home Share View
T0954V04^AAW > VTCserverScripts-20210420
Name Date modified Type Size
ServerPreparation 11/27/2023 7:37 PM Text Document 5 KB
VtcServerPreparation 10/30/2023 8:45 AM Windows PowerShell Sc... 35 KB

ServerPreparation - Notepad
File Edit Format View Help
PSVersion: 5.1.20348.1850
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.20348.1850
BuildVersion: 10.0.20348.1850
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
*****
Transcript started, output file is C:\Users\Administrator\Desktop\T0954V04^AAW\VTcserverScripts-20210420\ServerPreparation.log

Preparing Microsoft Windows Server 2022 Standard

VTC Server MS SChannel TLS configuration

Enable TLS 1.2
TLS 1.2 has been enabled (Server reboot required)
Configure .NET applications to use TLS 1.2
PS>TerminatingError(Get-ItemProperty): "The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set t
PS>TerminatingError(Get-ItemProperty): "The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set t
PS>TerminatingError(Get-ItemProperty): "The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set t
PS>TerminatingError(Get-ItemProperty): "The running command stopped because the preference variable "ErrorActionPreference" or common parameter is set t
TLS 1.2 has been enabled for .NET applications (Server reboot required)
Disabled weak TLS protocols
TLS 1.0 has been disabled (Server reboot required)
TLS 1.1 has been disabled (Server reboot required)
Disable weak ciphers and algorithms
Protocol TLS_DHE_RSA_WITH_AES_256_CBC_SHA is currently disabled
Protocol TLS_DHE_RSA_WITH_AES_128_CBC_SHA is currently disabled
Protocol TLS_RSA_WITH_AES_256_GCM_SHA384 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_128_GCM_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_256_CBC_SHA256 has been disabled (Server reboot required)
Protocol TLS_RSA_WITH_AES_128_CBC_SHA256 has been disabled (Server reboot required)

```

Complete the Server Preparation

Update the server with all critical updates recommended by Microsoft.

Finalize the server configuration according to corporate standards. This usually includes an anti-virus installation.

As the vBB is a dedicated server, its configuration must be compatible with the BackBox application software and the server access must be restricted to the server manager.

Virtual Server Naming

It is important to name carefully the virtual server, as vBackBox software uses part of that name to generate the virtual tape device serial number. The last three (3) alphanumeric characters of the given name are included in the auto-generated serial number.

For example, a vBackBox named vBBOX-1 will show devices with the following serial number: BBOX1100, BBOX1101 and BBOX1102.

The serial number always begins with BB followed by the three (3) alphanumeric characters taken from the VBackBox given name, followed by the adapter number (starting at 1), then by a target number.



In a multiple vBackBox environment, it is important to name the server in such a way as to ensure uniqueness in virtual devices serial number.

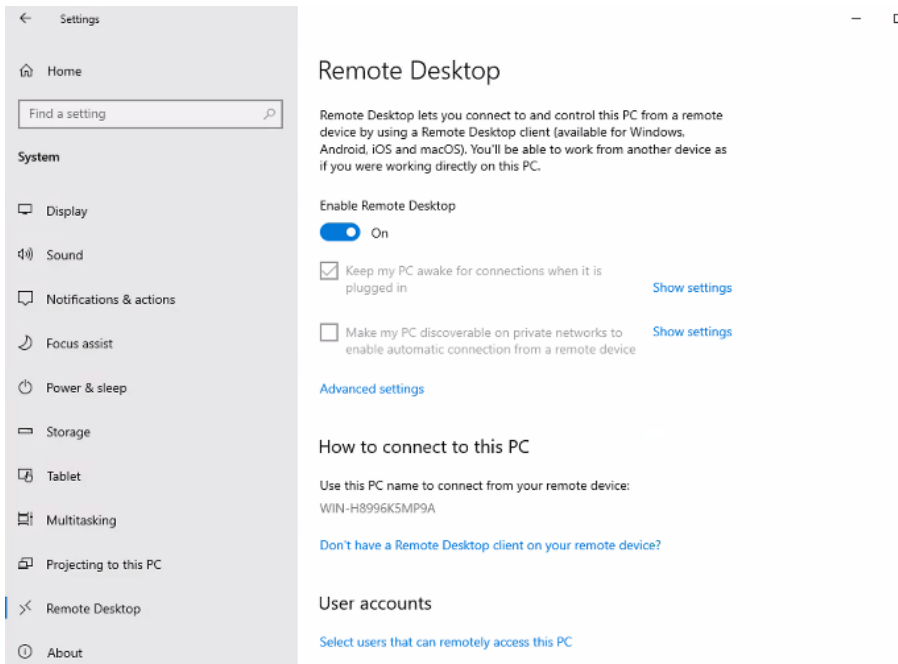
System Settings

Remote Desktop


Remote Desktop should be enabled to help server management.

To enable Remote Desktop:

- Press **Start**
- Select **Settings**
- Select **Remote Desktop**

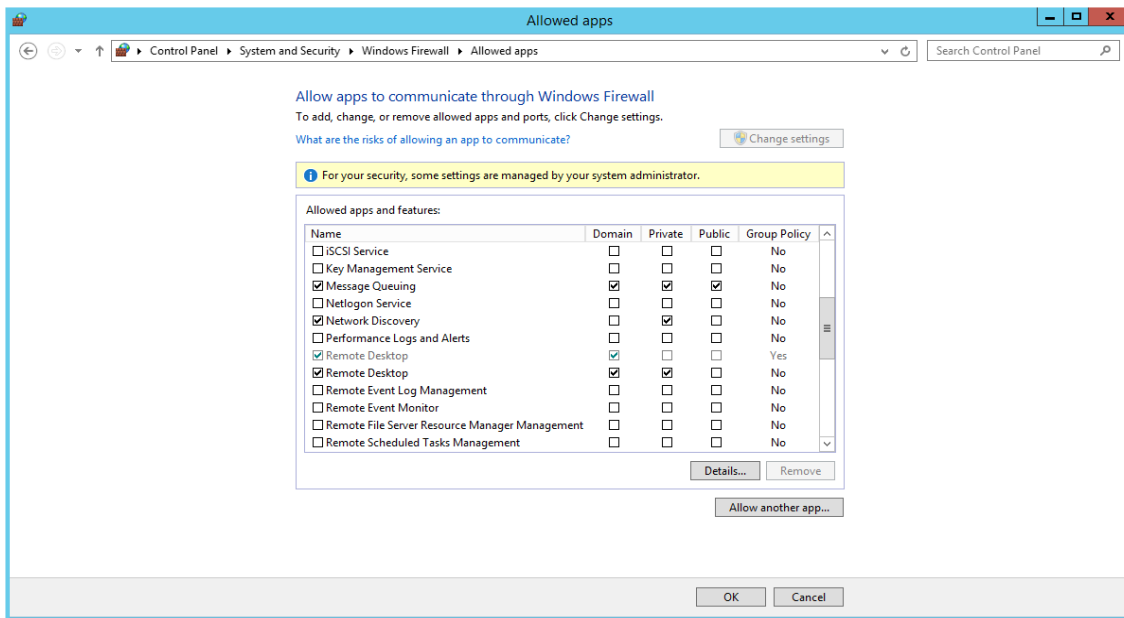


Enable Remote Desktop - On

	In case of a first-time configuration of the Remote Desktop – or if it needs to be re-enabled - a warning message will pop up. Enable the Firewall exception.
---	---

To enable the Firewall exception:

- Press **Start**
- Select **Control Panel**
- Select **System and Security**
- Under **Windows Firewall**, select **Allow a program through Windows Firewall**
- Scroll down to **Remote Desktop** and check the checkbox. Also check desired interface **Domain, Private and Public** check boxes



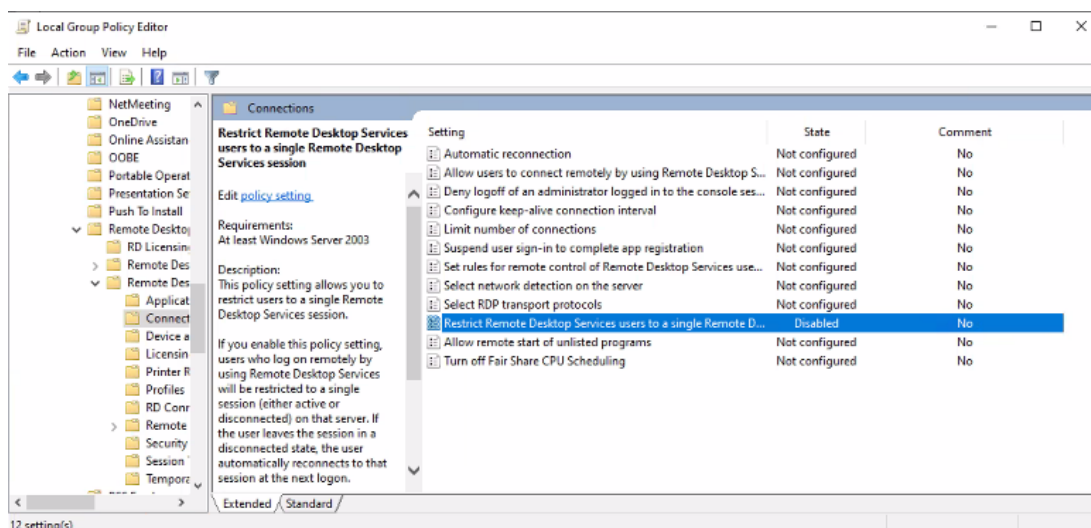
After opening the firewall, the warning message disappears from the Remote tab in the System Properties.

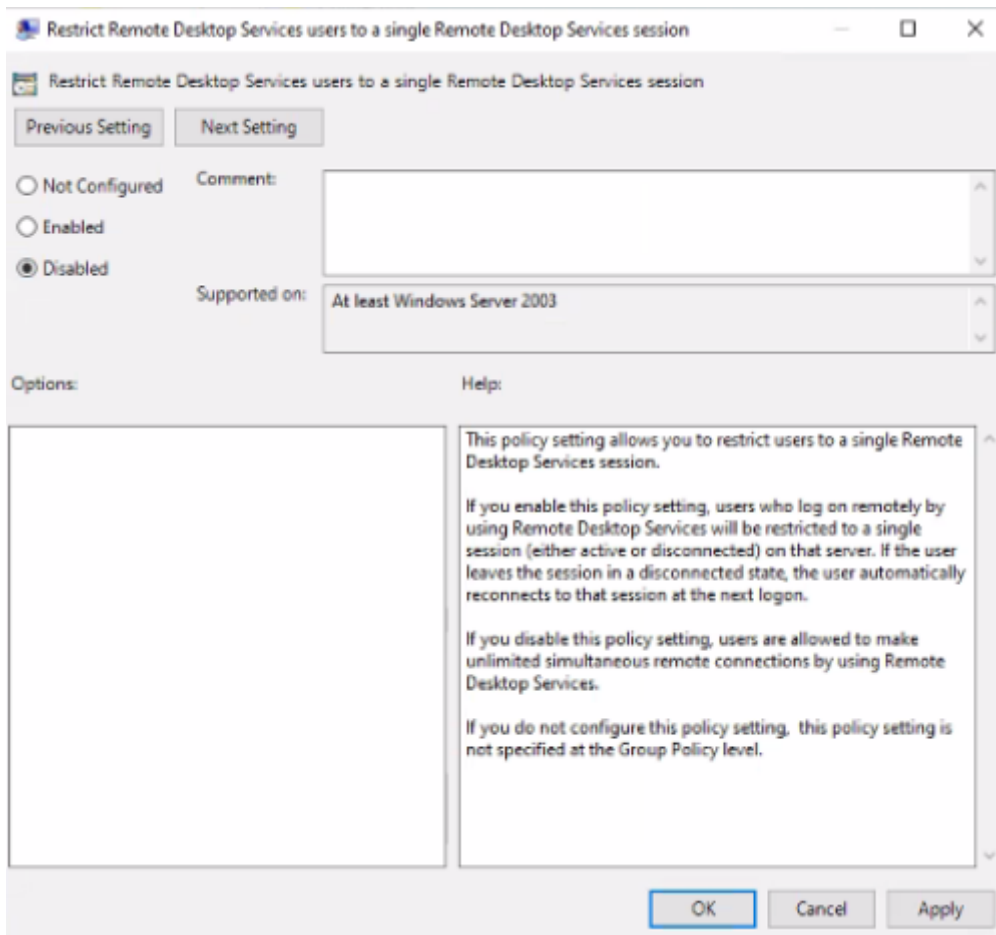
Remote Desktop Session Host Configuration

If two users attempt to perform a remote session using the same user credentials, the second user login session will be force-logged out by the first logged-in user's session. If there are two different users, who need to work on the same VTC using the same user's credentials, this restriction policy must be disabled in order to allow them to be connected in the same time.

To disable one user per session restriction policy:

- Press Start
- Type in the search dialog box gpedit.msc and start the program
- Navigate to: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections
- Locate the Restrict Remote Desktop Services users to a single Remote Desktop Services session setting
- To edit the setting, double click on it and a dialog box will appear
- Check Disabled.
- Apply the change and close the dialog by clicking OK





Windows Update

Windows Update feature should be disabled. To do so, set to download update only or just notify updates availability. Update installation should be managed on a case-by-case basis.

This will avoid unexpected server restart while tape activities are in progress.

To setup Windows Update:

- Press Start
- Select Control Panel
- Select Settings
- Select Windows Update and disable automatic updates.
- Refer to organization group policies to disable Windows Update, if they are managed by your organization.

Advanced Sharing Settings

Advanced sharing settings need to be configured to allow server share creation. BackBox Data store is using network share to access NAS or other BackBox data path.

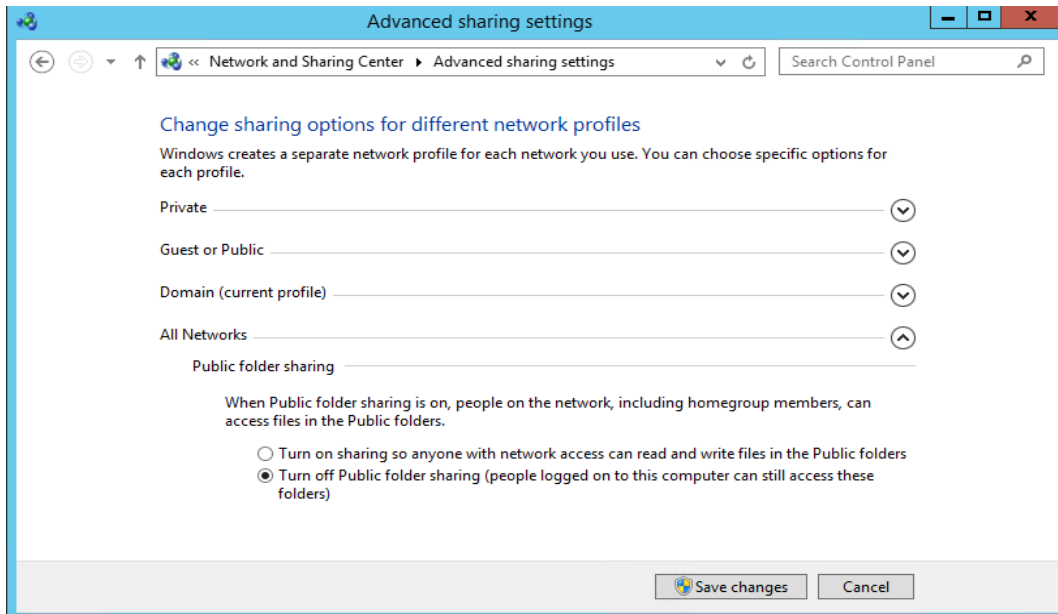
To configure the Advanced Sharing Settings:

- Press Start
- Select Control Panel
- Select Network and Internet
- Select Network and Sharing Center
- Select Change advanced sharing Settings

ATTENTION: If VTC server is part of a Workgroup, the Domain profile will not be shown. A new profile Domain will be added and will require to be set when the server joins the Active Directory.

	Private	Public	Domain	ALL Networks
--	---------	--------	--------	--------------

Network discovery	Turn off	Turn off	Turn off	n/a
File and printer sharing	Turn on	Turn on	Turn on	n/a
Public folder	n/a	n/a	n/a	Turn off



Firewall Settings

We recommend enabling ICMP incoming echo request (ping) for troubleshooting purposes or to allow monitoring tools to work properly. By default, ICMP incoming echo request (ping) firewall rules are defined, but disabled.

When the server gets the Files Server role installed with the Advanced sharing settings file and printer sharing turned on, ICMP incoming echo request firewall rules are automatically enabled. The server will answer to the ping request.

If the server has been prepared following the guidelines provided in this document, this setting is the recommended one.

In other cases, the rules can be manually activated by following these steps:

To manually activate ICMP incoming echo request (ping)

- Press **Start**
- Search for **Firewall and Network Protection**
- Go to **Advanced Settings**
- In the left pane and select the **Inbound Rules**
- Scroll down to **File and Printer Sharing (Echo Request)** and enable the rule for **Private**, **Public** rules and **Domain** rules if the VTC is under an **Active Directory**.



- Windows Defender Firewall with Advanced Security
 - Inbound Rules
 - Outbound Rules
 - Connection Security Rules
 - Monitoring

Name	Group	Profile	Enabled	Action
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domai...	Yes	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (SMB-QUIC-In)	File and Printer Sharing over...	All	No	Allow
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	All	No	Allow
iSCSI Service (TCP-In)	iSCSI Service	All	No	Allow
Key Management Service (TCP-In)	Key Management Service	All	No	Allow
mDNS (UDP-In)	mDNS	Public	Yes	Allow
mDNS (UDP-In)	mDNS	Private	Yes	Allow
mDNS (UDP-In)	mDNS	Domain	Yes	Allow
Message Queuing TCP Inbound	Message Queuing	All	Yes	Allow
Message Queuing UDP Inbound	Message Queuing	All	Yes	Allow
Microsoft Edge (mDNS-In)	Microsoft Edge	All	Yes	Allow
Microsoft Media Foundation Network Source IN [TC...	Microsoft Media Foundatio...	All	Yes	Allow
Microsoft Media Foundation Network Source IN [U...	Microsoft Media Foundatio...	All	Yes	Allow
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow

VTC Management Console

VTC Emulator (iSCSI)



These settings must not be changed before communicating with technical support.

When VTC Emulator (iSCSI) is selected, the available properties for the service are displayed on the screen in the right-hand side panel. There are no actions available when right-clicking on the VTC Emulator (iSCSI) setting node.

The screenshot shows the VTC Management Console interface. On the left, a tree view shows the 'Services' section expanded to 'VTC Emulator (iSCSI)'. The right-hand panel displays the 'VTC Emulator (iSCSI) Settings' with the following properties:

Common	
IP Port	8767

Diagnostic	
Device No Write	False
Enable LARGEBLOCKS Mode	True
Trace Level	0

At the bottom of the settings panel, there is a note for the 'Device No Write' property: "If true, the data is not written in the Data Store. ONLY FOR TEST PURPOSE: Works only for BACKUP and requires usage of UNLABELED volumes."

A window indicates read-only properties associated with the specified setting. When selected, any of the listed properties is shortly explained at the bottom of the window.

Any changes made to this page require restarting the services.

Domain Node

Add all Domain profile for each NonStop node be connected to the vBackBox.

The screenshot shows the VTC Management Console interface with the 'Domains' section expanded to 'ETISSL'. The right-hand panel displays the 'Domain ETISSL' settings:

- Log VT Controller messages on this Domain
- Guardian IP Port*: 4859
- Guardian IP Address(es)*: List of IP addresses including 192.168.20.63

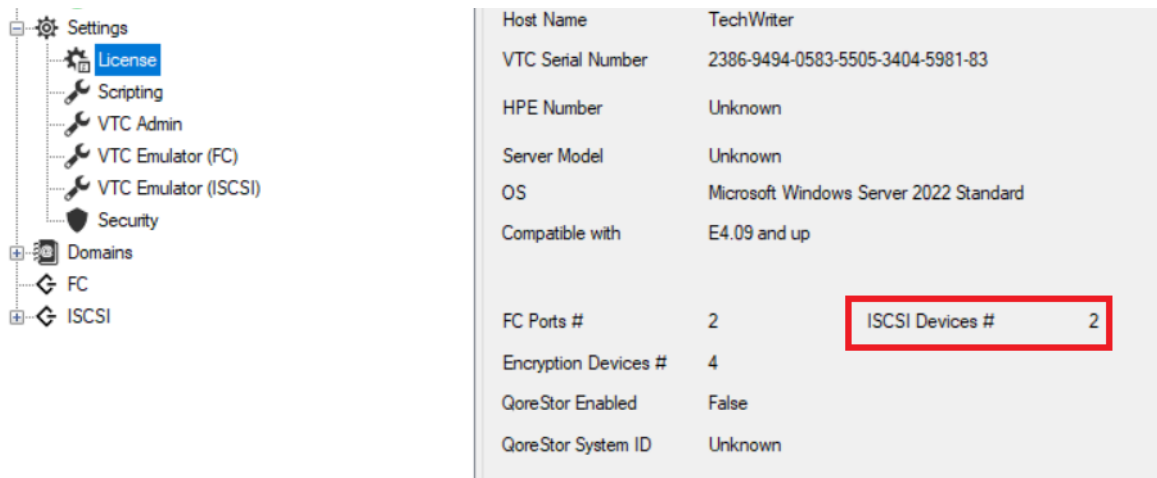
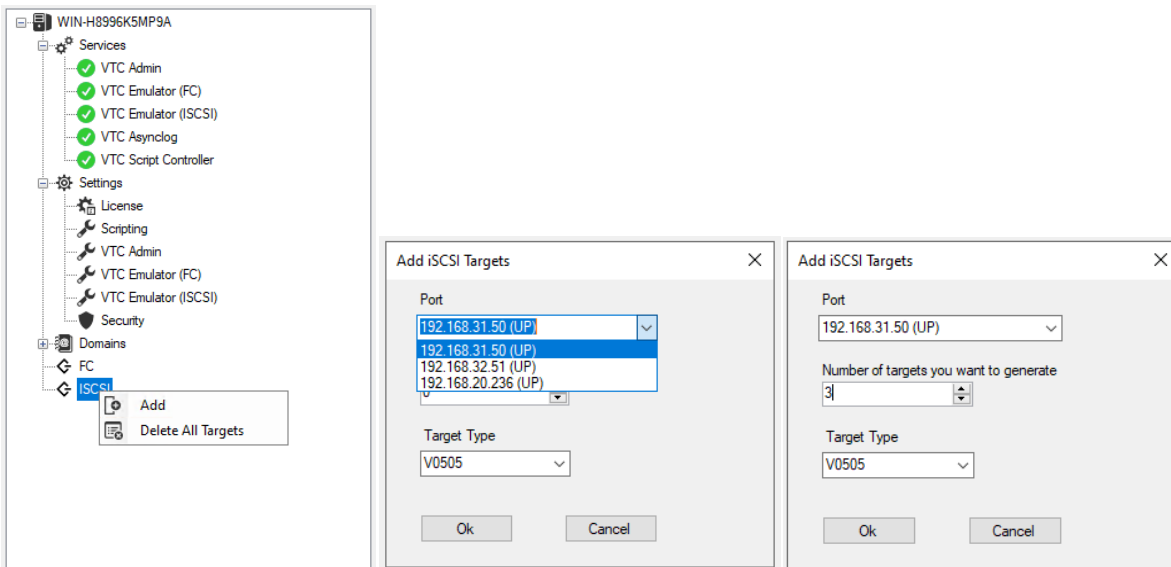
iSCSI Node

All VTC iSCSI configurations are grouped under the iSCSI category node. Changing any of the elements described below requires restarting services.

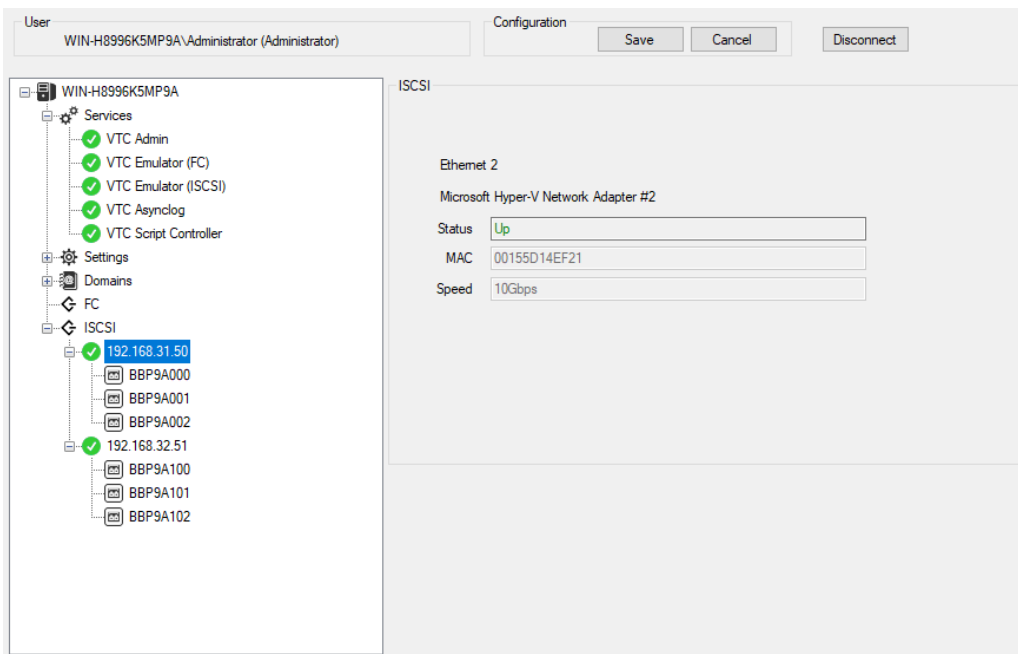
When the iSCSI category node is selected, no information is shown in the right-hand panel.

iSCSI Configuration

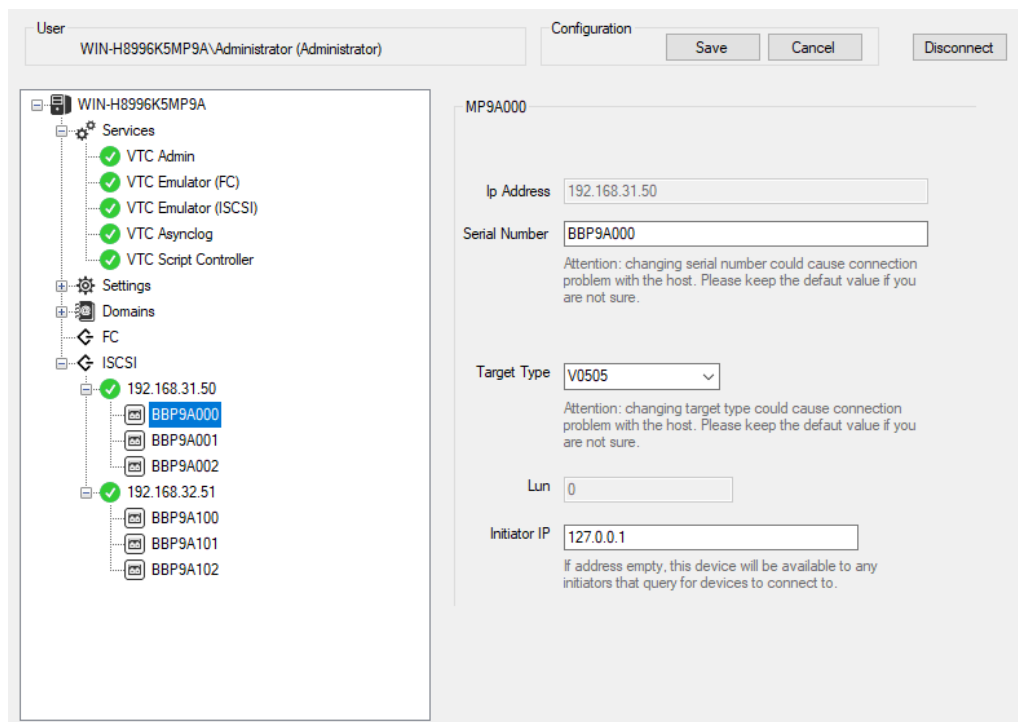
1. Configuration of the iSCSI is done through the VTC Management Console.
2. Add the NIC address to be used to connect with the Storage CLIM.
3. Provision virtual tape devices under the selected NIC address and several NIC addresses can be added. The virtual tape devices will need to be deployed across these NIC addresses.
4. Open the VTC Management Console and follow the procedure to add the iSCSI devices:
5. Right-click on the iSCSI node in the VTC Management Console and click Add to display the iSCSI device creation box.




6. In the pop-up window, first select a NIC address to be used for the Storage CLIM connection and choose the number of targets (up to maximum 12 devices per port) to be added with tape emulation type. If you have a limited number of targets licensed, you can either add them to the same storage CLIM or spread them across all ports. Click ok.
3. If you have multiple ports dedicated to different CLIM connection, the Add iSCSI Targets procedure needs to be redone for each port.
4. Once the targets are added, they will be shown under each IP address.



5. Select, one by one the targets and define its connection parameters. Changing the Serial Number and/or the target Type could cause connection errors.



- a. Serial Number is the target identifier and shouldn't be modified, as the connection is securely established with the host based on the serial number.
- b. Target Type is the emulation tape type to be used for the target (V0505, LT04, LT06 to LT08).
- c. Lun is assigned by default and cannot be changed, as it's used to provision virtual devices.
- d. Initiator IP links the selected target to a specific CLIM. Once linked, the iSCSI device will only answer to the discovery command from that specific storage CLIM. By default, new added device is assigned with a dummy value of 127.0.0.1 that must be changed with the CLIM storage IP address of the target device to be connected to. The new added device IP address can be left blank to answer to any CLIM storage.

	<p>If not updated and left with the default value (127.0.0.1), the target device will not answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD --addiscsitape.</p> <p>If updated to blank, the target device will answer to any CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD--addiscsitape.</p> <p>If updated to a specific CLIM address IP, the target device will only answer to that specific CLIM storage when attempting to adding iSCSI tape target devices by using the CLIMCMD --addiscsitape.</p>
--	--

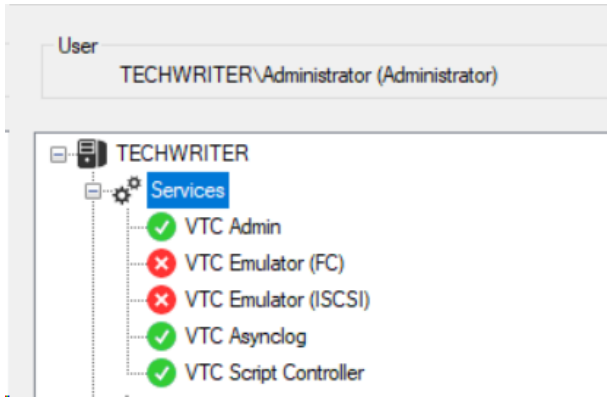
5. Save the configuration or Cancel it.



6. If you want to delete targets, select the target and right-click on it. Then Delete.



7. Once you have completed the change, restart VTC Services by right clicking on the Services node and selecting the Restart option.



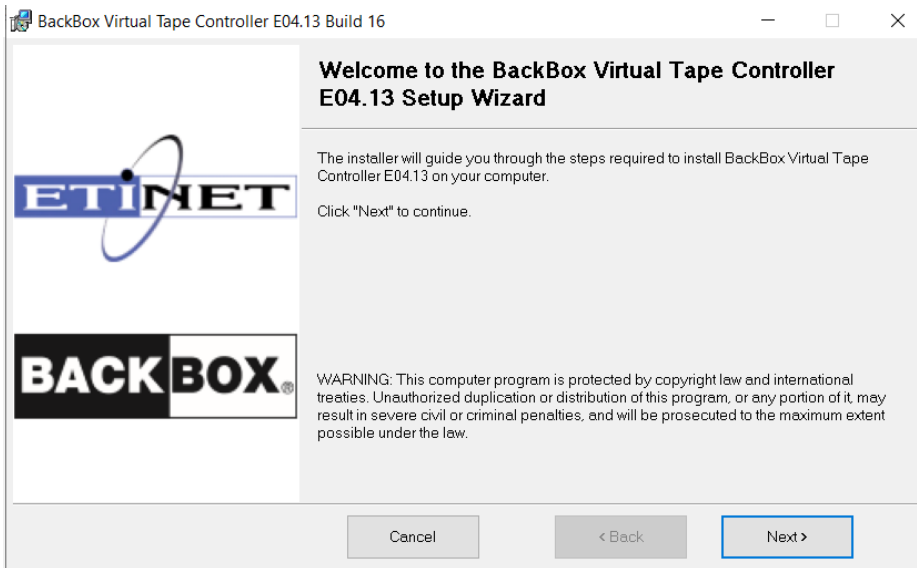
Install the Virtual Tape Controller Software

Requirements

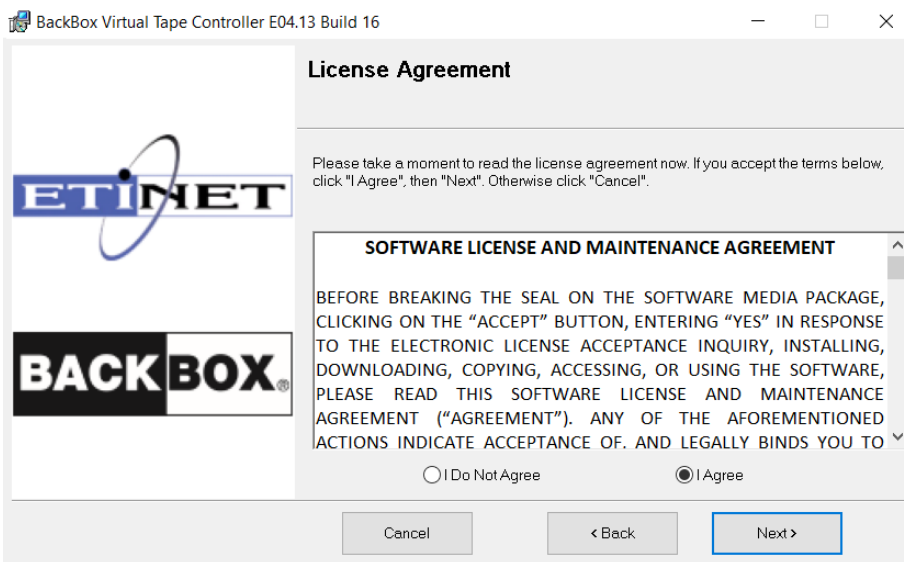
Administrator account under Windows on the server acting as the VTC

Description

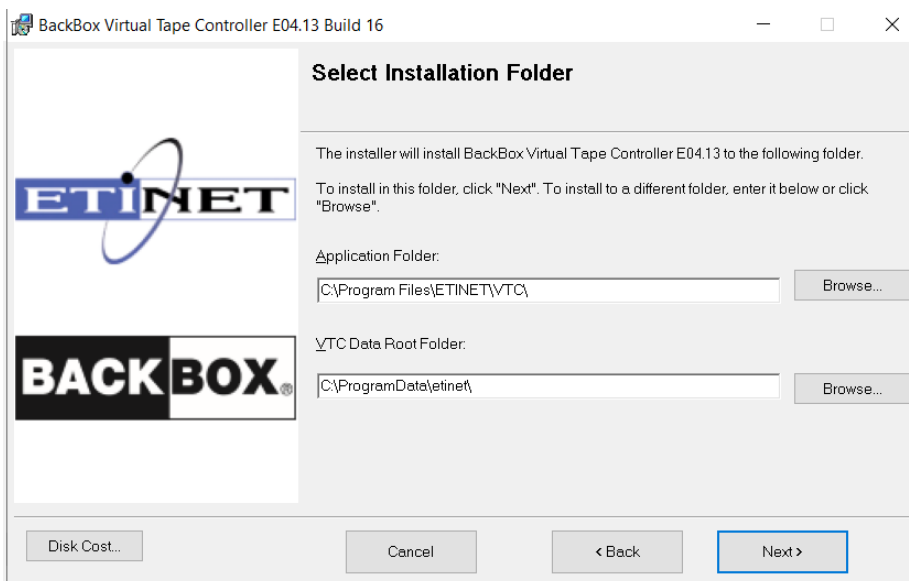
In the folder you uploaded the locate the VTC-E4.13 folder. Double-click on Setup.exe and follow the installer instructions.

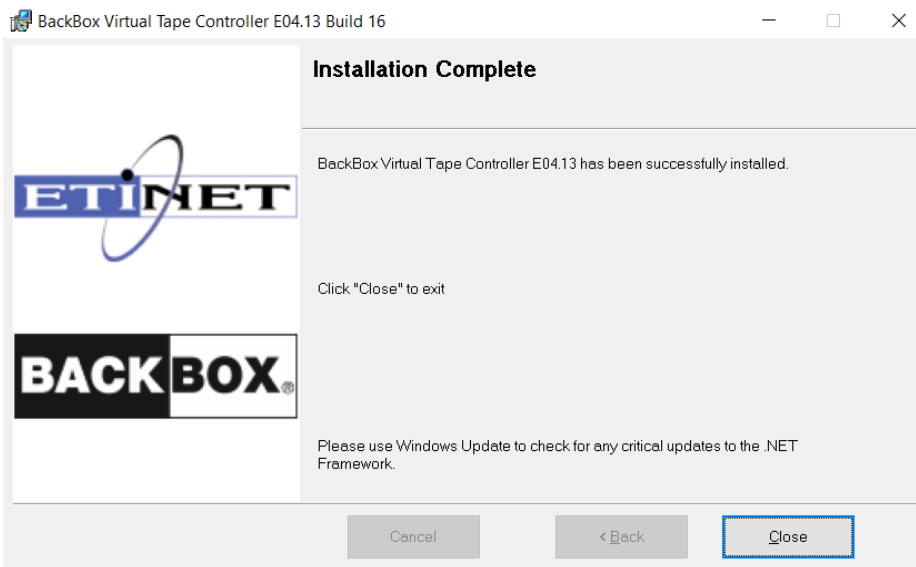
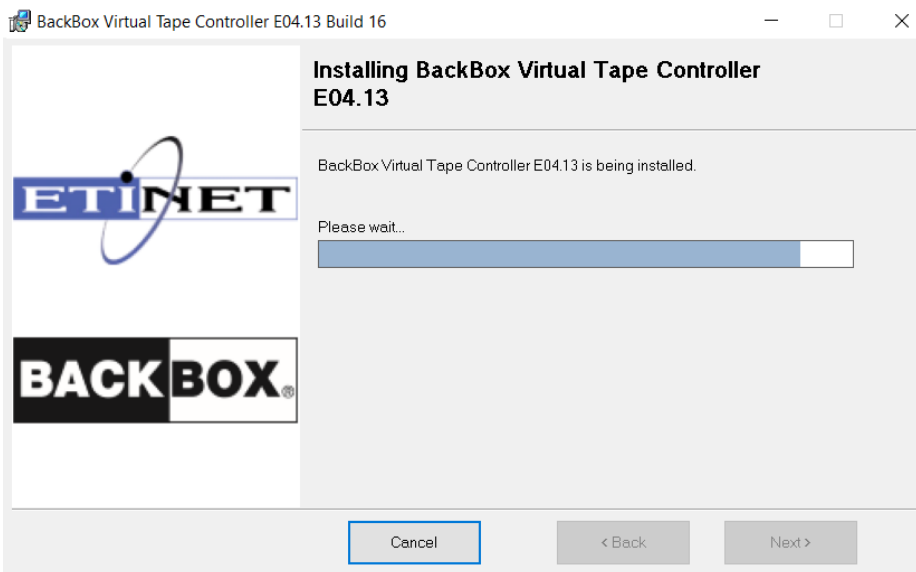
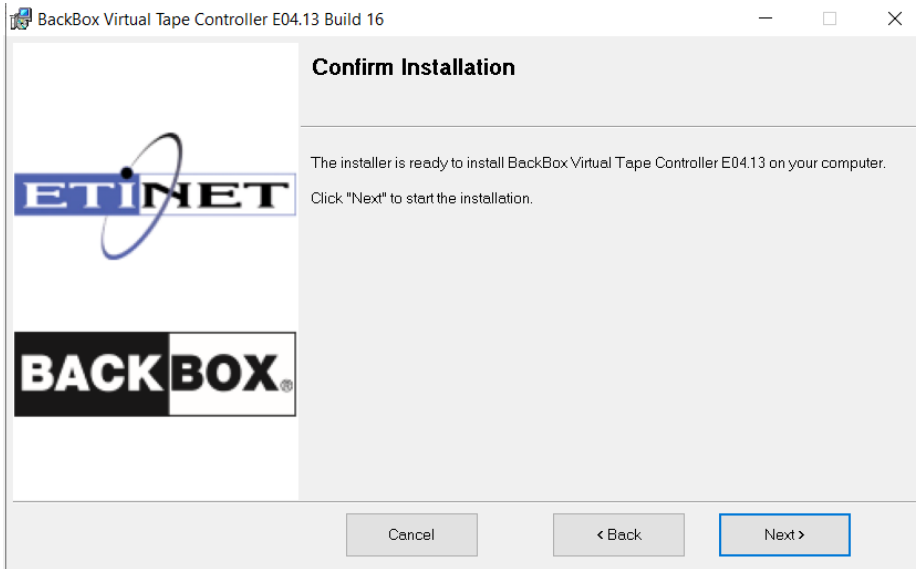



You will then be prompted to read and accept the license agreement. Click I Agree to proceed with the installation, a complete copy of the license agreement is available at the end of the present document.



Installation is now ready to start. Click the Next button to initiate the process.





 In case the VTC version comes with a patch, the patch is being installed along with the controller and is being mentioned between brackets.

Once the installation process is over, click the Close button. BackBox VTC software is installed, ready to be used.

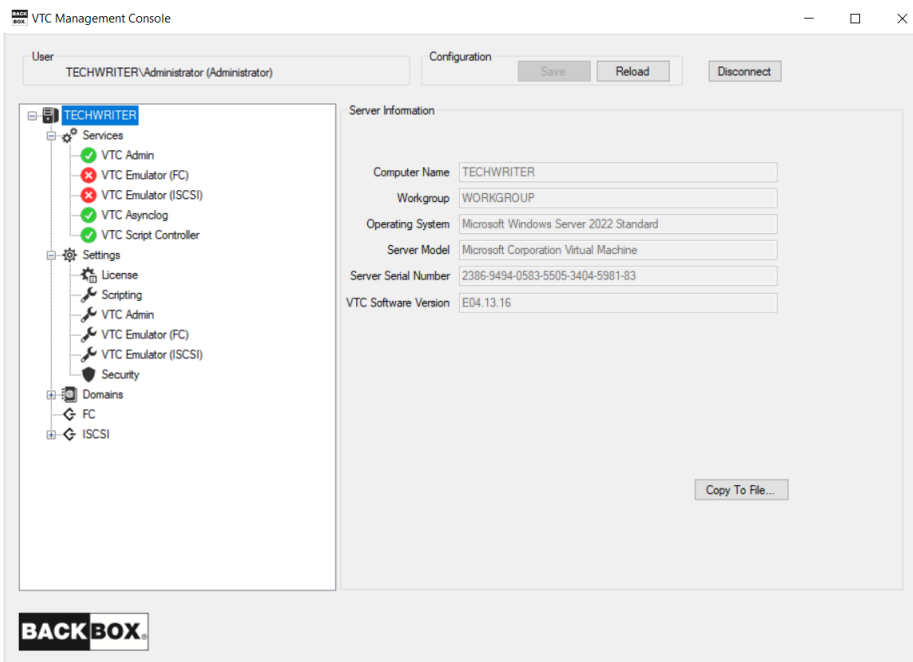
Host File

Edit the HOSTS file and map the server host name with all alias name to his loopback address. By doing so, you avoid bad DNS hostname resolution to local network resources, when one Ethernet adapter failed or it had network traffic down. This is a configuration requirement for cross-connected VTC pairs.

The host file is located in the system folder `Windows\System32\drivers\etc\`. For example, for a VTC with a server name BBOX1:

```
# localhost name resolution for BBOX1 handled within DNS to itself.  
127.1.1.1 localhost  
127.1.1.1 BBOX1.etinetlab BBOX1.backboxlocal BBOX1
```

License Request



For the license request, go to VTC MC > Server Information > Copy To File...

Use Copy to File ... button to save the server information in a .txt file. The file will be saved with the default name Server Information and default location Desktop. For support and reference purposes, location and name of the file can be changed at any time.

Request a vBackBox license through the License Desk, using the license information in the file.

Computer Name: TECHWRITER
 Workgroup: WORKGROUP
 Operating System: Microsoft Windows Server 2022 Standard
 Server Model: Microsoft Corporation Virtual Machine
 Server Serial Number: 2386-9494-0583-5505-3404-5981-83
 VTC Software Version: E04.13.16
 UUID: C351FC8E-6BA0-4CDD-BB1A-BE8BA197D1D5

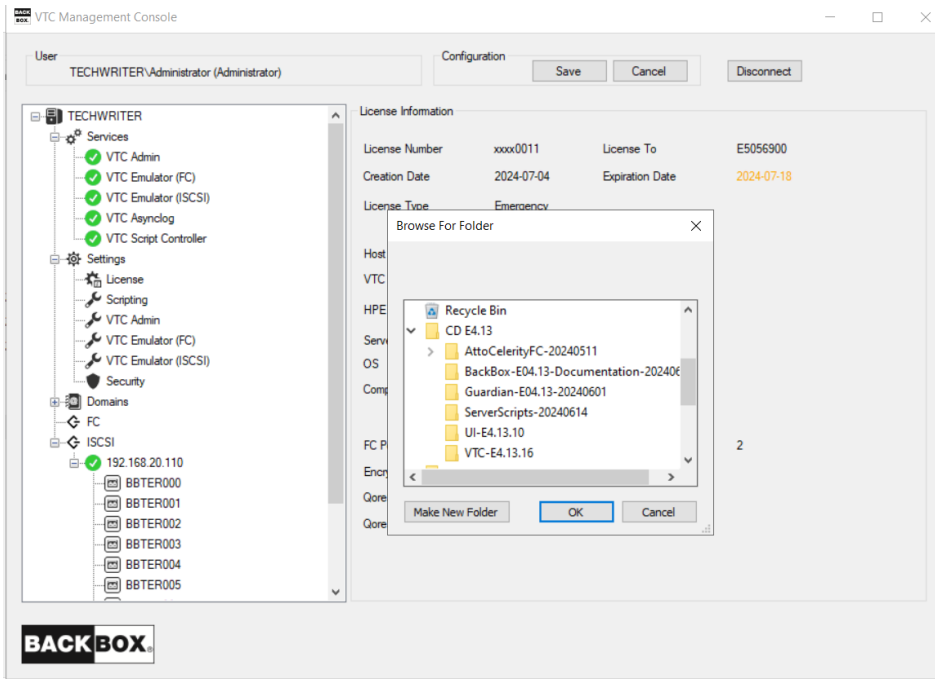
License Number: Unknown
 License Expiration : Unknown
 License Creation : Unknown
 License To: Unknown
 Serial Number: Unknown
 Hpe Number: Unknown
 License Type: Unknown
 Host Name: Unknown
 Release Version: Unknown
 Software Version: Unknown
 Product: Unknown
 Os Version: Unknown
 Number Of FC Ports : 0
 Number Of Encryption Devices: 0
 Number Of Iscsi Devices: 0
 Number Of Devices Per Port : 0
 QoreStor Enable: False
 QoreStor ID: Unknown

Once you receive the license file (XML format), upload it on the vBackBox and import it. Go to VTC MC, right-click on the License node under Setting and Import.

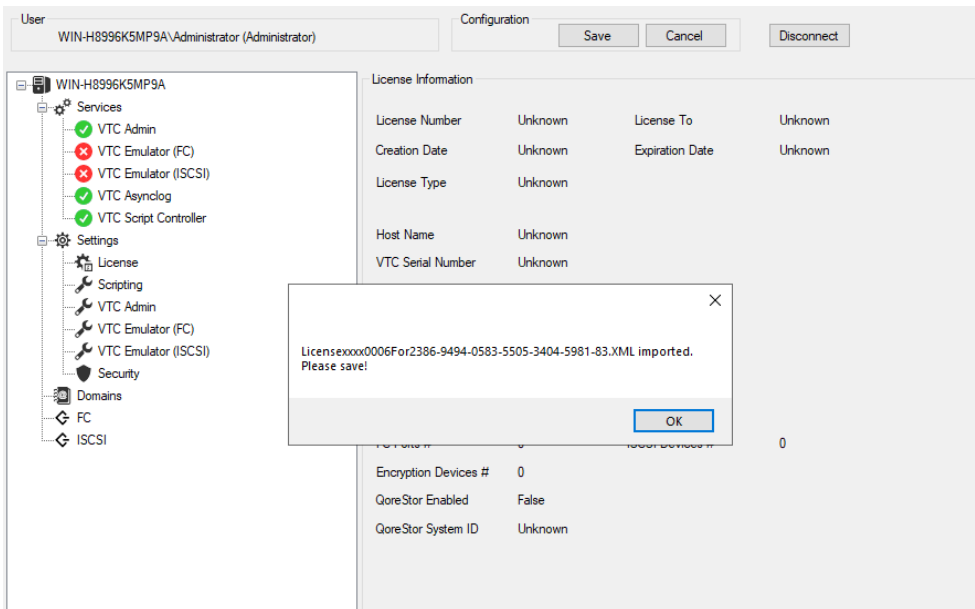
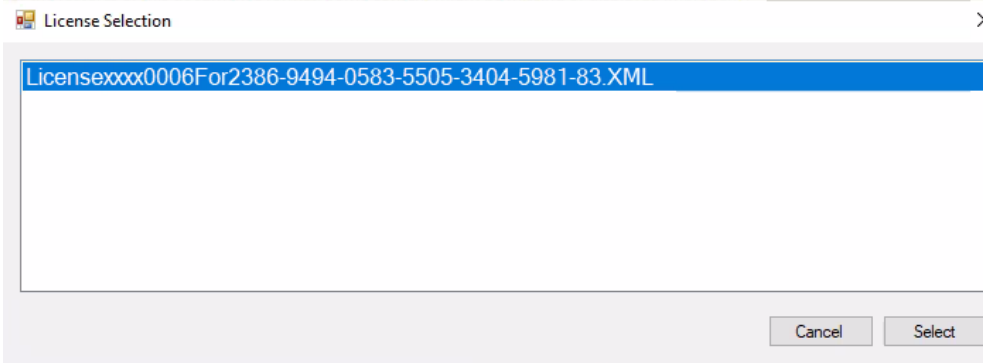
The screenshot shows the vBackBox configuration interface. The top bar displays the user 'WIN-H8996K5MP9A\Administrator (Administrator)' and configuration buttons: 'Save', 'Reload', and 'Disconnect'. The left sidebar shows a tree view of system settings, with 'Settings' expanded and 'License' selected. The main panel displays 'License Information' with the following data:

Field	Value	Field	Value
License Number	Unknown	License To	Unknown
Creation Date	Unknown	Expiration Date	Unknown
License Type	Unknown		
Host Name	Unknown		
VTC Serial Number	Unknown		
HPE Number	Unknown		
Server Model	Unknown		
OS	Unknown		
Compatible with	Unknown		
FC Ports #	0	ISCSI Devices #	0
Encryption Devices #	0		
QoreStor Enabled	False		
QoreStor System ID	Unknown		

In the pop-up window, browse for the folder the license file has been copied to and click the OK button. In this example the license file has been copied on the Desktop.

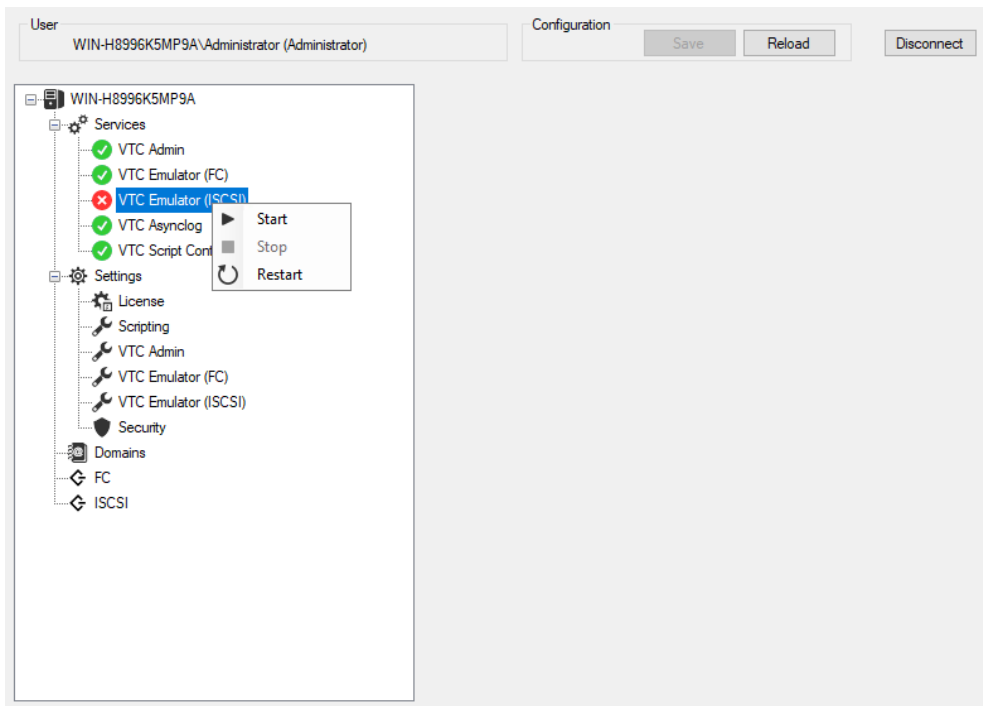


In the License Selection dialog select the license XML file. Click Select and then Save the configuration.



Start Services

Starting the services finishes the installation of the vBackBox VTC and it makes the system ready for configuration. Validate that all services listed under the Services node are started – marked with a green checkmark. An **X** icon will be shown in front of the service name, if the service has been stopped.



Connect Virtual Tape Device to Virtual NonStop System

Virtual tape devices are connected to a virtual NonStop system through the storage CLIM. The CLIMs provisions the network adapter accessible on the corporate LAN (different from the vNonStop maintenance LAN).

The following new commands are available to add and remove iSCSI tape target devices on a CLIM:

<p>-t or --addiscsitape</p>	<p><iscsi target ip address> Initiates a discovery request to an iSCSI target at the input IP address. Then it logs in to all new targets. The <code>addiscsitape</code> command is only applicable to virtual CLIMs.</p>
<p>--deliscsitape</p>	<p><iscsi target name> Initiates a logoff request to an iSCSI target at the input iSCSI target name and deletes the target from the database. The <code>deleteiscsitape</code> command is only applicable to virtual CLIMs.</p>

Adding and deleting iSCSI tape devices can be done using the `lunmgr` utility of a `climcmd`. A basic add command would look like this:

```
climcmd SCLIM000 lunmgr -t 192.168.30.20
```

This command would be adding all virtual iSCSI tape devices on the vBackBox located at the IP address **192.168.30.20**.

Install BackBox UI Client

To install the BackBoxUI Client:

1. Open the BackBox distribution set and navigate to the UI-v.vv.vvvvv directory.
2. Run Setup.exe.
3. Launch the UI Client Setup Wizard and follow the steps required to install the application. Click Next.
4. Select the installation folder. Use the default folder or browse to install the UI Client to a different folder. If the access to the UI Client must be restricted to the current user, select **Just me**.

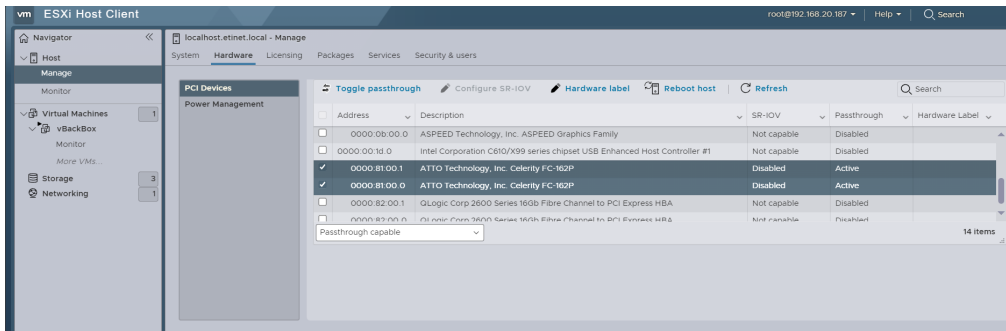


It is highly recommended to use no restriction. Choose Everyone to install the UI Client for anyone who may use this computer, especially when installing on a VTC.

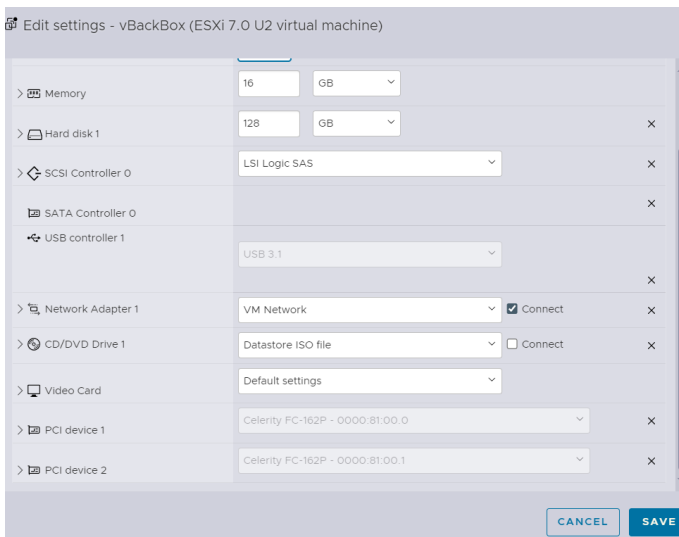
5. Follow the Wizard installation steps.
6. Once the installation is complete, close the Wizard and use BackBox User Interface to connect to each Domain configured.

Atto HBA Target Mode in VMWare ESXi Passthrough Mode

- Install the physical Atto HBA into the ESXi hypervisor server.
- In the ESXi client, find Atto HBA port and activate the Passthrough mode



- Assign Atto port in the vBackBox VM setting. The VM needs to be shut down. In the setting editor add a new PCI device.



- Start the VM. The new ATTO devices are displayed in Device Manager. Install the drivers from the distribution package provided (AttoCelerityFC-yyyymmdd) and resume the server preparation script (VTCTServerPreparation.ps1).

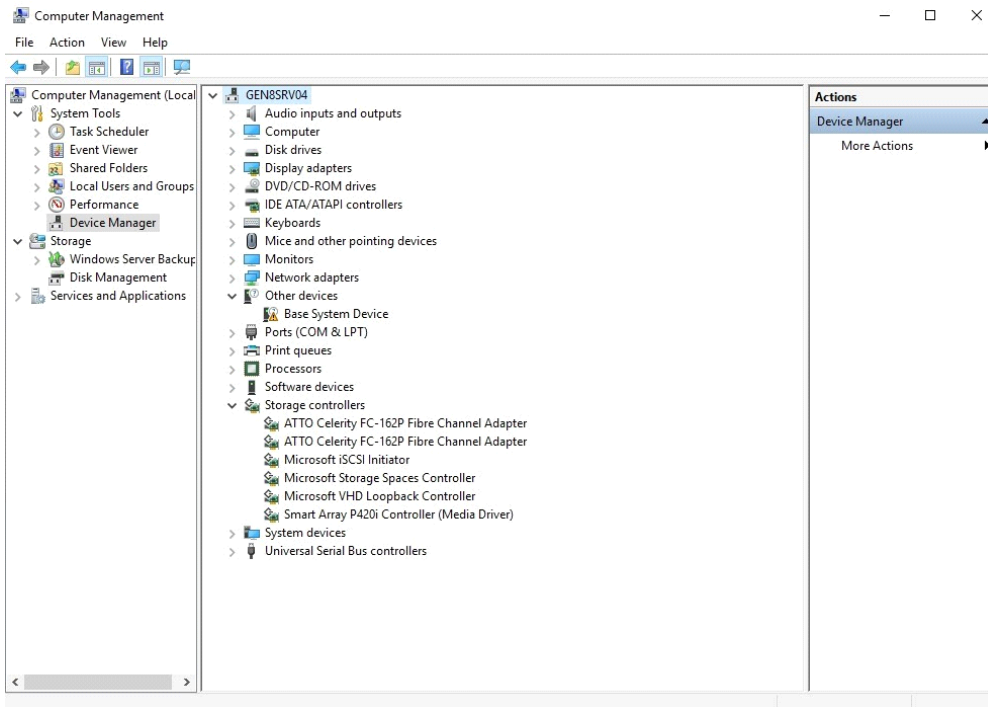
Install the FC Adapter Driver

Reach the appropriate installer at the location indicated in the software requirement table and double-click on Setup.exe. Follow the instructions in the installer.

Although we recommend using the latest release of the available driver, ATTO does not usually sign all their releases.

If it's mandatory to have a signed driver, they are provided in the package, under the folder marked has signed (ex: FC8\win_drv_celerity8\1.95-Signed).

In Device Manager, verify that all FC adapters have been correctly installed.



Install the FC Configuration Tool

Perform this sub-task only if there is no ATTO Configuration Tool already installed or if the currently installed version is an older one.

Access the repository folder and navigate to AttoCelerityFC-20191101 directory, sub directory Tools\win_app_configtool_438.

Double-click on ConfigTool_438.exe and follow the installer's instructions. You should accept all default settings and choose Full installation if the previous version of ATTO configuration tool has been already installed.

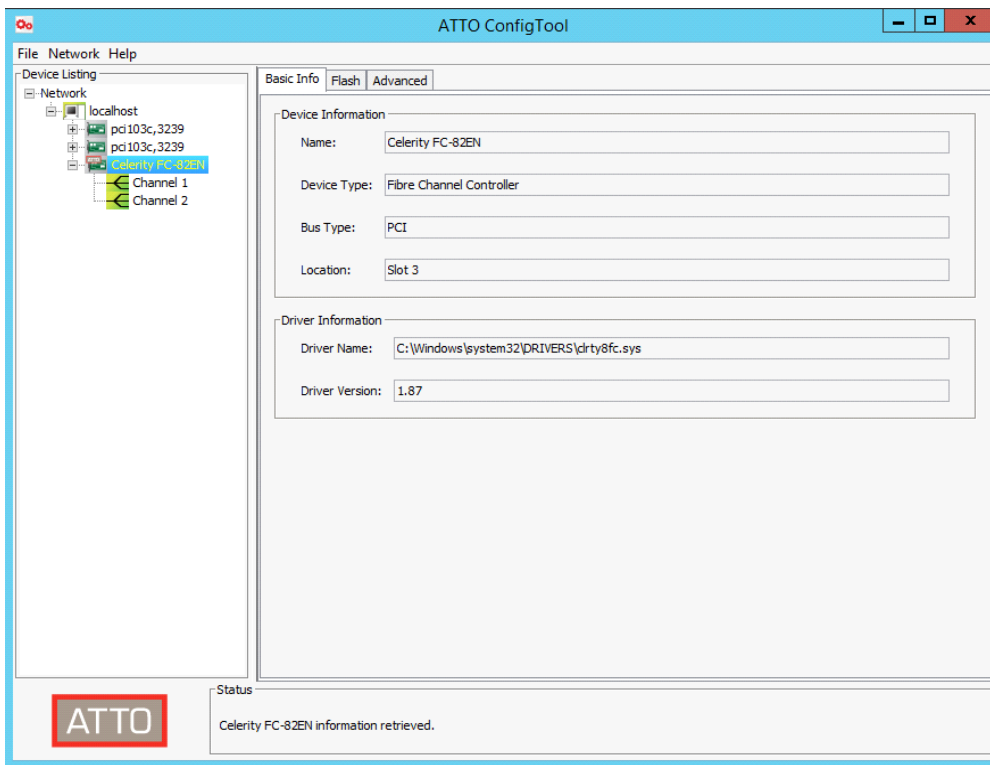
You may be prompted to uninstall the old version first.

Validate FC Card Channel Parameters

Start the ATTO ConfigTool (from the Windows>Start menu > All Programs > ATTO ConfigTool.) After it opens, login in as user with local administrator privileges. To log in, expand **local host node** in the left panel.

Once logged in, expand the localhost node in the left panel. For each Celerity Device listed perform the following operations:

1. In the Basic Info tab, check if the Driver Version id is matching the driver version that you just installed. If not, you will need to re-install the Celerity driver.



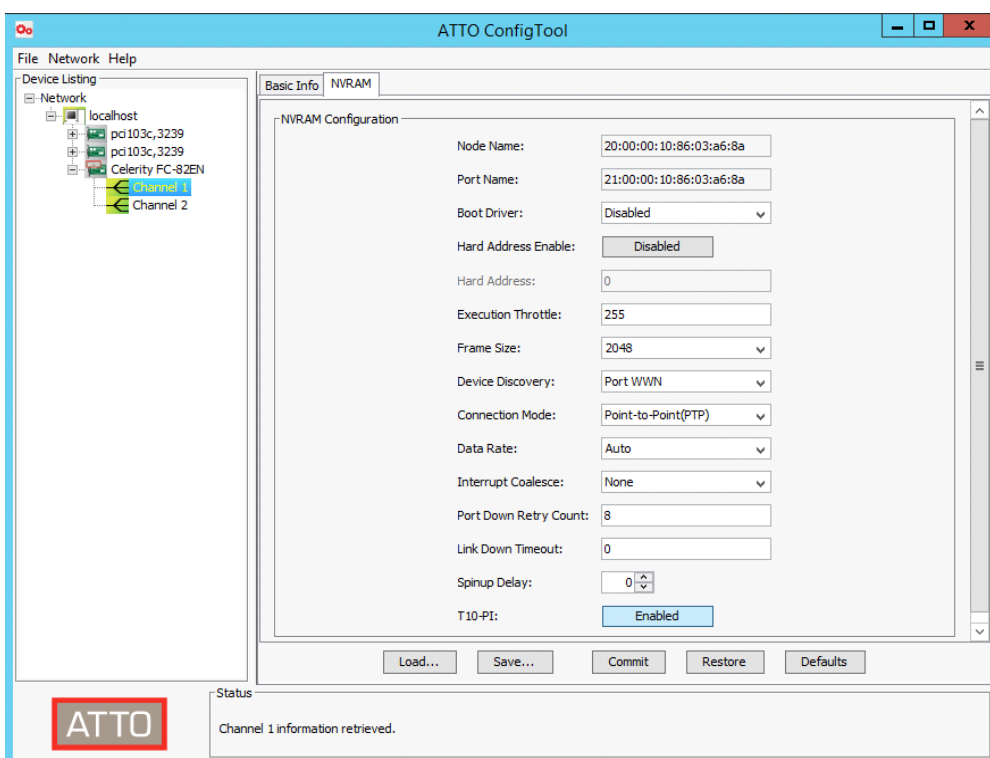
2. Expand the current Celerity Device node in the left panel.

For each listed channel, verify if the default values match the ones shown in the NVRAM tab. Update all mismatched fields.

The parameter(s) that may require changing is the Connection Mode. Make sure is set to "Point-to-Point".

3. When all ports have been verified and changed (if necessary), press the Commit button. Wait for the commit confirmation status message before continuing (see below Commit confirmation page). You have to press the Commit button for each channel being updated.

Complete all parameters changes and Flash updates before restarting the server.



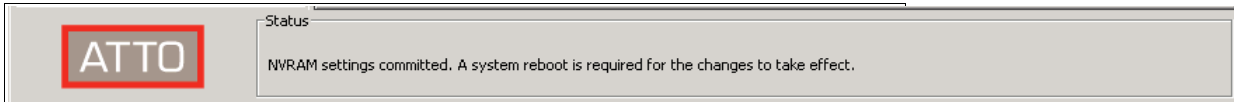


If a FC switch needs to be used to share a single NonStop FC port with multiple VTC FC ports, the following additional settings may be required:

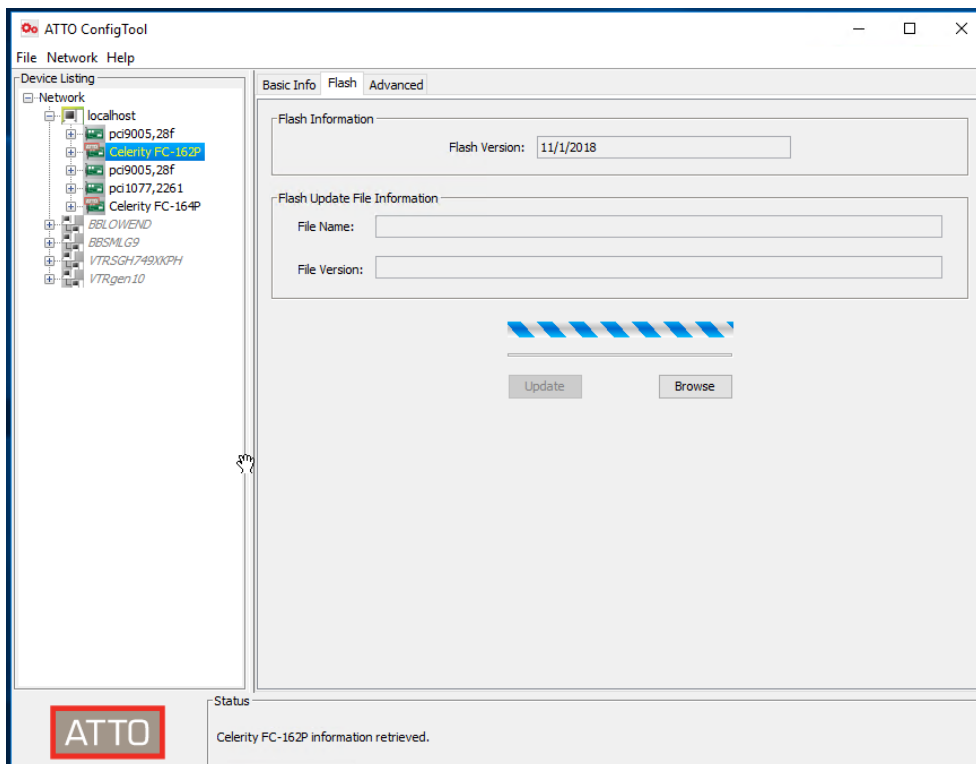
4. Configure a FC switch zone and customize switch setting.

Each switch and environment may require different settings. Contact [ETI-NET Support](#) for assistance.

Update FC Adapter Flash Version



This step is required only if the Flash version is older than 4/6/2018 (FC-8xEN and FC-16xP models).



To update the Flash version, press the **Browse** button, then navigate up to the repository folder **AttoCelerityFC-20191101 \FC8** or **\FC16** directory and select the **Flash Bundle** file suggested by the Configuration Tool.

To complete the selection, press the **Open** button. Review the selected **Flash Bundle** file information and start the process by pressing the **Update** button.

Wait for the Flash completion status message before proceeding to any other activity.

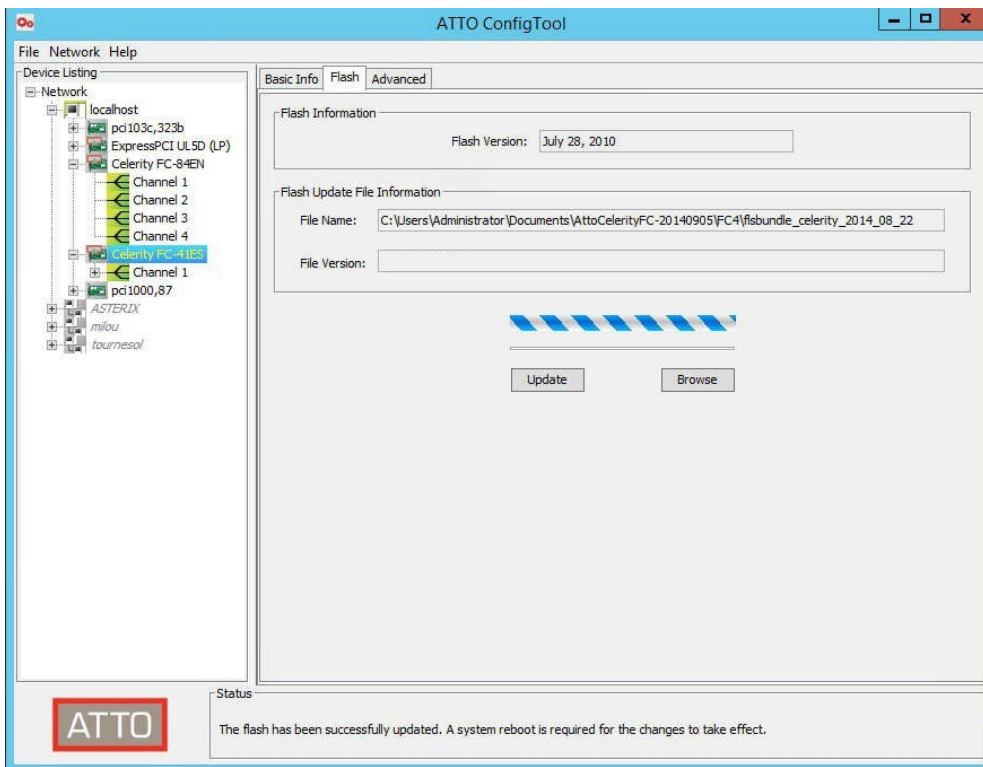
Complete all other celerity device Flash updates.



Do not power off! The server operation will be interrupted before Flash update report completion. Powering off could damage the FC card being updated.



You can complete all the changes to parameters, Flash updates and Target mode settings (as described above) before restarting the server. It is not necessary to restart multiple times.



Continue with PowerShell Execution Policy.

Appendix

Disaster Recovery Scenario when DataStore Type is QoreStor

Use the information in this Appendix to set up the environment for NonStop recovery purposes, in case the main system (local NonStop node) crashes and data needs to be recovered right away from a secondary system (DR NonStop node).

NonStop Systems:

- Primary [local NonStop node]
- Secondary [DR NonStop node]

Setup

1. Setup two systems:
 - VTC1 Primary [local NonStop node] with QoreStor Replication
 - VTC2 Secondary [DR NonStop node] with Win-Store



2. Configure Data Store[QoreStor] with QoreStor Replication in system VTC1 Primary [local NonStop node]

The screenshot shows the configuration page for 'VTC1 [INSIDX]' in a web-based management console. The page is divided into several sections:

- Data Store Information:** Shows 'Data Store ID*' as 'QS-CATSYNC-PRI', 'Data Store Type' as 'QoreStor', 'Status' as 'Active', and 'Domain Access to Data Store' as 'Primary'. A blue arrow points to the 'Data Store Type' dropdown.
- QoreStor Details:** Includes fields for 'User Account', 'Password', 'Confirm Password', 'Disk Space Warning Threshold (%)' (set to 50), and checkboxes for 'Check Volume Timestamp', 'Storage Optimization' (set to 'RapidCIFS'), 'Archive bit support', 'QoreStor Policies', 'Encryption at rest', 'Use QoreStor Replication' (checked), and 'Use QoreStor Cloud Tier'. A blue arrow points to the 'Use QoreStor Replication' checkbox.
- Catalog Sync Export Configuration:** A separate box containing 'Full Export Frequency' (0 Days), 'Export Check Delay' (0 Minutes), 'Export Report Location' ('\$S:\$INS_EXP'), 'Export Destination' ('\\ETINIUM.\$CATALIS.INSEXP'), 'Process Priority' (0), and 'Include DSM/TC Disk File Entries' (checked).
- Path*:** A text field containing the path '\\BBQS47REPLIC.ETINET.LOCAL\CRYPREPLICATA_BBQS47\UPE411\QS-CATSYNC-PRI\'. A blue arrow points to this field.
- VT Controller ID*:** A dropdown menu showing 'TOUTATUS'.
- QoreStor Pool:** A table with columns 'Storage Pool', 'Spare Pool', and 'Copy Pool'. The 'Copy Pool' is selected.
- QoreStor Storage Route Table:**

Path	Rank	Reserved for
\\BBQS47.ETINET.LOCAL\CRYP2REPLICATE\UPE411\QS-CATSYNC-PRI\	1	ANY

3. Set up Data Store [Windows File] in VTC2 Secondary [DR NonStop node].

VTC 2 [ETINIUM]

Data Store Information

Data Store ID*: QS-CATSYNC-SEC
 Data Store Type: Windows File
 Status: Active
 Domain Access to Data Store: Secondary
 Primary Data Store Id: QS-CATSYNC-PRI

Windows Details

User Account: BackBox
 Password: *****
 Confirm Password: *****
 Disk Space Warning Threshold (%): 90
 Check Volume Timestamp:
 Storage Optimization: RapidCIFS
 Archive bit support:

Catalog Sync Import Configuration

Import Source: \etinium.\$data15.insexp
 Import Report Location: \$\$.insexp
 Process Priority: 0
 Max Number of DISKFILE's per TMF Transaction: 20000
 Import to the secondary system which is different from the primary system but shares the same node name as the primary system.
 Allow to store replicated DSM/TC entries in a local DSM/TC catalogue that is not dedicated to this replication (i.e. merged with other replications or with local backups).

Nodes Replacement

You might want to change the node in the name of the backed-up DISKFILES cataloged in DSM/TC. Please consult the BackBox Catalog Sync Option Manual before configuring the modification of the DISKFILE name in DSM/TC

Original Node Name	New Node Name
UNSIDX	ETINIUM

Windows Pool

Storage Pool	Spare Pool	Copy Pool
Path*	Rank*	Reserved For
\\BBQS47REPLIC.ETINET.LOCAL\CRYPREPLICATA_BBQS47\UPE4111\QS-CATSYNC-PRI\	1	ANY

The Storage Optimization = RapidCIFS
Storage Pool path for [SECONDARY] = Copy Pool path of QoreStor for [PRIMARY]

QS-CATSYNC-PRI Administration **VTC1** Data Store QS-CATSYNC-PRI

Storage Route: First Available VTC Reply from: TOUTATUS Refresh

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare	960,646.67	8	1,064.23	8	1/18/2024 8:00:11 PM
Copy	1,045,917.23	8	1,064.23		1/18/2024 8:00:11 PM

Detail Report By: Path Volume Group Jobs

Pool	Volume SerialNumber	Disk Space	Disk Free Space	Path	Rank	Number of Files	User Data Size(MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)	Last Update	Path Status
Storage	3492060827	1 TB	945.94 GB 92.38 %	\\BBQS47.ETINET.LOCAL\CRYPREPLICATE\UPE4111\QS-CATSYNC-PRI\	1	8	1,064.23	8	1,064.23	1/18/2024 8:00:11 PM	Good
Copy	4209779393	1 TB	1,021.4 GB 99.75 %	\\BBQS47REPLIC.ETINET.LOCAL\CRYPREPLICATA_BBQS47\UPE4111\QS-CATSYNC-PRI\	0	0	1,064.23			1/18/2024 8:00:11 PM	Good

QS-CATSYNC-SEC Administration **VTC2** Data Store QS-CATSYNC-SEC

Storage Route: First Available VTC Reply from: GENSSRV04 Refresh

Pool	Free Space(MB)	Number Of Files	User Data Size(MB)	Non-Backed-Up Files	Last Update
Storage - Spare	1,045,917.23	8	1,064.23	8	1/18/2024 8:00:11 PM
Copy		0			

Detail Report By: Path Volume Group Jobs

Pool	Volume SerialNumber	Disk Space	Disk Free Space	Path	Rank	Number of Files	User Data Size(MB)	Number of Non-Backed-Up Files	Size of Non-Backed-Up Files(MB)	Last Update	Path Status
Storage	4209779393	1 TB	1,021.4 GB 99.75 %	\\BBQS47REPLIC.ETINET.LOCAL\CRYPREPLICATA_BBQS47\UPE4111\QS-CATSYNC-PRI\	1	8	1,064.23	8	1,064.23	1/18/2024 8:00:11 PM	Good

Copyright ETI-NET, 2003-2024

4. Check the export/import results.

```

UPE4111-BB051 - Catsync Export/Import process \INSIDX.S25V3 2024-01-23 21:39
UPE4111-W3162 Domain license will expire on 2024-01-30.
Data store : QS-CATSYNC-PRI
Process type : EXPORT FULL catalogs
DSM/TC disk files : included
Export id : 2024-01-23_21:39:01
Export destination : \ETINIUM.$DATA15.INSEXP

Volume Group Catalog status
-----
CATPR1 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=4
CATPR2 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=5
CATPR3 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=6
CATPR4 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=7
CATPR5 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=8
CATPR6 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=9
CATPR7 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=1
CATPR8 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=2
CATPR9 VG-QS-CATSYNC-PRI ASSIGNED QSCATA, gen=3

Volume group NSK primary catalog (pool name) Number of Nbr DSM/TC
----- Most recently written volume volumes disk files
-----
VG-QS-CATSYNC-PRI DSM/TC volcat \INSIDX.YINGTEST_VOLCAT, pool QS_CATSYNC_PRI
CATPR6 unloaded on 2024-01-23 21:37:14 9 0

UPE4111-I3279 \INSIDX.S25V3 exported FULL catalogs for data store
QS-CATSYNC-PRI (9 volumes processed). Report in $$.INS.EXP
UPE4111-BB051 Process \INSIDX.S25V3 ended on 2024-01-23 21:39
SETINET YINGQC 18>
  
```

5. For full or Update Export/Import and manual preparation of BBDBM, follow the procedure in the BackBox Catalog Sync Option document.



For more details regarding Catalog Sync customized environments and settings, contact [ETI-NET Support](#).