



NetApp Global File Cache 2.2.0

User Guide

Important: If you are using Cloud Manager to enable Global File Cache, you should use <https://docs.netapp.com/us-en/cloud-manager-file-cache/concept-gfc.html> for a step-by-step walkthrough.

Cloud Manager automatically provisions the GFC Management Server instance alongside the GFC Core instance and enables entitlement / licensing.

You can still use this guide as a reference. Chapter 7 through 13 contains in-depth information and advanced configuration parameters for GFC Core and GFC Edge instances.

Additionally, this document includes overall onboarding and application best practices.

TABLE OF CONTENTS

1	Introduction	7
1.1	The GFC Fabric: Highly Scalable and Flexible	7
1.2	Next Generation Software-Defined Storage.....	7
1.3	Global File Cache Software	7
1.4	Enabling Global File Cache using NetApp Cloud Manager.....	7
2	NetApp Global File Cache Requirements	8
2.1	Hardened Server Appliance	8
2.2	Physical Hardware Requirements.....	8
2.3	Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)	8
2.4	Cloud Deployments (such as Microsoft Azure, Google Cloud Platform or Amazon AWS).....	9
2.5	Operating System/Software Requirements	9
2.6	Backend File Server Requirements	10
2.7	Datatype requirements.....	10
2.8	Amazon FSx for ONTAP system requirements.....	10
2.9	Partition Sizing Requirements.....	11
2.10	GFC Intelligent File Cache Disk Requirements (D:\).....	12
2.11	Networking Requirements.....	12
2.12	Client Workstation Settings	13
2.13	NetApp Support Policy	14
2.14	Firewall and Antivirus Best Practices	15
3	Getting Started with NetApp Global File Cache	17
3.1	Example: Deployment Summary.....	17
3.2	Example: Centralized Data Store in the On prem, hybrid or public cloud	18
3.3	GFC Fabric	19
3.4	Sizing Guidelines	19
4	Deploying NetApp Global File Cache Virtual Template and Software Package	21
4.1	Before You Begin.....	21
4.2	Deploying the GFC Virtual Template	21
4.3	Network Configuration	22
4.4	Active Directory Configuration.....	24
4.5	Software Installation Package (Update)	26
5	Licensing	32
5.1	How It Works.....	32

5.2	Subscription Updates	32
5.3	Caching.....	32
5.4	Requirements.....	32
5.5	Deploying GFC LMS instance.....	33
6	Initial Configuration	40
6.1	Initial Configuration Wizard	40
6.2	Global File Cache Configuration Console	41
7	Designing and Deploying NetApp Global File Cache Core	44
7.1	GFC Core Stand-Alone Instance	44
7.2	GFC Core Load Distributed Design	44
7.3	Configuring GFC Core instance – Service Account	45
7.4	Configuring GFC Core instance – Backend File Servers	46
7.5	GFC Core Advanced Features.....	47
7.6	Global Exclusion List.....	47
7.7	Server Exclusion List	47
7.8	Remote Inclusion List.....	48
7.9	Selectable File Handling	49
7.10	Pre-population (legacy).....	50
7.11	Core Advanced Options	51
8	Designing and Deploying NetApp Global File Cache Edge	53
8.1	GFC stand-alone instance	53
8.2	GFC Edge Multi-Edge Deployment.....	53
8.3	Configuring the GFC Edge Role	58
8.4	GFC Edge Advanced Features.....	59
9	Deploying Cloud Volumes Edge Cache (CVEC)	65
9.1	Deploy and configuration of BlueXP	65
9.2	CVEC Configuration on GCP	67
9.3	CVEC Configuration on Azure	77
10	Designing and Deploying Policy Configuration	90
10.1	To Configure and Schedule a Pre-Population Job.....	91
10.2	To delete a scheduled Pre-Population Job	93
10.3	To edit a scheduled Pre-Population Job	94
10.4	To delete all scheduled jobs.....	95
10.5	To refresh the pre-population job list.....	96

11 DFS Namespace Integration	97
11.1 DFS Design.....	97
11.2 Site Definitions and Site Links.....	97
11.3 DFS Root Configuration Default.....	99
11.4 Site Costing Configuration	102
11.5 GFC Global Exclusion Configuration (DFS).....	103
12 NetApp Cloud Insights	105
12.1 Prerequisite.....	105
12.2 Cloud Insights API Token generation.....	105
12.3 Cloud Insights Configuration	107
12.4 Dashboards.....	108
12.4.1 Importing GFC Dashboards into CI	108
12.4.2 GFC Node Monitoring Dashboard	109
12.4.3 GFC Licensing Dashboard	110
12.4.4 GFC Core Monitoring Dashboard	111
12.4.5 GFC Edge Monitoring Dashboard	112
12.5 Alerts.....	113
12.6 Monitoring	114
12.6.1 GFC Core TService Monitor	114
12.6.2 GFC Edge TService Monitor.....	114
12.6.3 GFC Tum CPU Usage Monitor	115
12.6.4 Tum Memory Usage Monitor	115
12.6.5 GFC Edge Disconnection from Core Monitor	116
13 Client Application Requirements	117
13.1 Autodesk - Revit.....	117
13.2 Revit Requirements Summary	119
13.3 Autodesk – AutoCAD Requirements.....	120
13.4 Bentley – MicroStation Requirements.....	123
13.5 Adobe Creative Suite Requirements.....	125
14 End User Training.....	127
Accessing Project Folders and Files.....	127
Cold Files Versus Warm Files	127
Do's and Don'ts	127
Application-Specific Best Practices	128
15 Contact Details.....	128

Appendix A: Antivirus Application Suites.....	129
McAfee VirusScan	129
McAfee VirusScan - Central Management Console	137
Symantec Endpoint Protection 12.x.....	140
Sophos Endpoint Security and Control v10.x	147
Trend Micro Officescan	152
Kaspersky Endpoint Security Cloud	155
Windows Defender	157
Tanium	160
Cisco AMP.....	171
Appendix B: Disable VMware ESX(i) Hot Plug Capability	178
To Disable HotPlug Capability Using the vSphere Client	178
To Disable HotPlug Capability Using the vSphere Web Client	178
To Disable HotPlug Capability by Editing the Virtual Machine's .vmx File	178
Appendix C: NetApp Global File Cache (GFC) PowerShell Configuration	179
GFC Optimus PSM.....	179
Configuration Process	179
GFC Namespace for TUMMIPProvider.....	198
Appendix D: NetApp Global File Cache Event ID / Logging / 3rd Party Monitoring	208
NetApp Global File Cache Event IDs.....	208
GFC Logging	209
GFC File Transfer Summary Logging.....	210
GFC Processes / Services.....	211
Where to Find Additional Information	211

1 Introduction

Welcome to the NetApp Global File Cache User Guide. This manual will assist you in designing, deploying, managing, and maintaining your NetApp Global File Cache (GFC) infrastructure. The next few pages will provide a brief introduction and overview of GFC, and how it can be leveraged to enable data centralization, cloud storage consolidation, global file-sharing, and collaboration for distributed enterprises.

GFC allows businesses to centralize data, leveraging customer's on prem, hybrid or public cloud storage infrastructure, while consolidating distributed storage and IT assets. The software extends to users globally, providing real-time global file-sharing and collaboration to end users.

1.1 The GFC Fabric: Highly Scalable and Flexible

GFC transparently fits any IT environment, as the solution is storage cloud platform agnostic, supporting on prem NetApp Data ONTAP (AFF / FAS), Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files. Whether you want to leverage Microsoft Azure, Google Cloud Platform or Amazon Web Service public cloud storage infrastructure, GFC immediately extends the value of your central storage to your distributed locations.

In a nutshell, GFC creates an intelligent file caching software appliance at each distributed location, running on Microsoft Windows Server. The software overlays the Microsoft Windows File-Sharing mechanism, fully integrating with the Microsoft security principles like Active Directory, ACLs, and NTFS permissions, and allows it to work at a global scale, even in locations with low bandwidth or high latency.

1.2 Next Generation Software-Defined Storage

- GFC runs on Microsoft Windows Server 2016 and 2019.

- Fully integrates with customer's Microsoft ecosystem.

- (AD DS, DNS/DHCP, Print Services, SCCM, PowerShell).

- Available as software installation package or virtual appliance template.

1.3 Global File Cache Software

- Flexible: integrates with Cloud Volumes ONTAP, Cloud Volumes Service, Azure NetApp Files, AWS FSX for NetApp ONTAP or NetApp on premises AFF/FAS.

- Intelligent: Caches only what's needed at the branch (active dataset).

- Zero-touch: Automatically purges stale cached files over time (LRU).

- Performant: Compresses, streams, and reduces data.

- Consistent: Central file-locking for enterprise applications.

Important: This guide is designed for MANUAL deployment and enablement of the GFC solution.

For more information, including quick-start videos on the deployment of Global File Cache, visit: <https://cloud.netapp.com/global-file-cache/onboarding>

1.4 Enabling Global File Cache using NetApp Cloud Manager

For enablement of Global File Cache through Cloud Manager, please consult the following page for a step-by-step walkthrough: <https://docs.netapp.com/us-en/cloud-manager-file-cache/concept-gfc.html>

2 NetApp Global File Cache Requirements

NetApp Global File Cache (GFC) is cloud platform agnostic, and specifically designed to function across all platforms supporting Windows Server 2016 and 2019, bringing simplified IT to corporate distributed branch offices and beyond. Critically, GFC can be deployed on customers' existing hardware infrastructure, virtualization, or on prem, hybrid or public cloud environments in almost every case if they meet a few base-level requirements.

GFC requires the following hardware and software resources to function optimally. For more information about overall sizing guidelines, please consult Section 3 of this user guide.

2.1 Hardened Server Appliance

The GFC installation package creates a hardened software appliance on any Microsoft Windows Server 2016 or Windows Server 2019 instance. **DO NOT UNINSTALL THE GFC PACKAGE.** Uninstalling GFC will impact the functionality of the server instance and may require a full rebuild of the server instance.

IMPORTANT

2.2 Physical Hardware Requirements

Minimum 4 CPU Cores.

Minimum 16 GB RAM.

Dedicated Single or Redundant 1Gbps NIC.

10k RPM SAS HDD or SSD (preferred).

RAID controller with write-back caching functionality enabled * **IMPORTANT.**

2.3 Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)

Note: Hypervisor platforms are known to be subject to performance degradation from a storage subsystem perspective (e.g. latency). For optimal performance using GFC, a physical server instance with SSD is recommended.

For best performance in virtual environments, in addition to the physical host requirements, the following requirements and resource reservations must be met:

Microsoft Hyper-V 2016 R2 onwards

Processor (CPU): CPUs must be set as Static: Minimum: 4vCPU Cores.

Memory (RAM): Minimum: 16GB set as Static.

Hard Disk Provisioning: Hard Disks must be configured as "Fixed Disk".

VMware vSphere 6.x onwards

Processor (CPU) * **IMPORTANT:** Reservation of CPU Cycles must be set. Minimum: 4 vCPU Cores @ 10000MHz.

Memory (RAM) * **IMPORTANT:** Minimum: Reservation of 16GB.

Hard Disk Provisioning * **IMPORTANT:**

Disk Provisioning set as "Thick Provisioned Eager Zeroed",

Hard Disk Shares set to High,

Set "devices.hotplug" to "false" using the vSphere Client to prevent Microsoft Windows from presenting GFC drives as "removable".

See Appendix B for the steps to apply this setting

Networking * **IMPORTANT:** Network Interface needs to be set to VMXNET3 (requires VMTools).

Note: GFC runs on Windows Server 2016 and 2019, hence the virtualization platform needs to support the operating system, as well as integration with utilities enhancing the performance of the virtual machine's guest operating system and management of the virtual machine, such as VMTools.

2.4 Cloud Deployments (such as Microsoft Azure, Google Cloud Platform or Amazon AWS)

For best performance in public cloud environments, the following requirements must be met:

Public Cloud Deployments

Microsoft Azure

Standard D Series (i.e. D4s_v3) or equivalent

Minimum: 4 vCPU / 16GB RAM

See also: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general>

Amazon AWS (EC2)

M/C Instance Type (i.e. m4.xlarge) or equivalent

Minimum: 4 vCPU/16GB RAM

See also: <https://aws.amazon.com/ec2/instance-types/>

Google GCP

Standard Machine types (i.e. N2-standard-4) or equivalent

Minimum: 4 vCPU/16GB RAM

See also: https://cloud.google.com/compute/docs/general-purpose-machines#n2_machines

2.5 Operating System/Software Requirements

Windows Server 2016 Standard/Datacenter or Windows Server 2019 Standard/Datacenter.

Latest Microsoft updates should be installed to ensure optimal stability, performance, and security.

GFC server base deployment requirements:

Administrative Privileges (Domain Administrator),

A unique (geographical) NetBIOS name for the instance (i.e. NYC-FAST1),

IP Address, Subnet Mask, Gateway Address, and DNS Server details,

Active Directory Domain name.

GFC instances should be joined to the customer's Active Directory domain.

GFC instances should be managed in a GFC-specific OU (Organizational Unit) and excluded from inherited company GPO's.

Service Account: Username and Password for a domain user that has backup/restore privileges.

Service Account should be configured with the following account options:

User must change password at next logon = DISABLED (unchecked),

Password never expires = ENABLED (checked).

GFC instances must be on the same VLAN as the datacenter backend storage infrastructure (1 hop).

Service account users must have backup and restore security privileges.

Global File Cache Service Account & Azure NetApp Files

You can include additional accounts that require elevated privileges to the computer account created for use with Azure NetApp Files. The specified accounts will be allowed to change the NTFS permissions at the file or folder level. For example, you can specify a non-privileged service account used for migrating data to an SMB file share in Azure NetApp Files.

Please consult <https://docs.microsoft.com/en-us/azure/azure-netapp-files/create-active-directory-connections> to enable the “**ANFBackupOperator**” feature and add the Global File Cache service account to the Azure NetApp Files “**Backup Policy Users**” list.

Global File Cache Service Account on other platforms

This service account user must be a member of the local “Administrator” group on storage platforms like ONTAP, Cloud Volumes ONTAP or Cloud Volumes Service.

2.6 Backend File Server Requirements

Backend storage platform should present NetApp Cloud Volumes ONTAP, Cloud Volumes Service, Azure NetApp Files, AWS FSx for NetApp ONTAP and on premises AFF/FAS appliances.

Backend storage platform should present SMB File shares, Azure NetApp Files Shares, or iSCSI/FC Interface.

Backend storage platform should support NTFS File System, ACLs, and Local SAM Database when leveraging a Non-Windows SMB interface.

Network Latency between GFC and backend file storage should be < 1ms, Global File Cache Core instance needs to coexist with the backend storage platform in the same datacenter or cloud region / VNET or availability zone.

Important: Most storage tiering systems do not meet this requirement / SLA.

2.7 Datatype requirements

While GFC supports most file types, but large files such as ISO's, VMDK's, etc., should not be transferred through the shared file system

2.8 Amazon FSx for ONTAP system requirements

You need to prepare your Amazon FSx for ONTAP systems before you can deploy Global File Cache Core.

Prerequisites:

- Create an ONTAP filesystem.
- Create a Storage Virtual Machine (SVM).
- Ensure that the security rules of the subnet have access to the NetApp cloud license validation server.
- Have the following information available before creating the volume:
 - Storage Virtual Machine ID (svm-id)
 - AWS Region
 - AWS Endpoint URL
 - fsxadmin credentials

Steps:

On an Orchestrator Linux VM, run the following commands:

1. Create the volume:

```
aws fsx --region ${REGION} --endpoint ${ENDPOINT_URL} create-volume -- volume-  
type ONTAP --name --ontap-configuration  
JunctionPath=/gfcvol,SizeInMegabytes=1024,StorageVirtualMachineId=${SVM  
_ID},StorageEfficiencyEnabled=true
```

The volume will be created in 30-60 seconds. It will be created using the "unix" security-style instead of "ntfs"; which we need for the GFC Core

2. Using your FSxadmin credentials, login/ssh into the SVM.

3. Use the `volume modify -volume <vol_name> -security-style ntfs` command to change the volume security-style from "unix" to "ntfs".

4. Verify that the security-style is "ntfs" using the command `volume show -vserver <svm_name> -volume <vol_name> -instance`

5. Create a new DNS server mapping using the command `dns create -vserver <svm_name> -domains <directory_dns_name> -name-servers <dns_IPAddress>`

For example: `dns create -vserver svm01 -domains companygfcdmn.com -nameservers 10.1.2.103`

6. Create a CIFS server using the command `cifs create -cifs-server <cifs_server> -domain <directory_dns_name> -ou OU=<directory_netBIOS_name>`

For example: `cifs create -cifs-server GFCTEST -domain companygfcdmn.com -ou OU=companygfcqa`

7. Create a local user "gfcuser" on the SVM using the command `vserver cifs users-and-groups local-user create -vserver <svm_name> -user-name <cifs_server>\<user_name> -full-name <full_name>`

For example: `vserver cifs users-and-groups local-user create -vserver svm01 -user-name GFCTEST\gfcuser -full-name "GFC User"`

8. Add the user to the group BUILTIN\Backup Operators using the command `vserver cifs users-and-groups local-group add-members -vserver <svm_name> -group-name "BUILTIN\Backup Operators" -member-names <cifs_server>\<user_name>`

For example: `vserver cifs users-and-groups local-group add-members -vserver svm01 -group-name "BUILTIN\Backup Operators" -member-names GFCTEST\gfcuser`

Now you can deploy Global File Cache Core on your Amazon FSx for ONTAP system:

1. Deploy Base Windows Server 2016 or 2019.
2. Install GFC software.
3. Follow the remaining steps in this User Guide for GFC configuration information.

2.9 Partition Sizing Requirements

C:\ Minimum 250 GB (System/Boot Volume).

D:\ Minimum 1 TB (Separate Data Volume for GFC Intelligent File Cache*).

*Minimum size is 2x the active data set. The Cache Volume (D:\) can be extended and is only restricted by the limitations of the Microsoft Windows NTFS file system. A cache volume is not required on Cores as Cores do not cache data.

Note: Instances deployed in Azure have D:\ partition created by default as a temporary filesystem. This D:\ drive should not be used as GFC intelligent cache. For such instances, please create an additional partition E:\ and use as GFC Cache. Please contact GFC support for any such instances.

2.10 GFC Intelligent File Cache Disk Requirements (D:\)

Disk Latency should deliver < 0.5ms average IO Disk latency and 1MiB/sec throughput **per concurrent user**.

Download the DiskSpd tool from Microsoft to confirm storage performance on the GFC instance:

<https://gallery.technet.microsoft.com/DiskSpd-A-Robust-Storage-6ef84e62>

Perform the following command on D:\ (Cache Volume) to confirm.

Diskspd.exe -b8K -d60 -L -o2 -t4 -r -w30 -c500M D:\io.dat > results.txt

Confirm the results in results.txt

Total Read IO AvgLat should be < 0.500 ms

Total Write IO AvgLat should be < 0.500 ms

Write MiB/s should be 1MiB/s per user, i.e. for 100 concurrent sessions the Total Write MiB/s should be > 100 MiB/s

Example Result:

Read IO thread	bytes	I/Os	MiB/s	I/O per s	AvgLat	LatStdDev	file
0	3608035328	440434	57.34	7340.13	0.242	1.912	
D:\io.dat (500MiB)							
1	3857448960	470880	61.31	7847.54	0.227	1.805	
D:\io.dat (500MiB)							
2	3631136768	443254	57.71	7387.13	0.241	1.941	
D:\io.dat (500MiB)							
3	3721641984	454302	59.15	7571.25	0.234	1.882	
D:\io.dat (500MiB)							
total:	14818263040	1808870	235.52	30146.06	0.236	1.884	
Write IO thread	bytes	I/Os	MiB/s	I/O per s	AvgLat	LatStdDev	file
0	1546100736	188733	24.57	3145.36	0.066	0.933	
D:\io.dat (500MiB)							
1	1655848960	202130	26.32	3368.63	0.060	0.651	
D:\io.dat (500MiB)							
2	1559379968	190354	24.78	3172.38	0.064	0.794	
D:\io.dat (500MiB)							
3	1598201856	195093	25.40	3251.36	0.065	0.821	
D:\io.dat (500MiB)							
total:	6359531520	776310	101.08	12937.74	0.064	0.804	

2.11 Networking Requirements

- All client computers should be in the local LAN network connected to GFC Edge. In case of 'work from home' scenario, client computers typically connect over company's VPN to GFC Edge. In such scenarios, GFC performance is subject to many variables including quality of WAN link, VPN software, latency between client and Edge. In such scenarios, no performance guarantees can be made.

Firewall: TCP ports should be allowed between GFC edge and core instance.

GFC TCP Ports: 443 (HTTPS - LMS), 6618 – 6630, 6688.

Network optimization devices (i.e., Riverbed Steelhead) must be configured to “Pass-thru” GFC-specific ports (TCP 6618-6630), 6688.

MTU requirement: TCP Maximum Transmission Unit (MTU) between GFC Edge and GFC Core should be configured as not to fragment the TCP packets. This can be verified by executing ‘mturoute.exe’ tool.

Networking (External Access)

GFC License Management Server requires external access over HTTPS (TCP port 443) to these URLs:

If you are using GFC subscription-based licensing:

<https://rest.zuora.com/v1/subscriptions/<subscription-no>>

<https://rest.zuora.com/oauth/token>

If you are using NetApp legacy-based licensing:

<https://talonazuremicroservices.azurewebsites.net>

<https://talonlicensing.table.core.windows.net>

If you are using NetApp NSS-based licensing:

<https://login.netapp.com>

https://login.netapp.com/ms_oauth/oauth2/endpoints

https://login.netapp.com/ms_oauth/oauth2/endpoints/oauthservice/tokens

2.12 Client Workstation Settings

GFC transparently integrates into customer’s environments, allowing users to access centralized data using their client workstations, running enterprise applications. Using GFC, data is accessed through a direct drive mapping or through a DFS namespace. For more information about the GFC Fabric, Intelligent File Caching, and key aspects of the software, consult the Getting Started with NetApp Global File Cache section of this user guide.

To ensure an optimal experience and performance, it is important to comply with the Microsoft Windows Client requirements and best practices outlined below. This applies to all versions of Microsoft Windows.

Disable Offline Files and Folders When Using Multi-Path DFS Namespaces or Collaboration Data

To ensure data integrity, Offline Files and Folders (Sync Center) should be disabled on all client workstations. This can be accomplished through a registry setting or GPO that applies to Windows clients in the environment.

Registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSC

Specify the **Start** value to “4”

Group Policy

- a. Launch Group Policy Management console from Active Directory Users and Computers
- b. Navigate to the Domain policy or a specific policy that applies to Microsoft Windows Clients in your environment.
- c. Select User Configuration, expand Policies, expand Administrative Templates, expand System, and expand Folder Redirection.

- d. Right-click **“Do not automatically make all redirected folders available offline”** and click **Edit**.
- e. Click **Enabled**, followed by **OK**.

Depending on your environmental requirements (optional):

1. Right-click **“Do not automatically make specific redirected folders available offline”** window appears.
2. Click **Enabled**
3. In the **Options** pane, select the folders that should not be made available offline by selecting the appropriate check boxes
4. Click **Enabled**, followed by **OK**

Reference: [https://technet.microsoft.com/en-us/library/jj154097\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/jj154097(v=ws.11).aspx)

Microsoft Updates and Critical Patches

GFC diligently conducts QA testing and Microsoft patch validation within a week after initial release by Microsoft. It is highly recommended to test deployment of Microsoft Updates and Critical Patches after a week. Ideally, it would be recommended to roll out the updates to a test or single production instance to confirm successful deployment, before updating all GFC instances in the environment.

2.13 NetApp Support Policy

GFC instances are designed specifically for GFC as the primary application running on a Windows Server 2016 and 2019 platform. GFC requires priority access to platform resources, e.g. disk, memory, network interfaces, and can place high demands on these resources. Virtual deployments require memory / CPU reservations and high-performance disks.

For Branch Office deployments of GFC, supported services and applications on the server running GFC are limited to:

DNS/DHCP.

Active Directory Domain Controller (GFC cache must be on a separate volume).

Print Services.

Microsoft System Center Configuration Manager (SCCM).

GFC-approved client-side system agents & anti-virus applications.

NetApp Support and maintenance applies only to GFC.

“Line of Business” productivity software which are typically resource intensive, e.g. database servers, mail servers, etc. are not supported.

The customer is responsible for any non-GFC software which may be installed on the server running GFC.

If any third-party software package causes software or resource conflicts with GFC or performance is compromised, GFC’s support organization may require the customer to disable or remove the software from the server running GFC.

It will be the customer’s responsibility for all installation, integration, support and upgrade of any software added to the server running the GFC application.

Systems management utilities/agents such as anti-virus tools and licensing agents may be able to coexist. However, except for the supported services and applications listed above, these applications are not supported by GFC and the same guidelines as above must still be followed.

If a customer does install any third-party software package that causes, or is suspected to be causing, software or resource conflicts with GFC or performance is compromised, there may be a requirement by GFC’s support organization to disable/remove the software.

2.14 Firewall and Antivirus Best Practices

Note: While GFC makes a reasonable effort to validate that the most common antivirus application suites are compatible with GFC, we cannot guarantee and are not responsible for any incompatibilities or performance issues caused by these programs, or their associated updates, service packs, or modifications.

GFC does not recommend the installation nor application of monitoring or antivirus solutions on any GFC enabled instance (Core or Edge). Should a solution be installed, by choice or by policy, the following best practices and recommendations must be applied (See Appendix A for common antivirus suites).

Firewall Settings

Microsoft Firewall

Retain Firewall Settings as Default.

Recommendation: Leave Microsoft Firewall settings and services at the default setting of OFF, and not started for standard GFC Core or Edge instances.

Recommendation: Leave Microsoft Firewall settings and services at the default setting of ON, and started for Core or Edge instances that also run the Domain Controller role.

Corporate Firewall

GFC core instance listens on TCP ports 6618-6630, 6688 ensure that GFC edge instances can connect to these TCP ports.

GFC instances require communications to the License Management Server (LMS) on TCP port 443 (HTTPS).

Network Optimization solutions/devices must be configured to “Pass-thru” GFC-specific ports.

Antivirus Best Practices

This section helps you to understand the requirements when running antivirus software on a Windows Server instance running GFC. GFC has tested most commonly used antivirus products including Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky and Windows Defender (see appendix A) for use in conjunction with GFC.

Note: Adding antivirus to an Edge appliance may introduce a 10-20% impact on user performance.

Pre-Installation Notes

The antivirus software should be certified by GFC (See appendix A).

Individual Antivirus applications are supported when configured with proper exclusions.

Full security suites are not supported.

Restrict File Scanning

Applications that scan files and/or folders in order to gather statistics or other data sometimes only read metadata of the file without reading actual data contained within the file. Other applications may open each file individually to determine the type of data present in the file. In the case of pictures, music, or video files, certain applications may also create thumbnails or provide additional information about the contents of the file.

Scans that cause these types of file open operations should be avoided on the edge instance and on the client workstation. Any open of a file in this manner will cause the Edge instance to retrieve the file from the backend data center file server and cache it locally in the branch office. Scanning to gather statistics or provide thumbnails to picture files could also cause the Edge instance to retrieve and cache more data than the cache was originally sized to accommodate. Client-side software that searches, indexes, and/or scans network files and folders can cause unnecessary metadata and file transfers over the WAN, resulting in an additional load on the instance and should be avoided.

Antivirus Coverage Recommendation

Antivirus software installed on the backend data center file server and on client PCs is generally adequate protection against network viruses. GFC does allow data on its Edge and Core instances to be scanned, ensuring complete point-to-point protection.

However, on both Cores and Edges, the D:\ (cache drive) volume should be excluded from virus scanning as well as any GFC processes. Users' mapped network drives should never be scanned.

Configure Exclusions

Antivirus software or other third-party indexing or scanning utilities should never scan drive D:\ on the Edge instance. These scans of Edge server drive D:\ will result in numerous file open requests for the entire cache namespace. This will result in file fetches over the WAN to all file servers being optimized at the data center. WAN connection flooding and unnecessary load on the Edge instance will occur resulting in performance degradation.

In addition to the D:\ drive, the following GFC directory and processes should generally be excluded from all antivirus applications:

```
C:\Program Files\TalonFAST\  
C:\Program Files\TalonFAST\Bin\LMClientService.exe  
C:\Program Files\TalonFAST\Bin\LMServerService.exe  
C:\Program Files\TalonFAST\Bin\Optimus.exe  
C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe  
C:\Program Files\TalonFAST\Bin\tafsexport.exe  
C:\Program Files\TalonFAST\Bin\tafsutils.exe  
C:\Program Files\TalonFAST\Bin\tapp.exe  
C:\Program Files\TalonFAST\Bin\TappN.exe  
C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe  
C:\Program Files\TalonFAST\Bin\TService.exe  
C:\Program Files\TalonFAST\Bin\tum.exe  
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe  
C:\Program Files\TalonFAST\FastDebugLogs\  
C:\Windows\System32\drivers\tfast.sys  
\\?\TafsMtPt:\ or \\?\TafsMtPt*  
\Device\TalonCacheFS\  
\\?\GLOBALROOT\Device\TalonCacheFS\  
\\?\GLOBALROOT\Device\TalonCacheFS\*
```

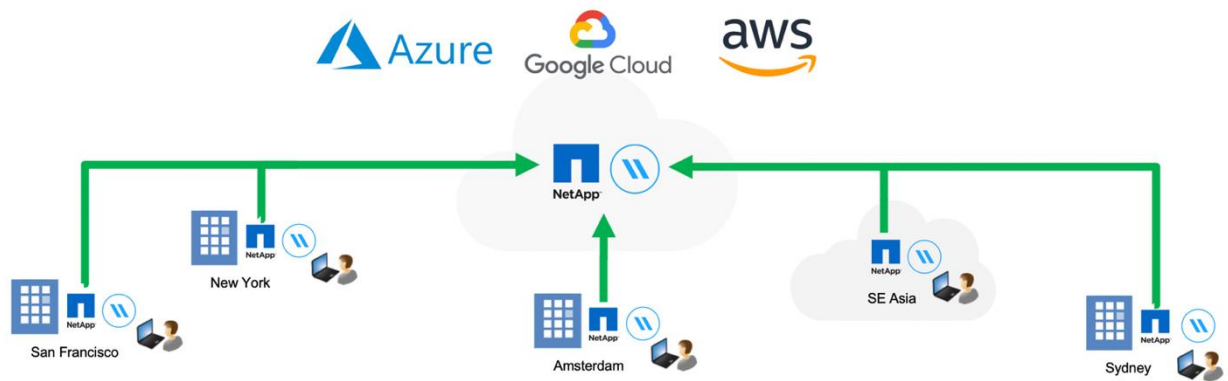
3 Getting Started with NetApp Global File Cache

NetApp Global File Cache (GFC) can be deployed in various ways, either on physical hardware or on virtualization platforms including Microsoft Hyper-V, VMware, or others. Depending on the client's needs, the software can be architected as a hub-and-spoke, symmetric, or hybrid deployment, which means that you can extend central file shares to multiple branch offices, allow branch offices to access file storage in both locations or a combination of both.

Typically, customers choose to centralize their data into one or multiple datacenters, which allows them to architect a so-called hub-and-spoke deployment. This means that all distributed locations can access centralized file storage, using the GFC Fabric, in real-time with the benefits of distributed file-locking.

Customers drive value from GFC by centralizing data and consolidating file storage from distributed branch offices into the on prem, hybrid or public cloud datacenter, i.e. Microsoft Azure, Google Cloud Platform, or Amazon Web Services.

Figure 1)



3.1 Example: Deployment Summary

The topology referenced in this example is a "hub and spoke" model, whereby the network of distributed offices/locations are all accessing one common set of data in the customer's datacenter. The key points of this example reference architecture are:

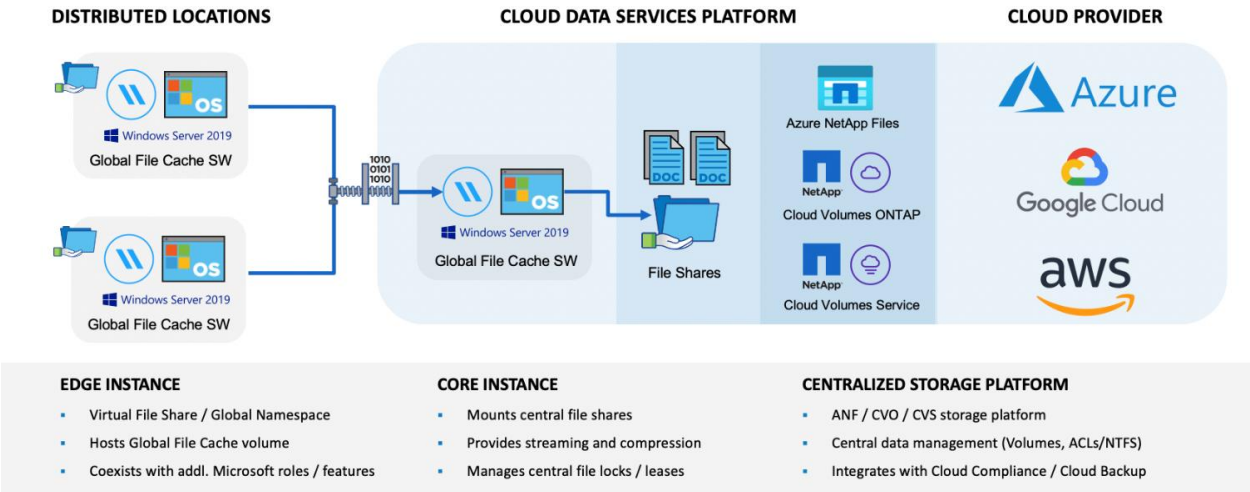
- Centralized data store: Enterprise storage in customer's on prem, hybrid or public cloud datacenter.
- GFC Fabric: Extension of the central data store to the distributed locations.
 - GFC Core Instance, mounting to corporate file shares (SMB).
 - GFC Edge Instance running in each distributed location.
 - Presents a Virtual File Share that provides access to central data.
 - Hosts the Intelligent File Cache on a custom-sized NTFS volume (D:\).
- Network configuration
 - MPLS, Virtual Private Network (VPN) connectivity or Public Internet (SSL).
- Integration with customer's Active Directory Domain Services.
- DFS-Namespaces for the use of a global namespace (recommended).

3.2 Example: Centralized Data Store in the On prem, hybrid or public cloud

The main repository for the unstructured data is a share (or number of shares) configured on the customer's on prem, hybrid or public cloud storage platform (Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files) leveraging SMB integration, or by presenting a local volume associated with an iSCSI target.

The customer's cloud storage platform solution provides volumes associated with corporate file shares hosted in the on prem, hybrid or public cloud.

Figure 2) Global File Cache: Cloud Platform Agnostic



This traditional approach to storage management enables organizations to scale storage area networks (SAN) and network-attached storage (NAS) with on-demand storage, providing a familiar solution for file capacity expansion, offsite storage, and data archiving.

Presenting data in a modernized storage model allows users to work with their applications in a non-disruptive manner. All the data you put into the centralized storage solution, whether primary, file, backup, or archive, is completely under your control, and integrates with your desired platforms, backups, RTO/RPO, and BCDR strategy.

Cloud Storage Platform

Provides transparent SMB utilization presented by Azure NetApp Files, Cloud Volumes ONTAP or Cloud Volumes Service.

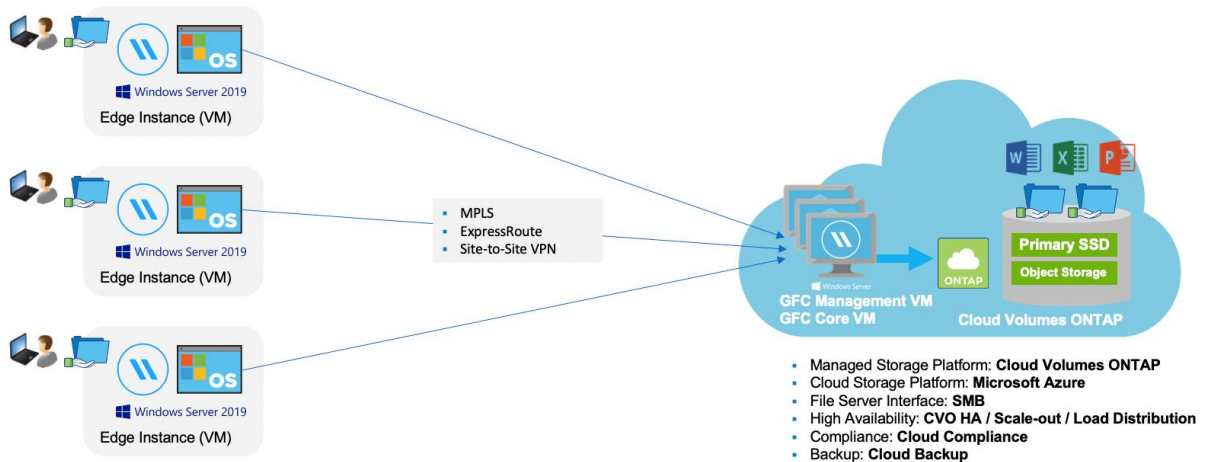
Centralized data management (Volumes, ACLs, NTFS Permissions).

Integrates with enterprise backup solutions (RTO/RPO).

3.3 GFC Fabric

By introducing GFC, integrating the GFC Fabric with Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files, all distributed locations can use the central file storage resources as if they were local. The result is a single, centralized storage footprint, versus a distributed storage architecture that requires local data management, backup, security management, storage, and infrastructure footprint, etc. in each location.

Figure 3) Example of GFC with Cloud Volumes ONTAP in Microsoft Azure



The GFC Edge instances transparently integrate with the GFC Fabric at the customer's cloud datacenter:

Distributed locations connect to cloud datacenter via the GFC Fabric.

Software provides a Virtual File Share and Intelligent File Cache at each location.

Virtual File Share is available as

\\Edge\FASTData\[datacenter]\[fileserver]\[share]\[folder]\

Access our data through DFS Namespace (recommended) or Drive Mapping.

Intelligent File Cache can be sized based on the customer's active data set (see product requirements).

Enables high performance global file sharing with real-time distributed file-locking.

3.4 Sizing Guidelines

There are a few sizing guideline ratios that you need to keep in mind when configuring the initial system. You should revisit these ratios after some usage history has accumulated to make sure you are using the system optimally. These include:

GFC Edges/Core Ratio

Distributed Users/GFC Edge Ratio

Distributed Users/GFC Core Ratio

Number of Edge instances per Core instance

Our guidelines recommend a maximum of 10 Edge instances per GFC Core. This is dependent to a significant degree upon the type and mean file size of the most common workload. In some cases, depending on the types and sizes of the file sets, it may be less than 10 Edges per GFC Core. Connecting more than 10 Edges per GFC Core is not recommended. NetApp Support should be contacted with any questions related to the number of Edge/Core instances.

Note: You can leverage multiple GFC Edge and Core instances simultaneously to scale out your infrastructure depending on the requirements. Multiple Core instances for a single set of user data is not supported when deployed using Cloud Manager at this time. The number of edges per core are specifically for Ontap /windows Backends. Other type of backends may need different scale.

Number of concurrent users per Edge instance

The GFC Edge handles the "heavy lifting" in terms of caching algorithms and file-level differencing. A single GFC Edge instance can serve up to 500 users per physical dedicated GFC Edge instance, and up to 300 users for dedicated virtual machine deployments. This is dependent to a significant degree upon the type and mean file size of the most common workload. For more common Office items with a mean file size <1MB, guide towards the 100% users per GFC Edge upper boundary (depending on physical or virtual deployment).

Note: GFC Edge detects whether it is running on a virtual or physical instance, and it will limit the number of SMB connections to the local virtual file share to the maximum of 300 or 500 concurrent connections depending on the instance type.

Consult your GFC Solutions Engineer to discuss the best options for your enterprise deployment.

4 Deploying NetApp Global File Cache Virtual Template and Software Package

4.1 Before You Begin

- Download the NetApp Global File Cache (GFC) Virtual Template(s) and Software Installation Packages from:
<https://cloud.netapp.com/global-file-cache/onboarding> (needs registration).
- To complete basic GFC configuration tasks, you will need the following information.
 - Static IP addresses for each GFC instance.
 - Subnet Mask
 - Gateway IP address.
 - The FQDN you wish to assign to each GFC server
 - The DNS suffix (optional).
- For GFC Core configuration only
 - The username and password of an administrative user in the domain
(or)
 - local username and password on the backend, that is added to local Backup Operators group on the backend.
- For GFC Edge configuration only
 - The FQDN and/or IP address of the associated Core server(s).
 - A Volume to be used as the Intelligent File Cache. It is recommended this be at least 2x the size of the “active” dataset. This should be formatted as NTFS and assigned as D:\.
- Commonly Used TCP Ports.
 - There are several TCP ports used by GFC services. It is mandatory the devices can communicate on these ports and they be excluded from any WAN Optimization devices or Firewall restriction policies.
 - GFC LMS and LMC Licensing TCP Port: 443.
 - GFC TCP Ports: 6618-6630, 6688

4.2 Deploying the GFC Virtual Template

If you are deploying GFC using OVA or .VHD virtual machine template, follow the steps as outlined in this section. In this document we assume that you understand how to deploy the .OVA or .VHD template on the designated hypervisor platform.

Note: Ensure that virtual machine preferences, including resource reservations, are in line with the requirements as outlined in section 2: “**Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)**”.

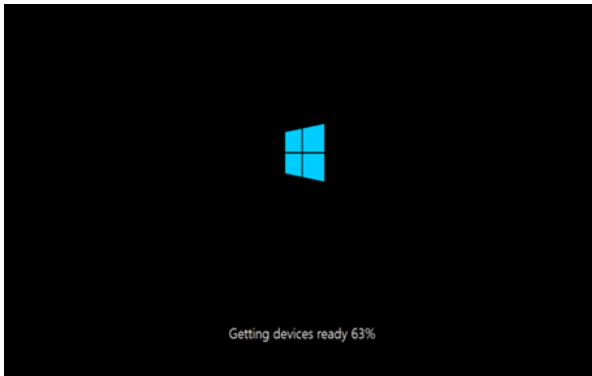
Once the Virtual Template has been deployed, and virtual machine settings have been configured, feel free to start the Virtual Machine.

During initial boot, when the Windows Server 2016 or 2019 operating system is preparing for first use, complete the out-of-the-box experience by installing the correct drivers and installing the necessary components for the respective hardware.

When the base install of the GFC virtual instance has been completed, the Windows Server 2016 or 2019 operating system will guide you through an initial configuration wizard to configure operating system specifics such as localization and product key.

Once the initial configuration wizard has completed, log in locally to the Windows Server 2016 or 2019 operating system with the following credentials:

Figure 4)



Login Credentials

Username: FASTAdmin

Password: Tal0nFAST!

Figure 5)



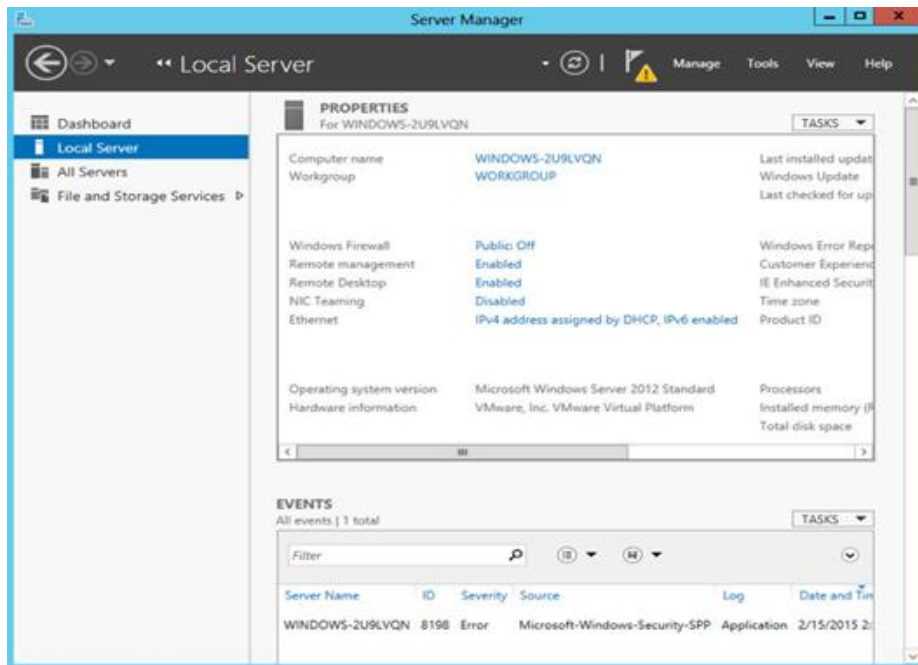
4.3 Network Configuration

To successfully deploy GFC, you need to configure some basic settings such as IPv4 address, NetBIOS name, and domain membership through the **Windows Server 2016 or 2019 Server Manager** management console, which is automatically started after logging in to the GFC instance using the local **FASTAdmin** account.

Click “Local Server” in the left pane and click the blue text next to “Ethernet” to open the Network Connections available to this instance.

Virtual appliances typically provide a single Local Area Connection to guest operating systems, which is based on the 1Gbps **VMXNET3** interface.

Figure 6)

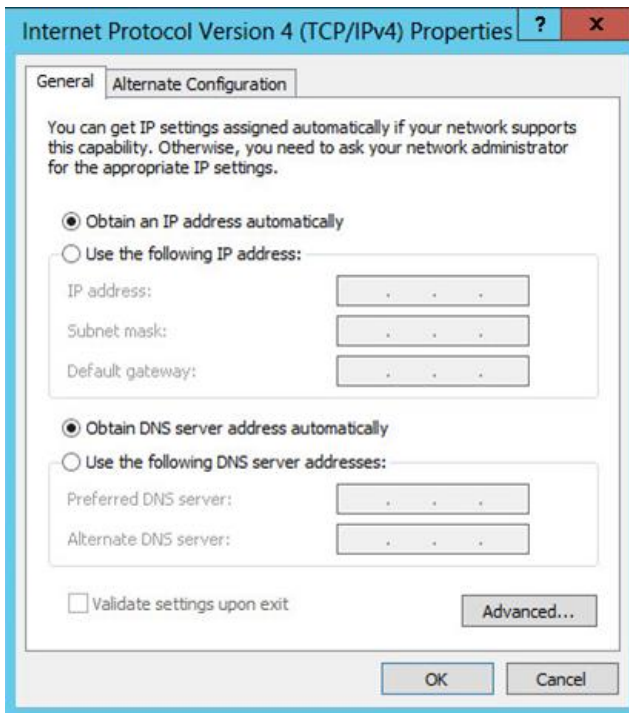


This document only covers the basic configuration of IPv4 addresses, subnet mask, gateway, and DNS server settings using the “Local Area Connection” virtual network adapter, which is applicable to any GFC appliance.

1. Right-click the “**Local Area Connection**” adapter
2. Click “**Properties**”
3. Select Internet Protocol 4 (TCP/IPv4)
4. Click “**Properties**”

This opens the basic IPv4 configuration window.

Figure 7)



In order to manually configure the IP address, gather network information from page 4 and fill out the following fields:

IP Address

Subnet mask

Default Gateway

Preferred DNS Server

Alternate DNS Server

Click “**OK**” to confirm configuration

The GFC instance is now configured to communicate with other devices on the network to join the Active Directory domain.

4.4 Active Directory Configuration

Please follow the NetBIOS and Domain configuration steps as outlined in this section.

Note: Screenshots used throughout this document based on Microsoft Windows Server 2012 R2. Your experience may vary from what is shown.

The GFC instance needs a unique NetBIOS computer name. It is recommended to adhere to the company’s naming scheme for ease of management.

In many cases, the NetBIOS computer name represents a logical name including a geographical location, i.e.

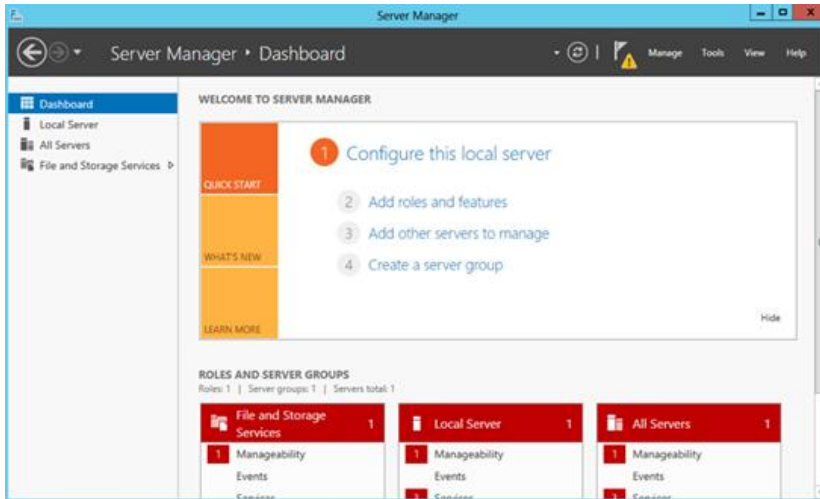
Core GFC instance located in Amsterdam

AMS-FAST1

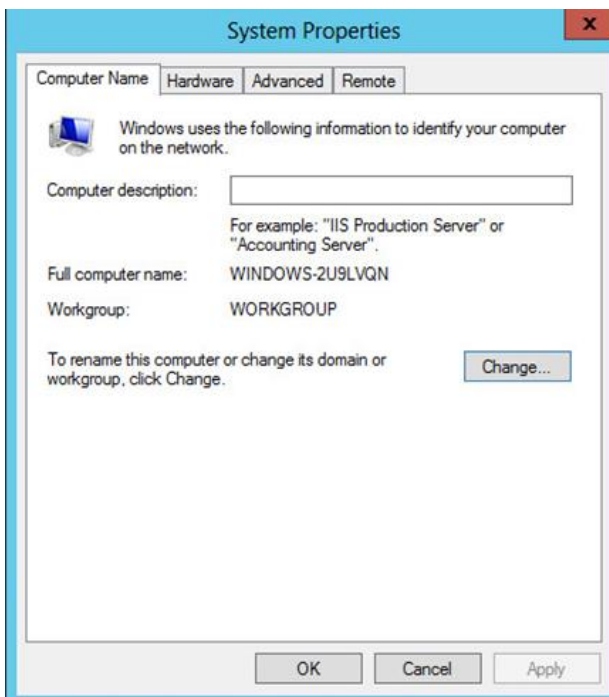
Edge GFC instance located in London

LON-FAST1

1. Use the Microsoft Windows Server 2016 and 2019 Server Manager console to configure the GFC instance's NetBIOS name by clicking "**Local Server**" in the left pane.



2. Click the blue entry next to "**Computer name**" to open the System Properties window.
3. Click the "**Change...**" button to open the Computer Name/Domain Changes window.

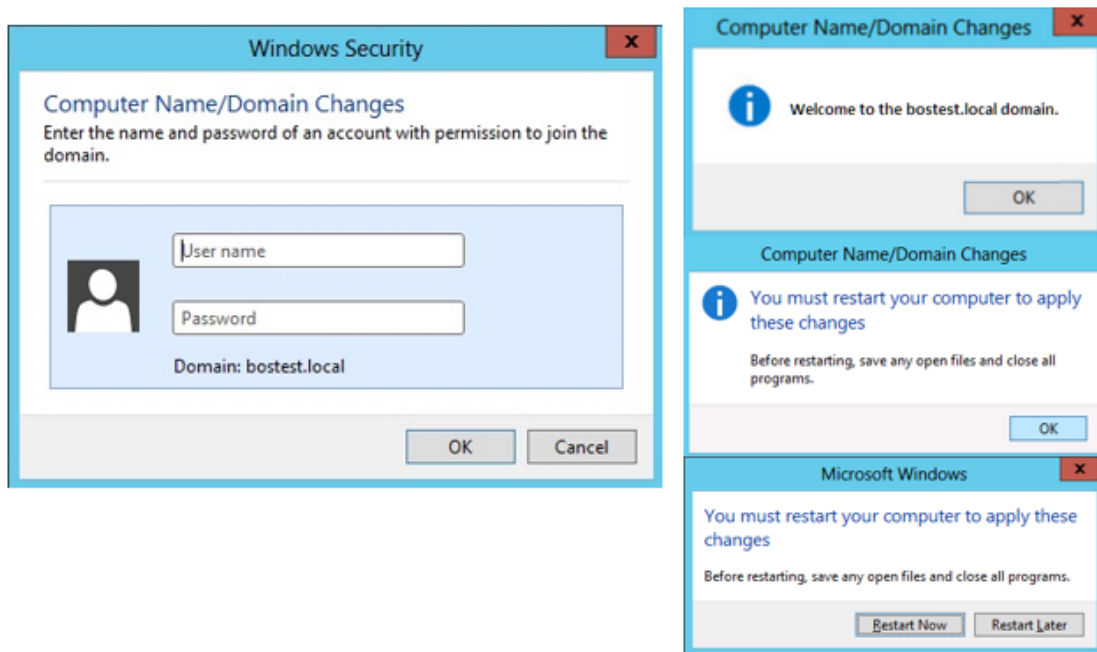


4. Type the desired NetBIOS name in the "**Computer Name**" field.
5. Select "**Member of**" Domain.
6. Type the Active Directory FQDN.
7. Confirm by clicking "**OK**".

Complete the Configuration:

1. Provide a Domain Administrator's **username** and **password**.

2. Confirm by clicking **"OK"**.



Once the GFC instance is successfully joined to your company's Active Directory domain, perform a system reboot by clicking **"Restart Now"**.

4.5 Software Installation Package (Update)

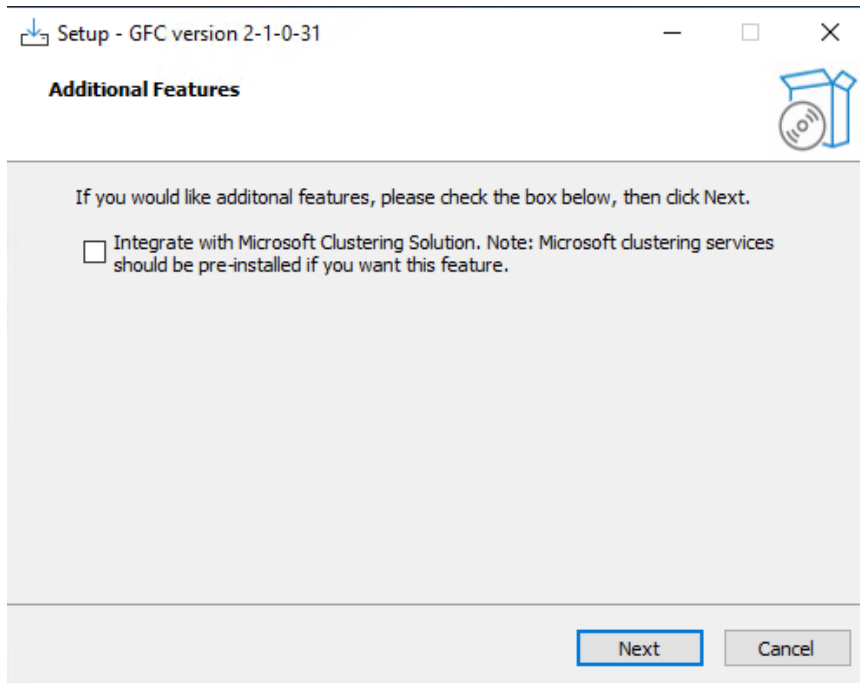
GFC often releases updates to the software, either patches, enhancements, or new features/functionality. Although the virtual template (.OVA and .VHD) images contain the latest GA release of the GFC software, it could be possible that a newer version is available on the NetApp Support Download portal.

Ensure that your GFC instances are up to date with the latest GA version available at <https://cloud.netapp.com/global-file-cache/onboarding>

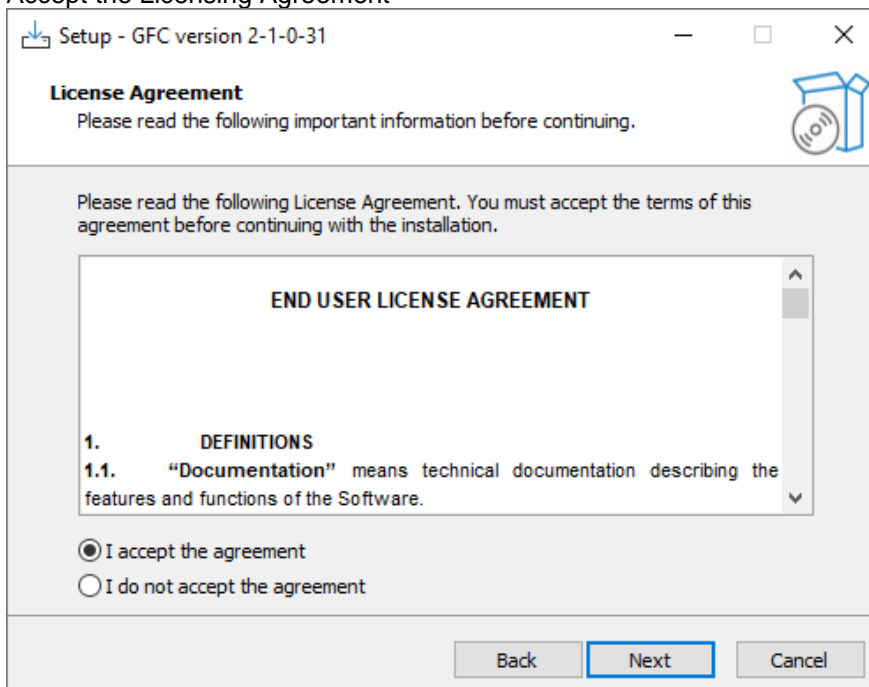
Note: This software package can also be used for pristine installations on Microsoft Windows Server 2016 Standard or Datacenter or Windows Server 2019 Standard or Datacenter edition or used as part of your upgrade strategy.

Below you can find the steps required to update the GFC installation package:

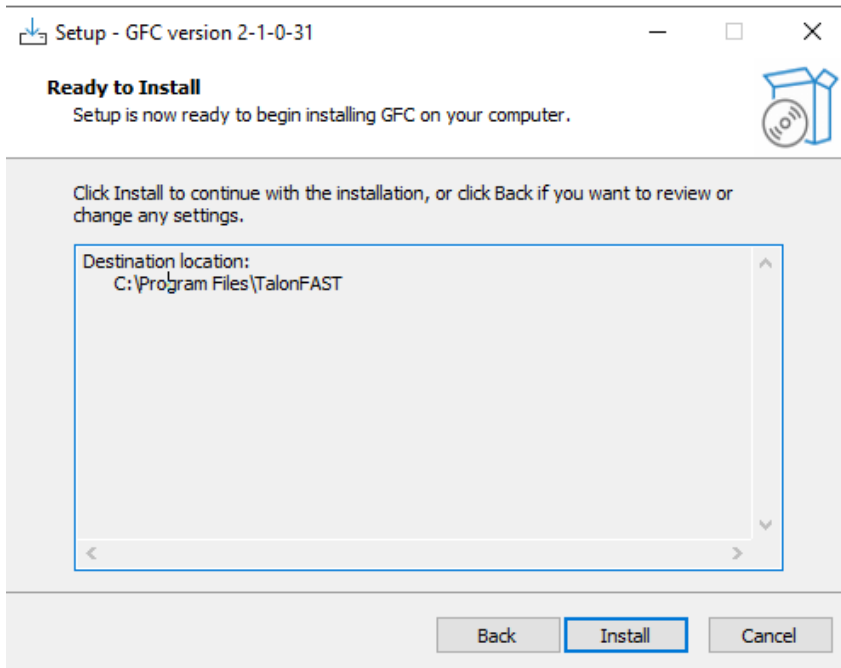
1. After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable.
2. Click the **"Next"** Button to continue the process.
3. Optional: check the desired boxes when configuring the Core using Microsoft Clustering Services.



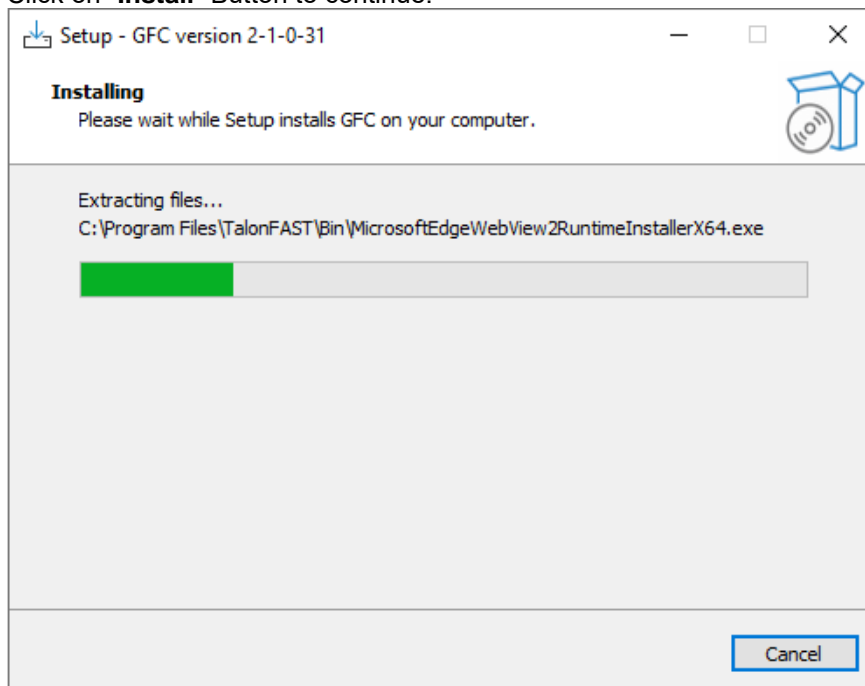
4. Click **"Next"** to continue.
5. Accept the Licensing Agreement



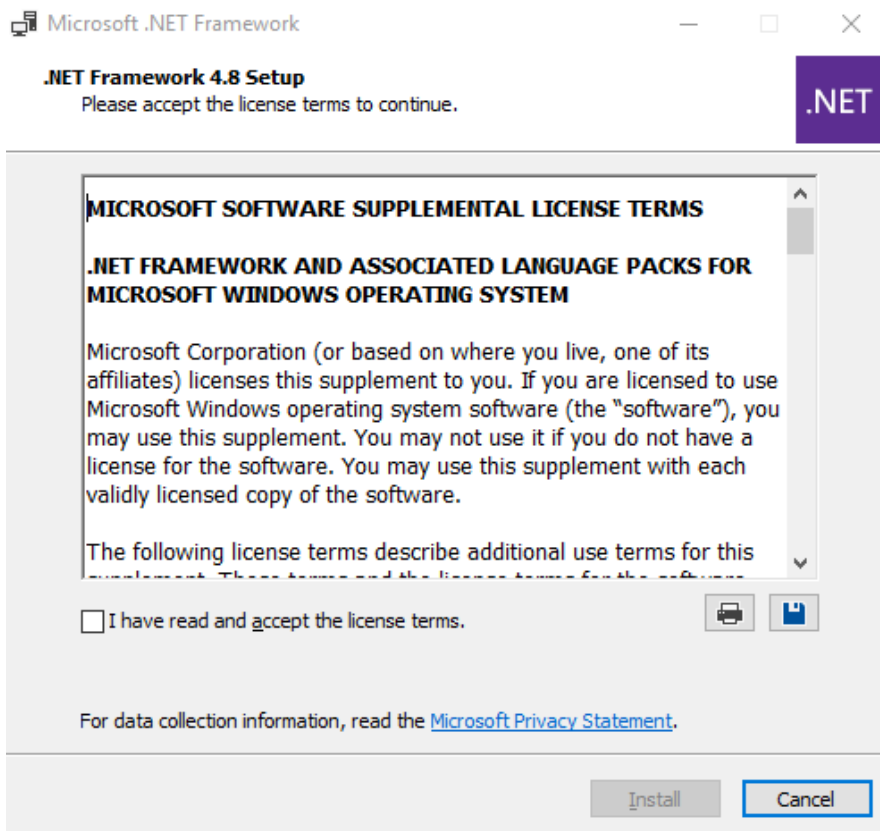
6. and click **"Next"** to continue
7. GFC installation is performed in default installation location "C:\Program Files\TalonFAST".



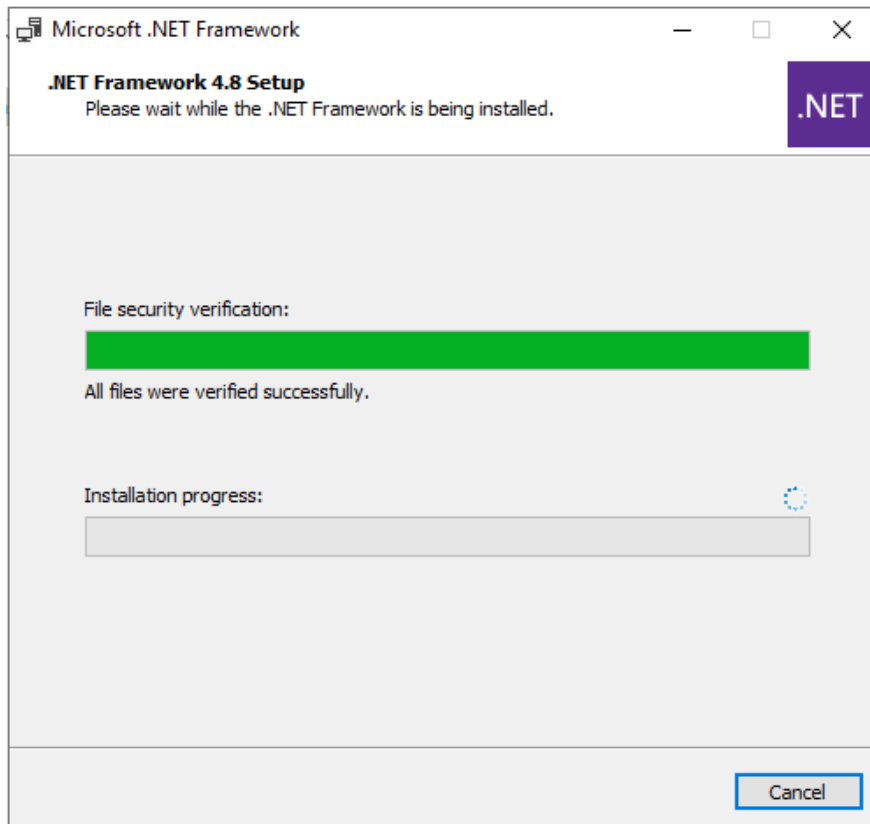
8. Click on “**Install**” Button to continue.



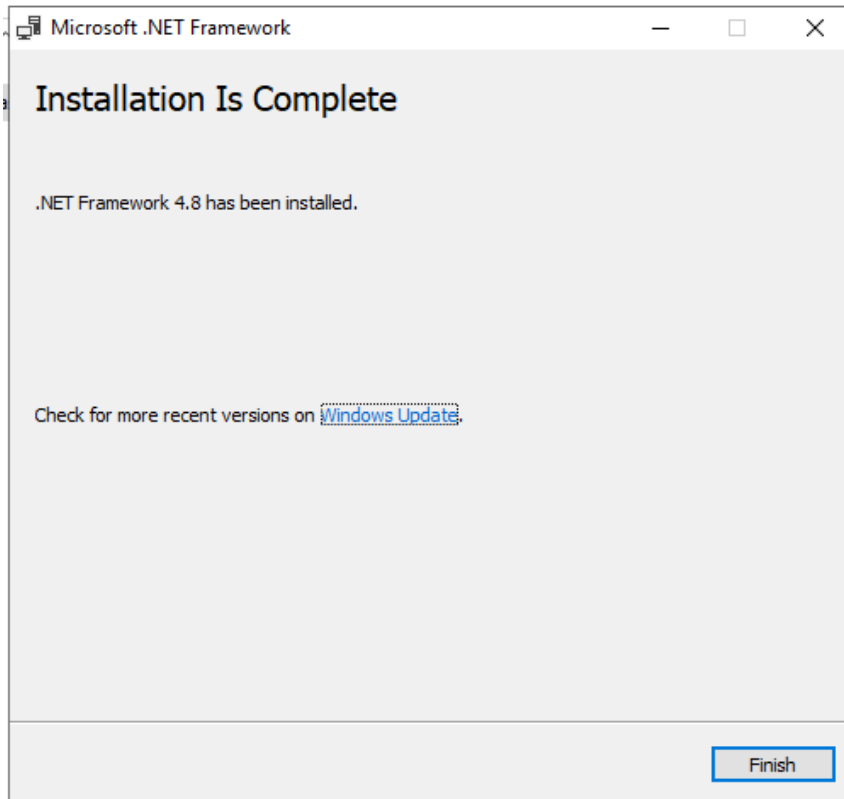
9. Next, Installer will verify for the minimum required .NET framework version. If not present, .Net framework installer will prompt for installation.



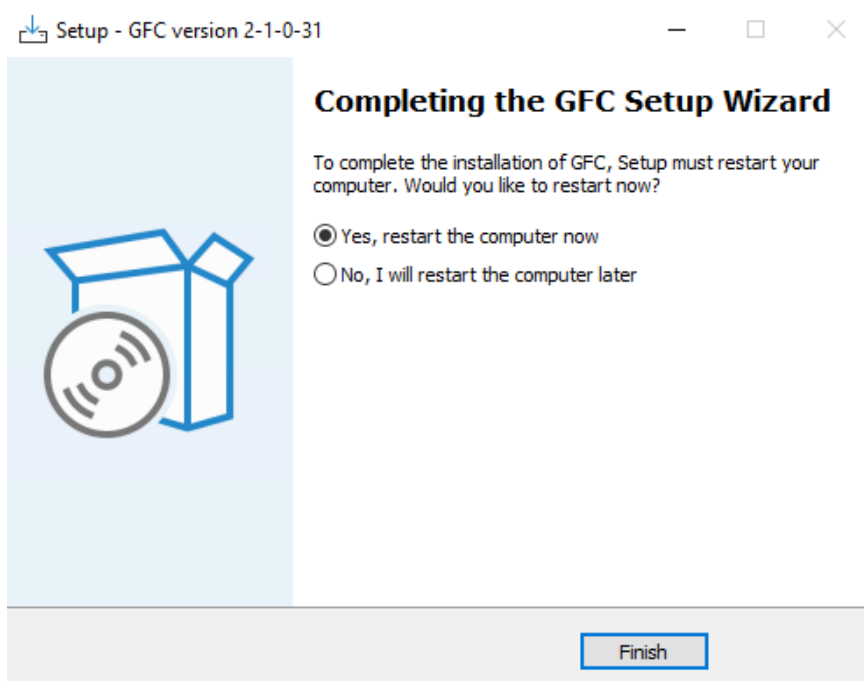
10. Accept the License agreement and click on “**Install**” to continue.



11. Click on “**Finish**” button after .NET framework installation is complete.



12. After installation of .Net Framework, WebView2 will be installed.
13. Post Installation steps will run by GFC installer .



14. Once the installation has completed, reboot the server when prompted.

5 Licensing

NetApp Global File Cache (GFC) includes a software-based License Management Server (LMS), which allows you to consolidate and simplify your overall license management and deploy licenses to all core and edge instances using an automated mechanism.

Important: If you are using Cloud Manager to enable Global File Cache, consult <https://docs.netapp.com/us-en/cloud-manager-file-cache/concept-gfc.html> for a step-by-step walkthrough.

5.1 How It Works

When you deploy your first core instance in the datacenter or cloud or standalone, you can choose to designate that specific instance to become the LMS for your organization. This LMS instance is configured once, connects to the subscription service (HTTPS) and validates your subscription using the customer ID provided by our support/operations department upon enablement of the subscription.

Once you have deployed your LMS instance, you need to associate your edge instances with the LMS by providing your customer ID and the IP address of the LMS instance. This process can be executed manually or automated. For automation options, either through registry, GPO or PowerShell DSC, consult your GFC Solutions Engineer.

5.2 Subscription Updates

The subscription service is designed to simplify license management. Once you have renewed or extended your subscription, our support/operations department will centrally update the license details, i.e. the number of sites or subscription end date. Once LMS queries (HTTPS) the subscription service, the license details will be automatically updated on the LMS instance and the (new) license details will apply to your GFC core and edge instances.

5.3 Caching

The LMS instance gathers the subscription information, including the number of sites and the end date associated with the subscription. The LMS instance caches these details so, in case LMS is disconnected from the internet or the subscription service is unavailable, you can continue to deploy and validate your licenses.

5.4 Requirements

The GFC LMS instance should be configured on a Microsoft Windows Server 2016 Standard or Datacenter edition or Windows Server 2019 Standard or Datacenter edition, preferably the GFC core instance in the datacenter or cloud.

If you require a separate GFC LMS instance, you need to install the latest GFC software installation package on a pristine Microsoft Windows Server instance.

GFC LMS instance needs to be able to connect to the subscription service (Azure Services / public internet) using HTTPS (TCP port 443).

GFC LMS instance needs to be able to connect to NetApp NSS services and GFC License Subscription service.

GFC core and edge instances need to connect to the GFC LMS instance using HTTPS (TCP port 443).

5.5 Deploying GFC LMS instance

In this example, we will configure the LMS service on an existing GFC core instance running GFC in the (on prem, hybrid or public cloud) datacenter. This is a one-time exercise that allows you to complete the GFC LMS deployment.

1. To start the LMS configuration, open the GFC Configuration Console from the designated GFC LMS instance (i.e., initial GFC core instance in the environment) and select the option in “**System Configuration**”.
2. To open a LMS Registration page in web browser, click a hyperlink “Click Here for LMS server configuration” under License Manager section.

The screenshot shows the NetApp Global File Cache Configuration Console. The main navigation bar includes 'System Overview', 'System Configuration', 'GFC Configuration', and 'Policy Configuration'. Under 'System Configuration', there is a 'License Manager' section with sub-tabs for 'Legacy Licensing', 'CI Configuration', and 'Cloud Manager Configuration'. The 'License Configuration' section is active, displaying a form titled 'Associate this instance with a License Manager Server'. The form contains three input fields: 'License Server Public IP Address/DNS name' with the value '10.19.89.168', 'Customer Id' with the value 'test', and 'Intended Server Role' with radio buttons for 'Core' and 'Edge' (where 'Edge' is selected). A 'Register' button is located at the bottom right of the form. Below the form, there is a 'License Server Configuration' section with a link that says 'Click Here for LMS server Configuration'.

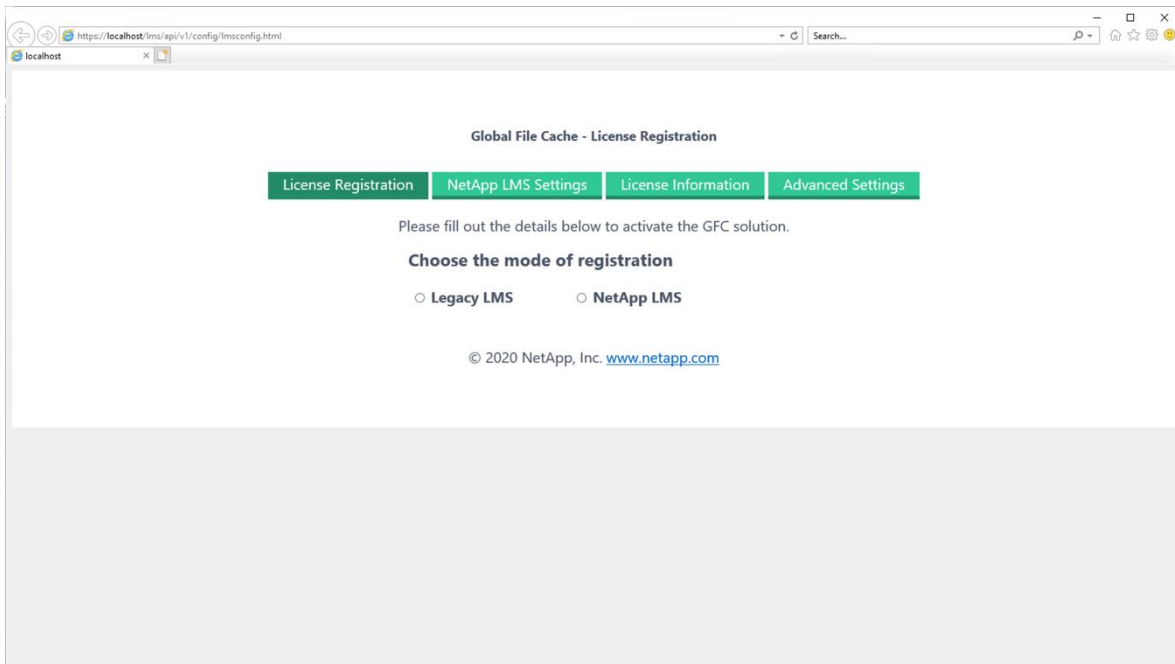
or open a web browser (Internet Explorer) and navigate to the following URL:

<https://localhost/lms/api/v1/config/lmsconfig.html>

Note: you can also access the URL from a client workstation using the following URL using the IP address of the GFC Management Server or LMS server:

[https://\[ip address\]/lms/api/v1/config/lmsconfig.html](https://[ip address]/lms/api/v1/config/lmsconfig.html)

3. Click “**Continue to this website (not recommended)**” to continue.
A webpage will be presented, which allows you to configure the LMS or check existing license information.



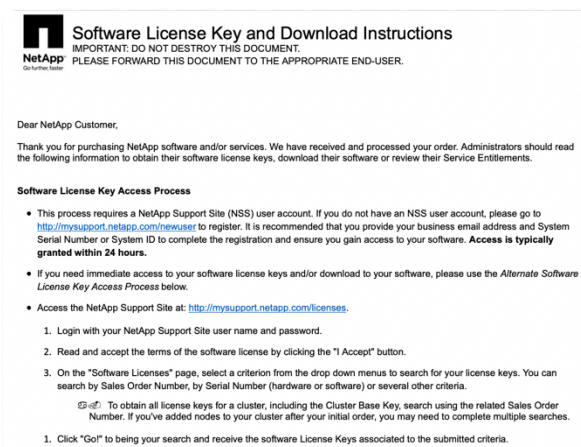
4. Choose the mode of registration by selecting “**Legacy LMS**” or “**NetApp LMS**”.

“**Legacy LMS**” is used for existing or trial customers that have received a Customer ID manually through NetApp Support. (Deprecated)

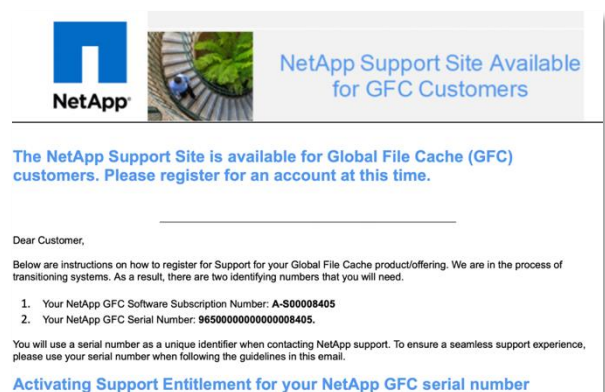
“**NetApp LMS**” is used for customers that have purchased NetApp Global File Cache edge licenses from NetApp or its certified partners. (Preferred)

Note: Depending on the activation email you received, your NSS credentials or Software Subscription Number (i.e., A-S00008405) will be required to enable Global File Cache.

NSS Credentials:



Software Subscription Number:



5. “Legacy LMS” (Deprecated, for Trial customers ONLY)

Global File Cache - License Registration

License Registration | NetApp LMS Settings | License Information | Advanced Settings

Please fill out the details below to activate the GFC solution.

Choose the mode of registration

☒ Legacy LMS ☐ NetApp LMS

Customer ID:

* Enter the unique Number/ID provided in the notification from NetApp Operations

You will be prompted to enter the Customer ID (case sensitive) as provided by NetApp Support/operations department, i.e. CUSTOMER.

6. “NetApp LMS” (Preferred)

In order to license and activate Global File Cache, you first need to enter a Subscription ID provided by Netapp Operations.

We recommend choosing a unique identifier, i.e., your email address for first-time registration of your LMS instance, once registered, follow the steps in order to associate your NSS credentials or your GFC Software Subscription Number.

Global File Cache - License Registration

License Registration | NetApp LMS Settings | License Information | Advanced Settings

Please fill out the details below to activate the GFC solution.

Choose the mode of registration

☐ Legacy LMS ☒ NetApp LMS

Subscription Number:


* Enter the unique Number/ID provided in the notification from NetApp Operations

Customer Name:

Depending on the activation email you received, your NSS credentials or Software Subscription Number (i.e., A-S00008405) will be required to enable Global File Cache.

7. Configuring “NetApp LMS Settings” using NSS Credentials

If you have received the [following email](#), you should activate your licenses by supplying your NSS credentials in the “NetApp LMS Settings” section.



Software License Key and Download Instructions


IMPORTANT: DO NOT DESTROY THIS DOCUMENT.
PLEASE FORWARD THIS DOCUMENT TO THE APPROPRIATE END-USER.

Dear NetApp Customer,

Thank you for purchasing NetApp software and/or services. We have received and processed your order. Administrators should read the following information to obtain their software license keys, download their software or review their Service Entitlements.

Software License Key Access Process

- This process requires a NetApp Support Site (NSS) user account. If you do not have an NSS user account, please go to <http://mysupport.netapp.com/newuser> to register. It is recommended that you provide your business email address and System Serial Number or System ID to complete the registration and ensure you gain access to your software. **Access is typically granted within 24 hours.**
- If you need immediate access to your software license keys and/or download to your software, please use the *Alternate Software License Key Access Process* below.
- Access the NetApp Support Site at: <http://mysupport.netapp.com/licenses>.
 1. Login with your NetApp Support Site user name and password.
 2. Read and accept the terms of the software license by clicking the "I Accept" button.
 3. On the "Software Licenses" page, select a criterion from the drop down menus to search for your license keys. You can search by Sales Order Number, by Serial Number (hardware or software) or several other criteria.

 To obtain all license keys for a cluster, including the Cluster Base Key, search using the related Sales Order Number. If you've added nodes to your cluster after your initial order, you may need to complete multiple searches.

1. Click "Go!" to bring your search and receive the software License Keys associated to the submitted criteria.

You will need your “NSS Credentials” to activate your GFC licenses.

Global File Cache - License Registration

License Registration

NetApp LMS Settings

License Information

Advanced Settings

☒ NSS Credentials ☐ GFC License Subscription

NSS username:

username

x

NSS password:

.....

☐ Update

SUBMIT

Click “**SUBMIT**” to complete the process.

Once completed, your licenses will be automatically activated for the LMS instance. Any subsequent purchases will automatically be added to your NSS credentials.

Update of NSS Credentials: Customers can change their NSS credentials by logging into <http://mysupport.netapp.com>. If changed, these credentials should be re-applied to License Management Server by visiting [https://\[ip address\]/lms/api/v1/config/lmsconfig.html](https://[ip address]/lms/api/v1/config/lmsconfig.html)

Global File Cache - License Registration

License Registration NetApp LMS Settings License Information Advanced Settings

☒ NSS Credentials ☐ GFC License Subscription

NSS username:

NSS password:

☒ Update

SUBMIT

Add the changed credentials in the username/password text box.
Click the 'Update' check box and then Click 'Submit' to complete the process.

Once completed, LMS service will restart and validate with the License server automatically an new credentials will be effective.

8. Configuring Capacity based licensing (CVEC)

Cloud Manager is used to deploy Cloud Volumes Edge Cache (CVEC) under a particular account id and a particular subscription as a PAYGO service. Once successfully deployed, CVEC is used as a backend file server that is provisioned with storage. Storage capacity provisioned in CVEC is converted into appropriate GFC Edge licenses based on the conversion factor. A minimum of 3TB should be provisioned that will provide 1 GFC license. and an additional GFC license for every 3 TB.

For example:

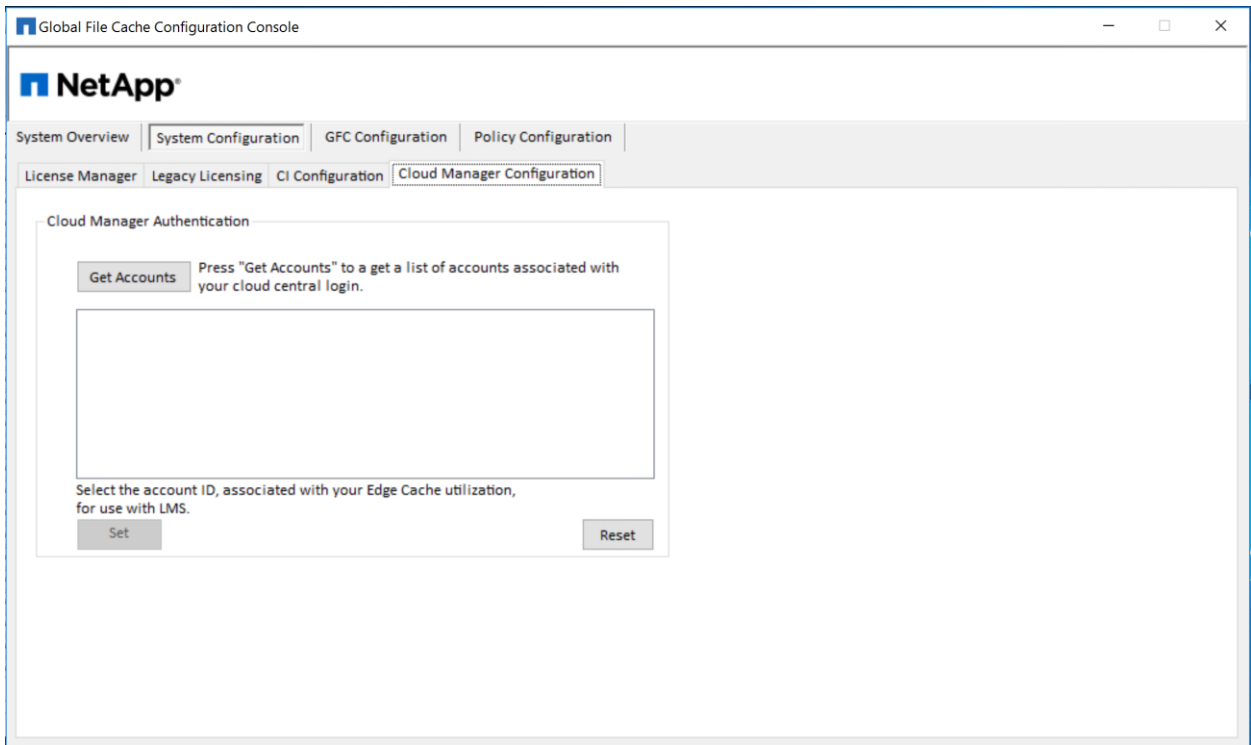
Case 1: if CVEC is provisioned with 4 TB of storage, then 1 GFC licenses are provided.

Case 2: if CVEC is provisioned with 22 TB of storage, then 7 GFC licenses are provided.

After successful CVEC deployment, further configuration should be performed on License Manager Server (LMS) instance

On LMS machine:

1. Open GFC Configuration Console.
2. Click System configuration in the main menu and and 'Click' Cloud Manager configuration.
3. Click 'Get Accounts' button to populate all accounts in the Configuration console.
4. Once populated, select the account that is used for querying provisioned storage on the CVEC.
5. After selection, click 'Set' button.



9. Configuring “NetApp LMS Settings” using Software Subscription Number

Once you have submitted your Customer ID to enable “**NetApp LMS**” license registration, you need to provide your “**GFC License Subscription**” details. These details will be supplied to you in the onboarding email as outlined below.



NetApp Support Site Available for GFC Customers

The NetApp Support Site is available for Global File Cache (GFC) customers. Please register for an account at this time.

Dear Customer,

Below are instructions on how to register for Support for your Global File Cache product/offering. We are in the process of transitioning systems. As a result, there are two identifying numbers that you will need.

1. Your NetApp GFC Software Subscription Number: **A-S00008405**
2. Your NetApp GFC Serial Number: **9650000000000008405**.

You will use a serial number as a unique identifier when contacting NetApp support. To ensure a seamless support experience, please use your serial number when following the guidelines in this email.

Activating Support Entitlement for your NetApp GFC serial number

You will need the “GFC Software Subscription Number” to activate your GFC licenses.

Global File Cache - License Registration

License Registration

NetApp LMS Settings

License Information

Advanced Settings

☐ NSS Credentials ☒ GFC License Subscription

GFC License Subscription:

A-S00008405

SUBMIT

Click **“SUBMIT”** to complete the process.

Once completed, your licenses will be automatically activated for the LMS instance. Any subsequent purchases will automatically be added to the GFC License Subscription.

Configuring “NetApp LMS Settings” using Software Subscription Number

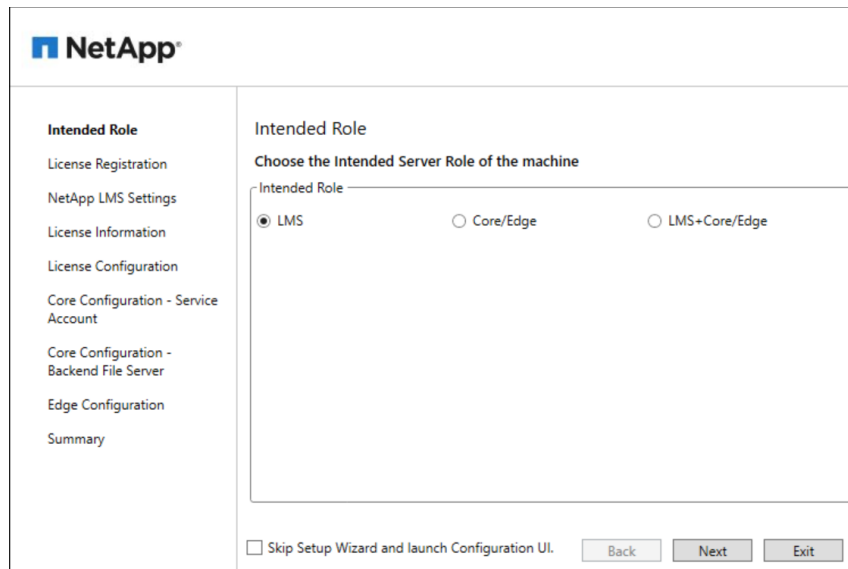
6 Initial Configuration

6.1 Initial Configuration Wizard

NetApp Global File Cache (GFC) includes a 'Configuration Wizard' for pristine installations of the software. This wizard will guide you through the process of License Manager Server (LMS) Configuration, associating GFC instance with existing license manager (see Section 5) and quickly deploy core or edge instances.

Once you completed the deployment of the GFC virtual instance and committed a reboot, you can start the configuration wizard by clicking the **Configuration Console** icon on the desktop.

1. Click on "Global File Cache Configuration" icon on Desktop.
2. In the opening screen, wizard provides three options to select from:
 - a) LMS
 - b) Core
 - c) (LMS+Core)



3. Based on the selection, wizard will appropriately show the screens for configuration.
4. Follow the steps prompted to complete the licensing configuration using the IP address of your LMS instance and the customer ID provided by GFC.
5. Based on your selection GFC Edge or Core instance, you will be guided through the process of deploying basic settings associated with the configuration.

Note: You may skip the Configuration Wizard and launch the GFC Configuration UI by checking the box on the initial Configuration Wizard screen and clicking "Exit".

6.2 Global File Cache Configuration Console

Once the initial configuration wizard has completed or you've selected "**Legacy Licensing**" during the wizard, you can launch the **Configuration Console** from the desktop. The Configuration Console allows you to configure basic System Settings, GFC Core and Edge settings (See also Section 7):

GFC Core Instance

1. Provide the Service Account.
Must be a member of backup operators' group on the datacenter file server (i.e. FS1).
2. Add the file server to the list of backend file servers i.e., FS1.
3. Configure Global / Server Exclusion Lists or Remote Inclusion Lists.
4. Configure Selectable File Handling.
5. Schedule Pre-population jobs.
6. Configure advanced options

GFC Edge Instance

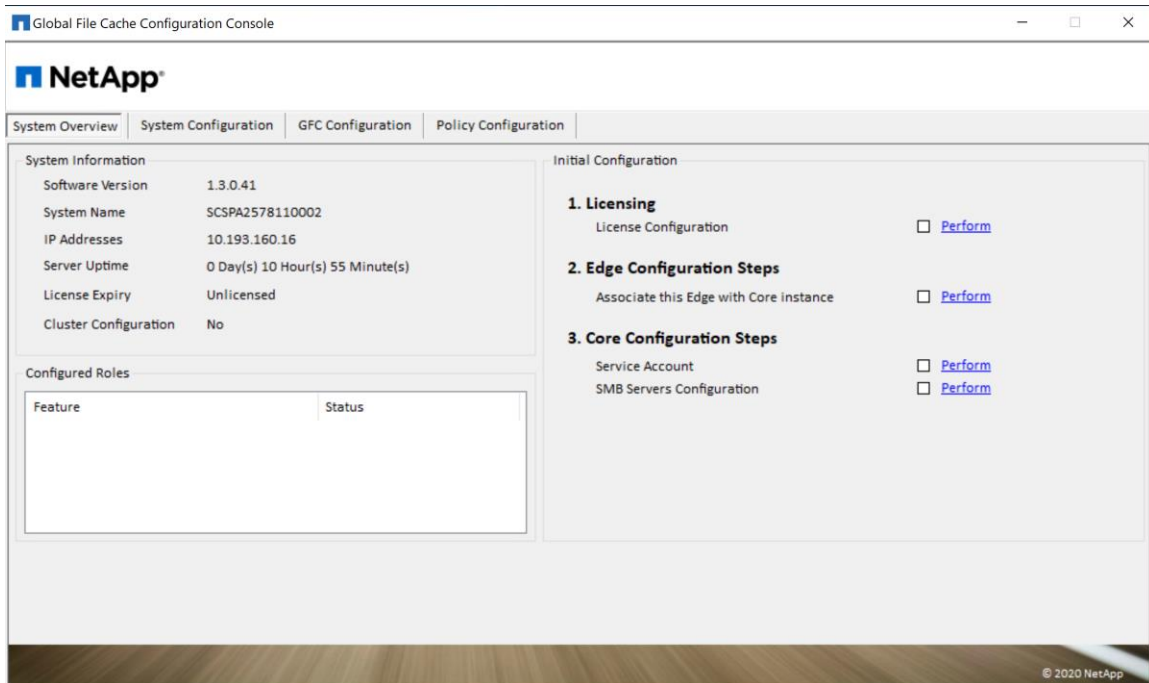
1. License the Edge Instance (LMS or Legacy).
2. Configure Edge sync settings.
3. Associate the Edge instance with the Core instance at the datacenter or in the cloud.
 - a. Cloud Fabric ID (Location)
 - b. IP Address / FQDN of the GFC Core instance
4. Pre-population jobs
5. Advanced Settings
6. Configure Throttling settings
7. Configure Cache Cleaner settings

Registering your GFC Core or Edge instance with GFC LMS

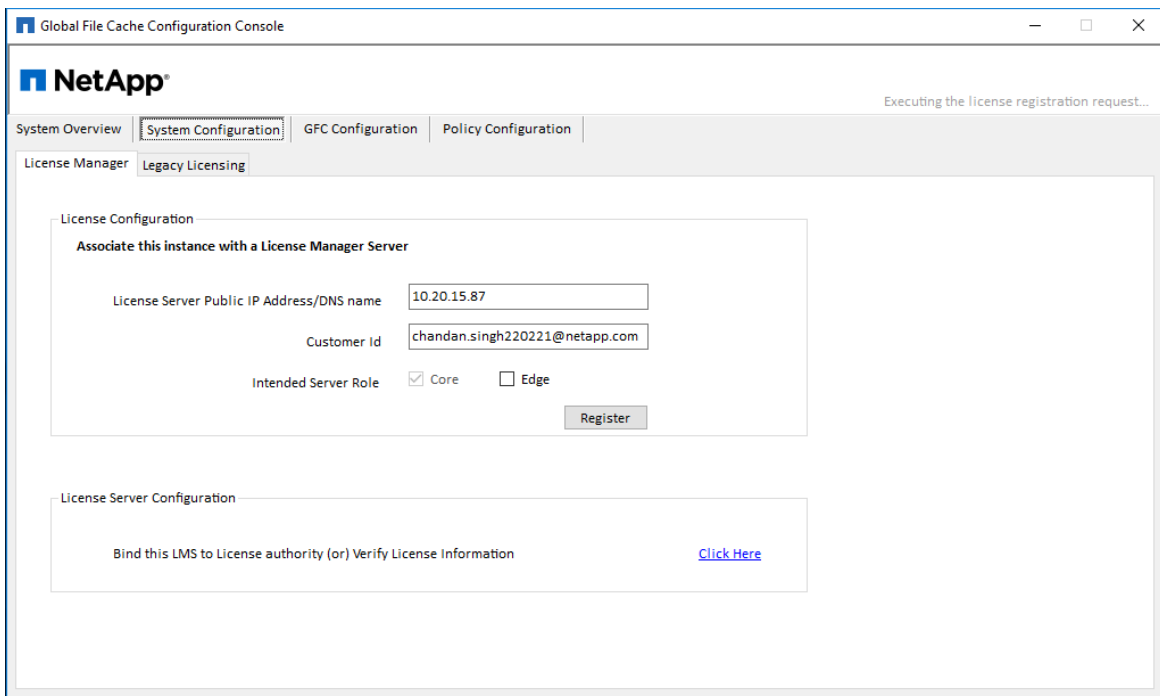
Note: The following steps are only required if you skipped the initial configuration wizard or upgraded from a previous release.

Now that the GFC LMS is correctly registered and associated with the subscription service, you need to license the first host in the environment, which is typically the Core instance.

1. Open the **Configuration Console** from the desktop.



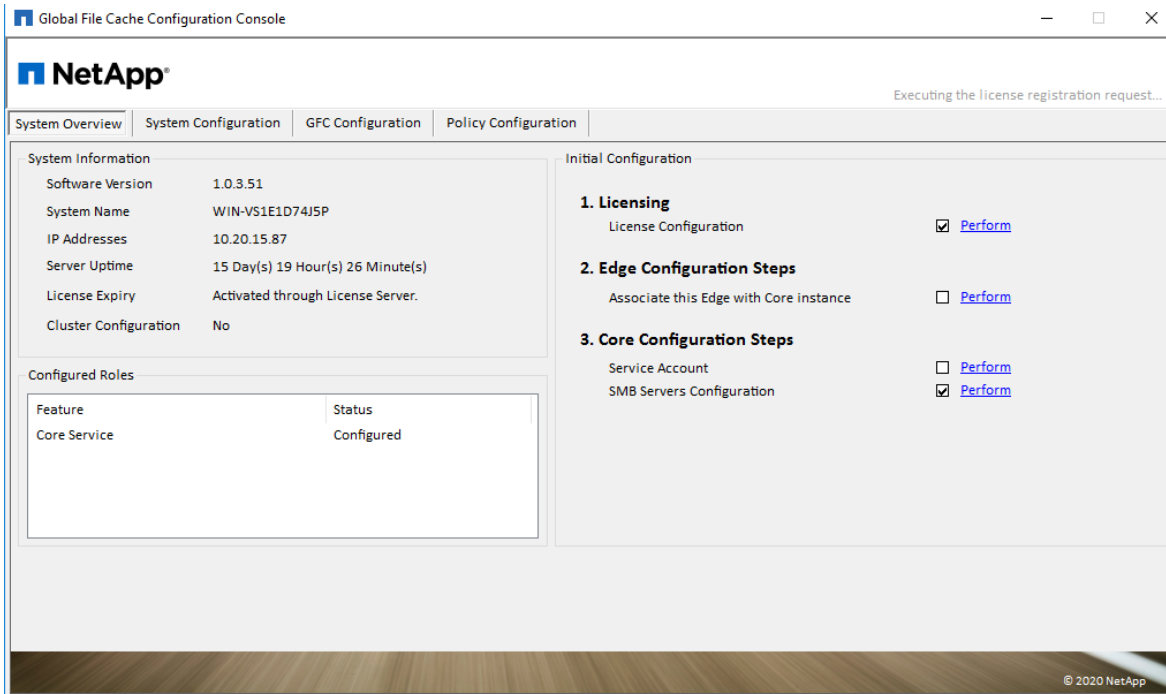
2. Click on “**Perform**” next to License Configuration in the Initial Configuration section or navigate to the “**System Configuration**” tab, which opens the License Manager tab.



3. Provide the IP address of the GFC LMS instance, i.e. 1.2.3.4 and Customer ID (i.e. XYZINC)
4. Select the intended server role, Core or Edge and click “**Register**” to confirm.

Once this GFC instance has been configured it will register with the GFC LMS instance and a confirmation message is shown that the site has been registered successfully.

5. Click “OK” to close this message.



6. Once completed you can check that the licensing has been completed by navigating back to the “**System Overview**” tab of the GFC Configuration Console. License Expiry will display “**(Activated through License Server)**”.
7. Repeat this process “**Registering your GFC Core or Edge instance with GFC LMS**” for each GFC instance in your environment.

Note: The configuration of the GFC core or edge instances can be automated through either GPO or PowerShell Desired-State Configuration. Consult your GFC Solutions Engineer or NetApp Support to discuss the options.

7 Designing and Deploying NetApp Global File Cache Core

Depending on your requirements you may need to deploy one or multiple NetApp Global File Cache (GFC) core instances to create the GFC Fabric. The core instance is designed to act as a 'traffic cop' between your distributed GFC edge instances and the datacenter file server resources, i.e. file shares, folders and files.

The GFC core instance creates the GFC Fabric which allows customers to centralize and consolidate unstructured data into a 'single set of data,' whether it resides on one or multiple storage platforms in the on prem, hybrid or public cloud.

When you are designing your GFC deployment you need to determine what's right for your environment in terms of scale, availability of resources and in terms of redundancy.

GFC core can be deployed in the following ways:

GFC core stand-alone instance.

GFC core Load Distributed design (Cold Standby).

Note: It is recommended to deploy GFC core instance as a virtual machine on a hypervisor platform that leverages high availability options.

7.1 GFC Core Stand-Alone Instance

When deploying a GFC core stand-alone instance, you need to provision a single virtual machine, either by deploying Windows Server 2016 Standard or Datacenter Edition or Windows Server 2019 Standard or Datacenter Edition or using the GFC.OVA or .VHD template which includes the three Windows Server operating system of choice and GFC.

Quick steps:

1. Deploy GFC Virtual Template or Windows Server 2016 virtual machine or Windows Server 2019 Standard or Datacenter edition
2. Ensure virtual machine is connected to the network, joined to the domain and accessible through RDP.
3. Optionally, if the VM is not joined to domain, username and password, that is added to local Backup Operators group on the backend is used.
4. Install the latest GFC Software Installation Package (Update)
5. License the GFC instance through the License Manager Server (see Section 5)
6. Configure the GFC Core role.

7.2 GFC Core Load Distributed Design

Enterprise customers that require multiple GFC core instances to ensure optimal scalability for their environment can leverage a distributed model of multiple core instances, including a cold-standby for disaster recovery. This model can also be leveraged to design a multi-fabric deployment with multiple active/active datacenters or to failover to a DR site, either in a separate location or in the cloud.

The model below allows you to provision multiple (i.e. region-specific) core instances, distribute the load between edges in a specific region to access the central data sets provided by the GFC Fabric.

In case a GFC core instance fails, and can't recovered in time, you can 'replace' the failed GFC core instance with a 'cold' standby instance by either changing the IP address of the 'cold' standby instance or updating the DNS record associated with the edge-to-core association (i.e. IP address, Cloud Fabric ID configured on the edge).

Note: Consult your GFC Solutions Engineer to discuss the best options for your enterprise deployment

7.3 Configuring GFC Core instance – Service Account

Once you have identified the right deployment strategy for your organization, provisioned the required VM instances, and have completed the licensing part (LMS), you need to start the core configuration.

When a GFC instance is designated the Core role, GFC Edge instances will connect to it to access datacenter fileserver resources. The services on this instance run as a specific domain user account. This account, also known as the “Service Account”, must have the following privileges on each of the SMB servers that will be associated with the GFC Core instance:

1. The provisioned Service Account must be a domain user.
Depending on the level of restrictions and GPOs in the network environment, this account may require domain admin privileges.
2. It must have “**Logon as a Service**” privileges.
3. The password should be set to “**Never Expire**”.
4. The account option “**User must change password at next logon**” should be **DISABLED** (unchecked).
5. Must be a member of the backend fileserver local **Backup Operators** groups.
6. Any shares that will be exposed through GFC must allow the “**Everyone**” group “**Full Control**” at the share level, while restricting permissions through NTFS permissions.

To configure the Service Account on your core:

1. Click the tab “**System Overview**” and click “**Perform**” next to the unchecked “**Service Account**” step listed in the “3. Core Configuration Steps” section of the Initial Configuration assistant.
2. This opens a new tab, “**GFC Core**” and shows the section “Service Account”. Enter the **User Name** and **Password** of the Service Account created in Active Directory.
3. Click “**Apply**” and confirm the configuration of the Service Account.

The screenshot displays the NetApp Global File Cache Configuration Console. The top navigation bar includes 'System Overview', 'System Configuration', 'GFC Configuration', and 'Policy Configuration'. The 'GFC Configuration' tab is active, showing 'GFC Core' and 'GFC Edge' sub-tabs. The 'Service Account' section is selected in the left sidebar. The main content area is titled 'Service Account' and 'Configure Core instance Service Account'. It contains fields for 'Domain Name' (MFLAB), 'User Name' (LocalSystem), and 'Password' (masked with dots). An 'Apply' button is located to the right of the password field. A status message at the top right indicates 'Executing the license registration request...'.

7.4 Configuring GFC Core instance – Backend File Servers

GFC core instances extend central file shares from configured datacenter backend file servers. GFC can also be configured in multiple ways to present a local share or an iSCSI LUN.

Please follow the steps below to connect file servers to the GFC Core instance.

1. Click the **“Backend File Servers”** item in the **“GFC Core”** tab of the Configuration Console or use the **“Backend File Servers Configuration”** step listed in the **“3. Core Configuration Steps”** section of the Initial Configuration assistant.
2. Select **“Generic SMB,”** or **“DAS/iSCSI Mount,”** depending on the backend file server to be added.

The screenshot shows the NetApp Global File Cache Configuration Console. The main navigation bar includes 'System Overview', 'System Configuration', 'GFC Configuration', and 'Policy Configuration'. Under 'GFC Configuration', there are tabs for 'GFC Core' and 'GFC Edge'. A left sidebar lists various sections, with 'Backend File Servers' highlighted. The main content area is titled 'Backend File Servers' and contains two sections: 'Add New Backend' and 'Configured Backend Servers'. The 'Add New Backend' section has a dropdown menu set to 'Generic SMB' and a 'New Backend Settings' form with fields for 'NetBIOS / FQDN', 'Local UserName', and 'Password(optional)'. An 'Add' button is to the right. The 'Configured Backend Servers' section shows a table with columns 'Backend Server' and 'Local Path'. One entry is visible: '127.0.0.1'. A 'Delete' button is at the bottom right.

3. To add a generic SMB server, provide a NetBIOS name or FQDN in the **“Add New Backend”** field containing the backend file server to publish throughout all connected GFC Edge servers.
4. Click the **“Add”** button to add the server to the **“Configured Backend Servers”** list. The changes are applied directly to the GFC Core server configuration without displaying a confirmation box.
5. To add data from a local path or resource, select **“DAS/iSCSI Mount”** from the dropdown and enter the Storage Name of the resource name as you wish it to display. Enter the path of the resource (Ex. F:\Data) containing shares and click **“Add.”** The changes are applied directly to the GFC Core server configuration without displaying a confirmation box.

For DAS/iSCSI configuration, a storage volume and NTFS filesystem must have already been created on the local GFC core instance prior to this configuration.

Note: You must allow the **“Everyone”** user group **“Full Control”** permissions on the ACL of each share on the backend file server.

Note: Using a DFS root or alias as your backend file server is not recommended and can lead to data loss.

7.5 GFC Core Advanced Features

Note: The following advanced Core features must be configured identically on each Core server if utilizing Microsoft Cluster Services.

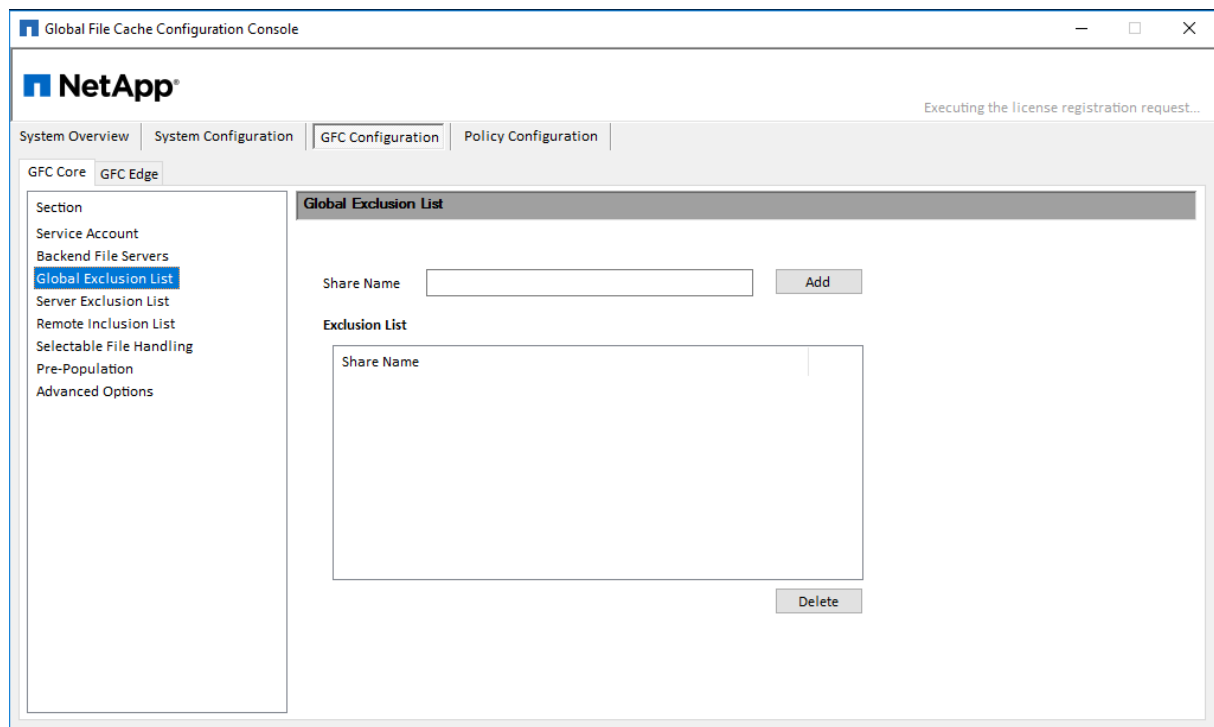
7.6 Global Exclusion List

The Global Exclusion List feature allows SMB/CIFS file server shares to be hidden from all GFC Edge servers, and subsequently from branch office end user clients. The shares with the configured names will not be available through GFC from any datacenter file server configured to the GFC Core server.

This feature may be used when there are multiple file shares with the same name on several backend file servers.

1. To hide named shares from all Edge instances.
2. Open the **Configuration Console**.
3. Select the “**Configuration**” tab and ensure that the “**GFC Core**” tab is active.
4. Click “**Global Exclusion List**”.
5. Enter a “**Share Name**” to prevent distribution through GFC.
6. Click “**Add**” to add a share name to the exclusion list.

Once added to the list, the change is applied.



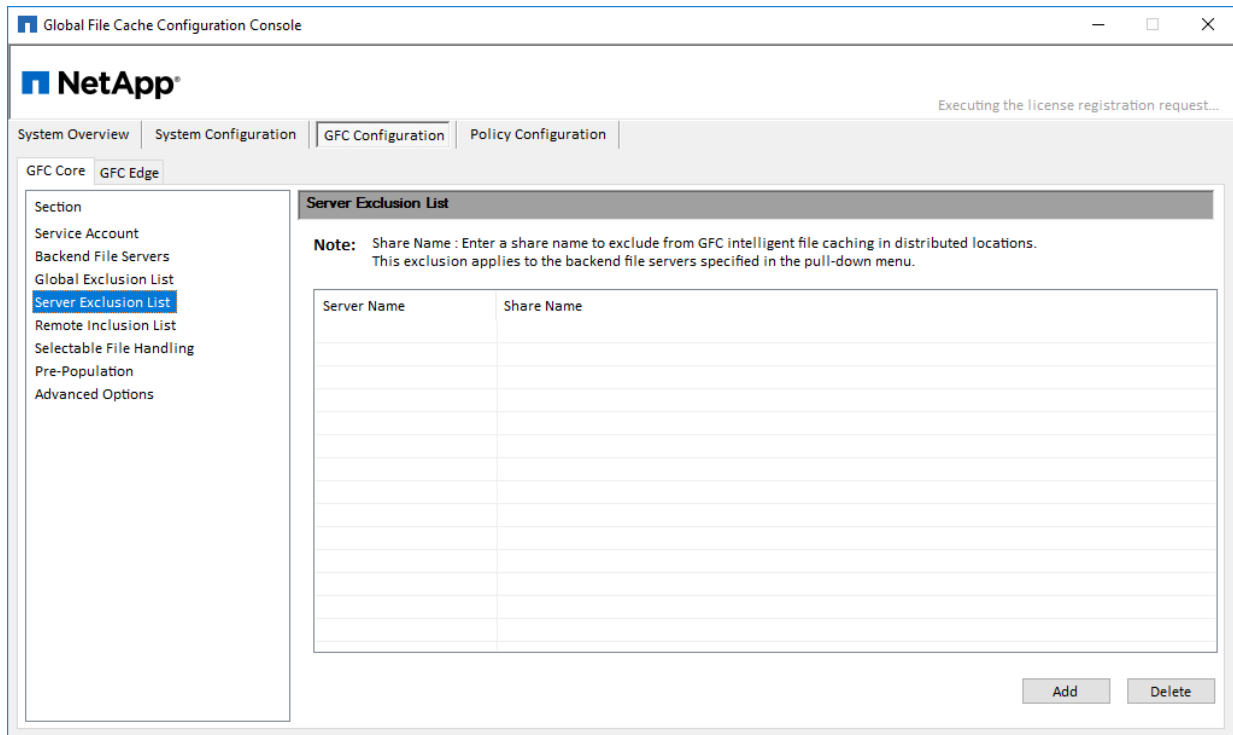
7.7 Server Exclusion List

The Server Exclusion List feature prevents specified shares from individual SMB/CIFS file servers from being shared with Edge servers via GFC. This feature can be used to achieve a level of granularity in control of what shares are presented as available via GFC to end users.

To hide specific shares from all Edge instances

1. Open the **Configuration Console**.

2. Select the **“Configuration”** tab, and select the **“GFC Core”** tab.
3. Click **“Server Exclusion List”**.
4. Click the **“Add”** button to display the **“Add Server Exclusion List”** window.
5. Select the desired backend file server from the dropdown menu.
6. Enter a **“Share Name”** to prevent distribution through GFC.
7. Click **“Apply”** to add a share name to the exclusion list.
Once added to the list, the change is applied.
8. Repeat this process for each server and share combination you wish to exclude.



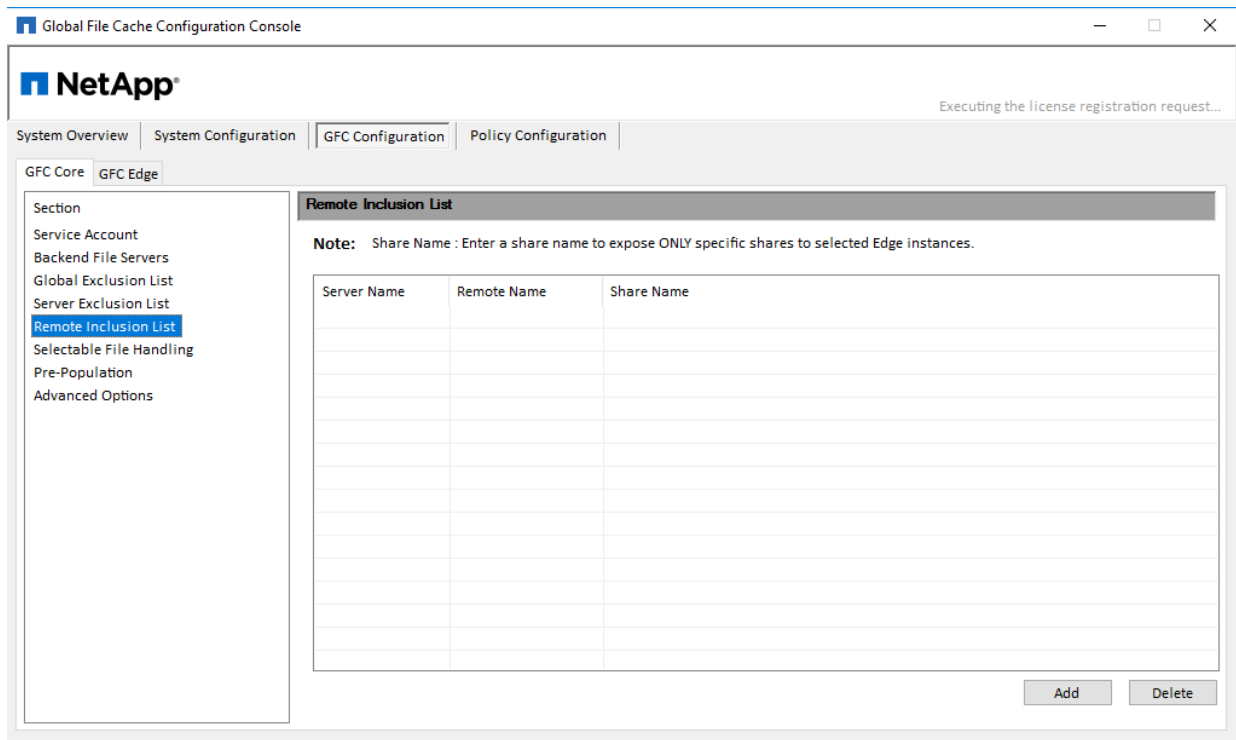
7.8 Remote Inclusion List

The Remote Inclusion List feature in GFC provides a method of control to expose specific shares to specified Edge servers. These may be used in the case where a branch office needs access to a share that has previously been excluded or a specific named share.

To allow inclusion of specific shares to specific Edge instances

1. Open the Configuration Console.
2. Select the **“Configuration”** tab, and select the **“GFC Core”** tab.
3. Click **“Remote Inclusion List”**.
4. Click the **“Add”** button to display the **“Add Remote Inclusion List”** window.
5. Select the desired backend CIFS file server from the dropdown menu.
6. Select a target Edge server **“Remote Name”** from the second dropdown menu.
7. Enter a **“Share name to include”** that exists on the datacenter file server in the dropdown menu.
8. Click **“Apply”** to add a share name to the inclusion list.
Once added to the list, the change is applied.
9. Repeat this process for each server and share combination you wish to include.

Figure 8)



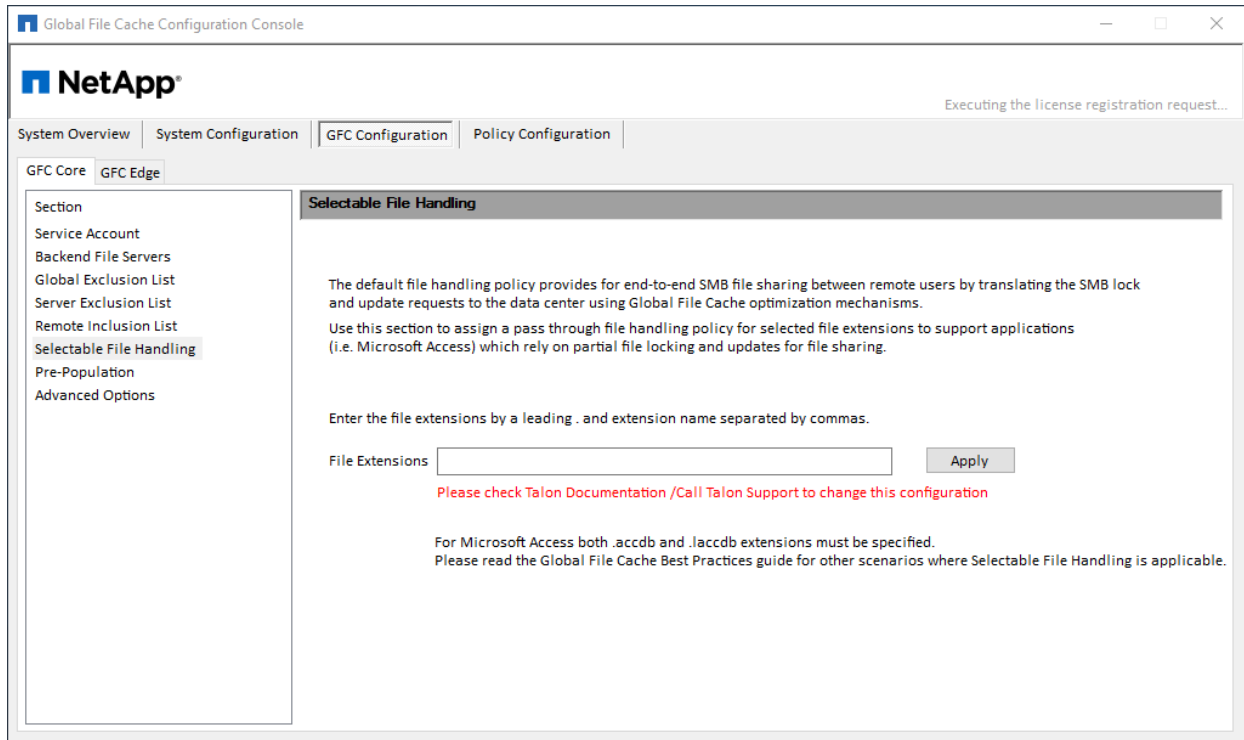
7.9 Selectable File Handling

Certain applications, such as Microsoft Access or Autodesk Revit, rely on partial file locking and partial file updates for file sharing coherency. In order to use these kinds of applications with GFC, you must first disable file locking for the file extensions associated with the application. Pass-through policies are applied to file patterns globally and cannot differ between Edge servers attached to the configured Core.

To modify Selectable File Handling

1. Open the **Configuration Console**.
2. Select the **"Configuration"** tab, followed by selecting the **"GFC Core"** tab.
3. Click **"Selectable File Handling"**.
4. Enter the file type extensions (used by the application) separated by commas and preceded by a period in the **"File Extensions"** text box.
5. Click **"Apply"** to apply the settings, a confirmation box will appear.
6. Click **"Yes"** to apply the changes immediately.

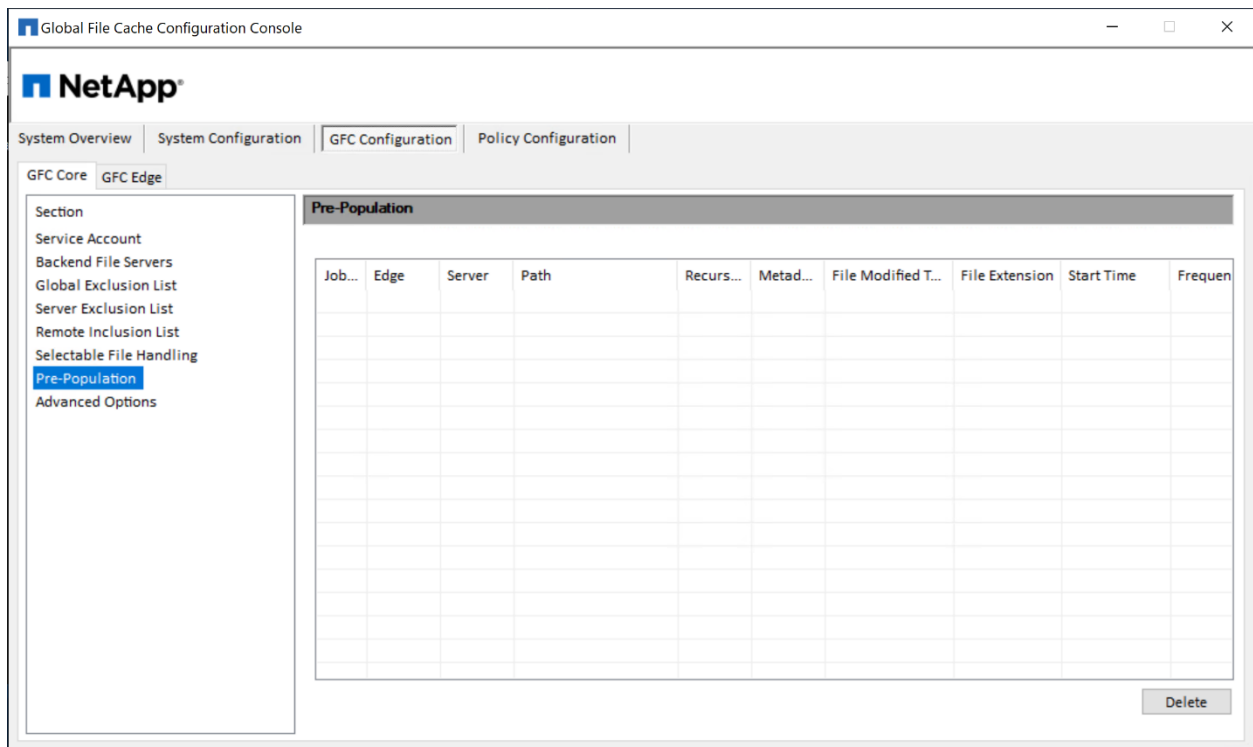
Figure 9)



7.10 Pre-population (legacy)

The pre-population feature updates shares, directories, folders, and/or files from datacenter servers to the branch office Edge server(s) at predetermined times and frequencies. This pre-populates GFC Edge caches with data that will be used by their connected clients, creating a 'warm' cache on the Edge server. Branch office clients access files from the warm cache much faster than 'cold' files, those that need to be fetched from datacenter servers and then sent over the WAN.

Pre-population jobs that were scheduled prior to release 1.0 will be shown in this section. For more information about Add/Edit/Delete using Next Generation Prepopulation, please consult Section 9 of this user guide.

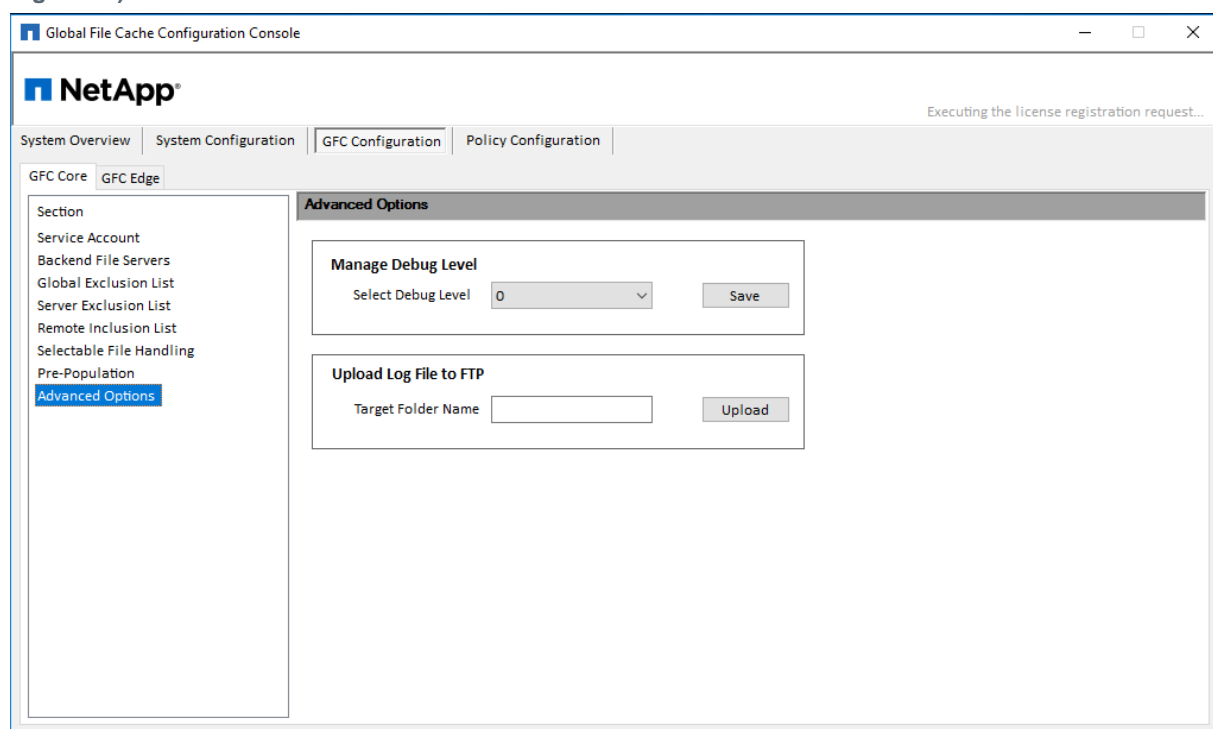


7.11 Core Advanced Options

Advanced Options give IT Administrators the ability to set the desired Debug Level for additional NetApp Support or Engineering information or troubleshooting. Additionally, a customer-specific folder can be automatically created, and relevant debug logs automatically uploaded using the associated Advanced Options.

Note: These should only be modified or utilized as instructed by a member of NetApp Support. Please contact NetApp Support for any questions or prior to sending any log files.

Figure 10)



Manage Debug Level

This feature allows for more verbose (higher numbers, MAX: 9) debug logging.

Upload Log File to FTP

This feature enables a direct transfer of requested log files to NetApp Support.

8 Designing and Deploying NetApp Global File Cache Edge

Depending on your requirements you may need to deploy one or multiple NetApp Global File Cache (GFC) edge instances based on the concurrent user sessions in a branch office. The edge instance presents the virtual file share to the end users within the branch office which has been transparently extended from the associated GFC core instance. The GFC edge should contain a “D:\” NTFS Volume which contains the cached files within the branch office.

For the GFC edge it is important to understand the sizing guideline in Section 3.4 of the User Guide. This will assist in making the correct design for your GFC deployment. You would also need to determine what's right for your environment in terms of scale, availability of resources, and in terms of redundancy.

GFC edge can be deployed in the following ways:

GFC edge stand-alone instance.

GFC edge multi-edge deployment.

8.1 GFC stand-alone instance

When deploying a GFC edge stand-alone instance, you need to provision a single virtual machine, either by deploying Windows Server 2016 Standard or Datacenter Edition or Windows Server 2019 Standard or Datacenter Edition or using the GFC.OVA or .VHD template which includes the three Windows Server operating system of choice and GFC.

Quick steps

1. Deploy GFC Virtual Template or Windows Server 2016 virtual machine or Windows Server 2019 Standard or Datacenter edition.
2. Ensure virtual machine is connected to the network, joined to the domain and accessible through RDP.
3. Install the latest GFC.
4. License the GFC instance through the License Manager Server (see Section 5).
5. Configure the GFC Edge role.

8.2 GFC Edge Multi-Edge Deployment

For sites that have more users than the sizing guidelines dictate ‘concurrent sessions’ AND the datasets are used by all of the users, meaning we can't separate the data to be associated with specific groups of users (i.e. Share1 is only used by Group HR which is only **X** users, and Share2 is only used by Group Finance which is **Y** users), we recommend to extend the user's sessions to a secondary (or 3rd) edge using a local Stand-alone DFS namespace in the respective site.

This means each GFC Edge instance is configured as a ‘stand-alone’ server instance in that site, with a unique NetBIOS name and IP address for each Edge instance and a dedicated cache volume for each separate Edge instance, which subsequently presents the local FASTData virtual file share(s) as part of a local stand-alone DFS root, which includes all of the feasible targets in that site as a valid target.

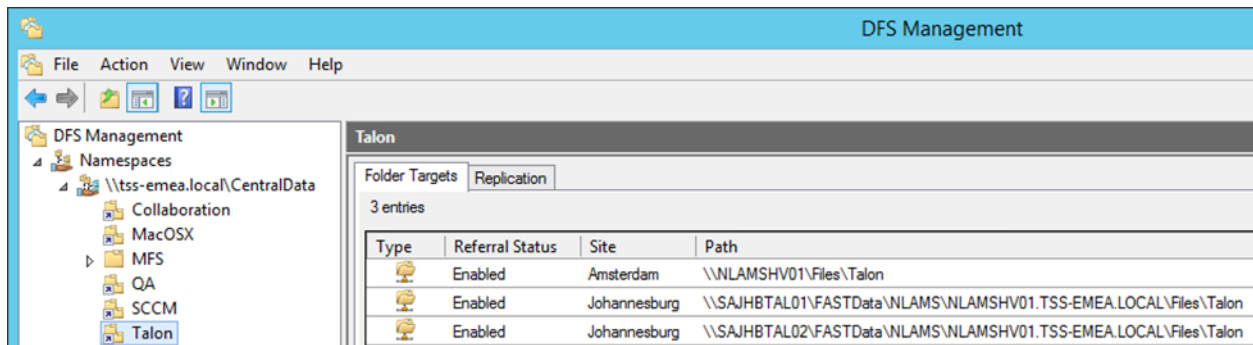
Each edge instance presents the central data hosted on the backend file server platform through a unique UNC path:

Edge1: \\Edge1\FASTData\Talon\FS1\Share\Folder\

Edge2: \\Edge2\FASTData\Talon\FS1\Share\Folder\

Edge3: \\Edge3\FASTData\Talon\FS1\Share\Folder\

Figure 11)



In order to facilitate for load balancing, a local stand-alone DFS namespace needs to be configured on each GFC edge instance, meaning that each edge hosts a DFS root that contains a DFS link with the primary target (the local FASTData share or subfolder on that Edge) and secondary targets (corresponding FASTData share or folder on other edges in that site).

This model allows it to actively distribute the load between stand-alone DFS-N targets, which means that User1 will use Edge1 and User2 will use Edge2, etc. This selection is based on the round-robin principle, which means that User1 could use Edge2 any other time of day as the cache timer expires for the namespace and associated targets. In that case it could be that a file that was previously warm (on Edge1) is now cold (on Edge2). If you schedule a nightly pre-population job you can overcome the cold files when users logging in in the morning.

Note: One of the requirements for this model is that local stand-alone namespace “**Random Order**” (rather than “**Lowest Cost**”) distributes the users across multiple edge instance instead of having userA to userE use Edge1, userF to userJ use Edge2, etc.

Stand-alone DFS Namespace should be configured as follows:

Namespace: \\Edge[X]\CentralData\

(Random when using Round-Robin)

Folder: Talon

Referrals:

\\Edge1\FASTData\Talon

\\Edge2\FASTData\Talon

\\Edge3\FASTData\Talon

Figure 12)

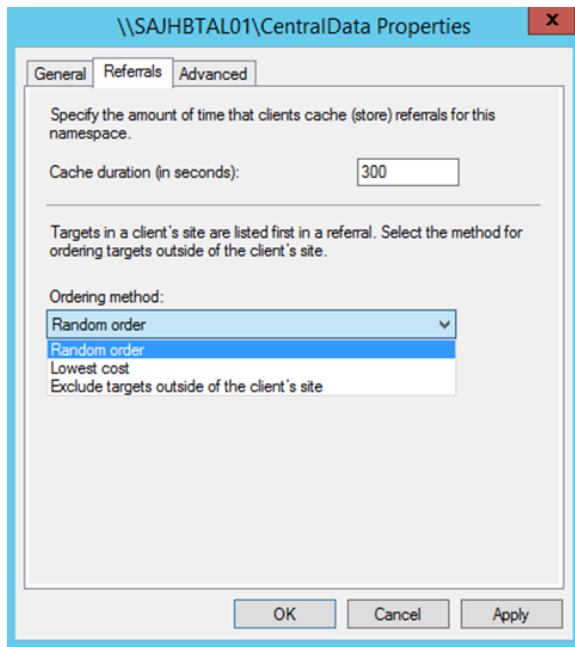
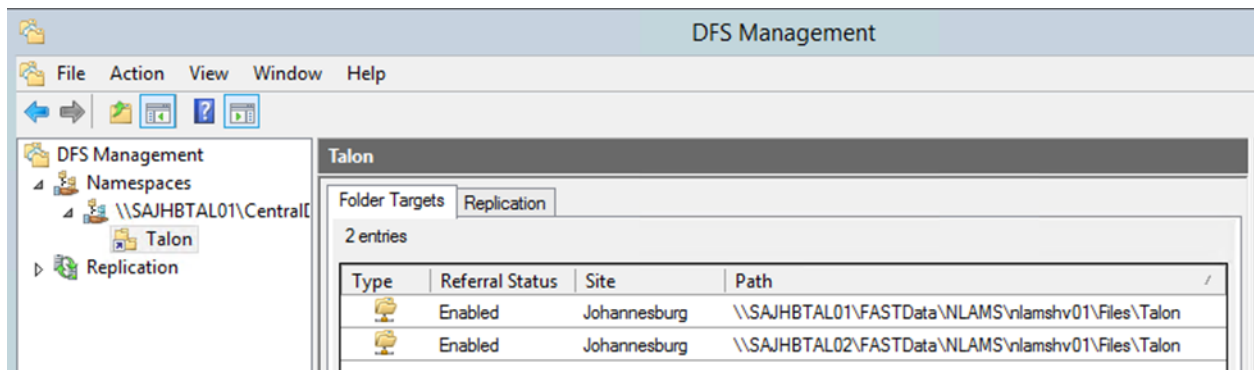


Figure 13)



Domain-Based DFS Namespace

The primary Stand-alone DFS target (\\Edge1\CentralData\Talon\FS1\Share\Folder) can then be added to the domain-based DFS namespace structure, which will subsequently resolve to the site where both end users and multiple edge instances reside in. For the Domain-Based DFS namespace it's important **"Exclude targets outside the client side"** is enabled on the DFS folder to reduce the list of feasible targets for a specific client workstation and its partition knowledge table to which the DFS-N resolves.

E.g. \\domain.local\MFS\Share\ is defined as a folder in the Domain-Based DFS- namespace, using the following referral(s):

```
\\Edge1\CentralData\Talon\FS1\Share (enabled)
\\Edge2\CentralData\Talon\FS1\Share (enabled)
\\Edge3\CentralData\Talon\FS1\Share (enabled)
\\FileServer\FS1\Share (last among all targets) <- native target
```

Figure 14)

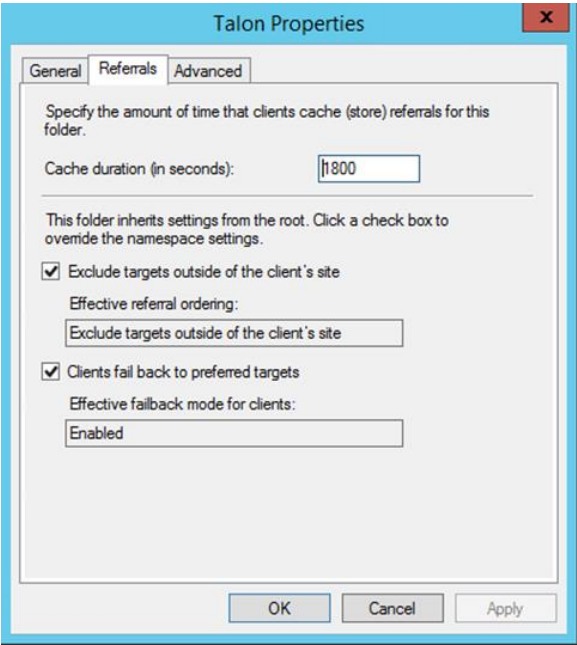
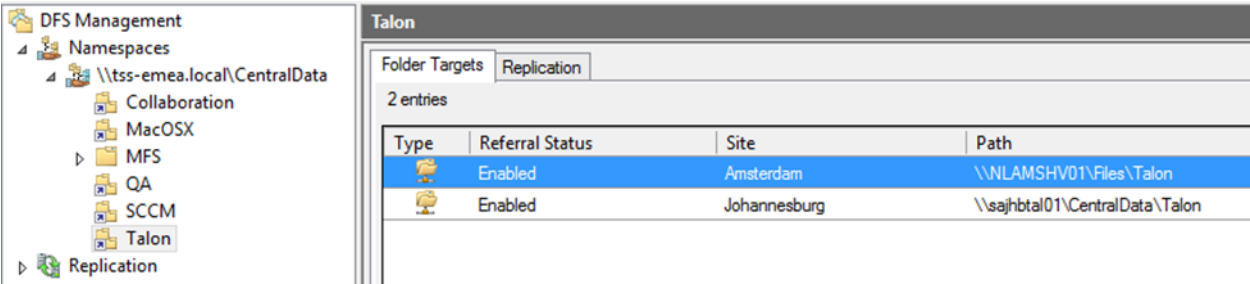


Figure 15)



Redundancy Options

For the purpose of redundancy, you can add the same standalone configuration to Edge2 and Edge3 and integrate them as referrals in the Domain-Based DFS-Namespace. Because each edge instance contains the 'same' local stand-alone DFS namespace, the users will enumerate the 'nearest' or preferred stand-alone DFS namespace server, i.e., `\\Edge1\CentralData\Talon\FS1\Share` which subsequently points to `\\Edge1\FASTData\Talon\FS1\Share` or `\\Edge2\FASTData\Talon\FS1\Share` if the user limit is exceeded.

In a nutshell, the local user maps to the Domain-Based DFS namespace, which has a referral to the local stand-alone DFS namespace, the local DFS namespace uses round-robin to distribute the users between all available edges, subsequently presenting the local edge FASTData virtual file share to the users.

In case of a full site outage, when all Edge instances in a respective site are down, the client will enumerate the `\\BackendFileServer\FS1\Share` target as “last among all targets” referral and point users directly to the backend file server in the datacenter.

Note: For more details relating to DFS Namespace refer to Section 3 of this user guide

8.3 Configuring the GFC Edge Role

Note: The Edge instance must be licensed prior to beginning the configuration. For more information on licensing, see “Registering your Core or Edge instance with GFC LMS.”

When a GFC instance is designated the Edge role, it will connect to a GFC Core to provide users at the branch office access to datacenter file server resources.

To configure the Edge Instance Role:

1. Click “**Perform**” next to the unchecked “**Core Configuration**” step listed in the “2. Edge Configuration Steps” section of the “Initial Configuration” assistant
2. This opens a new tab, “**GFC Edge**,” and shows the section “**Core Instances**”
3. Provide the **Cloud Fabric ID** of the GFC Core server. The Cloud Fabric ID is typically the NetBIOS name or the geographical location of the backend file server
4. Provide the **FQDN/IP Address** of the GFC Core server or cluster
 - c. (Optional) Check the “**SSL**” box to enable SSL support for Internet connections from the Edge to the Core
 - d. (Optional) Enter the User Name and Password which are the credentials of the Service Account used on the Core
5. Click “**Add**” to confirm the addition of the GFC Core appliance. A confirmation box will appear. Click “**OK**” to dismiss it

Global File Cache Configuration Console

NetApp

System Overview | System Configuration | GFC Configuration | Policy Configuration

GFC Core | GFC Edge

Section

- Core Instances
- Pre-Population
- Advanced Options
- Throttling
- Cache Cleaner

Core Instances

Core Auto Configuration ☐
(Requires License Manager Server)

Associate this Edge instance with a Core

Cloud Fabric ID

FQDN / IP Address

Enabled SSL ☐

User Name (Optional)

Password (Optional)

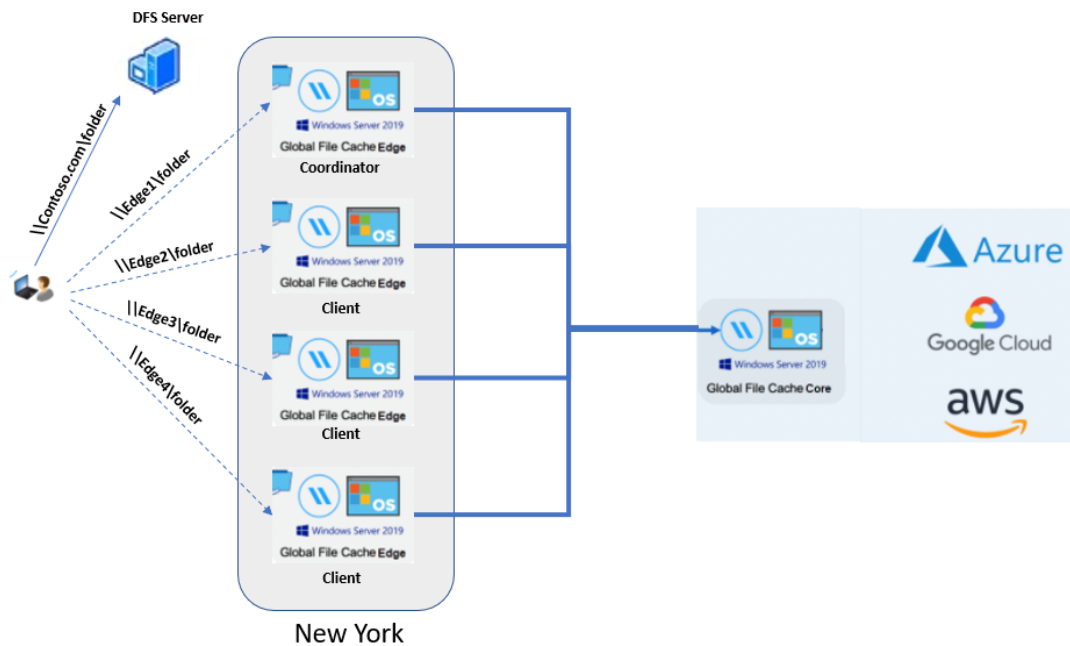
Cloud Fabric ID	FQDN/IP Address	SSL Enabled
<input type="checkbox"/> core-87	10.20.15.87	0

8.4 GFC Edge Advanced Features

Note: Edge instances should be configured the same to maintain consistency within large scale deployments. Specific parameters can be set on a per Edge basis. For example, 'Cache Cleaner' can vary between sites or edge instances.

Edge Sync Settings

Edge Sync settings should be configured when more than one Edges are in a particular geographical location connecting to same fabric Id or GFC Core. This topology is recommended in a large site with more than mentioned in the sizing guidelines for GFC Edge. GFC Edges are configured in a scale out model and users connect to GFC Edge using DFS namespace. Users connect to the Edge using DFS namespace or via static mapping. If mapped via DFS namespace, then the user is not guaranteed to map to same Edge every time they login because of DFS costing. User may end up on an Edge that may not be up to date and the data may not be cached. If "Edge Sync" feature is enabled, all edges participating in this feature will have latest data on cache. Users will see the same warm performance when they connect any edge, as the data is update and cached.



One Edge is nominated as "Coordinator" and all Other Edges should be configured as "Client".

Coordinator will communicate with all Clients and provide the relevant information to keep the cache up to date. Usually, the first Edge that is configured can be additionally configured as "Coordinator" and all other Edges as "Client".

To Enable Edge Sync coordinator setting:

- a. Click the “Enable coordinator” check box.
- b. Click “Add”

To Enable Edge Sync client setting:

1. Please enter Coordinator IP Address in the text box.
2. Click “Add”.

To Enable Metadata Sync only:

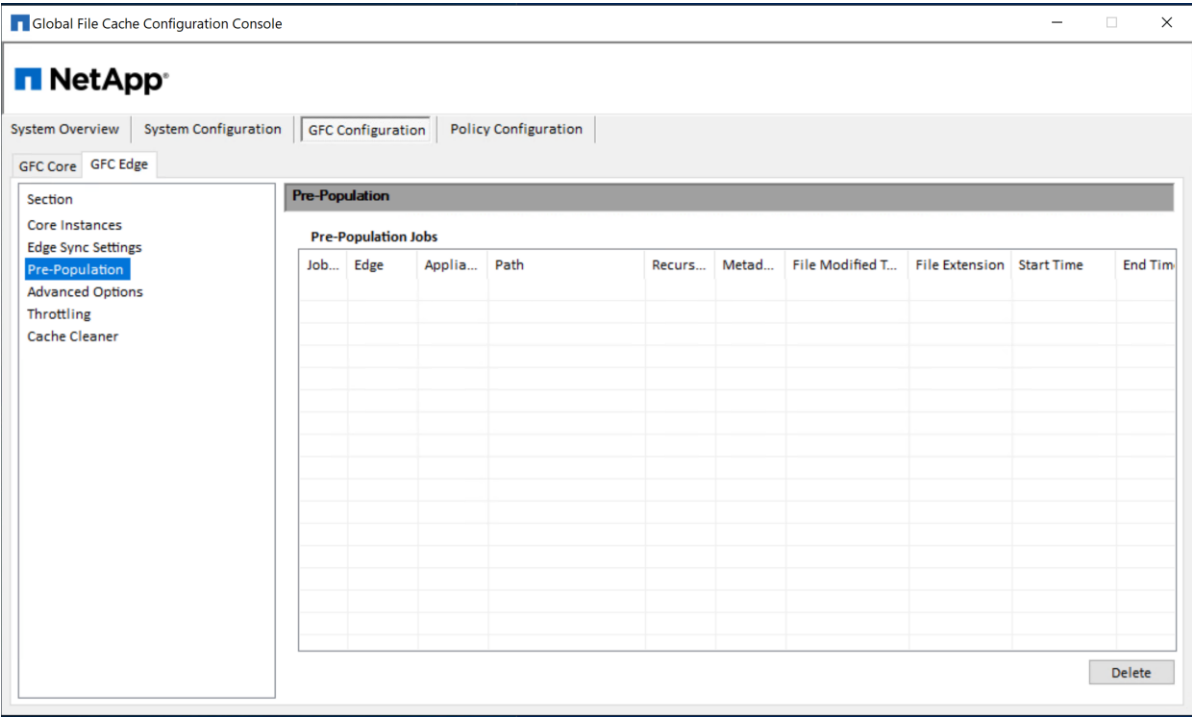
- a. Click the “Enable Metadata Sync” check box.
- b. Please enter Coordinator IP Address in the text box (if not added)
- c. Click “Add”.

When a GFC Edge that is designated as coordinator becomes offline, then the file synchronization among all the client nodes will fail. Files on the edge would remain cold or not in sync across with other clients. But when a user opens them on demand, the latest and greatest copy of the file would be fetched from the backend and sync the cache. If a coordinator edge is decommissioned, then another edge can be designated as a coordinator and all other edges have to be pointed to the new coordinator.

Edge Pre-population

Pre-population jobs can be viewed on an Edge instance.

Figure 16)

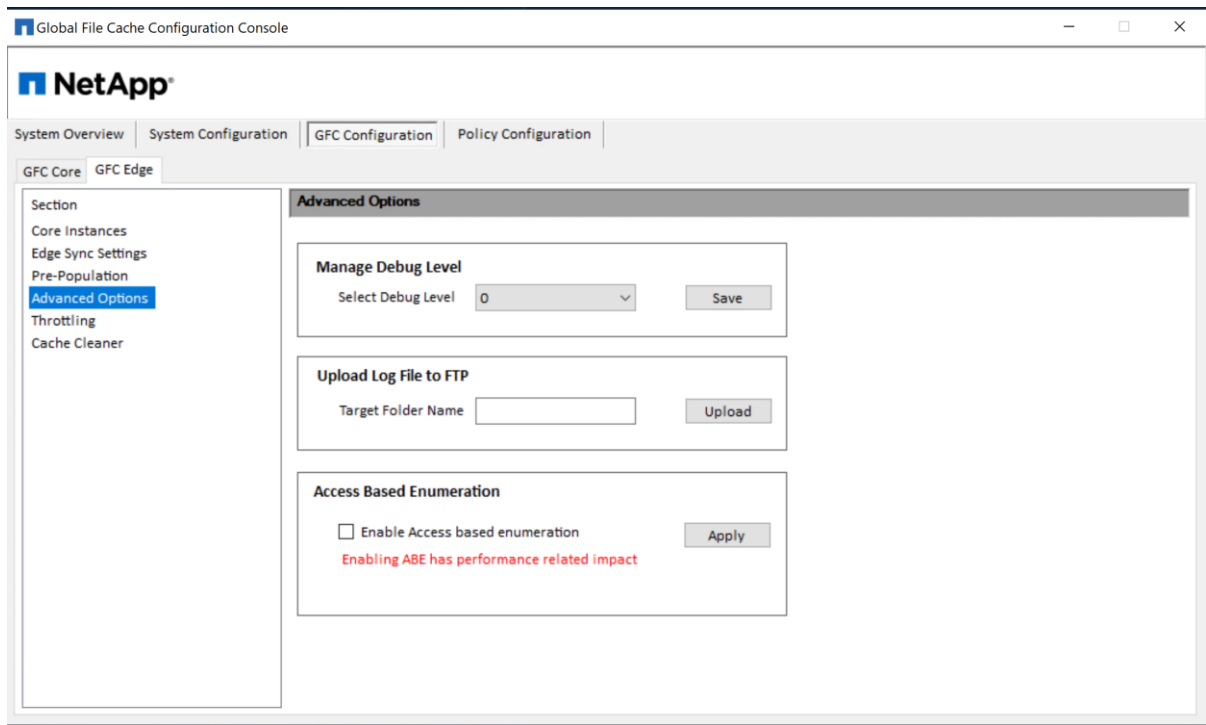


For more information, refer to the “Policy Configuration” section 9 of this document.

Note: The PowerShell Pre-population mechanism is only available from the Core instance.

Edge Advanced Options

Figure 17)



Manage Debug Level

This feature allows for more verbose (higher numbers, MAX: 9) debug logging.

Upload Log File to FTP

This feature enables a direct transfer of requested log files to NetApp Support.

Access Based Enumeration

This feature enables access-based enumeration on the FASTData Virtual File Share on the GFC Edge. Access Based Enumeration (ABE) allows you to hide specific files and folders for user who don't have access permission.

1. To enable access-based enumeration, check the respective check box.
2. Click "Apply," confirm that ABE has been enabled by browsing through the Virtual File Share [\\EdgeServer\\FASTData\\FabricID\\BackendFileServer\\](#) from a workstation in the same site using a non-administrative account.

Note: A reboot may be required to enforce ABE on the GFC Edge.

Throttling Feature

GFC enables specific controls over user behaviors when interacting with their local GFC Intelligent File Cache and Virtual File Share. The advanced Throttling options are set by default and should only be modified after discussing the current user workflow and behavior and consulting on these items with a member of NetApp Support.

Figure 18)

The screenshot shows the NetApp Global File Cache Configuration Console. The left sidebar lists sections: Core Instances, Edge Sync Settings, Pre-Population, Advanced Options, Throttling (highlighted), and Cache Cleaner. The main panel is titled 'Throttling Parameters' and includes a red warning: 'For use by NetApp Support ONLY.' Below this, there are three sections: 'Flush', 'Fetch', and 'Writes'. Each section has two input fields: 'Byte Max' (set to 1048576, default 1048576) and 'Byte Rate' (set to 1024, default 1024). At the bottom, a red note states: 'Changes to the above settings should not be made without first consulting NetApp Support.' and an 'Update' button is present.

Cache Cleaner

The GFC Edge Cache Cleaner mechanism can be adjusted to a specific behavior to meet specific time frames or low / high percentage thresholds.

Figure 19)

The screenshot shows the NetApp Global File Cache Configuration Console. The left sidebar lists sections: Core Instances, Edge Sync Settings, Pre-Population, Advanced Options, Throttling, and Cache Cleaner (highlighted). The main panel is titled 'Cache Cleaner' and contains four input fields: 'Start Hour' (set to 21), 'Stop Hour' (set to 6), 'Disk Max Percentage' (set to 80), and 'Disk Hard Max Percentage' (set to 95). An 'Update' button is located at the bottom right.

Start Hour / Stop Hour

The GFC Cache Cleaner mechanism is scheduled to begin at the specified hour (24hr clock) in the local time zone when the **Disk Max Percentage** has been reached. If a **Stop Hour** time is set, the Cache Cleaner will complete the cleaning of the current item and stop afterwards. The default setting is set to 9PM local time (21:00) and will run until 6AM the following morning (06:00).

Disk Max Percentage

This number (1-100) will signal to the Cache Cleaner at what percentage of cache disk utilization to schedule the Cache Cleaning process depending on the specified **Start Hour** as shown above. This percentage may vary among differently sized cache volumes across Edges. The default setting is 80% of the cache volume capacity.

Disk Hard Max Percentage

This number (1-100) will signal to the Cache Cleaner at what percentage of cache disk utilization to immediately begin the Cache Cleaning process. This is a very resource intensive process and may degrade user performance if it occurs during working hours. This percentage should be high enough to allow users to cache new data if the **Disk Max Percentage** value is reached but low enough where users will not be able to completely fill the cache volume. The default setting is 95% of the cache volume capacity.

Note: Depending on the age of the data, the purging of the cache will clean up 25-75% of stale cached data.

Note: To run a manual Cache Cleaner process, refer to the PowerShell Appendix C.

9 Deploying Cloud Volumes Edge Cache (CVEC)

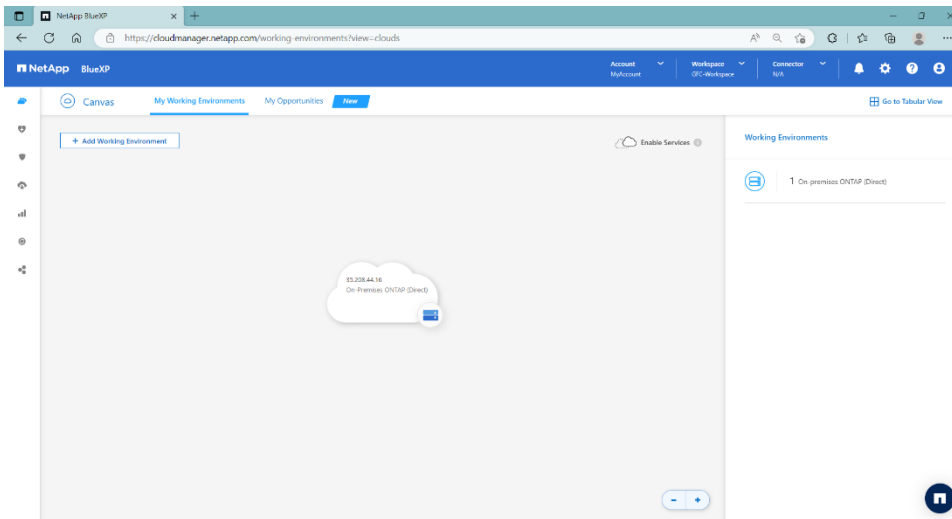
NetApp Cloud Volumes Edge Cache provides business continuity and data protection for the distributed enterprise. With central control of the organization's entire storage footprint, easy access to the storage for the end-users, and the ability to recover quickly gives IT Ops the peace of mind that they have their data under control, protected, and available to their users in the most efficient and cost-effective way possible. Cloud Volumes Edge Cache (CVEC) is a dimension under CVO family of offerings.

9.1 Deploy and configuration of BlueXP

CVEC can be easily deployed using BlueXP (formerly Cloud Manager). NetApp® BlueXP™ is a unified control plane delivering a simplified hybrid multicloud experience that enables the evolved cloud. BlueXP combines an intuitive interface with integrated data services and AI Ops automation for the evolved cloud experience.

To access NetApp® BlueXP™ please login to URL - <https://bluexp.netapp.com/>

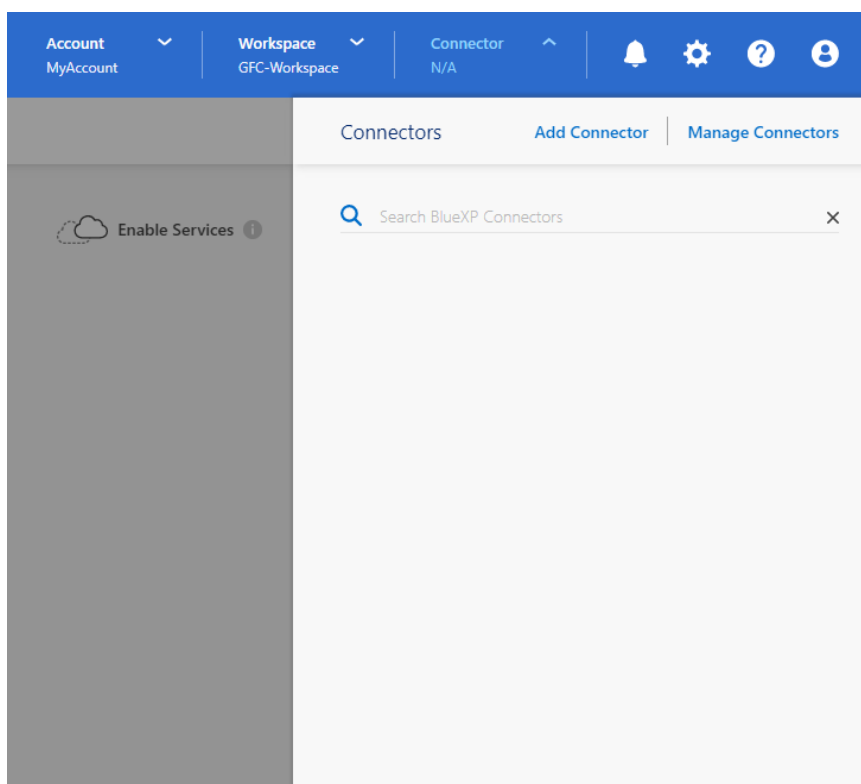
Please create an account otherwise login with the existing credentials. BlueXP canvas is shown below.



Setup a Connector

A BlueXP Account Admin will need to deploy a Connector in the appropriate hyperscaler (Azure, GCP) or on-premises network. The Connector is a crucial component for the day-to-day use of BlueXP. It enables BlueXP to manage the resources and processes within your public cloud environment.

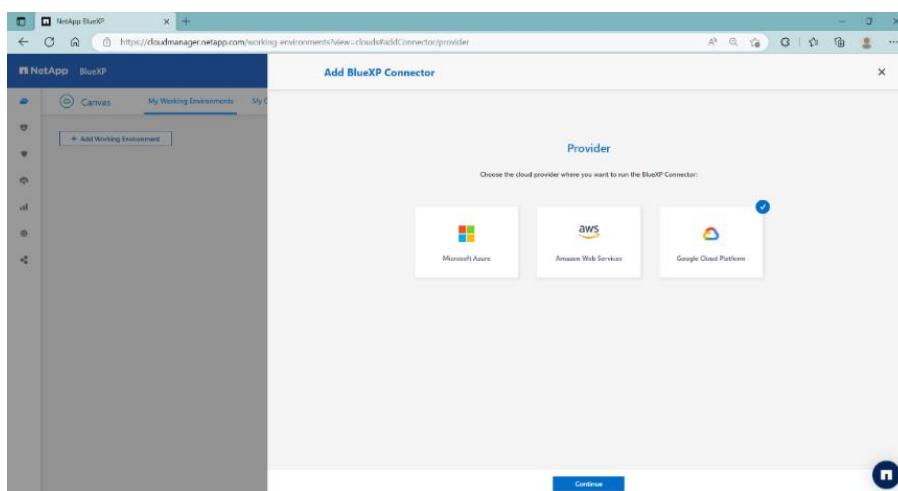
Click the Connector drop-down, select Add Connector



Create a Connector in appropriate Hyper scalar from BlueXP

Select Cloud Platform Provider

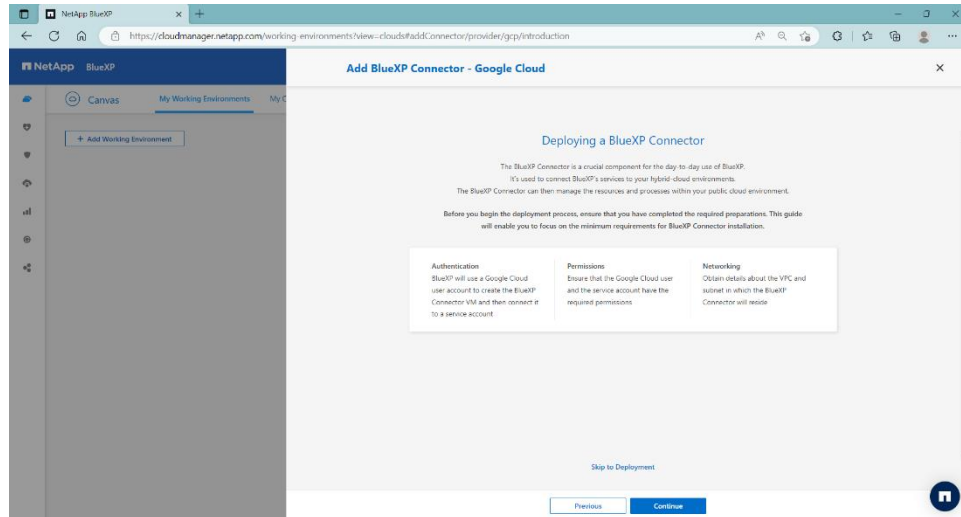
- Microsoft Azure
- Google Cloud Platform
- Amazon Web Services (Available next release)



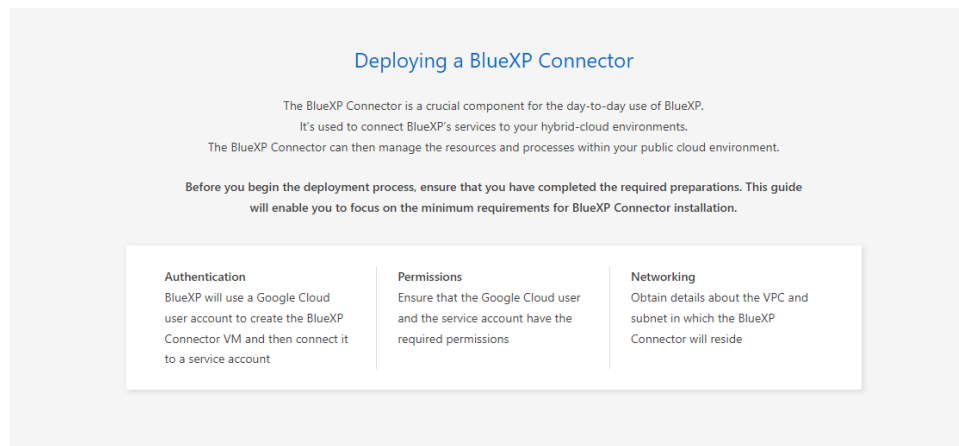
9.2 CVEC Configuration on GCP

This section will show all the configuration screens needed for deploying CVEC in Google Cloud Provider. Perform the steps as mentioned in the next few screens.

1. Before you begin the deployment process, ensure that you have completed the required preparations.



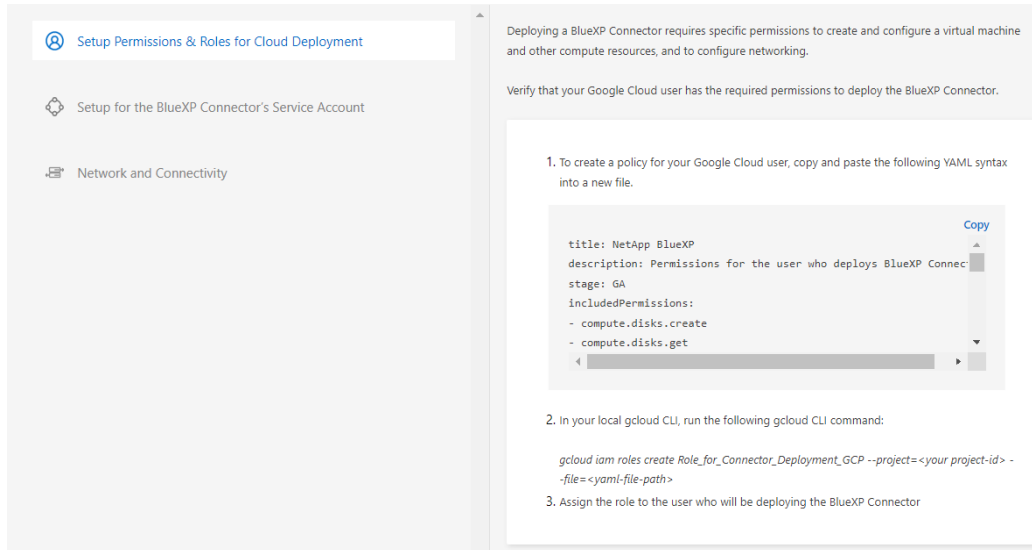
2. The following steps must be taken to manage resources in Google Cloud.
 - a. Authentication
 - b. Permissions
 - c. Networking



Setup Permissions & Roles for Cloud Deployment

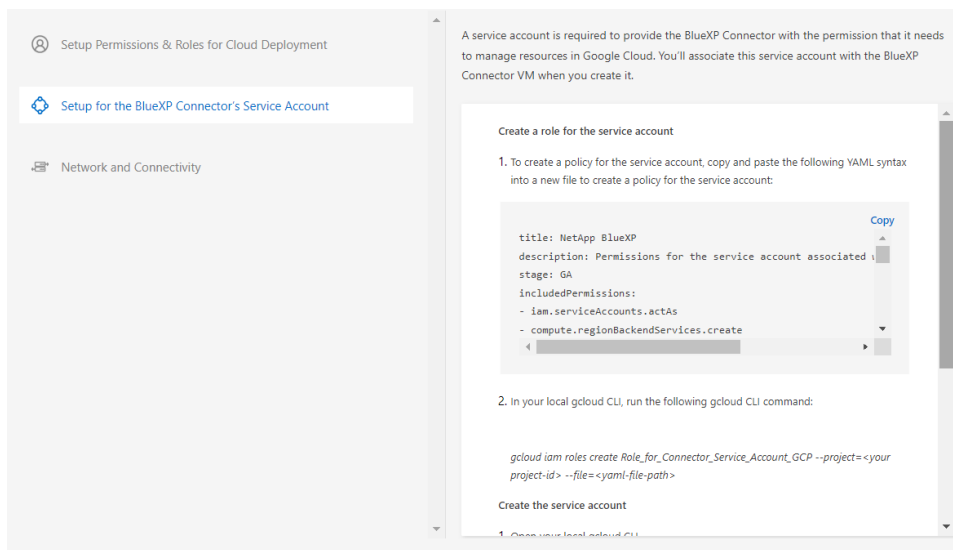
Deploying a BlueXP Connector requires specific permissions to create and configure a virtual machine and other compute resources, and to configure networking.

Verify that your Google Cloud user has the required permissions to deploy the BlueXP Connector.



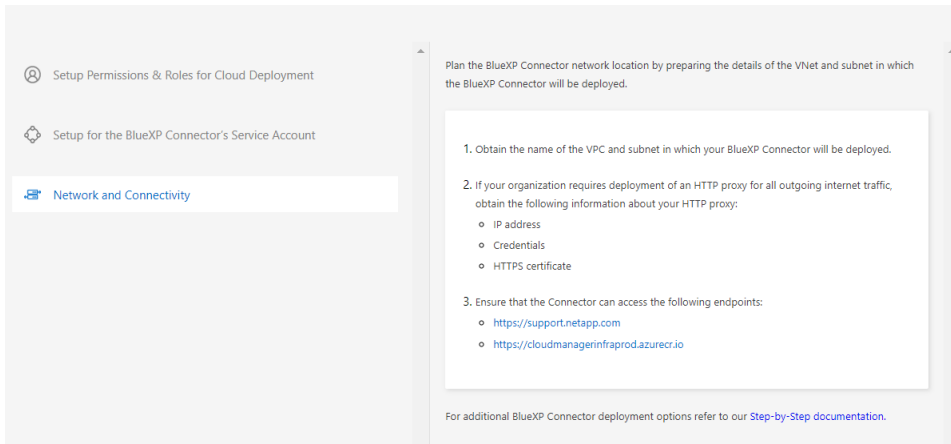
Setup for the BlueXP Connector's Service Account

A service account is required to provide the BlueXP Connector with the permission that it needs to manage resources in Google Cloud. You will associate this service account with the BlueXP Connector VM (Virtual Machine) when you create it.



Network and Connectivity

Plan the BlueXP Connector network location by preparing the details of the VNet (Virtual Network) and subnet in which the BlueXP Connector will be deployed.



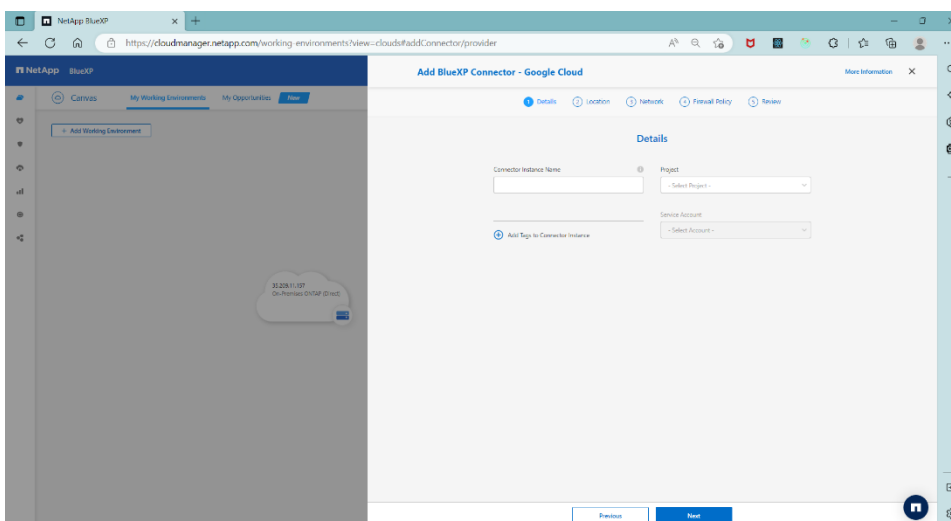
Note: Require (Private google access)

Enable Private Google Access on a subnet-by-subnet basis; it is a setting for subnets in a VPC (Virtual Private Cloud) network. To enable a subnet for Private Google Access and to view the requirements, see [Configure Private Google Access](#).

SUBNETS									
STATIC INTERNAL IP ADDRESSES FIREWALLS ROUTES VPC NETWORK PEERING PRIVATE SERVICE CONNECTION									
ADD SUBNET FLOW LOGS									
Filter Enter property name or value									
<input type="checkbox"/>	Name	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs
<input type="checkbox"/>	sk-vpc-network	us-central1	IPv4	172.16.0.0/20	None	None	172.16.0.1	On	Off
<input type="checkbox"/>	sk-vpc-network	us-east1	IPv4	172.17.0.0/20	None	None	172.17.0.1	On	Off

BlueXP will prompt login page if permissions and service account is set correctly for GCP (Google Cloud Platform).

Next, enter the connector details.



Next, enter location details.

The screenshot shows the 'Add BlueXP Connector - Google Cloud' wizard in the 'Location' tab. The left sidebar contains the NetApp BlueXP navigation menu. The main content area has tabs for 'Details', 'Location', 'Network', 'Firewall Policy', and 'Review'. The 'Location' tab is active, displaying the following fields:

- Region: us-central1
- Zone: us-central1-a
- VPC: default
- Subnet: default

At the bottom of the form are 'Previous' and 'Next' buttons. A 'More Information' link is located in the top right corner.

Next, enter Network details.

The screenshot shows the 'Add BlueXP Connector - Google Cloud' wizard in the 'Network' tab. The left sidebar contains the NetApp BlueXP navigation menu. The main content area has tabs for 'Details', 'Location', 'Network', 'Firewall Policy', and 'Review'. The 'Network' tab is active, displaying the following fields:

- Connectivity: Public IP (enable)
- Proxy Configuration (Optional): HTTP Proxy (Example: http://10.254.10.100)
- Define Certificates for this Proxy: Upload a root certificate

At the bottom of the form are 'Previous' and 'Next' buttons. A 'More Information' link is located in the top right corner.

Next, create or select firewall policy

The screenshot shows the 'Firewall Policy' step of the 'Add BlueXP Connector - Google Cloud' wizard. The breadcrumb trail is: Details > Location > Network > Firewall Policy > Review. The 'Firewall Policy' section has a note: 'The firewall policy must allow inbound HTTP, HTTPS and SSH access.' Below this, there are two tabs: 'Assign a firewall policy' (selected) and 'Select an existing firewall policy'. Under 'Assign a new firewall policy', there are three columns for different protocols: HTTP (Port 80), HTTPS (Port 443), and SSH (Port 22). Each column has a 'Source type' dropdown set to 'Custom' and a 'Source (CIDR)' text box containing '10.0.0.0/24'. At the bottom, there are 'Previous' and 'Next' buttons.

Next review the changes and Click Add to create the Connector.

The screenshot shows the 'Review' step of the 'Add BlueXP Connector - Google Cloud' wizard. The breadcrumb trail is: Details > Location > Network > Firewall Policy > Review. The 'Review' section has a link 'Go to the Troubleshooting Automation'. Below this, there is a table of configuration details:

BlueXP Connector Name	gcp-connector-prc
Project	Global File Cache CM
Service Account	SR BlueXP Service Account
Region	us-central1
Zone	us-central1-a
VPC	ak-vpc-network
Subnet	ak-vpc-network
Public IP	Enable
Proxy	None
Firewall Policy	vpc-fdr2-closed-ocm-firewall-rules-1

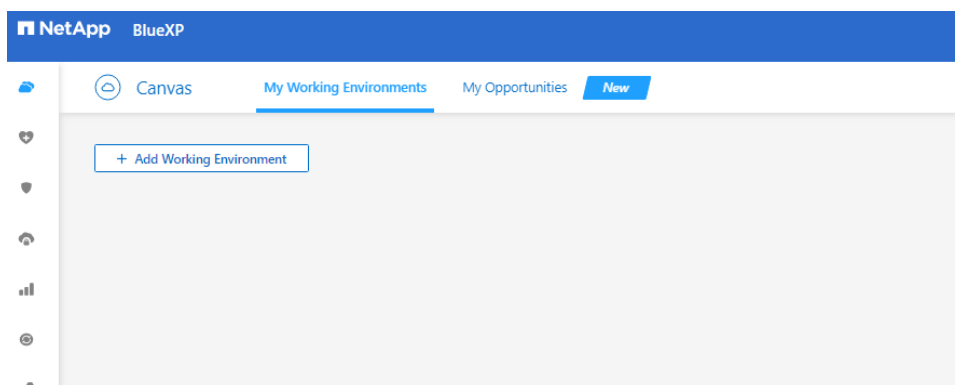
At the bottom, there are 'Previous' and 'Add' buttons.

BlueXP will deploy the Connector.

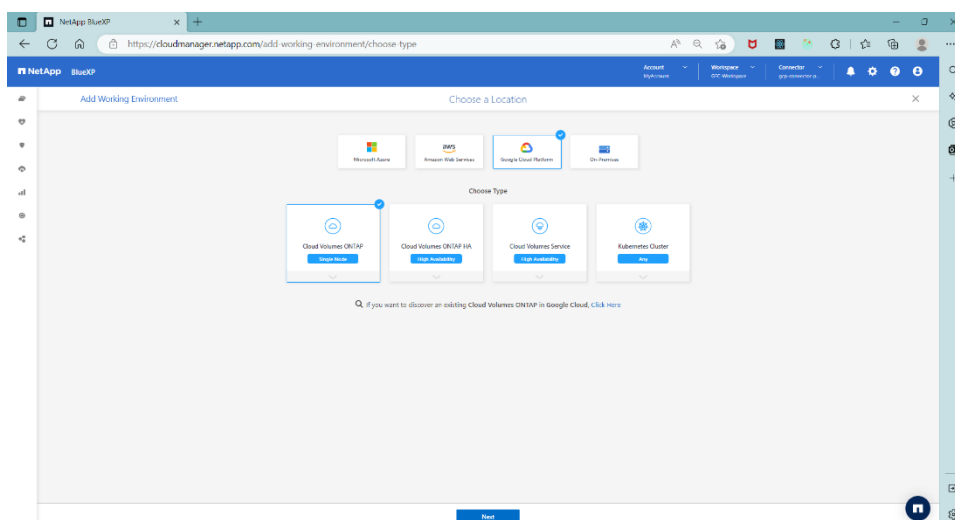
Once the Connector is Deployed successfully, the next step is to set up the Working environment.

Setup Working Environment

To create working environment, click on + Add Working Environment

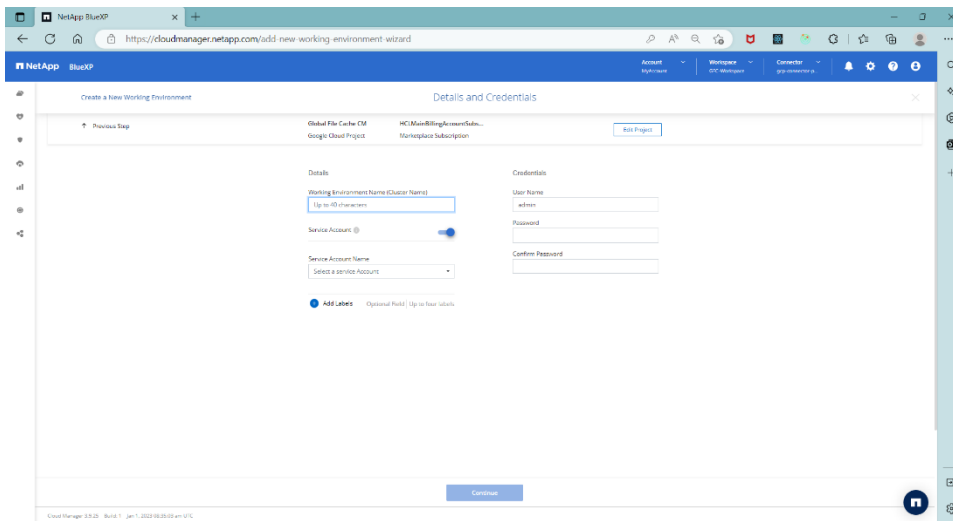


Next, select Google cloud platform and choose the appropriate type based on your requirement.

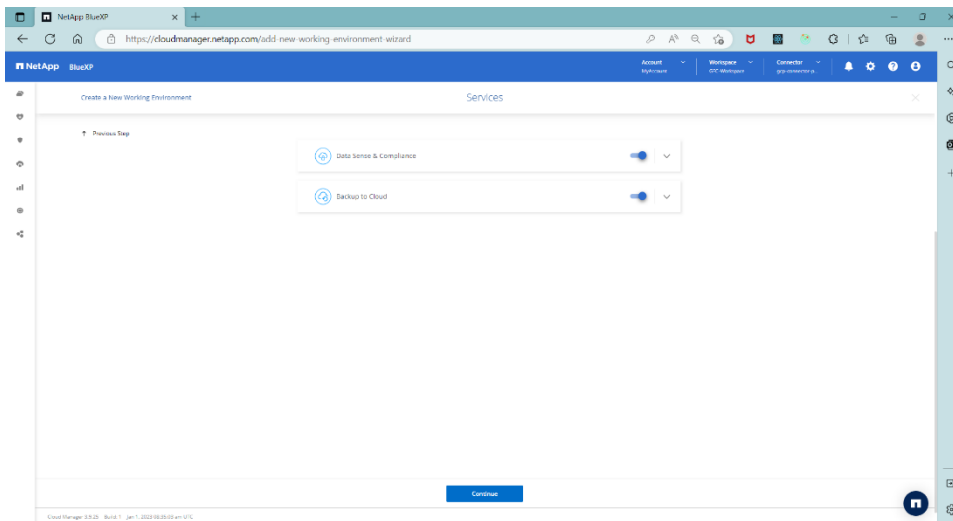


Next, enter details and credentials required for the working environment.

Note: For GCP, please disable service account to deploy CVO successfully, else an error is observed.



Next, select the services.



Next, enter location and connectivity details.

The screenshot shows the 'Location & Connectivity' step in the NetApp BlueXP 'Create a New Working Environment' wizard. The page is divided into two main sections: 'Location' and 'Connectivity'. Under 'Location', there are dropdown menus for 'GCP Region' (set to 'us-central1') and 'GCP Zone' (set to 'us-central1-a'). A checkbox 'I have verified connectivity between the target VPC and Google Cloud storage' is checked. Under 'Connectivity', there is a dropdown for 'VPC' (set to 'default-network') and a dropdown for 'Subnet' (set to '172.16.0.0/24'). There are two radio buttons for 'Firewall Policy': 'Generate firewall policy' (selected) and 'Use existing firewall policy'. Below these, there is a dropdown for 'Allow traffic within' (set to 'The selected VPC only (recommended)'). A 'Continue' button is at the bottom right.

Next, select Edge Cache charging method.

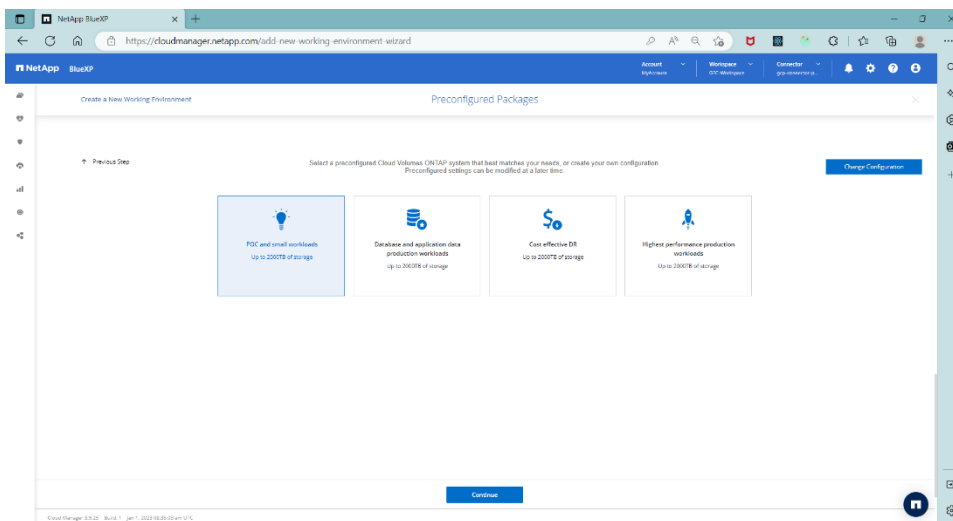
The screenshot shows the 'Cloud Volumes ONTAP Charging Methods & NSS Account' page. It features a 'Select Charging Method' section with several options: 'Professional', 'Edge Cache' (selected), 'Essential', 'Optimized', 'Essential (Up to 500 GB)', and 'Per Node'. Each option has a 'Go to details' link. Below the options, there is a link 'Learn more about NetApp Cloud Volumes ONTAP charging method'. A 'Continue' button is at the bottom right.

To select the Edge Cache charging method a marketplace subscription should be available.

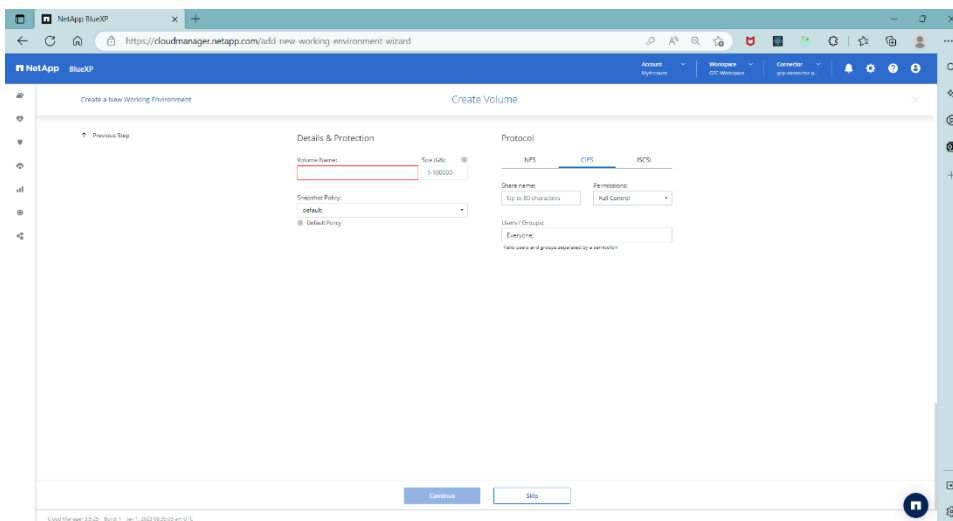
Next, Please go to GCP marketplace (<https://cloud.google.com/marketplace>)

The screenshot shows the NetApp BlueXP marketplace listing on Google Cloud. The header includes the NetApp logo and the product name 'NetApp BlueXP'. Below this, there is a description: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' There is a 'MANAGE ON PROVIDER' button and a 'Purchased on 1/4/23' status. The page has tabs for 'OVERVIEW', 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'OVERVIEW' tab is selected, showing an 'Overview' section with a description of BlueXP as a hybrid multicloud storage and data services experience. To the right, there is an 'Additional details' section with 'Type: SaaS & APIs', 'Last updated: 12/29/22', and 'Category: Analytics Developer tools Storage'. A video thumbnail is visible on the right side of the page.

Follow the instructions shown on screen to associate marketplace subscription.
Next, Select preconfigure package based on the requirement.



Next, create a volume and select CIFS protocol.



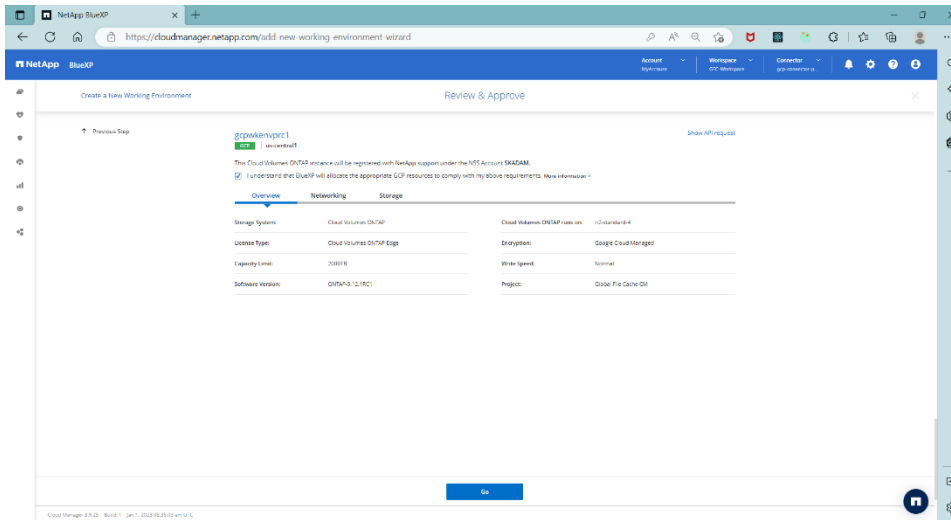
Next, Setup CIFS Server

The screenshot shows the 'CIFS Setup' wizard in the NetApp BlueXP interface. The title bar indicates 'Create a New Working Environment'. The main heading is 'CIFS Setup'. Below this, there's a section 'Set up your ONTAP CIFS server'. It contains several input fields: 'DNS Primary IP Address' (with a placeholder 'Example: 127.0.0.1'), 'DNS Secondary IP Address (Optional)' (with a placeholder 'Example: 127.0.0.1'), 'Active Directory Domain to join' (with a placeholder 'Example: yourdomain.com, up to 107 characters'), and 'Credentials authorized to join the domain' (with fields for 'administration' and 'Password'). There is also a link 'Edit advanced fields (Optional)'. At the bottom right, there is a 'Continue' button. The footer shows 'Cloud Manager 3.0.0 - Build 1.1 - Jan 1, 2023 10:25:00 am UTC'.

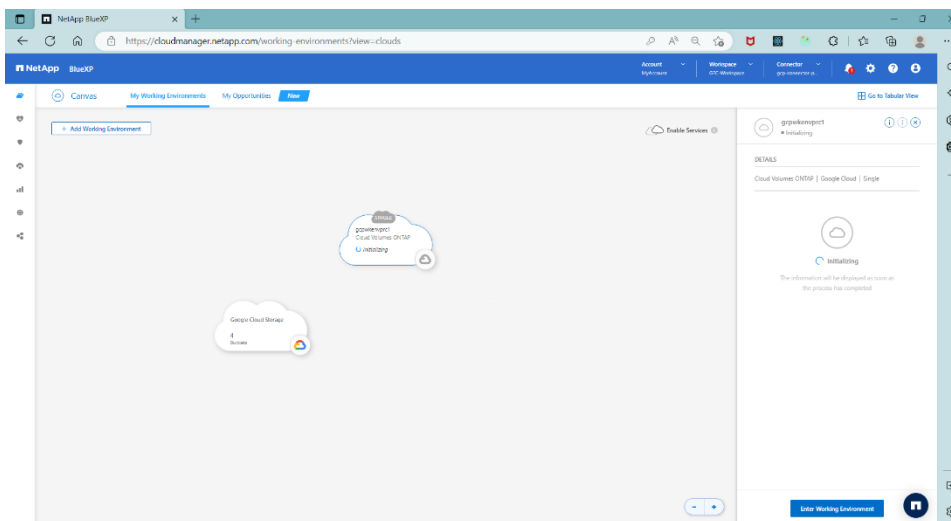
Next, select usage profile disk type and tiering policy.

The screenshot shows the 'Create Volume - Usage Profile Disk Type & Tiering Policy' wizard in the NetApp BlueXP interface. The title bar indicates 'Create a New Working Environment'. The main heading is 'Create Volume - Usage Profile Disk Type & Tiering Policy'. Below this, there are two radio button options: 'Storage Efficiency' (selected) and 'No Storage Efficiency'. The 'Storage Efficiency' option has a subtext 'Enables thin provisioning, deduplication, and compression'. The 'No Storage Efficiency' option has a subtext 'Use fully provisioned capacity'. Below these options, there is a section for 'Disk Type' with a 'SSD' icon and text: 'Cloud Manager will create the volume using the disk type that you previously selected. You can use different disk types with future volumes.' Below this, there is a section for 'Tiering data to object storage' with a 'Volume Tiering Policy' dropdown menu set to 'Auto'. At the bottom right, there is a 'Continue' button. The footer shows 'Cloud Manager 3.0.0 - Build 1.1 - Jan 1, 2023 10:25:00 am UTC'.

Next, Review and Approve working environment.



Next, Click on Go button and wait for working environment deployment to successfully completed.



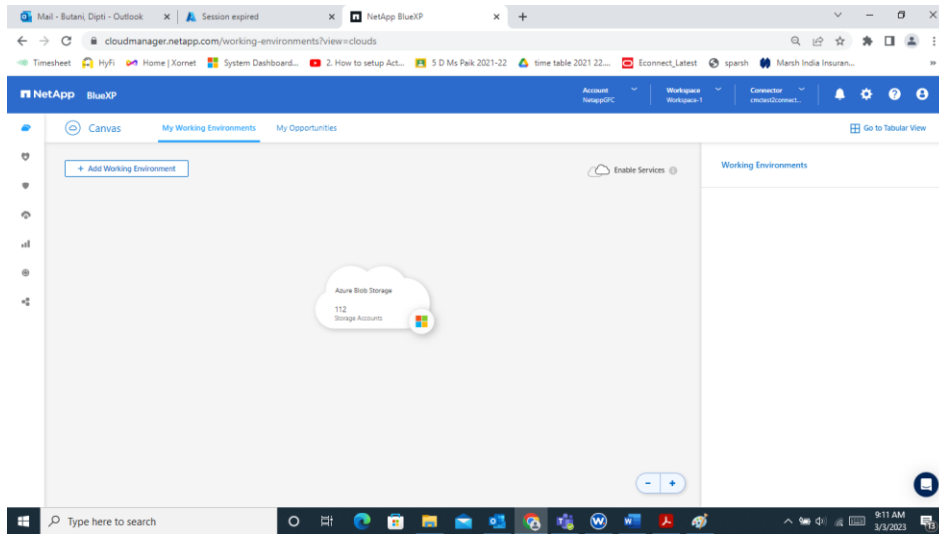
This completes the initialization of the working environment on Google Compute Platform (GCP)

9.3 CVEC Configuration on Azure

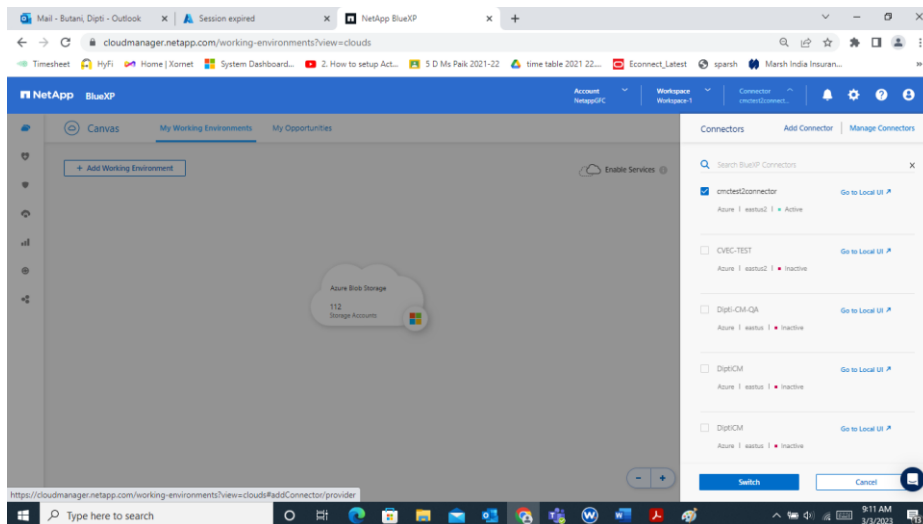
Perform the steps as mentioned in the next few screens.

This document explains how to create a CVO in Azure using CVEC option and how to register NetApp LMS for CVEC.

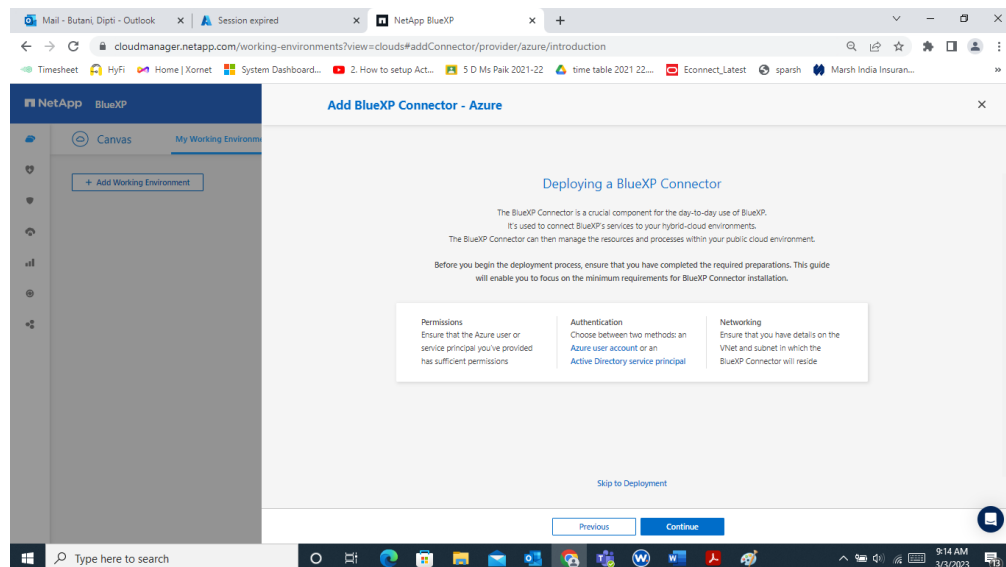
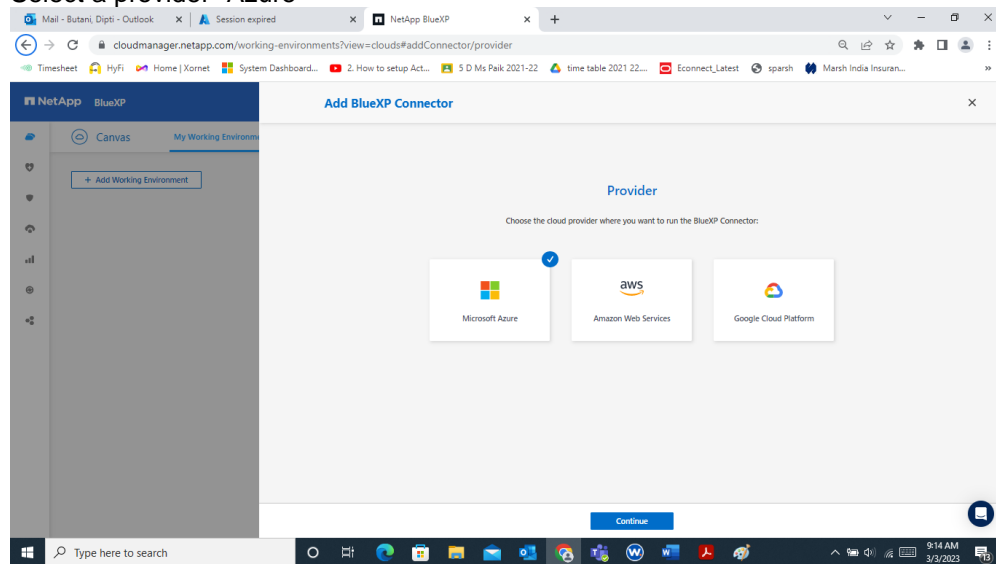
1. Login to <https://bluexp.netapp.com/>



2. Click on add connector.



3. Select a provider- Azure



4. Login to your NetApp account and select relevant tenant and subscription. Fill all the details and click on next.

Mail - Butani, Dipti - Outlook x Session expired x NetApp BlueXP x +

cloudmanager.netapp.com/working-environments?view=clouds#addConnector/provider

Timesheet HyFi Home | Xomet System Dashboard... 2. How to setup Act... 5 D Ms Paik 2021-22 time table 2021 22... Econnect_Latest sparsk Marsh India Insuran...

NetApp BlueXP

Canvas My Working Environm

+ Add Working Environment

Add BlueXP Connector - Azure More Information x

1 VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Virtual Machine Authentication

You are logged in with Azure user: diptib@netapp.com | Tenant: netappgfc

Subscription: GFC-Dev Authentication Method: ☒ Password ☐ Public Key

Location: East US User Name:

Resource Group: ☒ Create New ☐ Use Existing Enter Password:

Resource Group Name:

Previous Next

Type here to search 9:16 AM 3/3/2023

5. Give connector instance name and click on next

Mail - Butani, Dipti - Outlook x Session expired x NetApp BlueXP x +

cloudmanager.netapp.com/working-environments?view=clouds#addConnector/provider

Timesheet HyFi Home | Xomet System Dashboard... 2. How to setup Act... 5 D Ms Paik 2021-22 time table 2021 22... Econnect_Latest sparsk Marsh India Insuran...

NetApp BlueXP

Canvas My Working Environm

+ Add Working Environment

Add BlueXP Connector - Azure More Information x

1 VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Details

Connector Instance Name:

Connector Role: ☒ Create ☐ Attach existing ☐ Manual

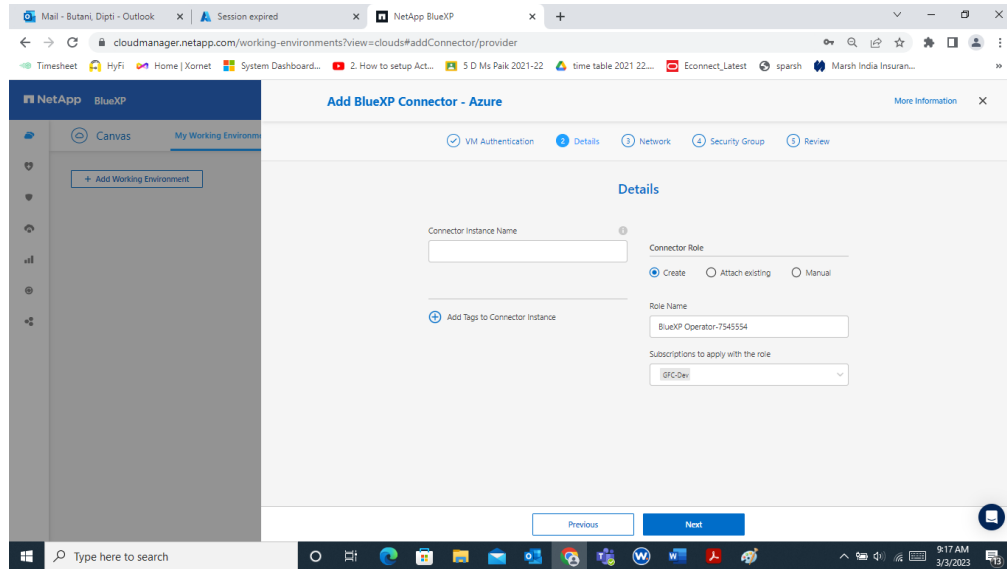
Role Name: BlueXP Operator-7545554

Subscriptions to apply with the role: GFC-Dev

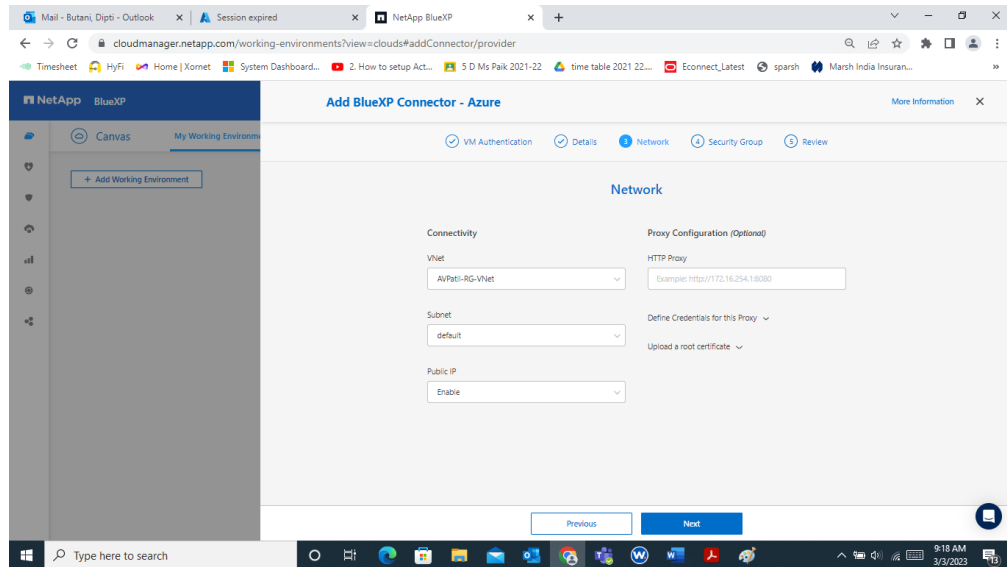
Previous Next

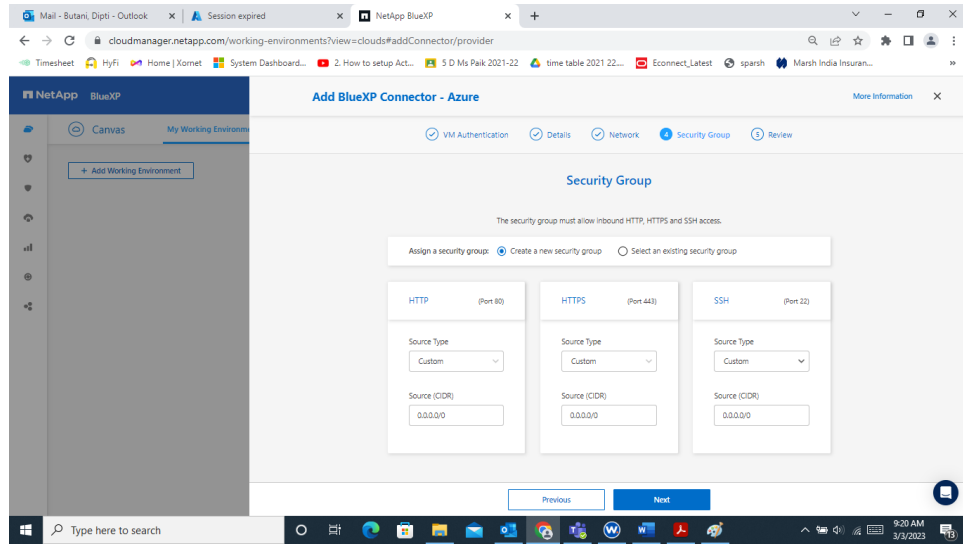
Type here to search 9:17 AM 3/3/2023

6. Give connector instance name and click next.

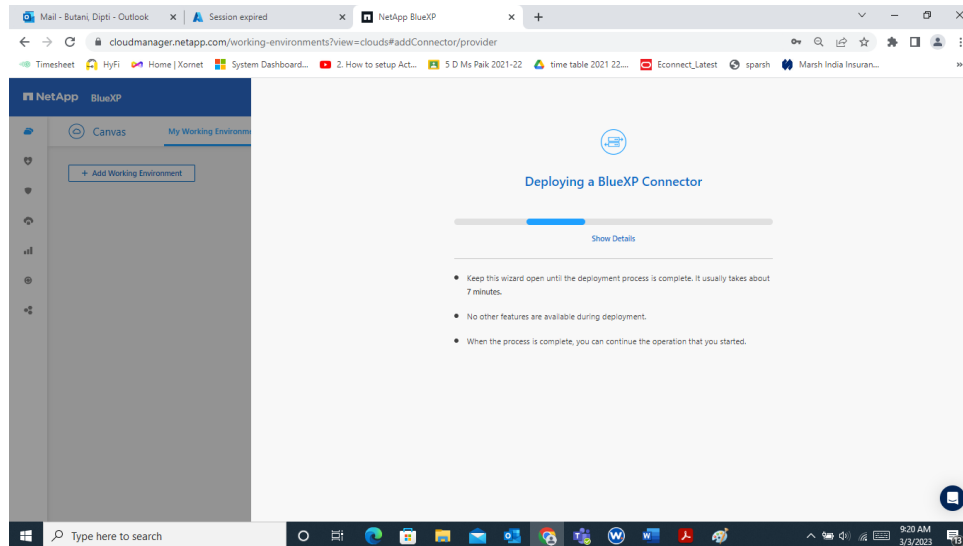


7. Add network and security group details

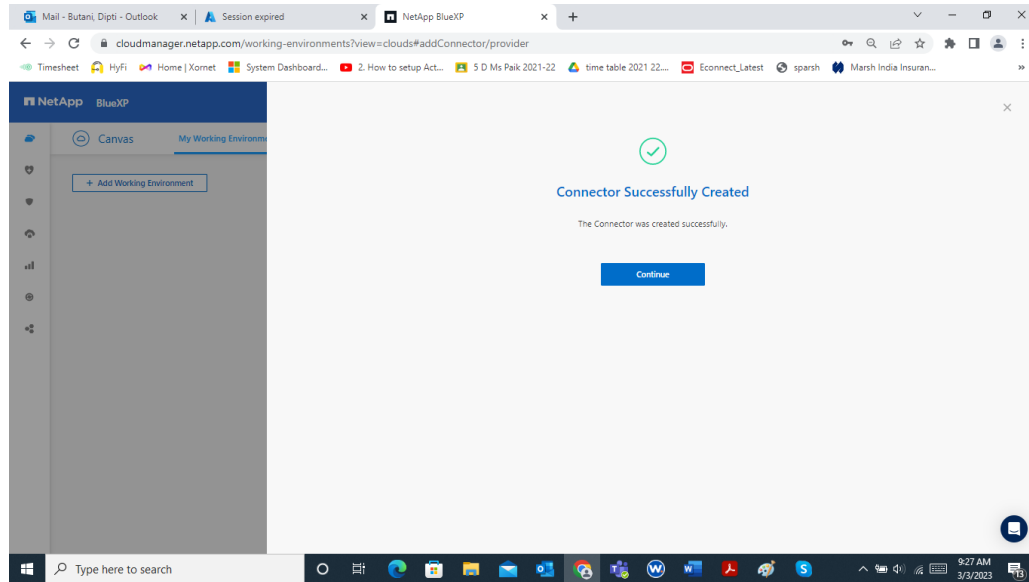




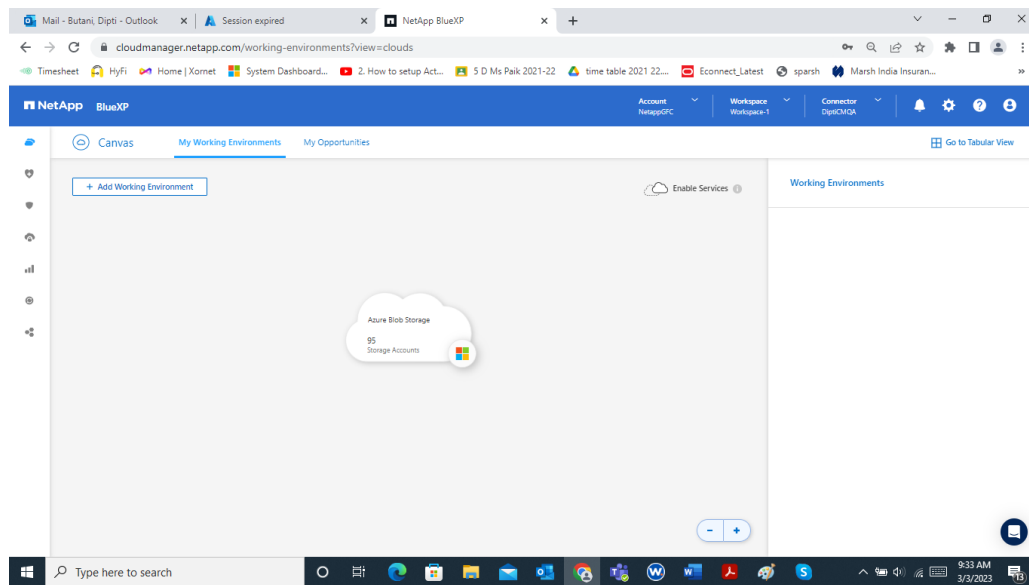
8. Review details and create



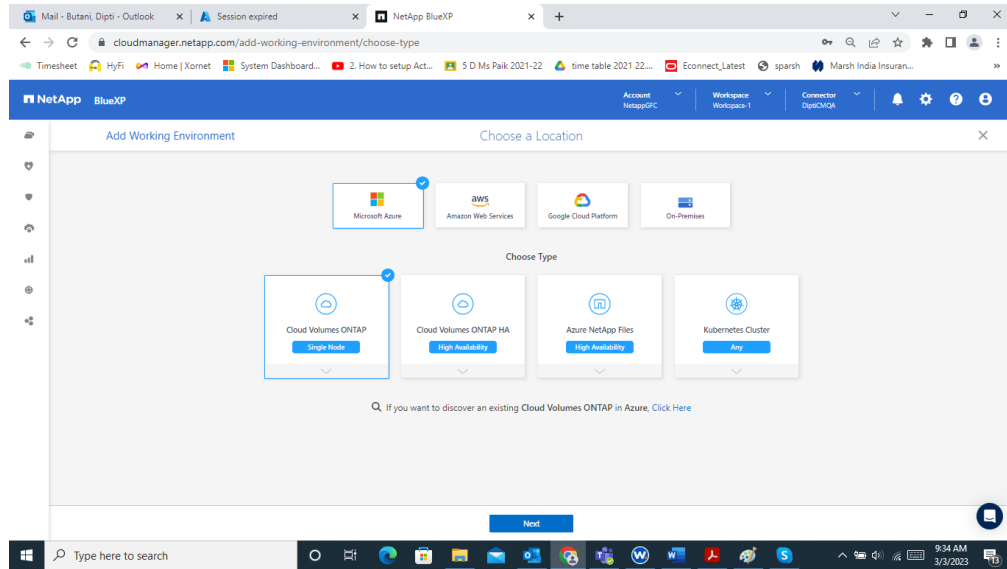
9. Connector created successfully.



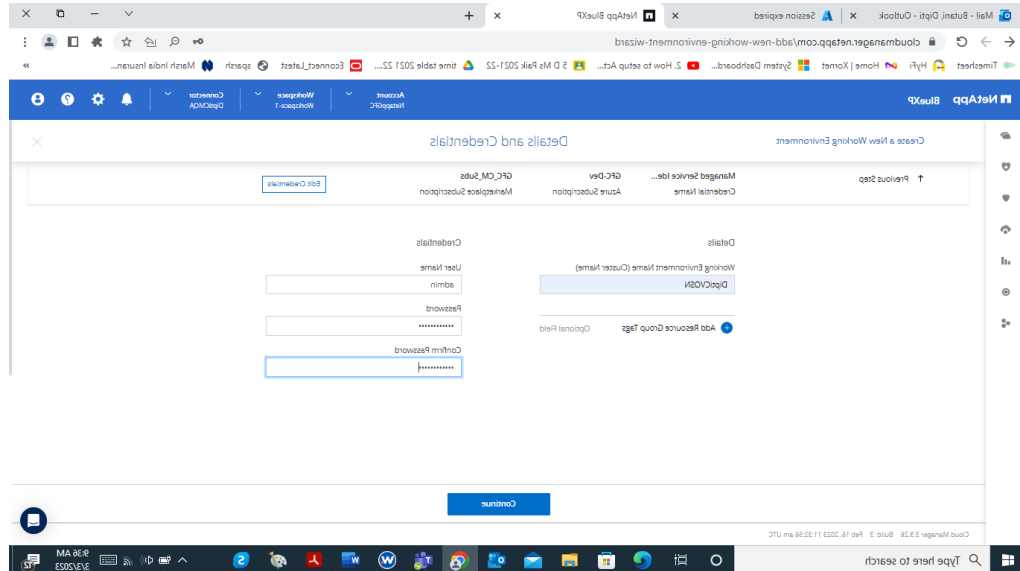
10. Select the same connector and create a CVO



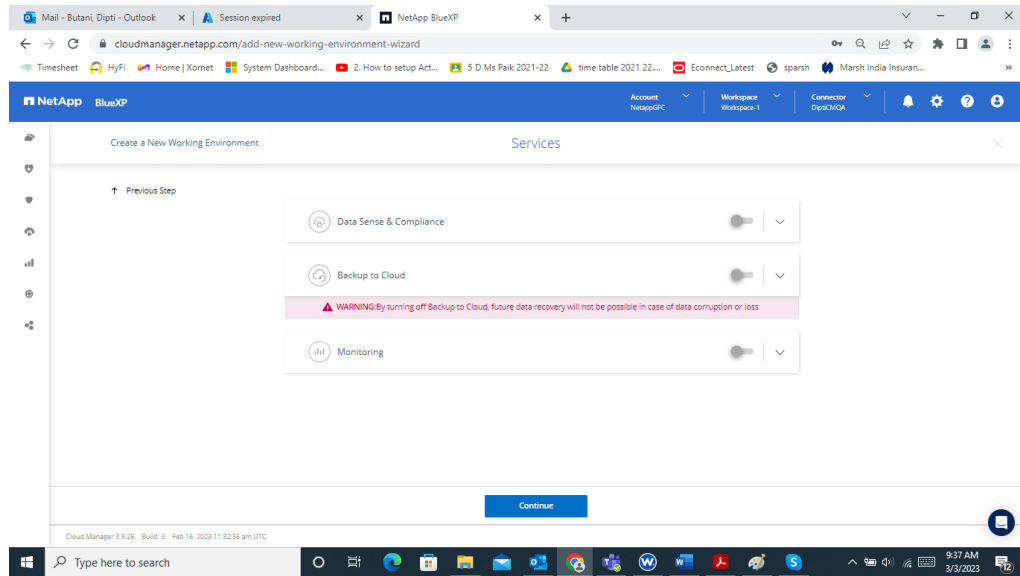
11. Select Cloud Volumes ONTAP in Azure



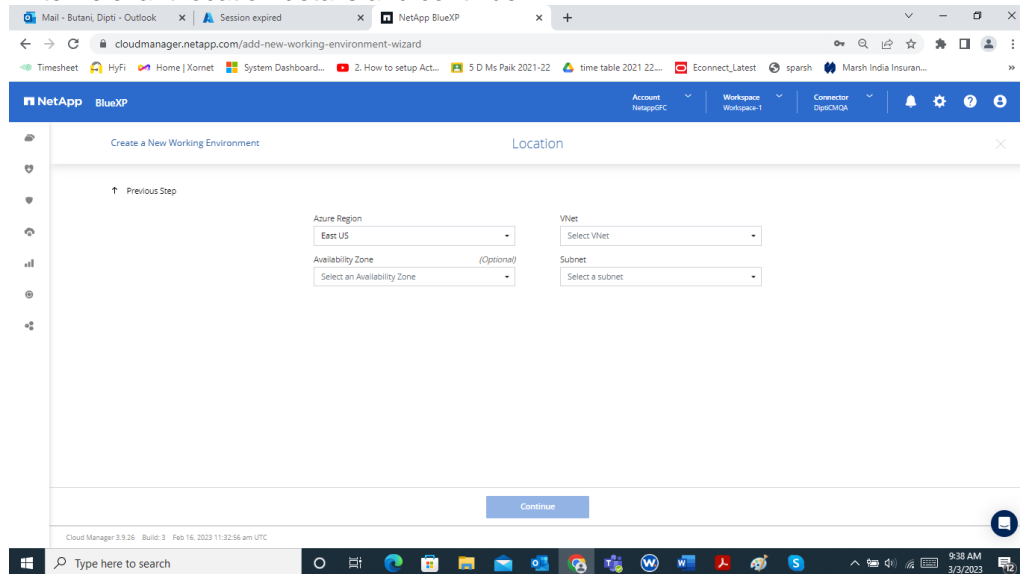
12. Enter all the relevant details and continue

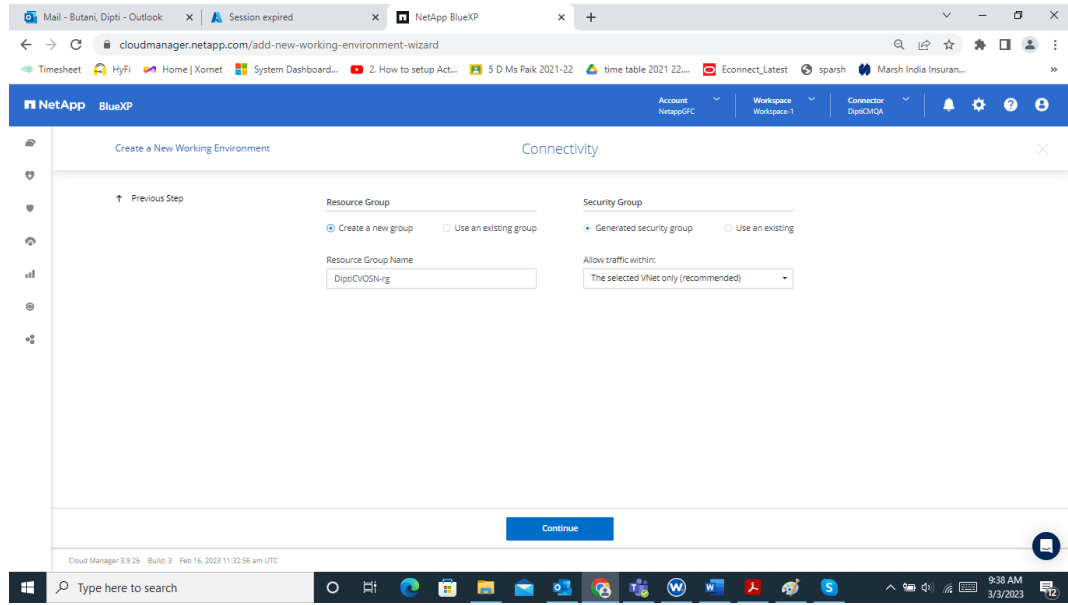


13. For testing to save cost, I disabled all the services.

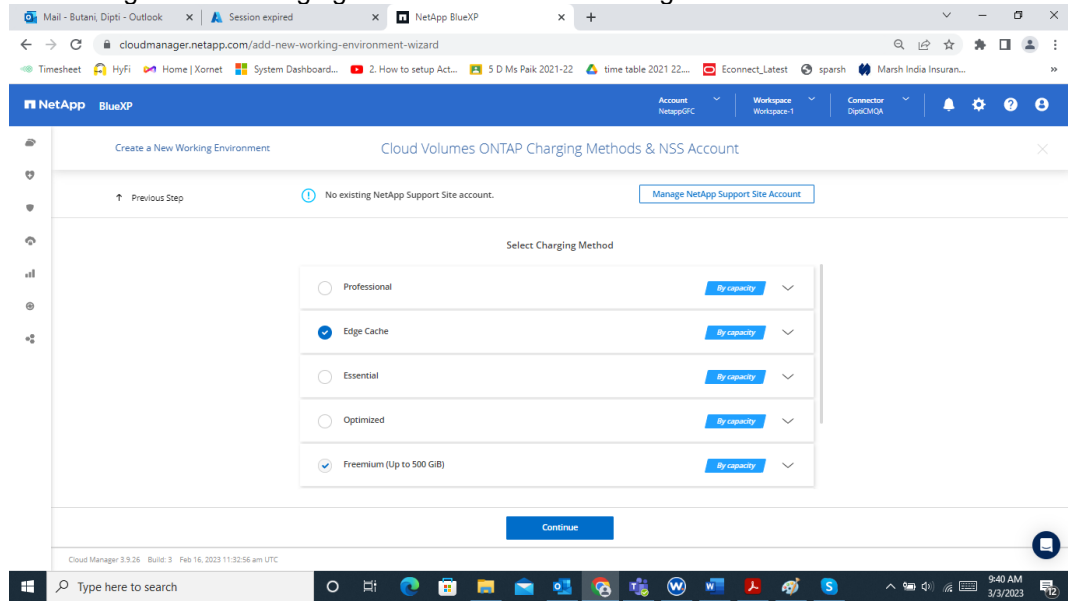


14. Enter relevant location details and continue

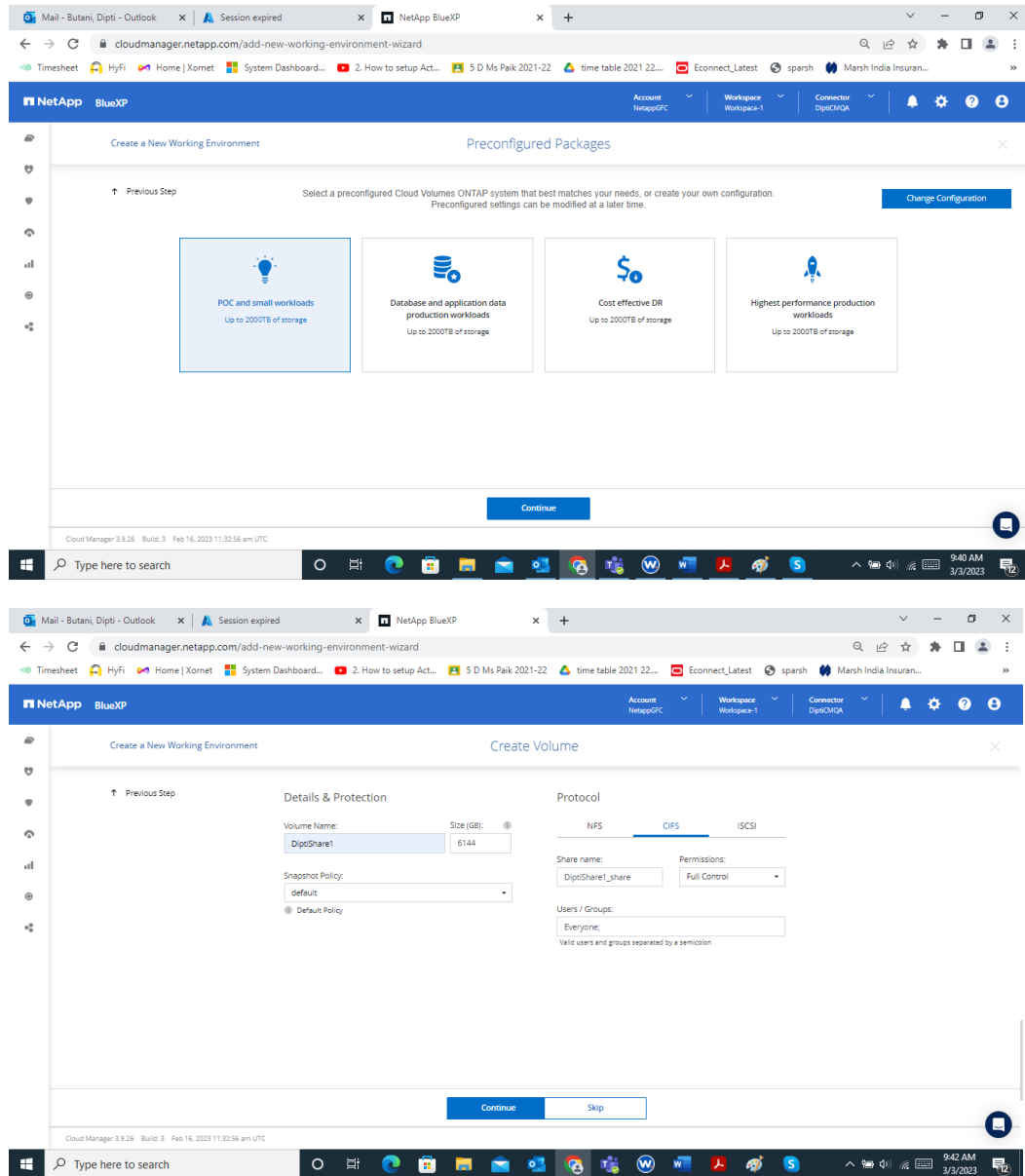


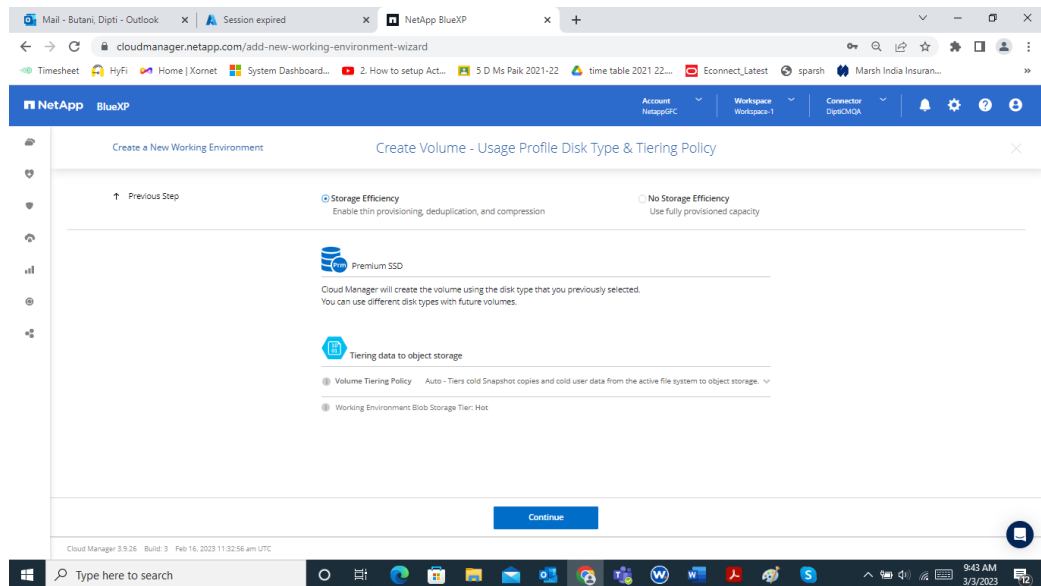
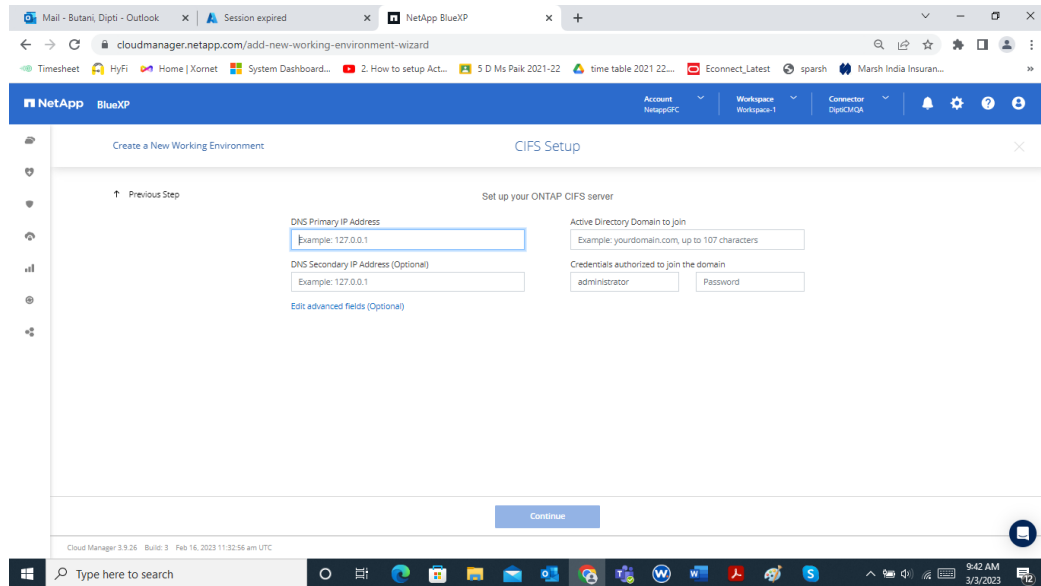


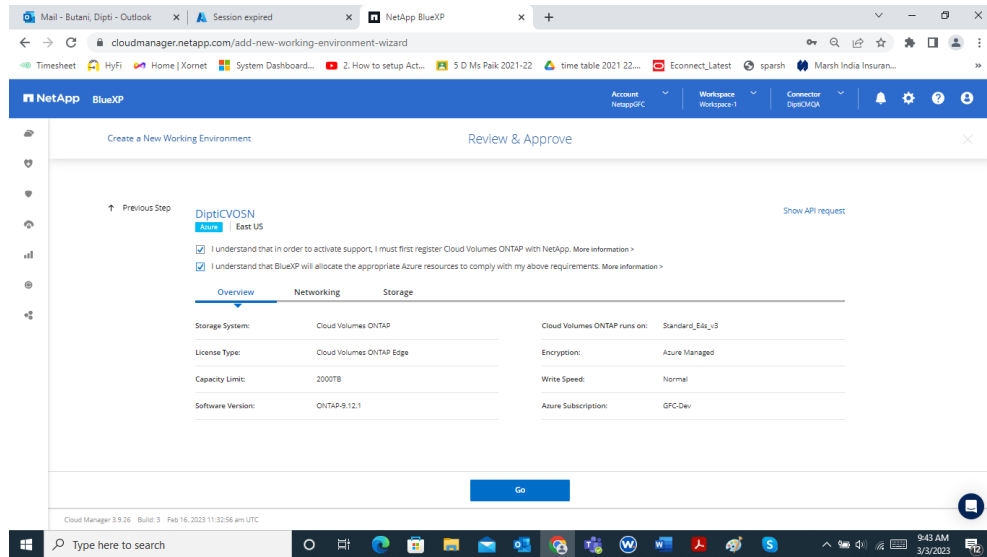
15. Select Edge Cache charging method for CVEC licensing



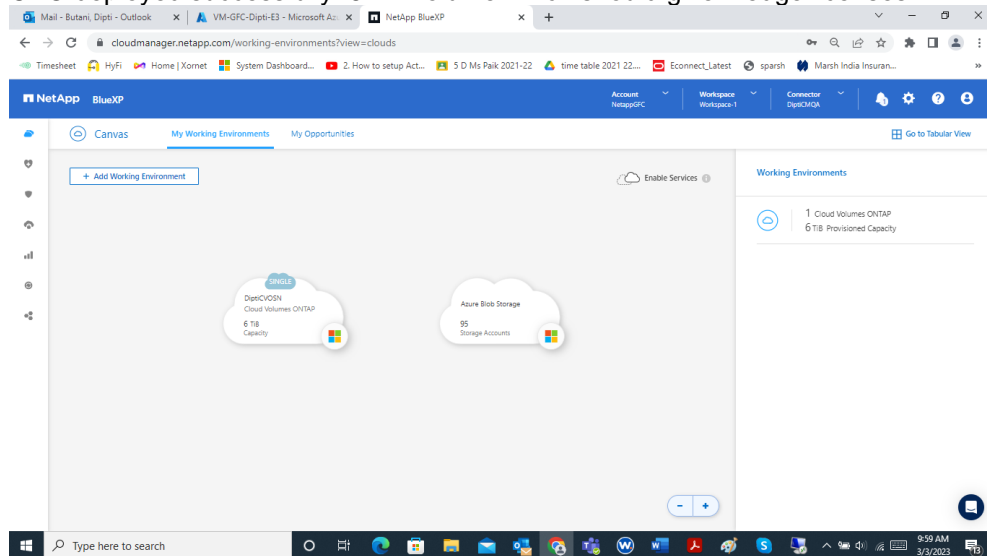
16. Create volume







17. CVO deployed successfully. 6 TB volume which should give 2 edge licenses.

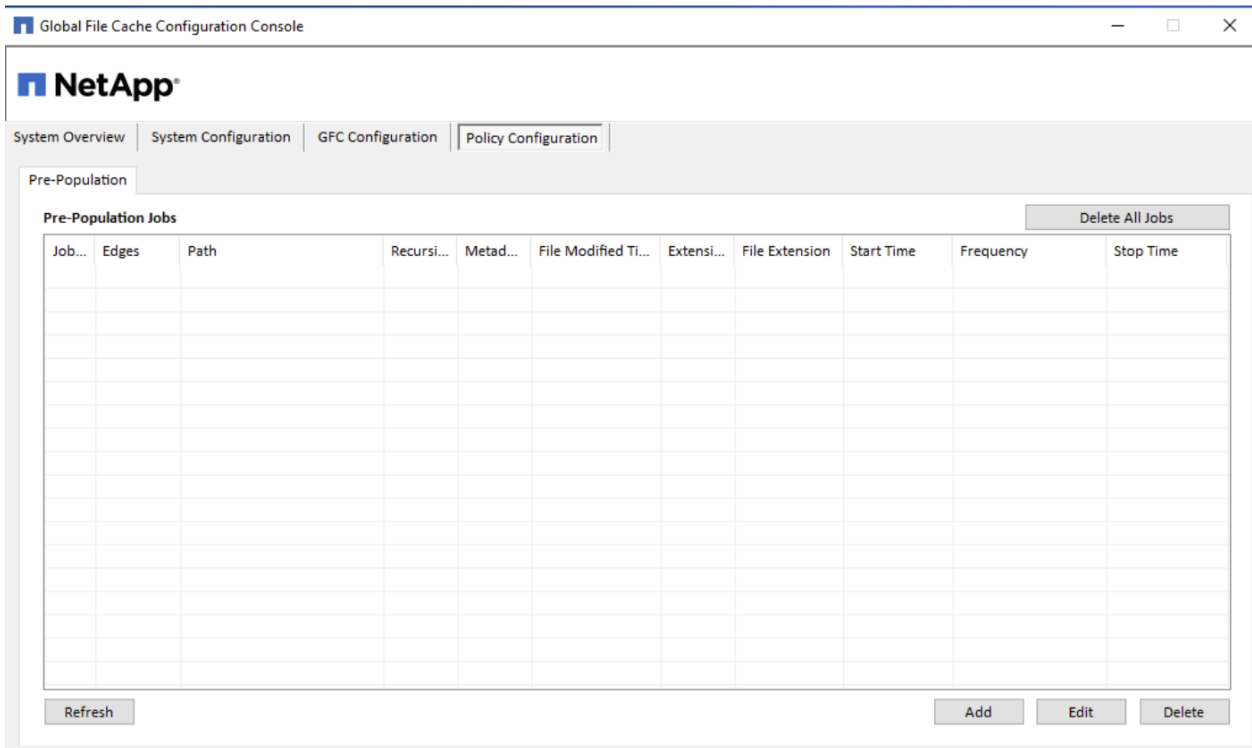


10 Designing and Deploying Policy Configuration

Depending on your requirements you may need to configure NetApp Global File Cache (GFC) Policies. GFC Cache's policies are configured via Policy Configuration tab.

The pre-population feature updates shares, directories, folders, and/or files from datacenter servers to the branch office Edge server(s) at predetermined times and frequencies. This pre-populates GFC Edge caches with data that will be used by their connected clients, creating a 'warm' cache on the Edge server. Branch office clients access files from the warm cache much faster than 'cold' files, those that need to be fetched from datacenter servers and then sent over the WAN.

Pre-population jobs can be scheduled from the LMS instance only, which triggers data fetches from the associated GFC Edge server(s). All times associated with pre-population correspond to the Edge server's local time.



Note: Before you define, schedule, or edit a pre-population job, the GFC core instance requires at least one associated datacenter file server as configured in the “**Backend File Servers**” section of the UI.

The Pre-Population page displays a list of jobs scheduled from the LMS to the GFC Edge servers. The Pre-population window displays the following information for each scheduled pre-population job.

Table 1)

Field name	Description
JobID	An automatically generated job identification number
Edge	Name of the GFC Edge server to be pre-populated with data (or All if data will be pushed from the specified server to all Edge servers).
Server	Name of the data center file server
Path	Path of the folder on the data center server with information to be shared, for example, \\myserver\folder\sharefolder
Recursive	If checked, the pre-population data is recursive, and will transfer the files in the indicated directory as well as all its subdirectories. If No, only the specified folder will be pre-populated.
Metadata Only	If checked, the pre-population mechanism only populates metadata from the specified files and directories, this does not write data to the branch office Edge cache.
File Modified Time	File modification times, if only data with specific modified by dates are to be pre-populated
File Extension	File extensions of any file types to be specifically included in or excluded from the Pre-population job
Start Time	Start time of the pre-population job (Edge server local time)
End Time	End time of the pre-population job if a one-time job (Edge server local time)
Frequency	Displays 'One Time' if a single job or displays the frequency of a recurring job
Stop Time	End time of the pre-population job schedule if a recurring job (Edge Server local time)

10.1 To Configure and Schedule a Pre-Population Job

1. Open the Global File Cache **Configuration Console**.
2. Click the “**Policy Configuration**” tab.

NetApp Add Pre-Population Job

Add Pre-population job

FAST™ Edge: *All*

Datacenter file server: 192.168.10.70

UNC Path: \\192.168.10.70\ Browse

☐ Recursive ☐ Metadata Only

Filter by modified time: ☐ Only include files modified within the last [] Minutes

Filter by file type: No limit [] Example: .mdb,.ldb

Start Date/Time: Monday, March 15, 2021 4:33:34 PM

Stop Date/Time: Thursday, January 1, 2099 12:00:00 AM

Frequency: ☒ One Time Job

☐ Repeat every day

☐ Repeat every Sunday

☐ Repeat every 1st at 4:33:35 PM

Apply Cancel

3. Click **"Add"** from the Pre-population page. The **"Add Pre-Population Job"** window opens.
 - a. Click the **"Edge"** drop-down menu and select a GFC Edge server to receive the files, or choose **"All"** to pre-populate files to all of the GFC Edges connected to the GFC Core.
 - b. From the **"Datacenter File Server"** drop-down menu, select the file server with the data to be pre-populated.
 - c. In the **"UNC Path"** field, enter the UNC path for the file or directory to be pre-populated (for example, `\\<server name>\<share name>\<directory>`).
 - d. **(Optional)** Enable the **"Recursive"** checkbox to make the pre-population job recursive, which transfers the files in the indicated directory as well as all its subdirectories. Pre-population jobs that are not recursive only transfer the files in the directory indicated by the path; they do not transfer files within any subdirectories.
 - e. **(Optional)** Enable the **"Metadata Only"** checkbox to only prepopulate Edge instances with specified Metadata. If this is unchecked, specified directories and files will be written to the Edge's local file cache.
 - f. **(Optional)** Enable the **"Filter by Modified Time"** checkbox to pre-populate only those files modified within a specified time interval. Click the drop-down menu to specify a time frame (minutes, hours, days) then type the number of minutes (between 0 to 59), hours (between 0 to 23), or days (between 0 to 31) in the text box.
 - g. **(Optional)** To pre-populate only specific types of data, click the dropdown box next to **"Filter by file type"** and select **"No Limit," "Include,"** or **"Exclude."** Type the file extensions (case sensitive) of the files to include or exclude in the entry blank, for example, .docx, .pdf, .html, or .xlsx. File extensions should be preceded by a period and multiple extensions must be separated by commas.
 - h. In the **"Start Date/Time"** and **"End Date/Time"** fields, set the start and end dates and times for the initial and final data subject to pre-population. If this is a one-time job, the **"Start Time"** field needs to be populated at least 30 minutes in advance and the **"End Time"** field should be set 24 hours later.

- i. **(Optional)** Select the desired **"Repeat every..."** radio button if the push should repeat multiple times. For repeating jobs, the **"Start Date/Time"** specifies the beginning of the window for which a repeating job can occur. A repeating job will begin on the time and days specified in the **"Frequency"** column, as long as those days are within the **"Start Date/Time"** and **"End Date/Time"** window. Set the end date and time for a repeating job using the drop-down menus next to the **"End Time"** field. Select a **"Frequency"** radio button to select the frequency the push job will repeat.
- j. To repeat by day interval: Click the **"Repeat every <day>"** radio button. By default, the repetitive push job is scheduled to repeat every day at the specified time. To repeat the job on other dates, click the drop-down list and select one of a series of dates ranging from every day to every 10 days or every fifteenth day. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur.
- k. To repeat by day of the week: Click the **"Repeat every <day of the week>"** radio button and click the drop-down list to select the day of the week the pre-population job could occur. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur on the specified day.
- l. To repeat by date of the month: Click the **"Repeat every <day of the month>"** radio button, then click the drop-down list to select the numerical date of the month that the pre-population job should occur. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur.

Note: Jobs scheduled for the fifteenth and thirtieth of the month will only occur once in February, on the 15th. Since it only has 28 or 29 days, the job will not repeat again until the next scheduled date on the 15th of March. Other months that have only 30 days will not complete the Pre-population job if it is specified to execute on the 31st.

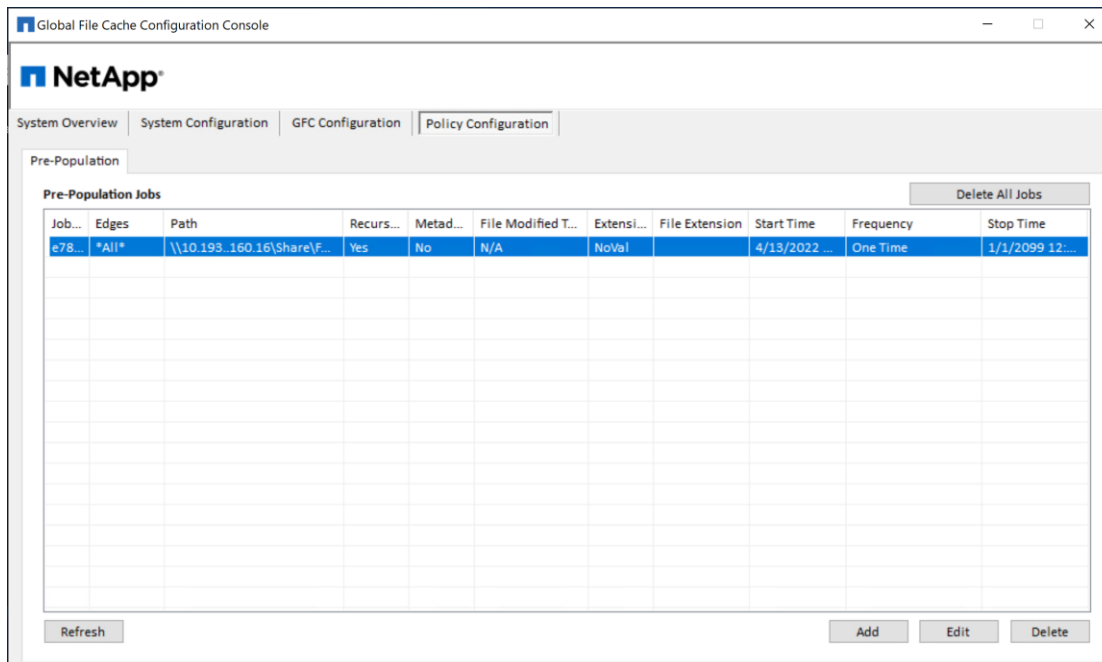
4. Click **"Apply"** to commit the pre-population job.
5. The **"Add Pre-Population Job"** window will close, and the new job will display in the table on the Pre-population page.
6. To configure a second scheduled pre-population job, repeat the process.
7. To edit a Pre-population job, click to highlight the job you wish to change and click the **"Edit"** button to change parameters.
8. Jobs can be deleted by highlighting the desired job and clicking the **"Delete"** button and confirming the action.

Note:

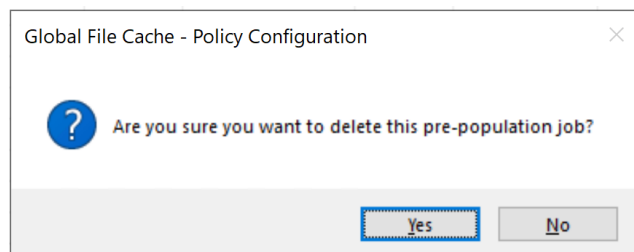
1. When scheduling pre-population jobs, all job times are relative to the time zone of the GFC Edge instance
2. Pre-population jobs should be scheduled at least 30 minutes ahead of the current time in the Edge's local time zone to allow Edges to pick up the newly scheduled jobs
3. Pre-population jobs should be scheduled to run during non-business hours. Running pre-population jobs during business hours will impact user performance.
4. Pre-population can be listed, added and deleted using the GFC PowerShell scripts. See Appendix C for more details and examples

10.2 To delete a scheduled Pre-Population Job

1. Open the Global File Cache **Configuration Console**.
2. Click the **"Policy Configuration"** tab.



3. Select the job to be deleted from the list of jobs displayed.
4. Click “Delete” button that will pop up a confirmation message.

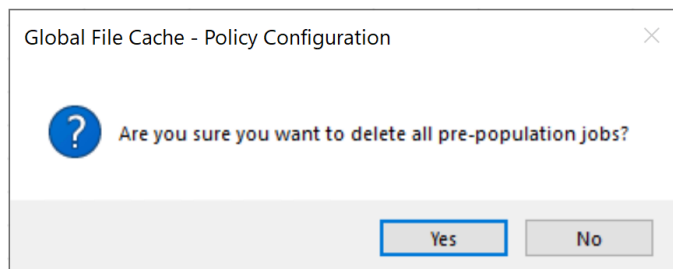


5. Click “Yes” button to confirm.
6. The selected job would be deleted from the pre-population job list.

10.3 To edit a scheduled Pre-Population Job

1. Open the Global File Cache **Configuration Console**.
2. Click the “**Policy Configuration**” tab.

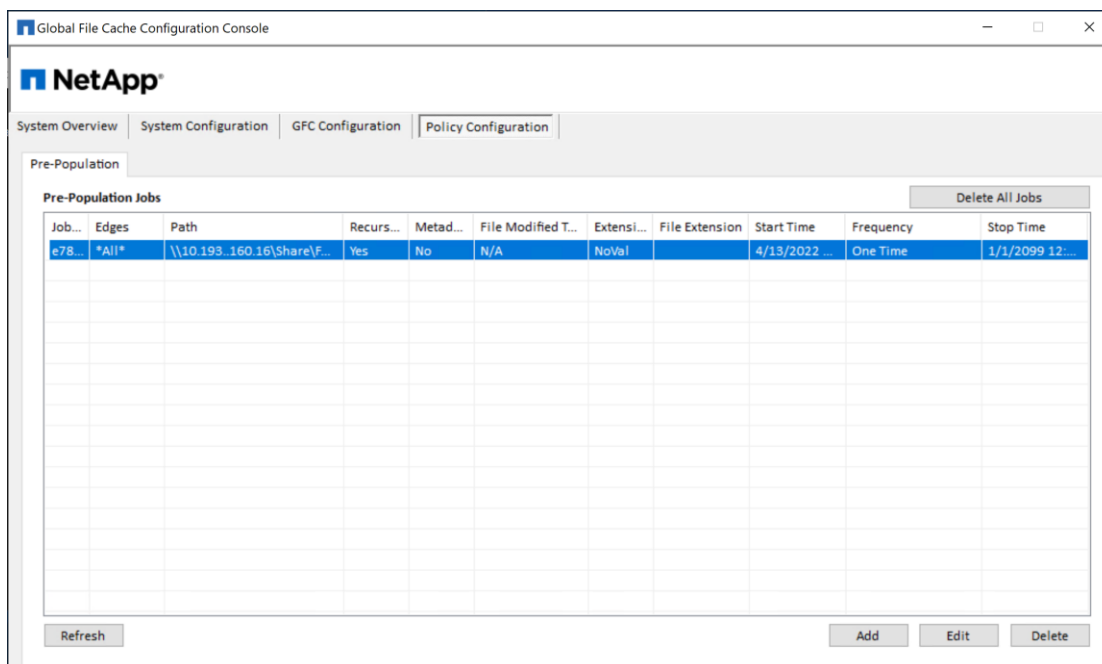
3. To Delete all the jobs in pre-population jobs list, Click the “Delete all Jobs” button located on the top right corner of the screen.
4. A confirmation pop up message is displayed.



5. Click “Yes”.
6. After this step, all jobs in the pre-population jobs list will be deleted.

10.5 To refresh the pre-population job list

1. Open the Global File Cache **Configuration Console**.
2. Click the “**Policy Configuration**” tab.



- 3.
4. In order to refresh the job list that has been configured on the LMS instance or from a different core instance, click “Refresh” button located in bottom left of the Configuration UI.
5. The job list will be refreshed and the list will be updated with latest job list information.

11 DFS Namespace Integration

Distributed File System (DFS) allows administrators to group shared folders located on different servers by transparently connecting them to one or more DFS namespaces. A DFS namespace is a virtual view of shared folders in an organization. Using the DFS tools, an administrator selects which shared folders to present in the namespace, designs the hierarchy in which those folders appear, and determines the names that the shared folders show in the namespace.

When a user views the namespace, the folders appear to reside on a single, high-capacity hard disk. Users can navigate the namespace without needing to know the server names or shared folders hosting the data. DFS also provides many other benefits, including fault tolerance and load-sharing capabilities, making it ideal for all types of organizations.

DFS namespace allows customers to present a 'single pane of glass' to their end users, regardless of the location they're in. The intelligence of Active Directory Sites and Services and client workstation's Partition Knowledge Table (PKT) allows the users to transparently access their centralized data through the 'nearest' NetApp Global File Cache (GFC) caching instance in their site and allow for failover to the 'native' central target in case of a local branch office outage.

More information on DFS: [https://technet.microsoft.com/en-us/library/cc782417\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc782417(v=ws.10).aspx)

11.1 DFS Design

The Microsoft Distributed File System (DFS) is a set of client and server services that allow a large enterprise to organize many distributed Server Message Block (SMB) file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the event of failure or heavy load by allowing shares in multiple locations to be logically grouped under one folder or DFS root. This can be configured in a domain-based or standalone configuration.

i.e. `\\corporate.local\root\share\folder`

Direct Share Mapping

Clients are given network-path mapped drives, which connect directly to the Edge appliance cache. This is usually done with a UNC path of the client folder, for example:

i.e. `\\< GFC edge>\<FASTData>\<FAST Fabric ID>\<file server>\<share>\<folder`

Configure Windows Server 2016 or 2019 Domain-Based DFS for GFC

Objectives:

Provide a unified namespace solution for both GFC Cached file/folder structures.

Introduce Client-side referral-based failover/failback solution based on Windows PKT info.

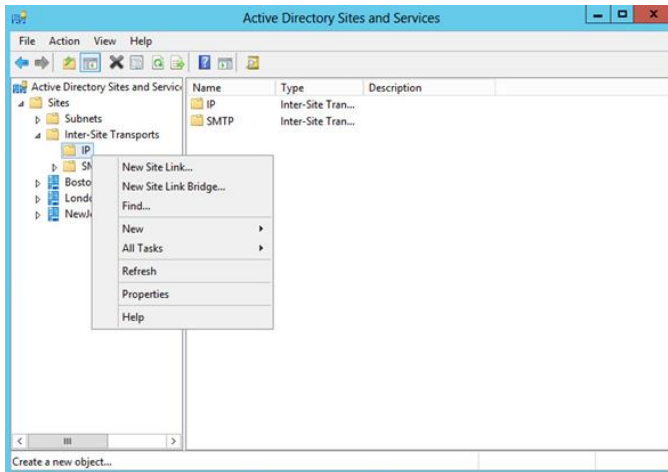
Exclude ANY other targets from the Windows Client referral list.

11.2 Site Definitions and Site Links

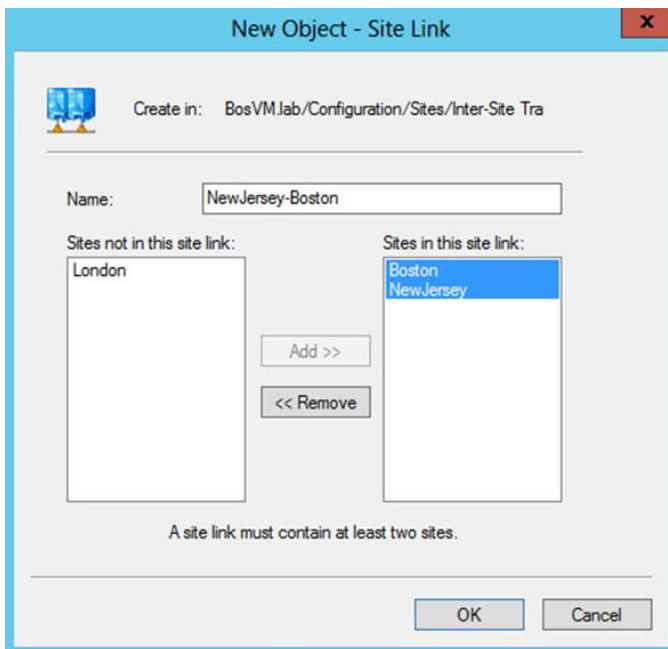
Each Active directory site/subnet must be defined in Active Directory Sites and Services. In order to document the logical network topology, which allows efficient replication of Active Directory; all subnets must be included and linked to a specific site definition.

It is recommended to configure site links based on a star-topology, i.e. Edge1 -> HQ (cost 200), Edge2 -> HQ (cost 500), but include the physical network topology in the design process of configuring Active Directory sites. If no altered Active Directory replication traffic is in place, you can keep the site costs the same (200). Site links define the scope of DFS Management target evaluation.

1. Create Site Links: (if more than two sites)
 - a. Open "Active Directory Sites and Services"

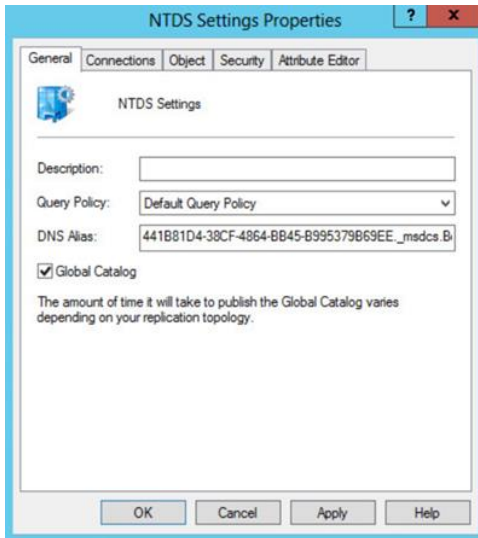


- b. Expand “Inter-Site Transports”
- c. Right click “IP”
- d. Select “New Site Link”
- e. Type a name describing which sites will use this link (i.e. NewJersey-Boston)

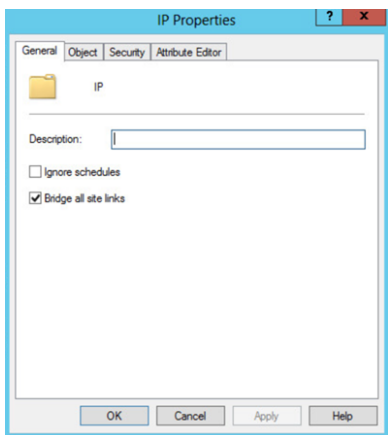


- f. Select sites from “Sites not in this site link”
 - g. Click “Add”
 - h. Click “OK”
- Repeat steps d-h for each site link that needs to be created.
2. Configure “Query Policy” and Global Catalog:
 - a. Double click on a site
 - b. Double click “Servers”
 - c. Select available Domain Controller within the site

- d. Right click **"NTDS Settings"** and select **"Properties"**
- e. Set the Query Policy to **"Default Query Policy"**
- f. Check **"Global Catalog"**
- g. Click **"OK"** to commit the changes



3. Bridge Links:
 - a. Return to the main screen and double click **"Inter-Site Transports"**
 - b. Right click **"IP"** and select **"Properties"**
 - c. Confirm **"Bridge all site links"** is checked.
If it is not checked, closest site selection will fail.
 - d. Click **"OK"** to commit the changes.
 - e. Close **"Active Directory Sites and Services"**



11.3 DFS Root Configuration Default

A domain-Based DFS root namespace includes all sites based on Lowest Cost, which can introduce issues in terms of client failover. In DFS Management you can configure target failover solution based on **"Exclude Targets outside of Clients site"** to circumvent that scenario. For each namespace, configure **"Allow Client Failback."** Please follow the steps below to complete the DFS configuration.

If you manage the DFS root from a Windows Server instance, you can generate the following structure as follows. In the exhibit below we are using "\\BosVM.Lab\DFSroot" as a namespace, and "TalonFAST" as a target referral.

1. Install the DFS management snap-in

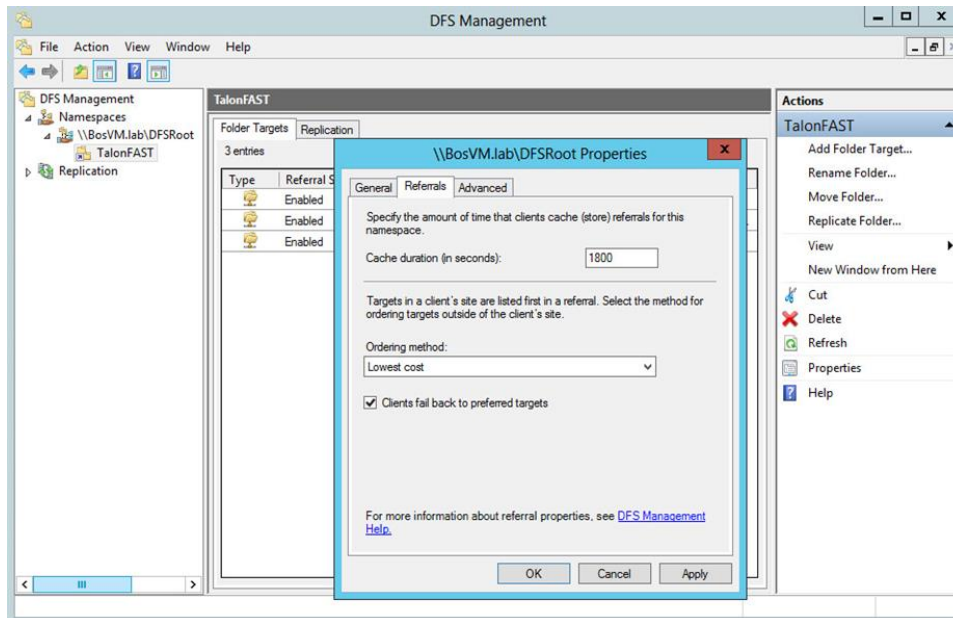
The DFS Management snap-in has been included since Windows Server 2003 R2 and allows extensive configuration of a DFS infrastructure. In order to comply with GFC best practices you should use the management snap-in. This is installed while adding the DFS Namespaces role via the Windows Server 2016 or 2019 **"Add Roles and Features Wizard"** found in the Server Manager console.

More information on installing DFS can be found at

https://msdn.microsoft.com/en-us/library/cc731089.aspx?f=255&MSPPErrors=-2147217396#BKMK_UI

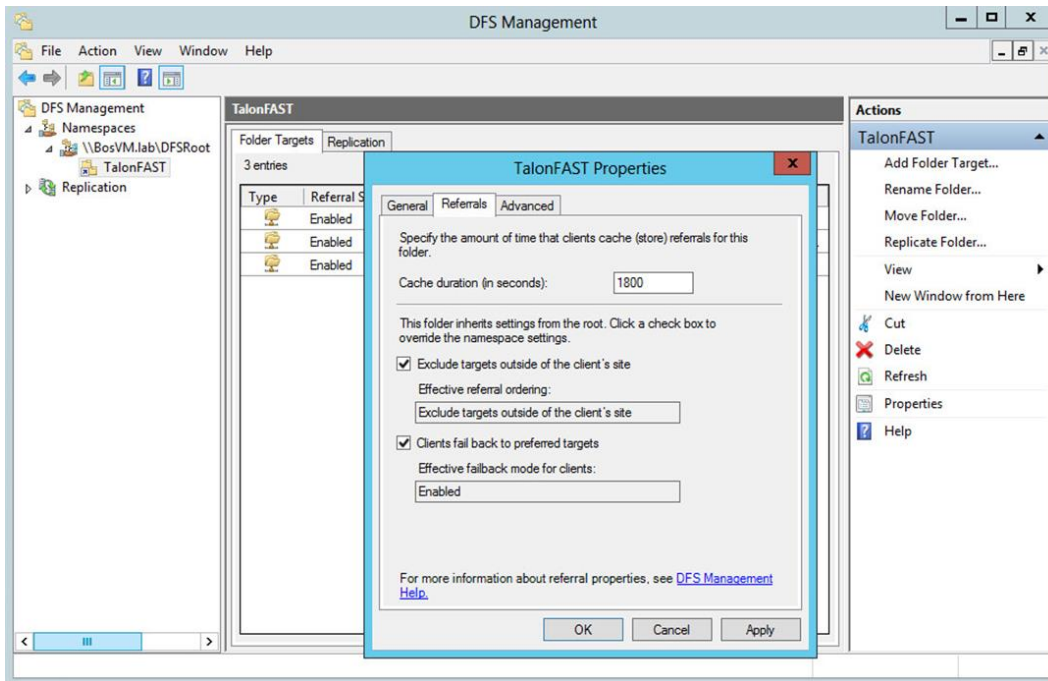
2. Configure the DFS namespace as follows

- Right-click the Namespace **"\\BosVM.lab\DFSroot"** and click **"Properties"**.
- On the Referrals tab, set the **"Cache Duration"** to 1800 seconds.
- Set the Ordering Method dropdown to **"Lowest Cost"**.
- Check the box **"Clients fail back to preferred targets"**.
- Click **"OK"** to confirm the configuration change.



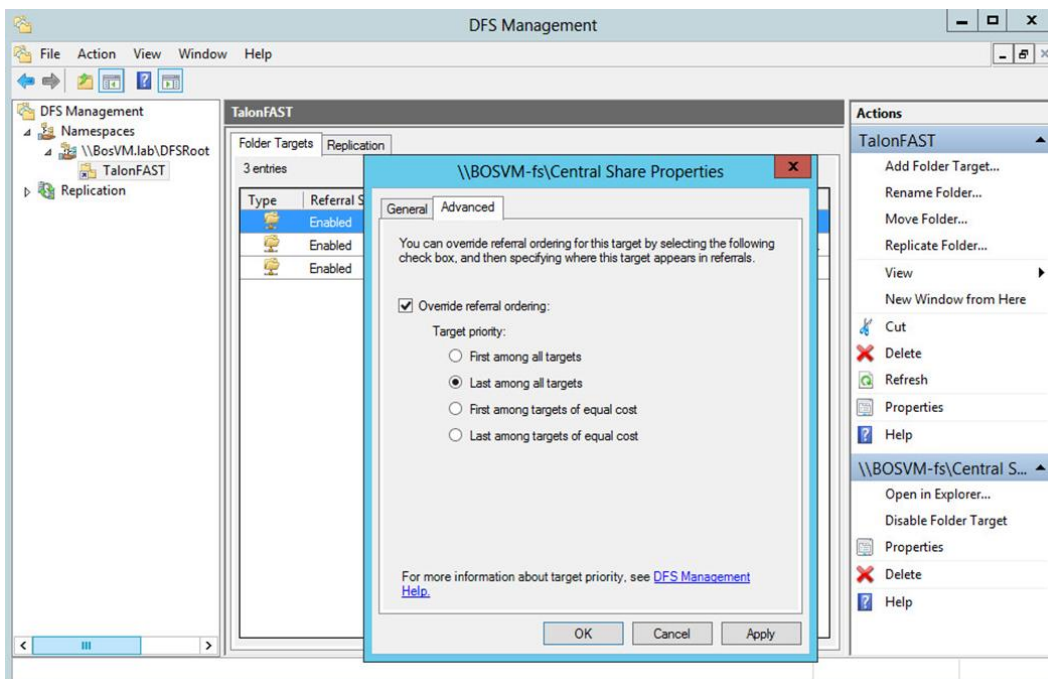
3. Configure the DFS referral to exclude any target references

- Right-click the referral and select **"Properties"**.
- For the reference, check the box for **"Exclude targets outside of the client's site"** and **"Clients Failback to preferred targets"**.
- Set the **"Cache duration"** to 1800 seconds.
- Click **"OK"** to confirm the configuration change.



4. Open the Target Referrals listed in the root folder referral list.

- Right-click the native backend referral, and click **"Properties"**.
- Click the **"Advanced"** tab and check the **"Override referral ordering"** box and change the priority to **"Last among all targets"**.
- Click **"OK"** to confirm the configuration change.
- For each GFC Edge referral, right-click the referral, select **"Properties,"** enter the Advanced tab, and ensure that the **"Override"** setting for referral ordering is unchecked. Click **"OK"** to confirm the configuration change.



Repeat steps 3 and 4 for each referral and target referral list in the namespace.

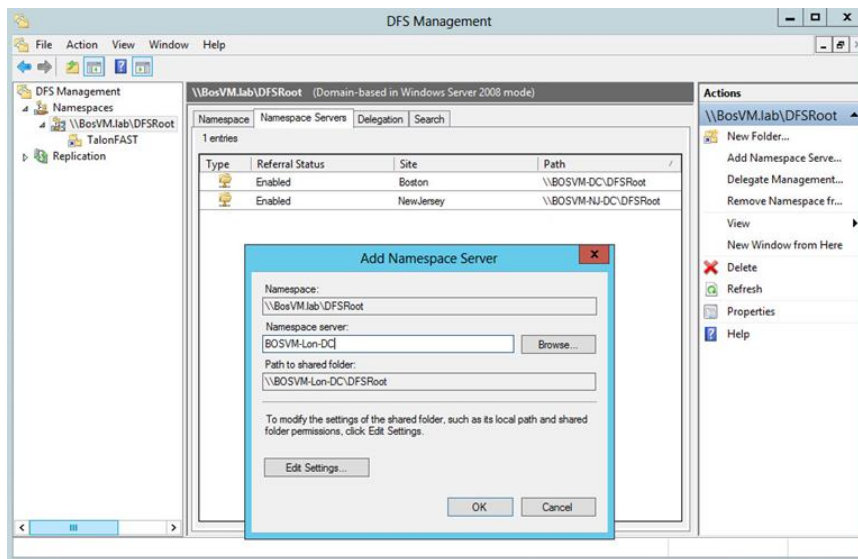
Make sure that your target referral list contains the FQDN of the referral path.

With the above settings, Windows XP SP2, Vista, 7, or 8 clients will only receive the local GFC edge and the native back-end file server referral in its "DFS Tab" or Partition Knowledge Table (PKT).

5. Final Steps

In order to complete the configuration of a distributed Domain-Based DFS infrastructure, create a replica of the namespace on each domain controller. By creating a local namespace replica, you will increase file system operations performance, as the clients will use their local domain controller. Completing the steps below can be done remotely, from any Windows Server or client, using the DFS Management console:

- Right-Click the "\\BosVM.lab\DFSroot" namespace.
- Click "Add Namespace Server".
- Select the Domain Controller which will host a replica of the DFS root.
- Complete the steps in order to create a DFS root replica on each Domain Controller.



Conclusion:

By using the FQDN as a UNC path, you will introduce a unified namespace and failover solutions for all users in your enterprise network. This simplifies the process of managing data structures, collaborating data between users, and mapping drives on Microsoft Windows clients.

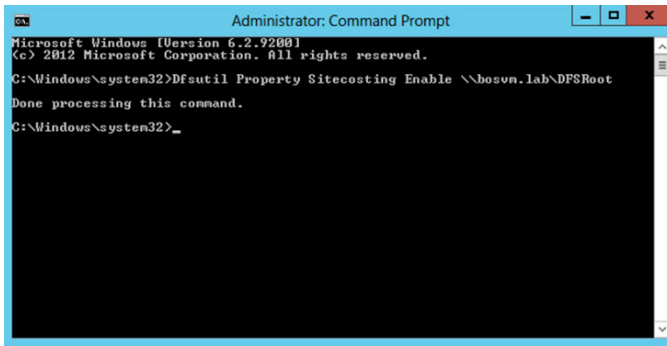
By utilizing a Domain-Based DFS root, using "Exclude Targets outside of Clients site" functionality for the target referral, in conjunction with the "Client-Side Target Failback" script, you will be guaranteed proper failover/failback operations. Microsoft Clients will never failover to any unwanted path.

11.4 Site Costing Configuration

For closest site selection to work on link targets, Inter-site Topology Generator (ISTG) must be running on Windows Server, and for closest site selection to work on link and root targets, all domain controllers must be running Windows Server 2016 or 2019. Please use DFSUTIL.exe from the command line to enable site costing:

Windows Server 2016 or 2019: Dfsutil Property Sitecosting Enable \\bosvm.lab\DFSroot.

Figure 20)



Domain Controller (DC) site costing is controlled separately on each DC using the following registry key:

HKLM\System\CurrentControlSet\Services\Dfs\Parameters\SiteCostedReferrals

DWORD 1 or 0

Please validate that the registry entry is applied and schedule a reboot of the respective DC.

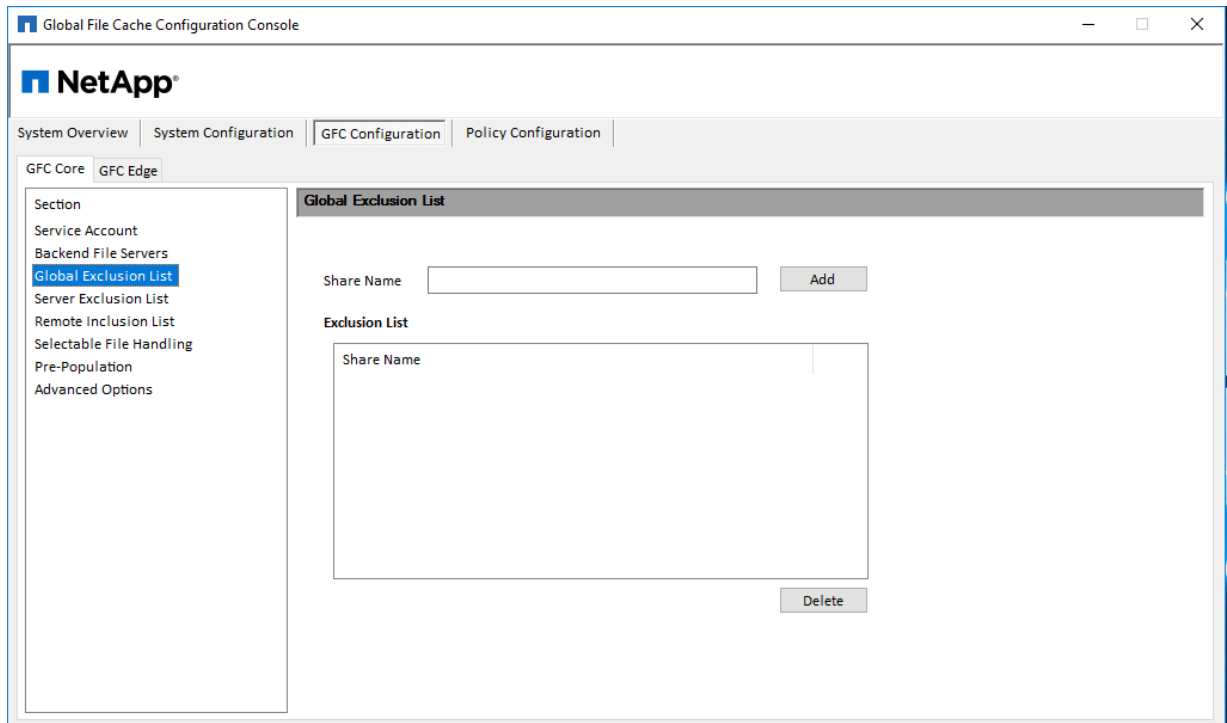
11.5 GFC Global Exclusion Configuration (DFS)

When the DFS root is being hosted by the same backed file server that you are configuring for optimization with GFC, it is recommended that you exclude the local DFS root share from being advertised.

For example, if the “**\\BosVM.lab\DFSroot**” DFS root is being hosted on Fileserver1, and Fileserver1 is also a server that you are advertising through GFC, you should exclude the “**DFSroot**” share.

This can be adjusted in the “**Global Exclusion List**” configuration on the GFC Core configuration page.

Figure 21)

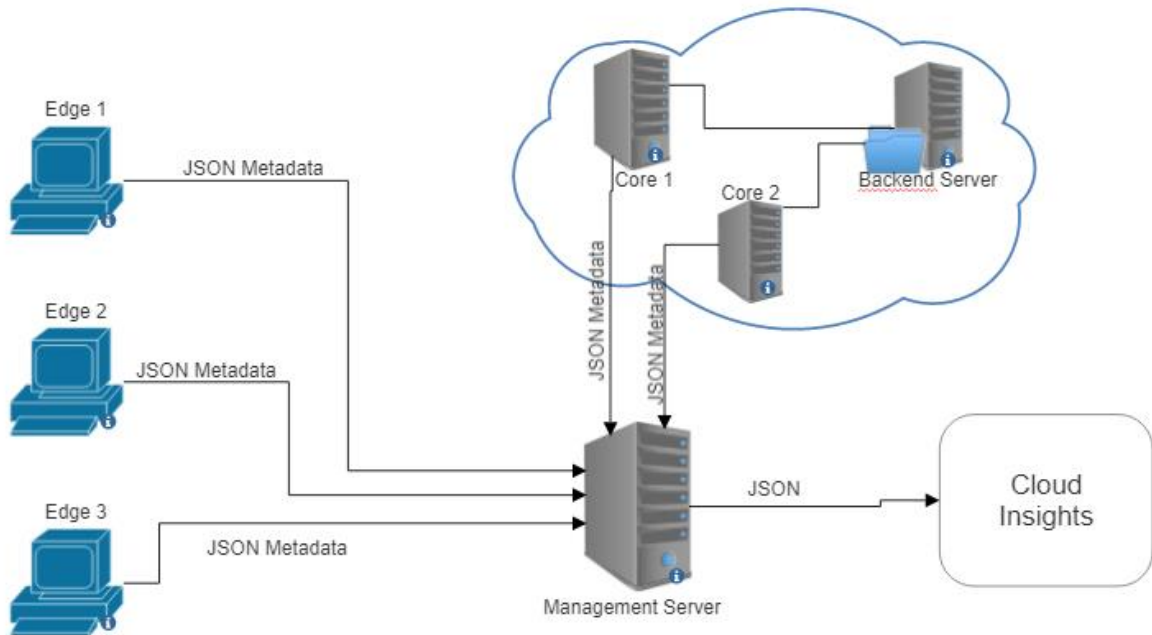


Note: Using a DFS root as your backend file server is not recommended and can lead to data loss.

12 NetApp Cloud Insights

NetApp Global File Cache (GFC) supports integration with NetApp Cloud Insights Product. NetApp Cloud Insights gives complete visibility into the infrastructure and applications. Cloud Insights can be used to monitor, troubleshoot and optimize all resources and applications across entire technology stack, whether it's on-prem or in the cloud.

GFC software includes the CIAgent that is running on every GFC instance. This agent will collect configuration and monitoring information and send them to Cloud Insights. CI Agent that is running on the GFC Edge and GFC Core will send the information to LMS. LMS in turn forwards this information to Cloud Insights. GFC License Manager Service acts as a proxy to send all the information to Cloud Insights.



12.1 Prerequisite

NetApp Cloud Insights should be pre configured and the appropriate license should be obtained from the Sales team.

Minimum GFC release that supports NetApp Cloud Insights is 2.0.0 build 15

12.2 Cloud Insights API Token generation

Tenant Account: <https://<tenanturl>.cloudinsights.netapp.com/>

1. Login to **Cloud Insights Environment** using appropriate Credentials.
2. Go to Admin -> API Access. It will show all the available access tokens.
3. Add a new API Token by clicking on **API Access Token**. A popup window will be displayed to Create an API Access Token.
4. Enter the Name for API Access Token in the text box.

5. Enter the Description in the text box.
6. Select what type of APIs will this Token be used to call.
7. Select Permissions for this Token.
8. Select Expire of Token.

Create an API Access Token

×

Name

Sample Token

Global File Cache sample token

What type of APIs will this token be used to call?

Alerts, Data Collection, Data Ingestion, Log Ingestion and User Management Monitoring ▼

Permissions

Read/Write ▼

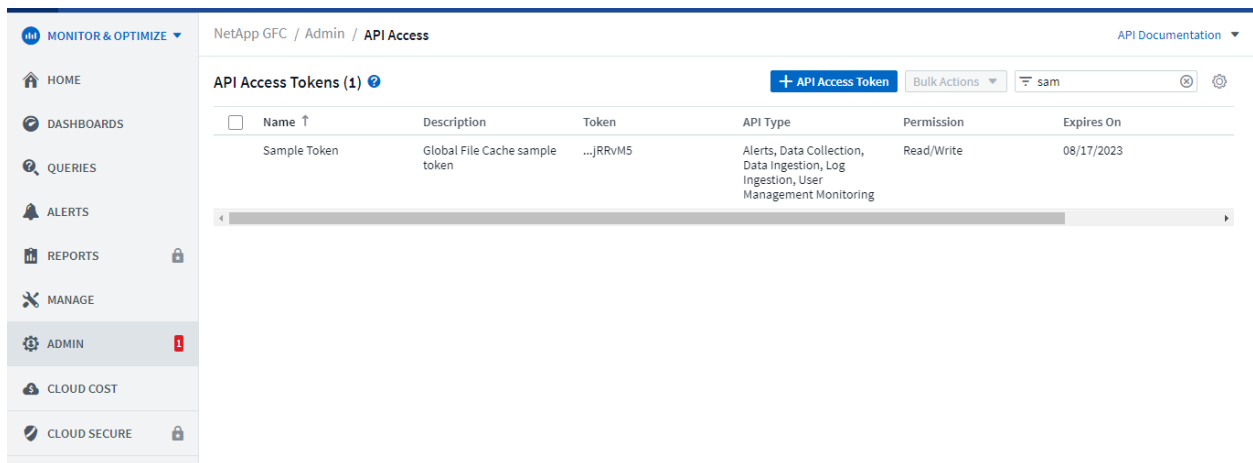
Token Expires In

1 Year ▼

Cancel

Save

9. After filling all the fields click on **save**.
10. Once Token Details are saved API token will be generated. Click on a **copy** and store the token somewhere.



Once the Create an API Access Token window is closed then the token cannot be accessed

12.3 Cloud Insights Configuration

Open the Global File Cache Configuration Console on LMS Instance.

1. Click 'System Configuration' tab and then click CI Configuration sub tab.
2. Enter the Cloud Insights URL in the text box.
3. Enter the API Access token in the text box.
4. Click "Register Instance to CI"
5. Click Yes to confirm registration

Global File Cache Configuration Console

NetApp®

System Overview | System Configuration | GFC Configuration | Policy Configuration

License Manager | Legacy Licensing | CI Configuration | Cloud Manager Configuration

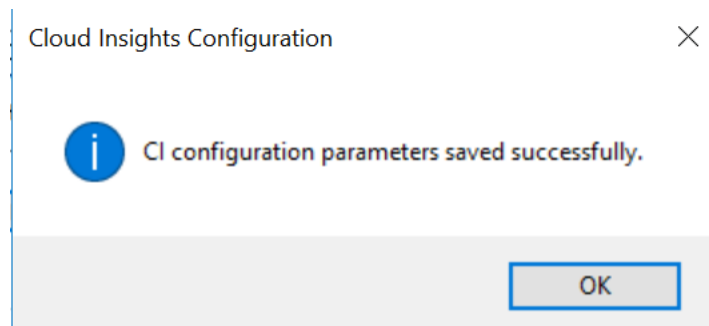
Cloud Insights Configuration

Associate this instance with Cloud Insights

Cloud Insights URL

API Access Token

Register Instance to CI

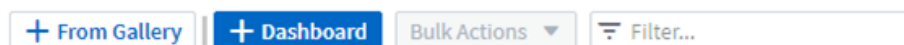


All Edges send the data to CI through LMS. This configuration is performed on LMS instance only.

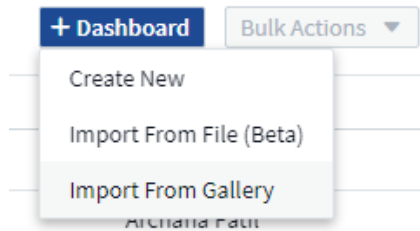
12.4 Dashboards

12.4.1 Importing GFC Dashboards into CI

1. Download the gfc-ci-dashboards-2.1.0.zip file from the netapp download site
2. Login to Cloud insights and click on Dashboards menu from left panel.
3. Press Ctrl and double click between the From Gallery and Dashboards button.



4. Now click on + icon of Dashboard button.
5. Select Import From File (Beta).

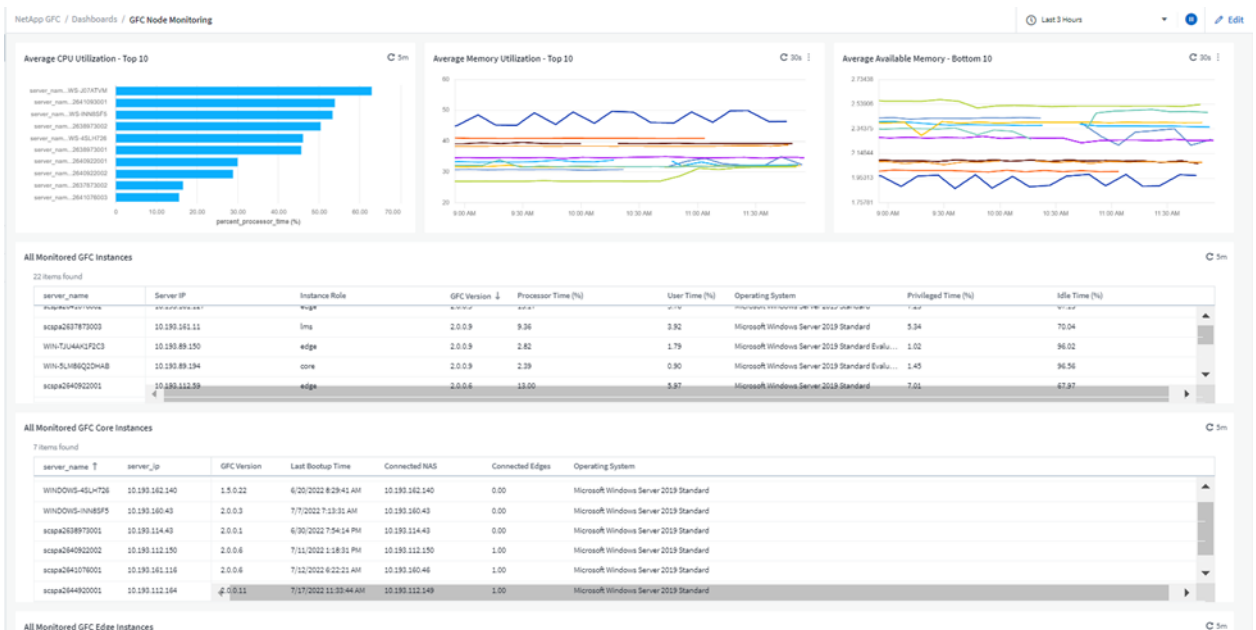


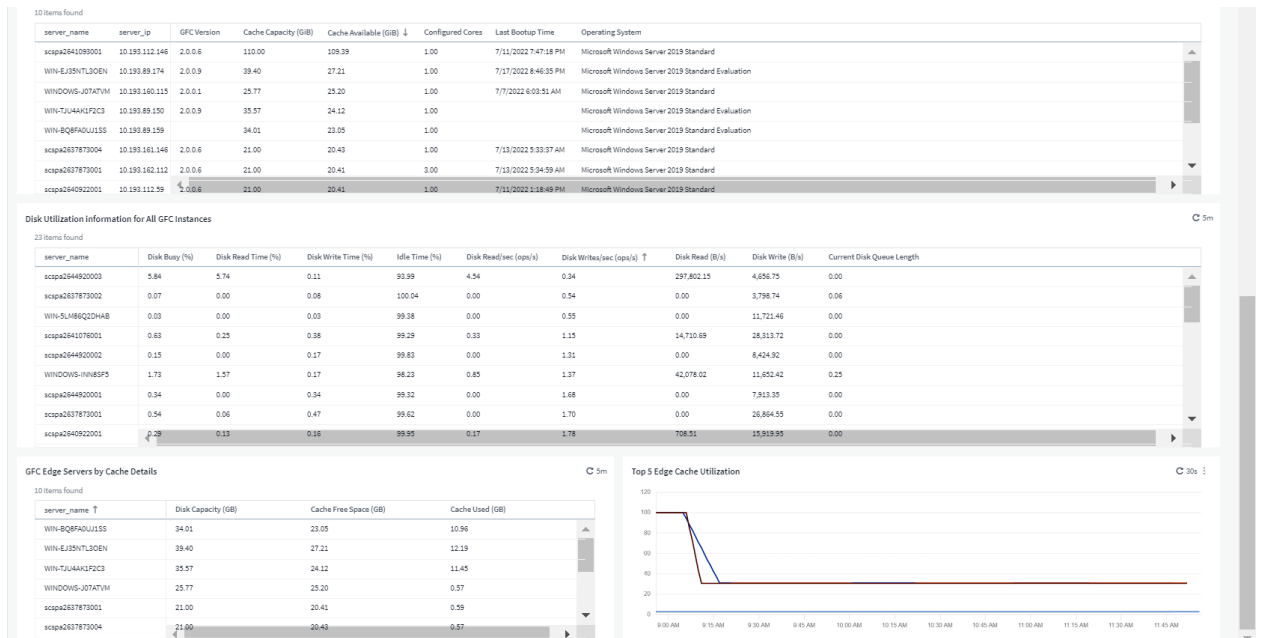
6. Import Dashboard pop-up should appear.
7. Select zip file to import and click on Import.
8. GFC Dashboards will be listed in Cloud Insights Dashboards.

12.4.2 GFC Node Monitoring Dashboard

Logon to Cloud Insights URL using appropriate credentials. Node monitoring dashboard has multiple widgets that show detailed information on GFC instances. Below are some of the widgets displayed in the Monitoring dashboard.

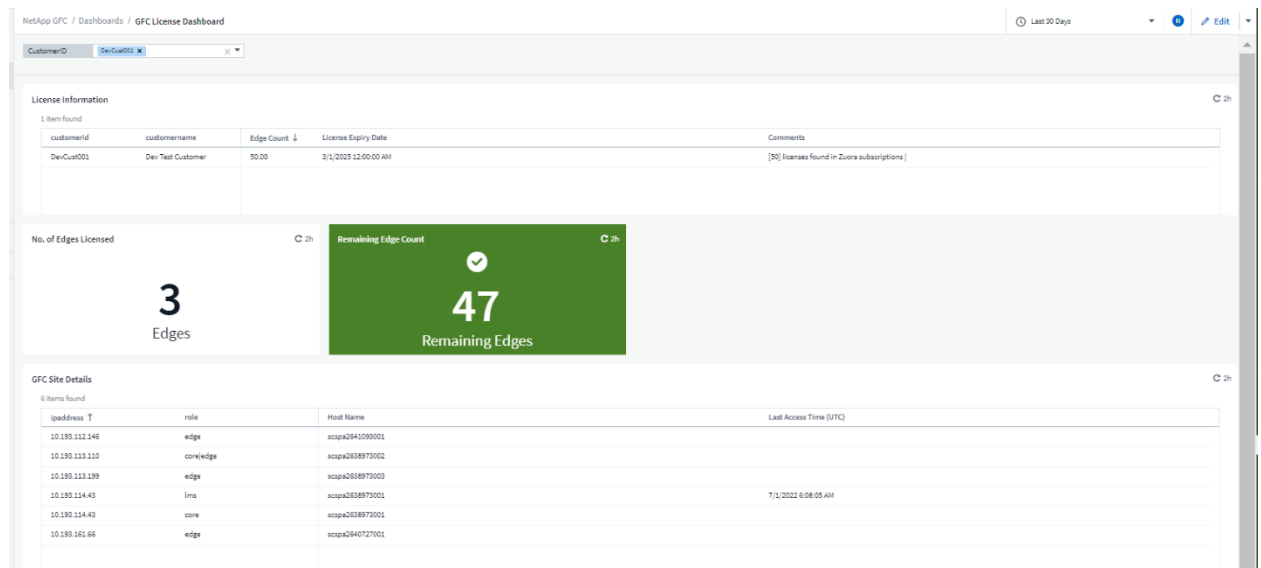
1. Top 10 instances with Average CPU utilizations.
2. Top 10 instances with Average memory utilizations.
3. Top 10 instances with less available memory.
4. Complete information of each GFC instance with server name, server ip, configured role, installed GFC version, processor time percentage, Operating System installed and other timers.
5. Complete information about GFC Core instances.
6. Complete information about GFC Edge instances.
7. Disk utilization on all GFC instances.
8. Display Cache free space of all GFC Edges
9. Show a chart to show top 5 Edge Cache utilization instances.



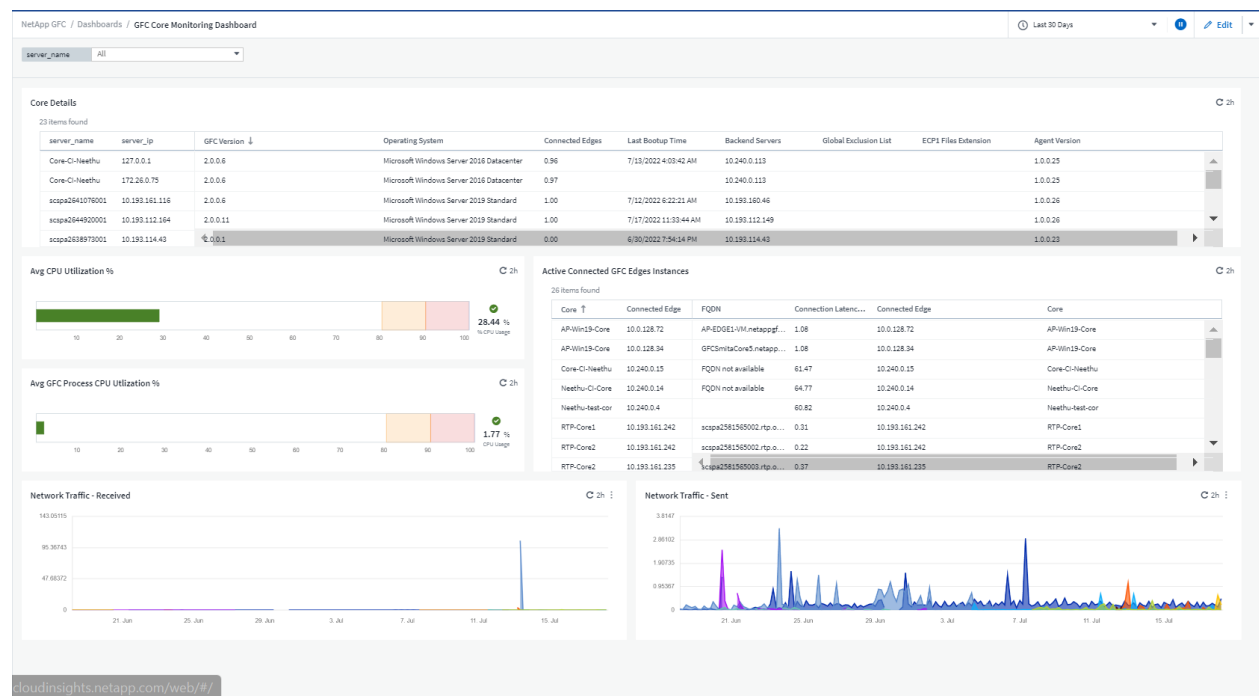


12.4.3 GFC Licensing Dashboard

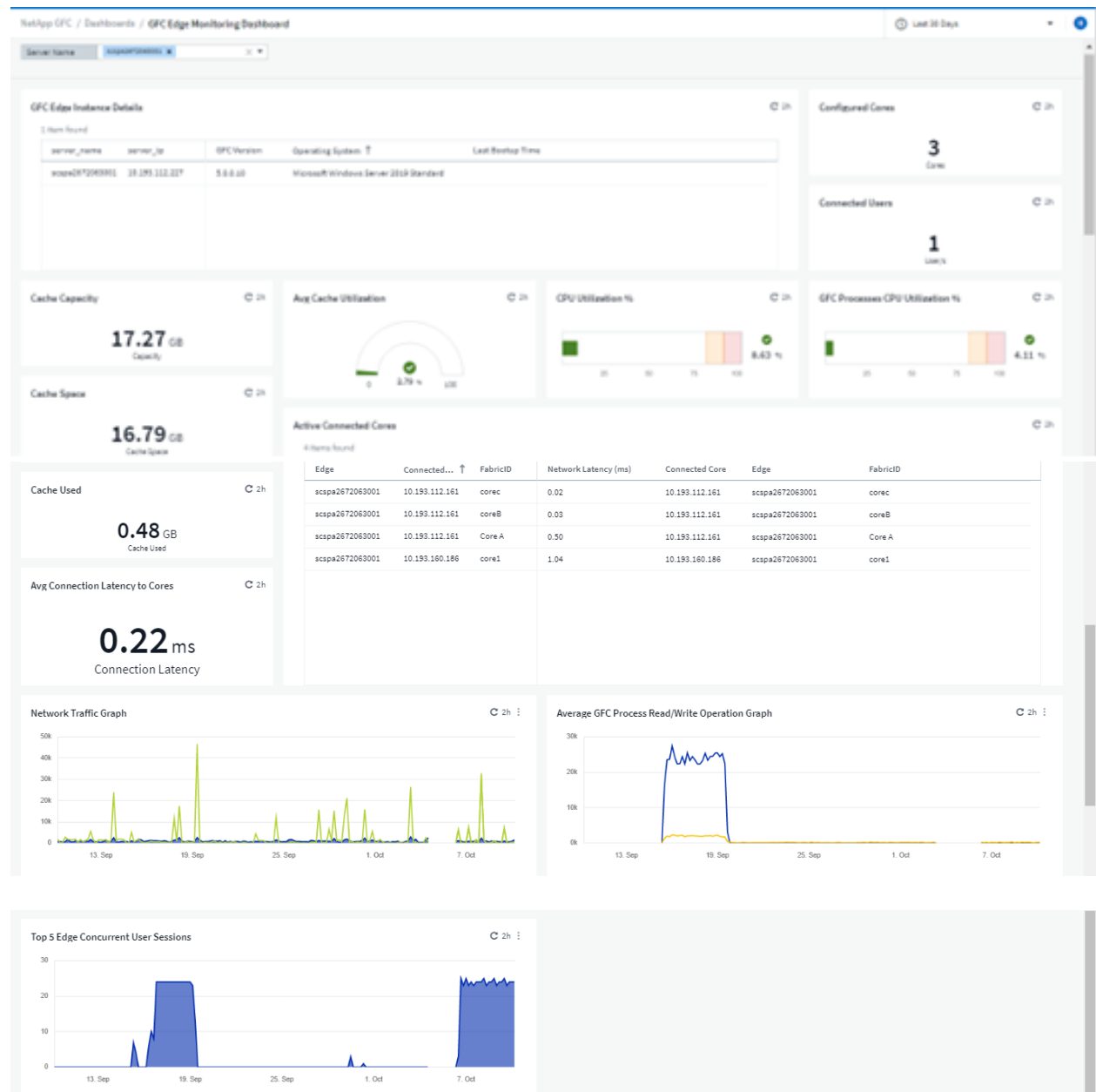
This dashboard shows information related to licensing data. The Licensing widget will display number of edges licensed and the total number of licenses along with licensed node information.



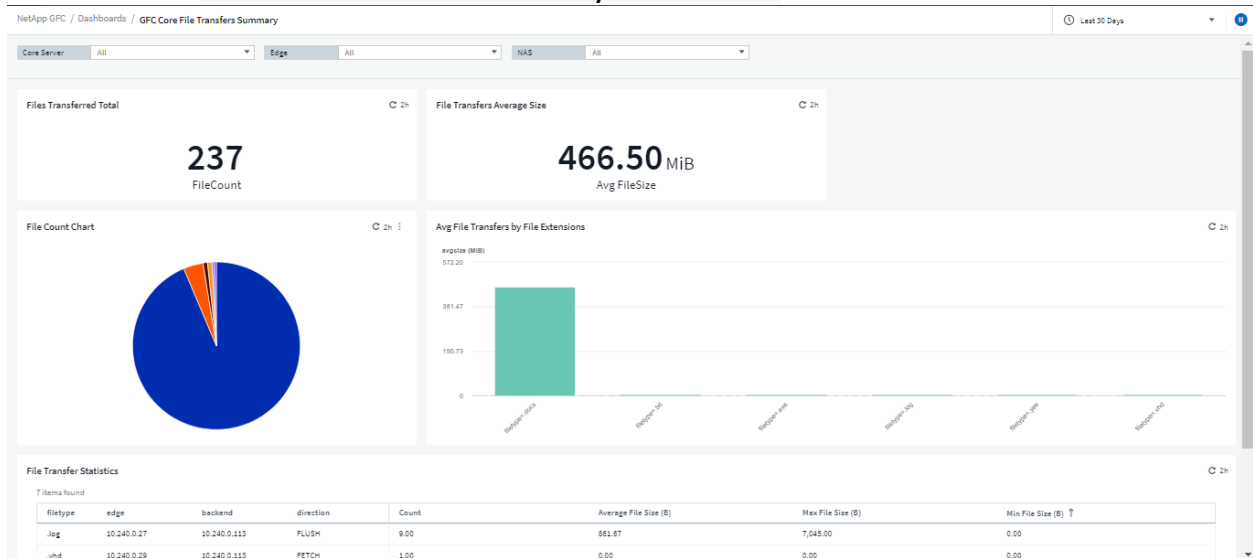
12.4.4 GFC Core Monitoring Dashboard



12.4.5 GFC Edge Monitoring Dashboard



6. GFC File Transfer Summary Dashboard



12.5 Alerts

NetApp GFC / Alerts / All Alerts Last 3 Hours

Active (4) Resolved (0)

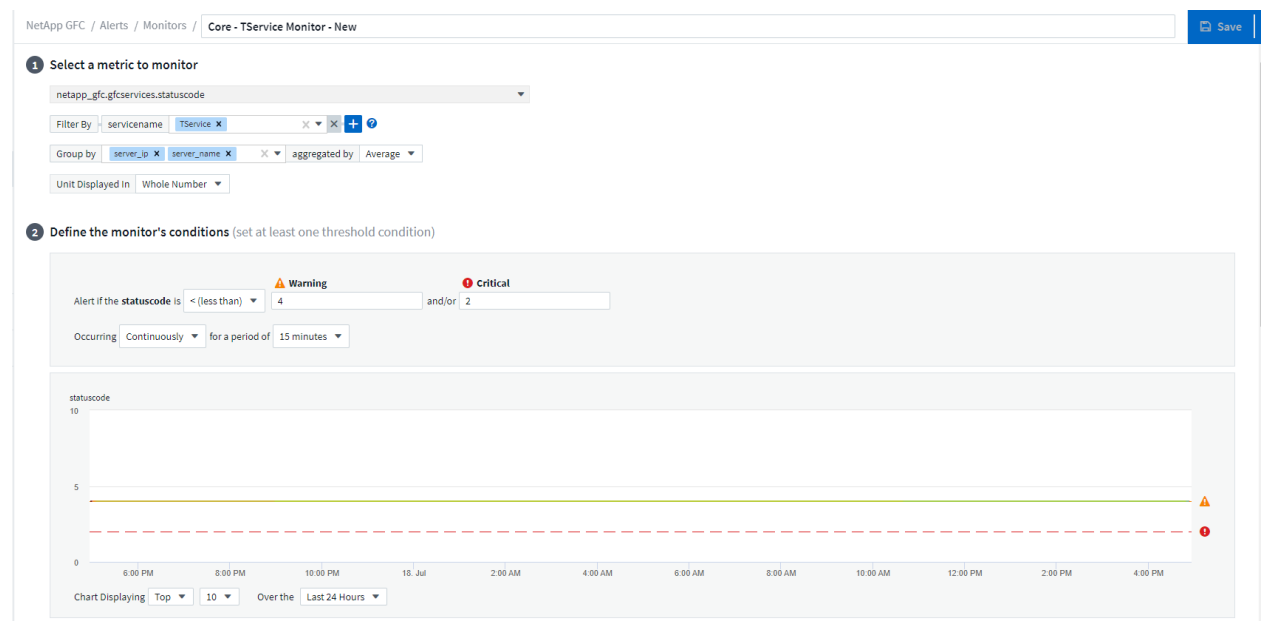
Filter By: status New X In process X currentSeverity Warning X Critical X

Alerts (4) Change All Alerts Status

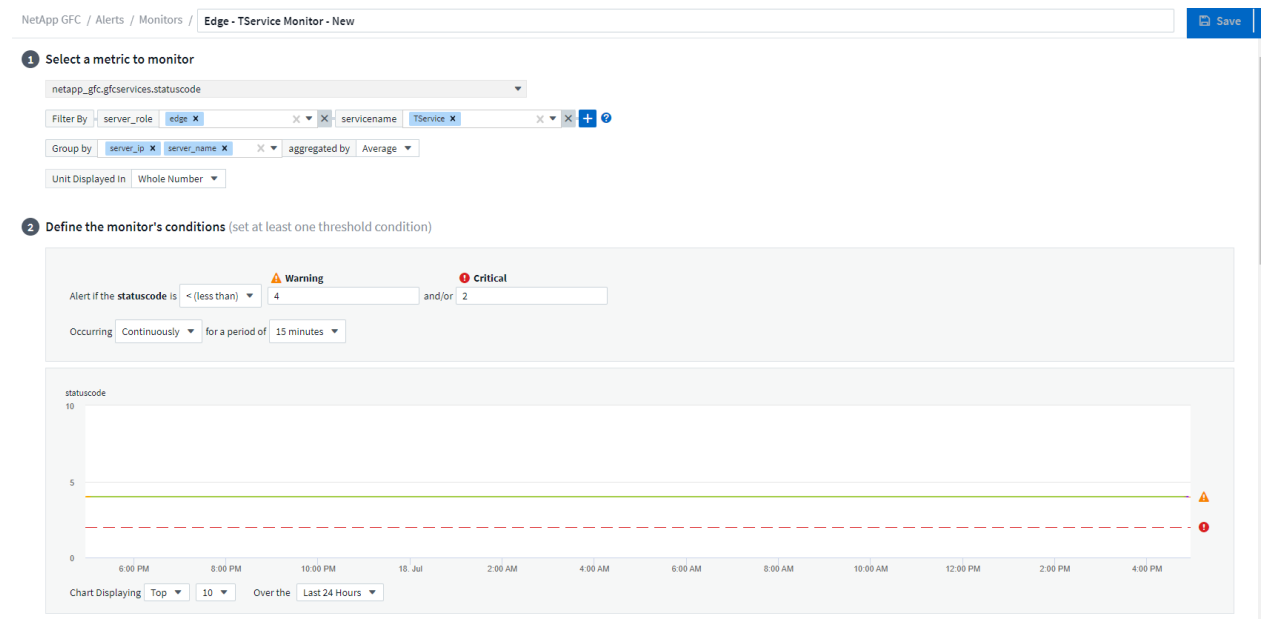
alertid	triggeredTime	currentSeverity	monitor	triggeredOn	status	hasCorrectiveActions
AL-862	6 hours ago Jul 18, 2022 11:05 AM	Critical	Core - TService Monitor - New	server_ip: 10.193.160.43 server_name: WINDOWS-INN85F5	New	✓
AL-855	3 days ago Jul 15, 2022 6:54 PM	Critical	Core - TService Monitor - New	server_ip: 10.193.89.194 server_name: WIN-SLM86Q2DHAB	New	✓
AL-847	5 days ago Jul 13, 2022 5:04 PM	Warning	Core - TService Monitor PLU	server_ip: 10.193.89.197 server_name: GFC-PLU-LMS	New	✓
AL-840	6 days ago Jul 12, 2022 2:56 PM	Warning	Core - TService Monitor PLU	server_ip: 10.193.89.151 server_name: GFC-PLU-CORE3-FB	New	✓

12.6 Monitoring

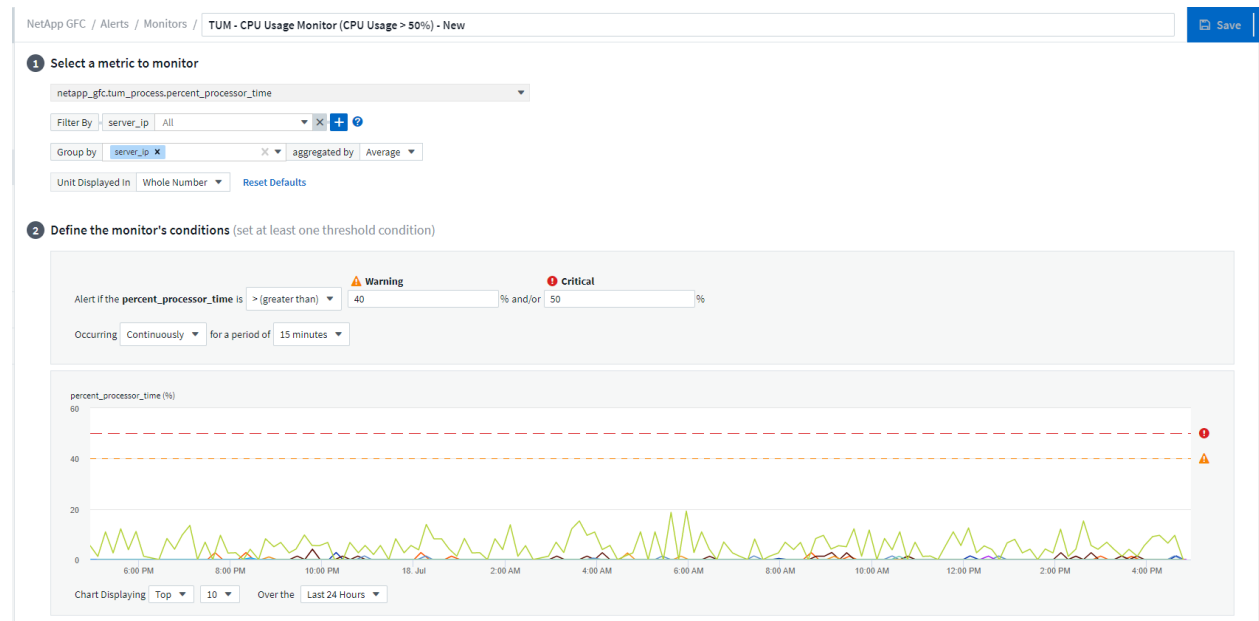
12.6.1 GFC Core TService Monitor



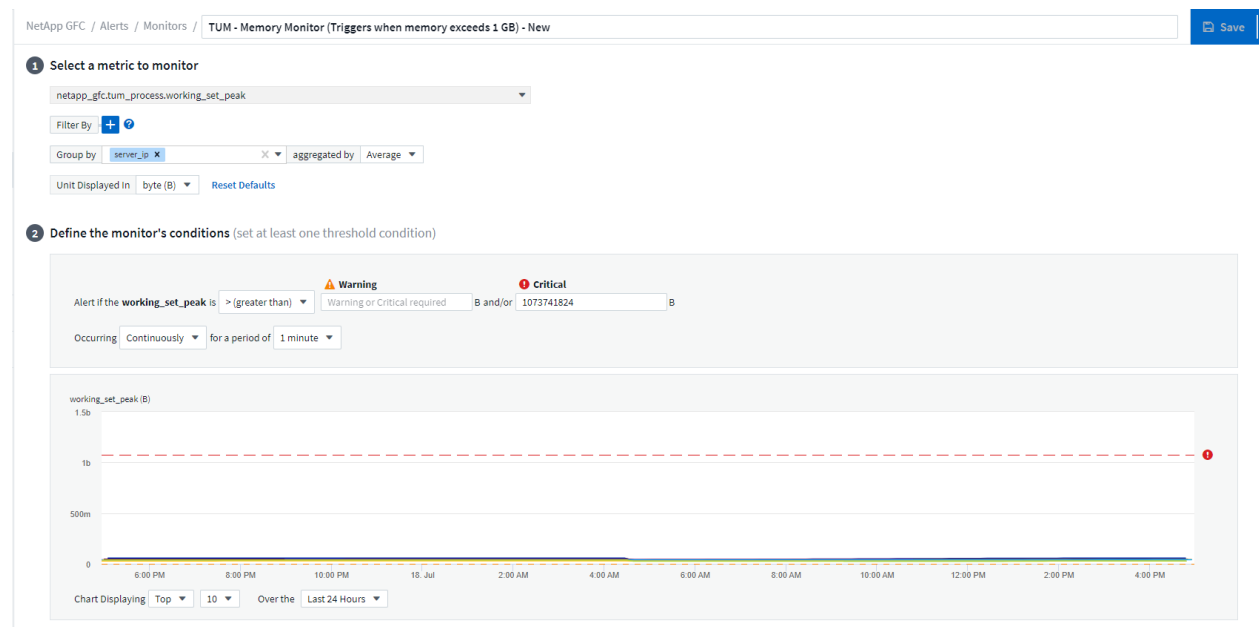
12.6.2 GFC Edge TService Monitor



12.6.3 GFC Tum CPU Usage Monitor



12.6.4 Tum Memory Usage Monitor



12.6.5GFC Edge Disconnection from Core Monitor

NetApp GFC / Alerts / Monitors / GFC Edge - Disconnection from Core

Edit log monitor

Filter in section 1 must not be empty. If alert resolution is based on log entry, section 3 filter also must not be empty.

1

Select the log to monitor

Log Source

logs.netapp_gfc.tum

Filter By

gfcrole

edge

eventid

337 - 337

8 items found

Last update 08/18/2022 12:58:46 PM

Refresh

timestamp	type	source	message
08/18/2022 4:33:56 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.228): error 10057.
08/18/2022 4:33:56 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.228): error 10057.
08/18/2022 4:33:56 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.228): error 10057.
08/18/2022 4:33:03 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.121): error 10057.
08/18/2022 4:33:03 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.121): error 10057.
08/18/2022 4:33:03 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.121): error 10057.
08/18/2022 4:33:03 AM	logs.netapp_gfc.tum	Tum	Error on connection(to 10.193.160.121): error 10057.

2

Define alert behavior

Create an alert at severity

Critical

 when the conditions above occur

4 times

 for a period of

1 minute

Associate this alert with

netapp_gfc.edgeserver

 objects identified internally by

server_name

 whose value found in the log in the column

machinename

 is an

exact match

116

User Guide

© 2023 NetApp, Inc. All Rights Reserved.

13 Client Application Requirements

13.1 Autodesk - Revit

Autodesk Revit users typically work in:

Revit Stand-alone Project File

Non-collaborative projects are often called “Stand-alone” projects. The project file is available from various locations, but typically used by one user at the time.

Revit Worksharing Central File

Collaborative projects are worked on with multiple users potentially from multiple sites. This may be in real-time or in a follow-the-sun schedule. A central file of the project is created and all users work across the network on this model. When a user wants to open a central file, the user should be opening the project through the “File” -> “Open” menu in the Revit application. When the central file is opened correctly in this fashion, a copy of the central file is placed locally on the user’s hard drive. There is a link formed between the central, authoritative file and the locally created copy of that central file.

Whenever the user wants to push updates to the central file and update their local copy with any changes in the central file from other collaborating users, they click the “Synchronize with Central” button.

The following application best practices must be adhered to when using the Autodesk Revit application on each NetApp Global File Cache (GFC)-enabled workstation:

Set the Revit Worksharing Frequency Update timer to Manual intervals

Users should routinely perform Central File Maintenance on the project to maintain file health (Autodesk Recommendation)

Before users create new local files through GFC, they should delete or archive/rename their existing local files and their backup folder. More information about this topic and general Revit best practices on Central Files can be found at <http://blogs.rand.com/support/2017/04/revit-central-file-maintenance.html>

Solving Revit UNC location awareness through a Unified Namespace

In order to use Revit with Worksharing enabled on a central model in a distributed branch office environment, it is required to implement a unified namespace such as a Domain-Based DFS Namespace which provides a unified naming convention for network stored projects and folders.

Adding .SLOG to the GFC Core(s) Selectable File Handling entries – Live Multisite Collaboration

Any Core servers which will be serving Revit files used in a live multisite collaborative situation, must have the .SLOG extension added to their Selectable File Handling entries.

Open Projects via Revit Menus

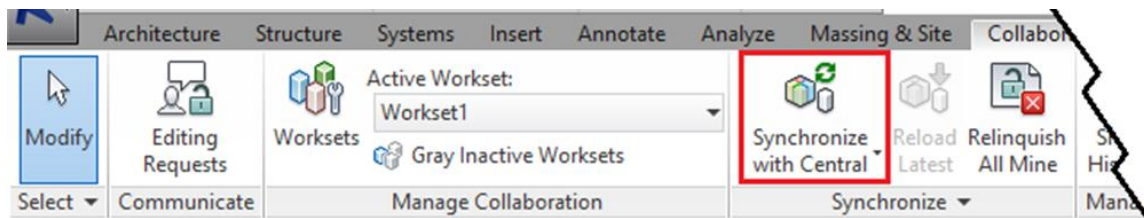
When a user wants to open a central file, the user must first open the Revit application and then the central file through the File -> Open option in the main menu.

Important: Do not open a central Revit file through Windows Explorer (Autodesk Recommendation).

If the central file is opened correctly, a copy of the central file is created locally on the user’s hard drive. A link is formed between the central file and the user’s local copy of the central file.

When the project opens, the user is making modifications to their local copy. When the user wants to push updates to the central file and update their local copy with any changes in the central file from other users, they click the “Synchronize with Central” button.

Figure 22)



Note: File saving time depends on number of changes and size of the project.

Borrow Worksets instead of Elements

When users create, add, or adjust single elements, checks are made with the Central Model and the borrowing requests are made to the affected users. When borrowing worksets, all elements of one type are 'owned' by a user and individual elements of that workset must be requested to be borrowed by other users.

Save Often, Sync less

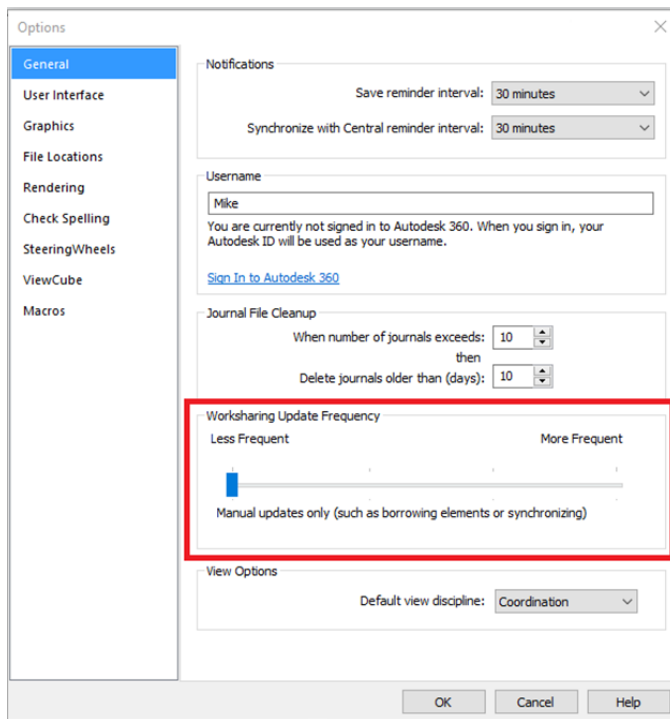
In order to reduce the total amount of data traversing the WAN, GFC recommends that users collaborating on a Revit worksharing project Save their project updates locally and Synchronize with Central less frequently. For example, Save as normal and sync to update other users' changes every few hours. Additionally, when working with a workset or elements, a synchronization will release the ownership which then needs to be regained after the sync completes. By reducing the number of times the central file is checked for updates and ownership of elements and worksets, this will provide an optimal work experience for all live collaborating users.


Controlling Worksharing Display Update Frequency in Revit

In Revit, the Central file is used to store the current ownership information for all entities and worksets in the project, and acts as the distribution point for all changes published to the file. When operating in Worksharing mode, users work on a local copy of the Revit model and can save changes to the Central file so that other users can see their work. The local file is the same size as the Central file and can exponentially increase the storage space required for a project when multiple local files are saved on the network. Revit's Worksharing display modes and editing requests are updated in model views and can be adjusted to reduce network traffic.

To change the Worksharing Update Frequency in Revit

Figure 23)



1. Click the  logo, and then click **“Options”**
2. In the **“Options”** dialog box, click the **“General”** tab
3. In the **“Worksharing Update Frequency”** area, move the slider all the way to the left for manual updates only. When set to **“manual,”** display mode information is only updated when borrowing elements; Worksharing display does not generate network traffic.
4. Click **“OK”**

13.2 Revit Requirements Summary

Please find below a summary of the Revit Best practices and requirements to ensure that the users will achieve an optimal experience:

1. Always use the global namespace or drive letter to log on specific project before opening Revit
2. Save more often to your local copy (Ctrl+S), synchronize with central model less often (every couple of hours - speak to BIM coordinator)
3. Always communicate with your team members via email or skype messaging whenever needed, do not assume things.
4. In case of issues with files or syncing speak to your BIM Coordinator first, if not available contact BIM Support
5. If Revit file was just created, it takes longer to open such file in overseas office for the first time (depends on RVT file size, in case of 500MB file it can take 30mins)
6. Do not attempt to copy large files from server overseas during work hours. If you do so you might slow network connections between offices and you or other Revit users might not be able to synchronize Revit models.
7. Change Worksharing Update Frequency in Revit from default 5 seconds to Manual to avoid unnecessary network traffic. Ask your BIM Coordinator if you do not know how to do it or consult the full version below.

8. "Accessing Model ..." warning is result of someone else synchronizing with central model at the same time you are trying or GFC synchronizing files between offices. You need to wait for your turn. If it takes too long you need to speak to your local IT Support to check whether network between offices is not 100% busy with some other tasks (see point 7) or whether there is network outage.

13.3 Autodesk – AutoCAD Requirements

Disable Digital Signatures

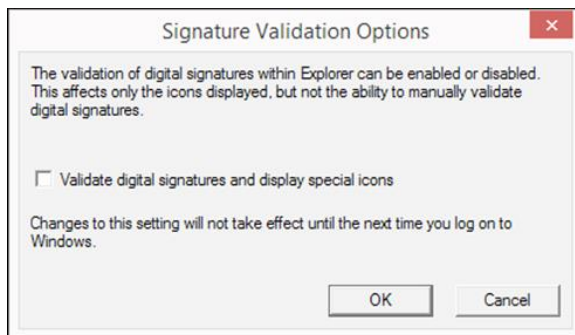
Digital signatures contribute to slow browsing of AutoCAD folders and files through GFC instances. For faster browsing, disabling digital signatures is recommended. In 2001, Autodesk introduced Digital Signature Extension, which lets AutoCAD attach digital signatures to any files compatible with the AutoCAD 2000 and later drawing-file formats. In AutoCAD 2004 and all later versions, drawings can be digitally signed directly without using the extension.

During the AutoCAD installation, a shell extension loads displaying a specific icon with the file in Windows Explorer, or in the Open/Save dialog box if it is digitally signed. To determine whether a file is digitally signed, the shell extension scans each drawing file as it is displayed. Folders that contain many drawing files cause this activity to slow the system and decrease productivity.

Disable Digital Signatures (Manual)

1. Use Windows Explorer and navigate to `C:\Windows\System32` directory.
2. Double-click the "**acsignopt.exe**" file.

The "**Signature Validation Options**" window displays.



3. De-select "**Validate digital signatures and display special icons**".
4. Click "**OK**".
5. Restart the computer.

Implementing AutoCAD Registry Setting Using AD Group Policies

1. Create a registry file called **autocad.reg** on the desktop.
2. Open the **autocad.reg** file in Notepad and add the following:
[HKEY_CURRENT_USER\Software\Autodesk\Autodesk Digital Signatures]
"IconOverlayEnabled"=dword:00000000
3. Save the **autocad.reg** file.
4. Copy the **autocad.reg** file to the logon share.
5. Create a batch file called autocad.bat.
6. Open Notepad and add the entries:
@echo off

```
regedit /s \\ServerName\Share\autocad.reg
```

Save the autocad.bat script in the NETLOGON share on a domain controller at
%systemroot%\sysvol\sysvol\<domain_DNS_name>\scripts

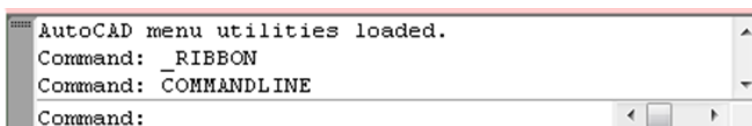
7. Start the “**Active Directory Users**” and “**Computers**” snap-in by clicking “Start > Administrative Tools > Active Directory Users and Computers”.
 8. In the console tree, right-click the local domain and select “Properties”.
 9. Click the “**Group Policy**” tab, click “New”.
 10. Type a name for the new policy (for example, AutoCAD Digital Sign), and press Enter
 11. Right-click the new policy name, select “**Properties**”.
 - a. Click the “**Security**” tab.
 - b. De-select the “**Apply Group Policy**” checkbox for the security groups that should not have this policy applied.
 - c. Select the “**Apply Group Policy**” checkbox for the groups that should have this policy applied.
 - d. Click “**OK**”.
 12. Click the “**Group Policy**” tab
 13. Select the appropriate group policy object (for example, AutoCAD Digital Sign), and click “**Edit**”.
The Group Policy Object Editor displays.
 14. Under “**User Configuration**” expand “**Windows Settings**”.
 15. Click “**Scripts (Logon/Logoff)**”.
 16. Right-click “**Logon select Properties.**” The “**Logon Properties**” window displays.
 17. Click “**Add.**” The “**Add a Script**” dialog box displays
Type the full UNC path to the shared folder that contains the script.
Example: \\ServerName\SysVol\domain.com\scripts\qq.bat.
- Note:** Do not browse to the location. Use the UNC path to the shared folder.
18. Click “**OK**”
 19. Click “**Apply**”
 20. Click “**OK**” to close
 21. Close the “**Group Policy Object Editor**” Console and the “**Active Directory Users**” and “**Computers**” snap-in. Have all users log out and log back into the domain. The end user PCs now have the following registry setting installed:

```
HKEY_CURRENT_USER\Software\Autodesk\Autodesk Digital Signatures  
"IconOverlayEnabled" =0
```

Set AutoCAD Sheet Set Manager Variables

Access and Edit Variables

1. Open the AutoCAD command window.
2. Type the name of the variable followed by the value to set it to.
3. Exit AutoCAD normally to save the new variable value.



Toggle Data Sheet Refresh State

The SSMSHEETSTATUS variable controls how the status data in a sheet set is refreshed.

Set the SSMSHEETSTATUS variable to 0. The status data in a data sheet does not automatically refresh.

OR

Set the SSMSHEETSTATUS variable to 2. The status data will be refreshed when the sheet set is loaded or updated.

This setting also indicates that the status data will be refreshed based on the time interval set by SSPOLLTIME.

Set Data Sheet Refresh Rate Intervals

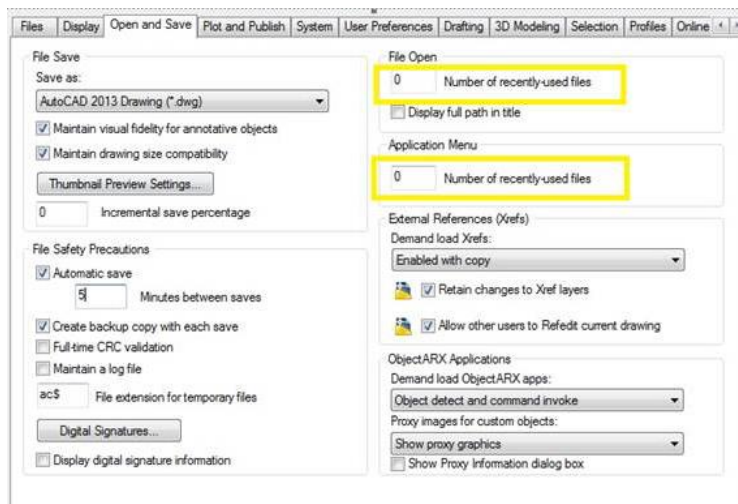
This variable controls the time interval between automatic refreshes of the data sheet status data. The time interval is in seconds and valid values are between 20 and 600. The default value is 60. Set SSPOLLTIME to 600.

Set XLOADCTL Variable Parameter to 2

This variable controls how xref files are loaded: pre-loaded or on-demand, and if they are locked for exclusive use or a locally sourced copy. Autodesk recommends setting the XLOADCTL variable to 2 to allow for on-demand loading of network resources. If set to 2, copies of xref drawings are loaded and locked, the authoritative xrefs are not locked exclusively.

Turn off File History for recently-used files

To turn File History off, change the Number of recently-used files to 0 for both *File Open* and *Application Menu* items in the “Open and Save” preferences (screenshot below)



Excluding Drawing Files from Antivirus Scanning

Recommendation: Keep AutoCAD drawing (DWG) files excluded from antivirus scans to accelerate the file open and file save processes.

13.4 Bentley – MicroStation Requirements

User Preference File (UPF) and Project Configuration file (PCF)

Bentley MicroStation often reads and writes the .UPF and .PCF files in order to update its profile settings. For each user session, the application will write the entire file to the destination location, in this case the GFC server that saves the file to the datacenter. In order to improve application performance, it is recommended to place the .UPF and .PCF files locally on the client, which is MicroStation's default location or on a local share:

```
_USTN_PREFNAMEBASE =  
C:\ProgramData\Bentley\MicroStation\Workspace\users\Talon\prefs\EYC
```

Disable Auto-Save or Set to Value of 600

Due to the way Bentley MicroStation responds to WAN interruptions, the MicroStation auto-save feature should be disabled and clients should save MicroStation files manually or set this value to 600.

In the event of a network or WAN interruption, MicroStation times out and displays a window that offers the options of retrying or cancelling the save operation. MicroStation does not offer a "Save As" option for files open on client PCs from the data center file server. The retry option causes MicroStation to retry the save operation for 300 seconds or until the network/WAN connection is reestablished, causing the application to appear as if it has frozen.

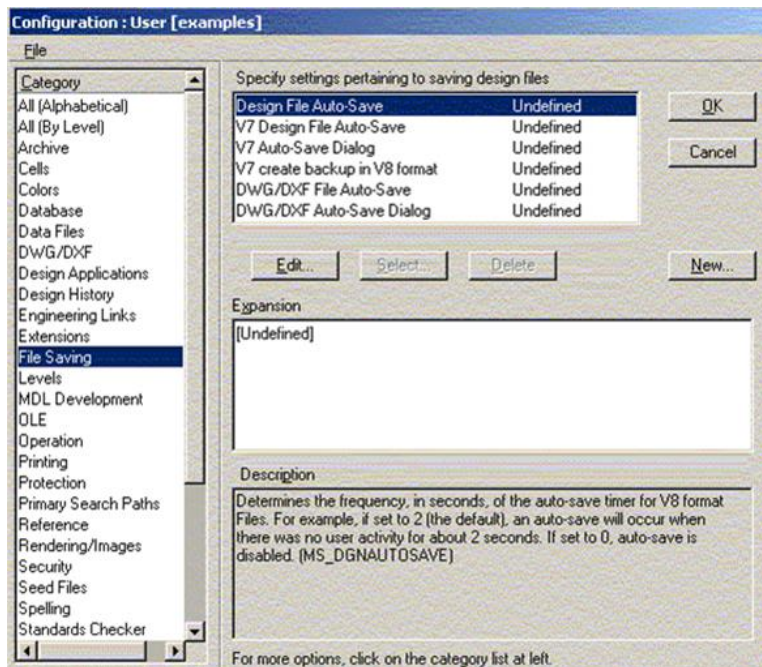
If a packet arrives during the retry operation, it causes the timer to reset and the operation starts from the beginning. The cancel option causes MicroStation to write the changes to a temporary file and then close. Once the original. dgn file is reopened, the changes are applied to it from the temporary file.

Starting with MicroStation V8 2004 Edition, auto-save can be set up either using configuration files or user preferences. The configuration file technique has the advantage that it can be set up by an administrator for an entire site or workgroup, and it allows more control over how auto-save works. For sites where the auto-save policy is left up to the user, the user preference method can be used. If the auto-save configuration variables are set, they take precedence over the user preference settings.

Adjusting AutoSave settings in Microstation

Under the Workspace Configuration settings, select "**File Saving**." Here users can set auto-save parameters (or review the settings that an administrator has made in site configuration files).

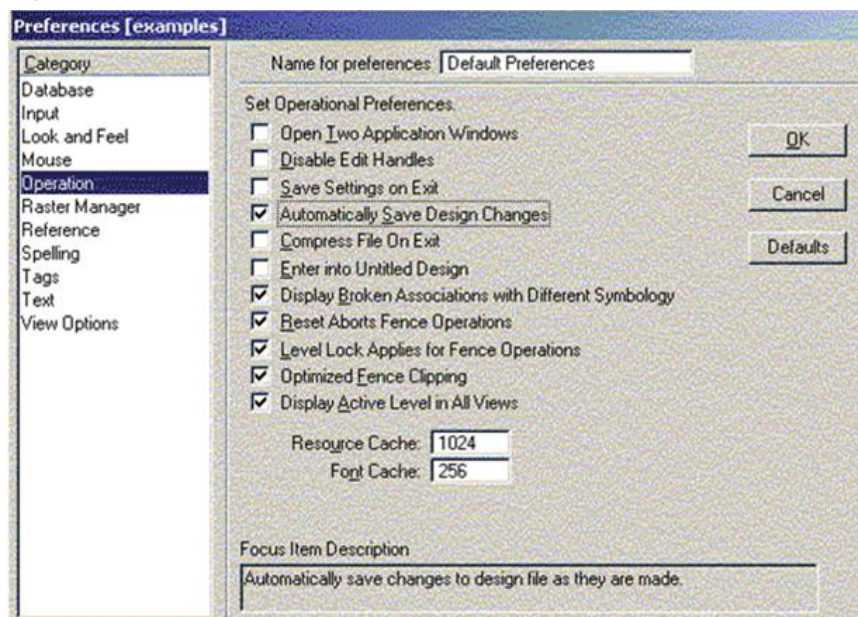
Figure 24)



Setting “**MS_DGNAUTOSAVE**” to 0 will turn off auto-save and prompt the user to save changes when exiting a file. Any other value allows users to set the number of seconds between auto-saves when editing V8 design files. The other configuration variables determine how auto-save works when editing v7 and DWG format files.

If none of the configuration variables have been set, the auto-save user preference determines the behavior. To review or change these settings, go to the “**Workspace > Preference**” pull-down menu and then go to the "Operation" category.

Figure 25)



Check the **“Automatically Save Design Changes”** box (which replaces the Immediately Save Design Changes toggle from previous versions). It is on by default. If any of the File Saving configuration variables are set, the preference is grayed out. Hovering over the preference will indicate that automatic saves are turned on by the **MS_DGNAUTOSAVE** configuration variable or **“Automatic save is turned off because MS_DGNAUTOSAVE is set to 0.”**

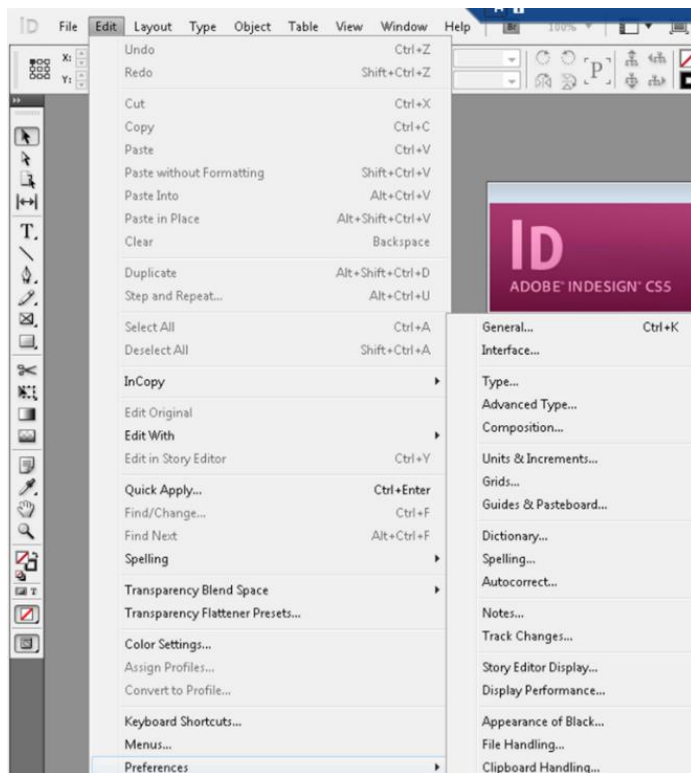
13.5 Adobe Creative Suite Requirements

InDesign

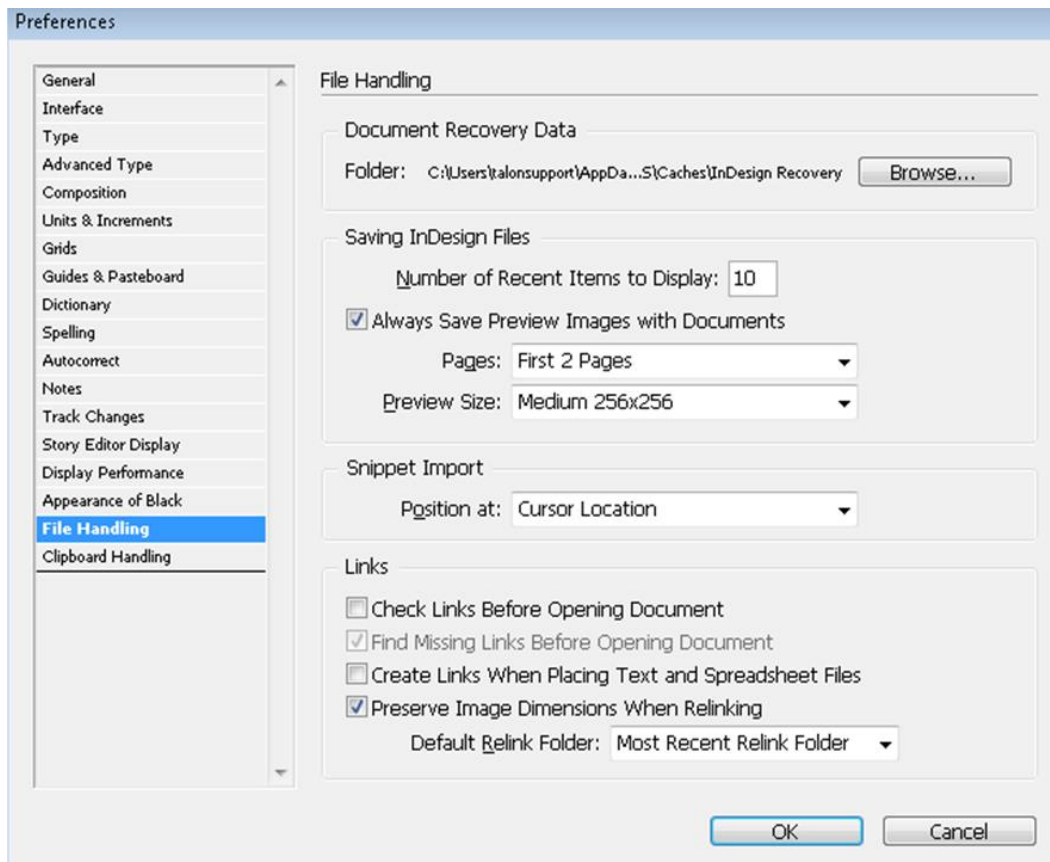
To prevent InDesign from checking for links between images within a document and with external documents, it's recommended to disable checking for links when opening a file. If this is left on, it may result in multiple file read or open operations which may impact performance.

To adjust the link check setting on the client workstation:

1. Click **“File”**.
2. Expand the **“Preferences”** menu.
3. Click **“File Handling”**.



4. Uncheck the box to **“Check links before opening document”**



The Link Check settings can also be adjusted via a script/GPO:

1. Create a new directory named **“Startup Scripts”** at
`C:\Users\<username>\AppData\Roaming\Adobe\InDesign\Version11.0\en_US\Scripts.`
 2. Create a new JavaScript file within the **“Startup Scripts”** directory with the following contents
`app.linkingPreferences.checkLinksAtOpen = false;`
 3. If InDesign is running, close and reopen the application to force the changes to take effect.
- Note:** This is an optional setting that, depending on the user's workflow, may or may not be feasible.

14 End User Training

Please find below an example introduction email for end users, including training materials, do's and don'ts and overall best practices that apply when working on a centralized data set / collaborative environment. You can leverage this template and tailor to fit your organization's needs.

[CUSTOMER] recently invested in an enterprise IT solution that enables the organization to centralize all project data, local file servers with the objective to simplify data management and deliver real-time collaboration for all users in all offices.

GFC software helps [CUSTOMER] users to centralize their organization's data and simplify infrastructure management while delivering Global File Sharing with File Locking to the branch office workforce.

In summary, GFC creates a central 'Single Set of Data' in [CUSTOMER]'s data center while its branch office GFC Intelligent File Caching mechanism transparently presents central file shares, documents and project files to the end user community in these branch offices. Additionally, GFC eliminates complexity, expensive storage and infrastructure at the branch while fully eliminating branch office backups.

In order to onboard the end user community, we have released a training video at <https://youtu.be/RYvhnTz4bEA> and for Architectural, Engineering and Construction customers at https://youtu.be/avMMA_IzY0.

Accessing Project Folders and Files

[CUSTOMER] has created a unified namespace for the organization that is accessible to everyone by navigating to `\\corporate.local\public\`.

This network location can be accessed through a drive mapping i.e. `I:\` or by navigating to the unified namespace using the network (UNC) path.

Cold Files Versus Warm Files

GFC only caches what's actively being used at the branch office locations, which means that some of the files within the central file set are cached and others are not.

Cold file: the first time you open a file (marked with a grey X) the transfer of the file will take place over the Wide Area Network, which may take some time to complete

Warm file: the second time you open the same file, the software will check if the cache maintains the latest version of the file, fetch any incremental updates from the central file server, and immediately serve the file to the end user

IMPORTANT: if you require access to a large-scale central project (i.e. > 500MB) that is not cached yet, it is recommended to schedule a pre-population job (overnight). You can request pre-population for a specific project folder by sending an email to support team at ...@...

Do's and Don'ts

In a 'GFC' world there are specific do's and don'ts to adhere to in order to get the most out the solution and ensure everyone in the organization an optimal end user experience.

Do: Work directly of the FASTData File Share

This file share will be presented to you by IT as a drive mapping (For example, `I:\`) or as a unified namespace using i.e. `\\corporate.local\public\`.

You will recognize the file share by the "X" mark on some of the files (cold / uncached).

Don't: Copy data back and forth to your local computer / server

Every file (when copied back) will be treated as a new file and therefore may impact bandwidth usage as minimum file differencing will take place at that moment.

May cause inconsistencies in files, data loss as you might overwrite other user's files.
Impacts the business and your own productivity.

Application-Specific Best Practices

There are specific applications that require additional attention from an end user perspective. Although [CUSTOMER] IT infrastructure teams have taken all measurements to automate the client-application best practices, some applications require additional settings to be configured or change in workflow.

Please consult the client application best practices documentation and training materials provided by your IT team.

For more information on GFC, please consult the following resources:

<https://cloud.netapp.com/global-file-cache>

15 Contact Details

Customer support for NetApp Global File Cache users with Cloud Volumes ONTAP, Cloud Volumes Services and Azure NetApp Files is available through these channels:

Product documentation, Case Management, Phone, Knowledgebase, Downloads, Tools, and more:
<https://cloud.netapp.com/gfc-support>

If you are an existing Talon Storage customer, please also use the link provided above for your support needs.

Appendix A: Antivirus Application Suites

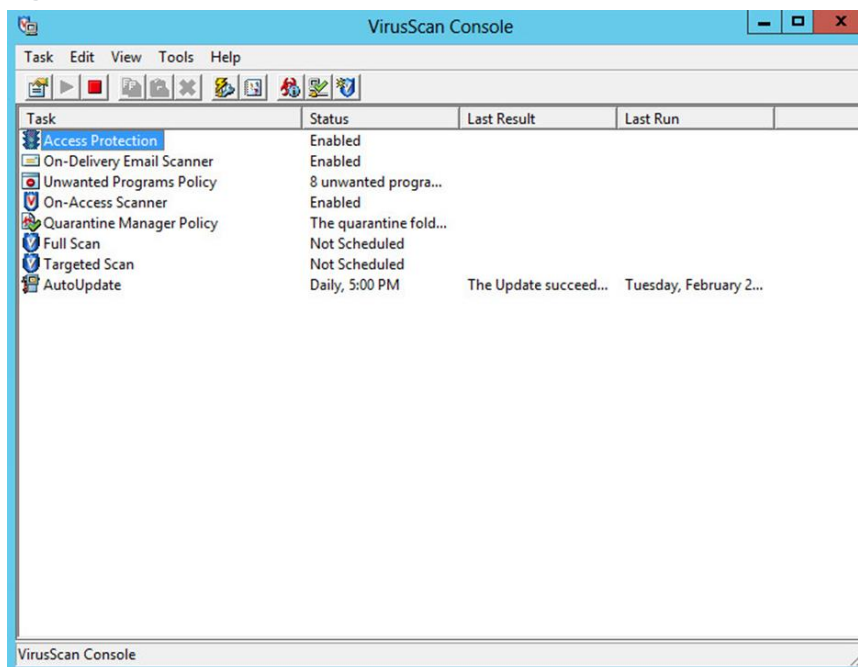
Note: Below are best practices for various Antivirus applications. In general, most AV apps have various modules such as AV module, deep scan module, app behavior module, anti-phishing module etc., Of all these, only 'AV module' should be active in GFC specific OU (Organization Unit). Other modules need not be included in GFC OU container.

McAfee VirusScan

Baseline Protection

After completing a Standard installation of the McAfee Virus Scan Enterprise and choosing to not perform the initial On-demand scan, follow the configuration specifics as outlined below, including On-Access Scanning, Full and Targeted Scan.

Figure 26)

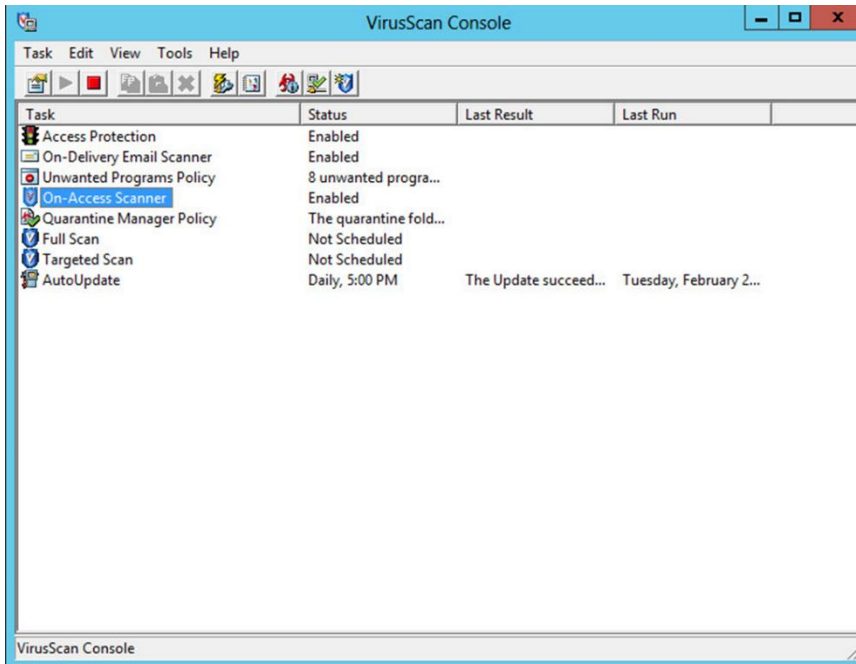


Excluding Services and Processes in McAfee VirusScan Console

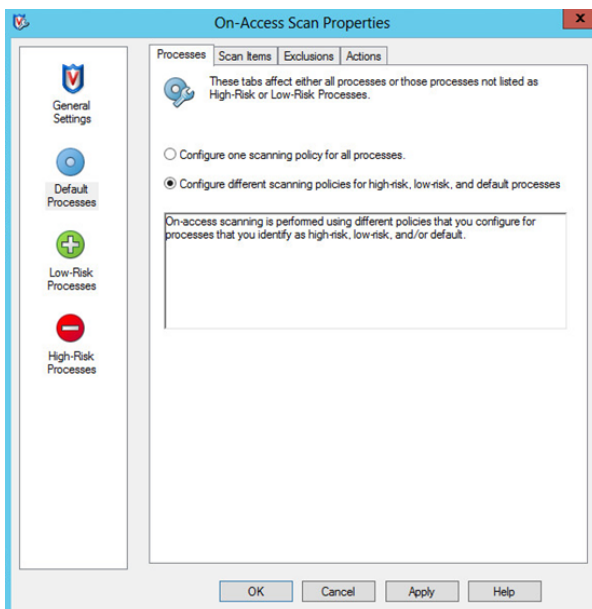
This section details how to exclude NetApp Global File Cache (GFC) processes on Core/Edge Servers and other remote appliances based on McAfee VirusScan scanning.

Note: Ensure that GFC processes, services, and drives are excluded on antivirus servers and clients and as a group policy for GFC users, if applicable.

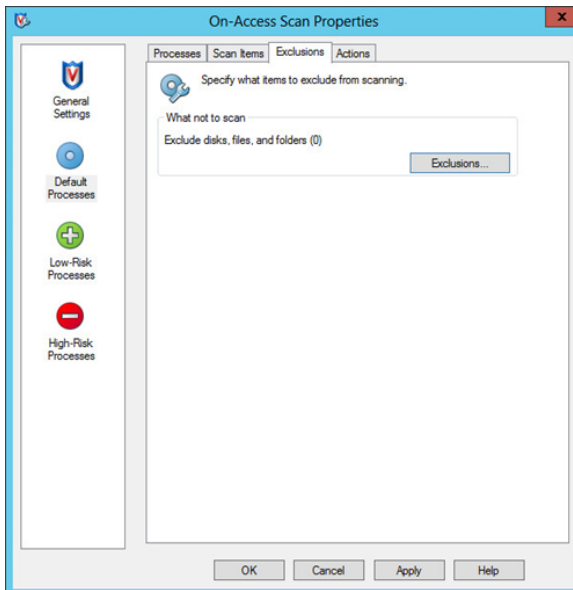
1. Double click the “**On-Access Scanner**” task in the main VirusScan Console window.



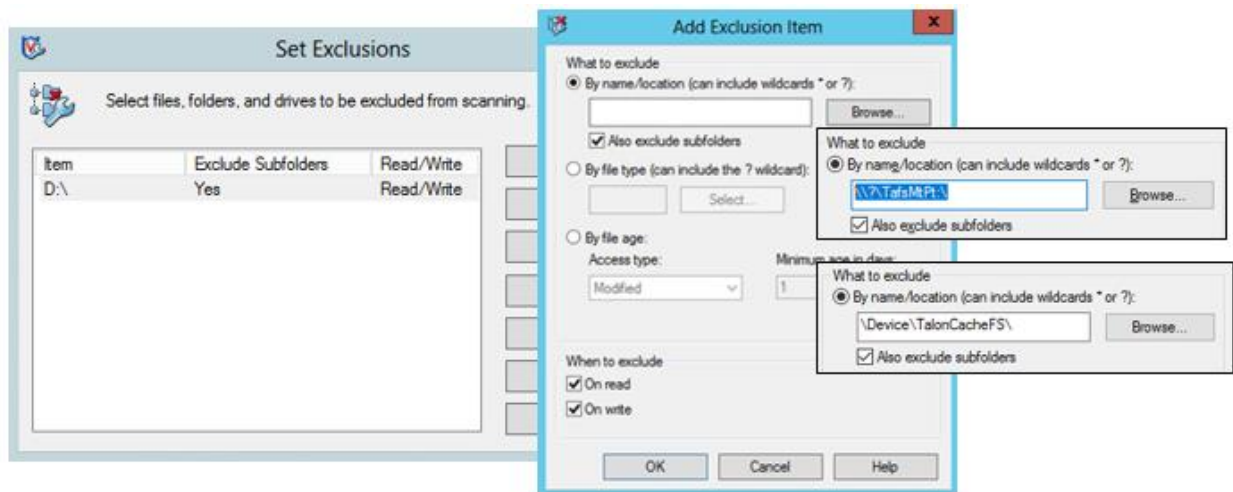
- Click **“Default Processes”** in the left pane and then select the radio button labeled **“Configure different scanning policies for high-risk, low-risk, and default processes”**



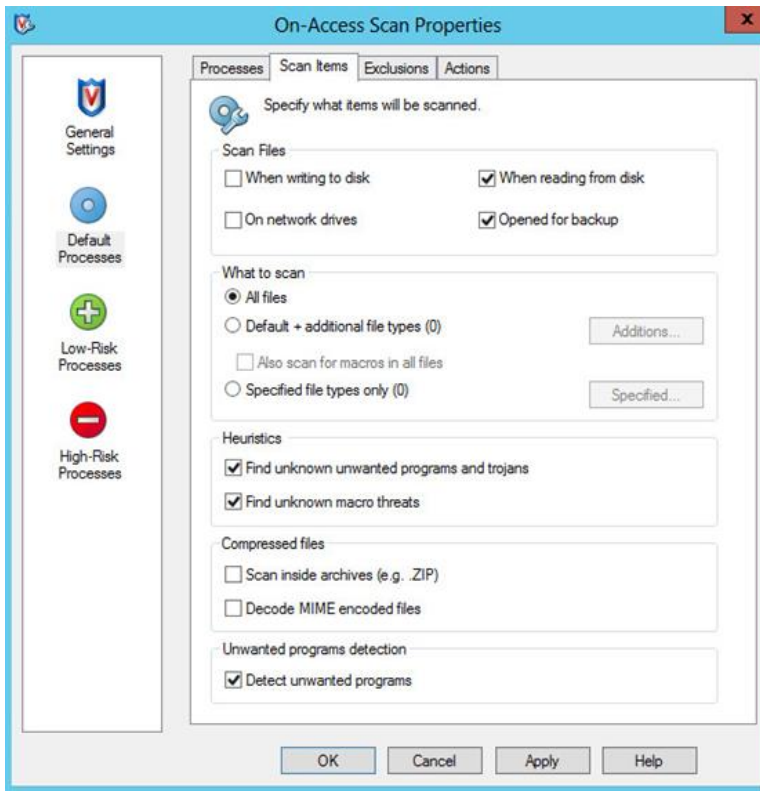
- Click the **“Exclusions”** tab and then click the **“Exclusions...”** button to configure them



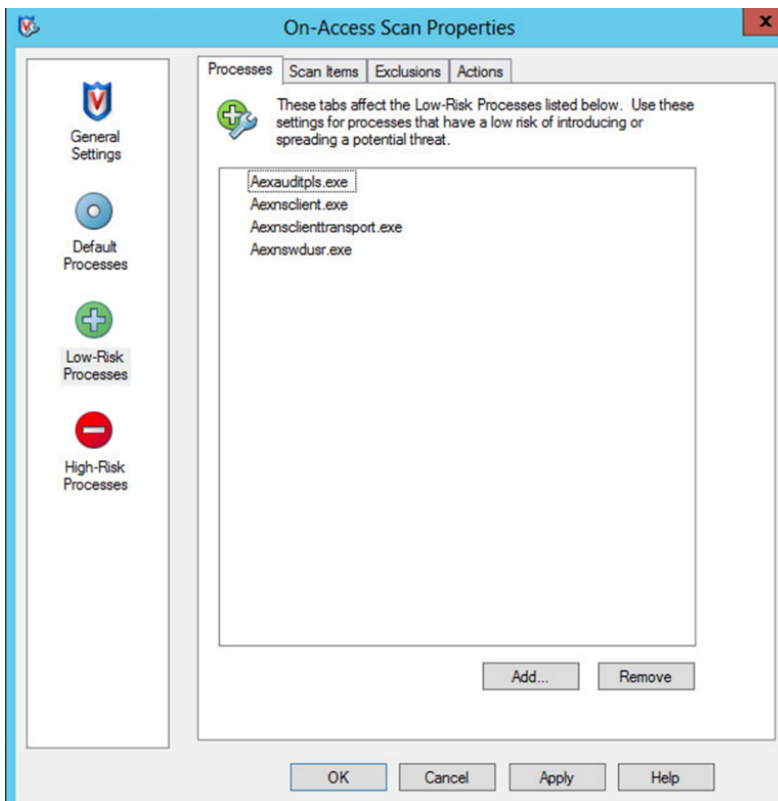
4. Add the D:\ drive to the Exclusions list. Additionally, add \\?\TafsMtPt:\ or \\?\TafsMtPt* and \Device\TalonCacheFS\ to the Exclusions list. Ensure that subfolders are also excluded from scans. Click **“OK”** when finished



5. Click the **“Scan Items”** tab and de-select **“When writing to disk”**

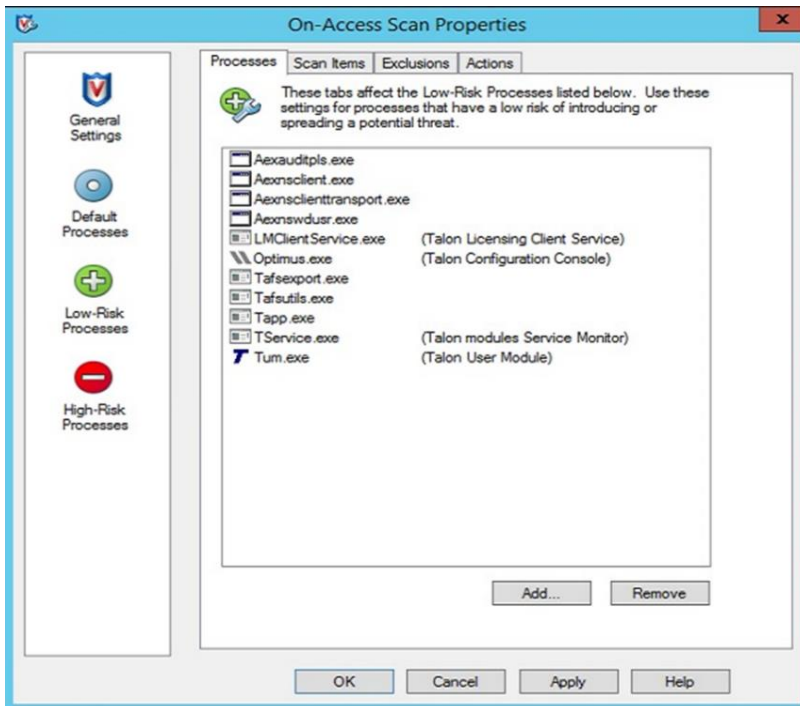


6. Click **“Low-Risk Processes”** in the left pane
7. Click the **“Add...”** button on the **“Processes”** tab

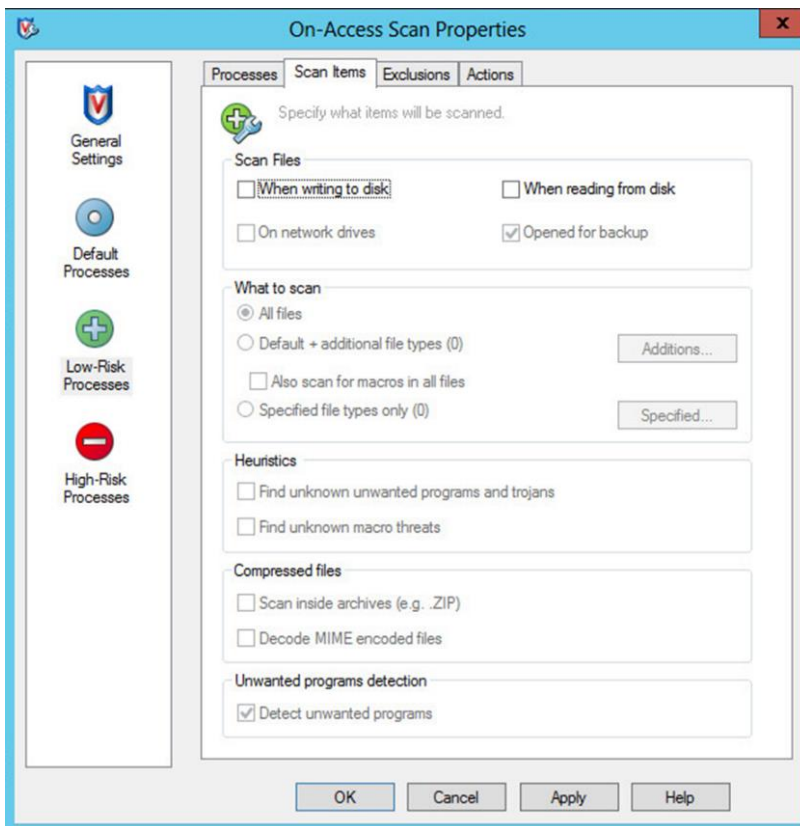


8. Once the list of available processes finishes populating, you may need to click the **“Browse...”** button and manually add the following processes:

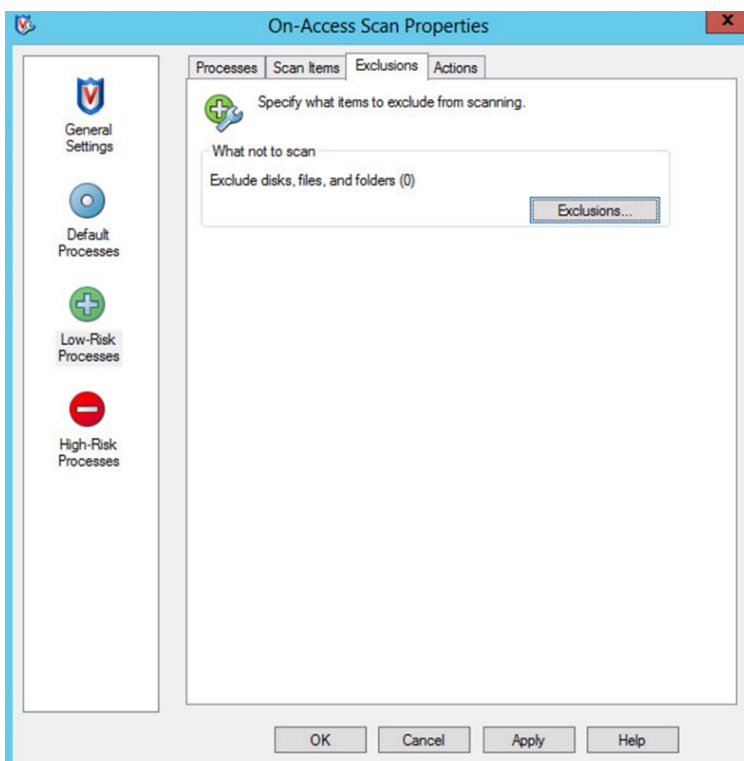
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
C:\Program Files\TalonFAST\Bin\Optimus.exe
C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe
C:\Program Files\TalonFAST\Bin\tafsexport.exe
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\TappN.exe
C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe
C:\Windows\System32\drivers\tfast.sys
C:\Program Files\TalonFAST\FastDebugLogs\



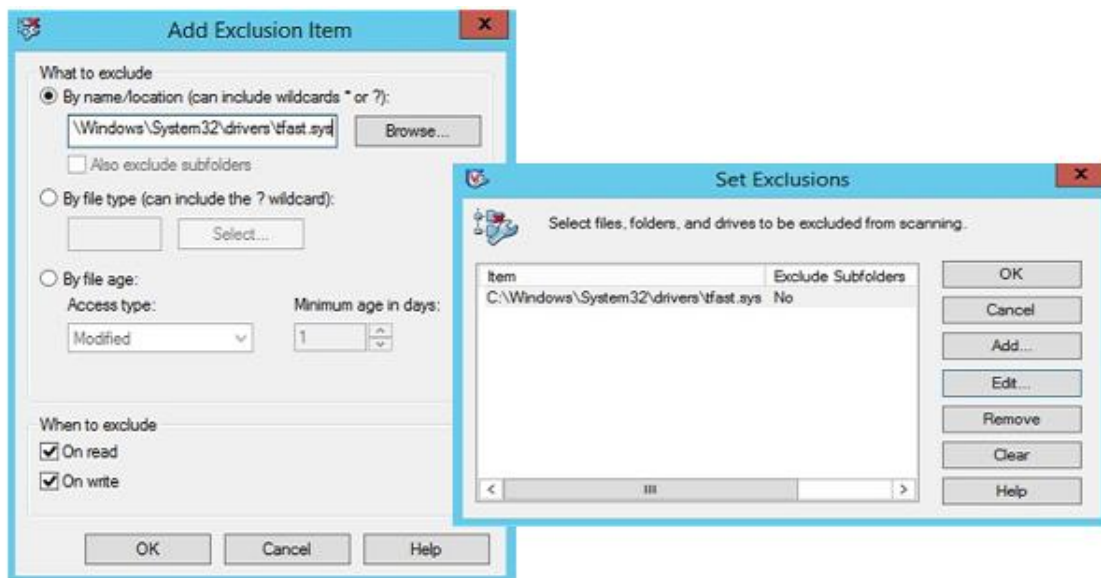
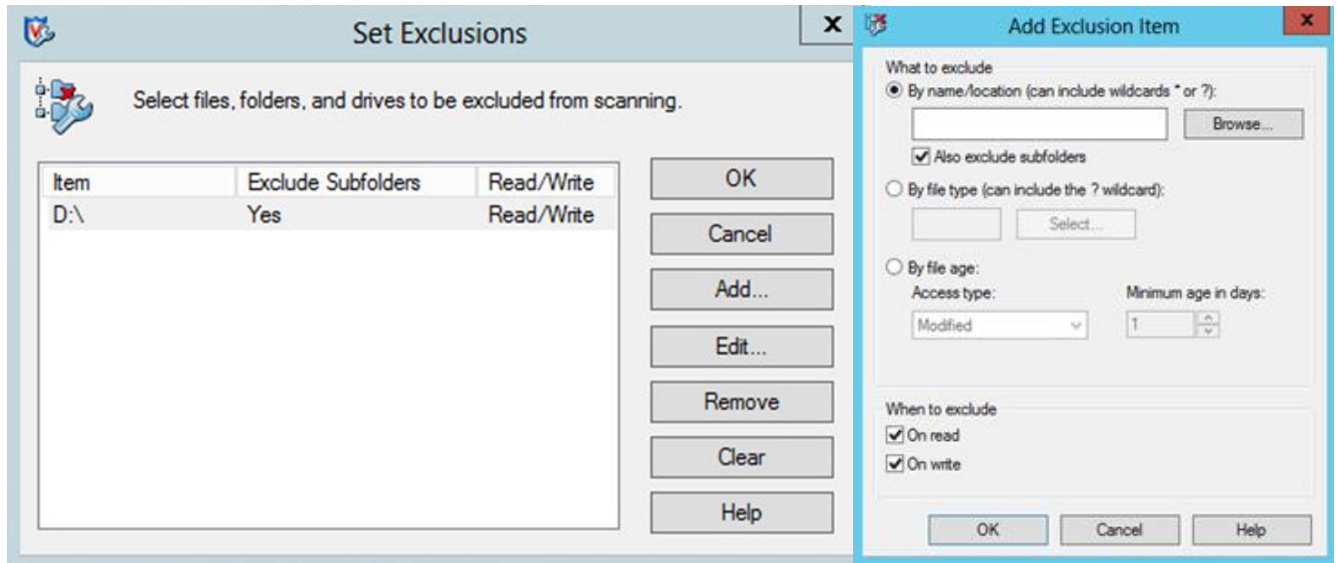
9. Click **“OK”** to apply the changes
10. Click the **“Scan Items”** tab and de-select **“When writing to disk”** and **“When reading from disk”**



11. Click the **“Exclusions”** tab at the top
12. Click the **“Exclusions...”** button



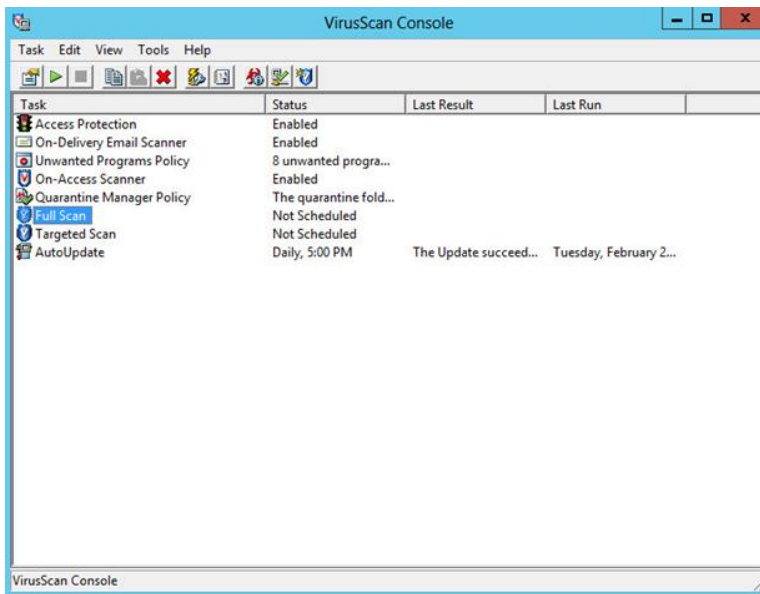
13. Add the D:\ drive to the Exclusions list. Additionally, add \\?\TafsMtPt:\ and \Device\TalonCacheFS\ to the Exclusions list. Ensure that subfolders are also excluded from scans. Click “OK” when finished
14. Add C:\Windows\System32\drivers\tfast.sys
Note: You may have to manually type in this path to add tfast.sys
15. Click “OK” when finished.



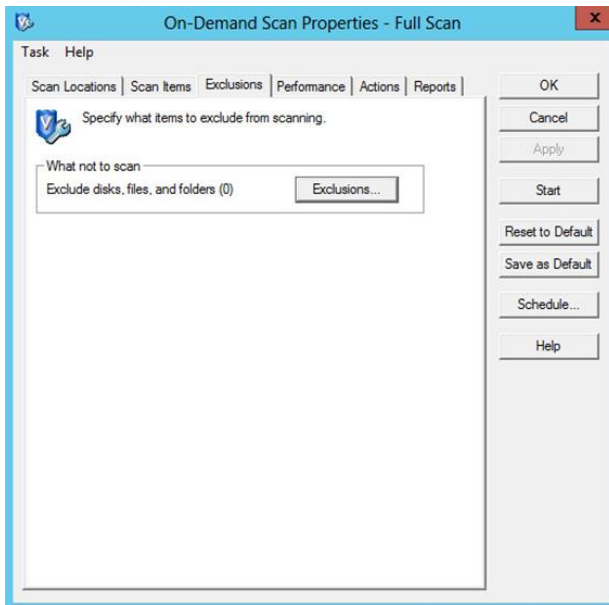
Full or Targeted Scans

If running a full or targeted scan on a GFC server, please follow the steps below

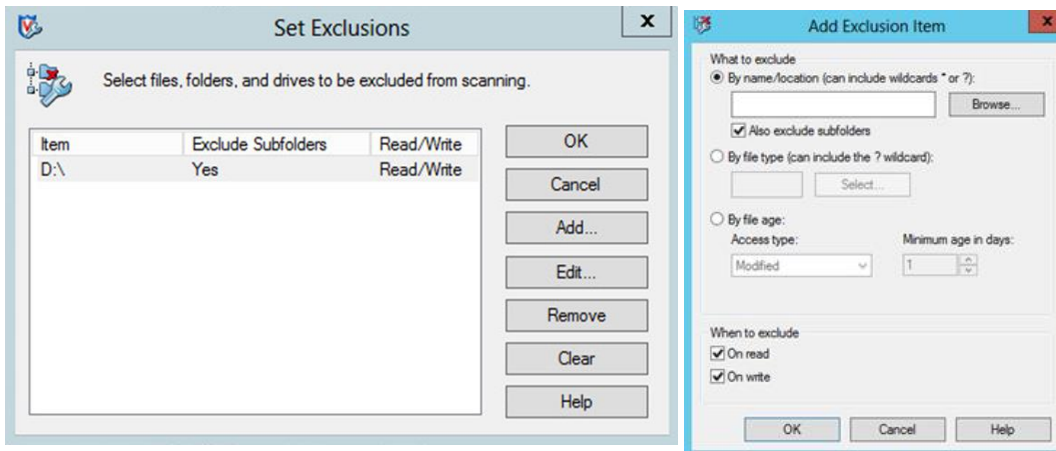
1. Double click either “**Full Scan**” or “**Targeted Scan**” from the VirusScan Console



- Click the **"Exclusions"** tab from the On-Demand Scan Properties window. Click the **"Exclusions..."** button.



- Add the D:\ drive to the Exclusions list. Additionally, add \\?\TafsMtPt:\ and \Device\TalonCacheFS\ to the Exclusions list. Ensure that subfolders are also excluded from scans. Click **"OK"** when finished

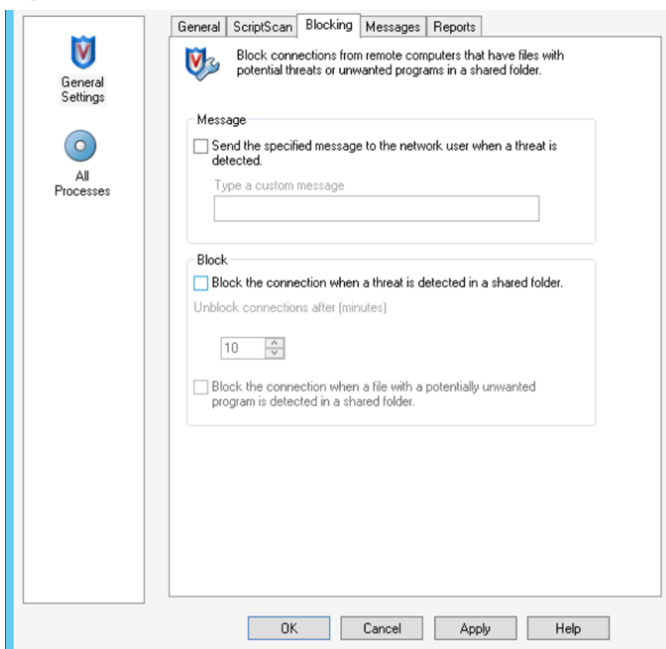


Prevent Connection Blocking in Shared Folders

With the exclusions of the D:\ drive, it is recommended that connections not be blocked from shared folders. This will provide consistent file access from the GFC Virtual File Share.

To disable the connection blocking, uncheck the box as shown below:

Figure 27)



McAfee VirusScan - Central Management Console

Go to the McAfee centralized management console and create a new Threat Prevention policy for the GFC servers and associate the GFC Core and Edge servers with the policy.

1. Open the GFC Policy and click on **“Show Advanced settings”**
2. Ensure the settings have been configured as below

Endpoint Security Threat Prevention : Policy Category > On-Access Scan > Default - Talon

Hide Advanced

On-Access Scan	<input checked="" type="checkbox"/> Enable On-Access Scan <input checked="" type="checkbox"/> Enable On-Access Scan on system startup <input checked="" type="checkbox"/> Allow users to disable On-Access Scan from the McAfee system tray icon <input checked="" type="checkbox"/> Specify maximum number of seconds for each file scan: <input type="text" value="45"/> <input checked="" type="checkbox"/> Scan boot sectors <input type="checkbox"/> Scan processes on service startup and content update <input type="checkbox"/> Scan trusted installers <input type="checkbox"/> Scan when copying between local folders <input checked="" type="checkbox"/> Scan when copying from network folders and removable drives <input type="checkbox"/> Detect suspicious email attachments <input type="checkbox"/> Disable read/write scan of Shadow Copy volumes for SYSTEM process (improves performance)
McAfee GTI	<input checked="" type="checkbox"/> Enable McAfee GTI Sensitivity level: <input type="text" value="Medium"/>
Antimalware Scan Interface	<input checked="" type="checkbox"/> Enable AMSI (provides enhanced script scanning) <input checked="" type="checkbox"/> Enable Observe mode (Events are generated but actions are not enforced)
Threat Detection User Messaging	<input checked="" type="checkbox"/> Display the On-Access Scan window to users when a threat is detected Message: <input type="text" value="McAfee Endpoint Security detected a threat."/>

3. The process settings need to be configured for High Risk and Low Risk
 - a. Ensure the tservice.exe and tum.exe are configured as “**Low Risk**”

Process Settings

☐ Use Standard settings for all processes
☒ Configure different settings for High Risk and Low Risk processes
 Standard settings will apply to all unlisted processes.

Process	Process Type
ypager.exe	High Risk
yupdate.exe	High Risk
Aexauditpls.exe	Low Risk
Aexnsclient.exe	Low Risk
Aexnsclienttransport.exe	Low Risk
Aexnsdusr.exe	Low Risk
tservice.exe	Low Risk
tum.exe	Low Risk

Process Types:

Scanning

When to scan:

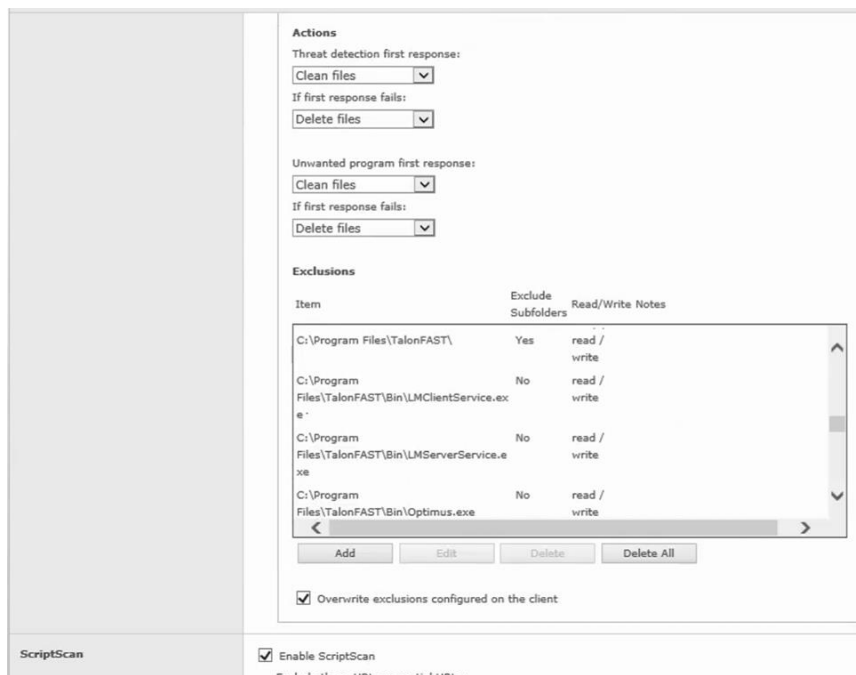
☐ When writing to disk
☐ When reading from disk
☒ Let McAfee decide

What to scan:

☒ All files
☐ Default and specified file types

4. The exclusion includes the following exclusions:
D:\

D:\LocalFASTData\
 C:\Program Files\TalonFAST\FastDebugLogs\
 C:\Program Files\TalonFAST\Bin\LMClientService.exe
 C:\Program Files\TalonFAST\Bin\LMServerService.exe
 C:\Program Files\TalonFAST\Bin\Optimus.exe
 C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe
 C:\Program Files\TalonFAST\Bin\tafsexport.exe
 C:\Program Files\TalonFAST\Bin\tafsutils.exe
 C:\Program Files\TalonFAST\Bin\tapp.exe
 C:\Program Files\TalonFAST\Bin\TappN.exe
 C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe
 C:\Program Files\TalonFAST\Bin\TService.exe
 C:\Program Files\TalonFAST\Bin\tum.exe
 C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe
 C:\Windows\System32\drivers\tfast.sys
 \Device\TalonCacheFS\
 \\?\TafsMtPt:\ or \\?\TafsMtPt* (Depends on the current version)
 *TAFS
 Policydb.xml



5. Under the low risk configuration for Process Type ensure scanning is set to the following
 - a. “Do not scan when reading from or writing to disk”.

Process Types:

Standard High Risk Low Risk

Scanning

When to scan:

☐ When writing to disk

☐ When reading from disk

☐ Let McAfee decide

☒ Do not scan when reading from or writing to disk

What to scan:

☒ All files

☐ Default and specified file types

☐ Specified file types only

☐ On network drives

☐ Opened for backups

☐ Compressed archive files

☐ Compressed MIME-encoded files

Additional scan options:

☒ Detect unwanted programs

☐ Detect unknown program threats

☐ Detect unknown macro threats

Actions

Threat detection first response:

Clean files

If first response fails:

Symantec Endpoint Protection 12.x

This section outlines best practices for Symantec Endpoint Protection version 12.x targeted for GFC appliances based on Windows Server.

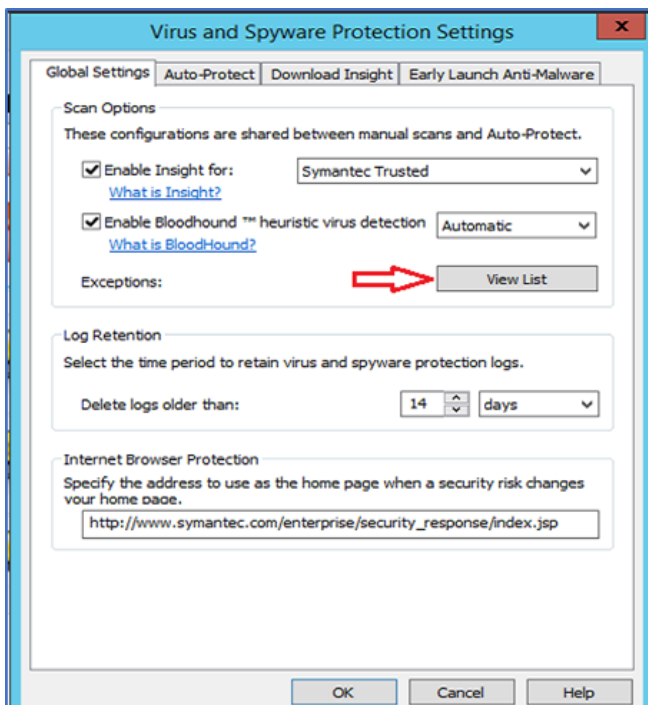
1. Double click the Symantec icon on the task bar



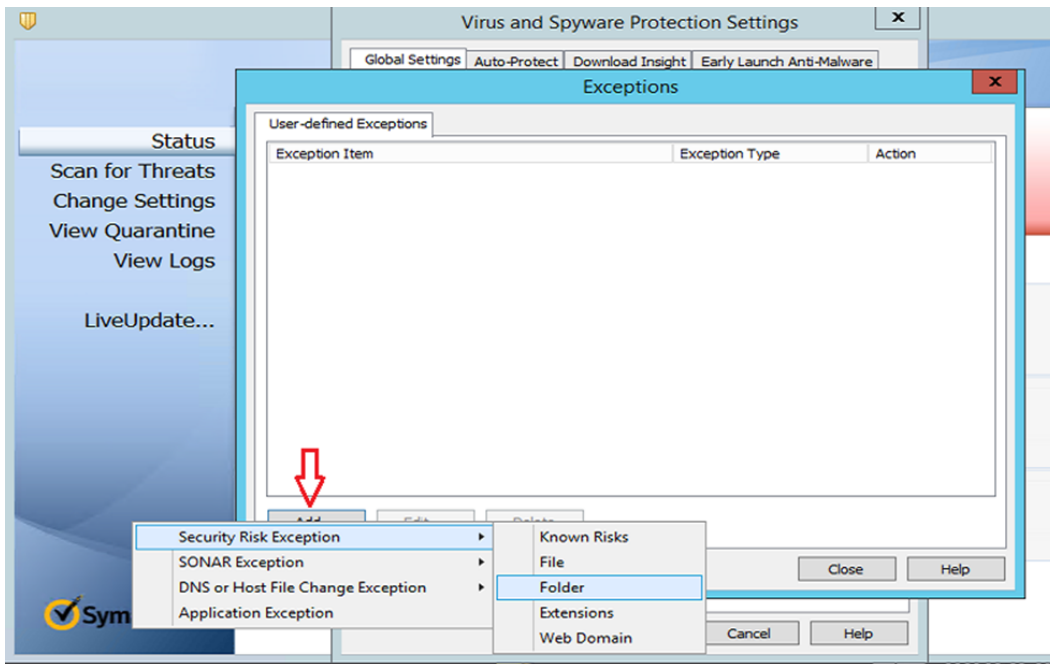
2. “Virus and Spyware Protection” -> Click “Options” -> “Change Settings”



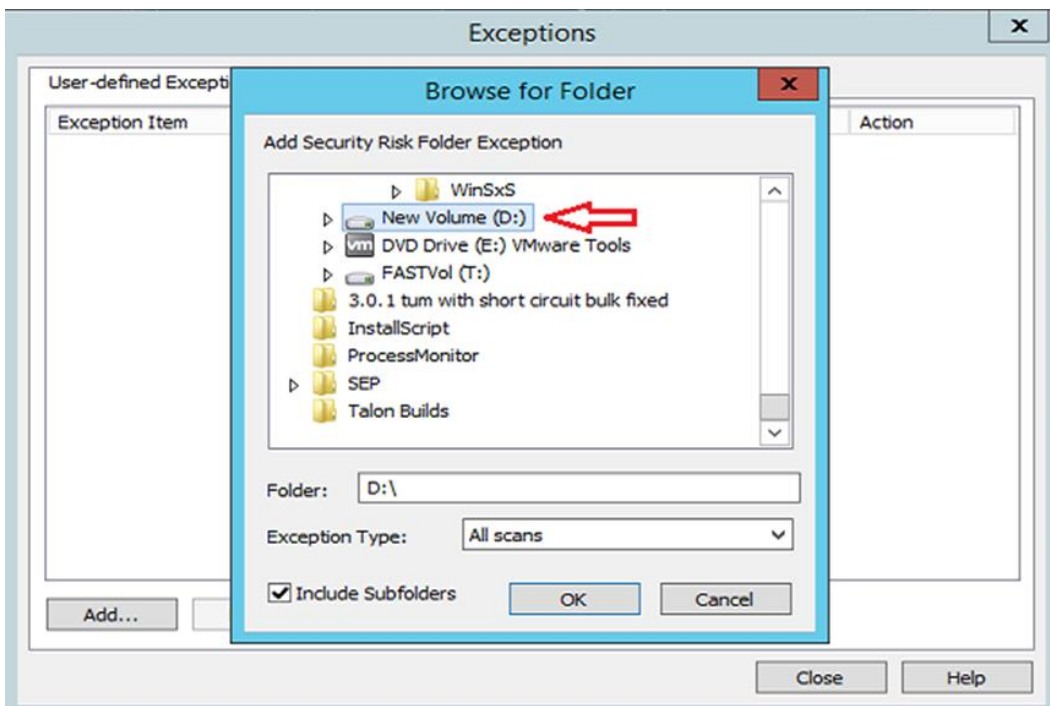
3. Click “View List”



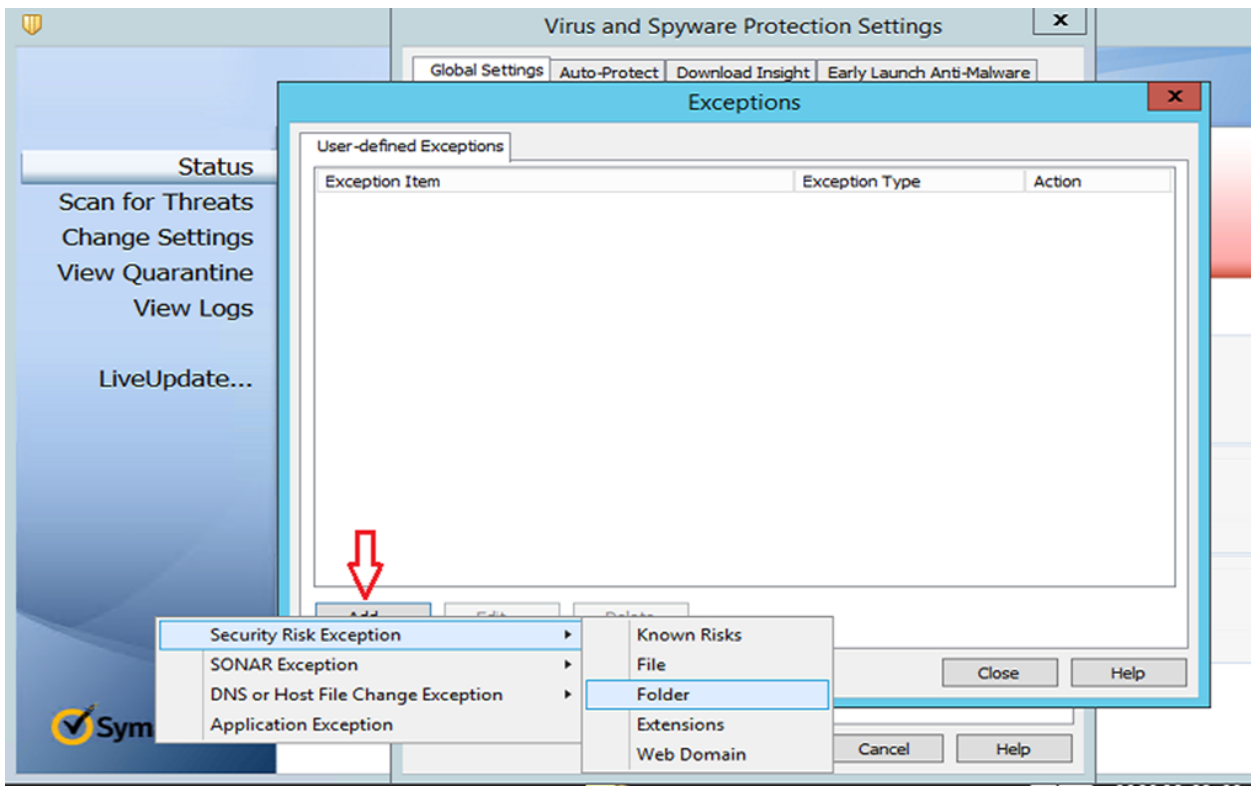
4. Click “Add” -> “Security Rick Exception” -> “Folder”



5. Scroll down, click on D:\, and click “OK”



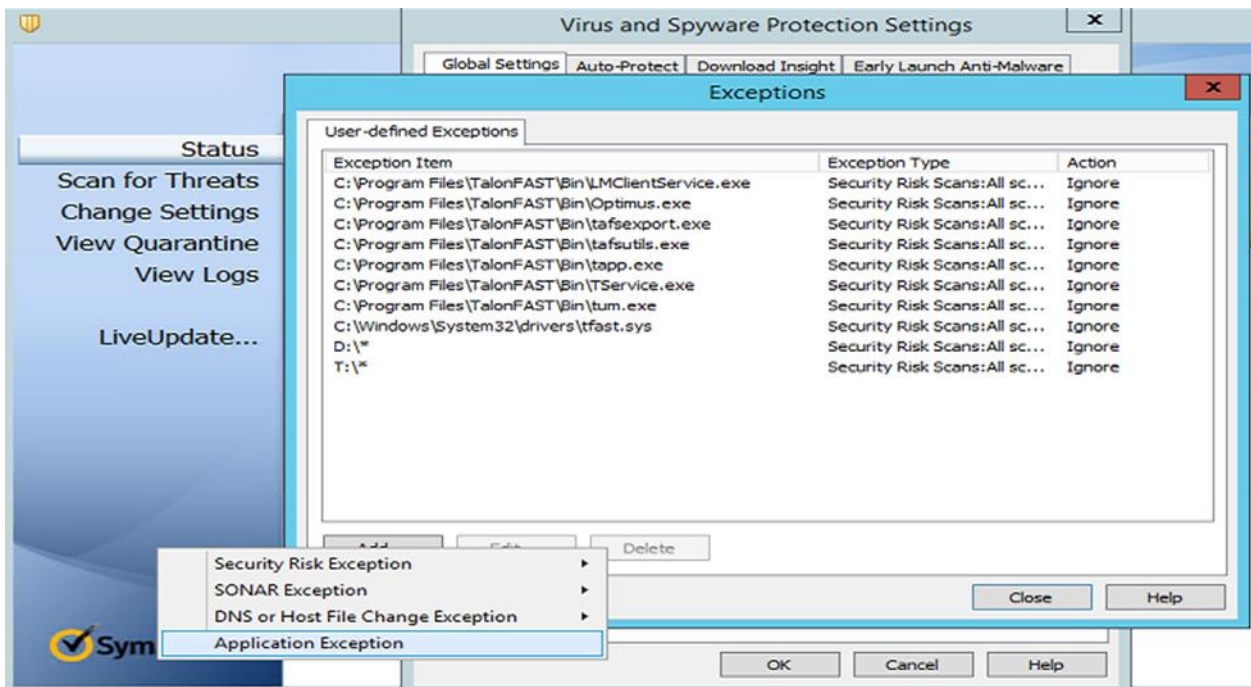
6. Click “Add” -> “Security Risk Exception” -> “Folder”



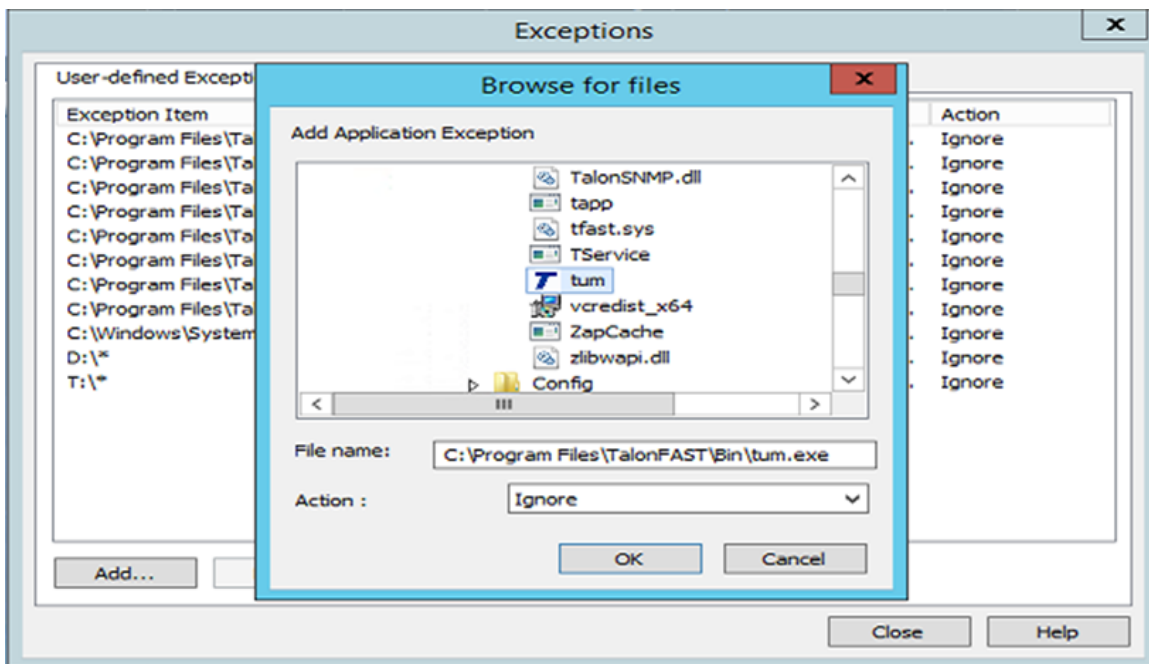
7. Add the following:

```
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
C:\Program Files\TalonFAST\Bin\Optimus.exe
C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe
C:\Program Files\TalonFAST\Bin\tafsexport.exe
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\TappN.exe
C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe
C:\Windows\System32\drivers\tfast.sys
C:\Program Files\TalonFAST\FastDebugLogs
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS\
```

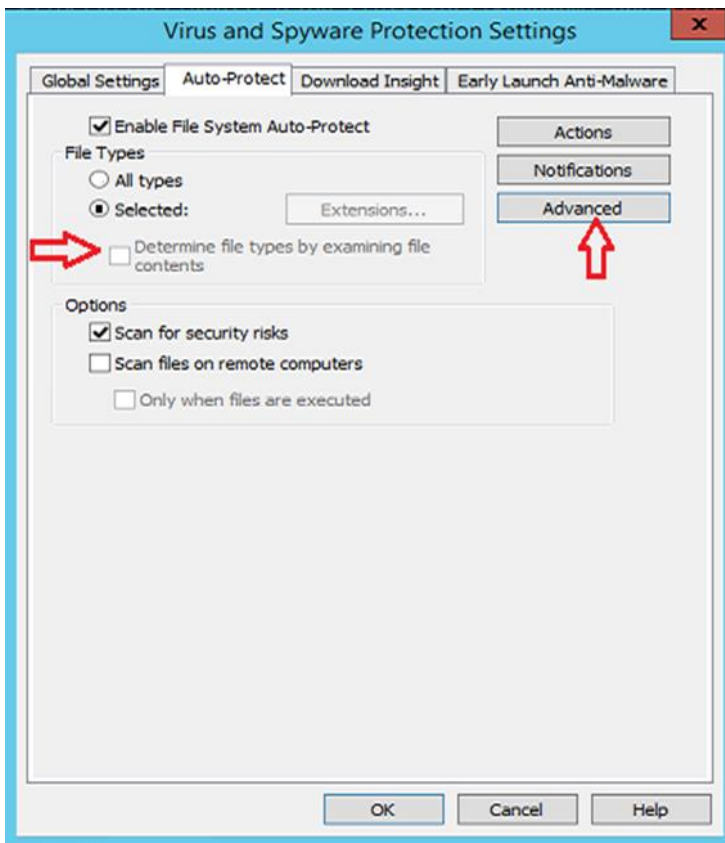
8. Click "Add" -> "Application Exception"



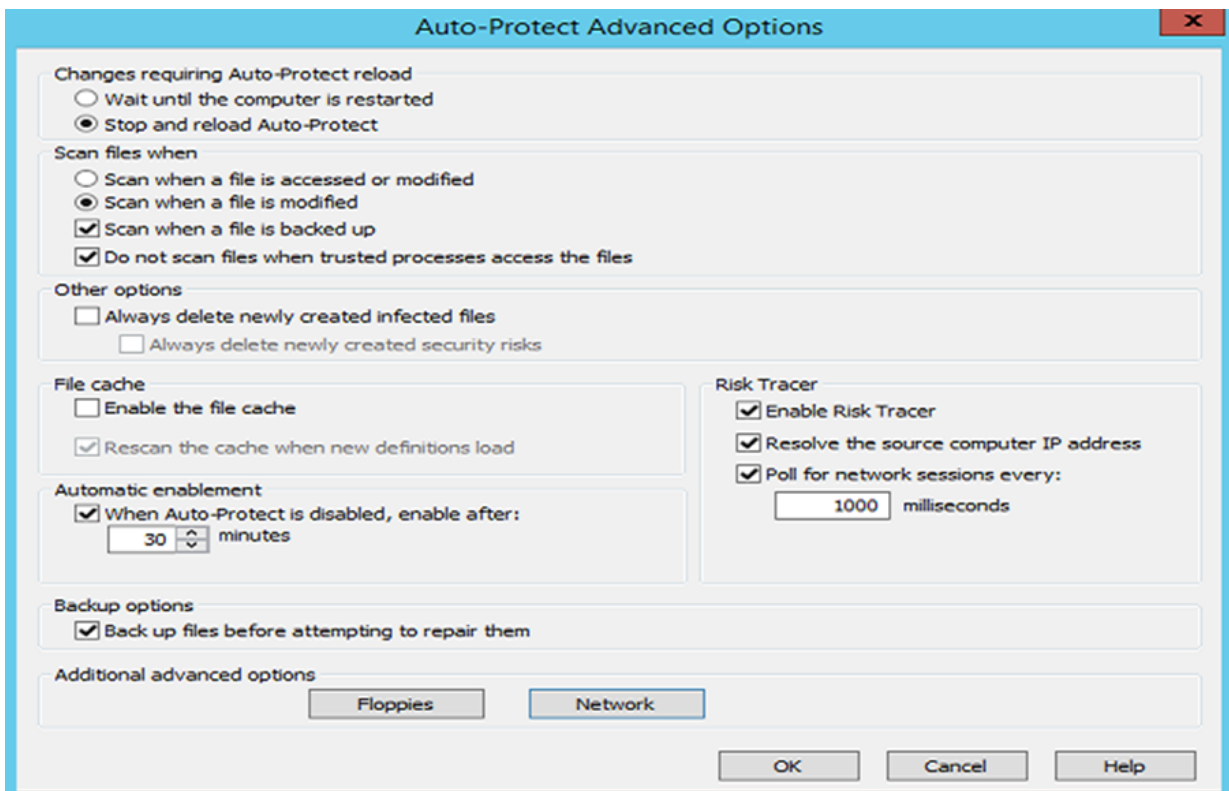
9. Browse to C:\Program Files\TalonFAST\Bin\ and add tum.exe



10. Click "OK"
11. Click on the "Auto-Protect" tab. Under "File Types," click "Selected." Uncheck "Determine file types by examining file contents." Click "Advanced."

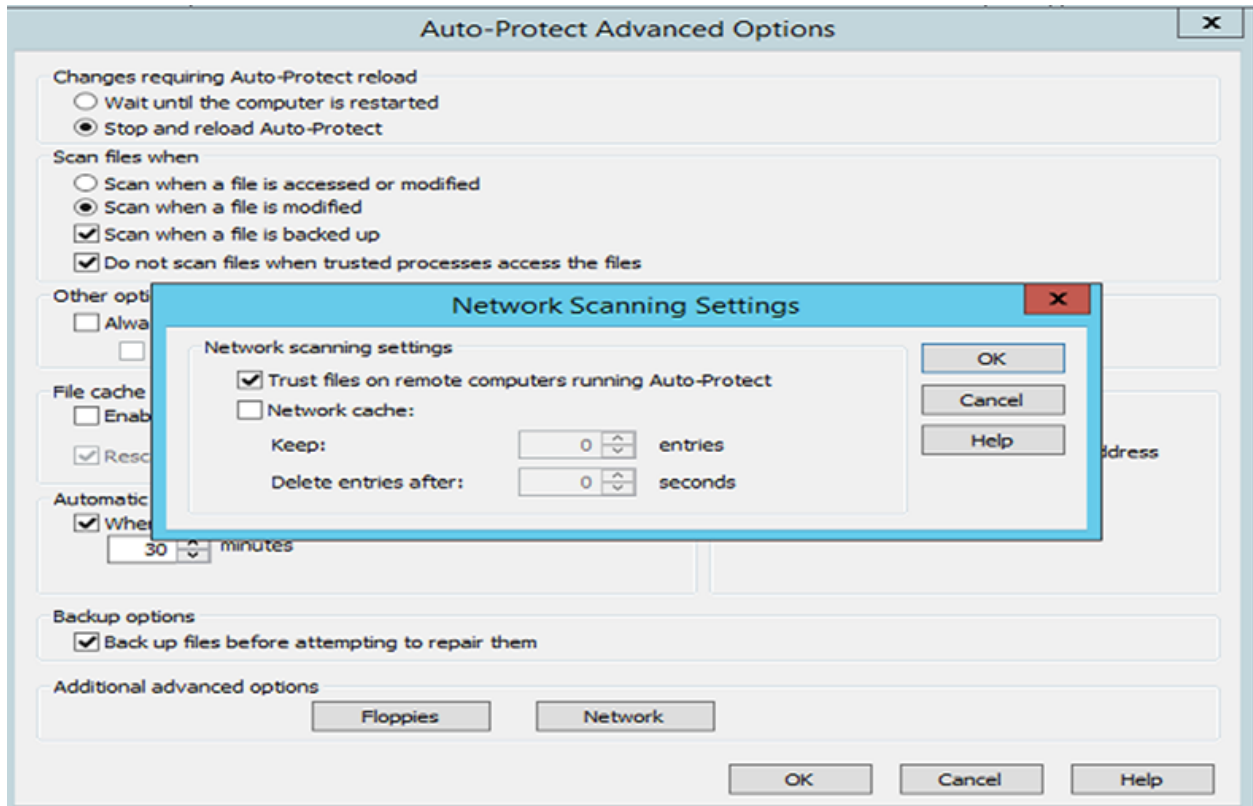


12. Adjust settings as shown below



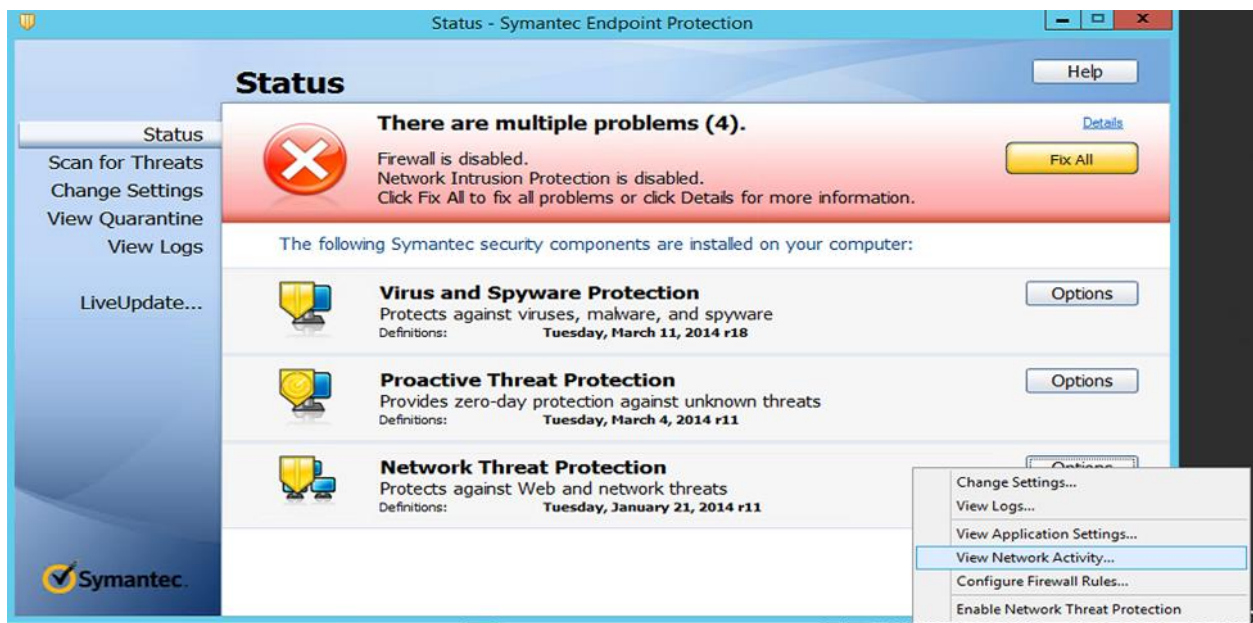
13. Click **“Network”**

14. Uncheck **“Network cache”**

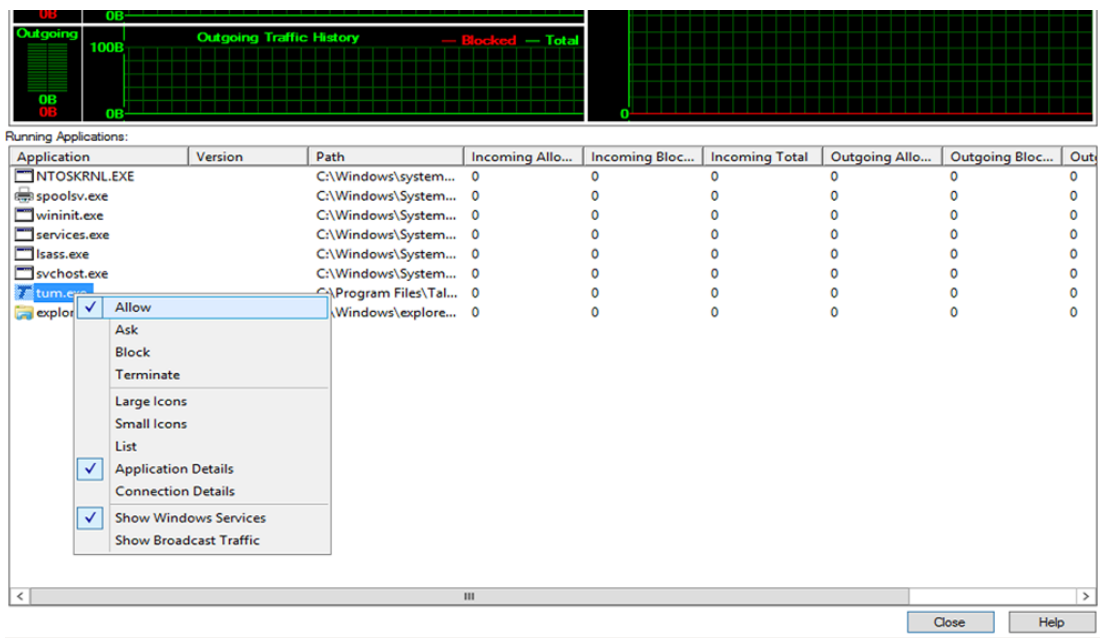


15. Click **“OK”**

16. **“Network Threat Protection”** -> Click **“Options”** and select **“View Network Activity”**



17. Right click `tum.exe` and select **“Allow”**



Configuration is complete.

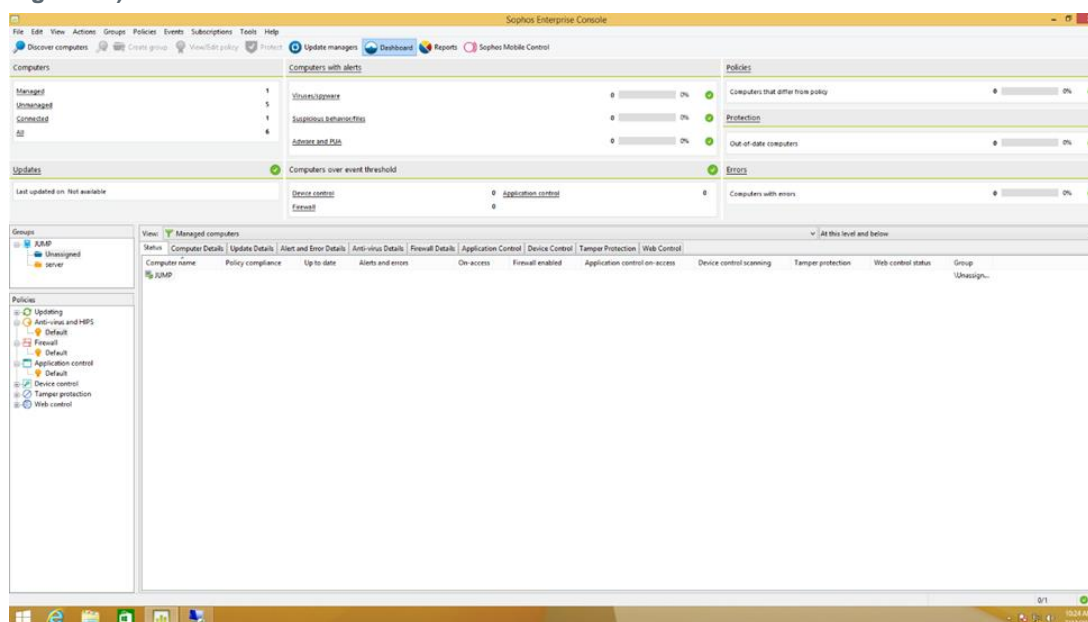
Sophos Endpoint Security and Control v10.x

This section outlines best practices for Sophos Endpoint Security and Control targeted for GFC appliances based on Windows Server.

Baseline Protection (Enterprise Console Configuration)

After completing a typical installation of the Sophos Enterprise Console, follow the configuration specifics as documented below. This process outlines the procedure to configure Sophos Endpoint Security and Control from a central configuration perspective.

Figure 28)



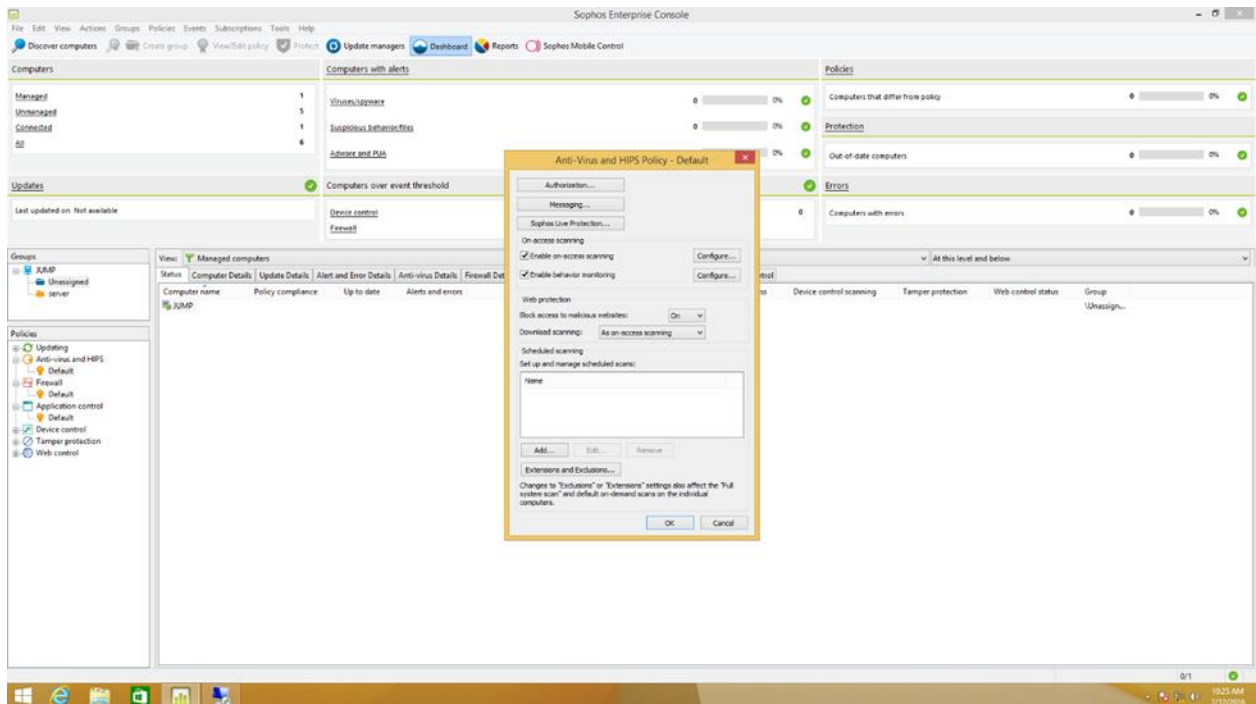
Excluding Services and Processes using Sophos Enterprise Control

This section details how to exclude GFC processes on server and remote appliances from Sophos antivirus scanning.

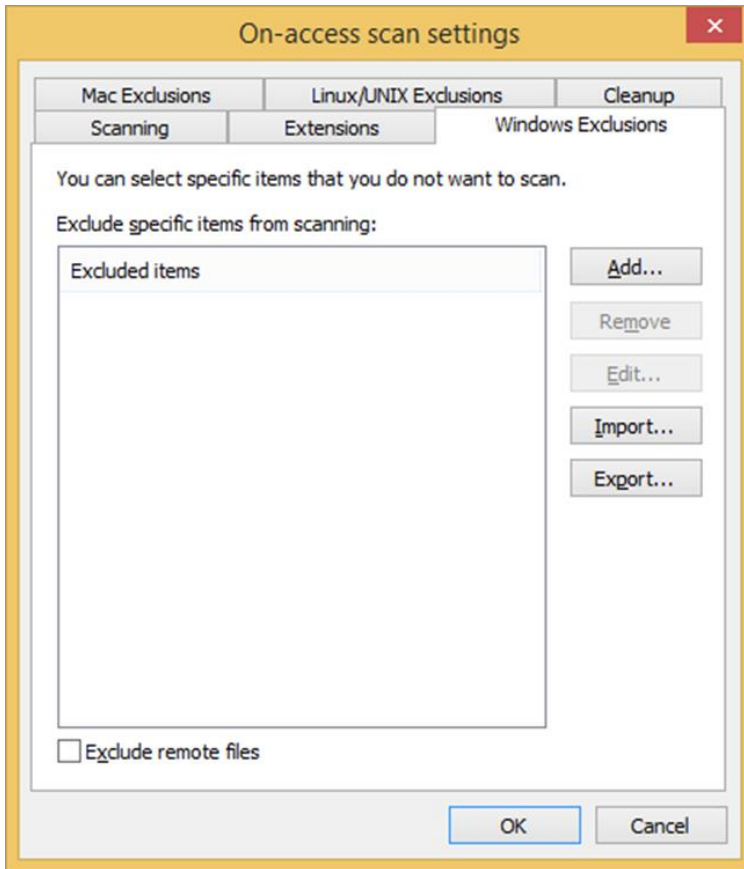
Note: Ensure that GFC processes, services, and drives are excluded from antivirus scanning

These changes should be made to Server and Client policies as well as group policy for GFC users if applicable:

1. Expand the **“Anti-Virus and HIPS”** tree in the **“Policies”** section of the Enterprise Console. Double-click the policy you wish to adjust.



2. Click the **“Configure...”** button next to Enable on-access scanning
3. Click the **“Windows Exclusions”** tab

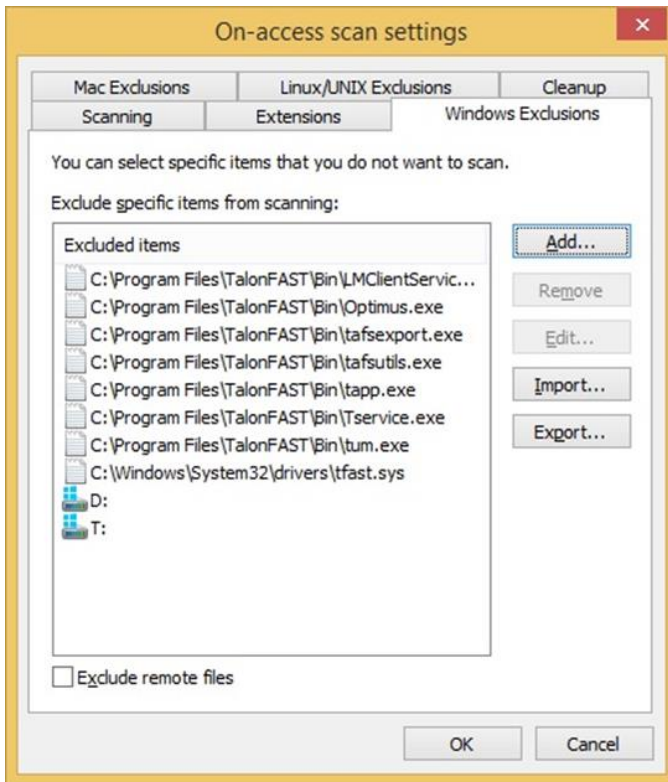


4. Add the following items to the Excluded Items list and click OK when finished:

```
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
C:\Program Files\TalonFAST\Bin\Optimus.exe
C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe
C:\Program Files\TalonFAST\Bin\tafsexport.exe
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\TappN.exe
C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe
C:\Windows\System32\drivers\tfast.sys
C:\Program Files\TalonFAST\FastDebugLogs
D:\
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\\?\GLOBALROOT\Device\TalonCacheFS\
\\?\GLOBALROOT\Device\TalonCacheFS\*
\Device\TalonCacheFS\
```

Exclude Process tum.exe

Exclude Process tapp.exe

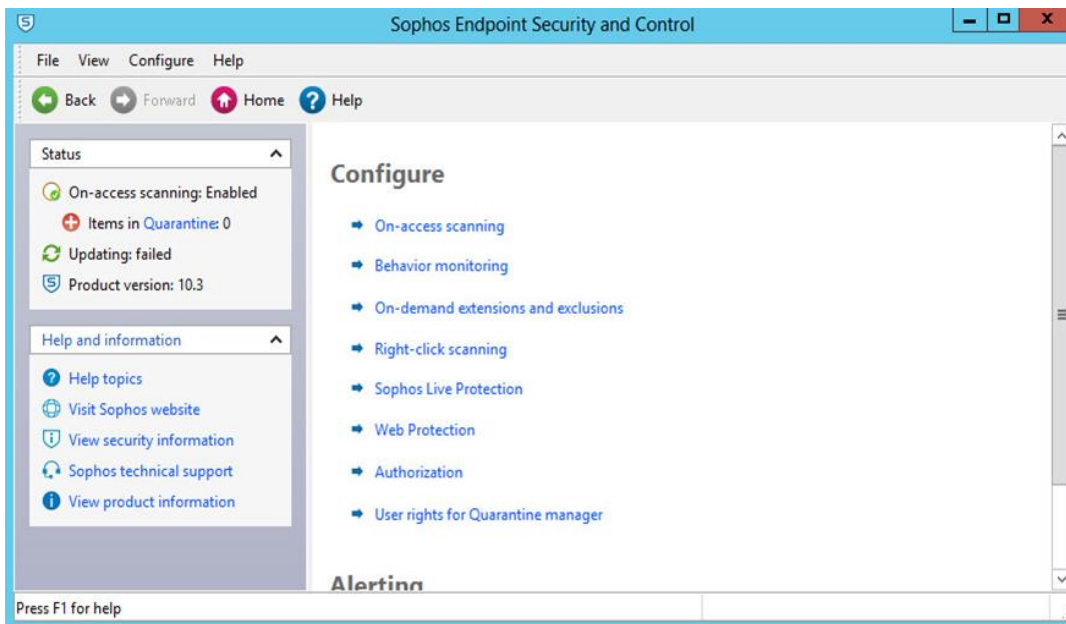


To verify the central configuration results on a connected client machine, we can use the Sophos Endpoint Security and Control panel.

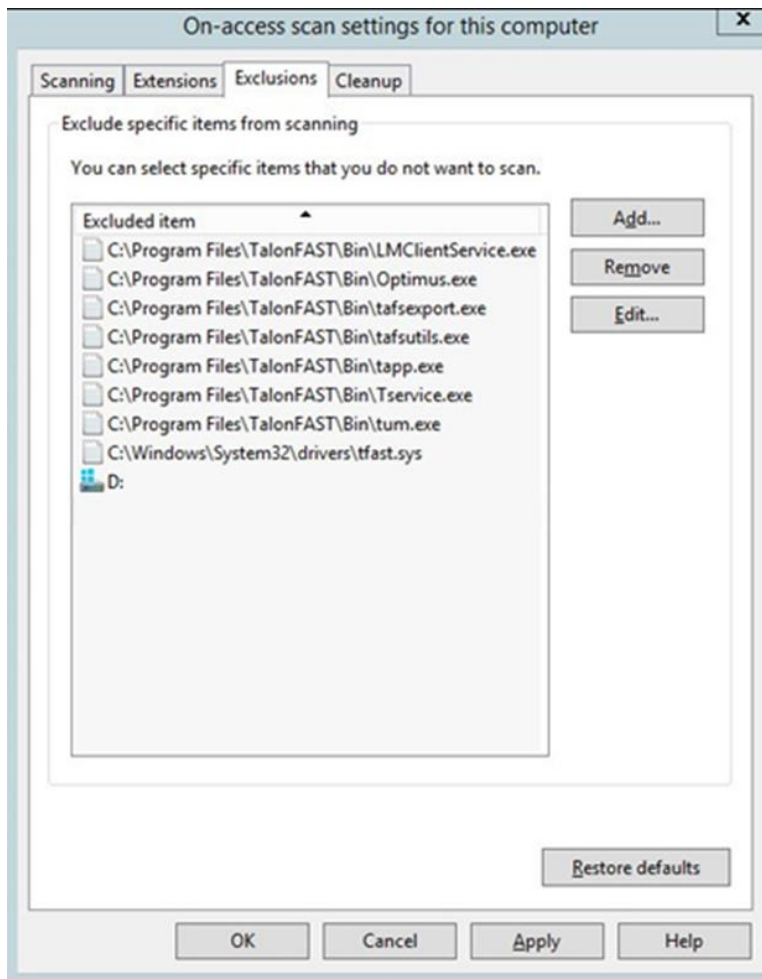
5. Click **“Configure anti-virus and HIPS”**.



6. Click “On-access scanning”



7. Click the “Exclusions” tab to verify that the correct policy and exclusions have been applied to the appliance



Sophos built in Firewall

Microsoft Windows Server 2016 and 2019 by default includes a Microsoft Windows Firewall. GFC automatically provides a script to perform Microsoft Windows firewall maintenance, allowing ports associated with GFC. GFC recommends the use of the Microsoft Windows firewall.

Trend Micro Officescan

1. Open the Management GUI and navigate to **"Networked Computers"** -> **"Client Management"**.

Summary

Current server: Win2k12-Trend2.tss.local

Scan Now for All Domains
Update Server Now

Summary
Security Compliance
Networked Computers

Activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Damage Cleanup Services

OfficeScan OfficeScan and Plug-ins Smart Protection Network

Client Connectivity

Latest data refresh: 06/13/2016 08:18 am

Status	Smart Scan	Conventional Scan	Total
Online	1	0	1
Offline	0	0	0
Roaming	0	0	0
Total	1	0	1

Security Risk Detections

Latest data refresh: 06/13/2016 08:18 am

Type	Detections	Infected Computers
Virus/Malware	0	0
Spyware/Grayware	0	0

Outbreaks

View Top 10 Security Risk Statistics

Alert	Type	Current Outbreak	Last Outbreak
Virus/Malware	None	None	None
Spyware/Grayware	None	None	None

Client Updates

Online Clients: 1, Smart Scan: 1, Conventional Scan: 0

Latest data refresh: 06/13/2016 08:18 am

Expand All	Collapse All	Current Version	Upgraded	Not Upgraded	Upgrade Rate
Antivirus		12.587.00	1	0	100%
Smart Scan Agent Pattern		12.587.00	0	0	0%
Virus Pattern		0.227.00	1	0	100%
IntelliTrap Pattern		1.299.00	1	0	100%
IntelliTrap Exception Pattern		9.850.1008	0	0	0%
		9.850.1008	1	0	100%

2. Navigate to "Scan Settings"-> "Real-Time Scan Settings"

Client Management

Select domains or computers from the client tree, and then select one of the tasks provided above the client tree.

Search for computers: Search Advanced search

Client tree view: View all

OfficeScan Server

- Tss
- Tss.local

Settings

- Scan Settings >>
 - Scan Methods
 - Manual Scan Settings
 - Real-time Scan Settings**
 - Scheduled Scan Settings
 - Scan Now Settings
- Web Reputation Settings
- Behavior Monitoring Settings
- Device Control Settings
- Update Agent Settings
- Privileges and Other Settings
- Additional Service Settings
- Spyware/Grayware Approved List
- Export Settings
- Import Settings

Real-time Scan Settings

☒ Enable virus/malware scan
☒ Enable spyware/grayware scan

Target **Action**

User Activity on Files

Scan files being: created/modified and retrieved ▼

Files to Scan

☐ All scannable files
☒ File types scanned by IntelliScan ⓘ
☐ Files with the following extensions (use commas to separate entries):

Scan Settings

☐ Scan floppy disk during system shutdown
☐ Scan network drive
☐ Scan the boot sector of the USB storage device after plugging in
☒ Scan compressed files
Maximum layers: 2 ▼ ⓘ
☒ Scan OLE objects
Maximum layers: 3 ▼ ⓘ
☒ Detect exploit code in OLE files ⓘ

Virus/Malware Scan Settings Only

☒ Enable IntelliTrap ⓘ

3. On the **"Target"** tab, enable **"File types scanned by IntelliScan"**.
4. Directory scanning. Scroll down and add the following exclusions to **"Scan Exclusion List (Directories)"** to prevent Trend Micro from scanning GFC related directories:

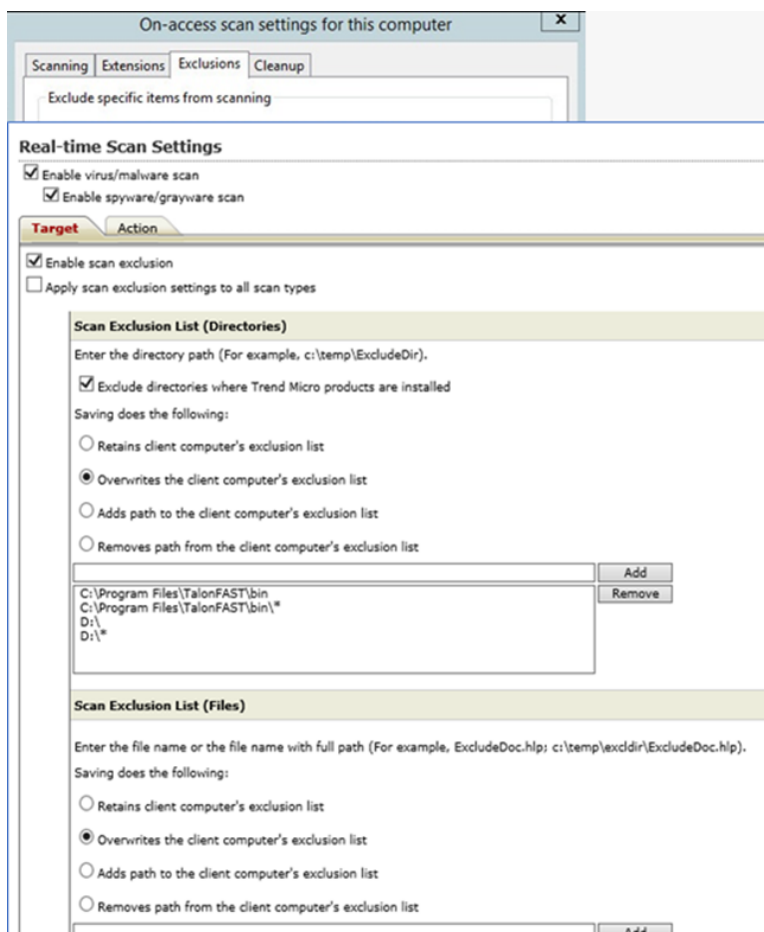

```
C:\Program Files\TalonFAST\bin\*
C:\Program Files\TalonFAST\bin
D:\*
D:
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS
```
5. Trend Micro will scan active processes before performing a folder/file scan. Scroll down and add the following exclusions to **"Scan Exclusion List (Files):"**

```
C:\Program Files\TalonFAST\Bin\*.exe
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
C:\Program Files\TalonFAST\Bin\Optimus.exe
C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe
C:\Program Files\TalonFAST\Bin\tafsexport.exe
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\TappN.exe
C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe
C:\Program Files\TalonFAST\Bin\TService.exe
```

```

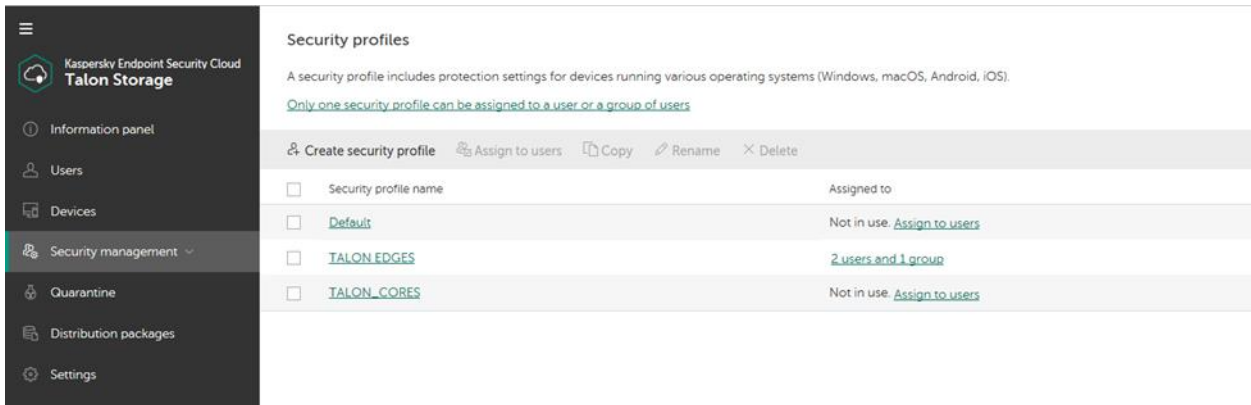
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe
C:\Windows\System32\drivers\tfast.sys
C:\Program Files\TalonFAST\FastDebugLogs
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS\
C:\Program Files\TalonFAST\FastDebugLogs\

```

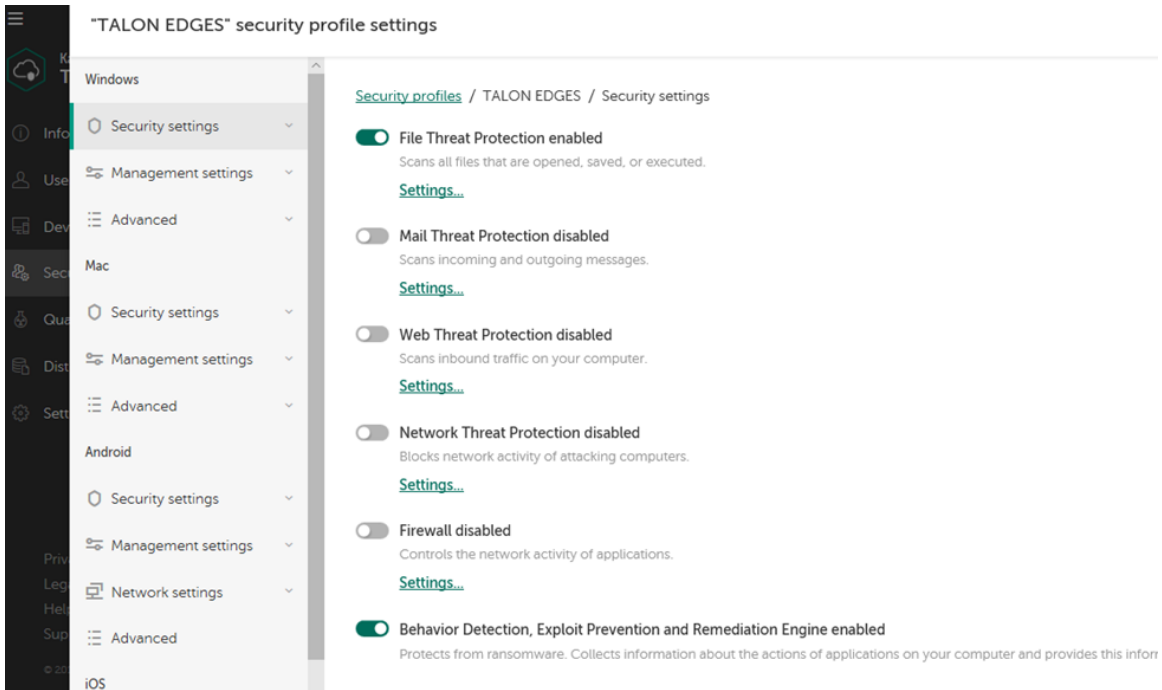


Kaspersky Endpoint Security Cloud

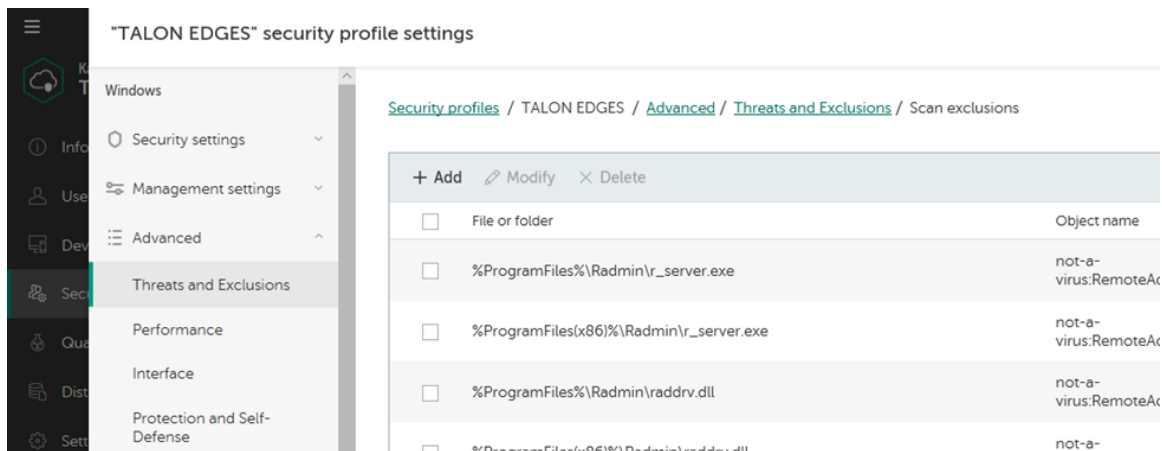
1. Open the Management GUI and navigate to “**Security Management**” -> “**Security Profiles**”.
2. Create a Separate GFC Edge Object OU in Kaspersky Console.



3. For the Security settings disable modules not related to file services. Only the following should be active:
 - a. “File Threat Protection”
 - b. “Behavior Detection, Exploit Prevention, and Remediation Engine”



4. Under “**Threats and Exclusions**” add the Folders / Files for the GFC Services



5. following exclusions to “Scan Exclusion List (Files):”

D:\

D:\LocalFASTData

C:\Program Files\TalonFAST\Bin*.exe

C:\Program Files\TalonFAST\Bin\LMClientService.exe

C:\Program Files\TalonFAST\Bin\LMServerService.exe

C:\Program Files\TalonFAST\Bin\Optimus.exe

C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe

C:\Program Files\TalonFAST\Bin\tafsexport.exe

C:\Program Files\TalonFAST\Bin\tafsutils.exe

C:\Program Files\TalonFAST\Bin\tapp.exe

C:\Program Files\TalonFAST\Bin\TappN.exe

C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe

C:\Program Files\TalonFAST\Bin\TService.exe

C:\Program Files\TalonFAST\Bin\tum.exe

C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe

C:\Windows\System32\drivers\tfast.sys

C:\Program Files\TalonFAST\FastDebugLogs

\\?\TafsMtPt:\ or \\?\TafsMtPt*

\\?\GLOBALROOT\Device\TalonCacheFS\

\\?\GLOBALROOT\Device\TalonCacheFS*

Tum.exe

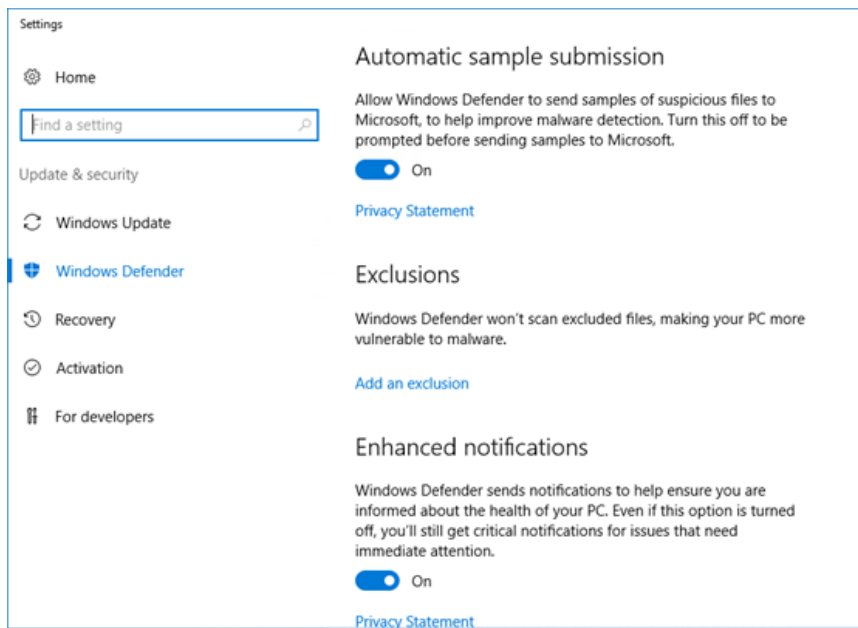
Tapp.exe

<input type="checkbox"/>	\\?\GLOBALROOT\Device\TalonCacheFS*	*	TalonFastVirtualDrive
<input type="checkbox"/>		tum.exe	Talon User Module
<input type="checkbox"/>		Tapp.exe	talon prepop mechanism

Note: The Edges should have the updated policy prior to any users begin working within the GFC Fabric.

Windows Defender

1. Open the Windows Defender Settings and under “**Exclusions**” click “**Add an Exclusion**”.



2. Under “Files and folders” add the GFC exclusions

D:\

D:\LocalFASTData

C:\Program Files\TalonFAST\Bin*.exe C:\Program Files\TalonFAST\Bin\LMClientService.exe

C:\Program Files\TalonFAST\Bin\LMServerService.exe

C:\Program Files\TalonFAST\Bin\Optimus.exe

C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe

C:\Program Files\TalonFAST\Bin\tafsexport.exe

C:\Program Files\TalonFAST\Bin\tafsutils.exe

C:\Program Files\TalonFAST\Bin\tapp.exe

C:\Program Files\TalonFAST\Bin\TappN.exe

C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe

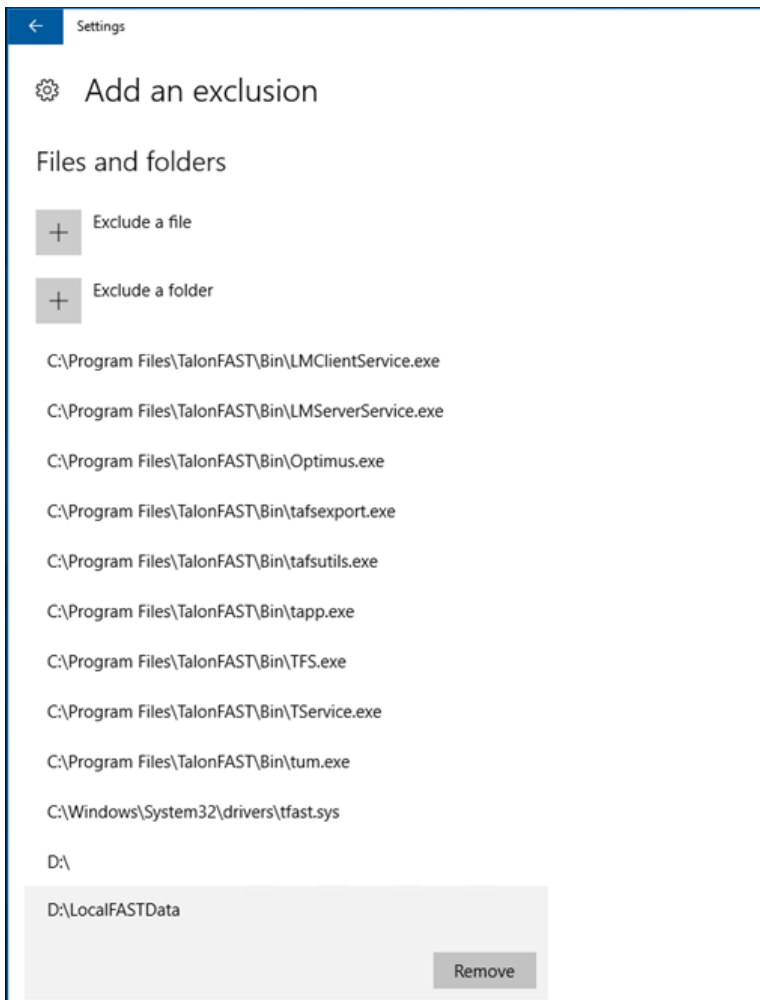
C:\Program Files\TalonFAST\Bin\TService.exe

C:\Program Files\TalonFAST\Bin\tum.exe

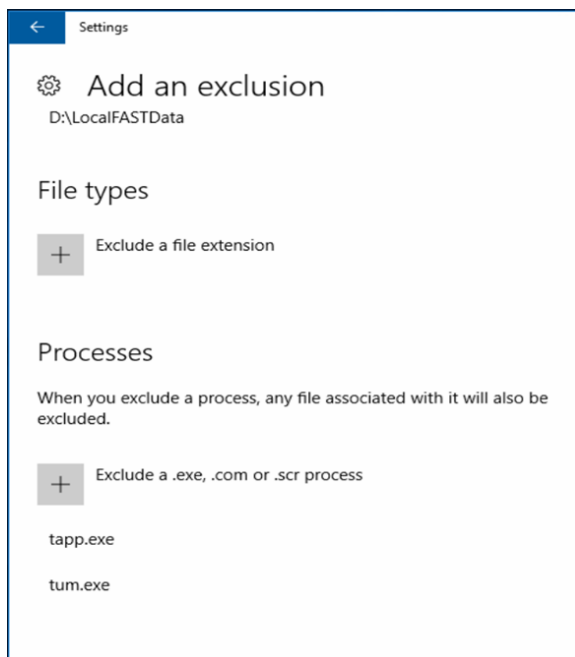
C:\Program Files\TalonFAST\Bin\GfcCIAgentService.exe

C:\Windows\System32\drivers\tfast.sys

C:\Program Files\TalonFAST\FastDebugLogs



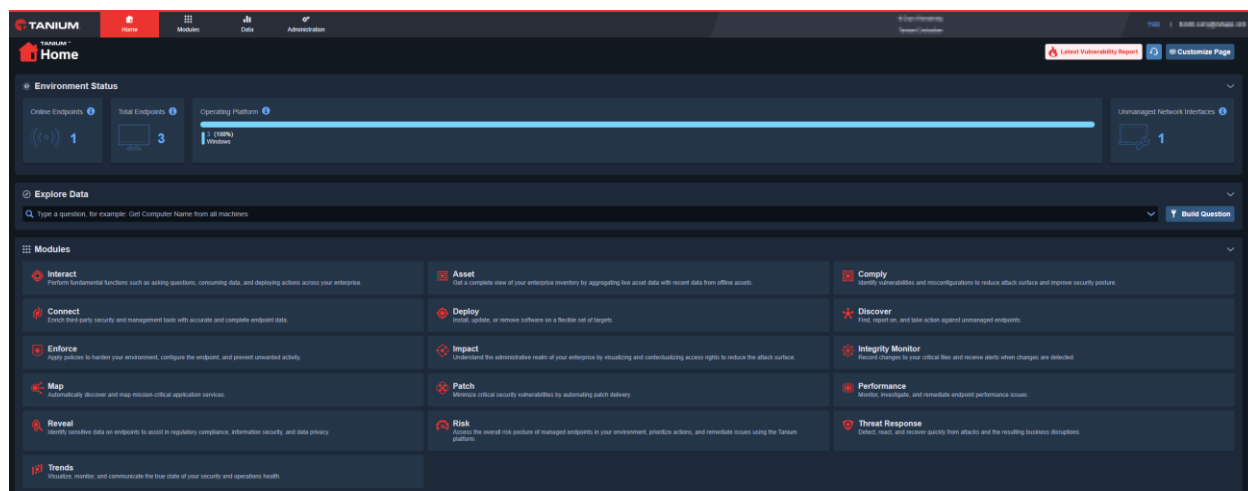
3. Under “**Processes**” exclusions add the following exclusions:
 - a. Tum.exe
 - b. Tapp.exe



Tanium

All configuration will be performed at the Tanium Central Management Suite.

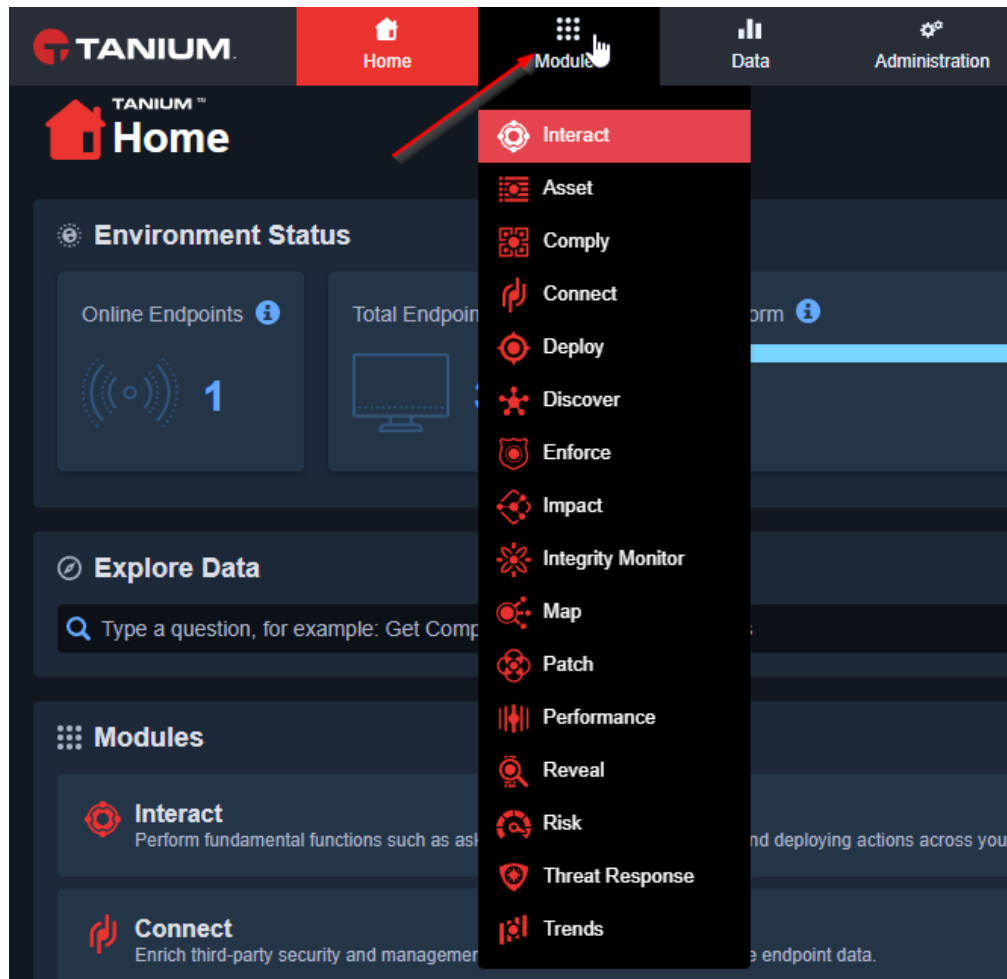
1. Log on with the credentials to Tanium Central Management Suite and below is their dash board.



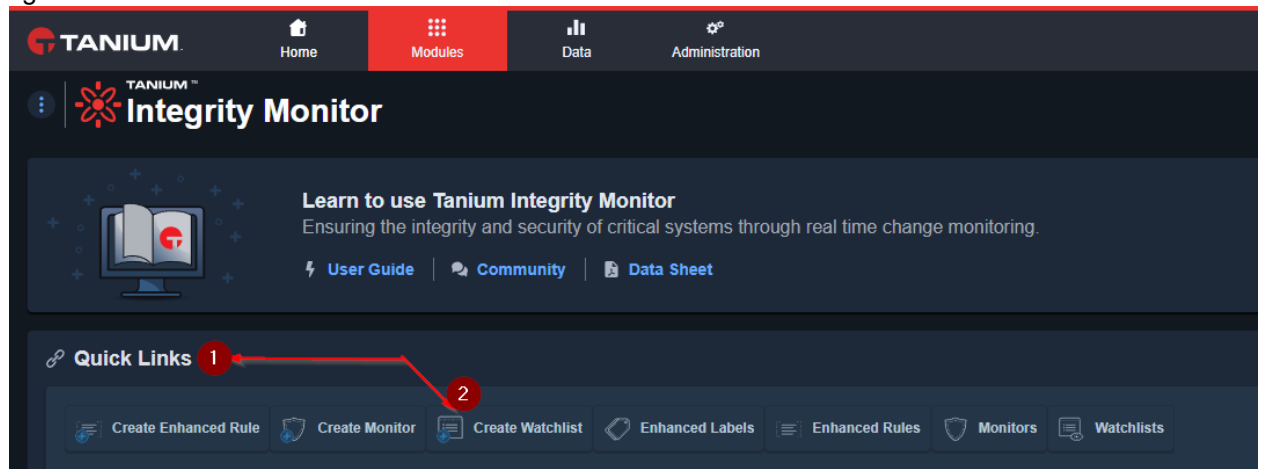
2. From the Central Management Suite click on “Modules”.

Select “Modules”-> “Integrity Monitor” and Click





- Once Integrity Monitor module is selected, observe a task bar labeled “**Quick Links**” as shown in figure. Select the “**Create Watchlist**” link.



- On the Create Watchlist page, enter the required information.
Enter the following:
Name: Global File Cache Critical Exclusions

Description: Exclusion list for NetApp Global File Cache critical paths.
Path Style: Windows



The screenshot shows the 'Create Watchlist' interface in the Integrity Monitor application. The header includes the 'Integrity Monitor' logo and title. The main section is titled 'Create Watchlist' and contains a 'Summary' subsection with the instruction 'Provide the identifying details of the watchlist.' Below this, there are three fields: 'Name' with the value 'Global File Cache Critical Exclusions', 'Description' with the value 'Exclusion list for NetApp Global File Cache critical paths.', and 'Path Style' with radio buttons for 'Windows' (selected) and 'Unix'.

Integrity Monitor

Create Watchlist

Summary
Provide the identifying details of the watchlist.

Name *
Global File Cache Critical Exclusions

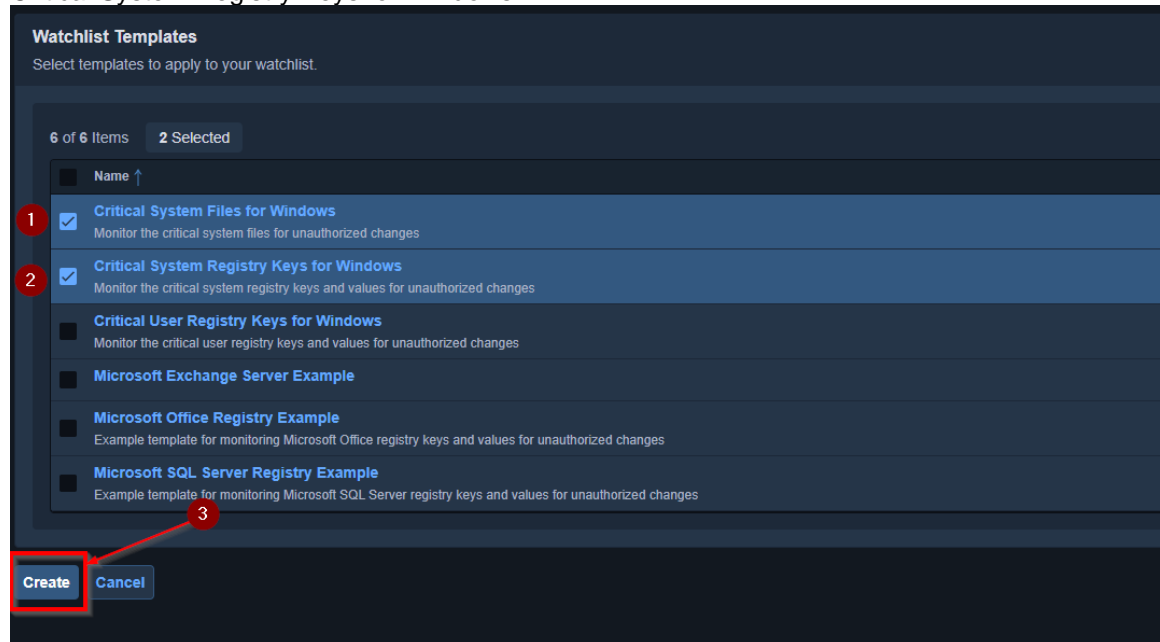
Description
Exclusion list for NetApp Global File Cache critical paths.

Path Style *
☒ Windows
☐ Unix

- Next, Select templates to base the watchlist on.
Select the following options under Watchlist Templates and press Create.

Critical System Files for Windows

Critical System Registry Keys for Windows



6. Once the Watchlist has been created pick the categories presented relating to Windows File Paths under the File Paths tab. The following are the concerned categories.
C:\Program Files
C:\Windows

7. Select a designated category, and press Edit Path.

The screenshot shows the 'Global File Cache Critical Exclusions' interface in the Integrity Monitor. The breadcrumb trail is 'Integrity Monitor > Watchlists > Global File Cache Critical Exclusions'. The main title is 'Global File Cache Critical Exclusions'. Below the title is the subtitle 'Exclusion list for NetApp Global File Cache critical paths.'.

The interface displays two categories of exclusions:

- Windows**: Path Style, 17 File Paths
- File Paths (11)**: Registry Paths (6)

The 'File Paths (11)' category is selected, and a list of 11 items is displayed. The items are:

- C:\Boot\BCD
- C:\Bootmgr
- C:\Documents and Settings
- C:\EFI
- C:\Program Files** (Selected)
- C:\Program Files (x86)
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
- C:\System Volume Information
- C:\Users
- C:\Users*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- C:\Windows

The 'C:\Program Files' item is selected, and the 'Edit Path' button is visible. The '11 of 11 Items' and '1 Selected' status is shown at the top of the list.

8. Once Edit Path is selected, navigate to, and click the Path Exclusions field at the bottom of the page:

TANIUM Home Modules Data Administration

Integrity Monitor > Watchlists > Watchlist Details > Edit Path

Edit Path

Details
Provide the identifying details of the path.

Path *
C:\Program Files
Enter an absolute path. Glob-style * and ? are supported.

Change Type *

- ☒ Create
- ☐ Write
- ☒ Delete
- ☒ Rename
- ☐ Permission

Inclusions and Exclusions
Use path includes and excludes to define the path's scope.

▶ Path Inclusions (0)

▼ Path Exclusions (1) **1**

Enter a relative path. Wildcard-style * and ? are supported.

*\

+ Add

Save Path Cancel

Click Add Path for each new exclusion path.

The following are the required exclusions under C:\Program Files

TalonFAST\
TalonFAST\bin\
TalonFAST\FASTDebugLogs\
FASTShare*

Select Save Path.

Inclusions and Exclusions
Use path includes and excludes to define the path's scope.

► Path Inclusions (0)

▼ Path Exclusions (5)

Enter a relative path. Wildcard-style * and ? are supported.

- **
- TalonFAST*
- TalonFAST\\Bin*
- TalonFAST\\FASTDebugLogs*
- FASTShare*

+ Add

Save Path Cancel

9. Select C:\\Windows and click Edit Path.
Click Add at the bottom of the page and add the following:
tfast.sys

TANIMUM Home Modules Data Administration

Integrity Monitor > Watchlists > Watchlist Details > Edit Path

- CbsTemp*
- ServiceProfiles\\NetworkService\\AppData\\Local\\Temp*
- ServiceProfiles\\LocalService\\AppData\\Local\\Iastalve*.dat
- ServiceProfiles\\NetworkService\\AppData\\Local\\Microsoft\\Windows Media Player NSS\\3.0\\Icon Files*.png
- assembly*
- CSC*
- DEBUG*
- security*
- System32\\WlmsData*
- Temp*
- *.log
- *.tmp
- *.temp
- *.hdr
- *.customdestinations-ms
- *.dat
- System32\\GroupPolicy*
- appcompat*
- SysWOW64\\GroupPolicy*.ini
- tfast.sys

+ Add

Save Path Cancel

Select Save Path.

10. On the Global File Cache Critical Exclusions Watchlist page, select Registry Paths.

TANIUM Home Modules Data Administration

Integrity Monitor > Watchlists > Global File Cache Critical Exclusions

Global File Cache Critical Exclusions

Exclusion list for NetApp Global File Cache critical paths.

Windows 17
Path Style File Paths

File Paths (11) **Registry Paths (6)**

6 of 6 Items

Name ↑
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Mail
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

11. On the right hand side of the page, select Add Paths->New.

Filter Items

Add Paths ▼

Inclusions

3

- New
- Import From File
- Import From Templates

For the Path, type:
HKEY_LOCAL_MACHINE

The screenshot shows the Tanium web interface for configuring a new path in the Integrity Monitor. The top navigation bar includes the Tanium logo and links for Home, Modules (highlighted in red), Data, and Administration. Below this, a breadcrumb trail shows the path: Integrity Monitor > Watchlists > Watchlist Details > Add Path. The main heading is 'Add Path'. The 'Details' section prompts the user to provide identifying details. The 'Path' field, marked with a red asterisk, contains 'HKEY_LOCAL_MACHINE'. A note below the field states: 'Enter an absolute path. Glob-style * and ? are supported.' The 'Change Type' section, also marked with a red asterisk, contains four checked checkboxes: 'Create', 'Write', 'Delete', and 'Rename'. The 'Inclusions and Exclusions' section prompts the user to use path includes and excludes to define the path's scope. It shows two expandable sections: 'Path Inclusions (0)' and 'Path Exclusions (0)'. At the bottom, there are two buttons: 'Add Path' and 'Cancel'.

TANIMUM Home Modules Data Administration

Integrity Monitor > Watchlists > Watchlist Details > Add Path

Add Path

Details

Provide the identifying details of the path.

Path *

HKEY_LOCAL_MACHINE

Enter an absolute path. Glob-style * and ? are supported.

Change Type *

- ☒ Create
- ☒ Write
- ☒ Delete
- ☒ Rename

Inclusions and Exclusions

Use path includes and excludes to define the path's scope.

- ▶ Path Inclusions (0)
- ▶ Path Exclusions (0)

Add Path **Cancel**

12. Next, select Path Exclusions at the bottom of the screen and add the following paths:

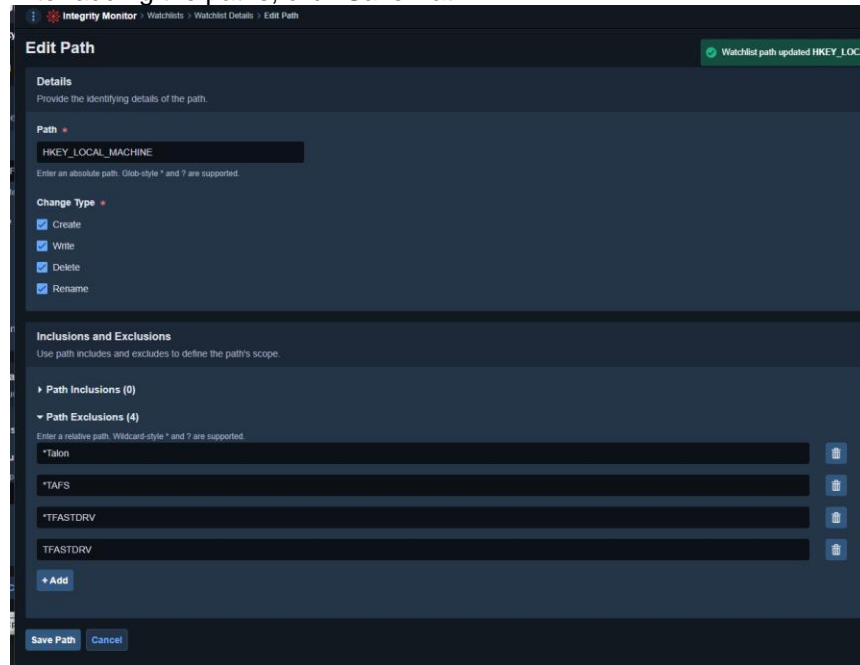
*Talon

TAFS

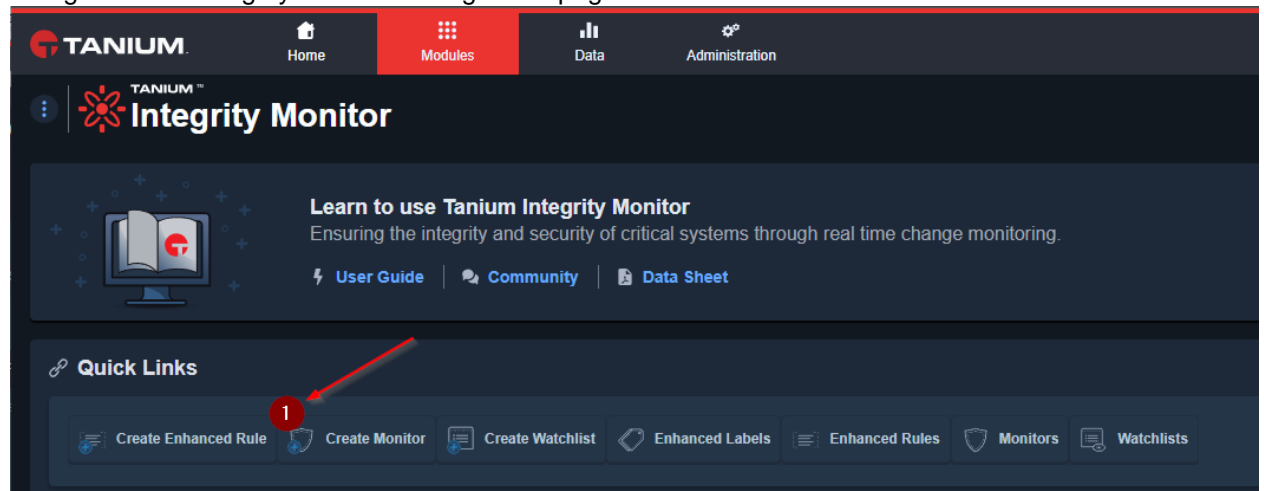
TFAST

TFASTDRV

After adding the paths, click Save Path.



13. Navigate to the Integrity Monitor management page and select Create Monitor:



14. Fill out the following fields as shown below:

Name: GFC monitor

Description: GFC Endpoint Monitor

Deployment Criteria:

Platform: Windows
Labeling Method: Basic Labeling
Monitoring Method: Event Monitoring (uncheck Hash Monitoring)
Targeting: All Windows Servers (or your secluded GFC computer group)
Windows Driver: Check Install Tanium Driver
WatchLists: Global File Cache Critical Exclusions

The screenshot shows the 'Integrity Monitor' configuration window. It is divided into several sections: 'Summary' with fields for 'Name' (GFC Monitor) and 'Description' (GFC Endpoint Monitor); 'Deployment Criteria' with a 'Platform' dropdown set to 'Windows', 'Labeling Method' with 'Basic Labeling' selected, 'Monitoring Method' with 'Event Monitoring' checked and 'Hash Monitoring' unchecked, and 'Windows Driver' with 'Install Tanium Driver' checked; 'Targeting' with a 'Select Computer Groups' button and a list showing '1 selected'; and 'Watchlists' with a search bar containing 'Global File Cache Critical Exclusions' and a list of four items where 'Global File Cache Critical Exclusions' is selected. At the bottom are 'Create' and 'Cancel' buttons.

Select: Create.

Reboot your GFC appliances for the Tanium driver install.

Cisco AMP

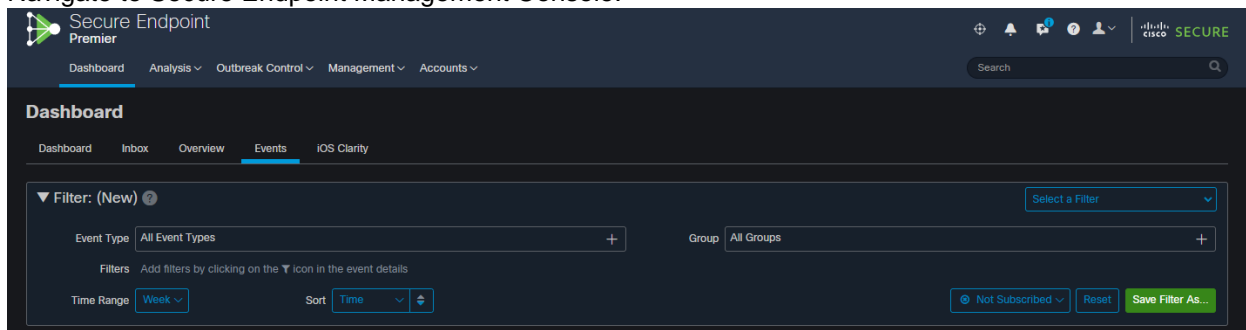
The purpose of this document is to provide best practices to support Cisco AMP platform and its configuration. In general most AV applications have various modules and each module have to be configured in such manner that they do not interfere with operation with GFC.

This intended audience for this document are Solution Engineers, GFC Administrators and GFC support.

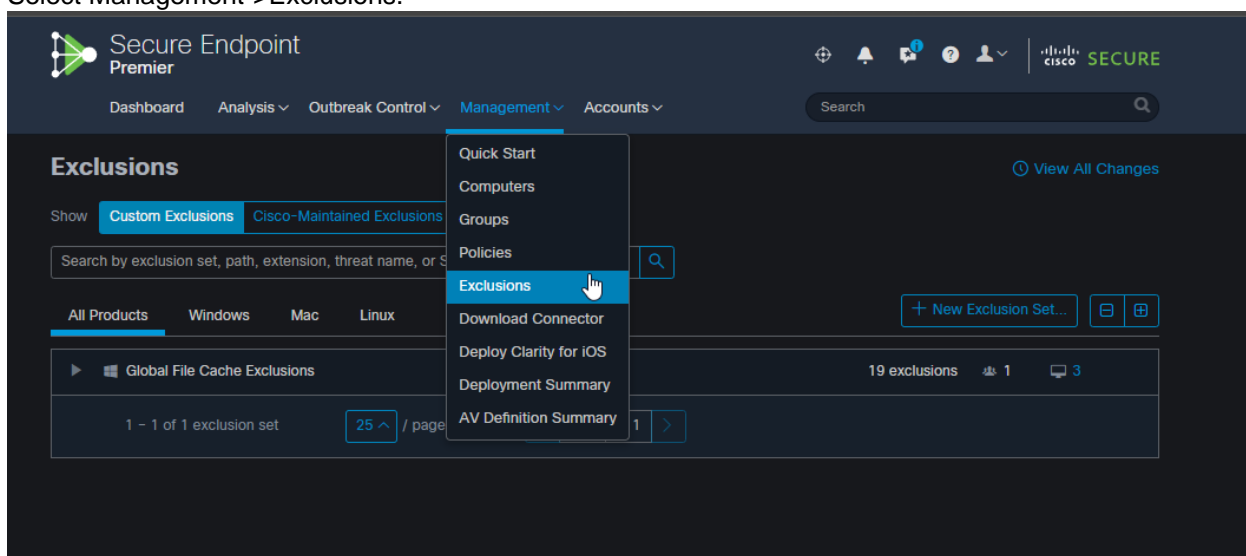
This document contains instructions on configuring and correctly implementing the watchlist exclusions for critical NetApp Global File Cache processes and folder paths.

All configuration will be performed at the Secure Endpoint Management Suite.

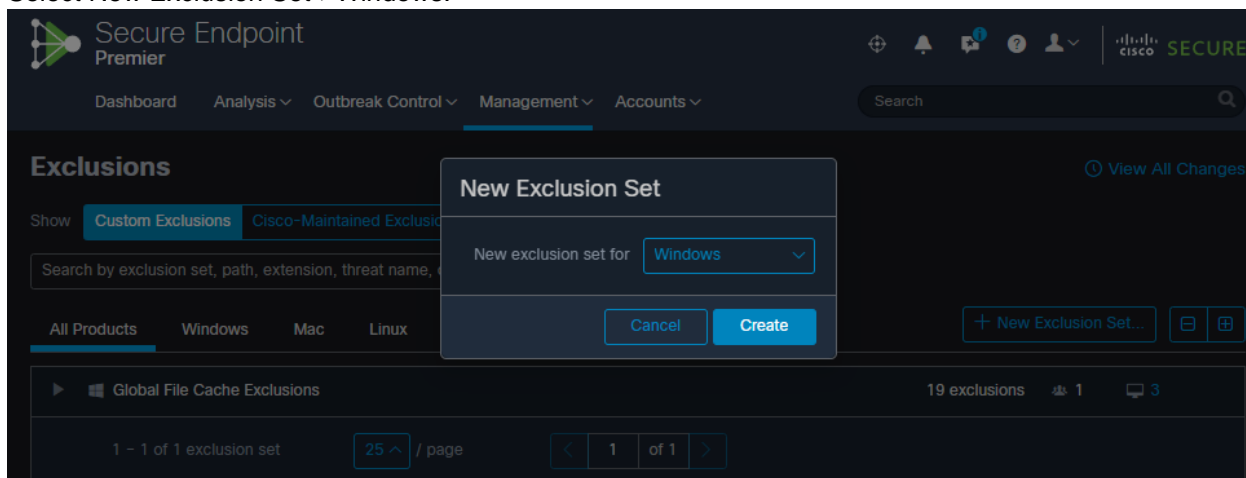
1. Navigate to Secure Endpoint Management Console:



2. Select Management->Exclusions.



3. Select New Exclusion Set->Windows:



4. Select Add Multiple Exclusions and add the following, then Save:

Wildcard: *TAFS

Wildcard: FTLSummaryGenerator.exe

Wildcard: LMClientService.exe

Wildcard: LMServerService.exe

Wildcard: Optimus.exe

Wildcard: Policydb.xml

Wildcard: RFASTSetupWizard.exe

Wildcard: tafsexport.exe

Wildcard: tafsutils.exe

Wildcard: tapp.exe

Wildcard: TappN.exe

Wildcard: TService.exe

Wildcard: tum.exe

Wildcard: GfcCIAgentService.exe

Path: C:\Program Files\TalonFAST\FastDebugLogs\

Path: C:\Windows\System32\drivers\tfast.sys

Path: D:\

Path: D:\LocalFASTData\

Path: GLOBALROOT\Device\TalonCacheFS\

Path: TafsMtPt*



5. Navigate to Management->Policies then select New Policy:

New Policy
Windows

Name:

Description:

Modes and Engines
Exclusions
1 exclusion set
Proxy
Outbreak Control
Product Updates
Advanced Settings

Conviction Modes

These settings control how Secure Endpoint responds to suspicious files and network activity.

Files

Quarantine **Audit**

Remove and report malicious files.

Network

Block **Audit** **Disabled**

Block and report malicious network connections.

Malicious Activity Protection

Quarantine **Block** **Audit** **Disabled**

End ransomware-like processes, remove their executable, and report them.

System Process Protection

Protect **Audit** **Disabled**

Block possible malicious tampering of critical operating system processes and report the activity.

Script Protection

Quarantine **Audit** **Disabled**

Stop, remove, and report malicious scripts when they execute.

Exploit Prevention

Block **Audit** **Disabled**

Detect binary code injection attacks against some processes, and the process, and report it.

Exploit Prevention - Script Control

Block **Audit** **Disabled**

Report when an application loads certain DLLs, but take no other action.

Behavioral Protection

Protect **Audit** **Disabled**

Detect malicious activity, take remedial actions as needed, and report it.

☐ Enable Event Tracing for Windows

Detection Engines

☒ TETRA

Recommended Settings

Workstation

- Files: Quarantine
- Network: Block
- Malicious Activity Protection: Quarantine
- System Process Protection: Protect
- Script Protection: Quarantine
- Exploit Prevention: Block
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

[Apply Workstation Settings](#)

Server

- Files: Quarantine
- Network: Disabled
- Malicious Activity Protection: Disabled
- System Process Protection: Disabled
- Script Protection: Quarantine
- Exploit Prevention: Audit
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

[Apply Server Settings](#)

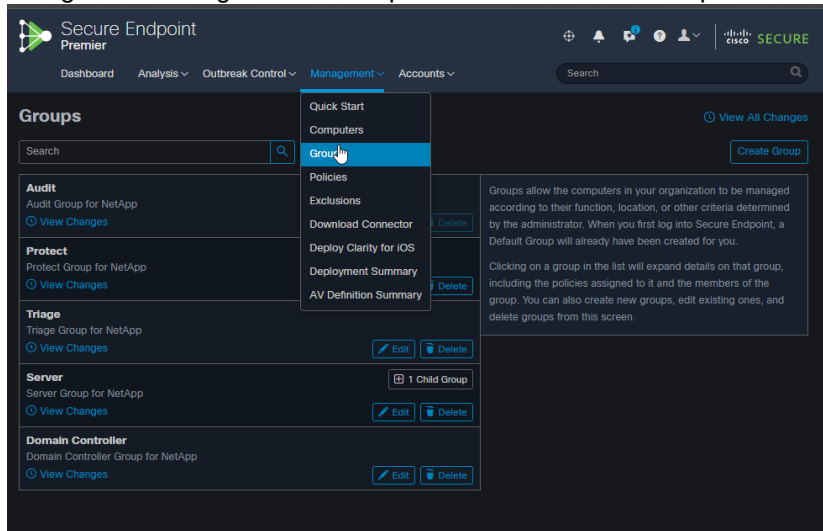
[Cancel](#) [Save](#)

Name: Global File Cache Policy

Description: GFC

- Select Audit for Exploit Prevention – Script Control
- Select Exclusions on the left.
- Under Custom Exclusions, select Global File Cache Exclusions and press save.

6. Navigate to Management->Groups and select Create Group



Name: GFC Appliances

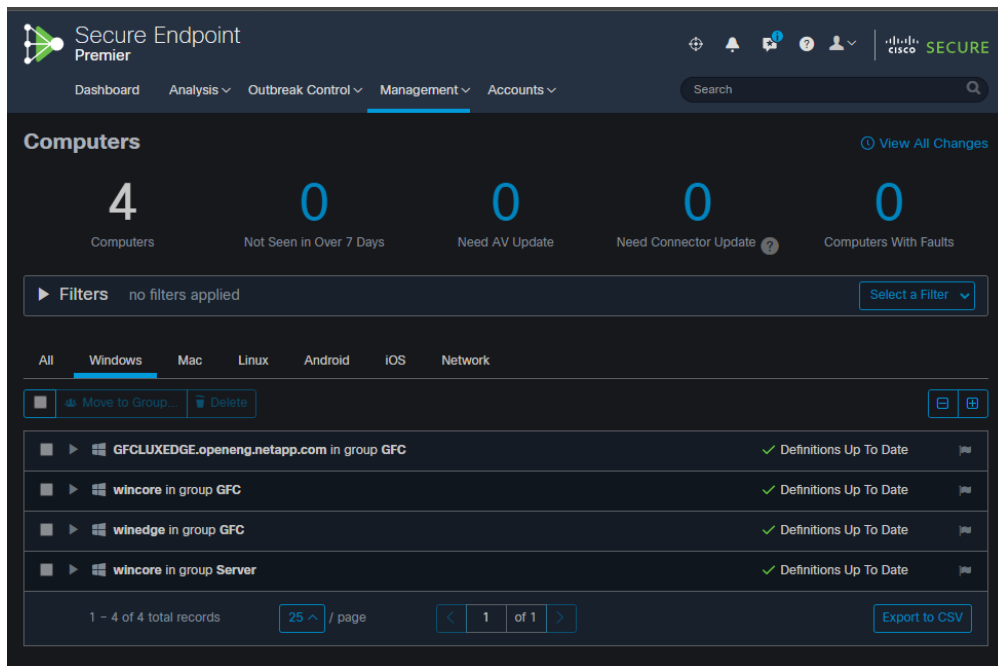
Description: GFC

Parent Group: Server

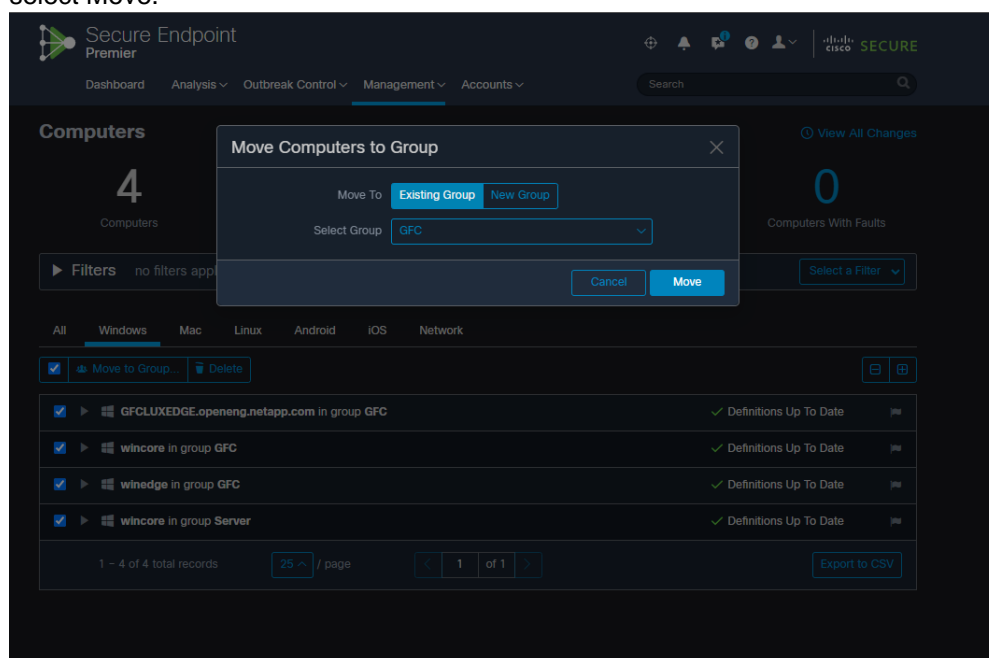
Windows Policy: Global File Cache Policy

Press Save.

7. Navigate to Management->Groups, Select Windows:



8. Select GFC appliances, select Move Group, and move them to the GFC group just created. And select Move.



9. Reboot the appliances.

Appendix B: Disable VMware ESX(i) Hot Plug Capability

GFC does not support caching of files and data on removable drives. Certain versions of VMware ESX will present hard disks as HotPlug/HotADD by default which Windows Server will define as “Removable.” This default behavior can be modified by editing the virtual machine’s .vmx file or within the vSphere Client.

To Disable HotPlug Capability Using the vSphere Client

1. Connect to the ESXi/ESX host or vCenter Server using the vSphere Client.
2. Power off the virtual machine.
3. Right-click the virtual machine and click “**Edit Settings**”.
4. Click the “**Options**” tab.
5. In the “**Advanced**” section, click “**General**”.
6. Click the “**Configuration Parameters**” Button.
7. Click the “**Add Row**” button.
8. Insert a new row with the name `devices.hotplug` and a value of “**false**”.
9. Power on the virtual machine.

To Disable HotPlug Capability Using the vSphere Web Client

1. From a web browser, connect to the vSphere Web Client.
2. Log in with Administrator credentials.
3. Navigate to the virtual machine you want to modify.
4. Right-click the virtual machine and select “**Edit Settings**”.
5. Click the “**VM Options**” tab.
6. In the “**Advanced**” section, click “**General**”.
7. Click “**Edit Configuration**”.
8. Click “**Add Row**”.
9. Insert a new row with the name `devices.hotplug` and a value of “**false**”.
10. Power on the virtual machine.

To Disable HotPlug Capability by Editing the Virtual Machine’s .vmx File

1. Power off the virtual machine.
2. Access the ESXi/ESX service console using an SSH client.
3. Open the virtual machine configuration file (.vmx) in a text editor. The default location is:
`/vmfs/volumes/datastore_name/vm_name/vm_name.vmx`
4. Add the line:
`devices.hotplug = "false"`
Note: This setting does not interfere with HotPlug CPU/memory.
5. Save and close the file.
6. Power on the virtual machine.

Appendix C: NetApp Global File Cache (GFC) PowerShell Configuration

GFC Optimus PSM

Software Requirements

Windows PowerShell 5.x (Administration / Elevated Permissions)

Windows Management Framework 5.x

GFC

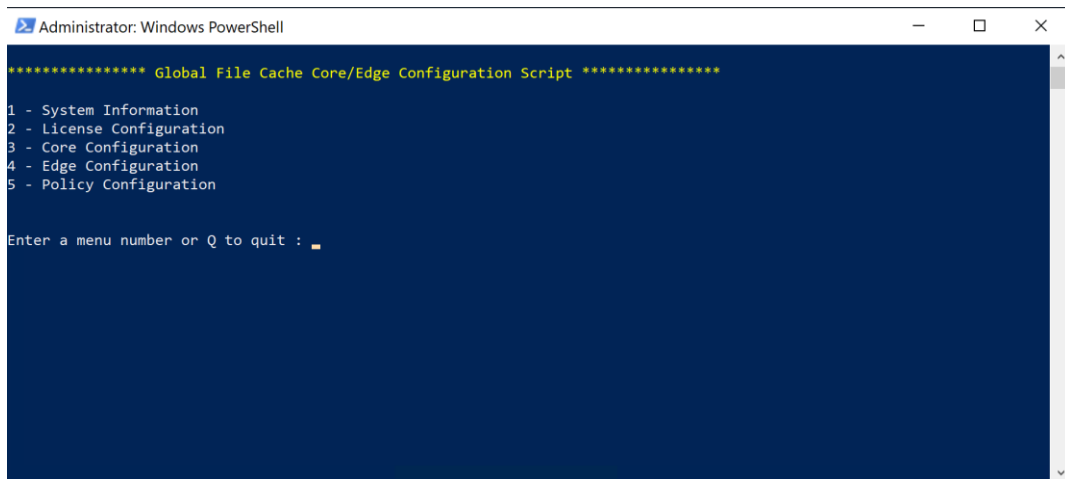
Launch GFC PowerShell Configuration CLI

To launch PowerShell configuration UI, give below command in PowerShell window. This will launch below UI.

```
&"C:\Program Files\TalonFAST\Bin\TalonFASTConfig.ps1"
```

Menu:

Figure 29)



Configuration Process

GFC configuration distributed in below sections:

System Information

License Configuration

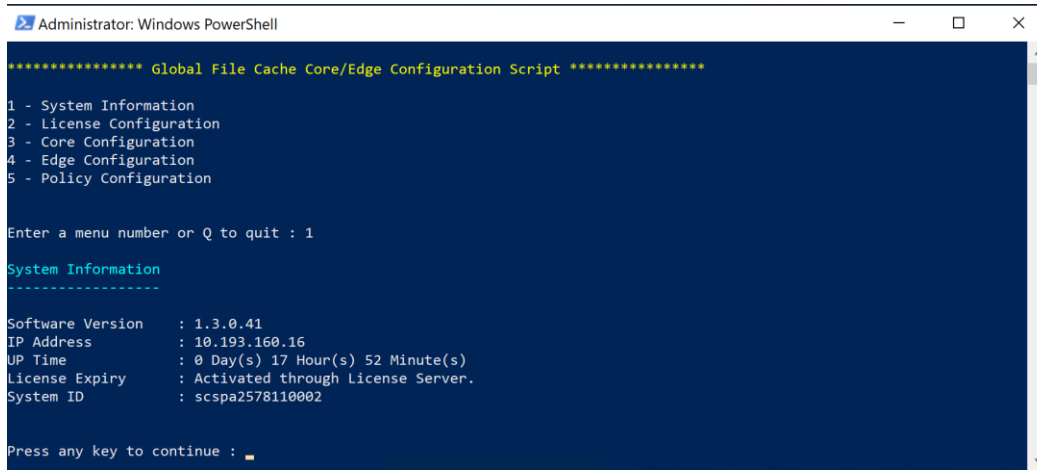
Core Configuration

Edge Configuration

Policy Configuration

System Information

Note: This menu item will display the system information and the GFC software version.



```
Administrator: Windows PowerShell

***** Global File Cache Core/Edge Configuration Script *****

1 - System Information
2 - License Configuration
3 - Core Configuration
4 - Edge Configuration
5 - Policy Configuration

Enter a menu number or Q to quit : 1

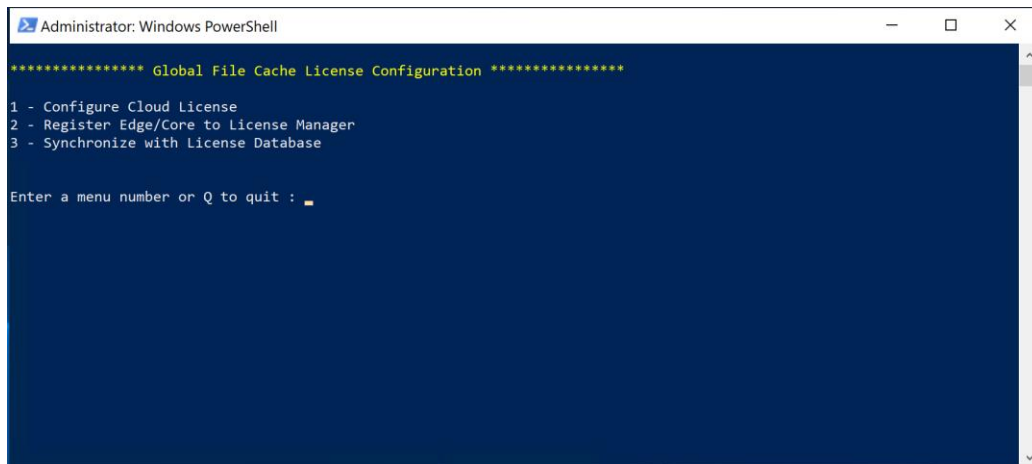
System Information
-----
Software Version   : 1.3.0.41
IP Address        : 10.193.160.16
UP Time           : 0 Day(s) 17 Hour(s) 52 Minute(s)
License Expiry    : Activated through License Server.
System ID         : scspa2578110002

Press any key to continue : █
```

License Configuration

License Configuration includes below menus.

Figure 30)



```
Administrator: Windows PowerShell

***** Global File Cache License Configuration *****

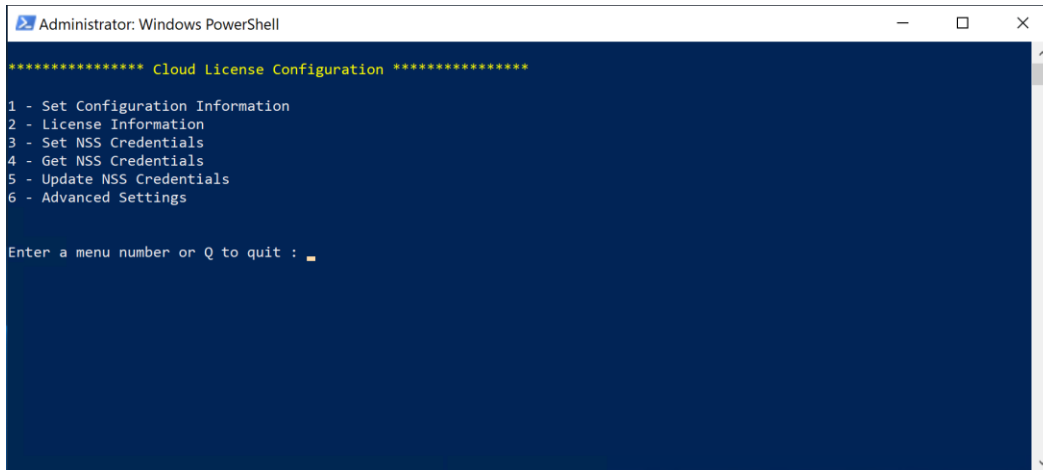
1 - Configure Cloud License
2 - Register Edge/Core to License Manager
3 - Synchronize with License Database

Enter a menu number or Q to quit : █
```

Configure Cloud License

All types of license configuration is performed under this menu context. License configuration is distributed in below sections:

- Setting license configuration information
- Display license information
- Setting NSS information
- Getting NSS information
- Updating NSS information
- Any Advanced settings



```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

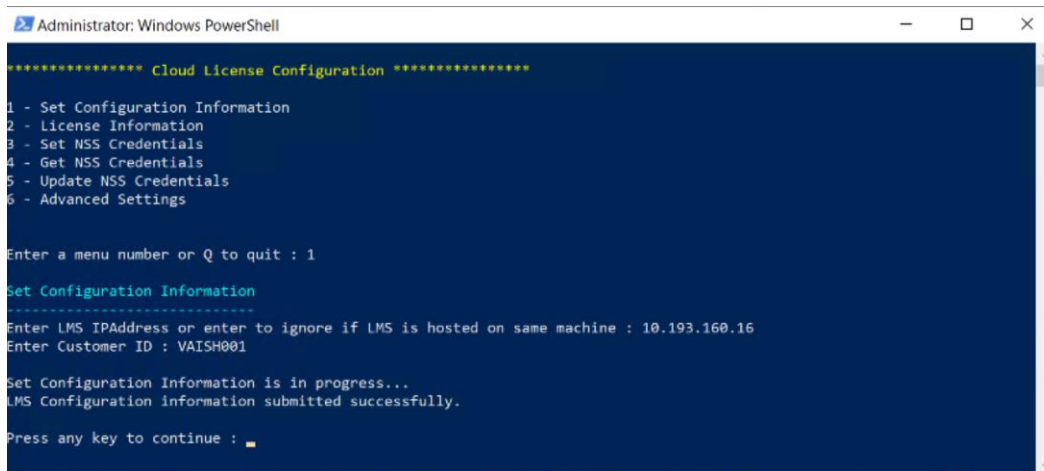
Enter a menu number or Q to quit : 
```

7. Set License configuration information:

a) This step is perform the binding process of LMS with the customer id.

License Server Public IP Address/DSN Name: Provide the FQDN or IP address of the GFC instance that has been deployed as central license manager server, i.e. 1.2.3.4

Customer ID: Provide the customer identifier, as provided by NetApp Support services, to associate this instance with your license manager server.



```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

Enter a menu number or Q to quit : 1

Set Configuration Information
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16
Enter Customer ID : VAISH001

Set Configuration Information is in progress...
LMS Configuration information submitted successfully.

Press any key to continue : 
```

8. Get License information:

Select this menu item for getting the information about the license.

```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

Enter a menu number or Q to quit : 2

License Information
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16

Fetching License Information from LMS is in progress...

CustomerID CustomerName EdgeCount LicenseExpiryDate
-----
VAISH001 VAISH001 0 12/31/9999 5:00:00 AM

Press any key to continue : _
```

9. Set NSS credentials:

If you have received an email with NSS information, you should activate your licenses by supplying your NSS credentials. NSS credentials can be obtained by logging into support.netapp.com and use NSS username and NSS password for licensing configuration.

```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

Enter a menu number or Q to quit : 3

Set NSS Credentials
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16
Enter NSS UserName: test
Enter NSS Password: ****

Setting NSS Credentials is in progress...
```

10. Get NSS credentials:

If NSS Credentials are used for LMS licensing configuration, these credentials can be displayed using “get NSS credentials” options.

```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

Enter a menu number or Q to quit : 4

Get NSS Credentials
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16

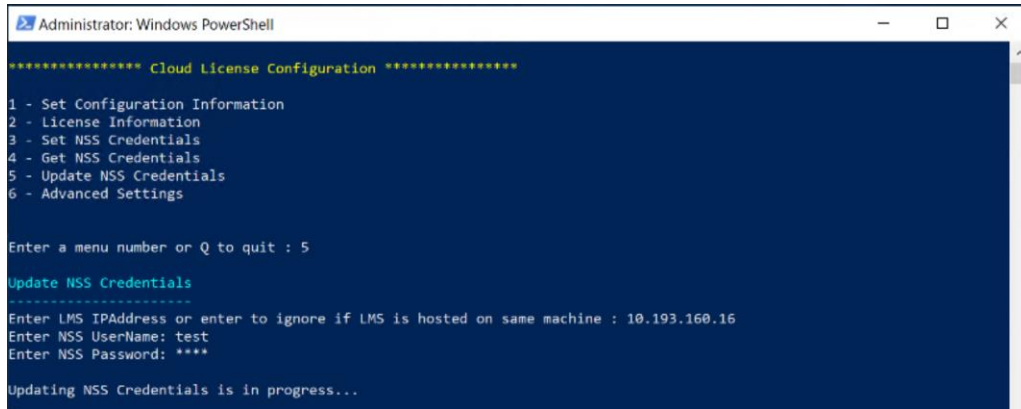
Fetching NSS Credentials is in progress...

username password updateCreds
-----
"" False

Press any key to continue : _
```

11. Update NSS Credentials:

When a NSS credentials are modified/updated in the support.netapp.com, they have to be immediately be updated on the LMS configuration. This will enable LMS service to run seamlessly .



```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

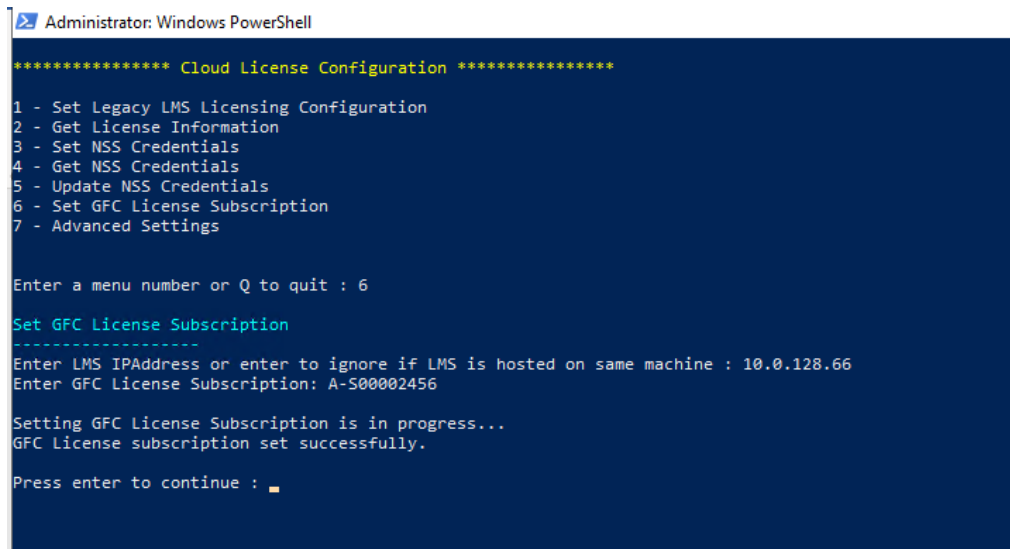
Enter a menu number or Q to quit : 5

Update NSS Credentials
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16
Enter NSS UserName: test
Enter NSS Password: ****

Updating NSS Credentials is in progress...
```

12. Set GFC License Subscription:

When user have GFC subscription number provided by Netapp Team instead of providing NSS credentials he/she can simply activate GFC services by providing that subscription number



```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Legacy LMS Licensing Configuration
2 - Get License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Set GFC License Subscription
7 - Advanced Settings

Enter a menu number or Q to quit : 6

Set GFC License Subscription
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.0.128.66
Enter GFC License Subscription: A-S00002456

Setting GFC License Subscription is in progress...
GFC License subscription set successfully.

Press enter to continue : █
```

13. Advanced settings:

This menu item is used to configure if LMS service connects to NSS/Subscription through an internal proxy.

```
Administrator: Windows PowerShell

***** Cloud License Configuration *****

1 - Set Configuration Information
2 - License Information
3 - Set NSS Credentials
4 - Get NSS Credentials
5 - Update NSS Credentials
6 - Advanced Settings

Enter a menu number or Q to quit : 6

Advanced Settings
-----
Enter LMS IPAddress or enter to ignore if LMS is hosted on same machine : 10.193.160.16
Enter proxy IPAddress : 10.0.1.1

Set Advanced Settings is in progress...

Press any key to continue configuration advanced settings
```

Core Configuration

This menu item is used to configure core instance:

1. Configure service user account
2. Manage Backend File servers
3. Manage legacy pre-population jobs

Figure 31)

```
Administrator: Windows PowerShell

***** Core Configuration *****

1 - Configure Service Account
2 - Manage Backend File Servers
3 - Manage Legacy Pre-Population Jobs

Enter a menu number or Q to quit : 
```

Service Account

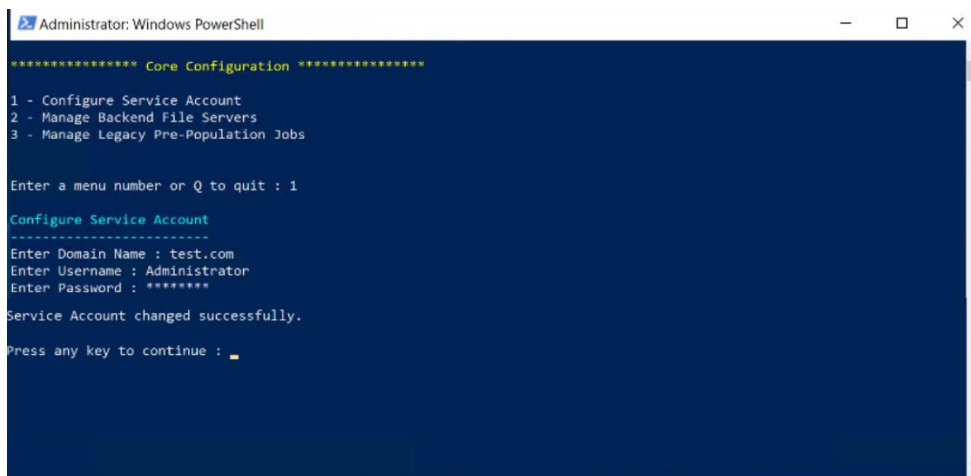
Configure Core instance Service Account with below parameters.

Domain: Provide the domain name information.

Username: Provide the Service Account username that will be used to start the GFC service. Note that this service account must be a member of the local backup operators' group or local administrators' group on the backend file server. See the GFC user guide for further information.

Password: Provide the password for the Service Account.

Figure 32)



```
Administrator: Windows PowerShell

***** Core Configuration *****

1 - Configure Service Account
2 - Manage Backend File Servers
3 - Manage Legacy Pre-Population Jobs

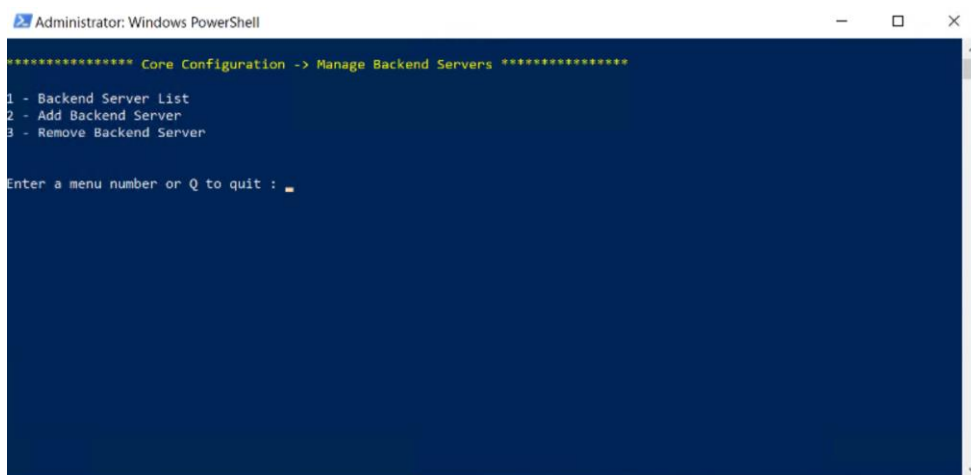
Enter a menu number or Q to quit : 1

Configure Service Account
-----
Enter Domain Name : test.com
Enter Username : Administrator
Enter Password : *****
Service Account changed successfully.
Press any key to continue : _
```

Manage Backend File Servers

Manage Backend File Servers contains the below menu items:

Figure 33)



```
Administrator: Windows PowerShell

***** Core Configuration -> Manage Backend Servers *****

1 - Backend Server List
2 - Add Backend Server
3 - Remove Backend Server

Enter a menu number or Q to quit : _
```

1. Add Backend Server:

```
Administrator: Windows PowerShell

***** Core Configuration -> Add Backend Server *****

1 - Generic SMB
2 - DAS / iSCSI Mount

Enter a menu number or Q to quit : 
```

There are two types of backend servers as listed below:

a. Generic SMB

NetBIOS / FQDN: Provide the NetBIOS name or FQDN of the backend file server, i.e. US-FS1 or US-FS1.CORPORATE.LOCAL

```
Administrator: Windows PowerShell

***** Core Configuration -> Add Backend Server *****

1 - Generic SMB
2 - DAS / iSCSI Mount

Enter a menu number or Q to quit : 1

Backend Server Type - Generic SMB
-----
Enter NetBIOS / FQDN : testserver
Enter Backend UserName(Optional) :
Enter Backend Password(Optional) :

Backend Server added successfully.

Press any key to continue : 
```

b. DAS / iSCSI Mount

Storage Name: Provide the Storage Name which is displayed to end users in the UNC path.

LocalPath: Provide the local path of the attached storage, i.e. F:\

```
Administrator: Windows PowerShell

***** Core Configuration -> Add Backend Server *****

1 - Generic SMB
2 - DAS / iSCSI Mount

Enter a menu number or Q to quit : 2

Backend Server Type - DAS / iSCSI Mount
-----
Enter Storage Name : mflab\local
Enter Local Path : \\mflabfileserver.mflab.local\Test

Backend Server added successfully.

Press any key to continue : _
```

2. Backend Server List:

```
Administrator: Windows PowerShell

***** Core Configuration -> Manage Backend Servers *****

1 - Backend Server List
2 - Add Backend Server
3 - Remove Backend Server

Enter a menu number or Q to quit : 1

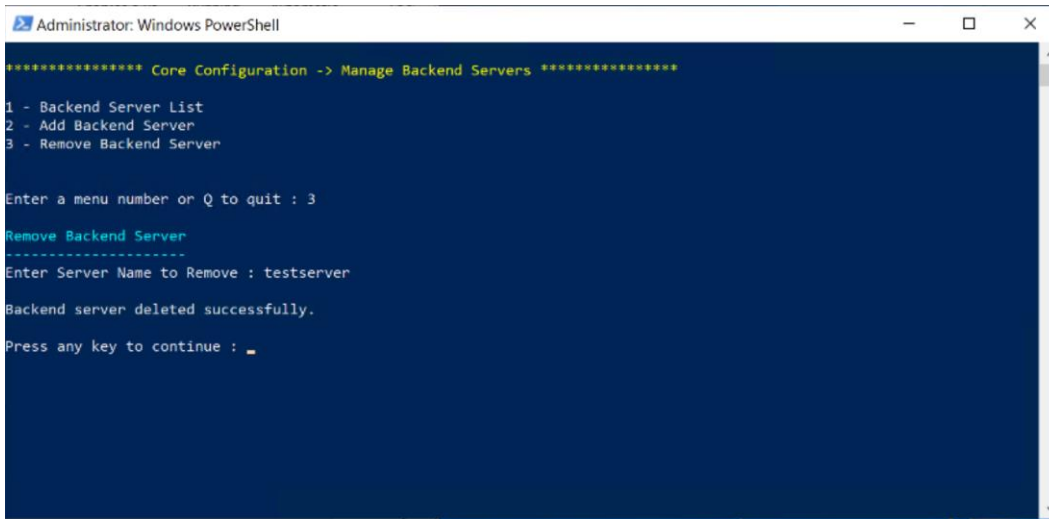
Backend Server List
-----

Server          LocalPath
-----
10.193..160.16
127.0.0.1
mflab
testserver

Press any key to continue : _
```

3. Delete Backend Server:

Enter the name of the backend server to delete from the list.



```
Administrator: Windows PowerShell

***** Core Configuration -> Manage Backend Servers *****

1 - Backend Server List
2 - Add Backend Server
3 - Remove Backend Server

Enter a menu number or Q to quit : 3

Remove Backend Server
-----
Enter Server Name to Remove : testserver

Backend server deleted successfully.

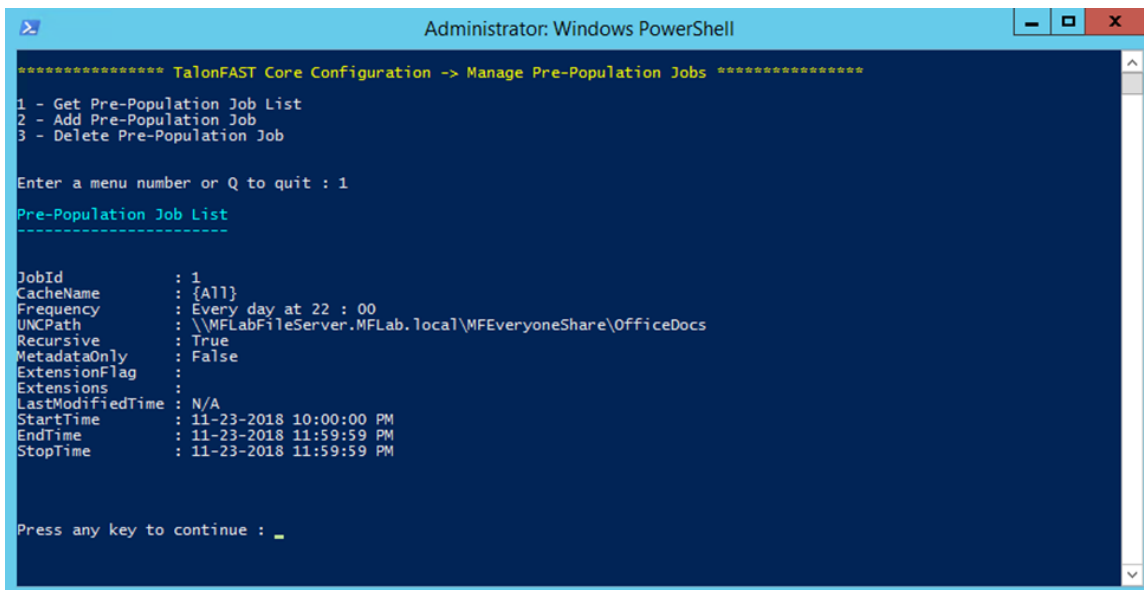
Press any key to continue : _
```

Manage legacy Pre-Population Jobs

Manage Pre-Population contains the below menu items:

1. Get Pre-Population Job List:

Get a list of all pre-population jobs that's have been scheduled to run



```
Administrator: Windows PowerShell

***** TalonFAST Core Configuration -> Manage Pre-Population Jobs *****

1 - Get Pre-Population Job List
2 - Add Pre-Population Job
3 - Delete Pre-Population Job

Enter a menu number or Q to quit : 1

Pre-Population Job List
-----

JobId           : 1
CacheName       : {All}
Frequency       : Every day at 22 : 00
UNCPath        : \\MFLabFileServer.MFLab.local\MFEveryoneShare\OfficeDocs
Recursive       : True
MetadataOnly    : False
ExtensionFlag   :
Extensions      :
LastModifiedTime : N/A
StartTime       : 11-23-2018 10:00:00 PM
EndTime        : 11-23-2018 11:59:59 PM
StopTime        : 11-23-2018 11:59:59 PM

Press any key to continue : _
```

2. Add Pre-Population Job:

Pre-population is divided into 3 components as below:

Path Filter Configuration
Frequency Configuration
Pre-population Job Configuration

Path Filter Configuration

These are filters added on given path, the object is saved and used for adding pre-population job. It has below parameters:

Path: UNC path for pre-population job.

Recursive: This filter includes all the child directories.

MetadataOnly: It will only contain metadata file, not the actual data.

Modified time: This will include file modified after the given time(days/hours/minutes)

FileType: This will include or exclude the files with given extensions.

Frequency Configuration

Specify the frequency of the pre-population Job.

One-time job or repetitive job.

If it's a repetitive job then select the frequency like daily, days interval, day of week, day of month

Specify the time for the repetitive job.

Pre-Population Job Configuration

This is the final execution point where job will be added.

Enter the edge server name where the job is to be executed. Job can be executed for all edge servers as well for that specify "All."

Enter the start time for the job. If the job is repetitive then the execution time given in frequency configuration and the time for the StartTime parameter should be the same.

Enter the stop time for the job.

```
Administrator: Windows PowerShell

***** TalonFAST Core Configuration -> Manage Pre-Population Jobs *****

1 - Get Pre-Population Job List
2 - Add Pre-Population Job
3 - Delete Pre-Population Job

Enter a menu number or Q to quit : 2

Add Pre-Population Job
-----

Path Filter Configuration

Enter UNC Path for Pre-population job: \\MFLabFileServer.MFLab.local\MFEveryoneShare\OfficeDocs
Include child directories and subdirectories (recursive)
Press [y] to include or enter to ignore: y
Include metadata file only,
Press [y] to include or enter to ignore:
Add filter based on modified time?
Press [y] to include or enter to ignore:
Add filter based on file type,
Press [i] to specify include filter, [e] to specify exclude filter or enter to ignore:

Configuration Summary
-----
UNCPath       : \\MFLabFileServer.MFLab.local\MFEveryoneShare\OfficeDocs
Recurse       : True
MetadataOnly  : False
ExcludeExt    :
IncludeExt    :
LastModifiedTime : 00:00:00

Frequency Configuration

Specify the frequency of the pre-population job.
Enter [o] for one time job or [r] for repetitive job: r

Enter [d] for daily job
[i] to specify interval in days (e.g. every 2 days, 3 days etc.)
[w] to specify day of week
[m] to specify day of month: d
Enter the time of execution(HH:mm:ss): 22:00:00

Configuration Summary
-----
Once          : False
Daily         : True
DaysInterval  : 0
DaysOfWeek    :
DayOfMonth    : 0
At            : 22:00:00

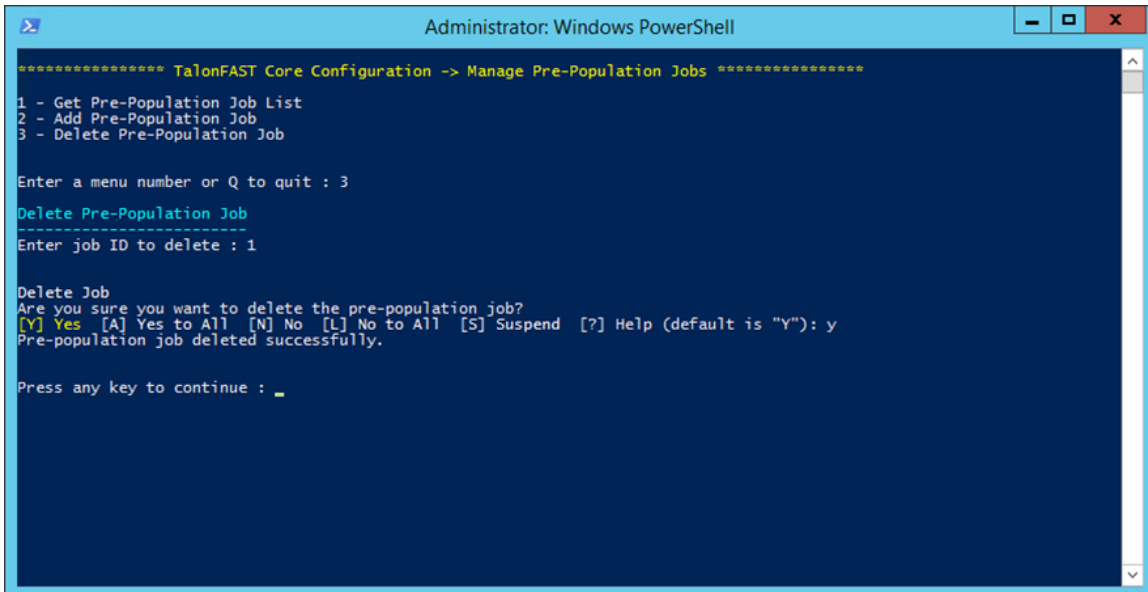
Pre-Population Job Configuration

Enter the Edge Server Name where the job is to be executed. Type [All] to include all edge servers: All
Enter Start Time for Job [mm-dd-yyyy HH:mm:ss]: 11-23-2018 22:00:00
Enter Stop Time for Job [mm-dd-yyyy HH:mm:ss]: 11-23-2018 23:59:59
Pre-population job added successfully.

Press any key to continue : _
```

3. Deleting Pre-Population Job:

JobID: Provide the JobID of the Pre-Population job you are deleting



```
Administrator: Windows PowerShell

***** TalonFAST Core Configuration -> Manage Pre-Population Jobs *****

1 - Get Pre-Population Job List
2 - Add Pre-Population Job
3 - Delete Pre-Population Job

Enter a menu number or Q to quit : 3

Delete Pre-Population Job
-----
Enter job ID to delete : 1

Delete Job
Are you sure you want to delete the pre-population job?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
Pre-population job deleted successfully.

Press any key to continue : _
```

Advanced: Core Pre-population using PowerShell

Note: This PowerShell-based approach can only be executed from a Core instance.

Software Requirements

Windows PowerShell 5.x (Administration / Elevated Permissions)

Windows Management Framework 5.x

GFC

Import GFC PowerShell Cmdlet Module

To import PowerShell cmdlets, enter the following command in the PowerShell window. The PowerShell cmdlet module contains many APIs for GFC configuration, including the cmdlet for **Add-PrePopulation Job**.

```
Import-Module "C:\Program Files\TalonFAST\Bin\OptimusPSM.dll"
```

Using Set-TLNPrePopulationPathFilter Cmdlet

Sets path filters for the pre-population job. This object can be used for multiple job creation.

Set-TLNPrePopulationPathFilter

```
-UNCPATH <String>
[-Recurse<bool>]
[MetadataOnly<bool>]
[-ExtensionFlag <String>]
[-Extensions <String[]>]
[-LastModifiedTime <TimeSpan>]
```

Examples:

1. Set job as Recursive. Add parameter -Recurse

```
Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents"
-Recurse $true
```

2. Set job as MetadataOnly. Add parameter -Metadataonly

```
Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents"
-MetadataOnly $true
```

If the job is only for metadata files then use MetadataOnly parameter. You cannot set ExtensionFlag, Extensions and LastModifiedTime parameters with MetadataOnly. an exception will be displayed.

3. Set job to filter by file types to include files of defined extensions.

```
Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents" -Recurse
$true -ExtensionFlag "1" -Extensions ".txt, .docx, .pptx"
```

4. Set the job that excludes specific file extension values

```
Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents"
-Recurse $true -ExtensionFlag "2" -Extensions ".png, .jpg"
```

Extensions filter can only be used with ExtensionFlag filter.

The value of ExtensionFlag filter can either be "1" or "2" where "1" is used for including and "2" is used for excluding the extensions provided.

5. Only include files modified with the defined timespan.

```
Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents"
-Recurse $true -LastModifiedTime 02:15:00
```

This cmdlet returns an object of PathFilter which will displayed like below:

```
PS C:\Users\Administrator.TSS> Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer\MFEveryoneShare\Documents" -Recurse
$true -ExtensionFlag "1" -Extensions ".txt, .docx, .pptx" -LastModifiedTime 02:15:00

UNCPath      : \\FileServer\MFEveryoneShare\Documents
Recurse      : True
MetadataOnly : False
ExtensionFlag : Include
Extensions   : .txt, .docx, .pptx
LastModifiedTime : 02:15:00
```

Using Set-TLNPrePopulationFrequency Cmdlet

Sets the frequency for the pre-population job. This is the execution schedule for the job. This cmdlet output is mandatory parameter for adding pre-population job. All parameters are basically a type of frequency for execution.

Set-TLNPrePopulationFrequency

```
-JobType<int>  
[-Value<int>]  
[-ExecuteAt<string in format HH:mm:ss>]
```

Examples:

1. To execute job only once i.e. One Time Job

```
Set-TLNPrePopulationFrequency -JobType 0
```

If the job is OneTime job then Value and ExecuteAt parameter is not mandatory.

2. Executing job on Daily Basis.

```
Set-TLNPrePopulationFrequency -JobType 1 -value 1 -ExecuteAt "02:30:00"
```

To execute everyday job, Value and ExecuteAt parameter is required along with JobType parameter. Value can be anything from 1,2,3,4,5,6,10,15, where 1 is every day, 2 is every two days,3 is every 3 days and so on, and ExecuteAt is the time at which the job will execute.

3. Set job on weekly basis.

```
Set- TLNPrePopulationFrequency -JobType 2 -value 1 -ExecuteAt "02:30:00"
```

This job will execute every Sunday at 2:30 AM.

The Value range is 1-7 where 1 is Sunday,2 is Monday and so on.

4. Set job frequency to day of the month.

```
Set- TLNPrePopulationFrequency -JobType 3 -value 21 -ExecuteAt "02:30:00"
```

Above job will be executed on 21st of every month at 2:30 AM.

This cmdlet returns an object of Frequency which will be displayed below:

```
PS C:\Users\Administrator.TSS> Set-TLNPrePopulationFrequency -JobType 1 -Value 1 -ExecuteAt "02:30:00"  
  
JobType Value ExecuteAt  
-----  
1 day 02:30:00
```

Using Add-TLNPrePopulationJob Cmdlet

This is the main cmdlet which creates a new pre-population job.

Add-TLNPrePopulationJob

```
[-AllEdgeServers]
[-EdgeServers <String[]>]
-StartTime <DateTime>
-StopTime <DateTime>
-Filter <PSObject>
-Frequency <PSObject>
```

Examples:

1. To execute job for all edge servers.

```
Add-TLNPrePopulationJob -AllEdgeServers -StartTime "01-11-2018 14:45:00" -StopTime
"01-31-2018 18:00:00" -Filter $objFilter -Frequency $objFrequency
```

This will create a job for all edge servers connected to core. -Filter and -Frequency PSObjects need to pass to this cmdlet which are mandatory parameters.

2. To execute a job on one or more Edge Servers

```
Add-TLNPrePopulationJob -EdgeServers EDGESERVER1, EDGESERVER2, EDGESERVER3 -
StartTime "01-11-2018 14:45:00" -StopTime "01-31-2018 18:00:00" -Filter $objFilter -
Frequency $objFrequency
```

This will create a job on one or more edge servers connected to core.

End-to-end Example of Cmdlet

For Add-PrePopulationJob cmdlet below is the complete example:

```
$objFilter = Set-TLNPrePopulationPathFilter -UNCPath
"\FileServer.local\MFEveryOneShare" -Recurse $true -ExtensionFlag "1" -Extensions
.jpeg, .txt, .docx
$objFrequency = Set-TLNPrePopulationFrequency -JobType 1 -Value 1 -ExecuteAt 14:45
Add-TLNPrePopulationJob -EdgeServers EDGESERVER1, EDGESERVER2 -StartTime "01-11-2018
14:45:00" -StopTime "01-31-2018 18:00:00" -Filter $objFilter -Frequency $objFrequency
```

```

PS C:\Users\Administrator.TSS> Import-Module "C:\Program Files\TalonFAST\Bin\OptimusPSM.dll"
PS C:\Users\Administrator.TSS> $objFilter = Set-TLNPRePopulationPathFilter -UNCPath "\\FileServer.local\MFEveryOneShare"
-Recurse $true -ExtensionFlag "1" -Extensions ".jpeg, .txt, .docx"
PS C:\Users\Administrator.TSS> $objFilter

UNCPath      : \\FileServer.local\MFEveryOneShare
Recurse      : True
MetadataOnly : False
ExtensionFlag : Include
Extensions   : .jpeg, .txt, .docx
LastModifiedTime : 00:00:00

PS C:\Users\Administrator.TSS> $objFrequency = Set-TLNPRePopulationFrequency -JobType 1 -Value 1 -ExecuteAt "14:45:00"
PS C:\Users\Administrator.TSS> $objFrequency

JobType Value ExecuteAt
-----
1 day 14:45:00

PS C:\Users\Administrator.TSS> Add-TLNPRePopulationJob -EdgeServers EDGESERVER1, EDGESERVER2 -StartTime "01-11-2018 14:45:00" -StopTime "01-31-2018 18:00:00" -Filter $objFilter -Frequency $objFrequency
Pre-population job successfully added on LMS.
PS C:\Users\Administrator.TSS>

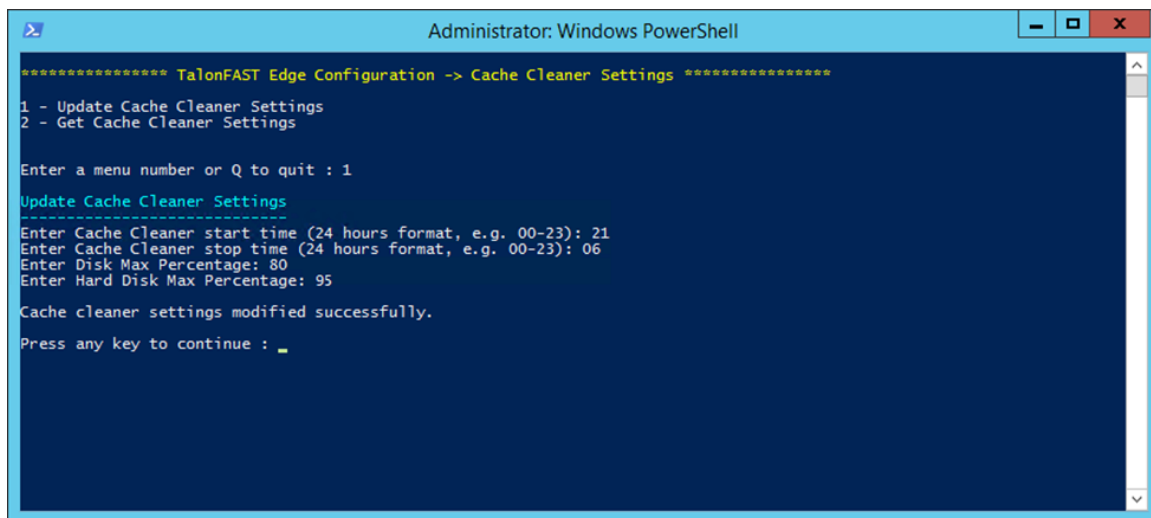
```

Edge Configuration

Cache Cleaner Settings

Includes following configurations settings.

1. Update Cache Cleaner Settings



2. Get Cache Cleaner Settings

```

Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> Cache Cleaner Settings *****
1 - Update Cache Cleaner Settings
2 - Get Cache Cleaner Settings

Enter a menu number or Q to quit : 2

Cache Cleaner Settings
-----
Key                Value
----
CleanerStartHour    21
CleanerStopHour     6
DiskMaxPercentage   80
DiskHardMaxPercentage 95

Press any key to continue : _

```

Throttling Settings

Includes following configuration settings.

1. Get Throttling Settings:

```

Select Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> File Throttling *****
1 - Get Throttling Settings
2 - Update Throttling Settings

Enter a menu number or Q to quit : 1

File Throttling Settings
-----
Key                Value
----
QOSOpenCountMaxStar10 10000
QOSOpenCountRateStar10 100
QOSCreateCountMaxStar10 5000
QOSCreateCountRateStar10 100
QOSWriteByteMaxKB 1048576
QOSWriteByteRateKB 1024
QOSFetchByteMaxKB 1048576
QOSFetchByteRateKB 1024
QOSFlushByteMaxKB 1048576
QOSFlushByteRateKB 1024

```

2. Update throttling settings

```

Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> File Throttling *****
1 - Get Throttling Settings
2 - Update Throttling Settings

Enter a menu number or Q to quit : 2

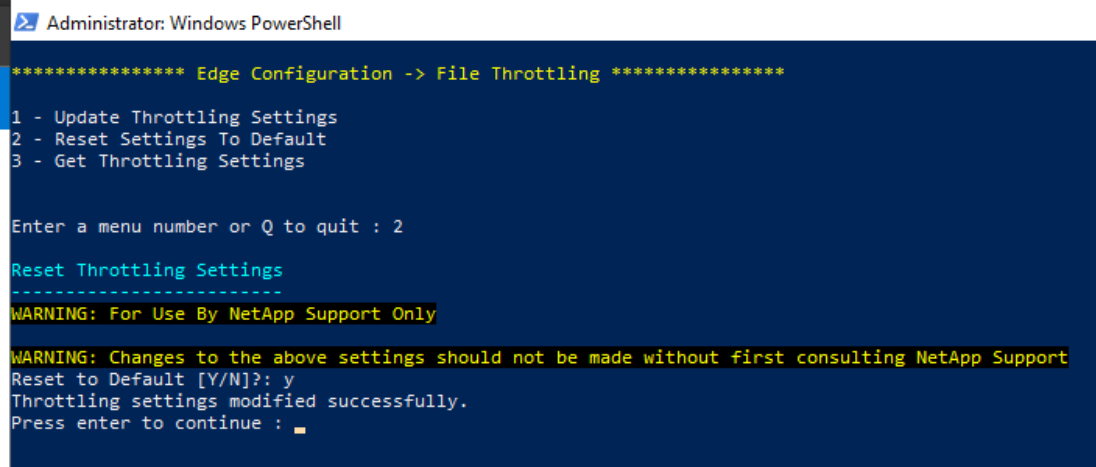
Update Throttling Settings
-----
Enter Max Open Count Rate ( Default 0 ): 0
Enter Open Count Rate ( Default 0 ): 0
Enter Max Create Count ( Default 0 ): 0
Enter Create Count Rate ( Default 0 ): 0
Enter Max Write Byte Rate ( Default 0 ): 0
Enter Write Byte Rate (Default 0 ): 0

Throttling settings modified successfully.

Press any key to continue : _

```

3. Reset throttling settings



```
Administrator: Windows PowerShell

***** Edge Configuration -> File Throttling *****

1 - Update Throttling Settings
2 - Reset Settings To Default
3 - Get Throttling Settings

Enter a menu number or Q to quit : 2

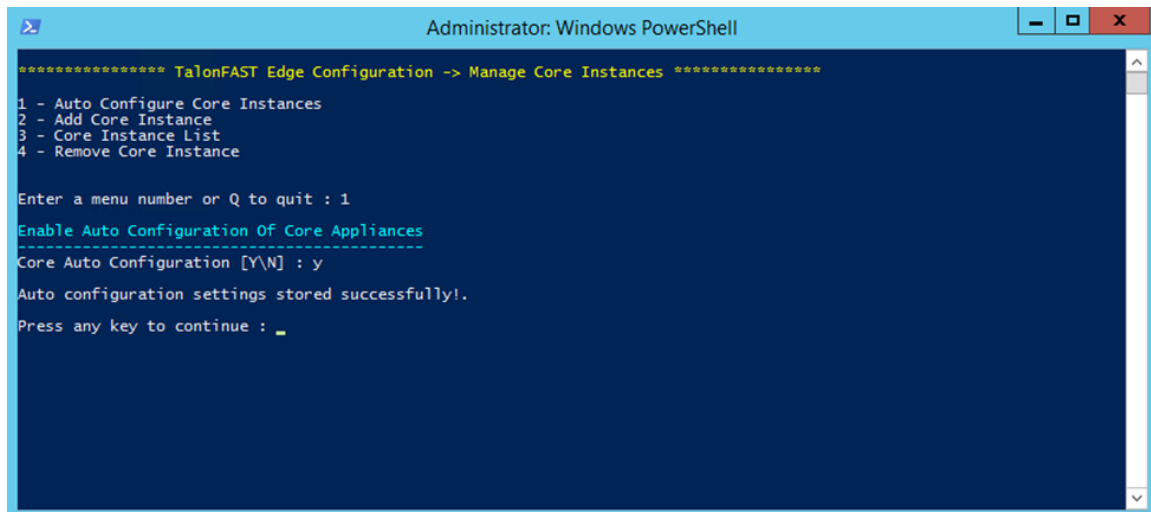
Reset Throttling Settings
-----
WARNING: For Use By NetApp Support Only

WARNING: Changes to the above settings should not be made without first consulting NetApp Support
Reset to Default [Y/N]?: y
Throttling settings modified successfully.
Press enter to continue : _
```

Manage Core Appliances

Manage Core Appliances which includes the below menu items:

1. Auto Configure Core Instances:



```
Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> Manage Core Instances *****

1 - Auto Configure Core Instances
2 - Add Core Instance
3 - Core Instance List
4 - Remove Core Instance

Enter a menu number or Q to quit : 1

Enable Auto Configuration Of Core Appliances
-----
Core Auto Configuration [Y\N] : y

Auto configuration settings stored successfully!.
Press any key to continue : _
```

2. Add Core Instances:

Cloud Fabric ID: Provide the name of the GFC Fabric or datacenter location, i.e. NYC.

FQDN / IP Address: Provide the FQDN or IP Address of GFC Fabric, i.e. 1.2.3.4.

Enabled SSL: This is enabled when GFC edge requires SSL encryption with the GFC, i.e. when using the public internet to connect to the GFC.

Username: Provide designated administrative credentials to enable SSL encryption, preferably the Service Account which authenticates this GFC edge instance with the GFC Fabric, i.e. FASTAdmin.

Password: Provide the password associated with the administrative username supplied to enable SSL encryption between the GFC edge instance and the GFC Fabric.


```
Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> Manage Core Instances *****

1 - Auto Configure Core Instances
2 - Add Core Instance
3 - Core Instance List
4 - Remove Core Instance

Enter a menu number or Q to quit : 2

Add Core Instance
-----
Enter FAST™ Fabric ID of Core : XYZ
Enter FQDN/IP Address of Core : 1.2.3.4
Do you want to activate SSL? [Y/N]: N
[Optional] Enter Username :
[Optional] Enter Password :

Core appliance added successfully.
Press any key to continue : _
```

3. Core Instances List:

```
Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> Manage Core Instances *****

1 - Auto Configure Core Instances
2 - Add Core Instance
3 - Core Instance List
4 - Remove Core Instance

Enter a menu number or Q to quit : 3

Core Instance List
-----

ApplianceID                IPAddress                SSL
-----
NLAMS                      NLAMSTAL02.tss-emea.local 0
XYZINC                     1.2.3.4                  0

Press any key to continue : _
```

4. Remove Core Instances:

```
Administrator: Windows PowerShell

***** TalonFAST Edge Configuration -> Manage Core Instances *****

1 - Auto Configure Core Instances
2 - Add Core Instance
3 - Core Instance List
4 - Remove Core Instance

Enter a menu number or Q to quit : 4

Remove Core Instance
-----
Enter FAST™ Fabric ID of Core : XYZINC

Core appliance removed successfully.
Press any key to continue : _
```

GFC Namespace for TUMMIPProvider

The recently added TUMMIPProvider give customers the ability to manage their GFC infrastructure through a number of PowerShell commands. These have been broken up into the two primary modes of operation for the TUM Service, TUM.exe -s "Server / Core" and TUM.exe -c "Client / Edge". In this section a command and their output examples will be provided for each scenario where these may be utilized.

Note: Prior to utilizing these scripts you should discuss this with the NetApp Support team for the most effective utilization.

TUMMIPProvider is divided into two namespaces as below:

root\TalonMIPProviderv1\Core

root\TalonMIPProviderv1\Edge

To run TUMMIPProvider cmdlets:

For Core instances, ensure the namespace is defined with root\TalonMIPProviderv1\Core

For Edge instances, ensure the namespace is defined with root\TalonMIPProviderv1\Edge

e.g.

GFC Core: Get-WmiObject -Namespace root\TalonMIPProviderv1\Core -Class TLN_TUMSettings

GFC Edge: Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class TLN_TUMSettings

Below is a list of classes within the TUMMIPProvider:

TUM Settings

Lease Manager

DBG Commands

Bulk Statistics

New Bulk Statistics

RPC Statistics

Dirty Files

Active Fetches

Active Flushes

TUM Settings

The TUM Settings provide the ability to view the details of the GFC server that has been provisioned. This can also allow for adjustments to Debug Level on a specific server for advanced troubleshooting.

1. Get instance of TUM Settings

Core Command:

```
Get-WmiObject -Namespace root\TalonMIPProviderv1\Core -Class  
TLN_TUMSettings
```

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class  
TLN_TUMSettings
```

Edge Output Example:

```

Administrator: Windows PowerShell
PS C:\Users\Inicholson> Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings

GENUS           : 2
CLASS           : TLN_TUMSettings
SUPERCLASS      :
DYNASTY         : TLN_TUMSettings
RELPATH         : TLN_TUMSettings.CreationClassName="TLN_TUMSettings"
PROPERTY_COUNT  : 3
DERIVATION      : {}
SERVER         : SAJHBTAL02
NAMESPACE      : root\TalonMIProviderv1\Edge
PATH           : \\SAJHBTAL02\root\TalonMIProviderv1\Edge:TLN_TUMSettings.CreationClassName="TLN_TUMSettings"
CreationClassName : TLN_TUMSettings
DebugLevel       : 0
TUMRole         : client
PSComputerName   : SAJHBTAL02

PS C:\Users\Inicholson>

```

2. Setting the Debug level

Get instance of TLN_TUMSettings and change debug level.

Core Command:

```

$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_TUMSettings
$obj.SetDebugLevel(3)
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_TUMSettings
$obj

```

Edge Command:

```

$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
$obj.SetDebugLevel(3)
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
$obj

```

Edge Output Example:

```

Administrator: Windows PowerShell
PS C:\Users\Inicholson> $obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
PS C:\Users\Inicholson> $obj.SetDebugLevel(3)
PS C:\Users\Inicholson> $obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
PS C:\Users\Inicholson> $obj

GENUS           : 2
CLASS           : TLN_TUMSettings
SUPERCLASS      :
DYNASTY         : TLN_TUMSettings
RELPATH         : TLN_TUMSettings.CreationClassName="TLN_TUMSettings"
PROPERTY_COUNT  : 3
DERIVATION      : {}
SERVER         : SAJHBTAL02
NAMESPACE      : root\TalonMIProviderv1\Edge
PATH           : \\SAJHBTAL02\root\TalonMIProviderv1\Edge:TLN_TUMSettings.CreationClassName="TLN_TUMSettings"
CreationClassName : TLN_TUMSettings
DebugLevel       : 3
TUMRole         : client
PSComputerName   : SAJHBTAL02

PS C:\Users\Inicholson>

```

Lease Manager

The lease manager scripts provide the ability to display the current leases, filter the leases to find specific open leases and revoke the lease from a specific file or set of parameters.

1. Get instance of TLN_LeaseManager

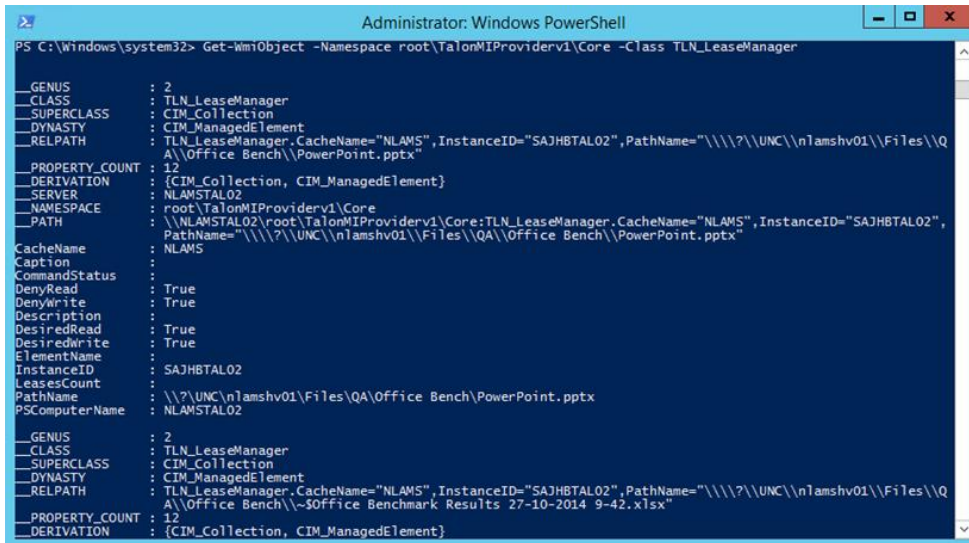
Core Command:

```

Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
TLN_LeaseManager

```

Output:

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the execution of the command: `PS C:\Windows\system32> Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_LeaseManager`. The output displays a list of properties for the `TLN_LeaseManager` class, including `_GENUS`, `_CLASS`, `SUPERCLASS`, `DYNASTY`, `RELPATH`, `PROPERTY_COUNT`, `DERIVATION`, `SERVER`, `NAMESPACE`, `PATH`, `CacheName`, `Caption`, `CommandStatus`, `DenyRead`, `DenyWrite`, `Description`, `DesiredRead`, `DesiredWrite`, `ElementName`, `InstanceID`, `LeasesCount`, `PathName`, and `PSComputerName`. The output is repeated twice, likely due to a scroll or refresh action.

```
PS C:\Windows\system32> Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_LeaseManager

_GENUS           : 2
_CLASS           : TLN_LeaseManager
_SUPERCLASS      : CIM_Collection
_DYNASTY         : CIM_ManagedElement
_RELPATH         : TLN_LeaseManager.CacheName="NLAMS",InstanceID="SAJHBTAL02",PathName="\\\\?\\UNC\\nlamshv01\\Files\\QA\\Office Bench\\PowerPoint.pptx"
_PROPERTY_COUNT  : 12
_DERIVATION      : {CIM_Collection, CIM_ManagedElement}
_SERVER          : NLAMSTAL02
_NAMESPACE       : root\TalonMIProviderv1\Core
_PATH            : \\NLAMSTAL02\root\TalonMIProviderv1\Core:TLN_LeaseManager.CacheName="NLAMS",InstanceID="SAJHBTAL02",
                  PathName="\\\\?\\UNC\\nlamshv01\\Files\\QA\\Office Bench\\PowerPoint.pptx"
CacheName        : NLAMS
Caption          :
CommandStatus    :
DenyRead        : True
DenyWrite       : True
Description      :
DesiredRead      : True
DesiredWrite     : True
ElementName      :
InstanceID       : SAJHBTAL02
LeasesCount      :
PathName         : \\?\\UNC\\nlamshv01\\Files\\QA\\Office Bench\\PowerPoint.pptx
PSComputerName   : NLAMSTAL02

_GENUS           : 2
_CLASS           : TLN_LeaseManager
_SUPERCLASS      : CIM_Collection
_DYNASTY         : CIM_ManagedElement
_RELPATH         : TLN_LeaseManager.CacheName="NLAMS",InstanceID="SAJHBTAL02",PathName="\\\\?\\UNC\\nlamshv01\\Files\\QA\\Office Bench\\PowerPoint.pptx"
_PROPERTY_COUNT  : 12
_DERIVATION      : {CIM_Collection, CIM_ManagedElement}
```

2. Filter instances of Lease Manager

Filtering the leases will give you the ability to identify a specific file that may be required to be unlocked.

The filter can be defined with any of the properties related to the leased file these properties are as follows:

CacheName, Caption, CommandStatus, DenyRead, DenyWrite, Description, DesiredRead, DesiredWrite, ElementName, InstanceID, LeaseCount, PathName, PSComputerName.

Replace `'\'` with `\\` while filtering with pathname.

Core Command:

```
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
TLN_LeaseManager -Filter {InstanceID="SAJHBTAL01"}
$obj
```

Output

```

Administrator: Windows PowerShell

PS C:\Windows\system32> $obj = Get-WmiObject -Namespace root\TalonMIPProviderv1\Core -Class TLN_LeaseManager -Filter {InstanceID="SAJHBTAL01"}
PS C:\Windows\system32> $obj

GENUS           : 2
CLASS           : TLN_LeaseManager
SUPERCLASS      : CIM_Collection
DYNASTY         : CIM_ManagedElement
RELPATH         : TLN_LeaseManager.CacheName="NLAMS", InstanceID="SAJHBTAL01", PathName="\\\\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\~$Office Benchmark Results NJtoNL.xlsx"
PROPERTY_COUNT  : 12
DERIVATION      : {CIM_Collection, CIM_ManagedElement}
SERVER          : NLAAMSTAL02
NAMESPACE       : root\TalonMIPProviderv1\Core
PATH            : \\NLAAMSTAL02\root\TalonMIPProviderv1\Core:TLN_LeaseManager.CacheName="NLAMS", InstanceID="SAJHBTAL01", PathName="\\\\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\~$Office Benchmark Results NJtoNL.xlsx"
CacheName       : NLAMS
Caption         :
CommandStatus   :
DenyRead        : True
DenyWrite       : True
Description     :
DesiredRead     : True
DesiredWrite    : True
ElementName     :
InstanceID      : SAJHBTAL01
LeasesCount     :
PathName        : \\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\~$Office Benchmark Results NJtoNL.xlsx
PSComputerName  : NLAAMSTAL02

GENUS           : 2
CLASS           : TLN_LeaseManager
SUPERCLASS      : CIM_Collection
DYNASTY         : CIM_ManagedElement
RELPATH         : TLN_LeaseManager.CacheName="NLAMS", InstanceID="SAJHBTAL01", PathName="\\\\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\Office Benchmark Results NJtoNL.xlsx"
PROPERTY_COUNT  : 12
DERIVATION      : {CIM_Collection, CIM_ManagedElement}
SERVER          : NLAAMSTAL02
NAMESPACE       : root\TalonMIPProviderv1\Core
PATH            : \\NLAAMSTAL02\root\TalonMIPProviderv1\Core:TLN_LeaseManager.CacheName="NLAMS", InstanceID="SAJHBTAL01", PathName="\\\\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\Office Benchmark Results NJtoNL.xlsx"
CacheName       : NLAMS
Caption         :
CommandStatus   :
DenyRead        : True
DenyWrite       : True
Description     :
DesiredRead     : True
DesiredWrite    : True
ElementName     :
InstanceID      : SAJHBTAL01
LeasesCount     :
PathName        : \\?\\UNC\\n\\amshv01\\Files\\QA\\Office Bench\\Office Benchmark Results NJtoNL.xlsx
PSComputerName  : NLAAMSTAL02

PS C:\Windows\system32>

```

3. Deleting lease. Follow steps from step (2) and run below command.

Core Command:

```
$obj.Delete()
```

Output

```

Administrator: Windows PowerShell

PS C:\Windows\system32> $obj.Delete()
PS C:\Windows\system32> $obj = Get-WmiObject -Namespace root\TalonMIPProviderv1\Core -Class TLN_LeaseManager -Filter{InstanceID="SAJHBTAL01"}
PS C:\Windows\system32> $obj
PS C:\Windows\system32>

```

DBG Commands

The DBG Commands provides the ability to manually clear the cache based on the Least Recently Used (LRU) algorithm to clear up between 25% and 75% of the available disk space. It can also provide the

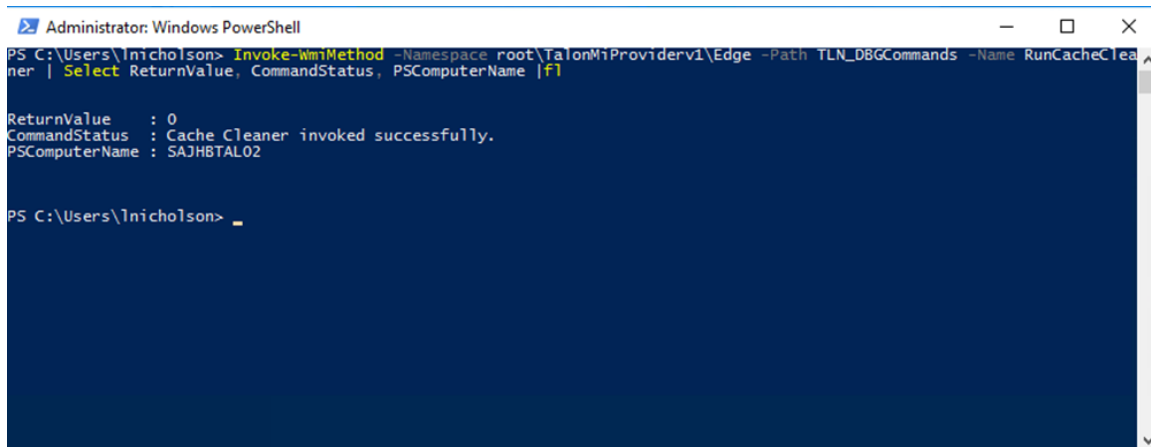
functionality to turn Toggle Event Profiling, Toggle Policy Engine Support and Toggle Light Weight Directory Support ON/OFF as required.

1. Run Cache Cleaner

Edge Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path  
TLN_DBGCommands -Name RunCacheCleaner | Select ReturnValue, CommandStatus,  
PSComputerName | fl
```

Output



```
Administrator: Windows PowerShell  
PS C:\Users\lnicholson> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path TLN_DBGCommands -Name RunCacheCleaner | Select ReturnValue, CommandStatus, PSComputerName | fl  
  
ReturnValue      : 0  
CommandStatus    : Cache Cleaner invoked successfully.  
PSComputerName   : SAJHB TAL02  
  
PS C:\Users\lnicholson> _
```

2. Toggle Event Profiling

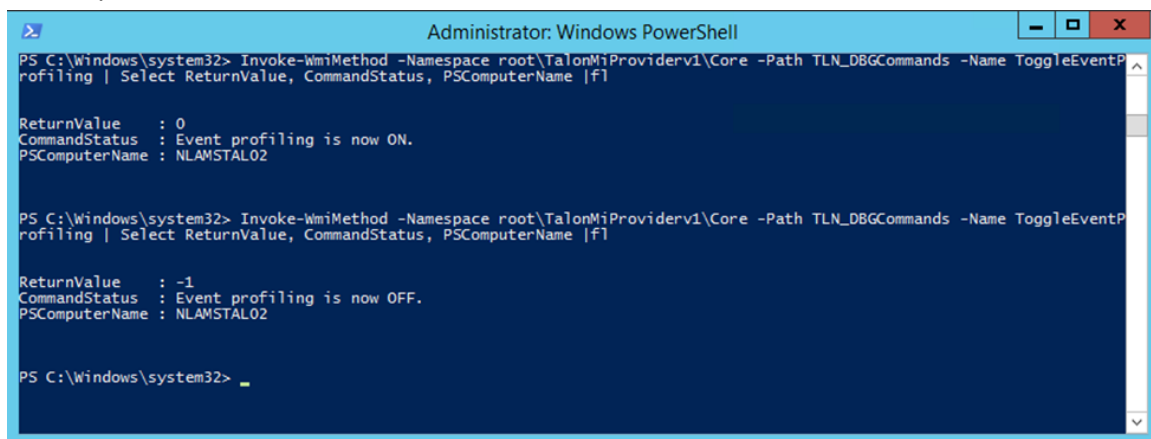
Core Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path  
TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue,  
CommandStatus, PSComputerName | fl
```

Edge Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path  
TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue,  
CommandStatus, PSComputerName | fl
```

Output



```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue, CommandStatus, PSComputerName | fl  
  
ReturnValue      : 0  
CommandStatus    : Event profiling is now ON.  
PSComputerName   : NLAMSTAL02  
  
PS C:\Windows\system32> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue, CommandStatus, PSComputerName | fl  
  
ReturnValue      : -1  
CommandStatus    : Event profiling is now OFF.  
PSComputerName   : NLAMSTAL02  
  
PS C:\Windows\system32> _
```

3. Toggle Policy Engine Support

Edge Command:


```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
TLN_DBGCommands -Name TogglePolicyEngineSupport | Select ReturnValue,
CommandStatus, PSComputerName | fl
```

Output:

```
Administrator: Windows PowerShell

PS C:\Users\lnicholson> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path TLN_DBGCommands -Name TogglePolicyEngineSupport | Select ReturnValue, CommandStatus, PSComputerName | fl

ReturnValue      : -1
CommandStatus    : Policy Engine support is now OFF.
PSComputerName   : SAJHBTAL02

PS C:\Users\lnicholson> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path TLN_DBGCommands -Name TogglePolicyEngineSupport | Select ReturnValue, CommandStatus, PSComputerName | fl

ReturnValue      : 0
CommandStatus    : Policy Engine support is now ON.
PSComputerName   : SAJHBTAL02

PS C:\Users\lnicholson> _
```

4. Toggle Light Weight Directory Support

Edge Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
TLN_DBGCommands -Name ToggleLightWeightDirectorySupport | Select
ReturnValue, CommandStatus, PSComputerName | fl
```

Output:

```
Administrator: Windows PowerShell

PS C:\Users\lnicholson> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path TLN_DBGCommands -Name ToggleLightWeightDirectorySupport | Select ReturnValue, CommandStatus, PSComputerName | fl

ReturnValue      : -1
CommandStatus    : Lightweight directory refresh support is now OFF.
PSComputerName   : SAJHBTAL02

PS C:\Users\lnicholson> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path TLN_DBGCommands -Name ToggleLightWeightDirectorySupport | Select ReturnValue, CommandStatus, PSComputerName | fl

ReturnValue      : 0
CommandStatus    : Lightweight directory refresh support is now ON.
PSComputerName   : SAJHBTAL02

PS C:\Users\lnicholson> _
```

Bulk Statistics

The Bulk Statistics provides you with the ability to read all the statics related to the compression, streaming and delta differencing with an overall transfer efficiency percentage, this can be run from a Core or an Edge.

1. Display Bulk Statistics

Core Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
TLN_BulkStatistics
```

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class
TLN_BulkStatistics
```

Edge Output:

```
Administrator: Windows PowerShell
PS C:\Users\Inicholson> Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_BulkStatistics

__GENUS           : 2
__CLASS           : TLN_BulkStatistics
__SUPERCLASS      : 
__DYNASTY         : TLN_BulkStatistics
__RELPATH         : TLN_BulkStatistics.CreationClassName="TLN_BulkStatistics"
__PROPERTY_COUNT  : 14
__DERIVATION      : {}
__SERVER         : SAJHBTAL02
__NAMESPACE       : root\TalonMIProviderv1\Edge
__PATH            : \\SAJHBTAL02\root\TalonMIProviderv1\Edge:TLN_BulkStatistics.CreationClassName="TLN_BulkStatistics"
CompressionEfficiencyReceived : 0
CompressionEfficiencySend    : 0
CreationClassName           : TLN_BulkStatistics
DifferencingEfficiencyReceived : 99,6856522715366
DifferencingEfficiencySend   : 100
DiskBytesRead               : 2151489
DiskBytesWrite              : 13361
FileBytesSent               : 54050798
NetBytesRead                : 57
NetBytesWrite               : 6365012
OverallTransferEfficiencyReceived : 99,5733852256568
OverallTransferEfficiencySend   : 0
RealBytesRead               : 42
RealBytesWrite              : 0
PSComputerName              : SAJHBTAL02

PS C:\Users\Inicholson>
```

New Bulk Statistics

The new bulk statistics provide you with the latest results related to the server for viewing which can be reset giving the ability to actively monitor a specific instance in real time.

1. Display New Bulk Statistics

Core Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_NewBulkStatistics
```

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_NewBulkStatistics
```

Core Output:

```
Administrator: Windows PowerShell
PSComputerName      : NLAHSTAL02

PS C:\Windows\system32> Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_NewBulkStatistics

__GENUS           : 2
__CLASS           : TLN_NewBulkStatistics
__SUPERCLASS      : 
__DYNASTY         : TLN_NewBulkStatistics
__RELPATH         : TLN_NewBulkStatistics.CreationClassName="TLN_NewBulkStatistics"
__PROPERTY_COUNT  : 12
__DERIVATION      : {}
__SERVER         : NLAHSTAL02
__NAMESPACE       : root\TalonMIProviderv1\Core
__PATH            : \\NLAHSTAL02\root\TalonMIProviderv1\Core:TLN_NewBulkStatistics.CreationClassName="TLN_NewBulkStatistics"
Bandwidth         : 0
CreationClassName : TLN_NewBulkStatistics
InputBlockedTime  : 0
InputFileReadCount : 2
InputFileReadTotal : 31
JobIterTotalTime  : 0
Md4Time           : 0
OutFileReadCount  : 0
OutFileReadTotal  : 0
Received          : 582
SocketRecvTotalTime : 0
SocketSendTotalTime : 0
PSComputerName    : NLAHSTAL02

PS C:\Windows\system32>
```

2. Reset New Bulk Statistics

Core Command:


```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path
TLN_NewBulkStatistics -Name ResetStat
```

Edge Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
TLN_NewBulkStatistics -Name ResetStat
```

Core Output:

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path TLN_NewBulkStatistics -Name ResetStat

__GENUS           : 1
__CLASS           : __PARAMETERS
__SUPERCLASS      : 
__DYNASTY         : __PARAMETERS
__RELPATH         : __PARAMETERS
__PROPERTY_COUNT  : 1
__DERIVATION      : {}
__SERVER          : NLAMSTAL02
__NAMESPACE       : ROOT\TalonMIProviderv1\Core
__PATH            : \\NLAMSTAL02\ROOT\TalonMIProviderv1\Core:__PARAMETERS
ReturnValue       : True
PSComputerName    : NLAMSTAL02

PS C:\Windows\system32>
```

3. Rerun “Display New Bulk Statistics” as per page 178:

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_NewBulkStatistics

__GENUS           : 2
__CLASS           : TLN_NewBulkStatistics
__SUPERCLASS      : 
__DYNASTY         : TLN_NewBulkStatistics
__RELPATH         : TLN_NewBulkStatistics.CreationClassName="TLN_NewBulkStatistics"
__PROPERTY_COUNT  : 12
__DERIVATION      : {}
__SERVER          : NLAMSTAL02
__NAMESPACE       : root\TalonMIProviderv1\Core
__PATH            : \\NLAMSTAL02\root\TalonMIProviderv1\Core:TLN_NewBulkStatistics.CreationClassName="TLN_NewBulkStatistics"
Bandwidth         : 0
CreationClassName : TLN_NewBulkStatistics
InputBlockedTime  : 0
InputFileReadCount : 0
InputFileReadTotal : 0
JobIterTotalTime  : 0
MtdTime           : 0
OutFileReadCount  : 0
OutFileReadTotal  : 0
Received          : 0
SocketRecvTotalTime : 0
SocketSendTotalTime : 0
PSComputerName    : NLAMSTAL02

PS C:\Windows\system32>
```

RPC Statistics

The RPC statistics provide you with information related to the GFC Fabric on a specific machine. It gives the time in milliseconds, counts, and Average number of retries for specific RPC protocols utilized.

1. Display RPC Statistics

Core Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_RPCStatistics
| Select RPCName, @{Name="Time (ms)";Expression="{0:N2}" -f($_.Time)}},
Count, @{Name="AvgRetries";Expression="{0:N2}" -f($_.AvgRetries)}
```

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_RPCStatistics
| Select RPCName, @{Name="Time (ms)";Expression="{0:N2}" -f($_.Time)}},
Count, @{Name="AvgRetries";Expression="{0:N2}" -f($_.AvgRetries)}
```

Edge Output:

```

PS C:\Users\Inicholson> Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class TLN_RPCStatistics | Select RPCName, Time(ms), Count, AvgRetries
RPCName      Time(ms) Count AvgRetries
-----
create_rpc_client 141,00      1 0,00
drop_release_rpc_client 134,76    380 0,00
lookup_rpc_client 109,50      2 0,00
get_release_rpc_client 126,06    384 0,00
move_bulk_rpc_client 126,17    196 0,00
ping_rpc_client 100,17   13064 0,00
set_attr_rpc_client 109,00      1 0,00
read_dir_plus2_rpc_client 603,62    121 0,00
write_rpc_client 328,00      1 0,00
auth_neg_rpc_client 111,50      8 0,00
get_policy_rpc_client 110,60     93 0,00

```

Dirty Files

The command gives you the ability to view any files that are currently in the Dirty Files DB.

Display Dirty Files

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class TLN_DirtyFiles |
Select FileID, FilePath
```

Edge Output:

Figure 34)

```

PS C:\Users\Inicholson> Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class TLN_DirtyFiles | Select FileID, FilePath
FileID      FilePath
-----
52:10000    \NLAMSLU\NLAMSLU-2\Data\Company Data\OfficeBench46\Excel\A_FY06 EPG Change Inventory Listv2.xls
54:10000    \NLAMSLU\NLAMSLU-2\Data\Company Data\OfficeBench46\Excel\Dashboard - June 2016.xls
72:190000   \NLAMSLU\NLAMSLU-2\Data\Company Data\OfficeBench46\Word\SharePoint Examples.docx
71:220000   \NLAMSLU\NLAMSLU-2\Data\Company Data\OfficeBench46\Office Benchmark Results 27-8-2018 11-6-27.xlsx
9D:20000    \NLAMS\lamshv01\Files\QA\OfficeBench474\Excel\A_FY06 EPG Change Inventory Listv2.xls
9E:20000    \NLAMS\lamshv01\Files\QA\OfficeBench474\Excel\Dashboard - June 2016.xls
ED:80000    \NLAMS\lamshv01\Files\QA\OfficeBench474\PowerPoint\200.YYL - K2 smartforms - Intermediate.pptx-temp.pptx
EE:20000    \NLAMS\lamshv01\Files\QA\OfficeBench474\PowerPoint\100.YYZ - K2 smartforms - Fundamentals.pptx-temp.pptx
EA:350000   \NLAMS\lamshv01\Files\QA\OfficeBench474\Office Benchmark Results 15-11-2018 12-7-42.xlsx
E9:3D0000   \NLAMS\lamshv01\Files\QA\OfficeBench474\Office Benchmark Results 15-11-2018 12-7-42.xlsx

```

Active Fetches

Provides you with the ability to check for any current Fetches within the GFC Fabric.

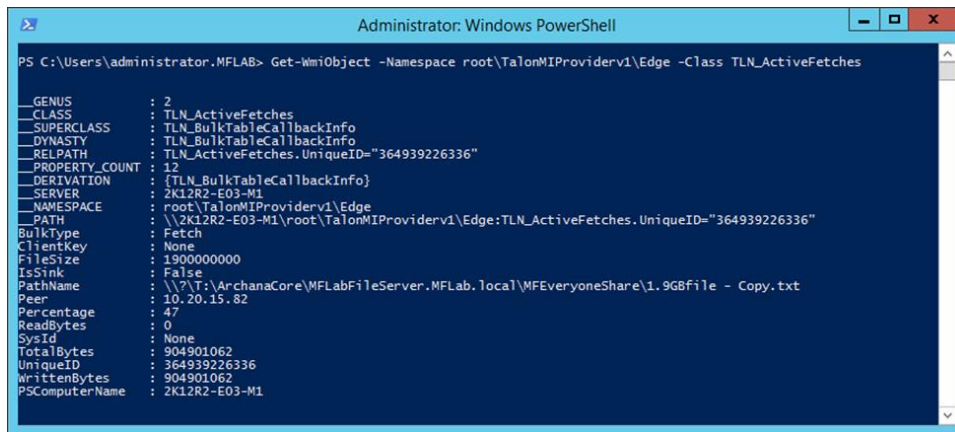
Display Active Fetches

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIPProviderv1\Edge -Class
TLN_ActiveFetches
```

Edge Output:

Figure 35)



```
Administrator: Windows PowerShell
PS C:\Users\administrator.MFLAB> Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_ActiveFetches

GENUS           : 2
CLASS           : TLN_ActiveFetches
SUPERCLASS      : TLN_BulkTableCallbackInfo
DYNASTY         : TLN_BulkTableCallbackInfo
RELPATH         : TLN_ActiveFetches.UniqueID="364939226336"
PROPERTY_COUNT  : 12
DERIVATION      : {TLN_BulkTableCallbackInfo}
SERVER         : 2K12R2-E03-M1
NAMESPACE      : root\TalonMIProviderv1\Edge
PATH           : \\2K12R2-E03-M1\root\TalonMIProviderv1\Edge:TLN_ActiveFetches.UniqueID="364939226336"
BulkType        : Fetch
ClientKey       : None
FileSize        : 1900000000
IsSink          : False
PathName        : \\?\T:\ArchanaCore\MFLabFileServer.MFLab.local\MFEveryoneShare\1.9GBFile - Copy.txt
Peer            : 10.20.15.82
Percentage      : 47
ReadBytes       : 0
SysId           : None
TotalBytes      : 904901062
UniqueID        : 364939226336
WrittenBytes     : 904901062
PSComputerName  : 2K12R2-E03-M1
```

Active Flushes

Provides you with the ability to check for any current Flushes within the GFC Fabric.

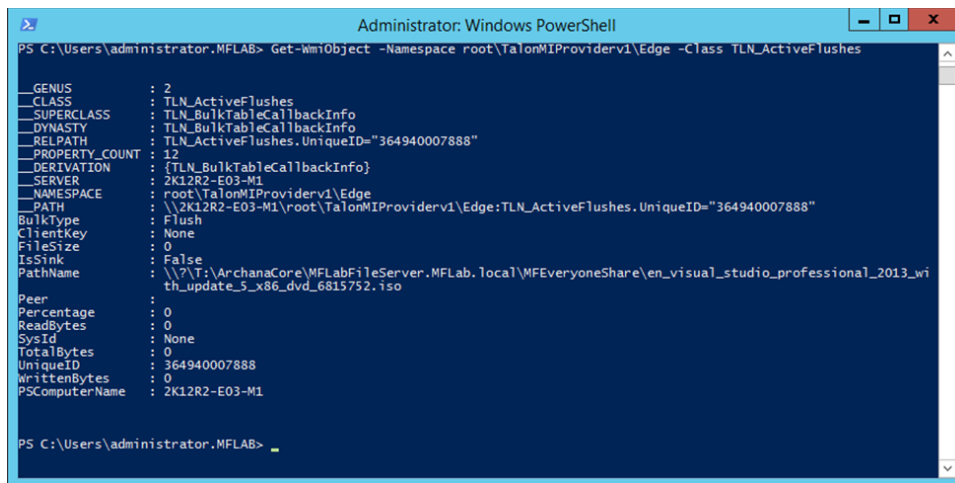
Display Active Flushes

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_ActiveFlushes
```

Edge Output:

Figure 36)



```
Administrator: Windows PowerShell
PS C:\Users\administrator.MFLAB> Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_ActiveFlushes

GENUS           : 2
CLASS           : TLN_ActiveFlushes
SUPERCLASS      : TLN_BulkTableCallbackInfo
DYNASTY         : TLN_BulkTableCallbackInfo
RELPATH         : TLN_ActiveFlushes.UniqueID="364940007888"
PROPERTY_COUNT  : 12
DERIVATION      : {TLN_BulkTableCallbackInfo}
SERVER         : 2K12R2-E03-M1
NAMESPACE      : root\TalonMIProviderv1\Edge
PATH           : \\2K12R2-E03-M1\root\TalonMIProviderv1\Edge:TLN_ActiveFlushes.UniqueID="364940007888"
BulkType        : Flush
ClientKey       : None
FileSize        : 0
IsSink          : False
PathName        : \\?\T:\ArchanaCore\MFLabFileServer.MFLab.local\MFEveryoneShare\en_visual_studio_professional_2013_wi
th_update_5_x86_dvd_6815752.iso
Peer            :
Percentage      : 0
ReadBytes       : 0
SysId           : None
TotalBytes      : 0
UniqueID        : 364940007888
WrittenBytes     : 0
PSComputerName  : 2K12R2-E03-M1

PS C:\Users\administrator.MFLAB> _
```

Appendix D: NetApp Global File Cache Event ID / Logging / 3rd Party Monitoring

NetApp Global File Cache Event IDs

NetApp Global File Cache (GFC) provides enhanced logging of system state, events and errors/warning associated with the solution deployment. The following events are logged in the Microsoft Windows Event Viewer as well as in the GFC log files as stored in

C:\Program Files\TalonFAST\FASTDebuglogs\<folder on each Core or Edge instance>.

Below Table 1 you can find the most common events to monitor, event ID, description and severity.

Table 1)

Event ID	Event	Description	Severity
262	Error on Connection to <IP address>	Indicator that network connectivity may have been briefly impacted between Edge and Core. The connections will re-establish automatically	Warning
274 (Core)	Connection from <Edge><EdgeIP> successfully established	Connections from Edge to the Core have been established successfully.	Information
274 (Edge)	Connections established and authenticate with <Core>	Connections between Edge and Core have been established successfully.	Information
280	From/To Datacenter (Gathered-Write)	Informational message that data is being read fetched from or flushed to the Datacenter. This will be visible from the Edge and from the Core	Information
285	Site key validated for all connections to <Core>. Transitioning to CONNECTED mode.	WAN disconnection resolved, Edge and Core are communicating as normal.	Information
287	Unable to get address for <core>: error 11001 (No such host is known)	Indicates a DNS error where Core cannot be resolved. 347 – Transitioning to DISRUPTED mode for <Core> Indicates a dropped or lost connecting to the Core. Potentially a WAN error or outage. This should be followed by ID 285.	Error
3328	Talon PrePopulation started at <Time> on <Date> with max_threads 15	Indicates the start time and date of a pre-population with the default thread count of 15.	Information
3329	Job is picked up for execution <BackendFS> (Edge)	Indicates a new Pre-population job has been picked up for execution on the Edge	Information
3329	Job has been completed <BackendFS> (Edge)	Indicates that a Pre-population job has started and completed	Information

Event ID	Event	Description	Severity
282	Cache Cleaner process is initiated	Automated purging mechanism is engaged. Indicated cache has reached 85% capacity. May adjust D:\ accordingly if desired	

GFC Logging

GFC log files are stored in C:\Program Files \TalonFAST\FASTDebugLogs\

The Logs are rotated every 8 Hours or every 1MB, keeping total of 72 hours.

The “Core” and “Edge” directories house logs associated with Core and Edge activity:

FAST File Transfer Logs

FAST Messages Logs

FAST Statistics Logs

Pre-Population Logs

Core-Internal and Edge-Internal Directories

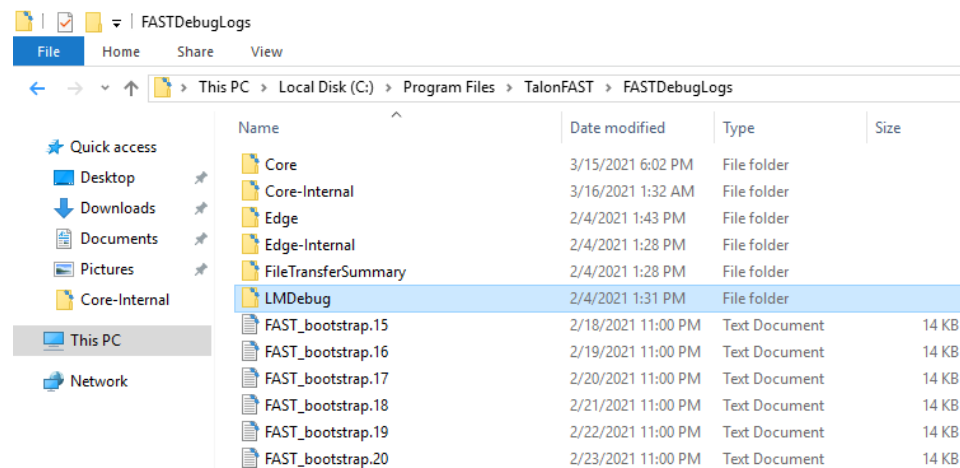
These directories house Engineering level logs

Logs in these directories may be requested from NetApp Support for troubleshooting purposes

LMDebug Directory

This directory houses Engineering logs for LMServer Service and LMClient service

Figure 37)



The content contained in the Log Files can be identified in the Table 2 below.

Table 2)

Log File	Description
File Transfer Log (Core and Edge) FAST_File_Transfer.txt	Logs individual file transfer activity Date and Path

Log File	Description
	File Size / Bytes Transferred / Bytes Exchanged / Transfer Efficiency
FAST Statistics Log (Core) FAST_Stats.txt	Logs Server-Side Statistics File Statistics Compression / Differencing Efficiencies Current File Leases
FAST Statistics Log (Edge) FAST_Stats.txt	Logs Client-Side Statistics Connected Core information Compression / Differencing Efficiencies
Messages Log FAST_Messages.txt	Logs system messages / error conditions
Pre-Population Log (Edge only) Tapp.txt	Logs start and end times of pre-population jobs Displays individual files / folders transferred

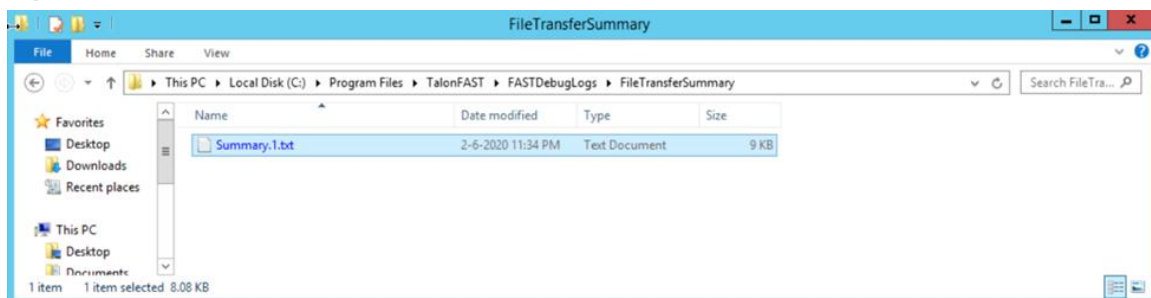
GFC File Transfer Summary Logging

Additional logging has been introduced to capture file activity, which can provide for optimized reporting purposes and analysis using any 3rd party log parsing tool.

The log file is automatically generated on the GFC core instance and can be found in the following location:

C:\Program Files\TalonFAST\FASTDebugLogs\FileTransferSummary\

Figure 38)



The log file contains a breakdown of the file type, direction (fetch / flush), backend file server hosting the source file storage, the backend file-share, the GFC edge instance that has been requesting the file(s), a count of the amount of files fetched or flushed over the WAN, the minimum and maximum file sizes, average file size and the average transfer efficiency. All statistics are aggregated in bytes traversing the WAN and

Figure 39)

FileType	Direction	Backend	Share	Edge	Count	MinSize	MaxSize	AvgSize	AvgTransEff
.xlsx	FLUSH	nlamshv01	Files	10.0.30.21	839	0	48654540	2227838.13	2367478.65
.docx	FLUSH	nlamshv01	Files	10.0.30.21	815	0	41921280	375460.55	397055.05
.doc	FLUSH	nlamshv01	Files	10.0.30.21	139	0	0	0	170.51
.tmp	FLUSH	nlamshv01	Files	10.0.30.21	118	0	3573766	206195.2	317879.6
.docx	FETCH	nlamshv01	Files	10.0.30.21	36	11549	731858	257751.86	1204.06
.DOC	FLUSH	nlamshv01	Files	10.0.30.21	50	0	0	0	173
.xls	FLUSH	nlamshv01	Files	10.0.30.21	101	55296	2642944	1361930.14	17246.64
.xls	FETCH	nlamshv01	Files	10.0.30.21	1	2100224	2100224	2100224	4189
.pptx	FLUSH	nlamshv01	Files	10.0.30.21	1010	0	3573772	175042.19	219181.81
.pptx	FETCH	nlamshv01	Files	10.0.30.21	64	408151	3573772	2945554.09	5840.5
.xlsx	FETCH	nlamshv01	Files	10.0.30.21	76	10211	824551	271537.66	613.11
.xlsx	FLUSH	nlamshv01	Files	192.168.1.210	645	0	185385075	13643943.84	13703453.72
.docx	FETCH	nlamshv01	Files	192.168.1.210	10	800020	6736830	2566284.7	2166806.2

GFC Processes / Services

GFC leverages different services and processes to establish and maintain the GFC Fabric and its associated GFC Core and GFC Edge instances. Some of these are dependent on other services and the TFAST.SYS file system kernel driver, which enables the GFC Virtual File Share and Intelligent File Cache on each GFC Edge instance.

The Table 3 below provides you with the details for each service and the functionality it provides.

Table 3)

Process/Service	Description
Tservice.exe (GFC Modules Service Monitor)	Job is to spawn Tum service in either Core, Edge or Hybrid mode Also spawns Tapp.exe and TFS.exe This is a Service
Tum.exe (GFC User Module)	Intelligent File Caching workhorse This is a process spawned on both GFC Core and Edge instance (Tum.exe -s & Tum.exe -c)
Tapp.exe (GFC Pre-Population)	Processed used for Pre-Population
Optimus.exe (GFC Configuration Console)	Configuration management software used when configuring an appliance This is a Process
LMCService.exe (GFC License Manager Client)	Used by GFC Servers to register with the license management server Spawns the Tservice.exe
LMSService.exe (GFC License Manager Server)	Used by GFC License management server Accepts the incoming client request for LMCService.exe

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

This video provides a general solution overview to admins and users as well as providing some GFC do's and don'ts.

<https://youtu.be/bH5T1KX79aM>

This video provides a general solution overview to admins and users as well as providing some GFC do's also provides a shortened general overview, basic do's and don'ts, and a focus on Autodesk Revit application best practices.

https://youtu.be/avMMA_ItZy0

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2020 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

Software Usage Limitations

You should be aware that the following additional limitations apply to your use of the GFC:

1. *Unless authorized explicitly in writing by NetApp, Customers who have initially licensed Talon FAST™ after March 9, 2020, are only authorized to run and install Talon FAST™ on the following backend products: NetApp's Cloud Volumes ONTAP® Software, NetApp's Cloud Volumes Service for Amazon Web Services, NetApp's Cloud Volumes Service for Google Cloud Platform, or Azure NetApp Files.*
2. *Provided it's released during the license term, Customers who have initially licensed Talon FAST™ after March 9, 2020, will, unless authorized explicitly in writing by NetApp, be required to upgrade to the next version of the Talon FAST™ Software (Global File Cache v. 1.0) when its released (tentatively Spring 2020).*
3. *Subject to the foregoing limitations, Customers which have been provided a license to Talon FAST™ at no charge are entitled to use that license for a period not to exceed 12 months from the date of initial software installation.*