



# Talon FAST™ 4.5

User Guide

Revision 20170907.1



## Introduction

Welcome to the Talon FAST™ 4.x User Guide. This manual will assist you in designing, deploying, managing and maintaining your Talon FAST™ infrastructure. The next few pages will provide a brief introduction and overview of the Talon FAST™ solution and how it can be leveraged to enable data centralization, storage consolidation and global file sharing and collaboration for distributed enterprises.

Talon FAST™ Enterprise Edition allows businesses to centralize data, leveraging customer's existing traditional datacenter or cloud storage infrastructure while consolidating distributed storage and IT assets. The software enables enterprises to centralize unstructured file data and transparently extend this to users globally to provide real-time global file sharing and collaboration to their end users.

## The FAST™ Fabric: Highly Scalable & Flexible

Talon FAST™ transparently fits any IT environment as the solution is storage agnostic. Whether you want to leverage your existing traditional file server or private / public cloud storage infrastructure, FAST™ immediately extends the value of your central storage to your distributed locations.

In a nutshell, Talon FAST™ software creates an intelligent file caching software appliance at each 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 that are challenged with poor connectivity (low bandwidth or high latency).

## Next Generation Software-Defined Storage

- ✓ Talon FAST™ Software runs on Microsoft Windows Server 2012 R2 and above
- ✓ Fully integrates with customer's Microsoft ecosystem
  - (AD DS, DNS/DHCP, Print Services, SCCM, SCOM, PowerShell CLI, Azure Automation / DSC)
- ✓ Available as software installation package or virtual appliance template

## Talon FAST™ Enterprise Edition

- ✓ **Flexible:** Storage agnostic, works with any SMB/CIFS infrastructure
- ✓ **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:** Distributed file locking for enterprise applications



## Contact Details

### 24x7x365 Worldwide Support

Talon offers a wide variety of resources to help our customers with their Talon FAST™ deployments. The following tools and resources are available 24/7 to help you manage, troubleshoot, and get the most out of your distributed file services infrastructure. Talon's support personnel have extensive product and file sharing technology expertise.

For technical support inquiries, please logon to the Talon Customer Portal at <http://www.talonstorage.com/support> and log your support case. These cases are treated non-critical, and is used to interact indirectly with our 24x7 support team.

For any urgent matters (P1 issues) our team is available by phone 24x7. Depending on the support contract's associated Service Level Agreement, Talon support will evaluate support on a case-by-case basis. Please use the phone details listed below in order to directly call our support team.

### Worldwide Support Phone Numbers

Toll Free: +1.877.280.4802 (option 2)

Toll: +1.856.481.3990

If you don't have a support contract with Talon please revisit the support services page or contact [sales@talonstorage.com](mailto:sales@talonstorage.com) for further information.

## Terms and Conditions

DISCLAIMER: THIS DOCUMENTATION IS PROVIDED BY TALON ON AN "AS IS" BASIS. TALON MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE OPERATION OF THE WEBSITE OR THE INFORMATION, CONTENT, MATERIALS, OR PRODUCTS INCLUDED IN THIS DOCUMENT. TO THE FULL EXTENT PERMISSIBLE BY APPLICABLE LAW, TALON DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

Although Talon has attempted to provide accurate information in this documentation, Talon assumes no responsibility for the accuracy or completeness of the information. Talon may change the programs or products mentioned in this document at any time without notice, and Talon makes no commitment to update the programs or products mentioned on this website in any respect. Mention of non-Talon products or services is for informational purposes only and constitutes neither an endorsement nor a recommendation.



## Table of Contents

<b>1. Talon FAST™ Requirements</b>	<b>7</b>
Hardened Server Appliance	7
Physical Hardware Requirements (i.e. DELL/EMC or HP or Hypervisor Host)	7
Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)	7
Cloud Deployments (i.e. Microsoft Azure or Amazon AWS)	8
Operating System / Software Requirements	9
Partition Sizing Requirements	9
Networking	9
Client Workstation Settings	10
Firewall and Antivirus best practices	12
<b>2. Getting Started with FAST™</b>	<b>14</b>
Example: Deployment Summary	14
Example: Centralized data store with On-Premise Storage	15
Talon FAST™ Fabric	16
Sizing Guidelines	17
<b>3. Deploying Talon FAST™ Virtual Template and Software Package</b>	<b>19</b>
Before You Begin	19
Deploying Talon FAST™ Virtual Template	20
Login Credentials	20
Network Configuration	21
Active Directory Configuration	22
Software Installation Package (Update)	24
<b>4. Licensing</b>	<b>29</b>
How it works	29
Subscription Updates	29
Caching	29
Requirements	29
Deploying Talon FAST™ LMS instance	30



<b>5. Initial Configuration</b>	<b>33</b>
Initial Configuration Wizard	33
Talon Configuration Console	34
FAST™ Edge Instance	34
FAST™ Core Instance	34
Registering your FAST™ Core or Edge instance with FAST™ LMS (Optional)	34
<b>6. Designing and Deploying Talon FAST™ Fabric</b>	<b>37</b>
FAST™ Core stand-alone instance	37
FAST™ Core HA clustered instance	38
FAST™ Core Load Distributed design	44
Configuring FAST™ Core instance – Service Account	45
Configuring FAST™ Core instance – Backend File Servers	46
FAST™ Core Advanced Options	48
Global Exclusion List	48
Server Exclusion List	49
Remote Inclusion List	50
Selectable File Handling	51
Core Pre-population	52
Configuring the Talon FAST™ Edge Role	56
Edge Pre-population	57
Edge Advanced Options	58
<b>7. DFS Namespace Integration</b>	<b>59</b>
DFS Design	59
Site Definitions and Site Links	60
DFS Root Configuration default	62
Site Costing Configuration	67
Talon FAST™ Global Exclusion Configuration (DFS)	68
<b>8. Central Monitoring using Microsoft SCOM</b>	<b>69</b>
Deploying Talon SCOM Management Pack	70
Dashboards and Reports	72
Personalized Views	73
Core Instances	74
Edge Instances	76
Where do I Find...?	79
Event Analysis	80
Log Analysis	81



<b>9.</b>	<b>FAST™ Web Access Portal</b>	<b>84</b>
	Deploying Talon FAST™ Web Access Portal	84
	Talon FAST™ Web Access Portal Deployment Instructions	85
	FAST™ Web Access Portal – Core Configuration	87
<b>10.</b>	<b>Client Application Best Practices</b>	<b>89</b>
	AutoDesk - Revit	89
	Revit Best Practices Summary	92
	Autodesk - AutoCAD	93
	Bentley – MicroStation	97
	Adobe Creative Suite	101
	Mac OSX Best Practices	103
<b>11.</b>	<b>End User Training</b>	<b>106</b>
	Additional Resources	107
	<b>Appendix A: Antivirus Application Suites</b>	<b>109</b>
	McAfee VirusScan	109
	Symantec Endpoint Protection 12.x	121
	Sophos Endpoint Security and Control v10.x	130
	Trend Micro Officescan	136
	<b>Appendix B: Disable VMware ESX(i) Hot Plug Capability</b>	<b>140</b>



## 1. Talon FAST™ Requirements

Talon FAST™ software is storage agnostic and specifically designed to function across all platforms supporting Windows Server 2012 R2 and above, bringing simplified IT to corporate distributed branch offices and beyond. Critically, Talon's FAST™ software can be deployed on customers' existing hardware infrastructure or virtualization or private / public cloud environments in virtually every case, as long as they meet a few base-level requirements.

Talon FAST™ software **requires** the following hardware and software resources to function optimally. For more information about overall sizing guidelines, please consult chapter 2 of this user guide.

### Hardened Server Appliance

The Talon FAST™ software installation package creates a hardened software appliance on any Microsoft Windows Server instance. **DO NOT UNINSTALL THE TALON SOFTWARE PACKAGE.** Uninstalling Talon FAST™ will impact the functionality of the server instance and may require a full rebuild of the server instance. \* **IMPORTANT**

### Physical Hardware Requirements (i.e. DELL/EMC or HP or Hypervisor Host)

- Minimum 2 CPU Cores (4 CPU Cores recommended)
- Minimum 8GB RAM (16GB recommended)
- Dedicated Single or Redundant 1Gbps NIC
- 7200 RPM SATA HDD or SATA SSD
- RAID controller with write-back caching functionality enabled \* **IMPORTANT**

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

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

Microsoft Hyper-V 2012 R2 onwards	
<b>Processor (CPU)</b>	<b>CPUs must be set as Static:</b> Minimum: 2vCPU Cores Recommended: 4vCPU Cores
<b>Memory (RAM)</b>	Minimum: 8GB set as Static Recommended: 16GB set as Static
<b>Hard Disk Provisioning</b>	Hard Disks must be configured as "Fixed Disk"

VMware vSphere 5.1 onwards	
<b>Processor (CPU)</b>	<b>Reservation of CPU Cycles must be set * IMPORTANT</b> Minimum: 2 vCPU Cores @ 6700MHz Recommended: 4 vCPU Cores @ 10000MHz
<b>Memory (RAM)</b>	Minimum: Reservation of 8GB Recommended: Reservation of 16GB
<b>Hard Disk Provisioning</b>	<ul style="list-style-type: none"> <li>▪ Disk Provisioning set as “Thick Provisioned Eager Zeroed”</li> <li>▪ Hard Disk Shares set to High</li> <li>▪ Set “devices.hotplug” to “false” using the vSphere Client to prevent Microsoft Windows from presenting Talon drives as “removable”</li> </ul> <b>See Appendix B for the steps to apply this setting</b>
<b>Networking</b>	Network Interface needs to be set to <b>VMXNET3</b> (requires VMTools)

**Note:** Talon FAST™ runs on Windows Server 2012 R2 and above, hence the virtualization platform needs to support the operating system and integration with utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine, such as VMTools.

## Cloud Deployments (i.e. Microsoft Azure or Amazon AWS)

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

Public Cloud Deployments	
<b>Microsoft Azure</b>	<b>Standard A/D Series (i.e. Standard_A3)</b> Minimum: 2 vCPU Cores / 7GB RAM Recommended: 4 vCPU / 14GB RAM  See also: <a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general">https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general</a>
<b>Amazon AWS (EC2)</b>	<b>M/C Instance Type (i.e. m4.xlarge)</b> Minimum: 2 vCPU Cores / 8GB RAM Recommended: 4 vCPU / 16GB RAM  See also: <a href="https://aws.amazon.com/ec2/instance-types/">https://aws.amazon.com/ec2/instance-types/</a>





## Operating System / Software Requirements

- Microsoft Windows Server 2012 R2 or Windows Server 2016 Standard, Datacenter
- Latest Microsoft updates should be installed to ensure optimal stability, performance and security
- Talon FAST™ 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
- Talon instances should be joined to the customer's Active Directory domain
- Talon instances should be managed in a Talon-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.
  - This user must be a member of the "Backup Operators" group on NetApp and Windows datacenter file servers.
  - EMC Isilon backend requires that the account has "run as root" privilege on each file share.
  - Service Account should be configured with the following account options:
    - User must change password at next logon = DISABLED (unchecked)
    - Password never expires = ENABLED (checked)
- Talon core instances must be on the same VLAN as the datacenter backend storage infrastructure (1 hop)

## Partition Sizing Requirements

- **C:\** Minimum 150GB (System/Boot Volume)
- **D:\** Minimum 250GB (Separate Data Volume for FAST™ 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.

## Networking

- Firewall: TCP ports should be allowed between Talon FAST™ edge and core instance
- FAST™ TCP Ports: 6618 – 6622
- FAST™ Web Access Portal: 4443, 8888, 60845-60850
- Network optimization devices (i.e. Riverbed Steelhead) must be configured to "Pass-thru" Talon-specific ports (TCP 6618-6622)



## Client Workstation Settings

Talon FAST™ transparently integrates into customer's environments, allowing users to access centralized data using their client workstations, running enterprise applications. Using Talon FAST™, data is accessed through a direct drive mapping or through a DFS namespace. For more information about the Talon FAST™ Fabric, Intelligent File Caching and key aspects of the software, consult the [Getting Started](#) 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 a Windows clients in the environment.

- **Registry**
  - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\CSC
  - Specify the **Start** value to "4"
  
- **Group Policy**
  - Launch Group Policy Management console from Active Directory Users and Computers
  - Navigate to the Domain policy or a specific policy that applies to Microsoft Windows Clients in your environment.
  - Select User Configuration, expand Policies, expand Administrative Templates, expand System, and expand Folder Redirection.
  - Right-click "**Do not automatically make all redirected folders available offline**" and click **Edit**.
  - Click Enabled, followed by OK.

### **Depending on your environmental requirements (optional) :**

- Right-click "**Do not automatically make specific redirected folders available offline**" window appears.
- Click Enabled.
- In the Options pane select the folders that should not be made available offline by selecting the appropriate check boxes.
- 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 DFS Namespace Resolver Patch for Windows 7**

To ensure that Windows 7 clients acquire the correct DFS referral, it is required that these Windows 7 clients contain the latest DFS hot fix (Windows6.1-KB2649905-x64.msu) released by Microsoft.

Reference: <https://support.microsoft.com/en-us/help/2649905/-an-unexpected-network-error-occurred-error-message-when-you-try-to-browse-a-dfs-folder-in-windows-7-or-in-windows-server-2008-r2>

### **Microsoft Updates and Critical Patches**

Talon 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 Talon FAST™ instances in the environment.



## Firewall and Antivirus best practices

**Note: While Talon makes a reasonable effort to validate that the the most common antivirus application suites are compatible with the Talon FAST™ solution, 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.**

**Talon does not recommend the installation nor application of monitoring or antivirus solutions on any FAST™ 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 Talon FAST™ 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
  - Talon FAST™ core instance listens on TCP ports 6618-6622, ensure that FAST™ edge instances can connect to these TCP ports.
  - When enabling the Talon FAST™ Web Access Portal service, you may need to open TCP ports 4443, 8888, 60845-60850 (see section 1 for the requirements)
- Network Optimization solutions/devices must be configured to “Pass-thru” Talon-specific ports

### Antivirus Best Practices

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

**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 Talon (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. Talon 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) and T:\ (virtual file share) volumes should both be excluded from virus scanning as well as any Talon FAST™ 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:\ or drive T:\ on the Edge instance. These scans of Edge server drives D:\ and T:\ 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.

The following Talon FAST™ directory and processes should 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\tafsexport.exe
- C:\Program Files\TalonFAST\Bin\tafsutils.exe
- C:\Program Files\TalonFAST\Bin\tapp.exe
- C:\Program Files\TalonFAST\Bin\tfs.exe
- C:\Program Files\TalonFAST\Bin\TService.exe
- C:\Program Files\TalonFAST\Bin\tum.exe
- C:\Windows\System32\drivers\tfast.sys

## 2. Getting Started with FAST™

Talon FAST™ software 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 FAST™ Fabric, in real-time with the benefits of distributed file locking.

Customers drive value from Talon FAST™ software by centralizing data and consolidating file storage from distributed branch offices to a traditional datacenter, hybrid or public cloud datacenter, i.e. Microsoft Azure, AWS or other cloud providers.



### 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:

1. **Centralized data store:** Enterprise storage in customer's traditional datacenter
2. **Talon FAST™ Fabric:** Extension of the central data store to the distributed locations
  - a. Talon FAST™ Core Instance, mounting to corporate file shares (SMB/CIFS)
  - b. Talon FAST™ Edge Instance running in each distributed location
    - i. Presents a Virtual File Share that provides access to central data
    - ii. Hosts the Intelligent File Cache on a custom-sized NTFS volume (D:\)
3. **Network configuration**
  - a. MPLS
  - b. Virtual Private Network (VPN) connectivity
  - c. Public Internet (SSL)
4. **Integration with customer's Active Directory Domain Services**
5. **DFS-Namespace for the use of a global namespace (recommended)**

## Example: Centralized data store with On-Premise Storage

The main repository for the unstructured data is a share (or number of shares) configured on the customer’s traditional storage platform leveraging CIFS / SMB integration or by presenting a local volume associated with an iSCSI target, provided by a 3<sup>rd</sup> party storage solution.

The customer’s datacenter file storage solution provides volumes associated with corporate file shares hosted on on-premise storage like Windows Server, DELL/EMC, HP or NetApp.



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 as data in a traditional 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.

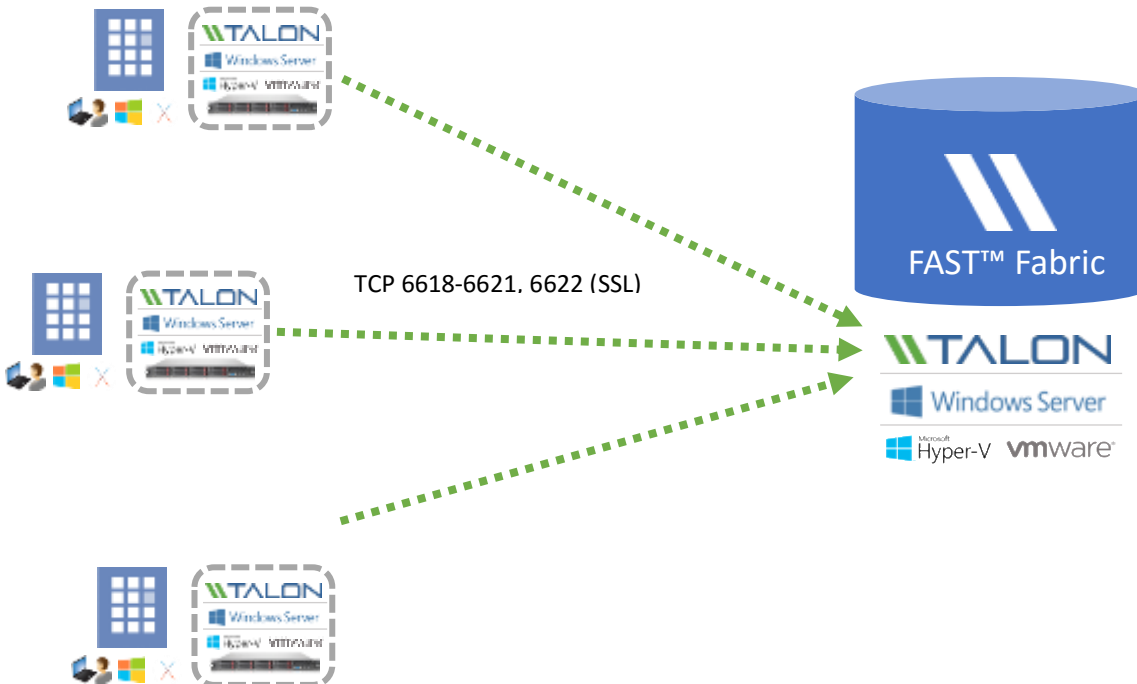
### **Datacenter Storage – Windows Server / Dell / EMC / NetApp / Etc.**

1. Provides transparent CIFS / SMB utilization presented by Windows File Server
2. Centralized data management (Volumes, ACLs, NTFS Permissions)
3. Integrates with enterprise backup solutions (RTO / RPO)

**Note:** For different deployment methodologies, including traditional datacenter, private cloud, hybrid cloud (i.e. Microsoft StorSimple or EMC CloudArray) or public cloud deployments with Microsoft Azure or Amazon AWS (i.e. SoftNAS Cloud NAS) please consult your Talon Sales representative or Solutions Engineer.

## Talon FAST™ Fabric

By introducing the Talon FAST™ software, integrating the FAST™ Fabric with traditional storage at the datacenter, 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.



The Talon FAST™ Edge instances transparently integrate with the FAST™ Fabric at the customer’s traditional or cloud datacenter:

1. Distributed locations connect to traditional or cloud datacenter via the Talon FAST™ Fabric
2. Software provides a Virtual File Share and Intelligent File Cache at each location
  - a. Virtual File Share is available as [\\Edge\FASTData\\[datacenter\]\\[fileserver\]\\[share\]\\[folder\]](#)
  - b. Access our data through DFS Namespace (recommended) or Drive Mapping
  - c. Intelligent File Cache can be sized based on the customer’s active data set (see product requirements)
3. Enables high performance global file sharing with real-time distributed file locking





## Sizing Guidelines

There are a few sizing guideline ratios that should be kept in mind when configuring the initial system, until history has accumulated. These include:

- Talon FAST™ Edges / Core Ratio
- Distributed Users / Talon FAST™ Edge Ratio
- Distributed Users / Talon FAST™ Core Ratio

### Number of Edge instances per Core instance

The recommended guidelines are from 10 – 20 edges per core instance. This is dependent to a significant degree upon the type and mean file-size of most common workload. For larger collaborative file types, guide towards the 10 edges/core lower boundary; for more common Office items with a mean file size < 1MB, guide towards the 20 edges/core upper boundary.

**Note:** You can leverage multiple Talon FAST™ edge and core instances simultaneously to scale-out your infrastructure depending on the requirements.

### Number of Distributed Users per Edge instance

The edge instance is highly scalable if provisioned according to the sizing guidelines in this document. As such, a single FAST™ edge instance should serve between 100 – 250 users per edge instance. This is dependent to a significant degree upon the type and mean file-size of most common workload. For larger collaborative file types, guide towards the 100 users/edge lower boundary; for more common Office items with a mean file size < 1MB, guide towards the 250 users/edges upper boundary.

### Number of Distributed Users per Core instance

By design, the core instance handles little ‘heavy lifting’ in terms of caching algorithms and file-level differencing; this is offloaded to the edge instances (where there is a much lower user/instance ratio). As a result, the core instance is extremely scalable, with a recommended range of 1,000 – 4,000 users/core. This is dependent to a significant degree upon the type and mean file-size of most common workload. For larger collaborative file types, guide towards the 1,000 users/core lower boundary; for more common Office items with a mean file size < 1MB, guide towards the 4,000 users/core upper boundary.

**Note:** Consult your Talon Solutions Engineer to discuss the best options for your enterprise deployment.





### 3. Deploying Talon FAST™ Virtual Template and Software Package

#### Before You Begin

Download the Talon FAST™ Virtual Template(s) and Software Installation Packages from:

- <http://www.talonstorage.com/support/downloads> (needs registration)

To complete basic FAST™ configuration tasks, you will need the following information:

- Static IP addresses for each Talon FAST™ instance
- Subnet Mask
- Gateway IP address
- The FQDN you wish to assign to each FAST™ server
- The DNS suffix (optional)
- The user name and password of an administrative user in the domain

**FAST™ Core instances only:**

- The domain name, username and password of the FAST™ Service Account.
- The FQDN server name of data center file servers

**FAST™ Edge instances 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:\.
- The drive letter T:\ must be available for use.

**Commonly Used TCP Ports:**

There are several TCP ports used by FAST™ services. It is mandatory the devices can communicate on these ports and they be excluded from any WAN Optimization devices or Firewall restriction policies.

- FAST™ TCP Ports: 6618 – 6622
- FAST™ Web Access Portal: 4443, 8888, 60845-60850

## Deploying Talon FAST™ Virtual Template

If you are deploying Talon FAST™ using the .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 1: “[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, the Windows Server 2012 R2 operating system is preparing for first use, completing 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 FAST™ virtual instance has been completed, the Windows Server 2012 R2 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, login locally to the Windows Server 2012 R2 operating system with the following credentials:



## Login Credentials

**Username: FASTAdmin**

**Password: TalOnFAST!**

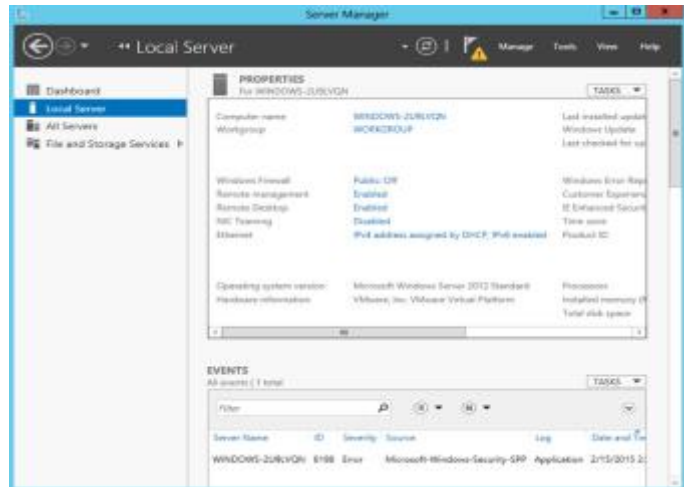


## Network Configuration

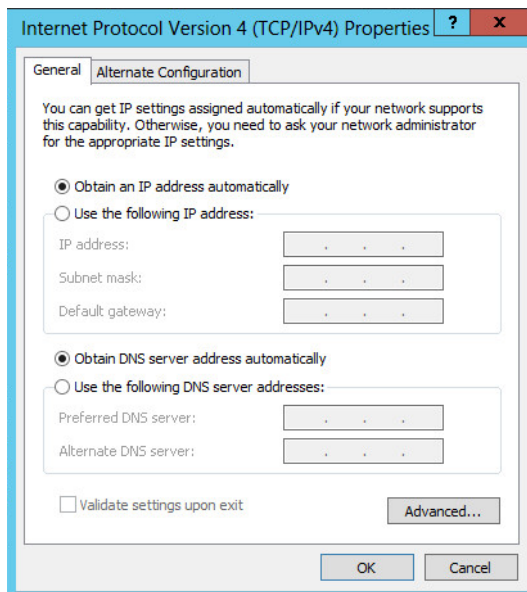
To successfully deploy Talon FAST™, you need to configure some basic settings such as IPv4 address, NetBIOS name and domain membership through the **Microsoft Windows Server 2012 R2 Server Manager** management console, which is automatically started after logging in to the FAST™ instance using the local **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 system which is based on the 1Gbps **VMXNET3** interface.



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 FAST™ appliance.



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

This opens the basic IPv4 configuration window. 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 FAST™ instance is now configured to communicate with other devices on the network to join the Active Directory domain.

## 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 Talon FAST™ instance needs a unique NetBIOS computer name. It is recommended to adhere to the company’s naming scheme for ease of management.

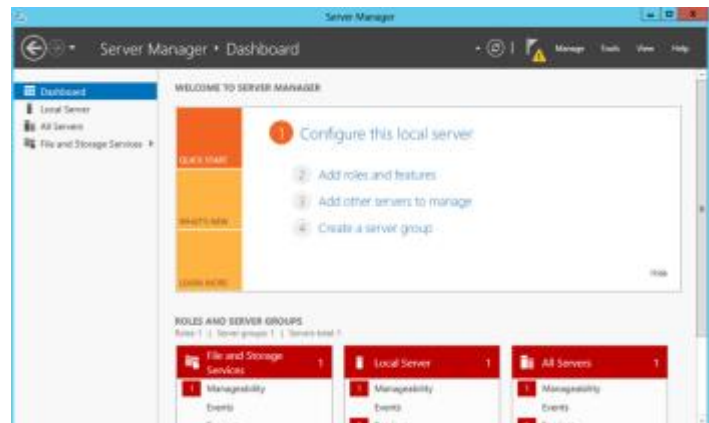
In many cases, the NetBIOS computer name represents a logical name including a geographical location, i.e.

Core FAST™ appliance located in Amsterdam

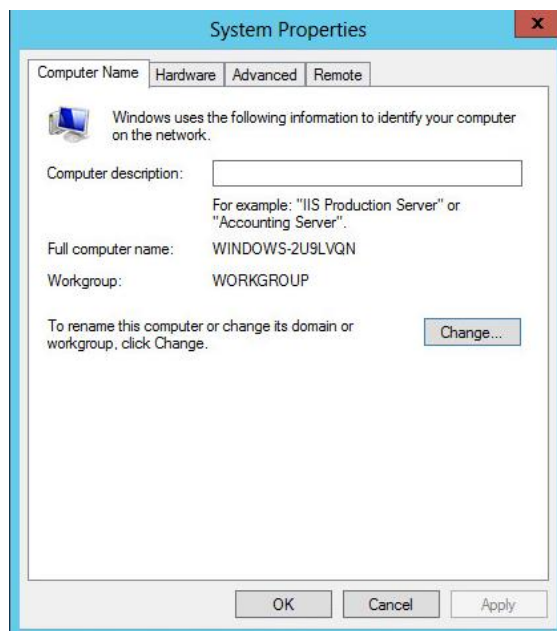
- **“AMS-FAST1”**

Edge FAST™ appliance located in London

- **“LON-FAST1”**



Use the Microsoft Windows Server 2012 R2 Server Manager console to configure the FAST™ instance’s NetBIOS name by clicking **“Local Server”** in the left pane.



Click the blue entry next to **“Computer name”** to open the System Properties window.

Click the **“Change...”** button to open the Computer Name/Domain Changes window

Type the desired NetBIOS name in the **“Computer Name”** field

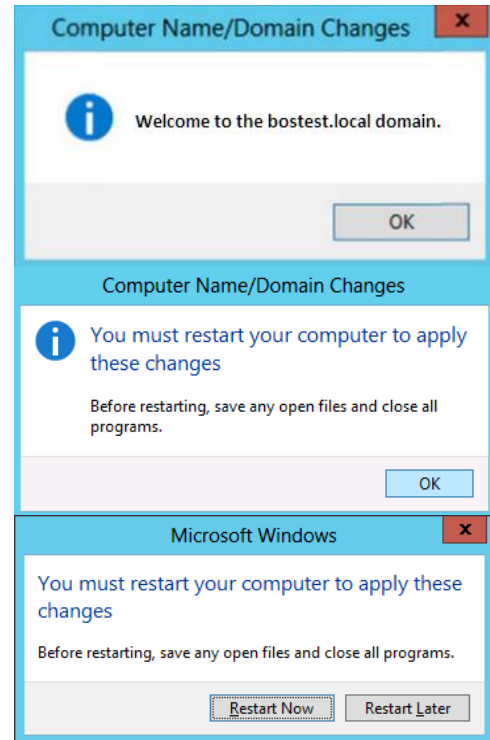
Select **“Member of”** Domain

Type the Active Directory FQDN

Confirm by clicking **“OK”**

## Complete the Configuration:

- Provide a Domain Administrator's **username** and **password**
- Confirm by clicking "**OK**"



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

## Software Installation Package (Update)

Talon 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 Talon FAST™ software, it could be possible that a newer version is available on the Talon Support Download portal.

Ensure that your Talon FAST™ instances are up to date with the latest GA version available at <http://www.talonstorage.com/support/downloads>

**Note:** This software package can also be used for pristine installations on Microsoft Windows Server 2012 R2 or Windows Server 2016 Standard or Datacenter or used as part of your upgrade strategy.

Below you can find the steps required to update the Talon FAST™ software installation package:

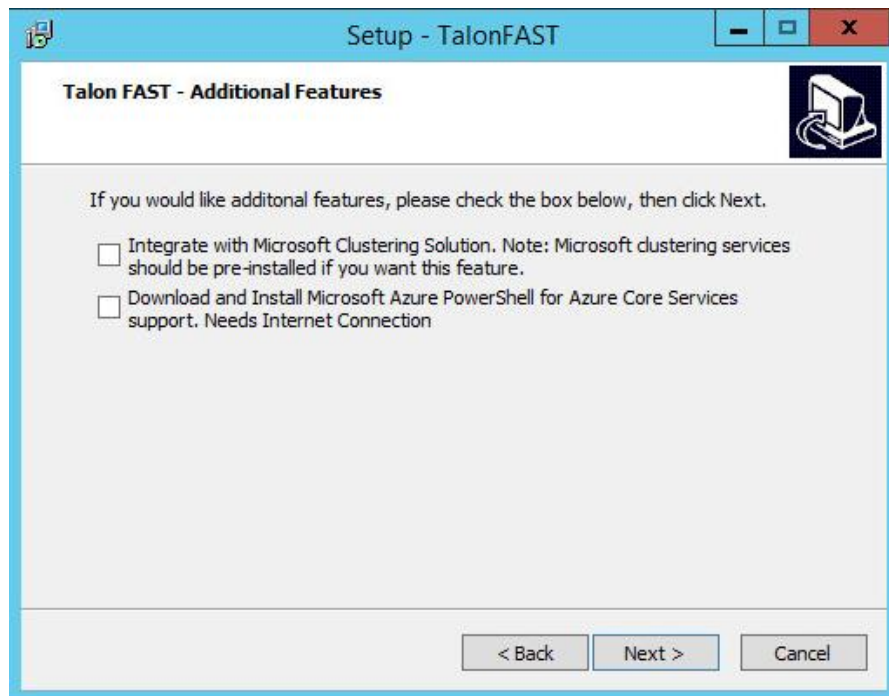
- After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable. (Your version number may differ slightly from what is shown below)



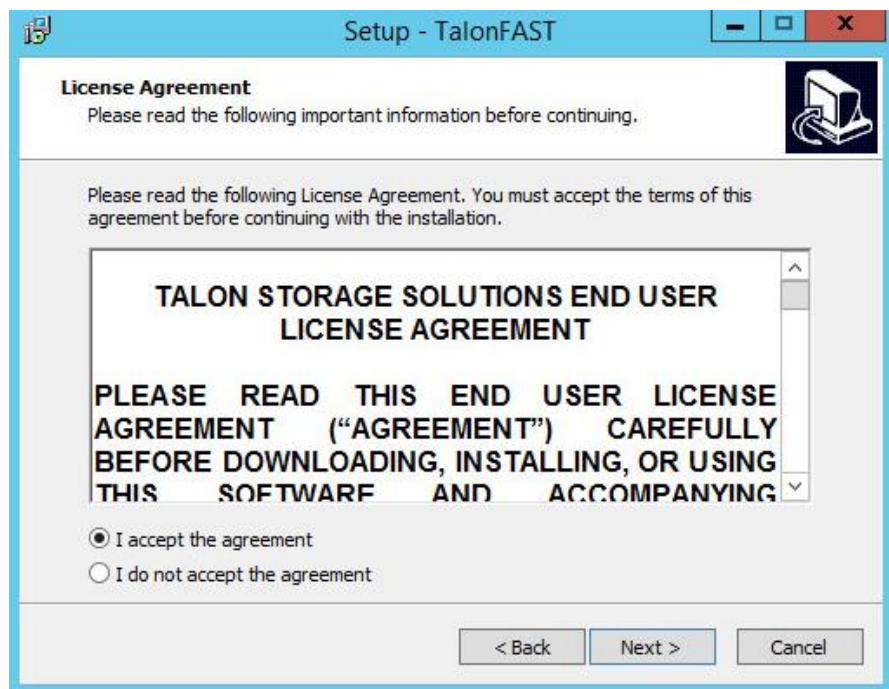
- Click the 'Next' Button to continue the process



- Optional: check the desired boxes if configuring the Core using Microsoft Clustering Services or if utilizing Azure Files as a backend server (internet access is required to install these additional features).



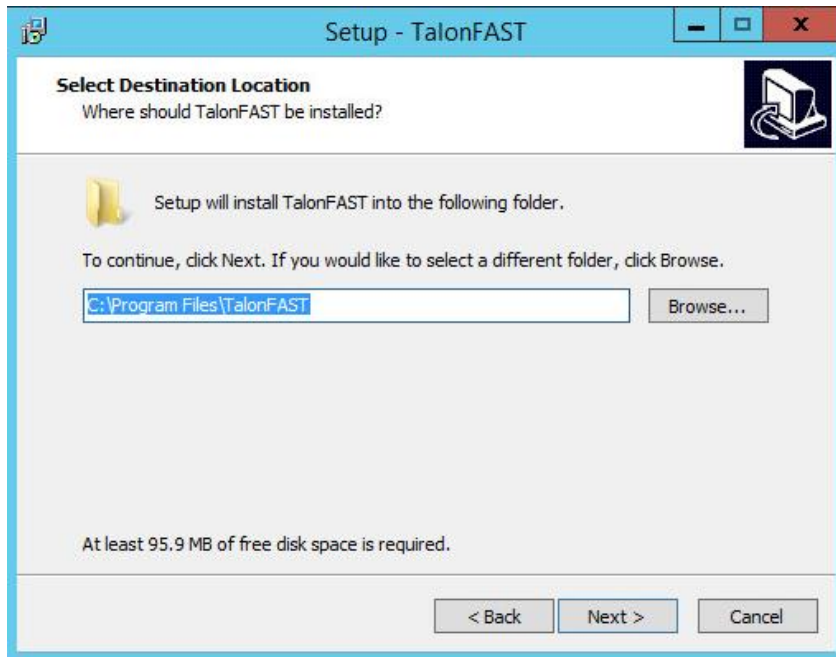
- Click 'Next' to continue



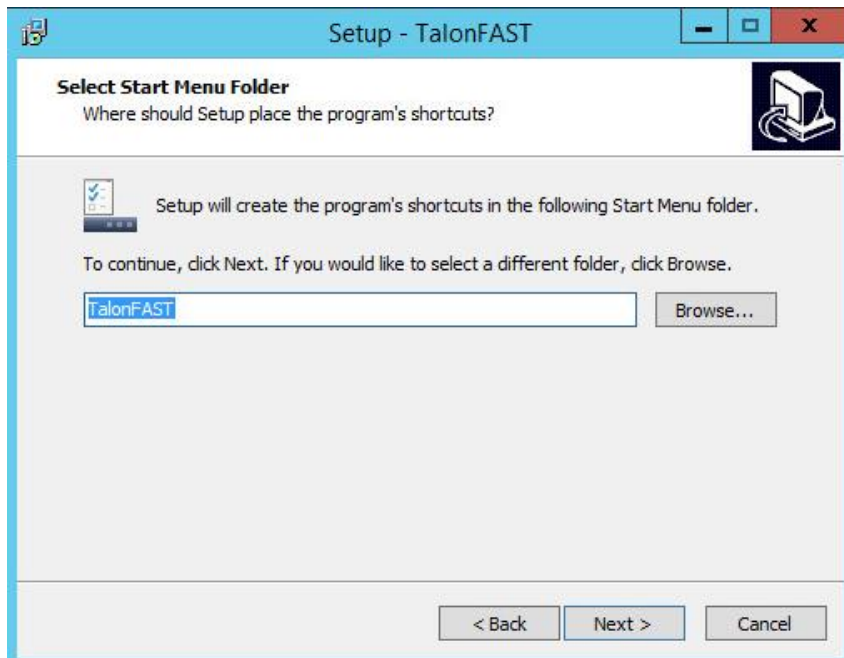
- Accept the Licensing Agreement and click 'Next'

- Select the desired Installation Destination Location.

**Note: it is recommended that the default installation location be used**

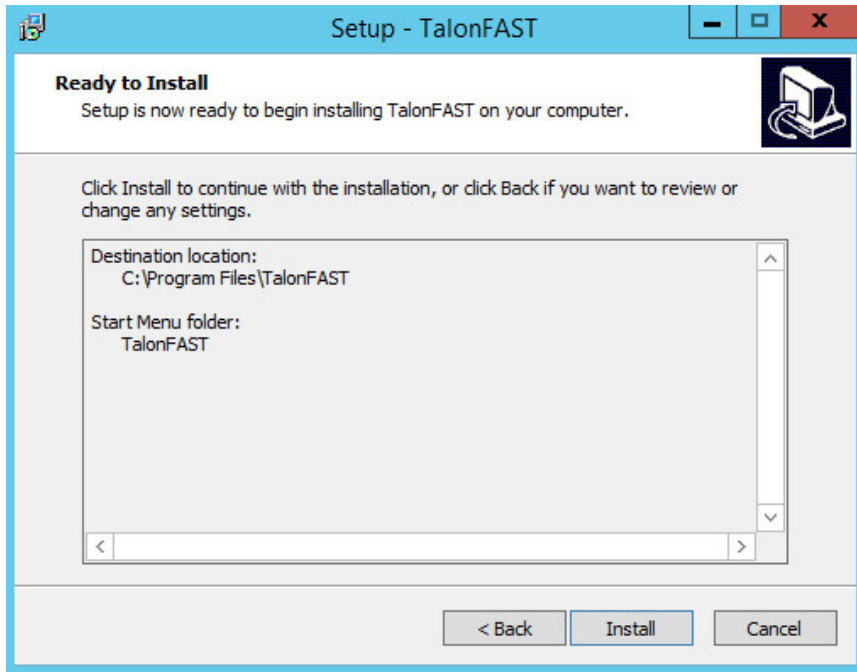


- Click 'Next' to continue
- Select the Start Menu Folder

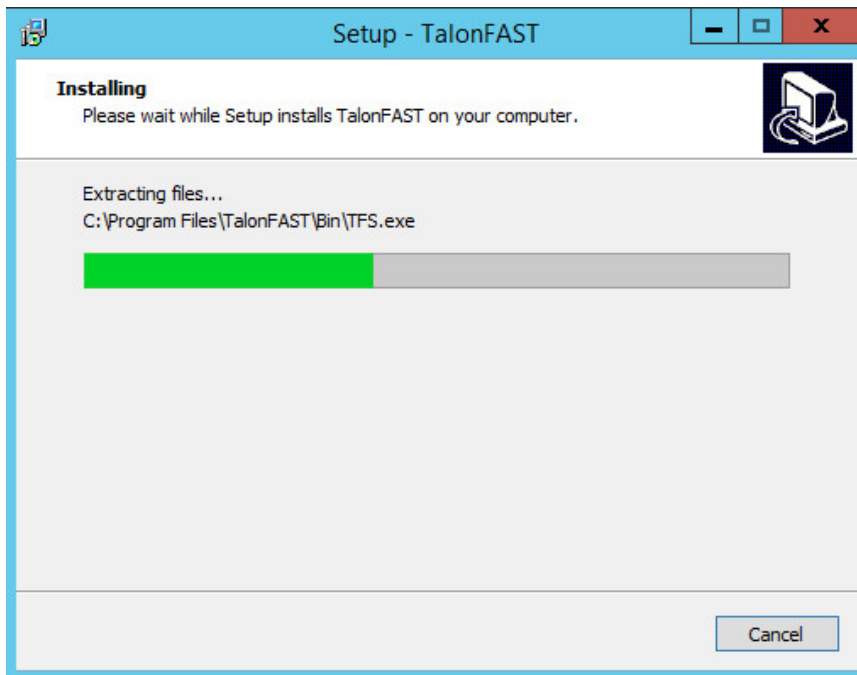


- Click 'Next' to continue

- Verify the desired installation parameters and click 'Install' to begin the installation



- The Installation Process will execute



- Once the installation has complete, reboot the server when prompted





## 4. Licensing

Talon FAST™ version 4.5 and above 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.

### How it works

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

### Subscription Updates

The Talon subscription service is designed to simplify license management. Once you have renewed or extended your FAST™ 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 FAST™ subscription service, the license details will be automatically updated on the LMS instance and the (new) license details will apply to your FAST™ core and edge instances.

### Caching

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

### Requirements

- FAST™ LMS instance should be configured on a Microsoft Windows Server 2012 R2 or Windows Server 2016 Standard or Datacenter edition, preferably the Talon FAST™ core instance in the datacenter or cloud
- If you require a separate FAST™ LMS instance, you need to install the latest FAST™ software installation package on a pristine Microsoft Windows Server instance
- FAST™ LMS instance needs to be able to connect to the FAST™ subscription service (Azure Services / public internet) using HTTPS (TCP port 443)
- FAST™ core and edge instances need to connect to the FAST™ LMS instance using HTTPS (TCP port 443)

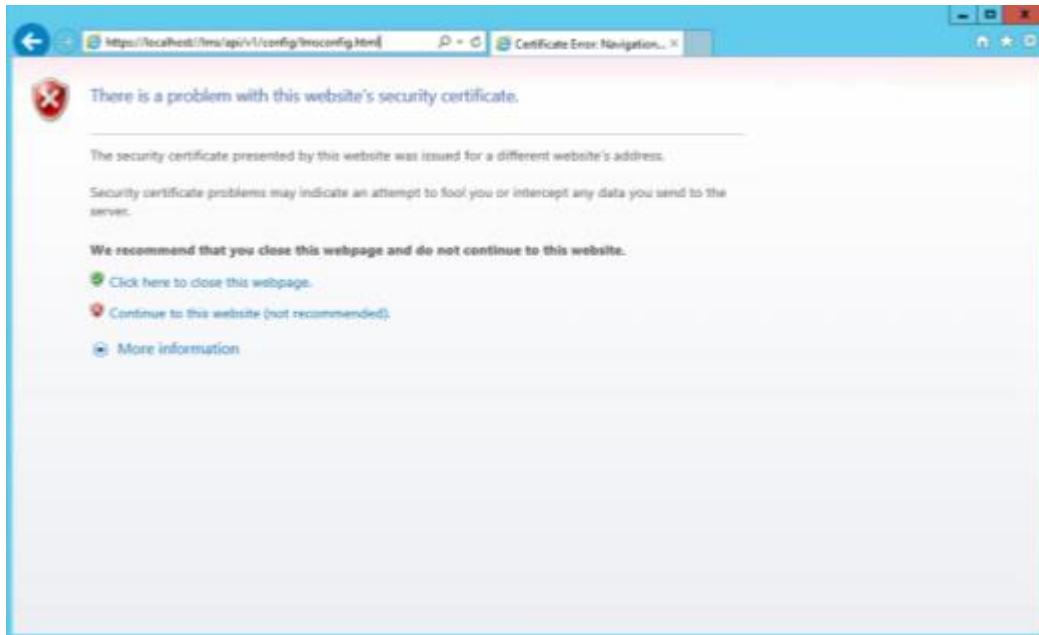
**Note:** Legacy customers, using a user-based subscription, can continue to use individual .XML license keys downloaded from the Talon licensing portal. If a change to site-based licensing (to take advantage of the LMS licensing feature) is desired please consult your Talon Sales representative.

## Deploying Talon FAST™ LMS instance

In this example, we will configure the LMS service on an existing Talon FAST™ core instance running Talon FAST™ 4.5 in an on-premise datacenter. This is a one-time exercise that allows you to complete the FAST™ LMS deployment.

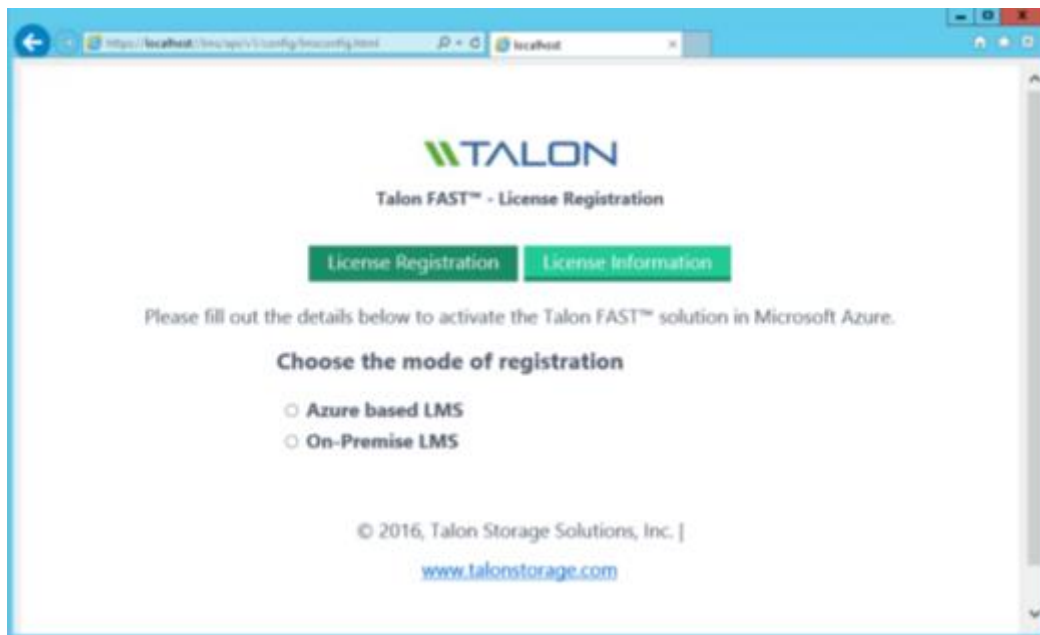
To start the LMS configuration open a web browser (Internet Explorer) and navigate to the following URL:

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



- Click **“Continue to this website (not recommended)”** to continue

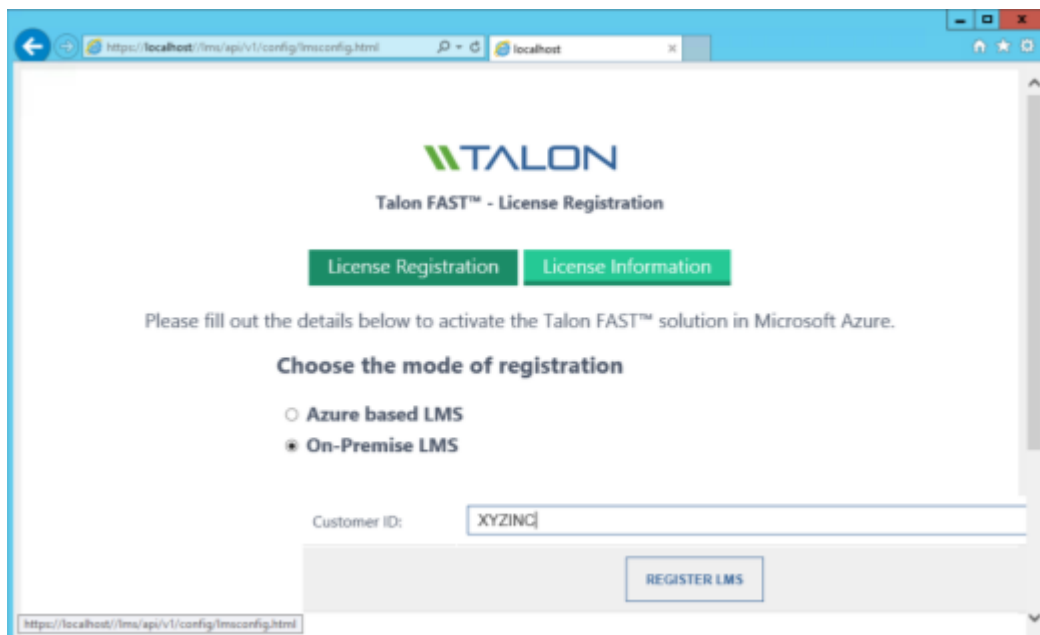
A webpage will be presented, which allows you to configure the LMS or check existing license information



- Choose the mode of registration by selecting “On-Premise LMS”

**Note:** Azure based LMS is only used when purchasing a Talon FAST™ BYOL or Pay-as-you-go subscription through Microsoft Azure Marketplace. For an on-premise deployment, select the “On-Premise LMS” option.

You will be prompted to enter the *Customer ID* (case sensitive) as provided by Talon support/operations department, i.e. XYZINC.



- Click “Register LMS” to complete the registration process.  
You will receive a message that confirms successful registration.





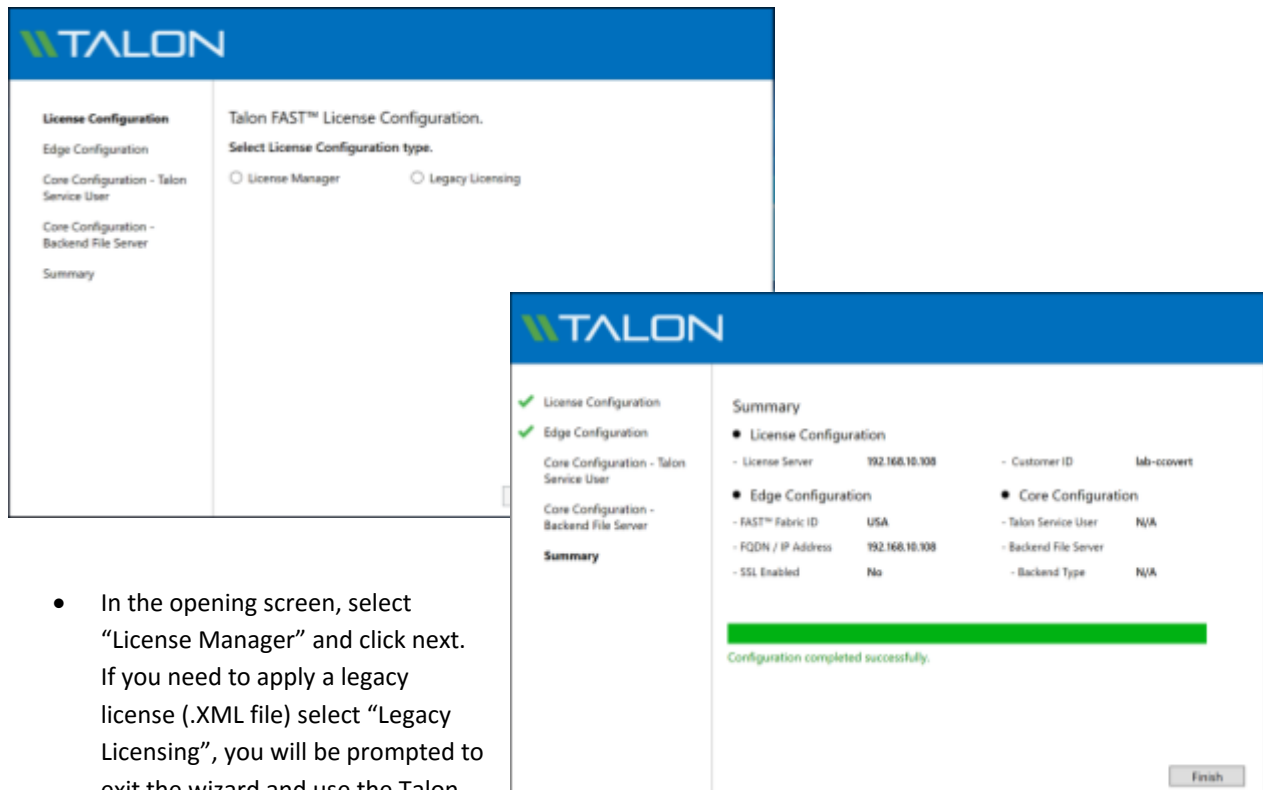
## 5. Initial Configuration

### Initial Configuration Wizard

Talon FAST™ 4.5 includes a new ‘Configuration Wizard’ for pristine installations of the software. This wizard will guide you through the process of associating your Talon FAST™ instance with your existing license manager (see chapter 4) and quickly deploy core or edge instances.

**Note: this configuration wizard only applies to customers with a site-based subscription that have deployed a licensing server (see chapter 4). If you do not have an LMS instance, follow the configuration steps as outlined in this chapter’s “Deploying Talon FAST™ LMS instance” section before starting the initial configuration wizard.**

Once you completed the deployment of the Talon FAST™ virtual instance and committed a reboot, you can start the configuration wizard by clicking the ‘Talon FAST™ Configuration Console’ icon on the desktop.



- In the opening screen, select “License Manager” and click next. If you need to apply a legacy license (.XML file) select “Legacy Licensing”, you will be prompted to exit the wizard and use the Talon Configuration Console to apply the license.
- Follow the steps prompted to complete the Talon FAST™ licensing configuration using the IP address of your LMS instance and the customer ID provided by Talon.
- Based on your selection FAST™ Edge or Core instance, you will be guided through the process of deploying basic settings associated with the configuration.

## Talon Configuration Console

Once the initial configuration wizard has completed or you've selected "Legacy Licensing" during the wizard, you can launch the "Talon FAST™ Configuration Console" from the desktop. The Talon FAST™ Configuration console allows you to configure basic System Settings, FAST™ Core and Edge settings (See also [chapter 6](#)) and FAST™ Web Access Portal ([chapter 9](#)):

### FAST™ 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 datacenter 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

### FAST™ Edge Instance

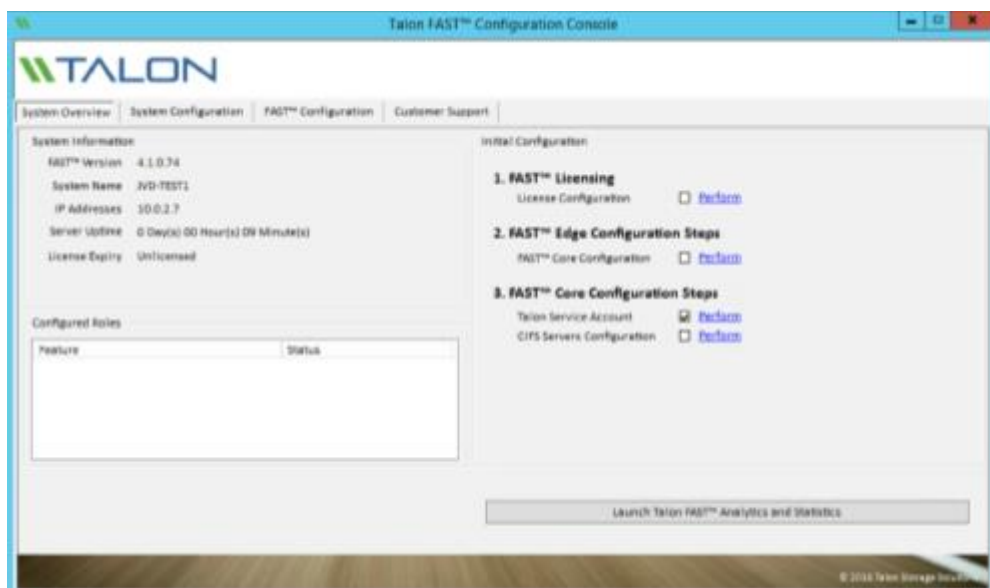
1. License the Edge Instance (LMS or Legacy)
2. Associate the Talon Edge instance with the Talon Core instance at the datacenter or in the cloud
  - Fabric ID (Location)
  - IP Address / FQDN of the Talon Core instance
3. Schedule Edge Pre-population jobs
4. Advanced Settings

## Registering your FAST™ Core or Edge instance with FAST™ LMS (Optional)

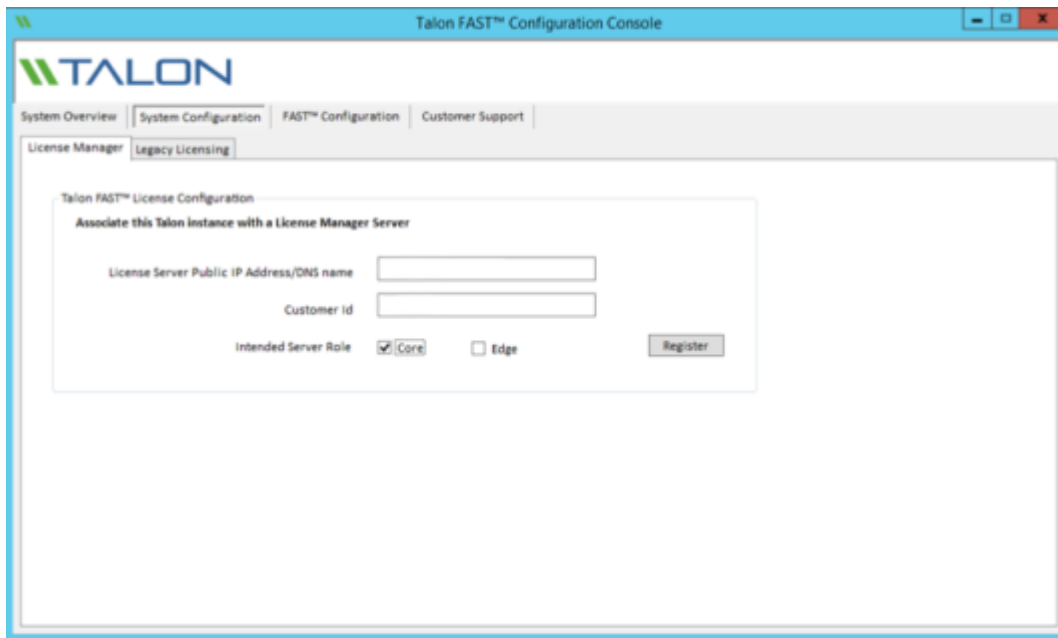
**Note: the following steps are only required if you skipped the initial configuration wizard or upgraded from a previous Talon FAST™ software release.**

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

- Open the Talon FAST™ Configuration Console from the desktop

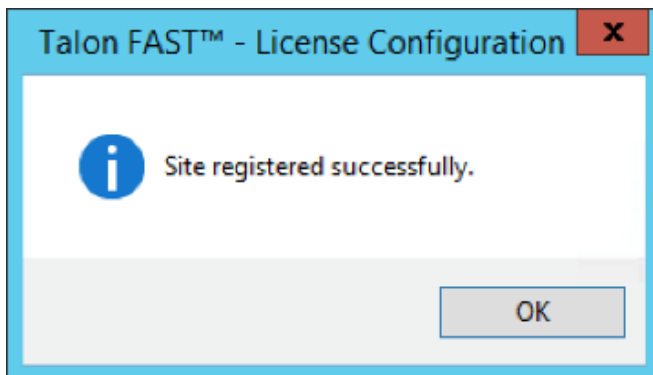


- Click on **“Perform”** next to License Configuration in the Initial Configuration section or navigate to the **“System Configuration”** tab, which opens the License Manager tab.

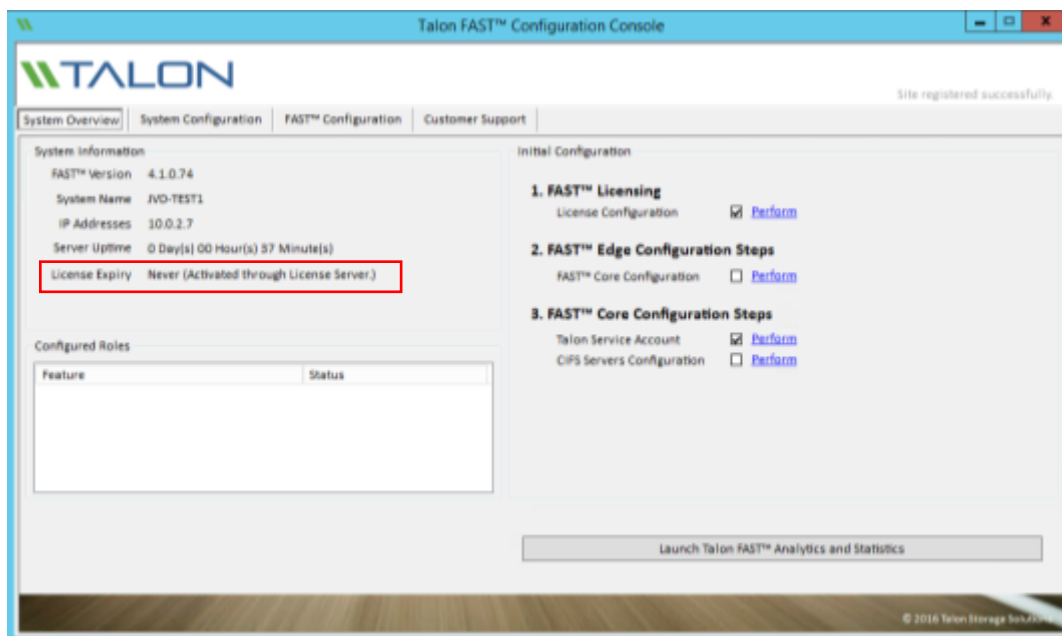


- Provide the IP address of the FAST™ LMS instance, i.e. *1.2.3.4* and *Customer ID* (i.e. XYZINC)
- Select the intended server role, Core or Edge and click **“Register”** to confirm

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



- Click **“OK”** to close this message.



- Once completed you can check that the licensing has been completed by navigating back to the **“System Overview”** tab of the FAST™ Configuration Console. License Expiry will display **“Never (Activated through License Server)”**
- Repeat this process **“Registering your FAST™ Core or Edge instance with FAST™ LMS”** for each Talon FAST™ instance in your environment.

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

## 6. Designing and Deploying Talon FAST™ Fabric

Depending on your requirements you may need to deploy one or multiple Talon FAST™ core instances to create the FAST™ Fabric. The core instance is designed to act as a ‘traffic cop’ between your distributed Talon FAST™ edge instances and the datacenter file server resources, i.e. file shares, folders and files.

The FAST™ core instance creates the FAST™ 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, on-premise, hybrid cloud or in the cloud.

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

Talon FAST™ core can be deployed in the following ways:

- FAST™ core stand-alone instance
- FAST™ core HA clustered instance (Microsoft Clustering)
- FAST™ core Load Distributed design (Cold Standby)

**Note:** it is recommended to deploy Talon FAST™ core instance as a virtual machine on a hypervisor platform that leverages high availability options.

### FAST™ Core stand-alone instance

When deploying a Talon FAST™ core stand-alone instance, you need to provision a single virtual machine, either by deploying Windows Server 2012 R2 or Windows Server 2016 Standard or Datacenter Edition, or using the Talon FAST™ .OVA or .VHD template which includes both the Windows Server operating system of choice and the Talon FAST™ software package.



#### Quick steps

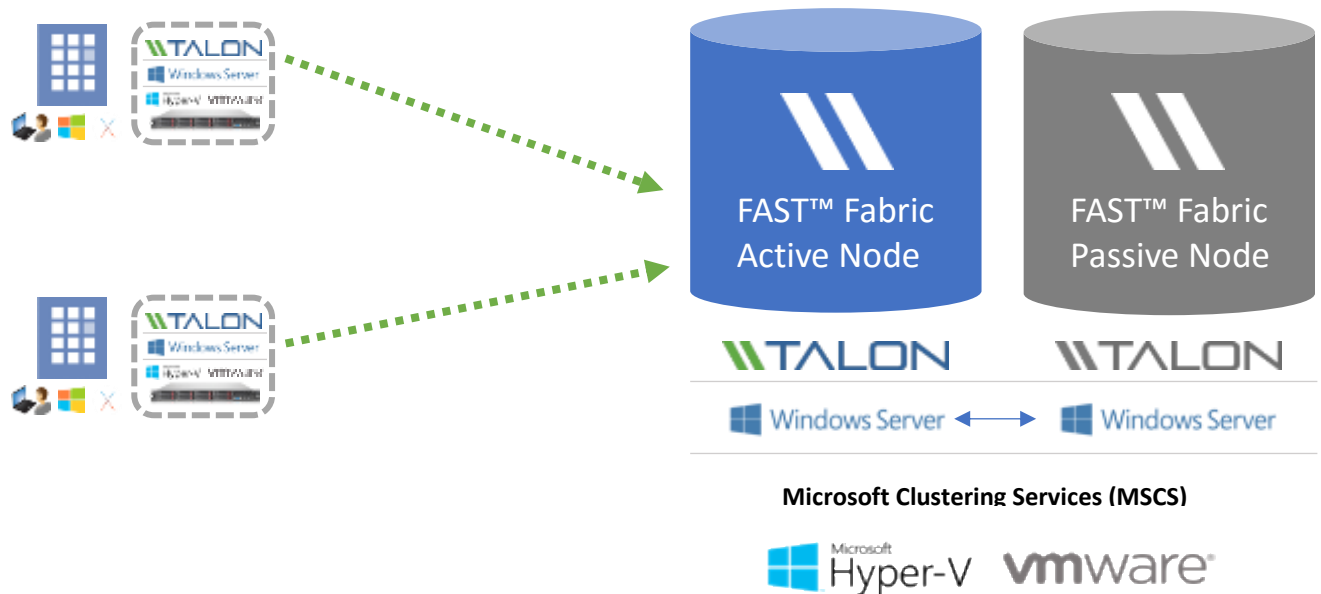
1. **Deploy Talon FAST™ Virtual Template or Windows Server 2012 R2 virtual machine**
2. **Ensure virtual machine is connected to the network, joined to the domain and accessible through RDP**
3. **Install the latest Talon FAST™ Software Installation Package (Update)**
4. **License the Talon FAST™ instance through the License Manager Server (see section 4)**
5. **Configure the Talon FAST™ Core role (see page 44)**

## FAST™ Core HA clustered instance

### Microsoft Cluster Services Integration Configuration

FAST™ Core instances can be configured with Microsoft Cluster Services in a high availability configuration to support failover between different Core instances. If you wish to use this service, prior to the installation of Talon FAST™ software, you must have a 2 node Failover Cluster with 1 available clustered disk, labeled D:\ for uniformity. This drive should be shared with Failover Sharing. (i.e. in Failover Manager -> Storage -> Disks, there must be an available disk listed.)

**Note:** This configuration is for FAST™ core instances only. The edge role will be automatically disabled once the installation process has completed.

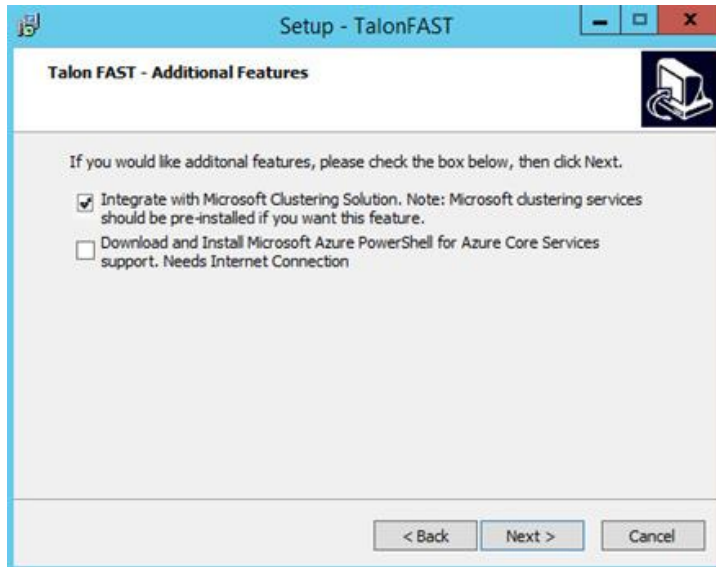


### Quick steps

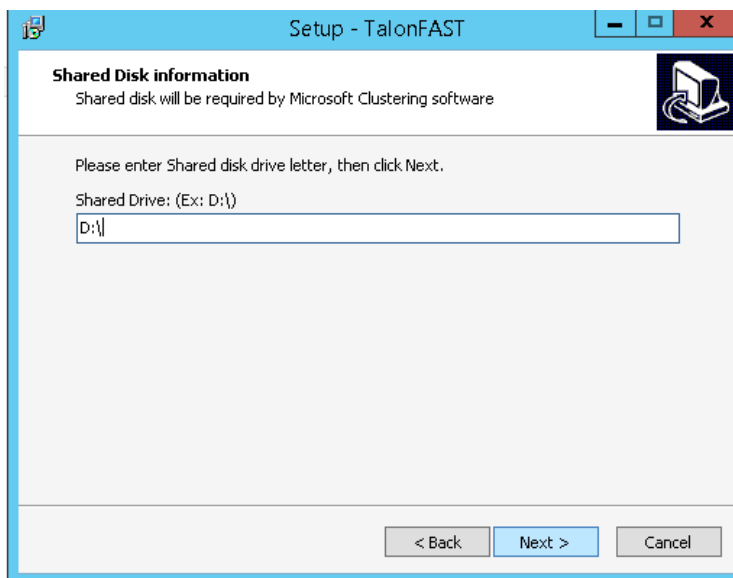
1. Deploy two Windows Server 2012 R2 virtual machine instances on different (hypervisor) hosts
2. Ensure a shared drive (D:\) is available to all cluster nodes in the failover cluster (i.e. iSCSI target)
3. Install Talon FAST™ Software Installation Package on each instance as per instructions below

### Installing the FAST™ Core instance using Microsoft Cluster Services

- Begin the installation of the FAST™ software on the Primary/Owner Node
- During the installation process, check the box to “Integrate with Microsoft Clustering Solution” and click “Next”

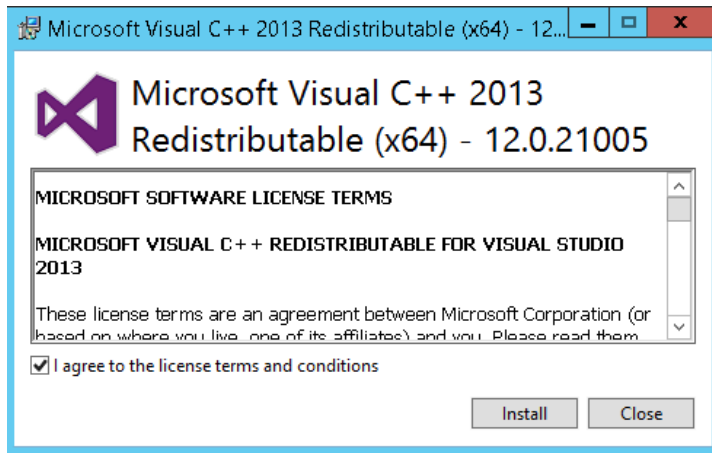


- Enter the shared drive letter in the cluster (in this example, D:\) and click “Next”



- Accept the license agreement and click “Next”
- Click “Install” to begin the process

- When prompted to install Microsoft Visual Studio C++ 2013, agree to the license and click “Install”



When the installation completes, you will be prompted to reboot the server. When the first node reboots, the second node in the cluster should become active. Verify the correct behavior and adjust your cluster configuration as needed.

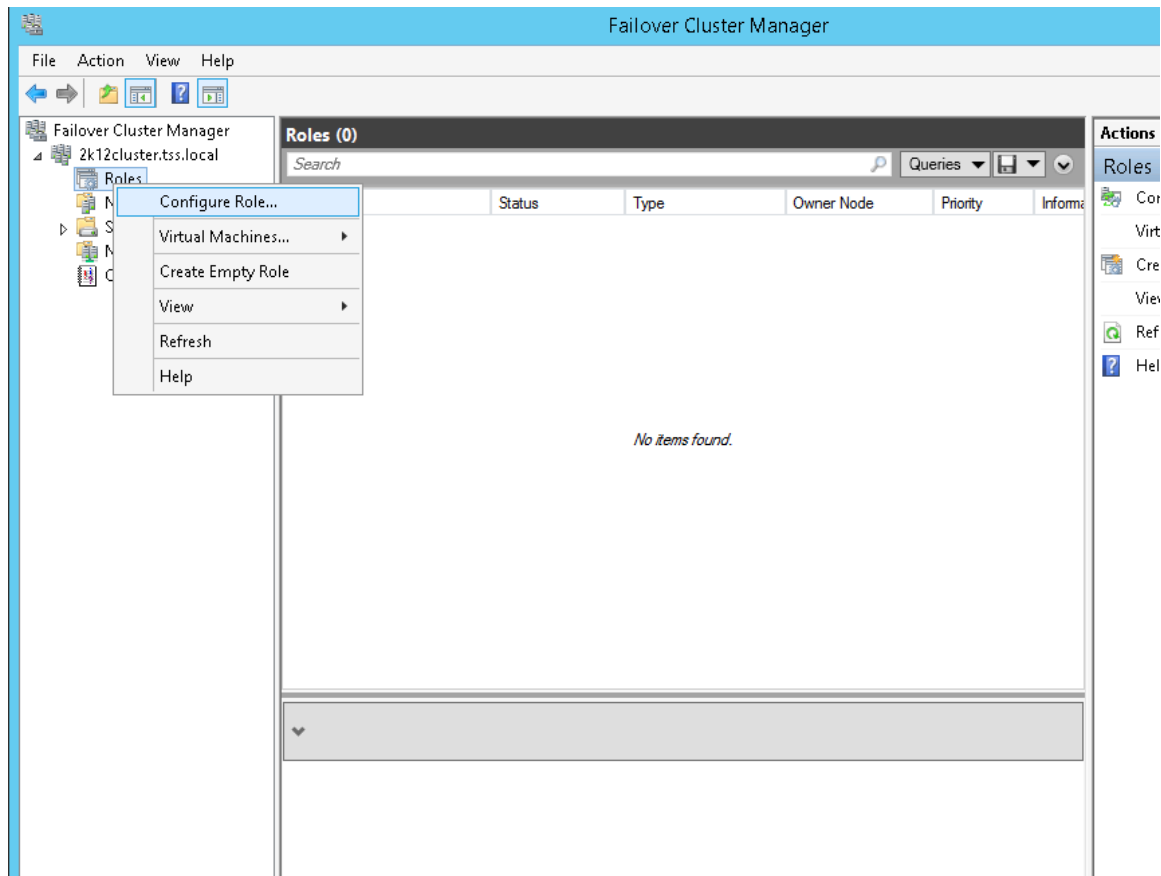
Repeat the steps outlined above to install Talon FAST™ on the second node in the cluster. When the installation completes and the second node reboots, the first node will come back as active.

- Manually start TService on the primary cluster server. Leave the service as ‘Manual’
- Change the Talon service account in the Talon FAST™ Configuration Console (see the section “Configuring FAST™ Core instance – Service Account”)
- Manually change the active cluster server to secondary server or reboot the primary server.
- Repeat the above three (3) bullet point steps on the secondary server
- Configure the backend file server or local path to data on the Owner node / Core instance. When the configuration has been completed, reboot the server to make the second node active.



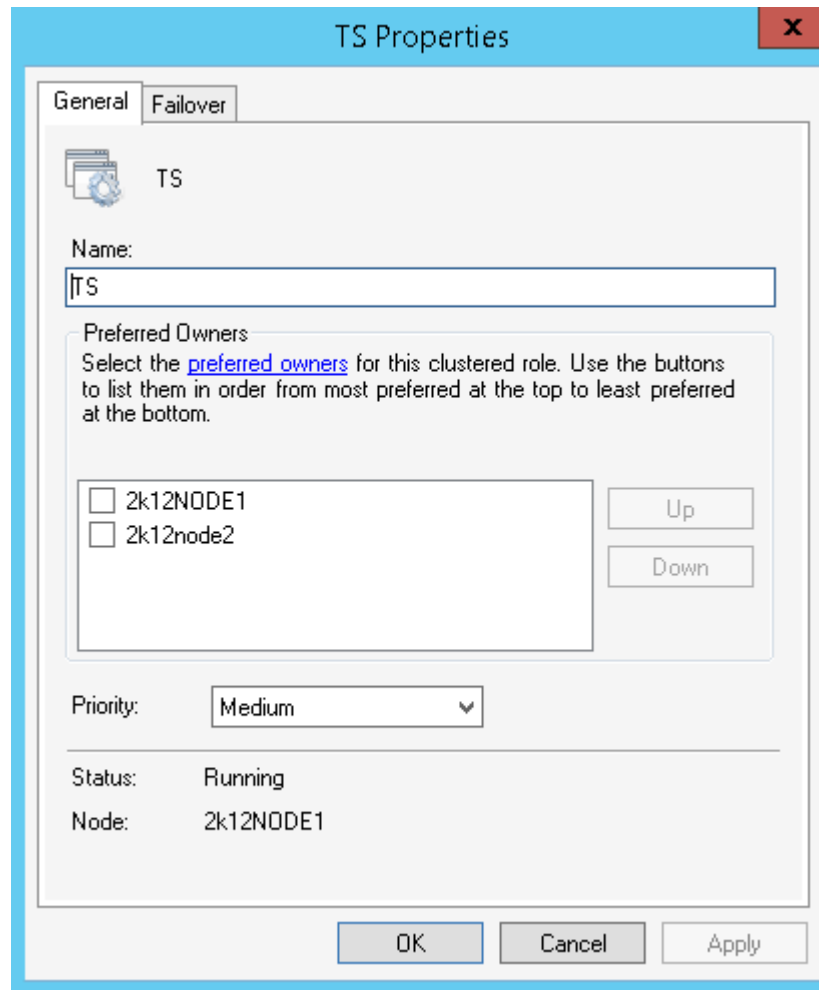
**To configure the control of the Talon FAST™ service during a failover event:**

- Open the Failover Cluster Manager utility
- Expand the Cluster that you've configure for the Talon FAST™ solution
- Right-click on Roles and select "Configure Role..."



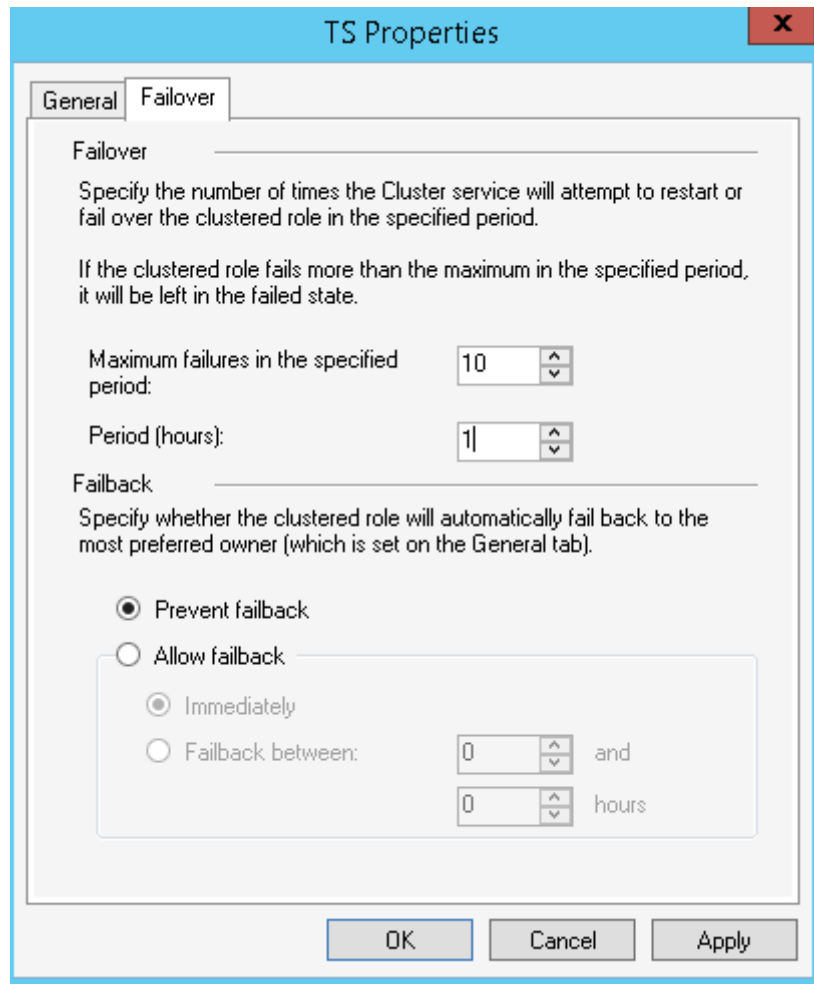
- The High Availability Wizard will open. Click "Next" to continue to "Select Role"
- Select "Generic Service" from the available list and click "Next"
- Click the "Talon TService" from the "Select Service" list and click "Next"
- Assign a name and an IP address to the role
- Assign the available storage (Drive D:\)
- Click 'Next' until the process completes
- Upon completion, the role you created will be visible in the Roles list
- Right-click the new role and choose "Properties" to display the Properties window

Customize the HA/clustering settings for the TS role:



- You do not need to make any changes to the settings on the “General” tab

- Click the “Failover” Tab at the top and adjust the settings to reflect the following changes:
  - **Maximum failures in the specified period: 10**
  - **Period (hours): 1**
  - **Prevent failback: selected**



- Click “OK” to commit the changes

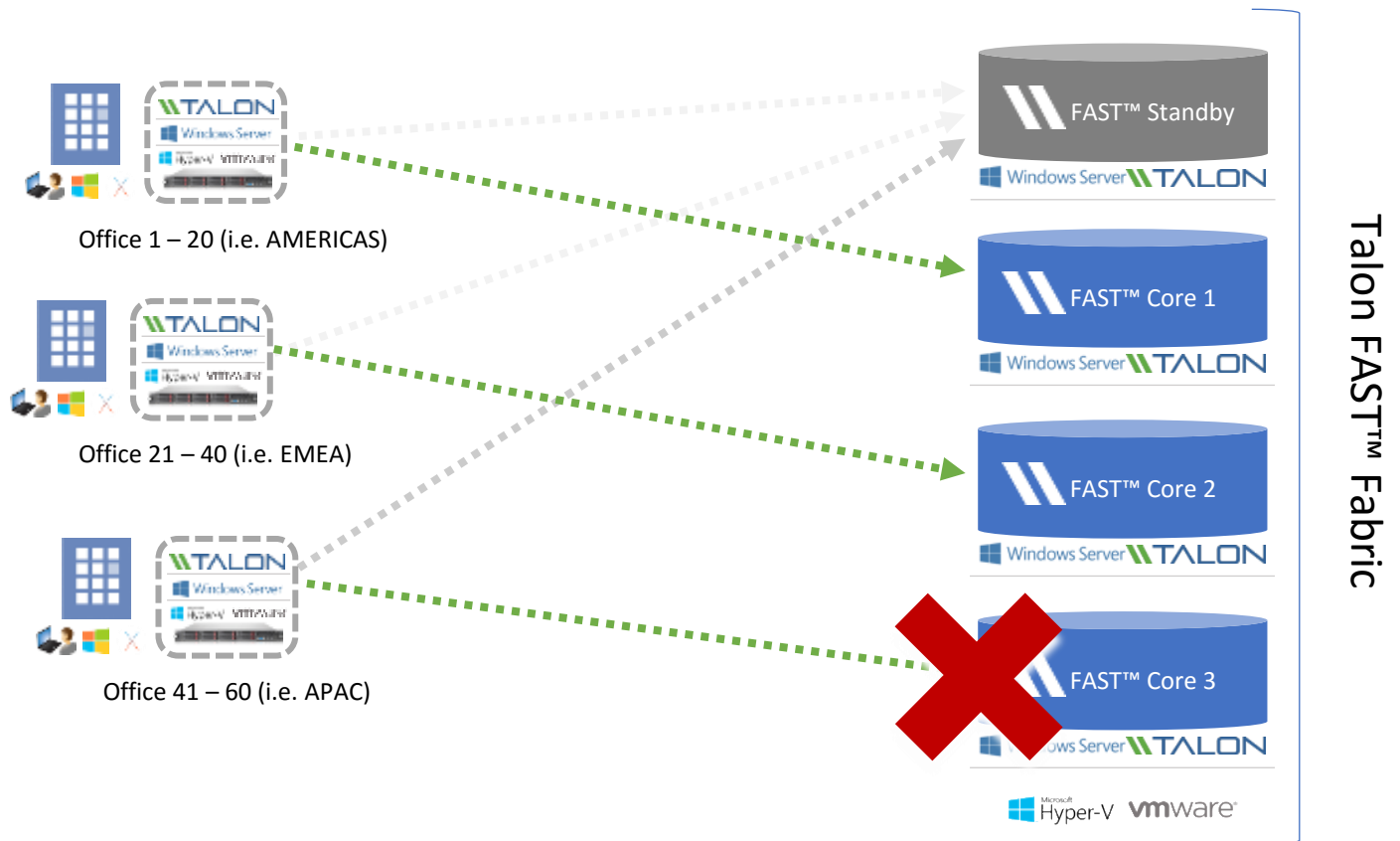
## FAST™ Core Load Distributed design

Enterprise customers that require multiple Talon FAST™ 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, i.e. Microsoft Azure.

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 FAST™ Fabric.

In case a FAST™ core instance fails, and can't be recovered in time, you can 'replace' the failed FAST™ 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, FAST™ Fabric ID configured on the edge).

**Note:** Consult your Talon Solutions Engineer to discuss the best options for your enterprise deployment.



## Configuring FAST™ 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 Talon FAST™ instance is designated the Core role, FAST™ Edge instances will connect to it to access datacenter files server 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/CIFS servers that will be associated with the FAST™ Core instance:

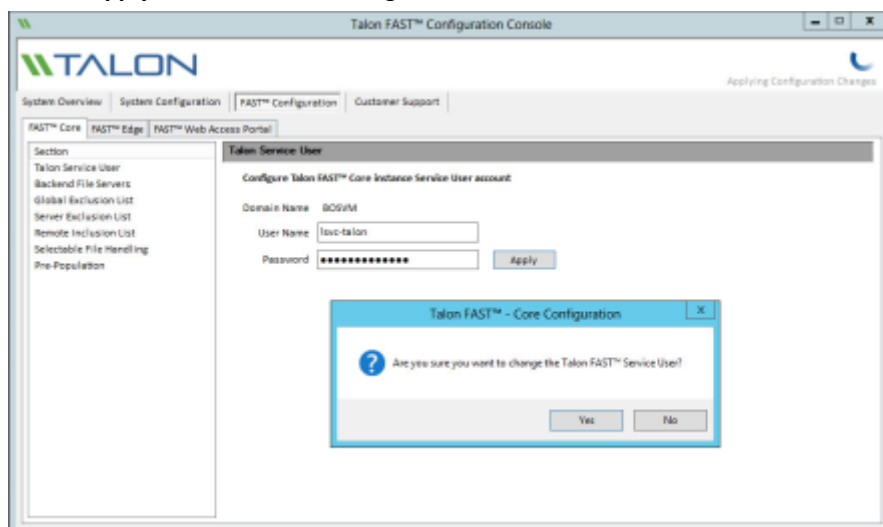
- The provisioned Service Account must be a domain user
  - Depending on the level of restrictions and GPOs in the network environment, this account may require domain admin privileges.
- It must have “Run as a Service” privileges
- The password should be set to “Never Expire”
- The account option “User must change password at next logon” should be DISABLED (unchecked)
- Must be a member of the backend files server local “Backup Operators” groups

**Note:** For backend files servers that are not Microsoft Windows Server-based:

- **NetApp** – The account must be a member of the server’s “Backup Operators” and “Local Administrators” groups.
- **EMC Isilon/VNX** - The service account must be configured to run as “root” on file shares.
- Any shares that will be exposed through Talon FAST™ must allow the “Everyone” group “Full Control” at the share level, while restricting permissions through NTFS permissions.

**To configure the Talon Service Account on your core:**

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

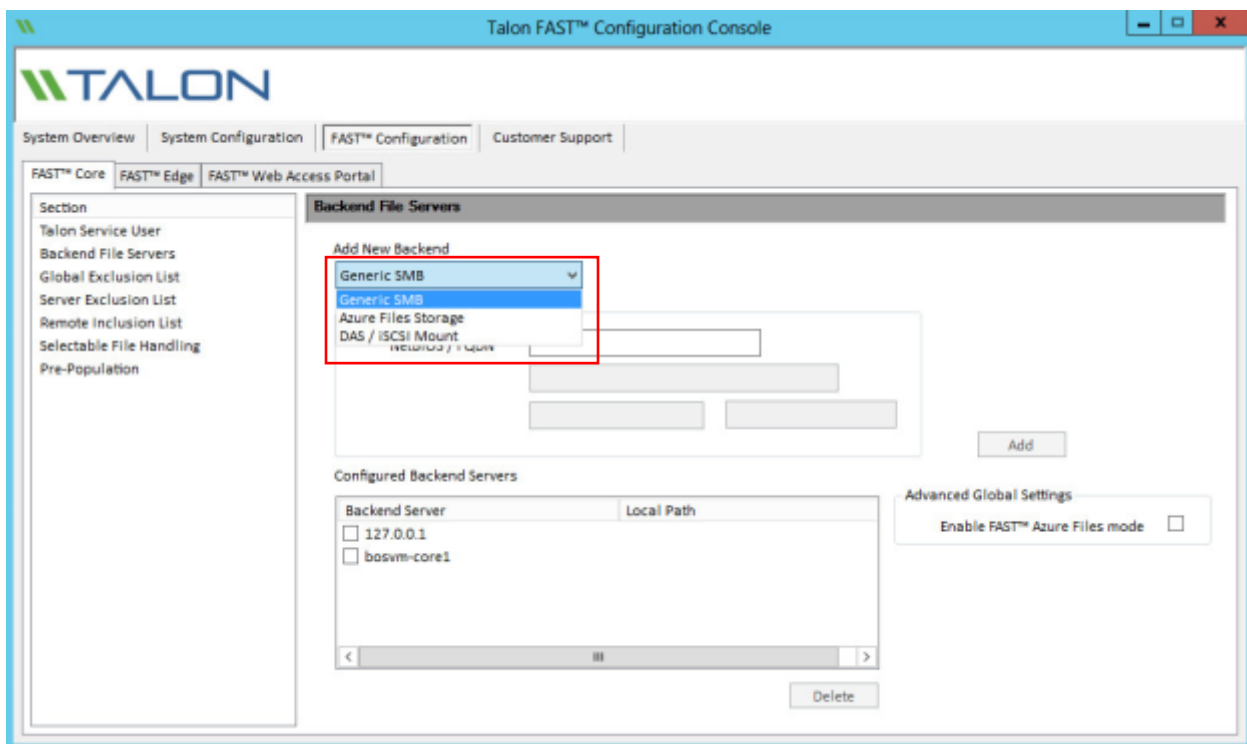


## Configuring FAST™ Core instance – Backend File Servers

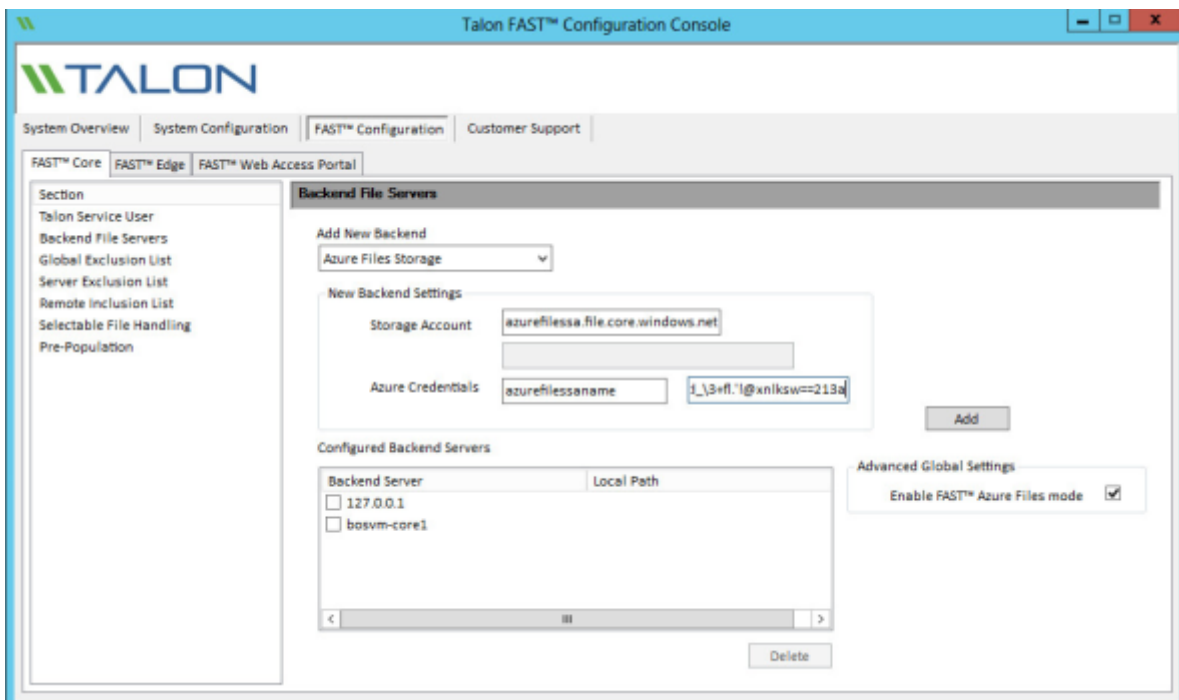
Talon FAST™ core instances extend central file shares from configured datacenter backend file servers. Talon FAST™ can also be configured in multiple ways to present a local share, an iSCSI LUN, or from Microsoft Azure Files.

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

- Click the **“Backend File Servers”** item in the **“FAST™ Core”** tab of the Talon FAST™ Configuration Console or use the **“CIFS Servers Configuration”** step listed in the **“3. FAST™ Core Configuration Steps”** section of the **“Initial Configuration”** assistant
- Select **“Generic SMB”**, **“DAS/iSCSI Mount”**, or **“Azure Files Storage”** depending on the backend file server to be added



- 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 FAST™ Edge servers
- Click the **“Add”** button to add the server to the **“Configured Backend Servers”** list. The changes are applied directly to the FAST™ Core server configuration without displaying a confirmation box
- To add data from a local path or resource (i.e. StorSimple iSCSI, SAN to iSCSI storage, etc.), select **“DAS/iSCSI Mount”** from the dropdown and enter the Storage Name of the resource name as you wish it to display (Ex. StorCloud). Enter the path of the resource (Ex. F:\Data) containing shares and click **“Add”**. The changes are applied directly to the FAST™ 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 Talon FAST™ core instance prior to this configuration.
- To add a Microsoft Azure Files storage share, select **“Azure Files Storage”** from the dropdown menu and check the box labeled **“Enable FAST™ Azure Files Mode”**. Enter the FQDN of the Storage Account for Azure Files. Enter the information in the associated Azure Credentials fields:
  - Left Field - Enter the associated Azure Storage Account Name
  - Right field – Enter the associated Azure Storage Account Primary Key
    - Click **“Add”** to add the Azure Files Storage Account to the Configured Backend Servers list



**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.

## FAST™ Core Advanced Options

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

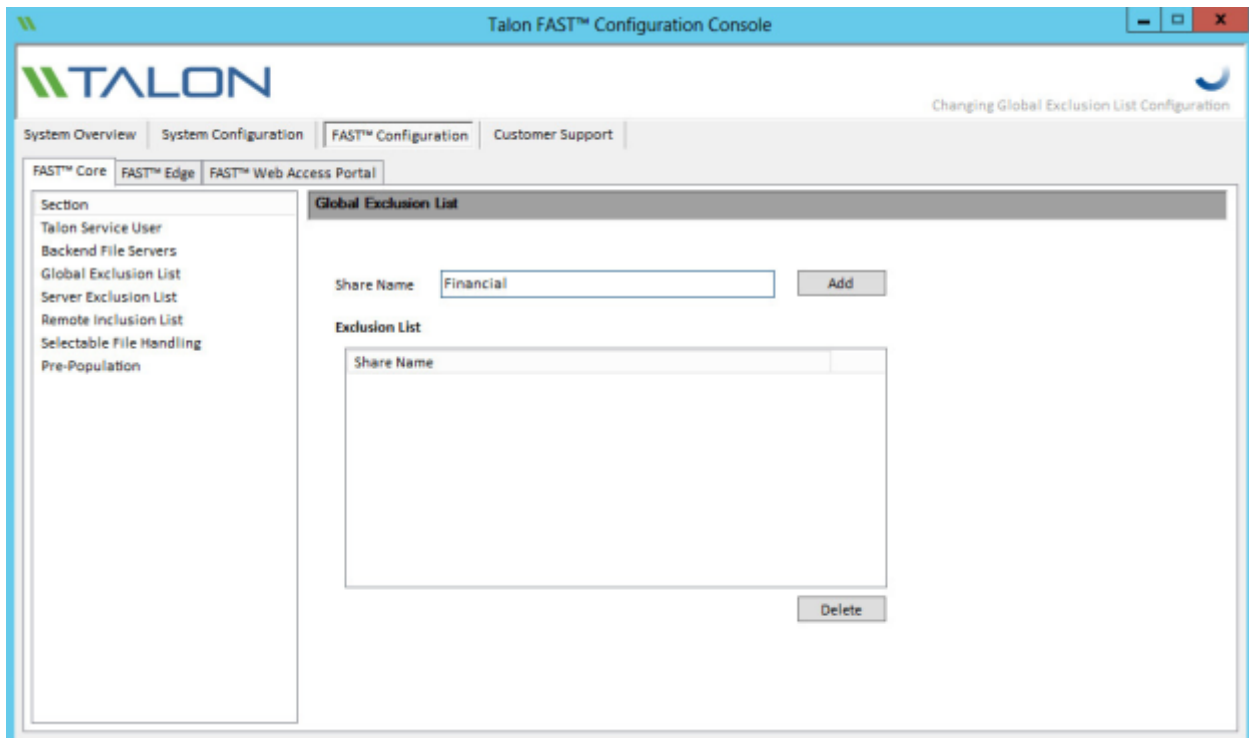
### Global Exclusion List

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

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

#### To hide named shares from all Edge instances

- Open the “Talon FAST™ Configuration Console”
- Select the “FAST™ Configuration” tab. Ensure that the “FAST™ Core” tab is active.
- Click “Global Exclusion List”
- Enter a “Share Name” to prevent distribution through Talon FAST™
- Click “Add” to add a share name to the exclusion list
  - Once added to the list, the change is applied



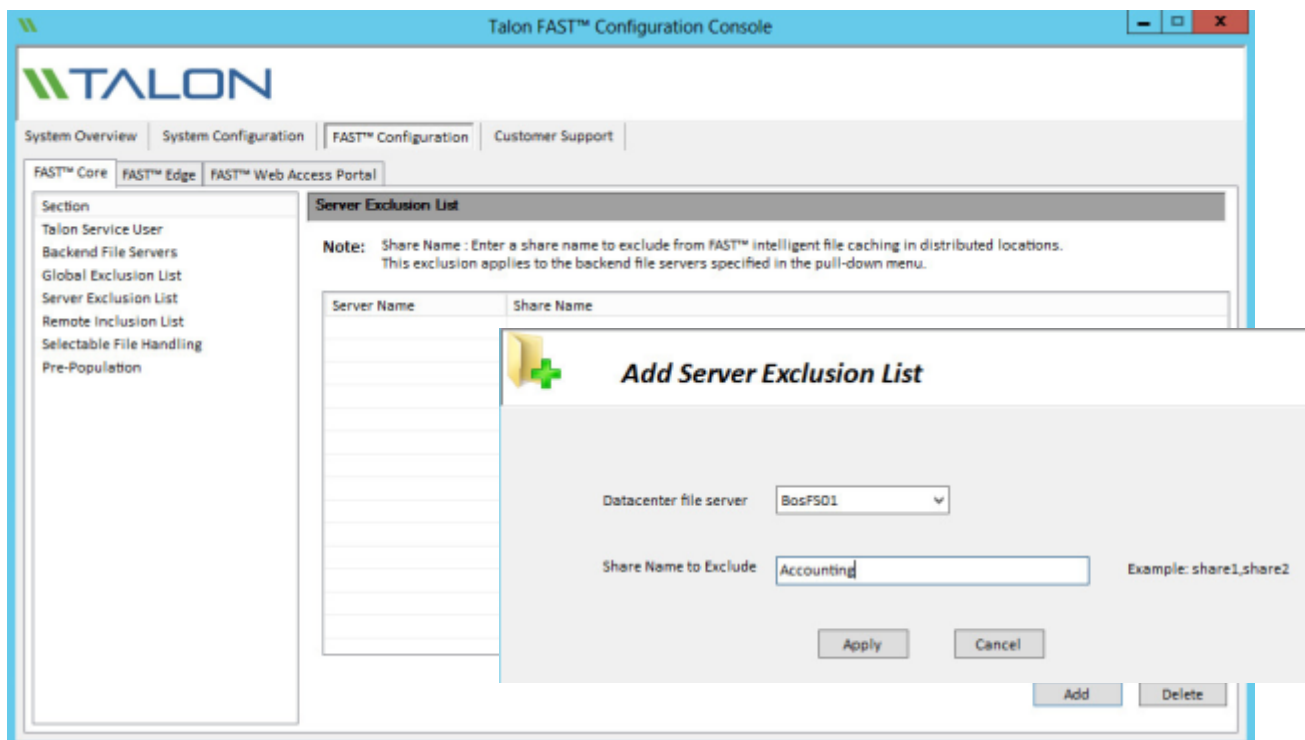


## Server Exclusion List

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

### To hide specific shares from all Edge instances

- Open the “Talon FAST™ Configuration Console”
- Select the “FAST™ Configuration” tab, and select the “FAST™ Core” tab
- Click “Server Exclusion List”
- Click the “Add” button to display the “Add Server Exclusion List” window
- Select the desired backend file server from the dropdown menu
- Enter a “Share Name” to prevent distribution through Talon FAST™
- Click “Apply” to add a share name to the exclusion list
  - Once added to the list, the change is applied
- Repeat this process for each server and share combination you wish to exclude

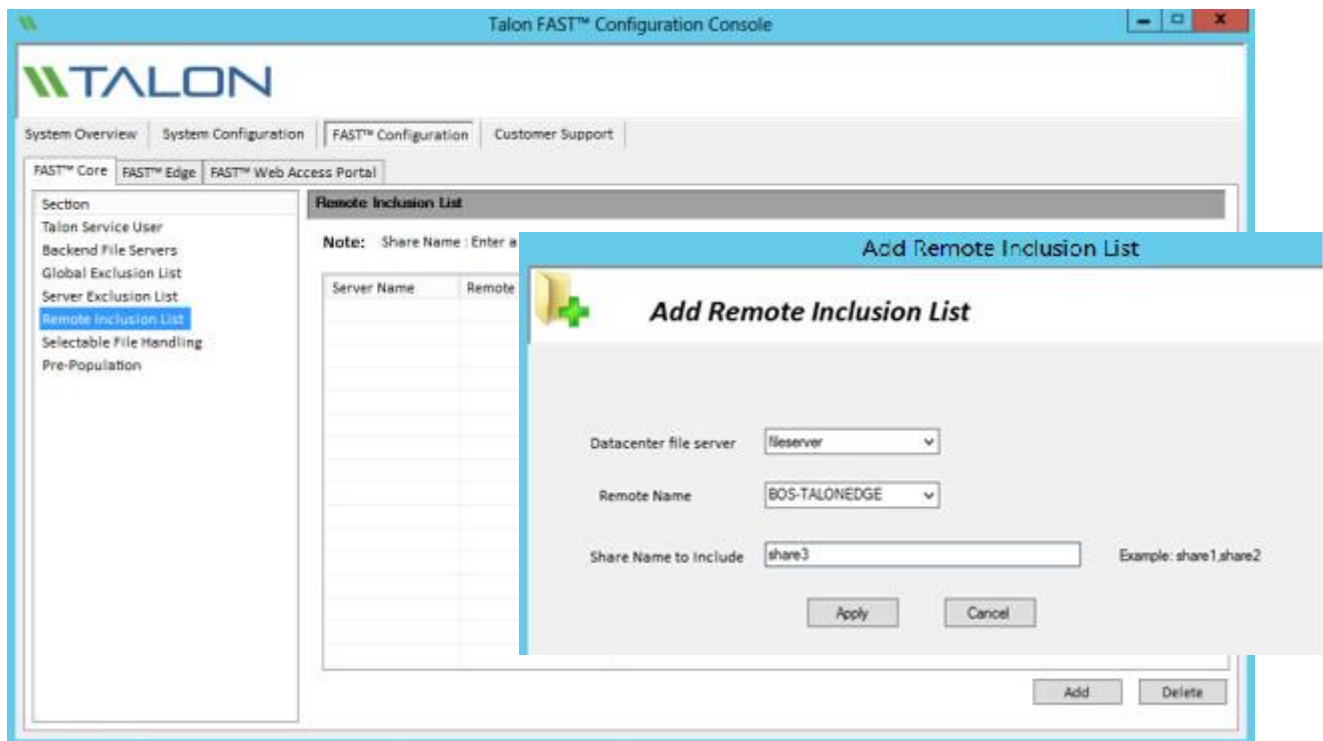


## Remote Inclusion List

The Remote Inclusion List feature in Talon FAST™ 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

- Open the “Talon FAST™ Configuration Console”
- Select the “FAST™ Configuration” tab, and select the “FAST™ Core” tab
- Click “Remote Inclusion List”
- Click the “Add” button to display the “Add Remote Inclusion List” window
- Select the desired backend CIFS file server from the dropdown menu
- Select a target Edge server “Remote Name” from the second dropdown menu
- Enter a “Share name to include” that exists on the datacenter file server in the dropdown menu
- Click “Apply” to add a share name to the inclusion list
  - Once added to the list, the change is applied
- Repeat this process for each server and share combination you wish to include

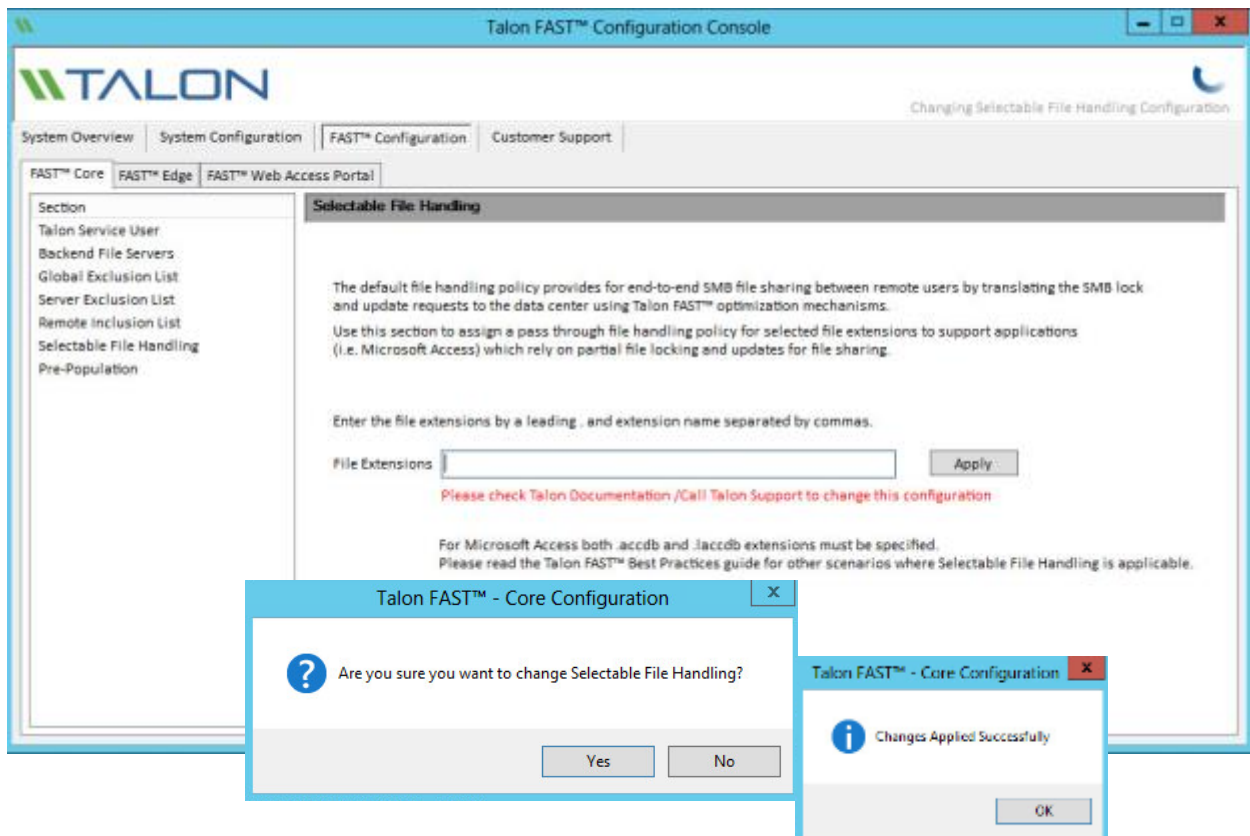


## Selectable File Handling

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 Talon FAST™, 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

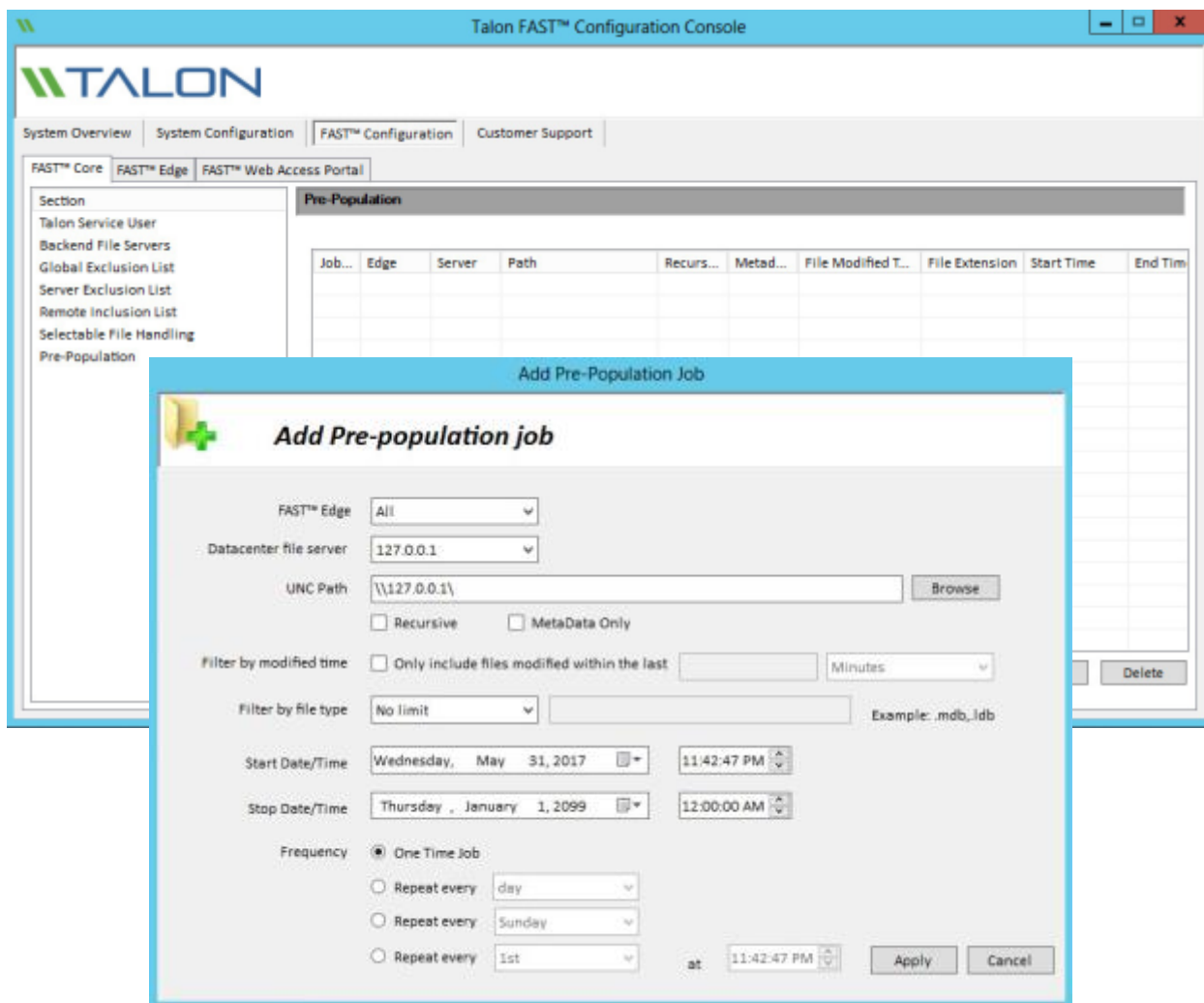
- Open the **Talon FAST™ Configuration Console**
- Select the **“FAST™ Configuration”** tab, followed by selecting the **“FAST™ Core”** tab
- Click **“Selectable File Handling”**
- Enter the file type extensions (used by the application) separated by commas and preceded by a period in the **“File Extensions”** text box
- Click **“Apply”** to apply the settings, a confirmation box will appear
- Click **“Yes”** to apply the changes immediately



## Core Pre-population

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 FAST™ 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 Core or Edge instance, which triggers data fetches from the associated FAST™ Edge server(s). All times associated with pre-population correspond to the Edge server’s local time.



**Note:** You must have at least one datacenter file server configured for the FAST™ core instance before you can define, schedule, or edit pre-population jobs.

### Pre-Population (continued)

The Pre-Population page displays a list of data push jobs scheduled from the Core to the FAST™ Edge servers. The Pre-population window displays the following information for each scheduled pre-population job.

Field name	Description
<b>JobID</b>	An automatically generated job identification number
<b>Edge</b>	Name of the FAST™ Edge server to be pre-populated with data (or All if data will be pushed from the specified server to all Edge servers)
<b>Server</b>	Name of the data center file server
<b>Path</b>	Path of the folder on the data center server with information to be shared, for example, \\myserver\folder\sharefolder
<b>Recursive</b>	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, <u>only</u> the specified folder will be pre-populated.
<b>Metadata Only</b>	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.
<b>File Modified Time</b>	File modification times, if only data with specific modified by dates are to be pre-populated
<b>File Extensions</b>	File extensions of any file types to be specifically included in or excluded from the Pre-population job
<b>Start Time</b>	Start time of the pre-population job (Edge server local time)
<b>End Time</b>	End time of the pre-population job schedule (Edge server local time)
<b>Frequency</b>	Displays 'One Time' if a single job or displays the frequency of a recurring job

## To Configure and Schedule a Pre-Population Job

- Open the Talon FAST™ Configuration Console
- Select the “FAST™ Configuration” tab and then select the “FAST™ Core” tab
- Click “Pre-Population”
- Click “Add” from the Pre-population page. The “Add Pre-Population Job” window opens
  - Click the **FAST Edge** drop-down menu, and select a FAST™ Edge server to receive the files, or choose ‘All’ to pre-populate files to all of the FAST™ Edges connected to the FAST™ Core.
  - From the **Datacenter File Server** drop-down menu, select the file server with the data to be pre-populated
  - 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>).
  - (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
  - (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
  - (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, hours, or days in the box
  - (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
  - 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 20 minutes in advance and the End Time field should be set 24 hours later.
  - (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.
  - 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.

- 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.
- 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 31<sup>st</sup>.
- Click “**Apply**” to commit the pre-population job
- The “**Add Pre-Population Job**” window will close, and the new job will display in the table on the Pre-population page
- To configure a second scheduled pre-population job, repeat the process
- To edit a Pre-population job, click to highlight the job you wish to change and click the “**Edit**” button to change parameters
- Jobs can be deleted by highlighting the desired job and clicking the “**Delete**” button and confirming the action

**Notes:**

- When scheduling pre-population jobs, all job times are relative to the time zone of the FAST™ Edge instance
- Pre-population jobs should be scheduled at least 20 minutes ahead of the current time in the Edge’s local time zone to allow Edges to pick up the newly scheduled jobs
- Pre-population jobs should be scheduled to run during non-business hours. Running pre-population jobs during business hours will impact user performance

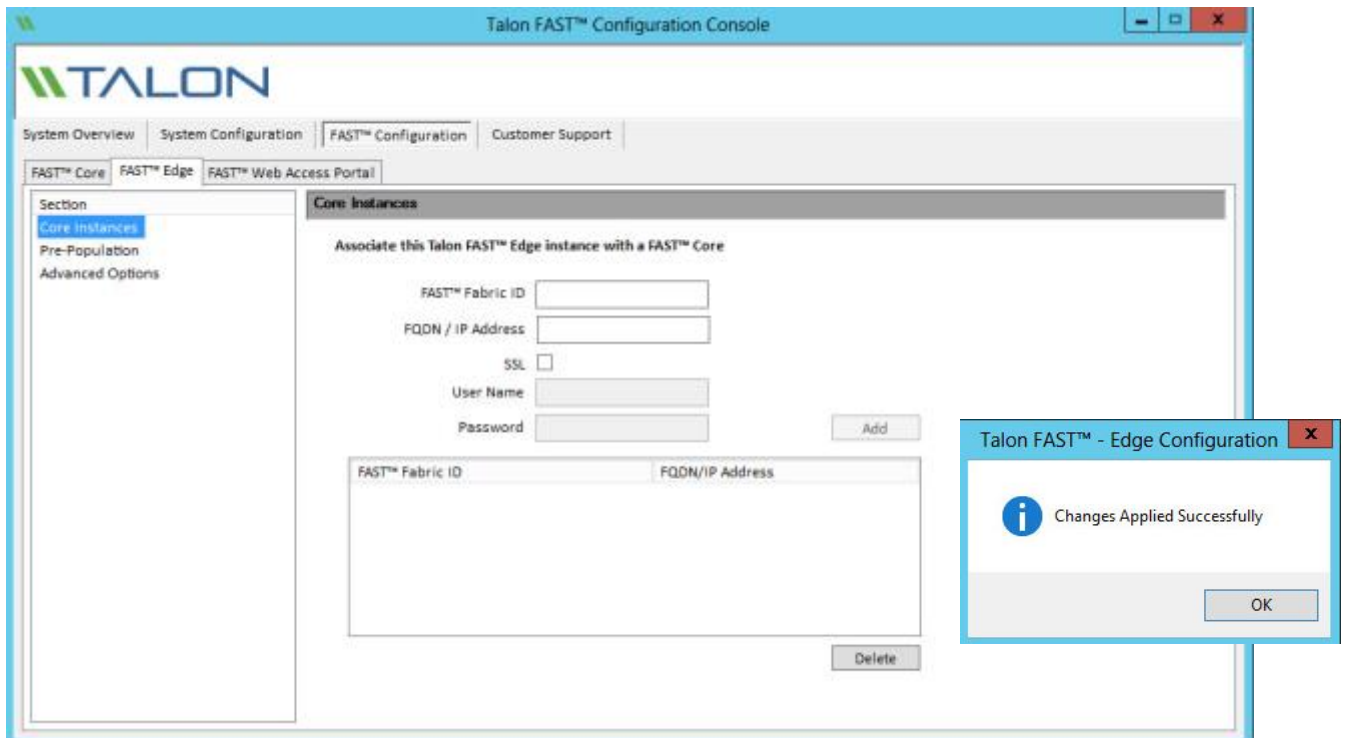
## Configuring the Talon FAST™ Edge Role

**Note:** The Edge instance must be licensed prior to beginning the configuration. For more information on licensing, see section 4 for “Registering your Core or Edge instance with FAST™ LMS”

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

To configure the Edge Instance Role:

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





## Edge Pre-population

One-time or recurring pre-population jobs can be configured on an Edge instance.

**Add Pre-Population Job**

**Add Pre-population job**

Core FAST™ Appliance ID

Path

Recursive  MetaData Only

Filter by modified time  Only include files modified within the last  Minutes

Filter by file type  Example: .mdb, .ldb

Start Date/Time  12:01:29 PM

Stop Date/Time  12:00:00 AM

Frequency  One Time Job

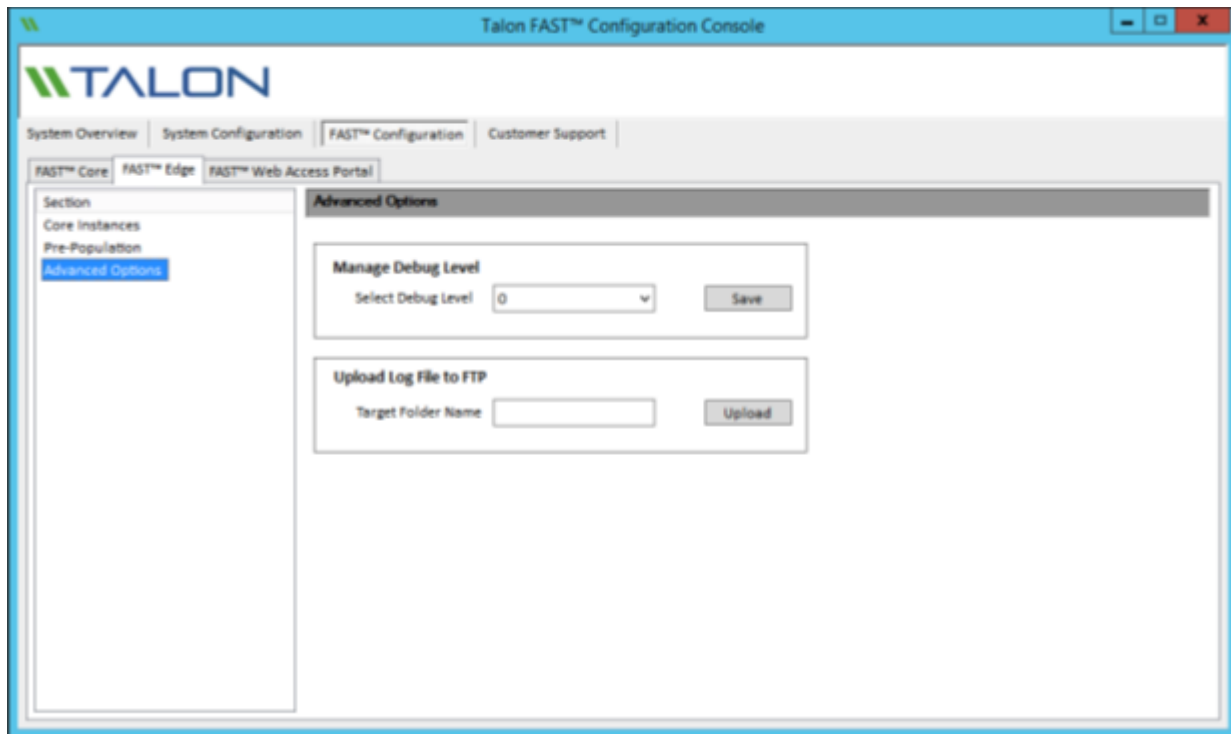
Repeat every

Repeat every

Repeat every  at

For more information, refer to the “Core Pre-population” section of this document.

## Edge Advanced Options



### Manage Debug Level

This feature allows for more verbose (higher numbers, MAX: 9) debug logging. This setting should only be adjusted when advised by Talon Support.

### Upload Log File to FTP

This feature enables a direct transfer of requested log files to Talon Support. This feature should only be used when advised by Talon Support.



## 7. 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' Talon FAST™ 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)

### 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. \\<Talon FAST edge>\<FASTData>\<FAST Fabric ID>\<file server>\<share>\<folder

## Configure Windows Server 2012 R2 Domain-Based DFS for Talon FAST™

### Objectives:

- Provide a unified namespace solution for both Talon FAST™ 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

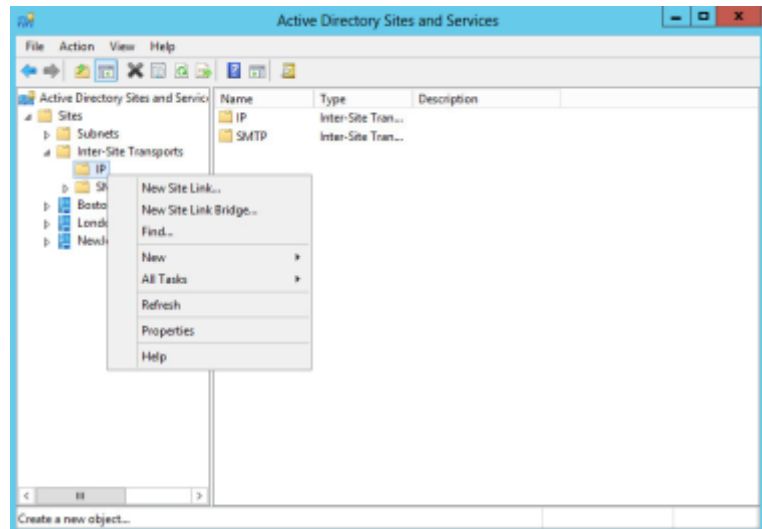
## Site Definitions and Site Links

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.

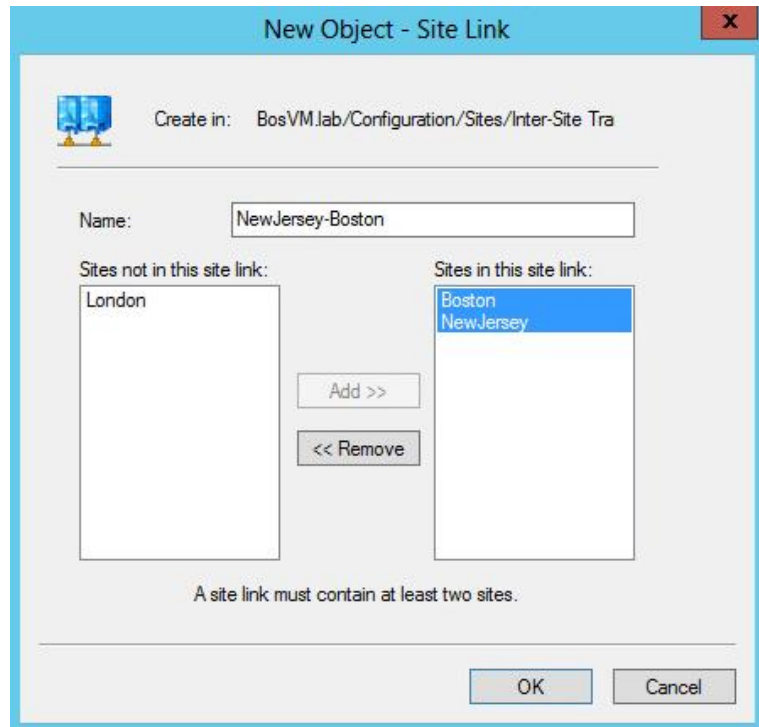
### Step 1: Create Site Links: (if more than two sites)

1. Open *Active Directory Sites and Services*
2. Expand “Inter-Site Transports”
3. Right click “IP”
4. Select “New Site Link”
5. Type a name describing which sites will use this link  
(i.e. NewJersey-Boston)



6. Select sites from “Sites not in this site link”
7. Click “Add”
8. Click “OK”

Repeat steps 3-8 for each site link that needs to be created.



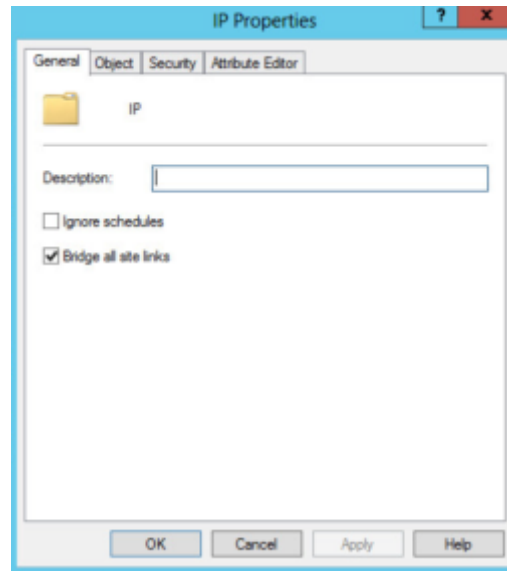
**Step 2: Configure “Query Policy” and Global Catalog:**

1. Double click on a site
2. Double click “Servers”
3. Select available Domain Controller within the site
4. Right click “NTDS Settings” and select “Properties”
5. Set the Query Policy to “Default Query Policy”
6. Check “Global Catalog”
7. Click “OK” to commit the changes.



### Step 3: Bridge Links:

1. Return to the main screen and double click "Inter-Site Transports".
2. Right click "IP" and select "Properties"
3. Confirm "Bridge all site links" is checked.
  - If it is not checked, closest site selection will fail.
4. Click "OK" to commit the changes.
5. Close "Active Directory Sites and Services"



## 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 2008 R2 or 2012 R2 server, you can generate the following structure as follows. In the exhibit below we are using "\\BosVM.Lab\DFSroot" as a namespace, and "Talon Fast" as a target referral.

### 1. Install the DFS management snap-in

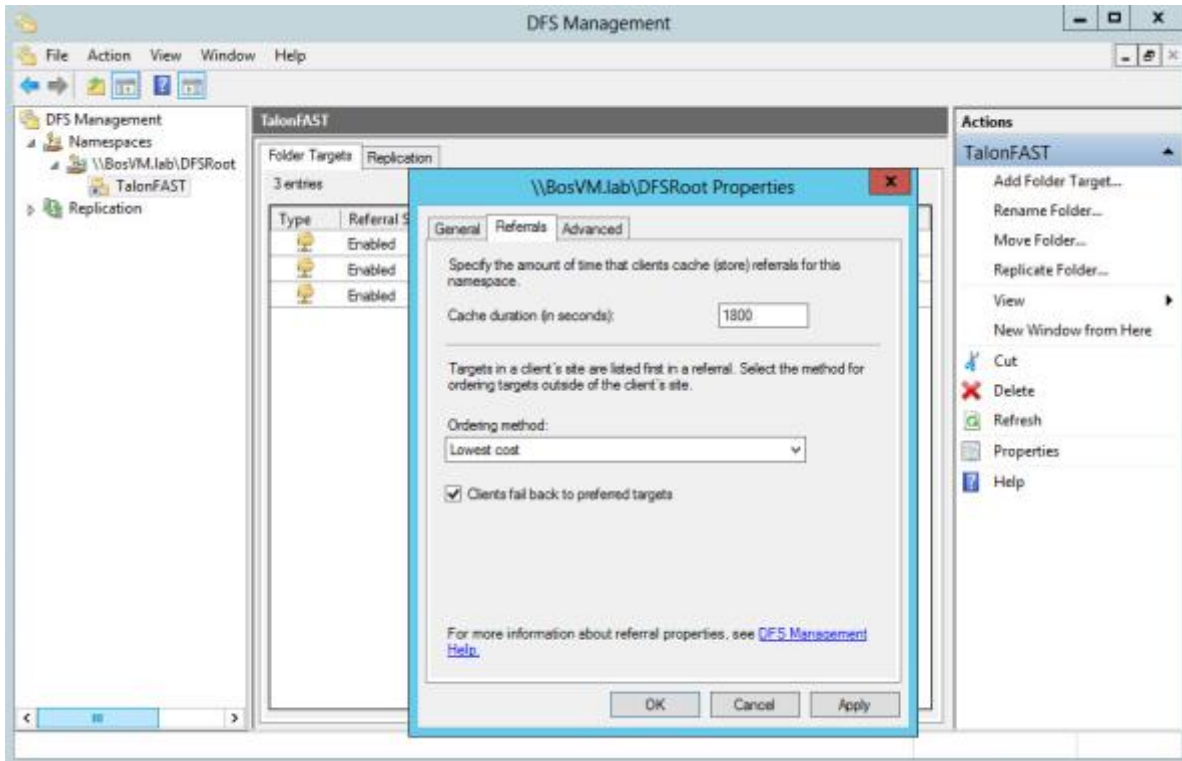
The DFS Management snap-in has been included since Windows Server 2003 R2, and allows extensive configuration of a DFS infrastructure. In order to comply with Talon FAST™ best practices you should use the management snap-in. This is installed while adding the DFS Namespaces role via the Server 2008 R2 or 2012 R2 "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&MSPPError=-2147217396#BKMK\\_UI](https://msdn.microsoft.com/en-us/library/cc731089.aspx?f=255&MSPPError=-2147217396#BKMK_UI)

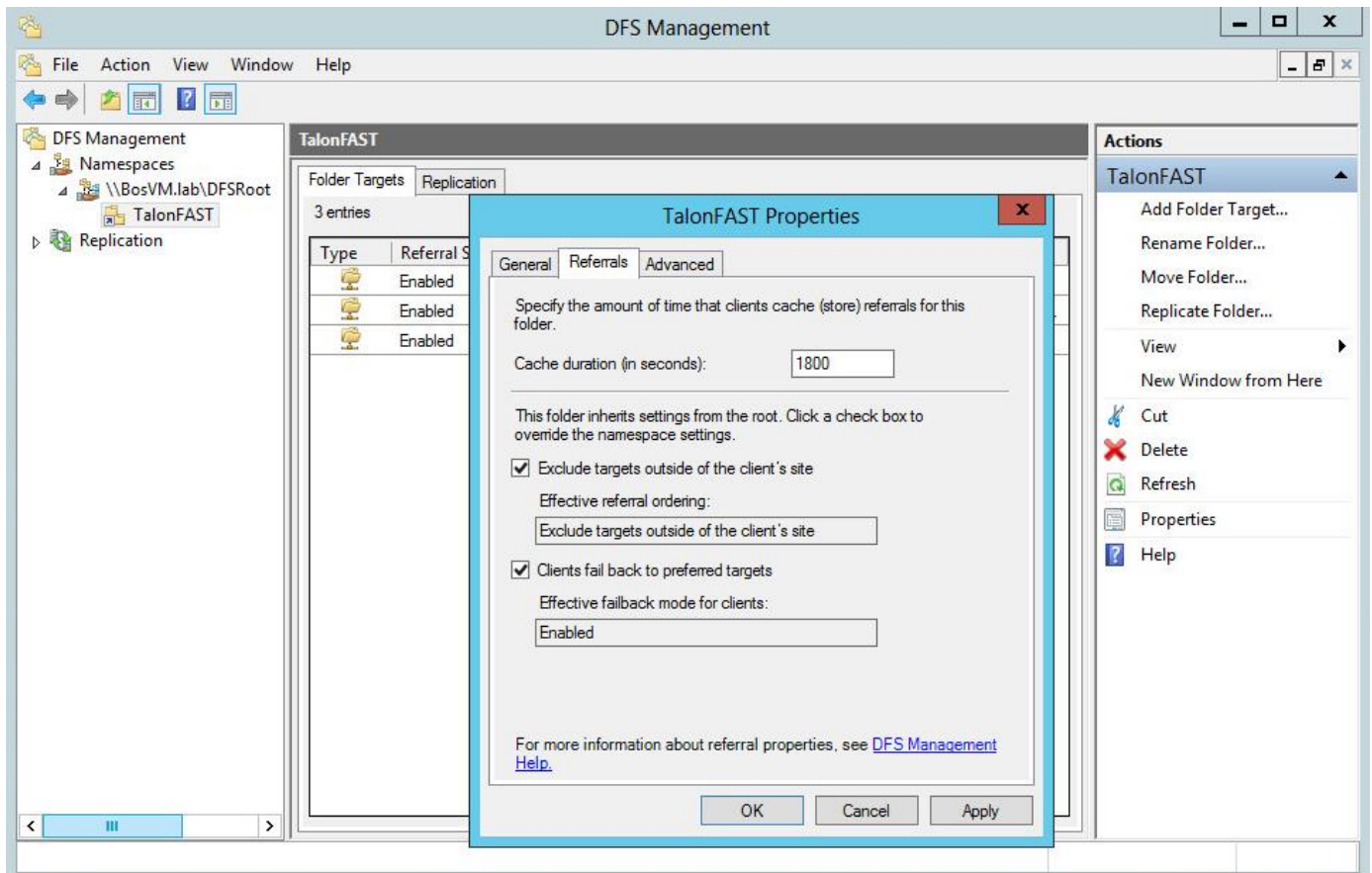
## 2. Configure the DFS namespace as follows

- 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

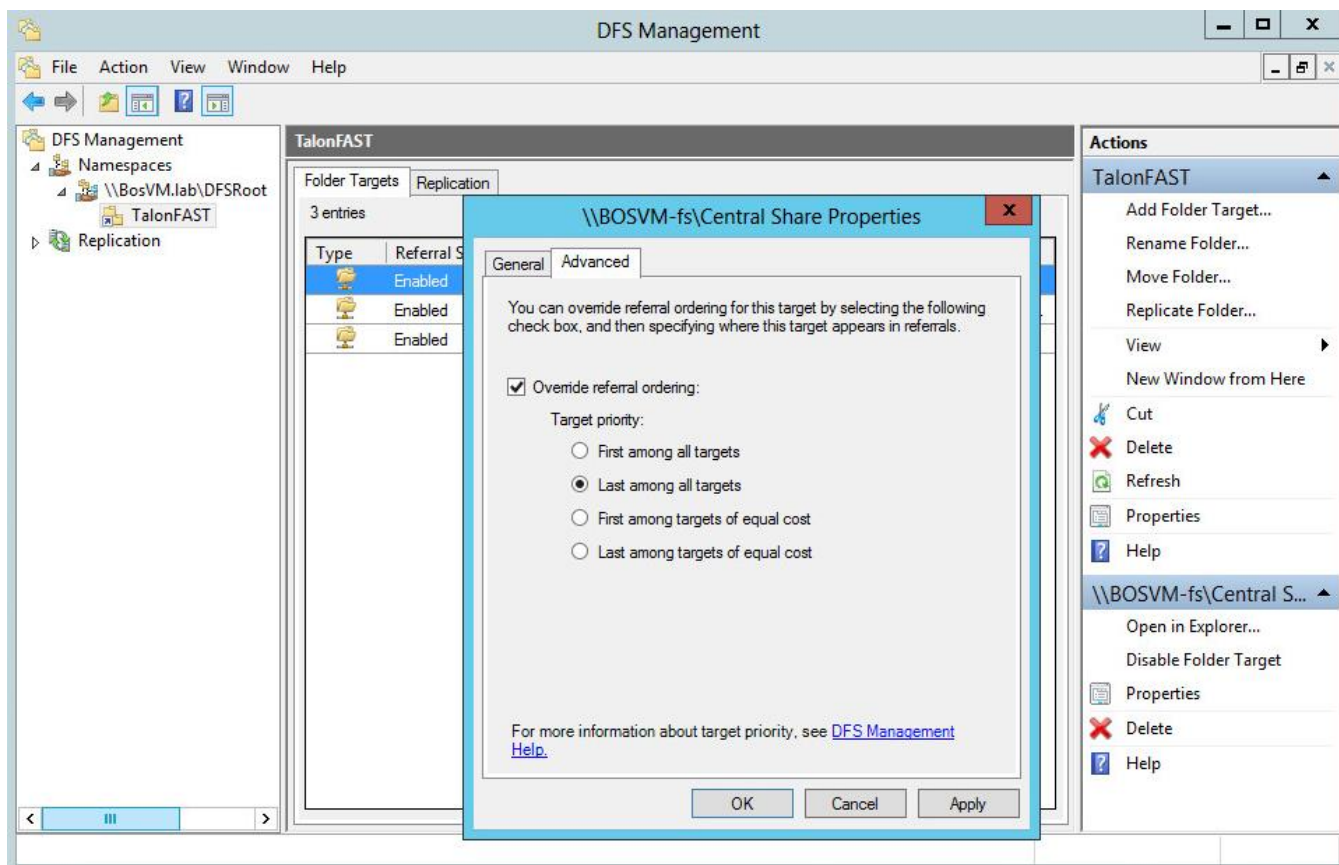
- Right-click the referral "Talon Fast" and select "properties"
- For the "Talon Fast" referral, check the box for "Exclude targets outside of the client's site" and "Clients failback to preferred targets"
- Set the Cache duration to 1800 seconds
- Click OK to confirm the configuration change





4. Open the Target Referrals listed in the "Talon Storage" 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 Talon FAST™ 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.

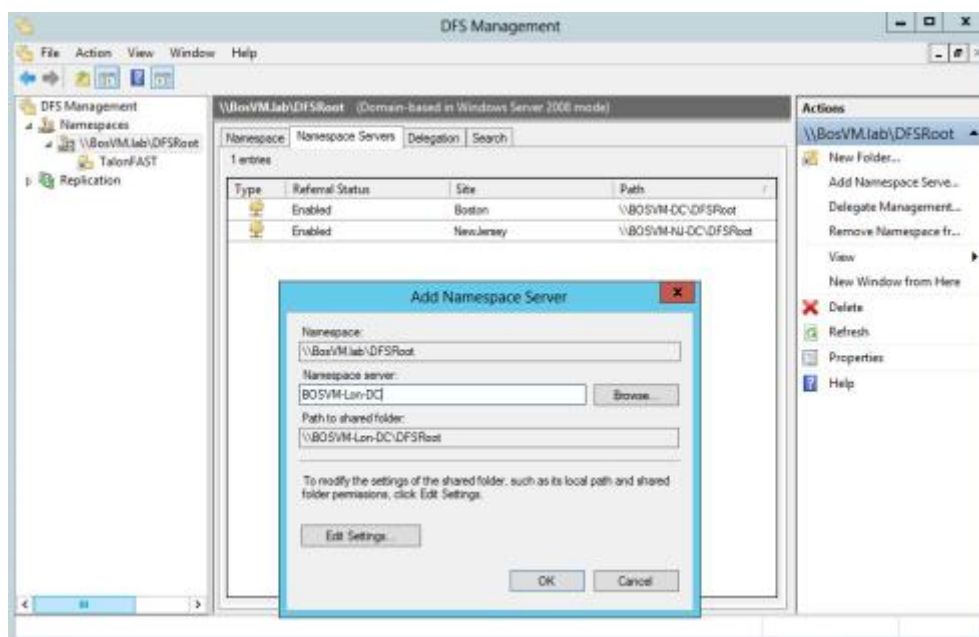
**Make sure that your target referral list contains the FQDN of the referral path.**

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

## 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:

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



**Important: Windows Server 2008 R2 Standard only allows a single namespace replica. All enterprise versions of Server 2012 R2 and above allow multiple Domain-Based DFS roots.**

## Conclusion:

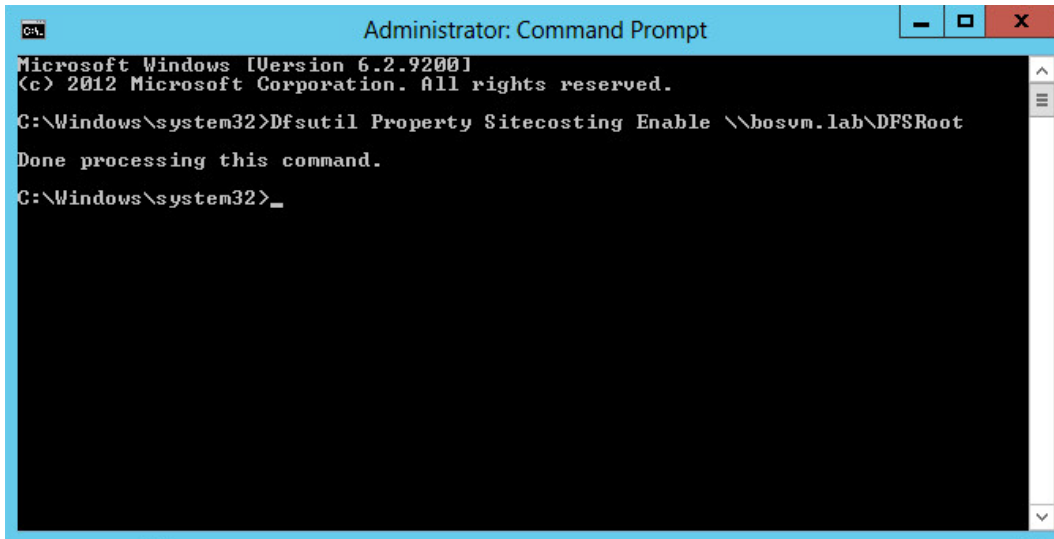
By using the FQDN as a UNC path, you will introduce a unified namespace and failover solutions for all users in your enterprise network. This simplifies the process of managing data structures, collaborating data between users, and mapping drives on Microsoft Windows clients.

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.

## Site Costing Configuration

For closest site selection to work on link targets, Inter-site Topology Generator (ISTG) must be running on Windows Server 2012 R2, and for closest site selection to work on link and root targets, all domain controllers must be running Server 2012 R2. Please use DFSUTIL.exe from the command line to enable site costing:

### Windows Server 2012 R2 : Dfsutil Property Sitecosting Enable \\bosvm.lab\DFSroot



```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\Windows\system32>Dfsutil Property Sitecosting Enable \\bosvm.lab\DFSroot
Done processing this command.
C:\Windows\system32>_
```

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**

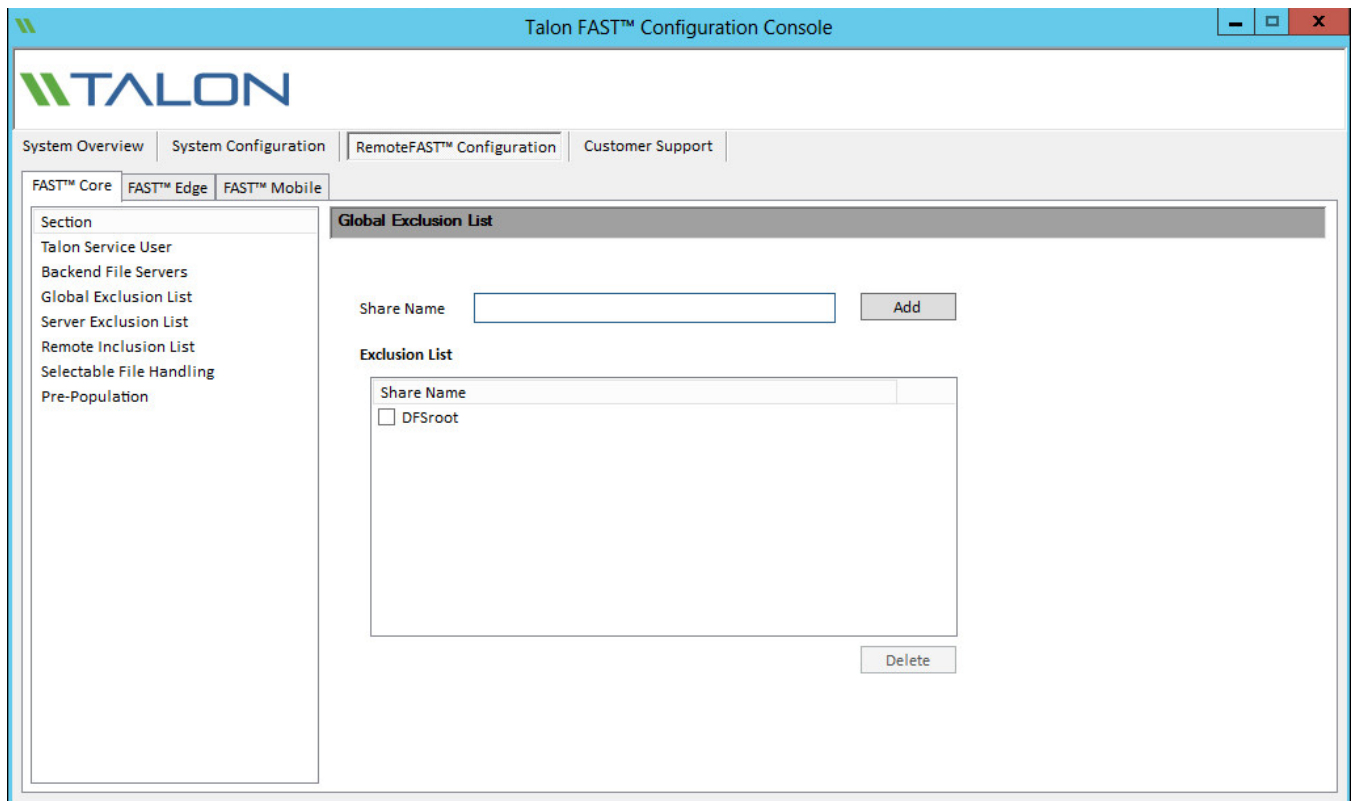
Please validate that the registry entry is applied, and schedule a reboot of the respective DC

## Talon FAST™ Global Exclusion Configuration (DFS)

When the DFS root is being hosted by the same backed file server that you are configuring for optimization with Talon FAST™, 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 Talon FAST™, you should exclude the “DFSroot” share.

This can be adjusted in the “Global Exclusion List” configuration on the Talon FAST™ Core configuration page.



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



## 8. Central Monitoring using Microsoft SCOM

Talon FAST™ supports integration with Microsoft Systems Center Operations Manager (SCOM) in order to manage different aspects around the solution and integration with Microsoft Windows Server.

This “Talon FAST™ Management Pack” release includes the following aspects:

- **Operational Management**
  - Systems level inventory
  - Patch level inventory
  
- **Availability Management**
  - Systems Health Status
  - Event Viewer
  - SCOM alerting
    - i.e. Key services not running
  
- **Systems Optimization**
  - % Cache Utilized
  - Cache Purge alert via SCOM

### Dependencies:

- Windows Server 2012 R2
- Systems Center Operations Manager 2012, 2012 R2 (SP1)
- Administrative Credentials to manage SCOM Operations Manager Console
- Systems Center Management Pack for Windows Server Operating System
- Windows Computer Management Pack
- Talon FAST™ 3.x or later Software
- Latest Talon FAST™ Management Pack

**Important:** Before installing Talon FAST™ .mpb file, you have to install "SC Management Pack for Windows Server Operating System.msi" which can be downloaded from, <https://www.microsoft.com/en-us/download/details.aspx?id=9296>

**Note:** If a previously existing management pack is deleted, please wait for 48 hours to re-import the management pack. Otherwise, health rollups may not functional correctly. For additional information, please visit <http://www.vroege.biz/?p=768>

## Deploying Talon SCOM Management Pack

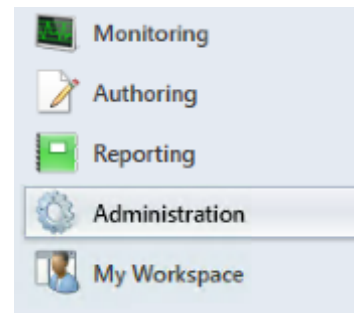
This section describes installing and upgrading the Talon FAST™ SCOM management pack. You can install or upgrade the Talon FAST™ SCOM management pack by copying the management pack files to the SCOM server instance and following the steps outlined below.

**Download the latest software update from <http://www.talonstorage.com/support/downloads>**

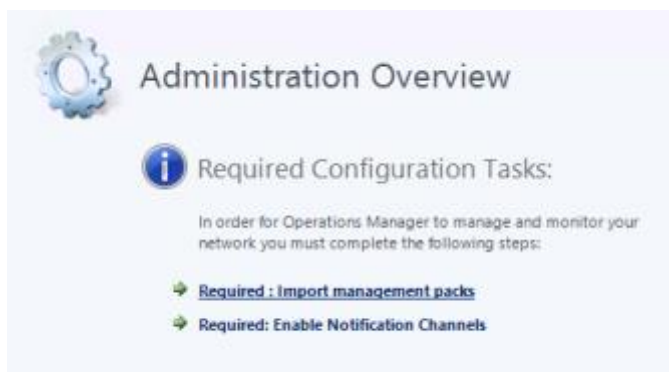
The Talon SCOM management pack includes an .mpb file that needs to be imported within your Microsoft Systems Center Operations Manager 2012 R2 Operations Management Console.

In order to implement the management pack, follow these steps:

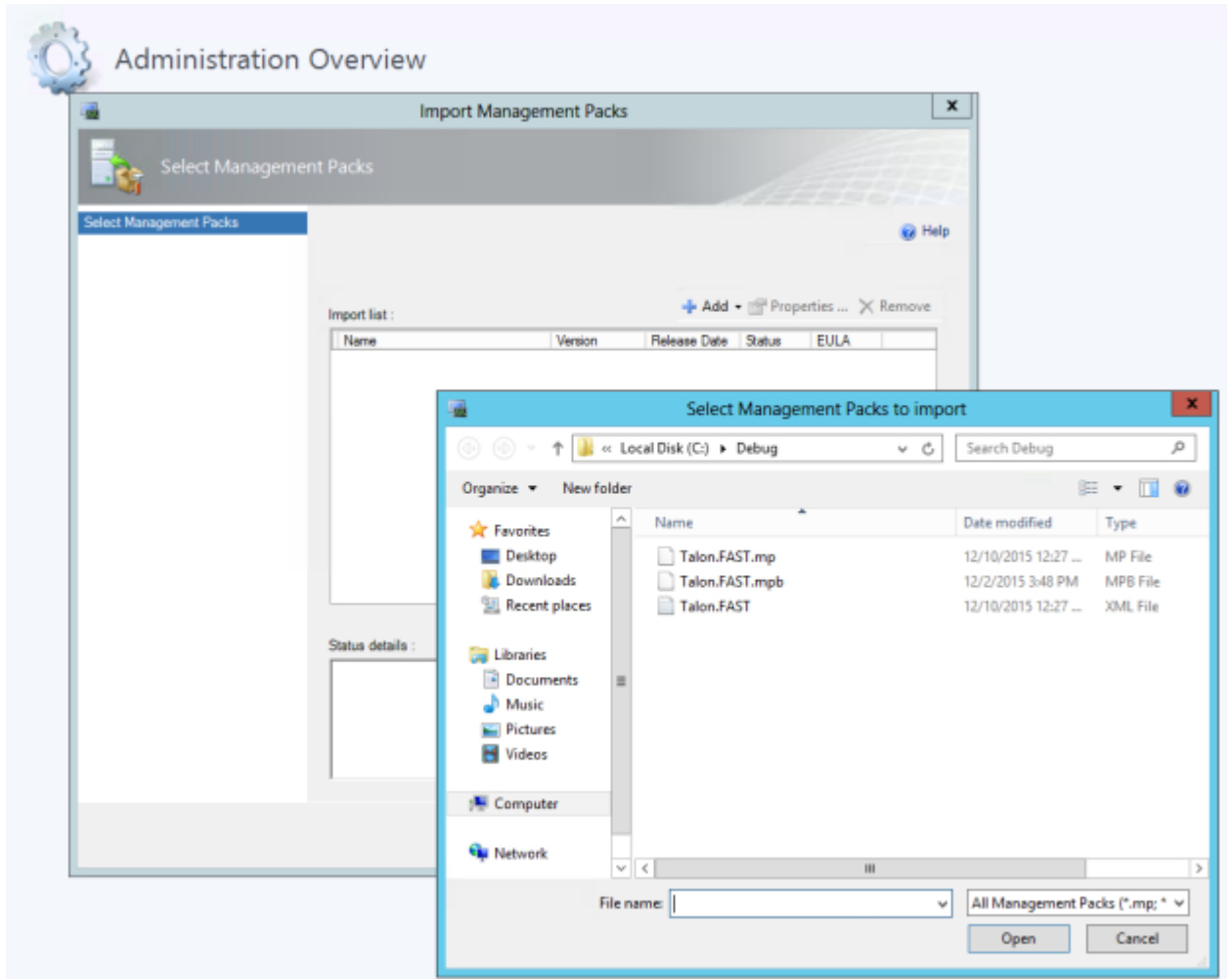
1. Open the Microsoft Operations Management Console
2. In the left-bottom window pane, select 'Administration'



3. Within the 'Administration Overview' section of the management console, select the 'Import Management Packs' option



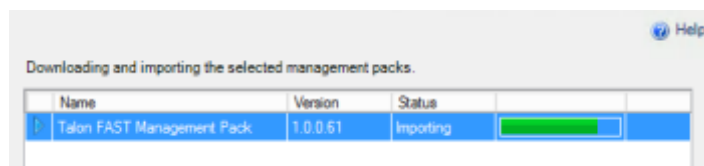
4. Select 'Add from Disk' from the 'Import Management Packs' console and navigate to the latest management pack file (i.e. Talon.FAST.mpb file)



5. Click 'Open' to confirm the selection.
6. The management pack will be listed in the 'Import List' section and will be validated

**Note:** If you are upgrading the Talon FAST™ SCOM Management Pack, you can commit the upgrade in-place.

7. Once confirmed, the 'import' process will take approx. 10-15 minutes to complete.





## Dashboards and Reports

Talon SCOM Monitoring Console contains the following dashboards and overviews associated with the FAST™ software. From within the console, select the 'Talon Service Monitoring' folder. This folder contains all of the monitored aspects of the Talon FAST™ software and is organized as follows:

### Talon Service Monitoring

- **Service Dashboard**
- **Service Overview**
- **Core Instances**
  - Core Servers
  - Error and Warning Logs
  - TService Backend Status
  - TUM Monitoring
  - FAST™ Service
    - FAST™ Service Alerts
    - FAST™ Service Inventory
  - File Transfer
    - Event Log
- **Edge Instances**
  - Edge Servers
  - Error and Warning Logs
  - Total Connected Users
  - TUM & TAPP Monitoring
  - Cache Monitoring
    - Cache Cleaner
    - Edge Server Cache Disk Free Space
  - FAST™ Service
    - FAST™ Service Alerts
    - FAST™ Service Inventory
  - File Transfer
    - Event Log



## Personalized Views

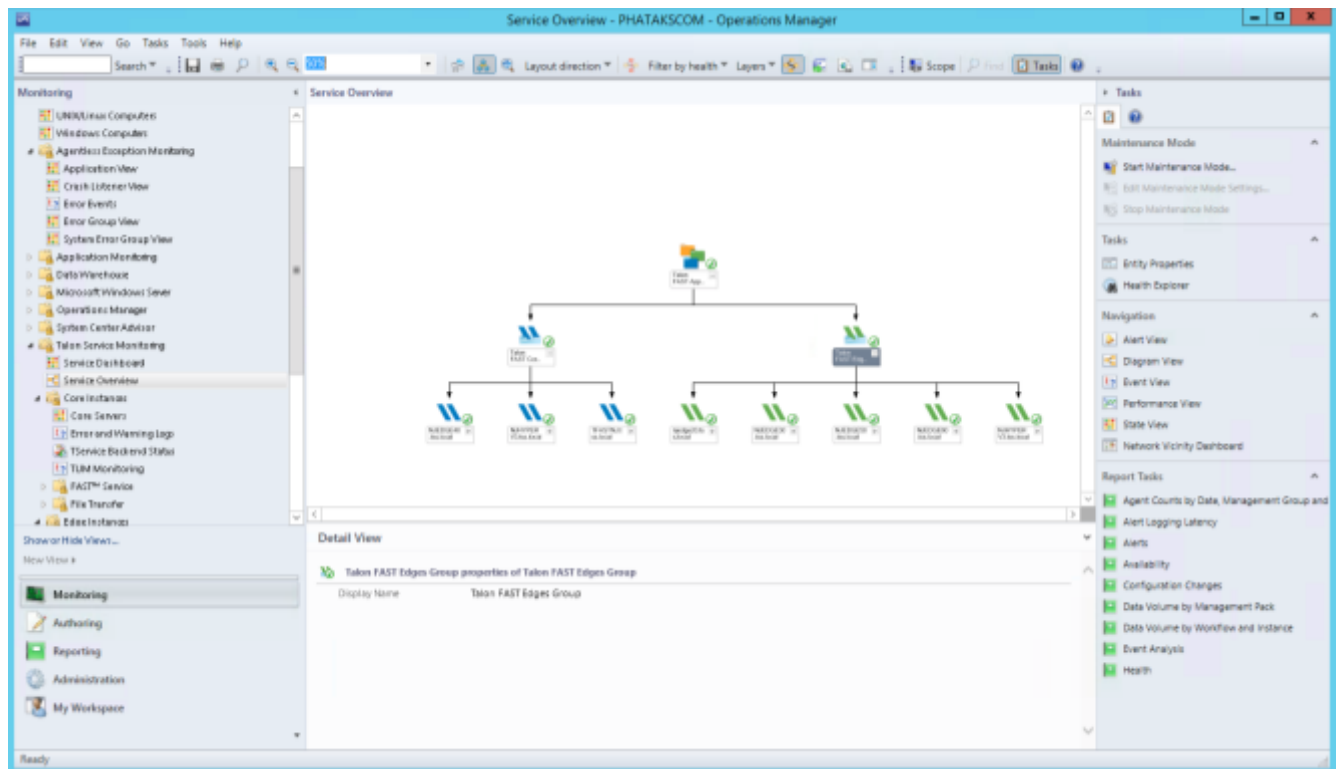
Microsoft Systems Center Operation Manager 2012 provides dashboards and views that can be modified to show or hide the most relevant information for IT administrators. By using this functionality, called 'Personalized Views', you can show or hide specific pieces of information such as the Name of the server, if it's in Maintenance Mode, the state of Talon FAST™ services, etc.

### Service Dashboard

The service dashboard contains a list overview of all Talon FAST™ instances including parameters concerning their health and general configuration. This list includes configuration parameters for both FAST™ Core and Edge roles.

### Service Overview

The service overview contains a logical graphically organized overview of all Talon FAST™ instances divided into groups of FAST™ Cores and Edges. This provides users with a high level overview of the structure and general health of all Talon FAST™ instances.

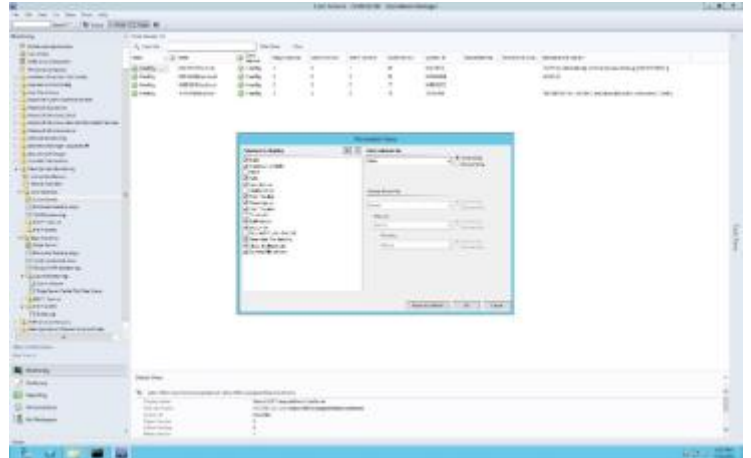


## Core Instances

- **Core Servers**

The following information can be enabled through Personalized Views

- State
- Maintenance Mode
- Path – displays FQDN
- Core Service – Running or not
- Major/Minor/Patch/Build Version
- System ID – Displays NetBIOS
- Selectable File Handling (plain text)
- Global Exclusion list (plain text)
- Backend File Servers (plain text separated by pipes “ | “)



- **Error and Warning Logs**

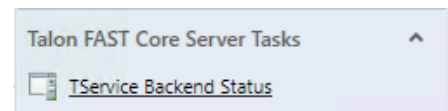
This view contains an extract of logs and warnings from FAST™ core instances. Including ‘Event Number’ in the Personalized View will help with quickly identifying Talon-specific notifications.

- Level
- Date and Time
- Event Number
- Logging Computer

- **TService Backend Status**

This contains an overview of tasks initiated by the ‘TService Backend Status’ Core Server Task.

This task can be started from the *Core Instances*\Core Servers view, which validates privileges and checks permissions on each backend file server associated with the FAST™ core instances in the environment.



- **TUM Monitoring**

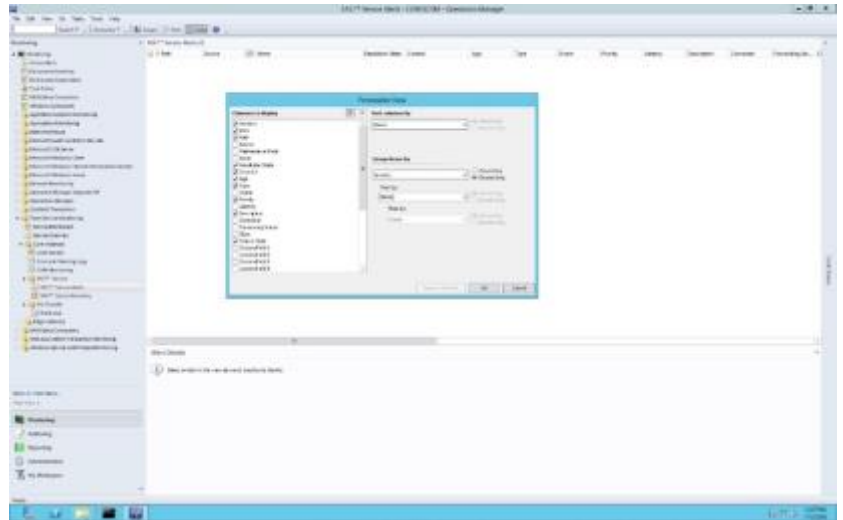
This contains an overview of the listed Talon FAST™ instances and any associated TUM information.

- Level
- Date and Time
- Event Number
- Logging computer

- **FAST™ Service Alerts**

This contains overview information for all service messages associated with the Talon FAST™ core role, see chapter 7 “Event Analysis” for more information.

- Severity
- Icon
- Path
- Resolution State
- Created
- Age
- Type
- Priority
- Description
- Time Resolved
- Time in State
- Time Resolved
- Last State Change
- Site
- Repeat Count



- **FAST™ Service Inventory**

This contains an overview of Core Servers, the currently associated Service User Account, and the state of the Talon T-Service.

- State
- Maintenance Mode
- Name
- TService Service Account
- TService Start Mode

- **File Transfer Event Log**

This contains log entries related to Talon File Transfer events. These can be parsed to determine file flushes and fetches.

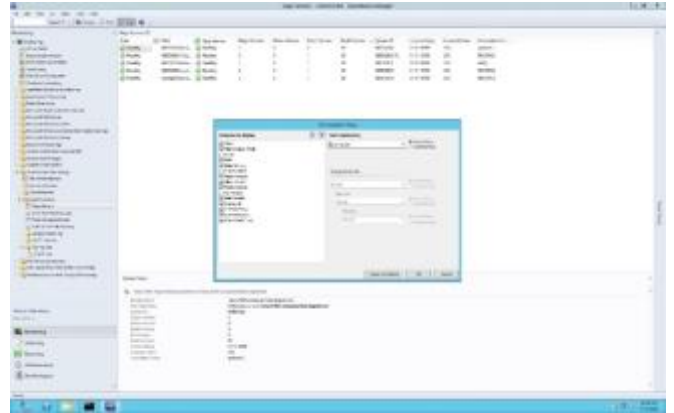
- Date and Time
- Event Number
- Log Name
- Logging Computer

## Edge Instances

- **Edge Servers**

The following information can be enabled through Personalized Views

- State
- Maintenance Mode
- Path – displays FQDN
- Edge Service – Running or not
- Major/Minor/Patch/Build Version
- System ID – Displays NetBIOS
- Licensed Expiry
- Licensed Users
- Associated Cores (plain text separated by pipes “ | “)



- **Error and Warning Logs**

This view contains an extract of logs and warnings from FAST™ edge instances. Including ‘Event Number’ in the Personalized View will help with quickly identifying Talon-specific notifications.

- Level
- Date and Time
- Event Number
- Logging Computer

- **Total Connected Users**

This view shows all connected Edge servers and statistics of the number of connected users per Edge server currently and over time.

- **TUM and TAPP Monitoring**

This contains Event Log entries in relation to the Edge’s TUM and TAPP Processes. This will help with quickly identifying Talon-specific notifications.

- Level
- Date/Time
- Event Number
- Logging Computer

- **Cache Cleaner**

This contains Event log entries in relation to Edge instances' automated cache cleaner mechanism.

- Level
- Date/Time
- Event Number
- Logging Computer

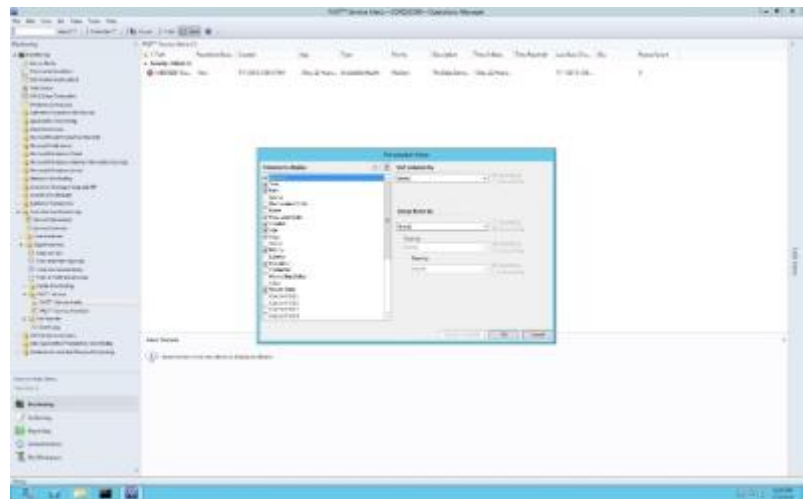
- **Edge Server Cache Disk Free Space**

This view provides a view at each selected Edge server to monitor the amount of available cache space (D:\)

- **FAST™ Service Alerts**

This contains overview information for all service messages associated with the Talon FAST™ edge role, see chapter 7 “Event Analysis” for more information.

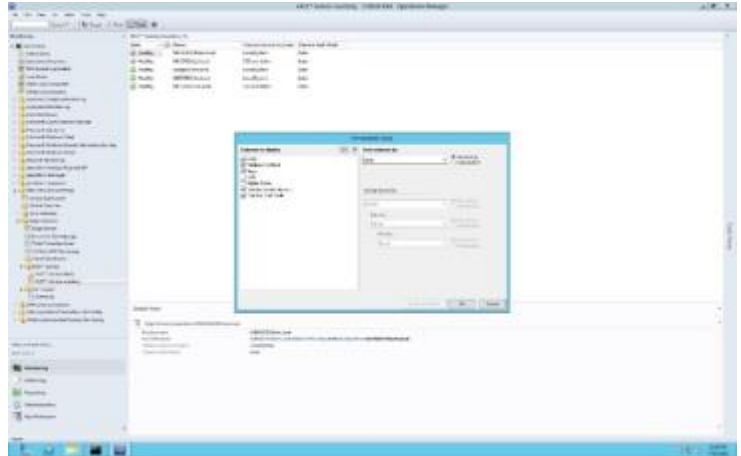
- Severity
- Icon
- Path
- Resolution State
- Created
- Age
- Type
- Priority
- Description
- Time in State
- Time Resolved
- Last State Change
- Site
- Repeat Count



- **FAST™ Service Inventory**

This contains an overview of Core Servers, the currently associated Service User Account, and the state of the Talon TService.

- State
- Maintenance Mode
- Name
- TService Service Account
- TService Start Mode



- **File Transfer Event Log**

This contains log entries related to Talon File Transfer events. These can be parsed to determine file flushes and fetches.

- Date and Time
- Event Number
- Log Name
- Logging Computer



## Where do I Find...?

Below are some commonly asked questions and examples of where to find commonly referenced configurations or informational events and their associated IDs.

### CONFIGURATION

#### **Identify whether all Talon FAST™ instances are on the same software version**

In the Talon Service Dashboard you can validate the software version using the FAST Major/Minor/Patch/Build Version field names. Once correlated you understand what version you're on, i.e. 3.0.1.99

#### **Ensure Selectable File Handling has been enabled for specific file types (.SLOG, .acddb, .laccdb)**

In the Core Servers dashboard, you are able to review and verify any Cores and their entries for Selectable File Handling using the Selectable File Handling field name. This will display a text entry for any file extensions associated to the listed Core instances.

#### **Understand number of users connected to my Talon FAST™ instance**

Using the Edge Instances dashboard, an overview of Total Connected Users is presented and displays currently connected users as well as watermarks for user connections over time. Specific Edge instances can be displayed or hidden using the checkboxes in the Performance Counter pane.

#### **Understand the amount of cache space being used on my Talon FAST™ instance**

Using the Edge Instances dashboard, a view for Edge Server Cache Disk Free Space is available to display current disk capacity and utilization levels. Specific Edge instances can be displayed or hidden using the checkboxes in the Performance Counter pane.

#### **Validate my core instance(s) has the correct configuration**

In the Talon Core Servers dashboard, you can validate the status of each Core's Core Service, the software version, and the associated backend file servers using the appropriately named fields.

#### **Validate my edge instance(s) are connected to the correct core instances**

In the Talon Edge Servers dashboard, you can validate the status of each Edge instance, the software version, and the associated Core Instance using the appropriately named fields.

### FUNCTIONALITY

#### **Validate Files are being transferred**

All File Transfers can be validated from the Core Instances File Transfer Event Log. This will detail all files fetched and flushed from the backend file server. Edge specific file transfers can be validated and parsed from the Edge Instances File Transfer Event Logs. This allows users to correlate and validate all data fetches and flushes across the Talon FAST™ environment.

#### **Understand Pre-population Job has started and/or completed**

Pre-population job status information can be validated from the Edge Instances TUM & TAPP Monitoring dashboard. Associated Edge instances will list events for both the start and completion of scheduled pre-population jobs.



## Event Analysis

The following Event ID's are commonly utilized throughout a Talon environment. These are provided to allow users to quickly record, monitor, or report on the provided logging statistics from the connected Talon FAST™ instances.

- **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
- **274 (Core) – Connection from <Edge><EdgeIP> successfully established**
- **274 (Edge) – Connections established and authenticate with <Core>**
  - Connections between Edge and Core have been established successfully.
- **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.
- **285 – Site key validated for all connections to <Core>. Transitioning to CONNECTED mode.**
  - WAN disconnection resolved, Edge and Core are communicating as normal.
- **287 – Unable to get address for <core>: error 11001 (No such host is known)**
  - Indicates a DNS error where Core cannot be resolved. Talon recommends connecting Edges to Core by IP
  - 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
- **3328 – Talon PrePopulation started at <Time> on <Date> with max\_threads 15**
- **3329 – Job is picked up for execution <BackendFS> (Edge)**
- **3329 – Job has been completed <BackendFS> (Edge)**
  - Indicates that a Pre-population job has started and completed.
- **282 - Cache Cleaner process is initiated**
  - Automated purging mechanism is engaged.
  - Indicated cache has reached 85% capacity.
  - May adjust D:\ accordingly if desired.



## Log Analysis

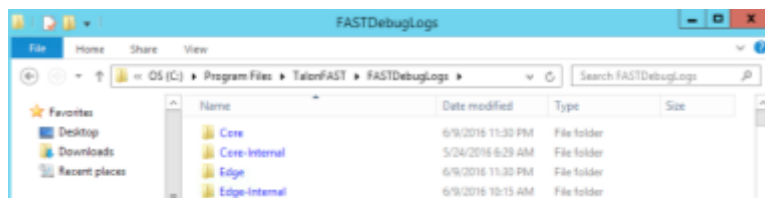
Finally, Talon FAST™ uses four sets of files to capture logging on the global file sharing paradigm, which are accessible to the systems and storage administrators via a web-based interface. These files are stored in a structured .TXT text format, to allow both easy viewing for immediate problem determination, or to facilitate export (via .CSV or other formats) to management reporting infrastructures such as SCOM, Splunk, Nagios, Zabbix, etc.

The four areas of FAST™ management logging are:

- FAST File Transfer Log
- FAST Message Log
- FAST Stats Log
- TAPP Log

Each of these provides insight into different aspects of the globally consolidated storage environment that Talon FAST™ enables for customers.

The Talon FAST™ logs can be found in **C:\Program Files\TalonFAST\FASTDebugLogs\** location on each core or edge instance and collects logs for each role instantiated, i.e. Core or Edge. In addition to traditional logs, a folder can be found that includes *Internal* information, typically used for support and engineering purposes only.



### FAST File Transfer Log

The logging here provides information regarding files that are handled via the Talon FAST™ services. Basically, these are files that are either opened on the edge appliance from the datacenter/core, or those that are written to the datacenter core (including updates, saves, copy, and paste type actions). This log allows the administrators to see what files have been accessed (including the full path name), the size of the files, and how well optimized/compressed the actions were. Parameters reported include:

- Date
- Time
- Type of message (Info only, Warning, etc.)
- File path and name
- File size
- Bytes to be transferred (before compression)
- Bytes actually exchanged over the network (after compression)
- Transfer efficiency (% of data transfer optimized relative to standard file size)
  - Note: this is higher with uncompressed file types, lower with pre-compressed file types
- User Account SID



### *FAST Message Log*

The FAST Message Log offers insight as to connections over the network between the core and edge appliances, status of licenses in use, as well as general messages. The insight provided includes:

- Date
- Time
- Type of message
- Message text / error descriptor / event descriptor

### *FAST Statistics Log*

The FAST Statistics Log is a static repository in the core/edge which is updated periodically to offer snapshots regarding outstanding connections/leases between the core and edge devices. From the core, the information provided includes:

- Current leases (file locks) outstanding and active
- Updated on a periodic schedule

This information allows a trending analysis, historically, as to the usage patterns of the system globally.

From the edge devices the FAST Statistics Log provides insight as to which core(s) the edge devices is connected to, and the state of that connection (connected vs. disconnected). This information is useful in configuration and availability management for more complex configurations where an edge may be connected to more than one cloud or datacenter core.

### *TAPP Log*

The TAPP Log is used in cases where pre-population (i.e. prepop) is part of the configuration or workflow. In order to allow the administrators a high level of confidence that prepop has been completed in the time window necessary for workflows (used often in highly complex configurations, or often-changing environments), the TAPP Log provides information as to:

- Date
- Time
- Type of message (Info only, error, etc.)
- Message text (file transfer started, file transfer completed, error encountered, etc.)



## 9. FAST™ Web Access Portal

Talon FAST™ Web Access Portal allows users to access privately managed file shares or folders through a web browser of their choice, either from desktop or laptop PC's, Mac OSX or devices. The FAST™ Web Access Portal is storage agnostic and integrates with either on-premise or cloud-based corporate file sharing infrastructure.

Documents uploaded, downloaded and shared through the FAST™ Web Access Portal, automatically synchronize with the central authoritative copy of your files. This guarantees data consistency for all FAST™ branch office and FAST™ Web Access Portal users.

The Talon FAST™ Web Access Portal requires an additional component to be installed in your environment, leveraging the existing Talon FAST™ core infrastructure and a newly deployed FAST™ Web Access Portal virtual instance in the cloud, your DMZ or as a server inside your Local Area Network (LAN).

The FAST™ Web Access Portal provides a Webserver frontend that's accessed by your users, so – depending on your requirements – you can deploy the virtual machine instance.



### Deploying Talon FAST™ Web Access Portal

Talon provides Centos 7.0 based virtual appliance template (900MB) that includes the basic services and the FAST™ Web Access Portal redistributable. The virtual machine can be deployed on VMware vSphere 5.1 or higher and leverages 2 vCPU cores and 4GB of RAM.

- The Web Access Portal listens for user sessions on TCP ports 4443 (HTTPS) and 8888 (HTTP) to access the front-end interface. Ensure that these ports are publicly accessible (or through VPN).
- The Web Access Portal connects with a Microsoft Windows Server instance that runs the TFS.EXE process, typically your Talon FAST™ core instance, on TCP ports 60845-60850; ensure that your firewall allows traffic established from the core instance to the FAST™ Web Access Portal.

Depending on your requirements you can customize the Linux operating system, add packages and commit package and operating system updates (yum update).

**Note:** Talon releases updated RPM packages that are automatically downloaded and updated by your FAST™ Web Access Portal on a weekly basis. Check the logs in `/var/log/TalonWebPortal` for more information.

## Talon FAST™ Web Access Portal Deployment Instructions

1. Download OVA template from <http://www.talonstorage.com/software/talon-wap01.ova>  
MD5: a6b6e589c42e4b738ad2f965bf219a5c
2. Deploy OVA template on VMware vSphere 5.1 or higher
  - a. Associate the LAN adapter (E1000) with your DMZ or internal VLAN (when using NAT)
3. Complete the deployment process and log in to the console using standard credentials
  - a. Username: **root**
  - b. Password: **TalOnFAST!**
4. Configure your network settings
  - a. Type **ifconfig** to list all active network interface adapters
    - i. Note the name of the adapter, i.e. ens160 (in this example ens160)
  - b. Change directory by typing **cd /etc/sysconfig/network-scripts**
    - i. Edit the configuration file associated with ens160
      1. List the configuration files by typing **ls -als**
      2. Type **nano ifcfg-ens160** (where ens160 is the available adapter)
        - a. Provide the IP address (IPADDR), Subnet Mask (PREFIX) and default gateway (GATEWAY) settings associated with your environment

```

GNU nano 2.3.1 File: ifcfg-ens160
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="ens160"
UUID="2462149c-8c1e-4450-bbdf-3fd8aafac98a"
DEVICE="ens160"
ONBOOT="yes"
DNS1="19.168.1.1"
IPADDR="192.168.1.212"
PREFIX="24"
GATEWAY="192.168.1.1"
IPV6_PEERINGS="yes"
IPV6_ROUTE6="yes"
IPV6_PRIVACY="no"

```

4. Type **CTRL+O** to save the file and **CTRL+X** to exit nano editor
  5. Type **ifdown ens160**
  6. Type **ifup ens160**
  7. Ensure that the device is up and running by typing **ifconfig** (ens160 should be listed)
  8. Test connectivity by pinging the gateway, type **ping 192.168.1.1** (where 192.168.1.1 is the gateway address)
- ii. Optionally, change the hostname of the Talon Web Access Portal, follow these steps:
    1. Change directory by typing **cd /etc/sysconfig**
    2. Type **nano network**
    3. Edit the file to change the hostname
    4. Type **CTRL+O** to save the file and **CTRL+X** to exit nano editor



- iii. Optionally, to enable internal DNS, you can change the `/etc/resolv.conf` file using the same steps as in the previous commands (nano)
5. Validate that the Talon FAST™ services are started
  - a. Type `service TalonWebPortal status`
    - i. Service should be started
  - b. Type `netstat -ln|grep "608"` to identify whether the application is listening on TCP ports 60847 and 60848
6. Configure your Talon FAST™ Web Access Portal settings by following these steps:
  - a. Change directory by typing `cd /opt/TalonWebPortal`
  - b. Type `./admin.py`
  - c. Choose to Add a server instance by typing `Add`
  - d. Provide the `Servername` (needs to be an easy name, i.e. Company)
  - e. Provide the `Password` (use a complex password, this is used to associate the Talon FAST™ instance (core) with the Talon FAST™ Web Access Portal)
  - f. To delete a portal configuration, repeat the process but type `Del` in step 6c
7. Change the root password by typing `passwd`
8. Restart the Talon FAST™ Web Access Portal by typing `shutdown -r now`
9. Validate that the Talon FAST™ Web Access Portal is running by navigating to the following URL in a browser:
  - a. <https://192.168.1.212:4443/Web/mobilefast/index.html#/login> (where 192.168.1.212 is the IP address of the Web Access Portal server)
  - b. A login screen should be presented

## FAST™ Web Access Portal – Core Configuration

10. To finalize the configuration, continue with the configuration of the Talon FAST™ Web Access Portal settings on your Talon FAST™ (core) instance
11. RDP to your Talon FAST™ Core Instance
12. Open the Talon FAST™ Configuration Console and select the Talon FAST™ Web Access Portal tab
13. Configure the Portal Configuration by providing the following information
  - a. Web Portal Name: **NEEDS** to be **TFSTornado**
  - b. Web Portal IP address: the IP address of the Web Access Portal service deployed in your DMZ or LAN (NAT)
  - c. UserName: the Servername configured in step 6d
  - d. Password: The Password configured in step 6e
  - e. Click "Add" to commit the changes

**Talon FAST™ Web Access Portal Configuration**

Once you've deployed and configured the Web Access Portal service (which is LINUX), please associate this Talon FAST™ instance with the Web Access Portal to complete the configuration.

Web Portal Name	TFSTornado	<input type="button" value="Add"/>
Web Portal IP Address	192.168.1.212	
UserName	servername	
Password	●●●●●●●●	

14. Configure the Roots by adding SMB/CIFS file share locations to the root configuration, specify the following information:
  - a. Root unique ID: a number that identifies the file share ID, i.e. 1
  - b. SMB share or path: the UNC path of the file share presented to the Talon FAST™ Web Access Portal
  - c. Root traverse: Disable when you do not allow users to browse the parent or root paths within the SMB share or path included above
  - d. Click "Add" to commit the changes

**FAST™ Web Access Portal Root Configuration**

Configure SMB share or path roots to be accessible through FAST™ Web Access Portal

Root unique ID	1	<input type="button" value="Add"/>
SMB share or path	\\fileserver\share	
Root traverse	<input checked="" type="checkbox"/>	

**Note:** you may need to restart the Talon FAST™ - TService service through the Services Console (services.msc)

You can now navigate to the Talon FAST™ Web Access Portal's login screen and login using your Active Directory credentials, Domain Name and Servername (step 6d).







## 10. Client Application Best Practices

### AutoDesk - Revit

Autodesk Revit users typically work in:

#### 1. *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.

#### 2. *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 Talon-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 the Talon FAST™ solution, 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/2011/10/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 Talon FAST™ Core(s) Selectable File Handling entries – Live Multisite Collaboration

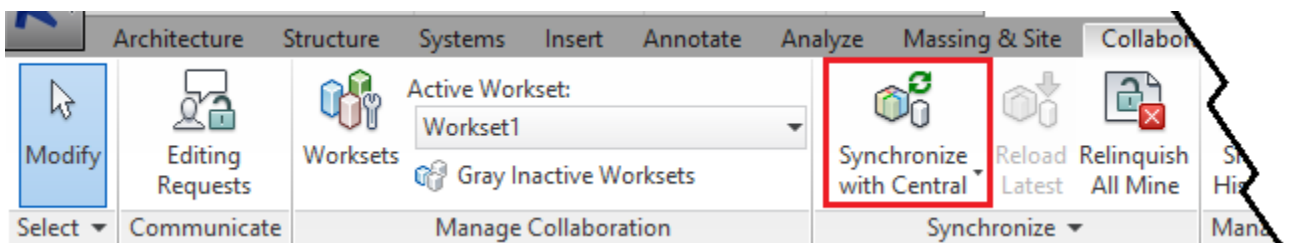
Any Core servers which will be serving Revit files used in a live multisite collaborative situation, must have the .SLOG extension added to their Selectable File Handling entries.

### 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.



**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.

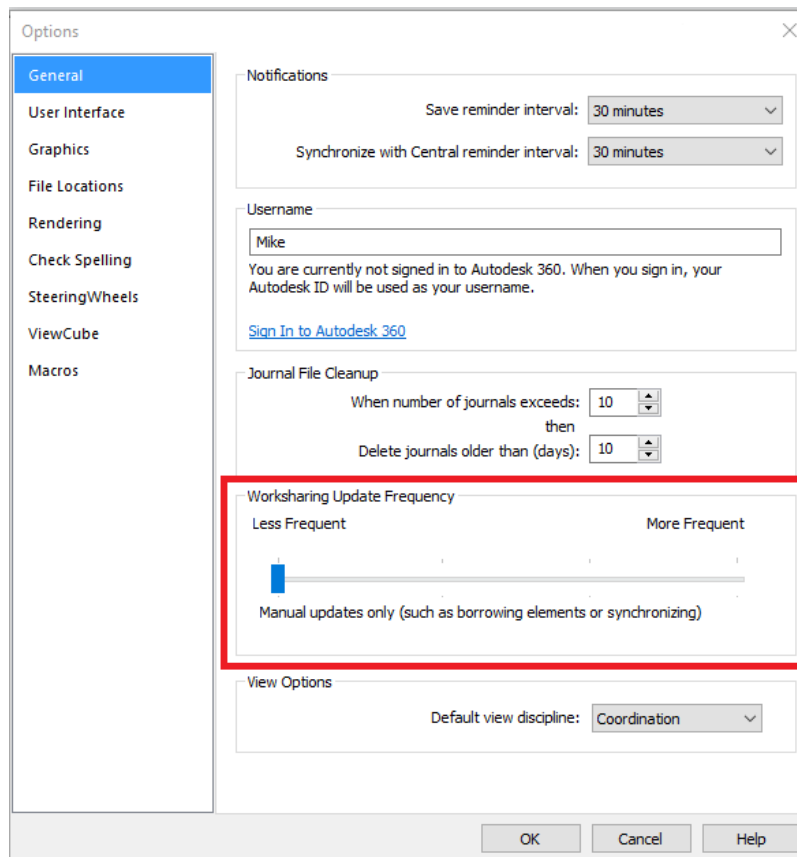
### Save Often, Sync less


In order to reduce the total amount of data traversing the WAN, Talon 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



- Click the  logo, and then click **Options**.
- In the **Options** dialog box, click the **General** tab.
- 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.
- Click **OK**.



## Revit Best Practices 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 bring network connection between offices to hold and you or other Revit users might not be able to synchronize Revit model.**
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 TALON 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.**

## Autodesk - AutoCAD

### Disable Digital Signatures

Digital signatures contribute to slow browsing of AutoCAD folders and files through Talon FAST™ 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.

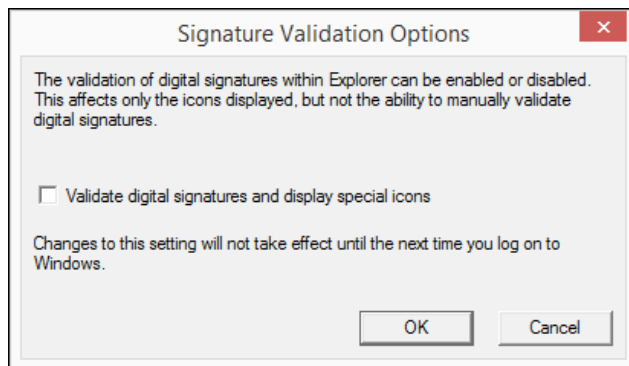
During the AutoCAD installation, a shell extension loads displaying a specific icon with the file in Windows Explorer, or in the Open/Save dialog box if it is digitally signed. To determine whether a file is digitally signed, the shell extension scans each drawing file as it is displayed. Folders that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

### Disable Digital Signatures (Manual)

Use Windows Explorer and navigate to C:\Windows\System32 directory.

- Double-click the acsignopt.exe file.

The Signature Validation Options window displays.



- De-select Validate digital signatures and display special icons.
- Click OK.
- Restart the computer.

## Implementing AutoCAD Registry Setting Using AD Group Policies

- Create a registry file called autocad.reg on the desktop.
- Open the autocad.reg file in Notepad and add the following:

```
[HKEY_CURRENT_USER\Software\Autodesk\Autodesk Digital Signatures]
"IconOverlayEnabled"=dword:00000000
```

- Save the autocad.reg file.
- Copy the autocad.reg file to the logon share.
- Create a batch file called autocad.bat.
- 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\\scripts
- Start the Active Directory Users and Computers snap-in by clicking Start > Administrative Tools > Active Directory Users and Computers.
- In the console tree, right-click the local domain and select Properties.
- Click the Group Policy tab, click New.
- Type a name for the new policy (for example, AutoCAD Digital Sign), and press Enter.
- Right-click the new policy name, select Properties.
  - Click the Security tab.
  - De-select the Apply Group Policy checkbox for the security groups that should not have this policy applied.
  - Select the Apply Group Policy checkbox for the groups that should have this policy applied.
  - Click OK.
- Click the Group Policy tab.
- Select the appropriate group policy object (for example, AutoCAD Digital Sign), and click Edit.

## Implementing AutoCAD Registry Setting Using AD Group Policies (Continued)

The Group Policy Object Editor displays

- Under User Configuration, expand Windows Settings.
- Click Scripts (Logon/Logoff).
- Right-click Logon, select Properties. The Logon Properties window displays.
- 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.

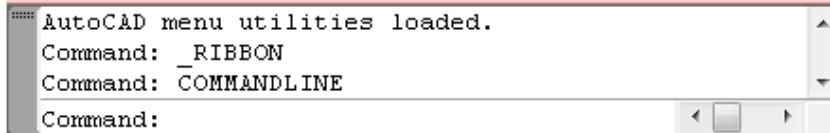
- Click OK.
- Click Apply.
- Click OK to close.
- Close the Group Policy Object Editor Console and the Active Directory Users and Computers snap-in. Have all users log out and log back into the domain. The end user PCs now have the following registry setting installed:

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

## Set AutoCAD Sheet Set Manager Variables

### Access and Edit Variables

- Open the AutoCAD command window.
- Type the name of the variable followed by the value to set it to.
- 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 **SSMPOLLTIME**.

### **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 **SSMPOLLTIME** 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.

### **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.





## Bentley – MicroStation

### **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 FAST™ 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.

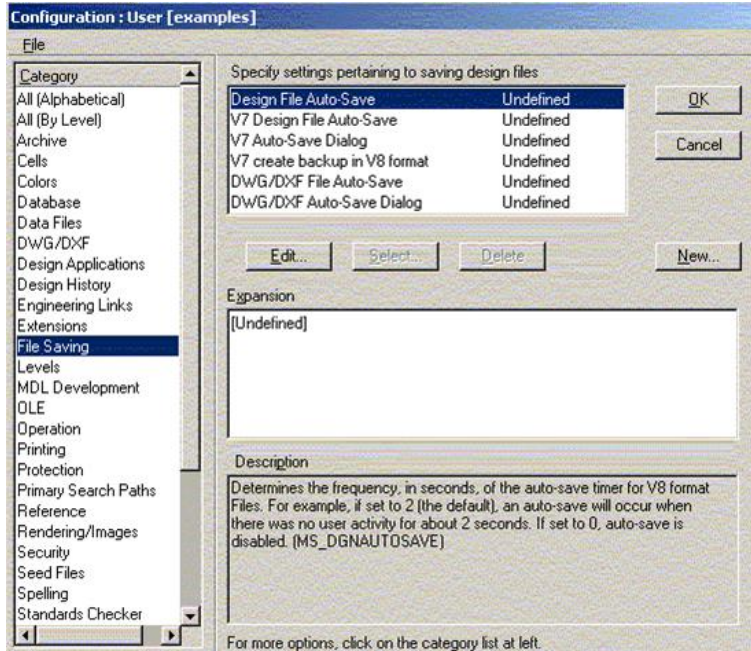
In the event of a network or WAN interruption, MicroStation times out and displays a window that offers the options of retrying or cancelling the save operation. MicroStation does not offer a "Save As" option for files open on client PCs from the data center file server. The retry option causes MicroStation 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

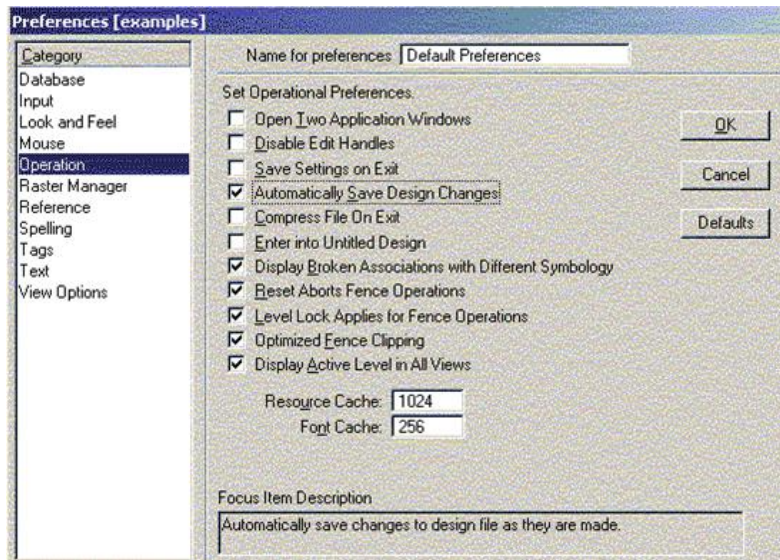
Under the Workspace Configuration settings, select File Saving. Here users can set auto-save parameters (or review the settings that an administrator has made in site configuration files).



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.

## Adjusting AutoSave settings in Microstation (Continued)

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.



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".



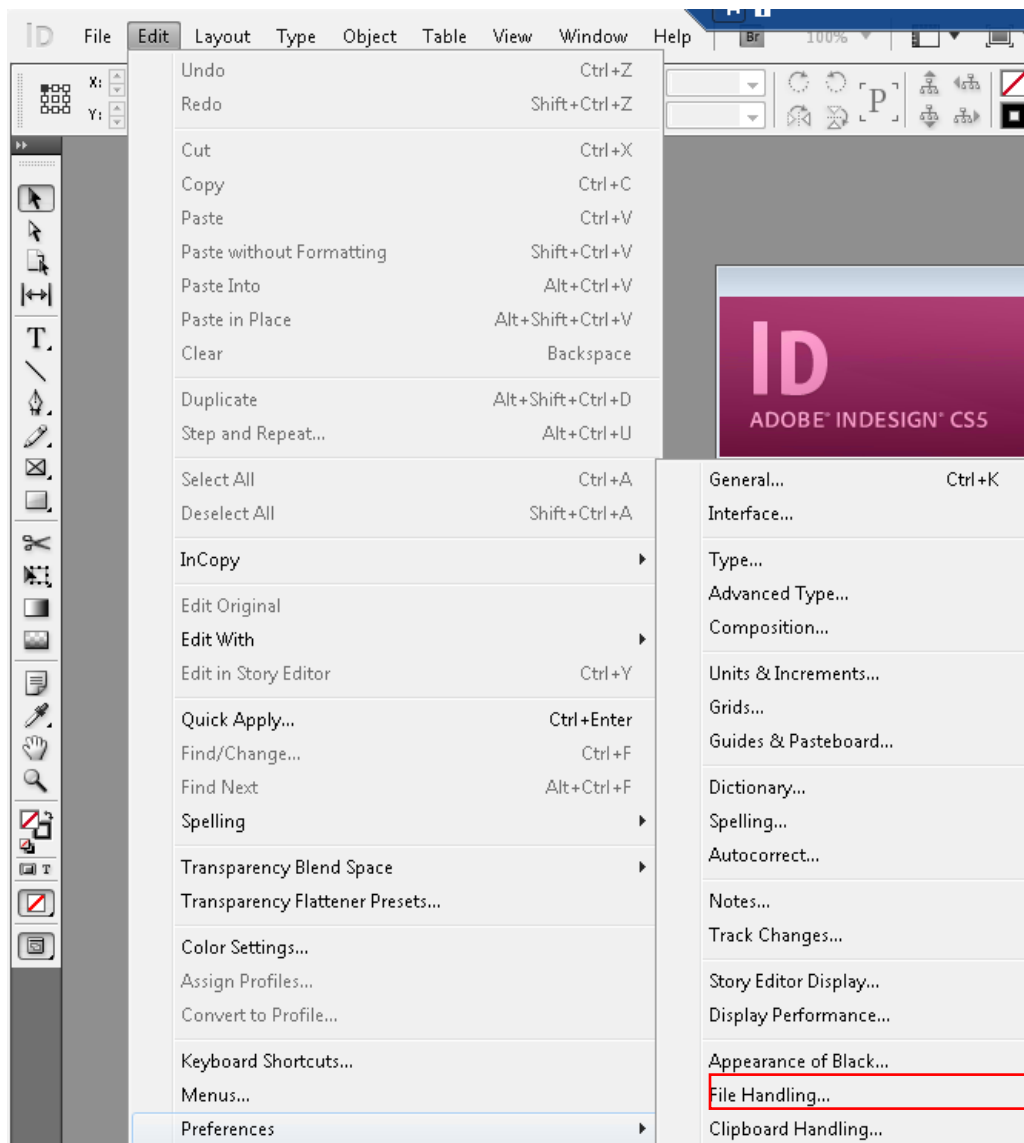
## Adobe Creative Suite

### InDesign

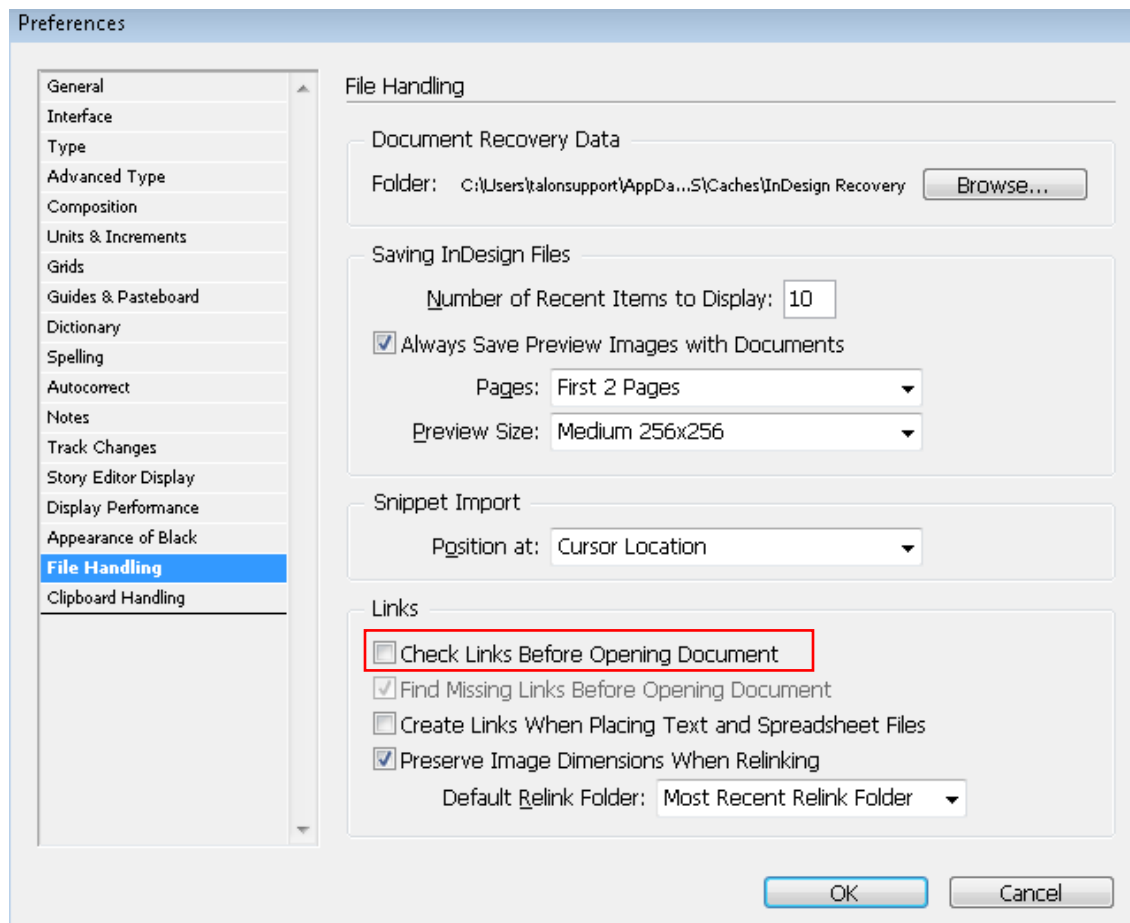
To prevent InDesign from checking for links between images within a document and with external documents, it's recommended to disable checking for links when opening a file. If this is left on, it may result in multiple file read or open operations which may impact performance.

To adjust the link check setting on the client workstation:

- Click "File"
- Expand the "Preferences" menu
- Click "File Handling"



- Uncheck the box to “Check links before opening document”



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

- Create a new directory named ‘Startup Scripts’ at
  - C:\Users\\AppData\Roaming\Adobe\InDesign\Version11.0\en\_US\Scripts
- Create a new JavaScript file within the ‘Startup Scripts’ directory with the following contents
  - app.linkingPreferences.checkLinksAtIOpen = false;
- 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**



## Mac OSX Best Practices (10.11 onwards)

### Offline Attribute not recognized by Mac OSX

By default, Mac OSX SMB/CIFS implementation does not support the use of the Offline Attributes on files and folder structures (see also: <https://discussions.apple.com/thread/6002286?tstart=0> ), this means that when browsing through the FASTData file share, cold files (not cached) and metadata objects (i.e. file/folder name, ACLs) are not visible at first. Once browsing into a path structure, a user may need to manually refresh the folder's metadata by right-clicking in the folder and click 'Get Info' for the folder contents to appear.

Solution: To circumvent users from having to manually refresh the folder contents by right-clicking in the folder and click 'Get Info', pre-population of metadata would improve the end user experience as it immediately displays file/folders contents and ACLs cached on the Talon FAST™ edge instance. This allows the users to see and work on cold files immediately.

### Adding a Network Location to your favorites, (i.e. DFS Namespace)

Right+Click a network share or folder from your finder window, hold CMD button drag it into Favorites

### Disable Indexing of Network Locations (OSX 10.12)

Preventing Spotlight from Indexing Time Machine Backups, External Disks and Network locations on a Mac:

1. Connect the volume you want excluded to the Mac, even if Spotlight is currently indexing.
2. Launch "System Preferences" and click on "Spotlight" followed by the 'Privacy' tab.
3. Drag the drives icon into the Privacy window.

### Disable .DS\_Store file creation (OSX 10.4)

Mac OSX workstations create a file named .DS\_Store which stores information about the custom attributes of its containing folder. These files are created automatically by Finder within any browsed directory. These files should be disabled from being created in order to maintain user performance while navigating a network directory structure. This change affects network drives using SMB/CIFS, AFP, NFS, and WebDAV.

- Close all 'Finder' Windows
- Open a 'Terminal' session
- Execute the following command

```
defaults write com.apple.desktopservices DSDontWriteNetworkStores true
```

- Restart the workstation or log off and log in to the user account

More information can be found at <https://support.apple.com/en-us/HT1629>

## Disable Spring-loaded Folders and Windows

Spring-loaded folders open folders in new windows while clicking-and-dragging items through a directory structure. This behavior can potentially cause unnecessary or unwanted caching of folder metadata as users traverse folders

### Mac OSX 10.12

- Open System Preferences
- Navigate to “Accessibility”
- Select “Mouse & Trackpad”
- Uncheck the box “Spring-loading delay”



### Mac OSX 10.5

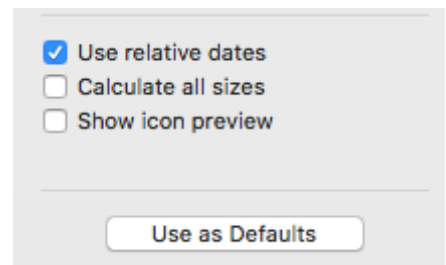
- Open ‘Finder’
- Open ‘Finder Preferences’
- Click the ‘General’ Tab
- Uncheck the box “Spring-loaded folders and windows”



## Disable Icon Previews

Some Icons in Finder can dynamically update based on the file’s contents. If the content of the item is updated, then the item’s icon will update to reflect those changes. This may cause the file to be cached locally at the branch office and may impact the user experience while navigating the virtual file share.

- Open a ‘Finder’ window
- Click the ‘View’ menu
- Click “Show View Options”
- Uncheck the box to “Show Icon Preview”
- Click the button to “Use as defaults”







## 11. 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.

Talon FAST™ 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.

A detailed description on the Talon FAST™ solution can be found at <http://www.talonstorage.com/gettingstarted>

In summary, FAST™ creates a central “Single Set of Data” in **[CUSTOMER]**'s data center while it's branch office FAST™ Intelligent File Caching mechanism transparently presents central file shares, documents and project files to the end user community in these branch offices. Additionally, FAST™ 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/dxVP21HOQyY>

### 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

Talon FAST™ 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 "Talon" 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 the Talon FAST™ solution, please consult the following resources:

[www.talonstorage.com](http://www.talonstorage.com)

---

## Additional Resources

Talon has made video training materials available for customer distribution to their IT staff and end users.

The video at <https://youtu.be/dxVP21HOQyY> provides a general solution overview to admins and users as well as providing some Talon FAST™ do's and don'ts.

The video at <https://youtu.be/-REkaKXR234> also provides a shortened general overview, basic do's and don'ts, and a focus on Autodesk Revit application best practices.

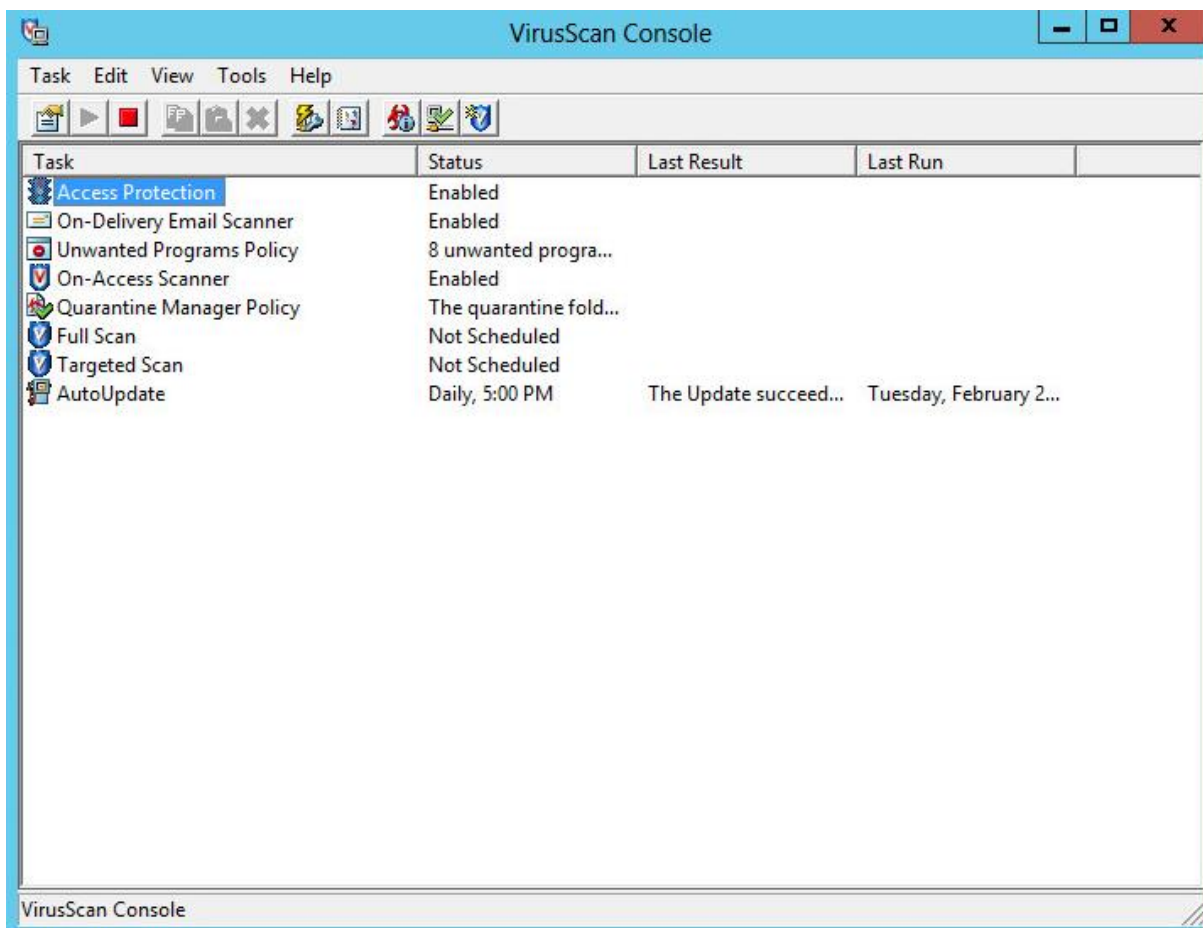


## Appendix A: Antivirus Application Suites

### 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.

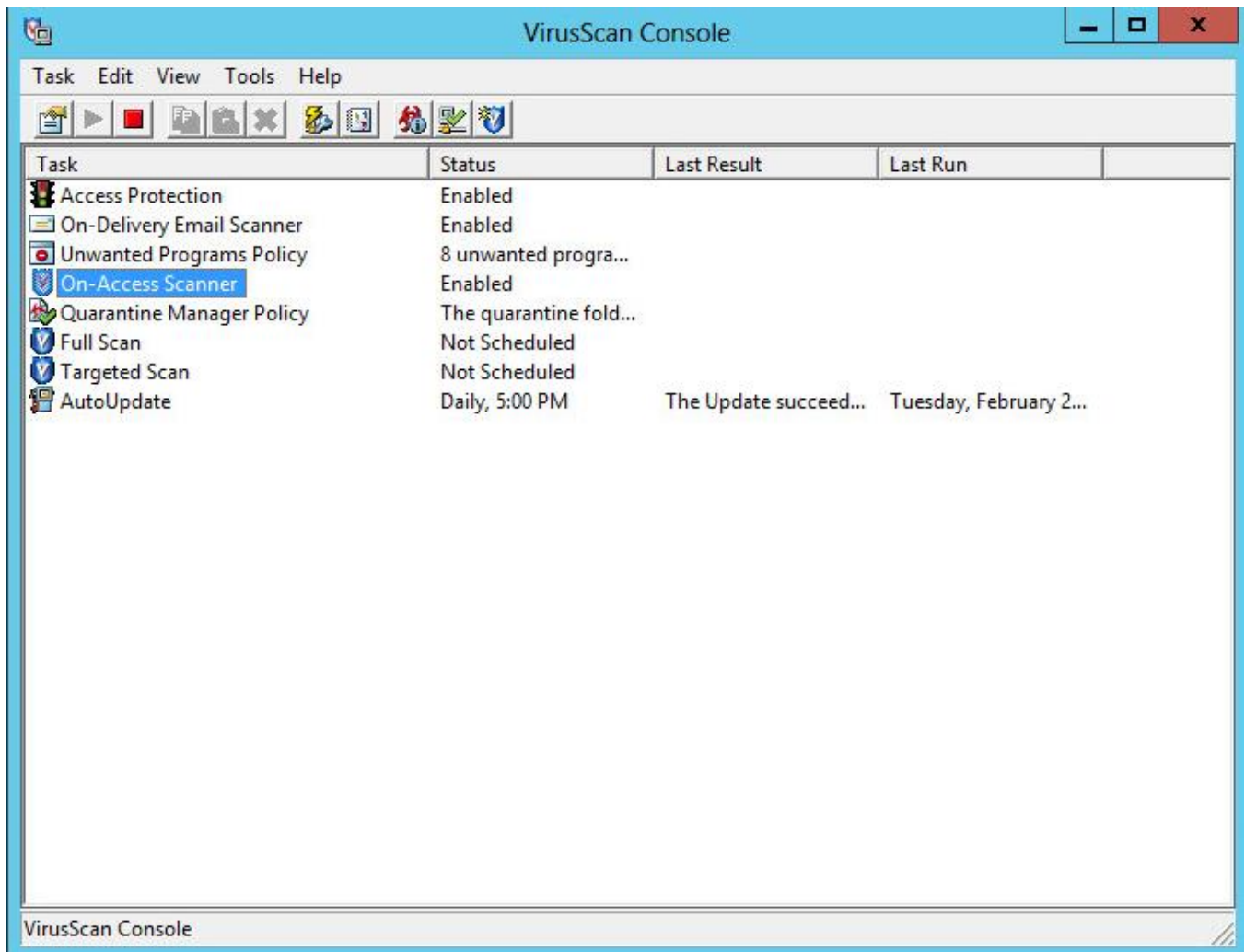


## Excluding Services and Processes in McAfee VirusScan Console

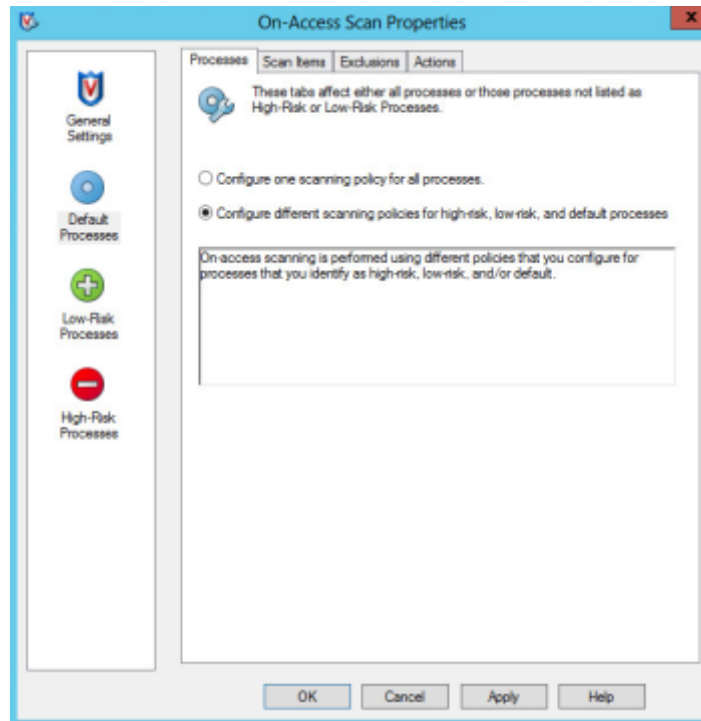
This section details how to exclude Talon FAST™ processes on Core/Edge Servers and other remote appliances based on McAfee VirusScan scanning.

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

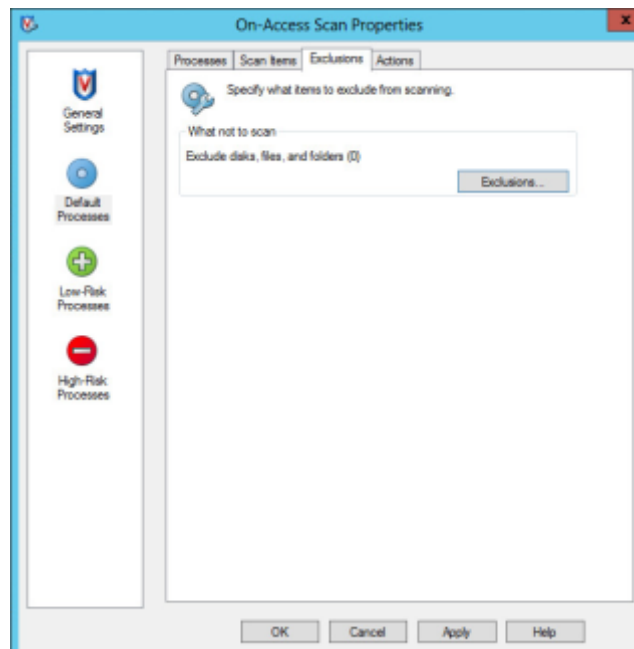
- Double click the “On-Access Scanner” task in the main VirusScan Console window.



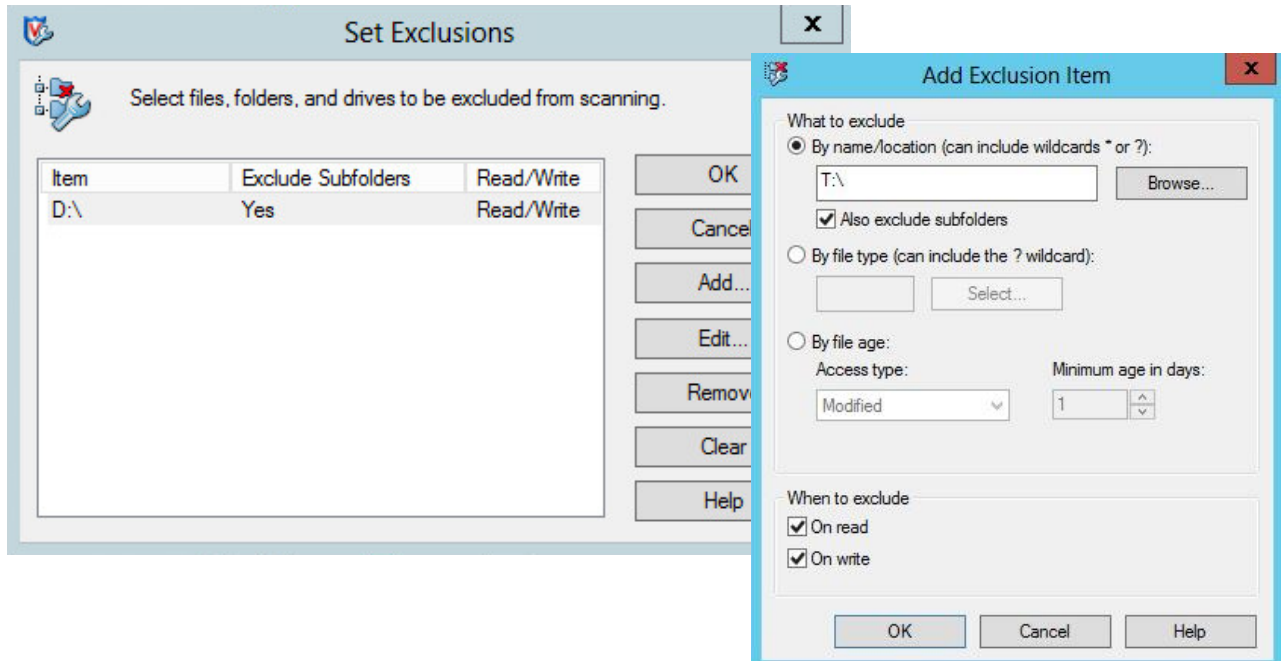
- Click “Default Processes” in the left pane and then select the radio button labeled “Configure different scanning policies for high-risk, low-risk, and default processes.”



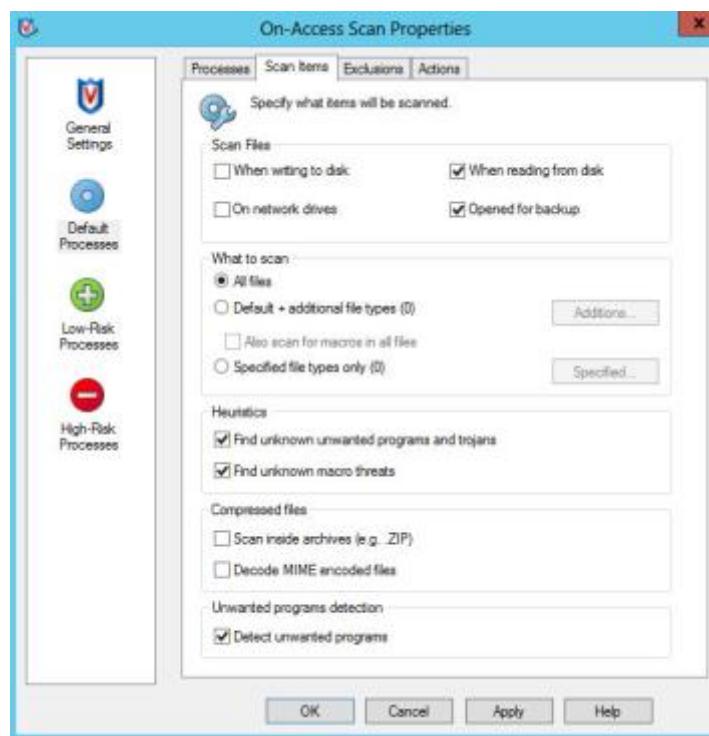
- Click the “Exclusions” tab and then click the “Exclusions...” button to configure them.



- Add the T:\ and D:\ drives to the Exclusions list. Ensure that subfolders are also excluded from scans. Click OK when finished

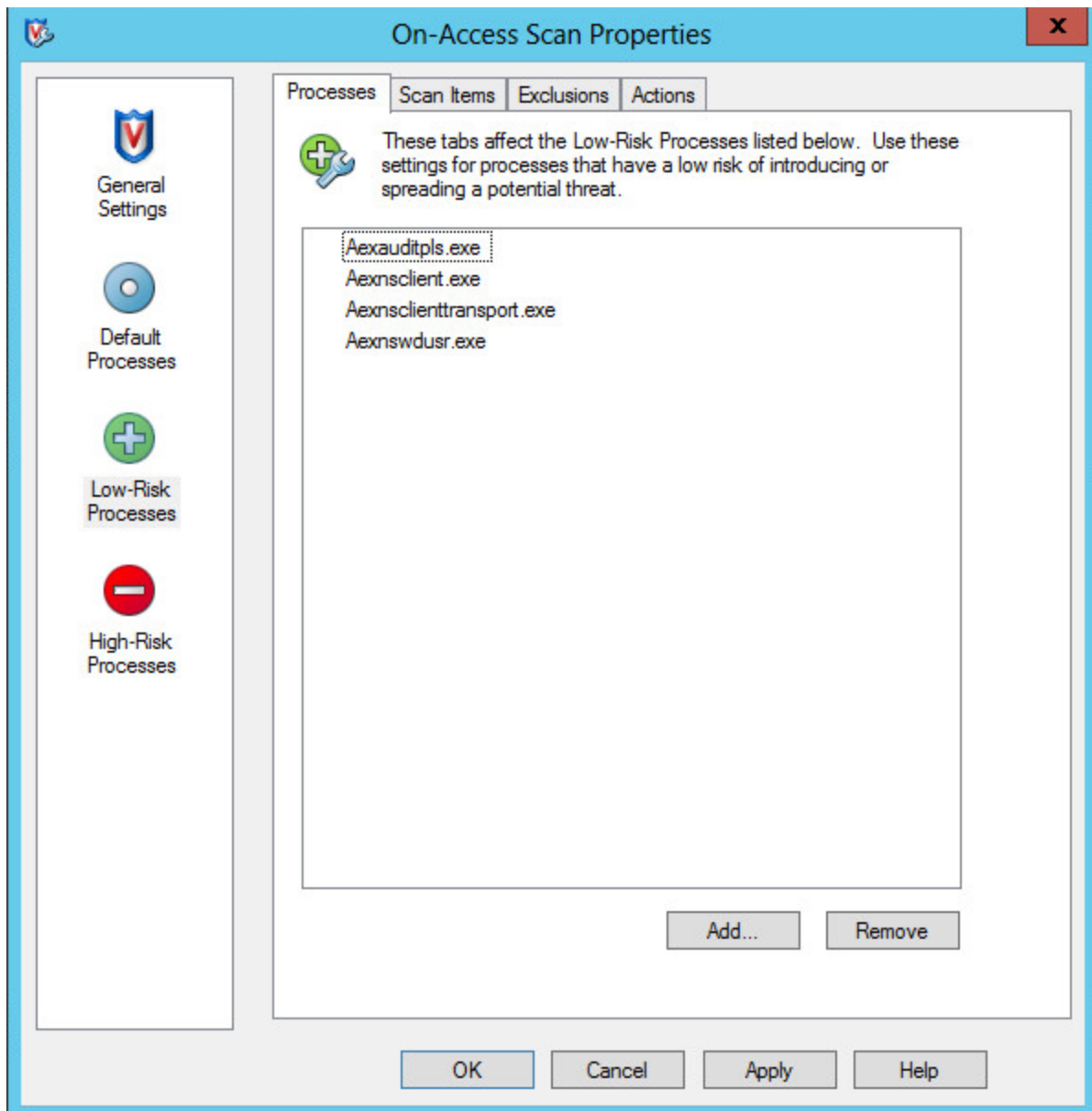


- Click the Scan Items tab and de-select “When writing to disk”

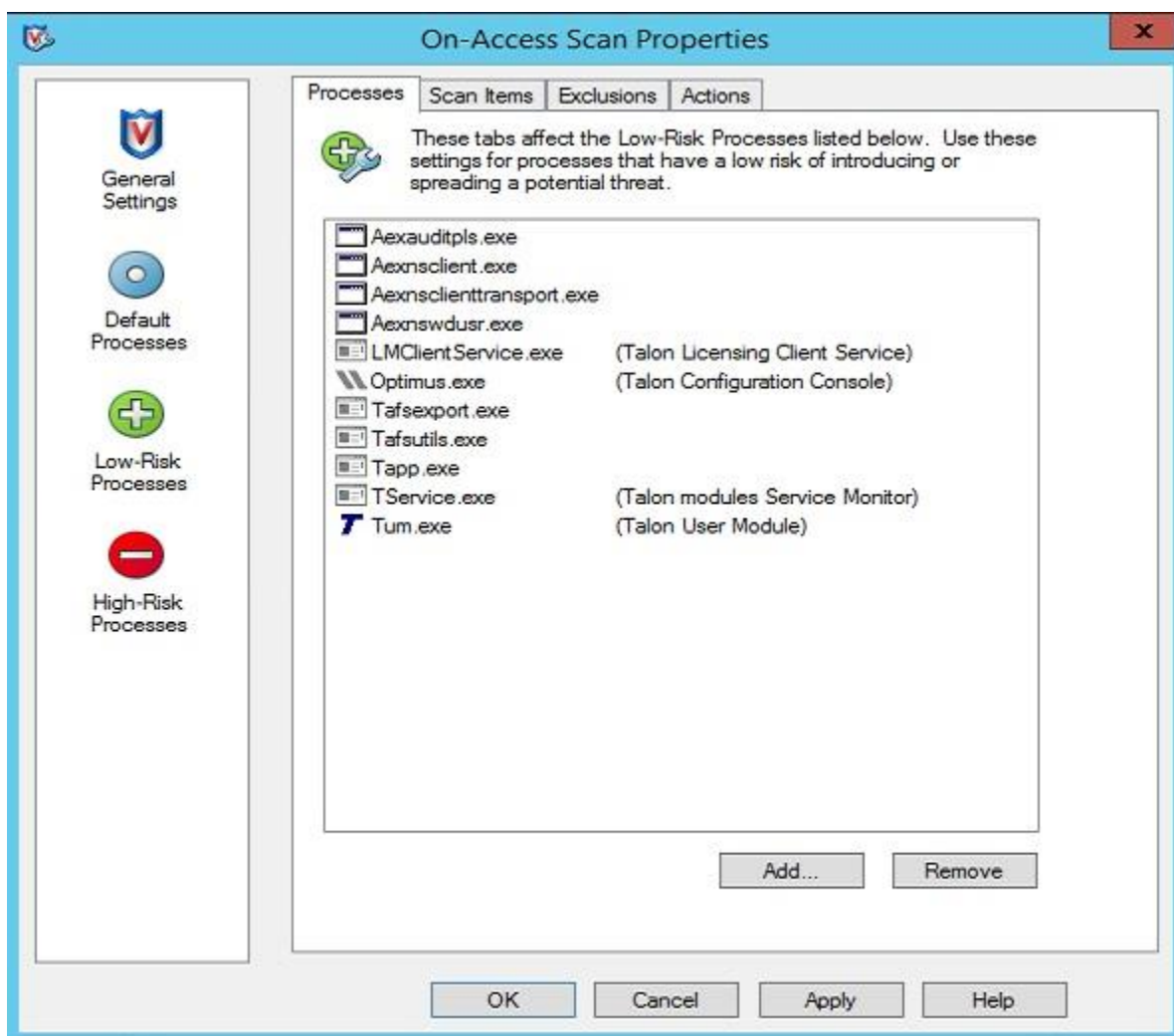




- Click “Low-Risk Processes” in the left pane.
- Click the “Add...” button on the “Processes” tab.

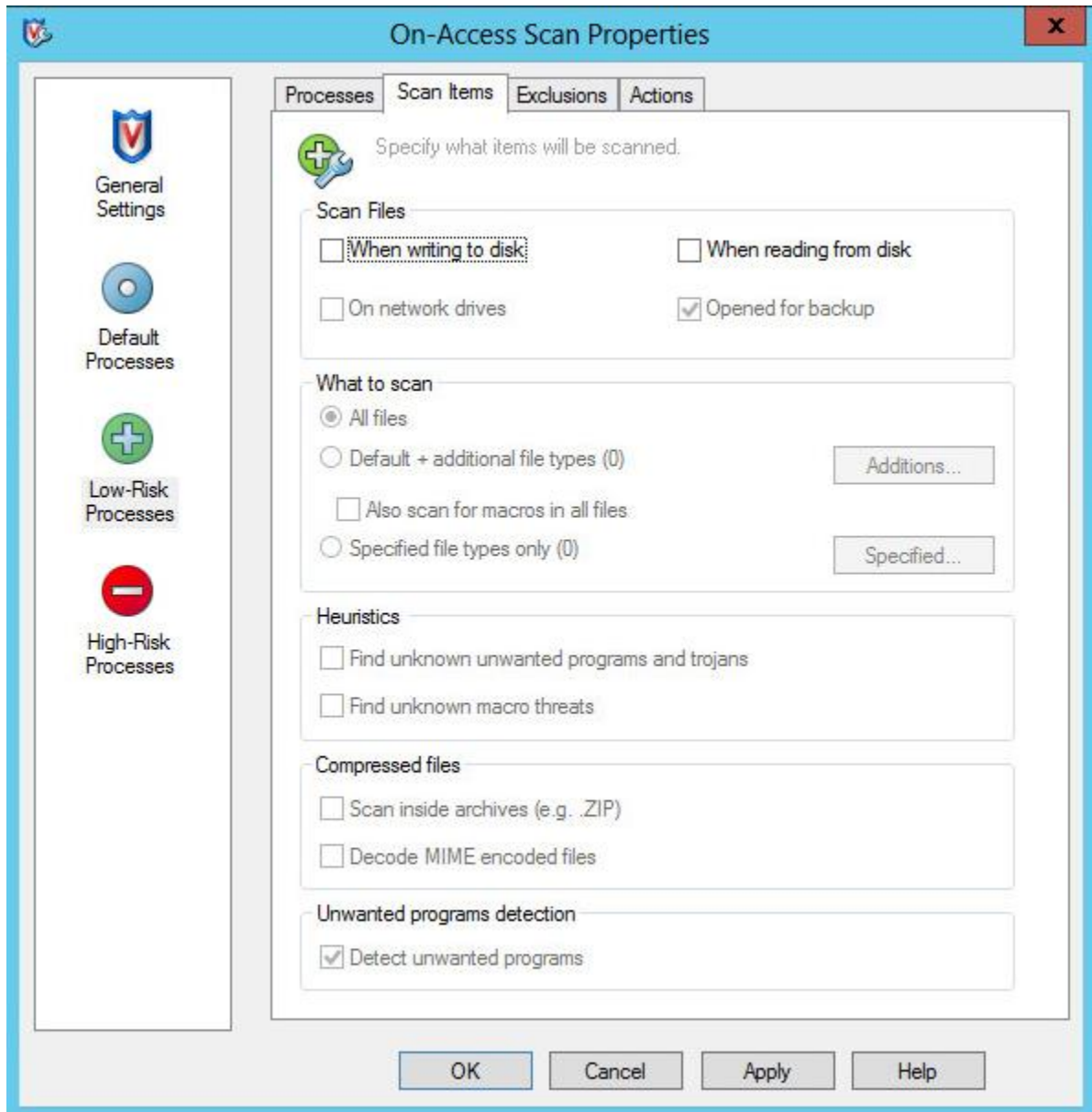


- Once the list of available processes finishes populating, you may need to click the “Browse...” button and manually add the following processes:
  - C:\Program Files\TalonFAST\Bin\LMClientService.exe
  - C:\Program Files\TalonFAST\Bin\LMServerService.exe
  - C:\Program Files\TalonFAST\Bin\Optimus.exe
  - C:\Program Files\TalonFAST\Bin\tafsexport.exe
  - C:\Program Files\TalonFAST\Bin\tafsutils.exe
  - C:\Program Files\TalonFAST\Bin\tapp.exe
  - C:\Program Files\TalonFAST\Bin\tfs.exe
  - C:\Program Files\TalonFAST\Bin\TService.exe
  - C:\Program Files\TalonFAST\Bin\tum.exe
  - C:\Windows\System32\drivers\tfast.sys

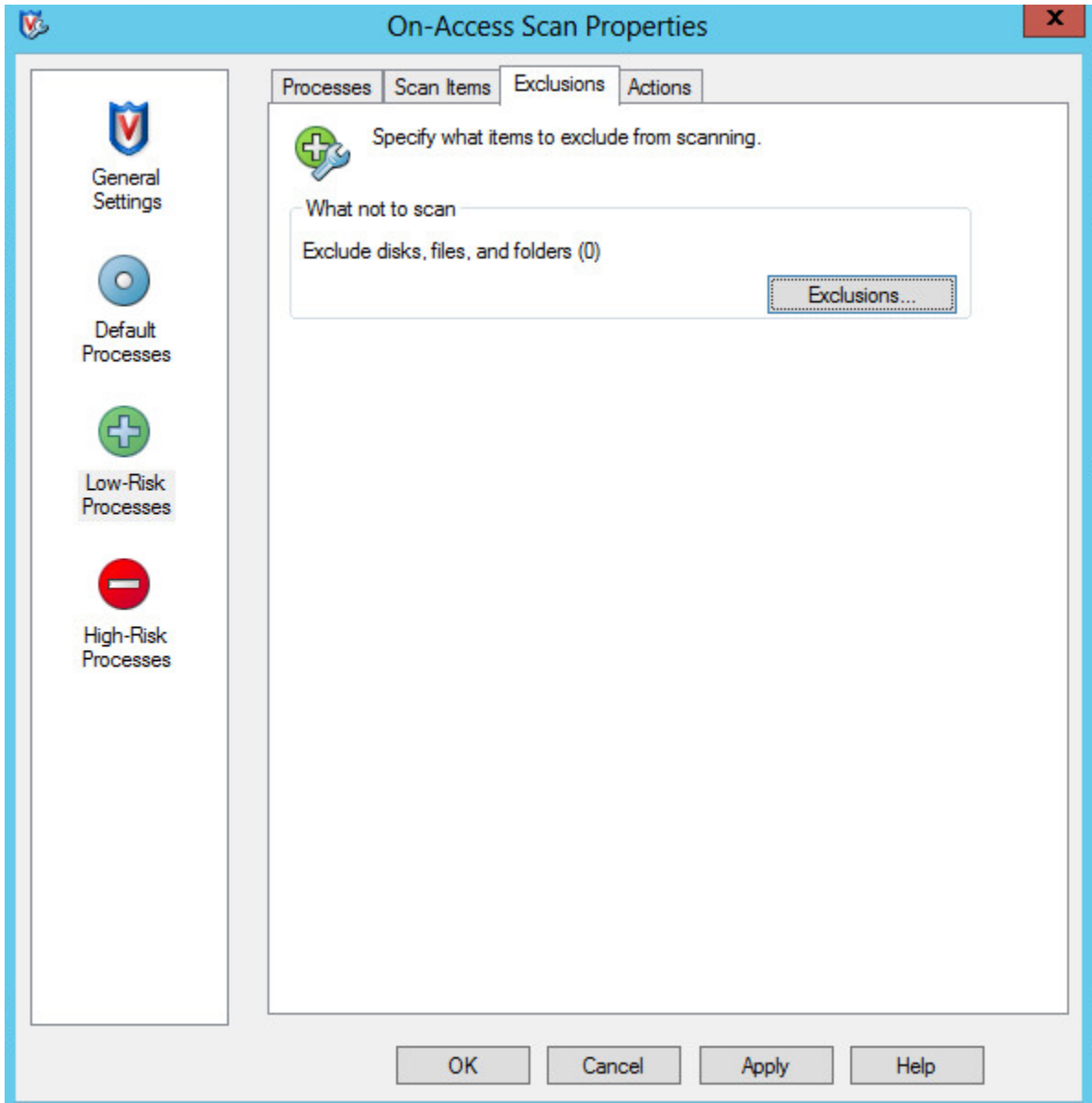


- Click OK to apply the changes.

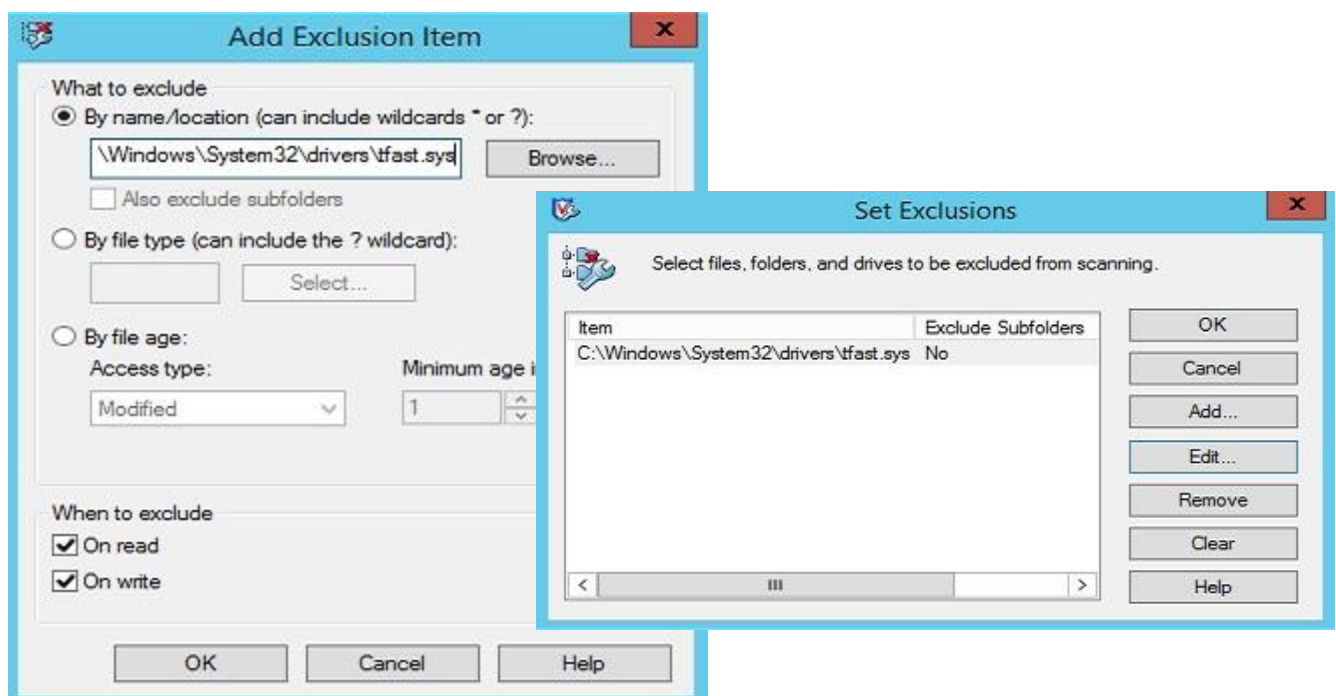
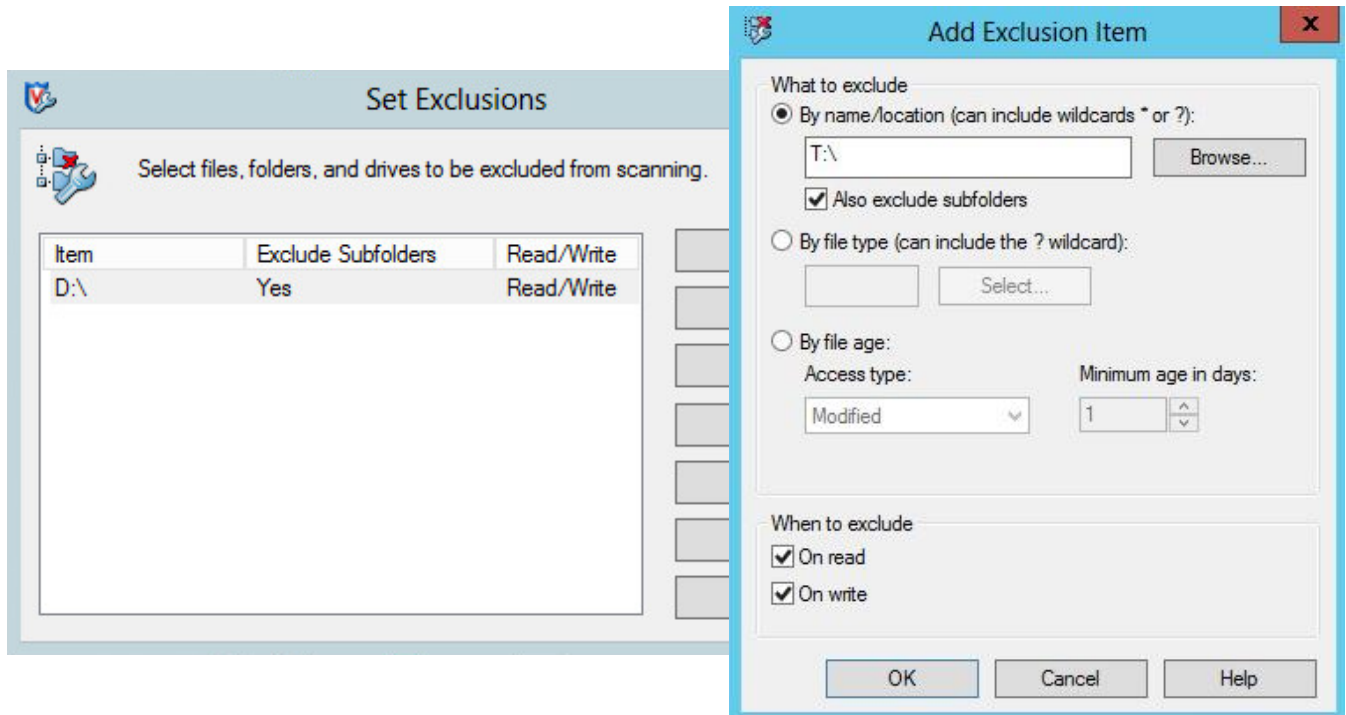
- Click the “Scan Items” tab and de-select “When writing to disk” and “When reading from disk”.



- Click the “Exclusions” tab at the top.
- Click the “Exclusions...” button



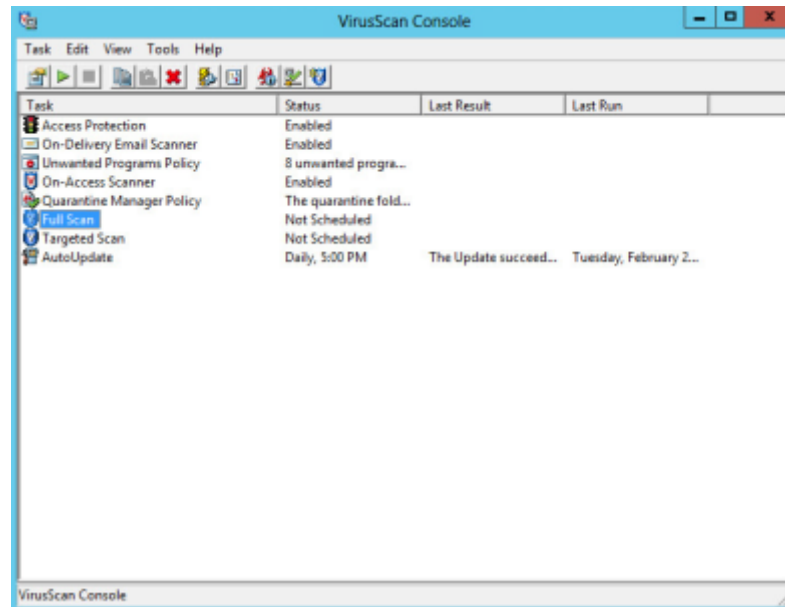
- Add the T:\ and D:\ drives to the Exclusions list. Ensure that subfolders are also excluded from scans.
- Add C:\Windows\System32\drivers\tfast.sys.  
**Note:** You may have to manually type in this path to add tfast.sys
- Click OK when finished.



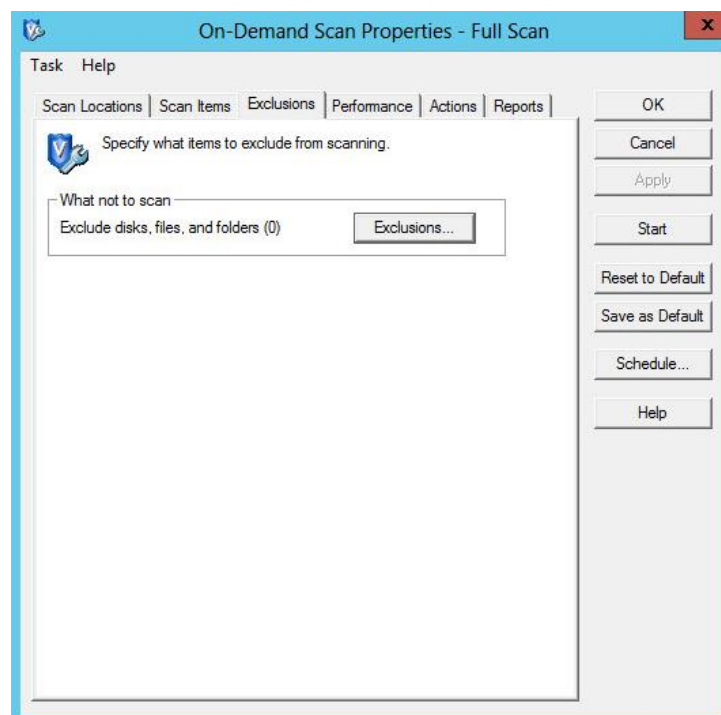
## Full or Targeted Scans

If running a full or targeted scan on a Talon FAST™ server, please follow the steps below

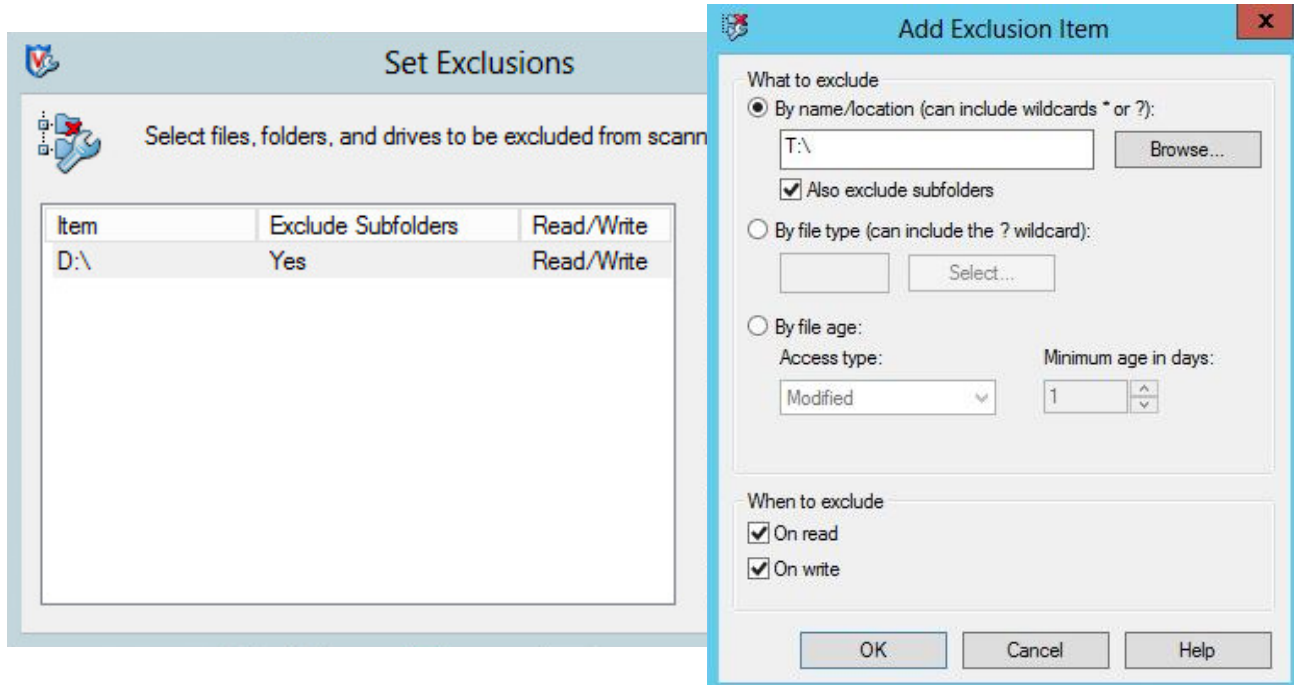
- Double click either Full Scan or Targeted Scan from the VirusScan Console



- Click the “Exclusions” tab from the On-Demand Scan Properties window. Click the “Exclusions...” button.



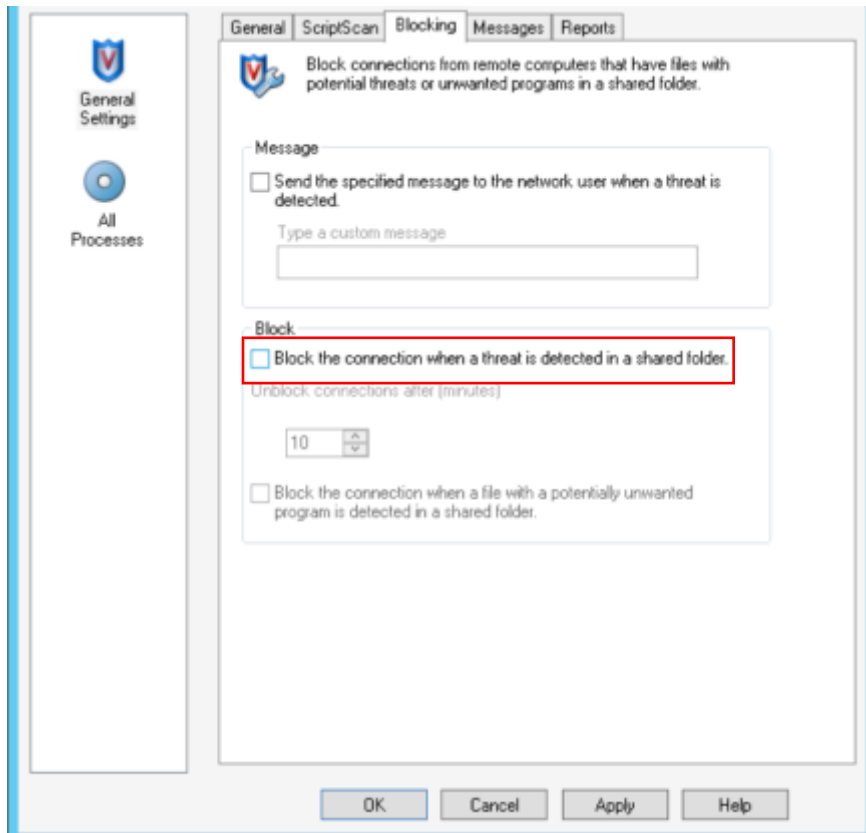
- Add the T:\ and D:\ drives to the Exclusions list. Ensure that subfolders are also excluded from scans. Click OK when finished.



## Prevent Connection Blocking in Shared Folders

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

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





## Symantec Endpoint Protection 12.x

This section outlines best practices for Symantec Endpoint Protection version 12.x targeted for Talon FAST™ appliances based on Windows Server 2012 R2.

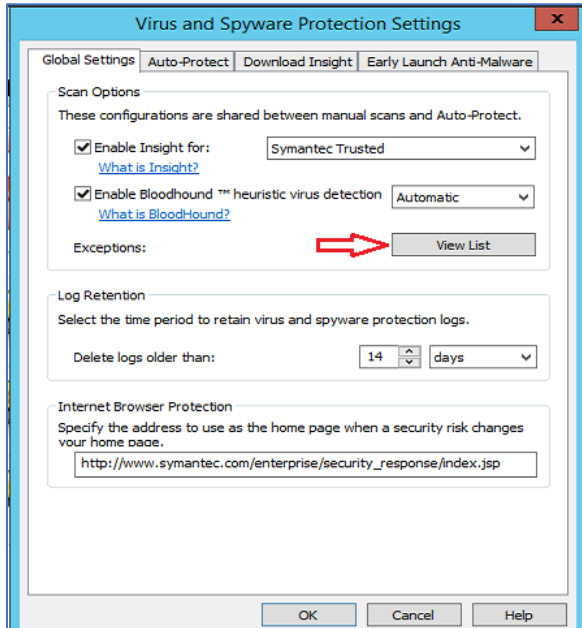
- **Double click the Symantec icon on the task bar**



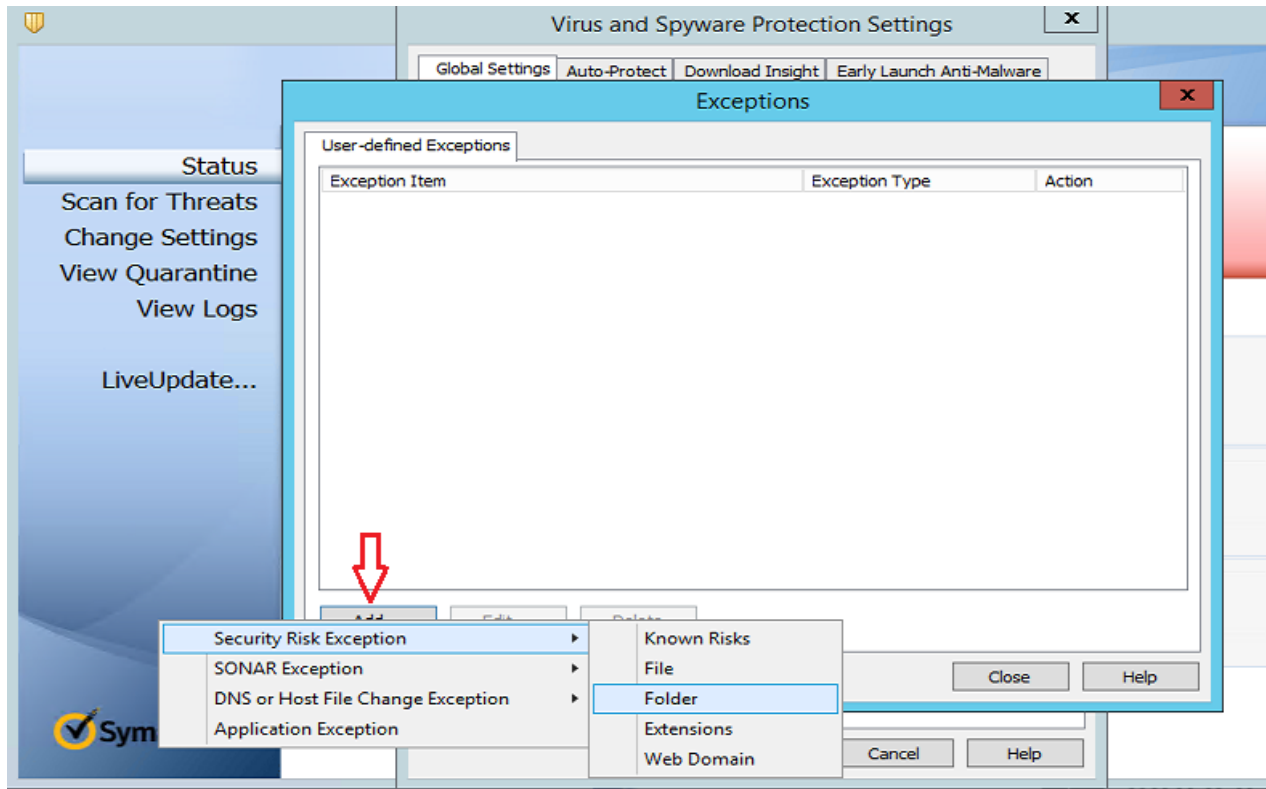
- **Virus and Spyware Protection -> Click Options -> Change Settings**



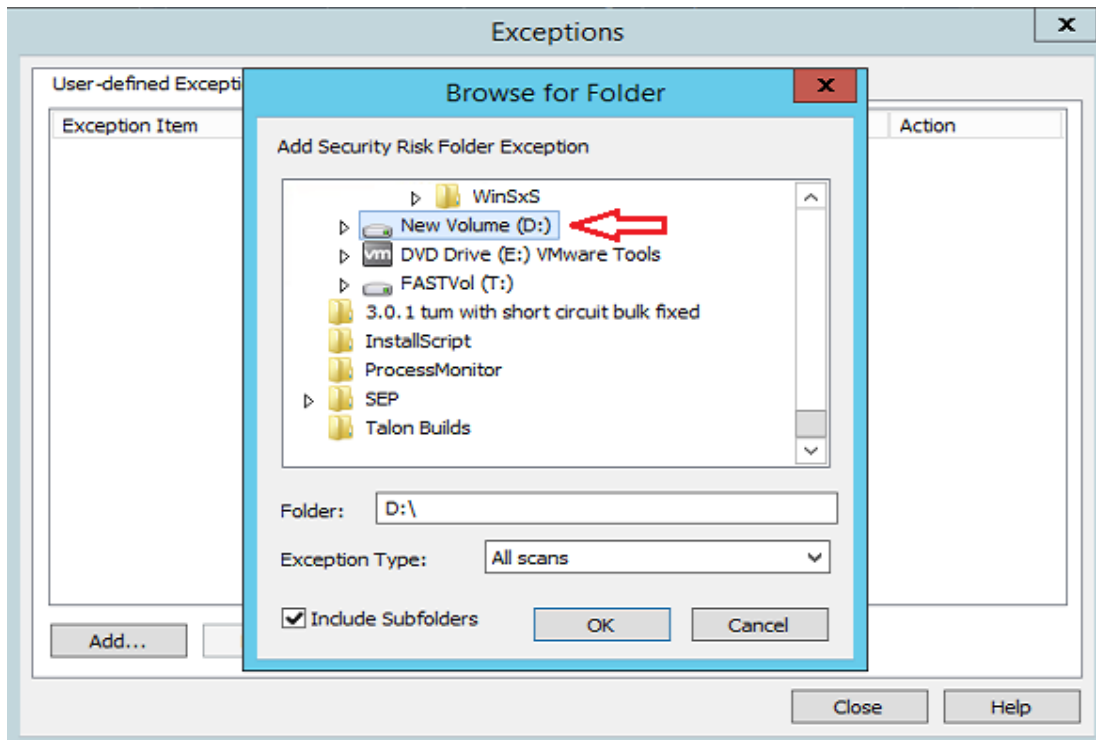
- Click **View List**



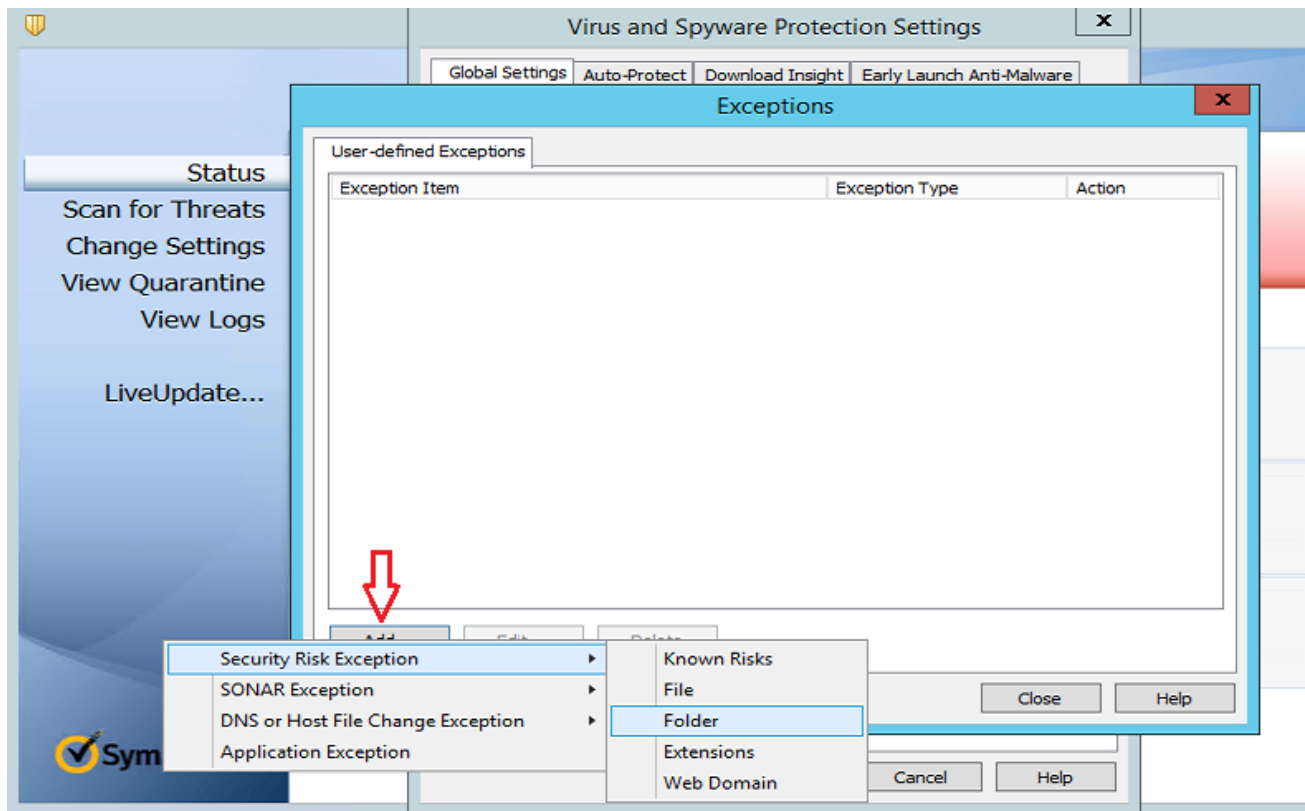
- Click **Add ->Security Risk Exception ->Folder**



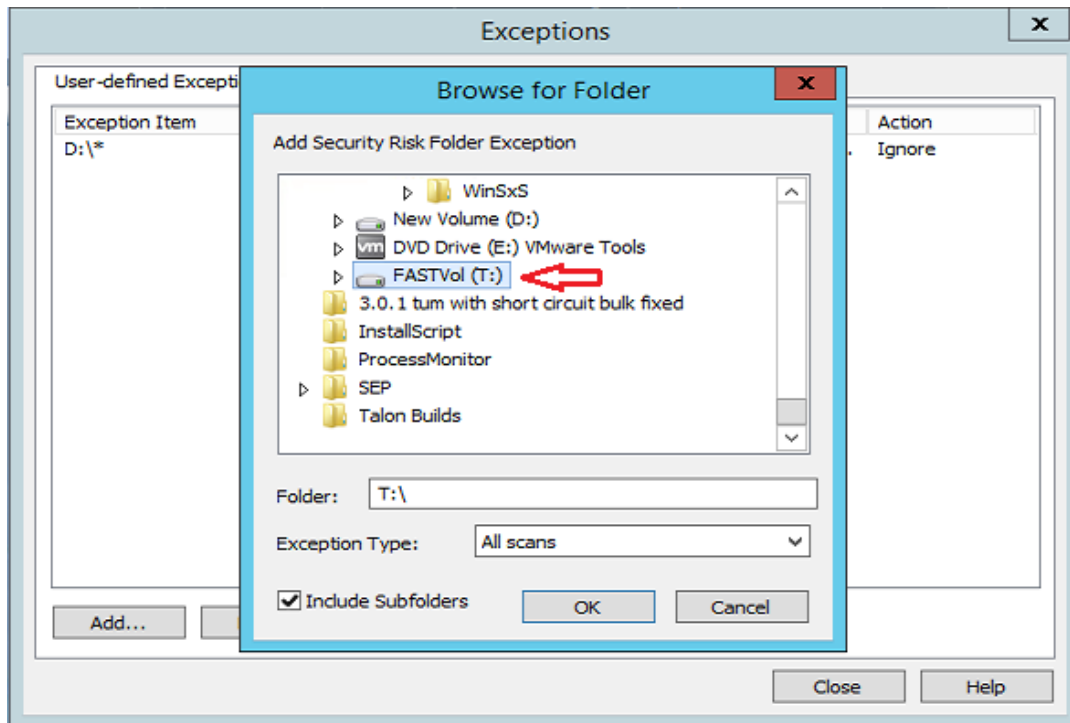
- **Scroll down**, click on **D**, and click **OK**



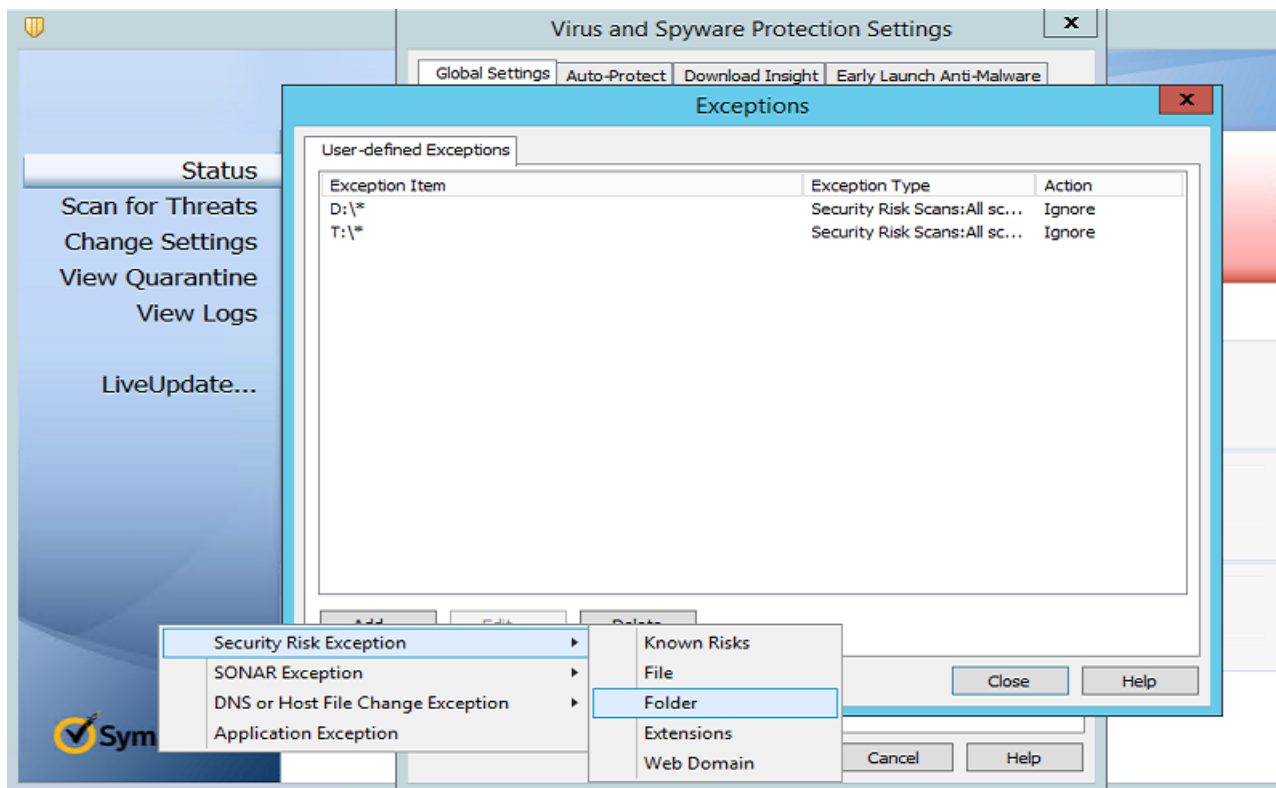
- **Click Add ->Security Risk Exception ->Folder**



- **Scroll down**, click on **T**, and click **OK**

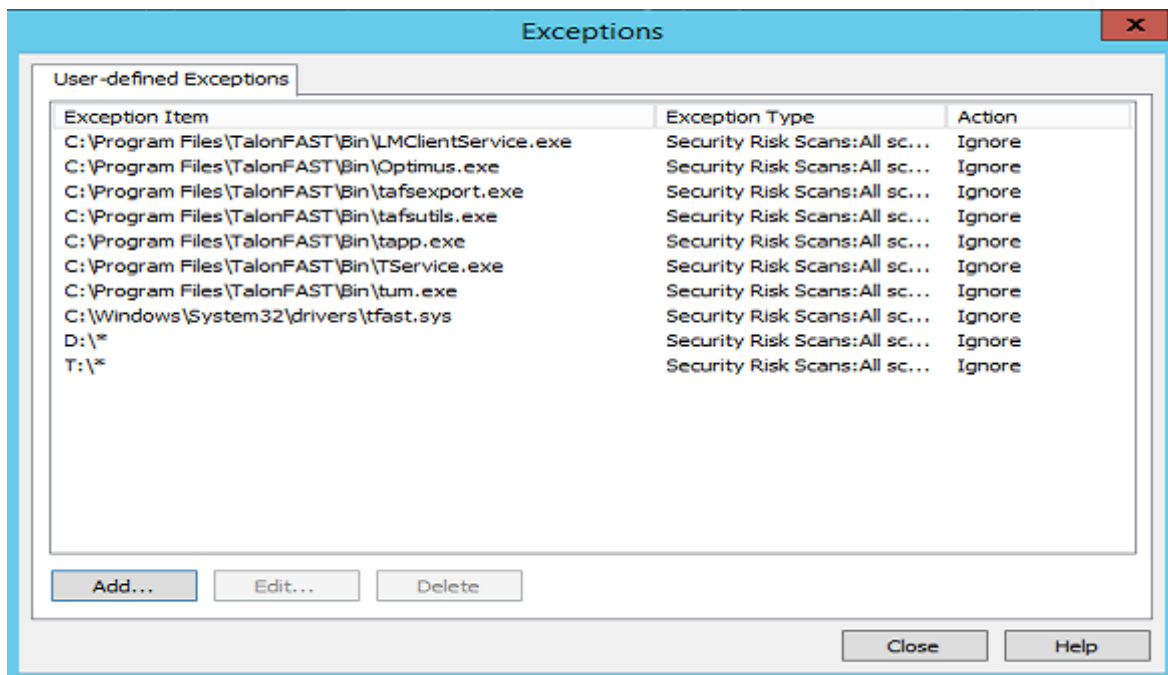


- Click **Add** -> **Security Risk Exception** -> **Folder**

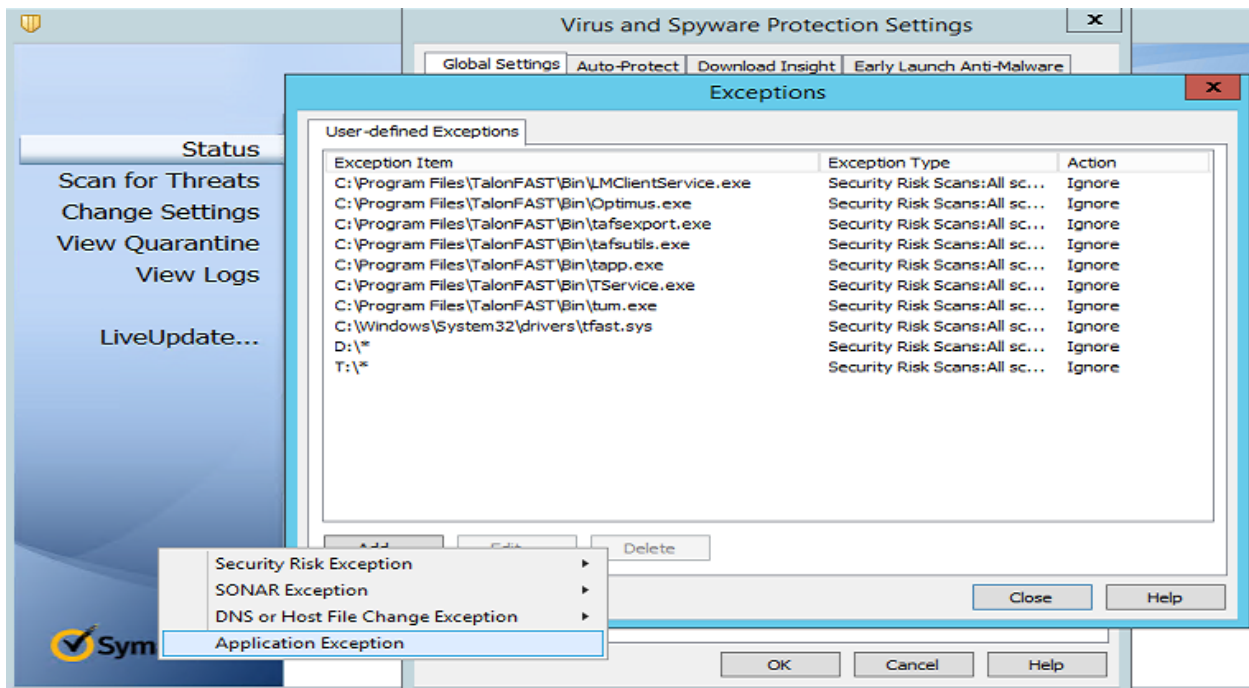


Add the following:

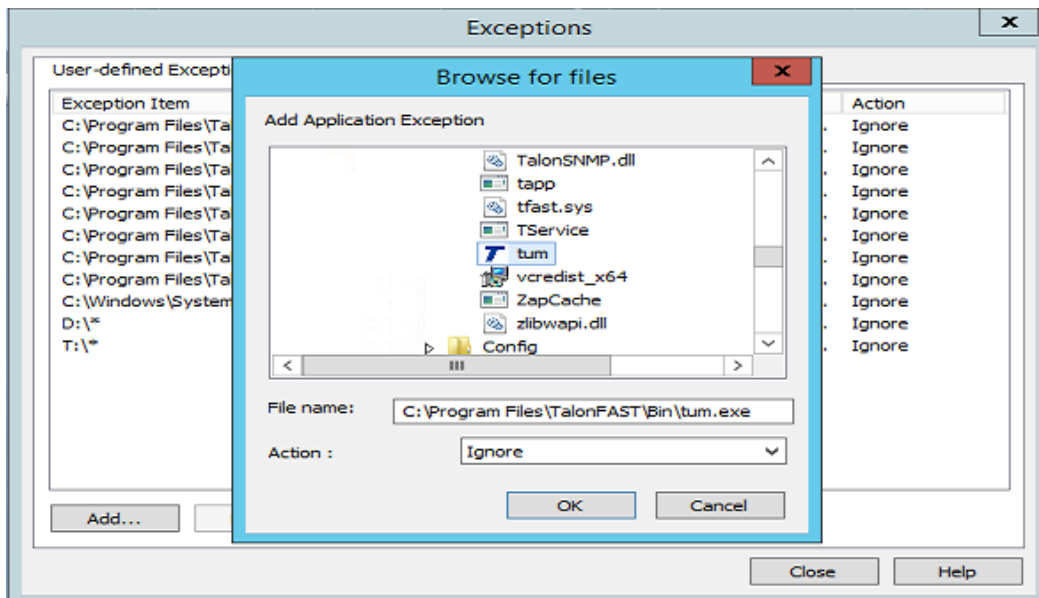
- C:\Program Files\TalonFAST\Bin\LMClientService.exe
- C:\Program Files\TalonFAST\Bin\LMServerService.exe
- C:\Program Files\TalonFAST\Bin\Optimus.exe
- C:\Program Files\TalonFAST\Bin\tafsexport.exe
- C:\Program Files\TalonFAST\Bin\tafsutils.exe
- C:\Program Files\TalonFAST\Bin\tapp.exe
- C:\Program Files\TalonFAST\Bin\tfs.exe
- C:\Program Files\TalonFAST\Bin\TService.exe
- C:\Program Files\TalonFAST\Bin\tum.exe
- C:\Windows\System32\drivers\tfast.sys



Click Add -> **Application Exception**

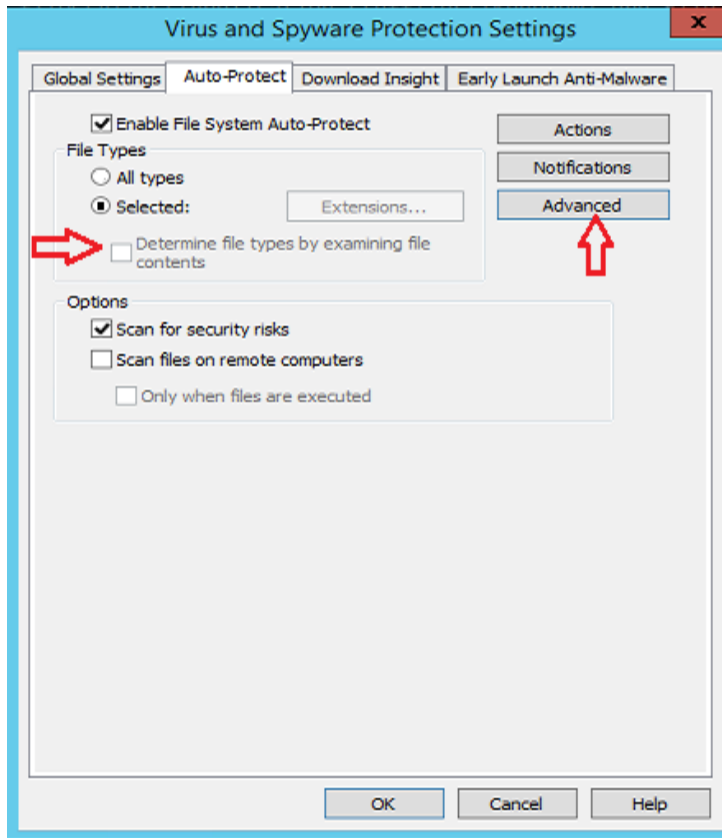


- Browse to C:\Program Files\TalonFAST\Bin\ and add tum

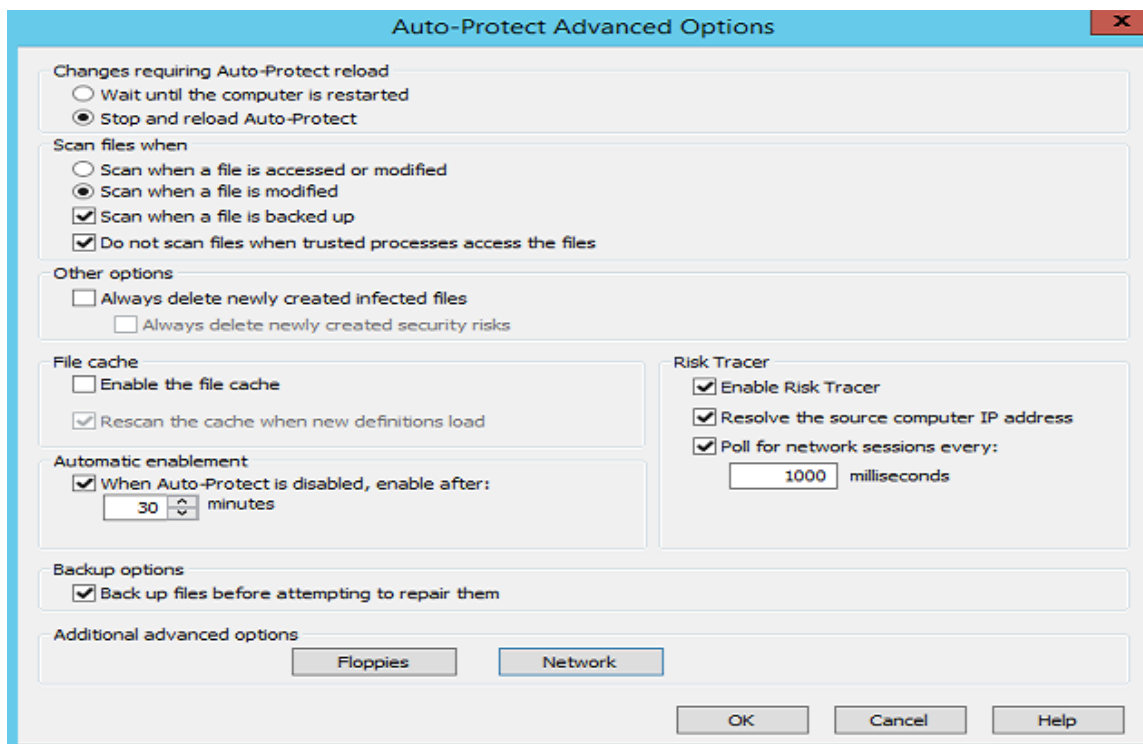


Click OK

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

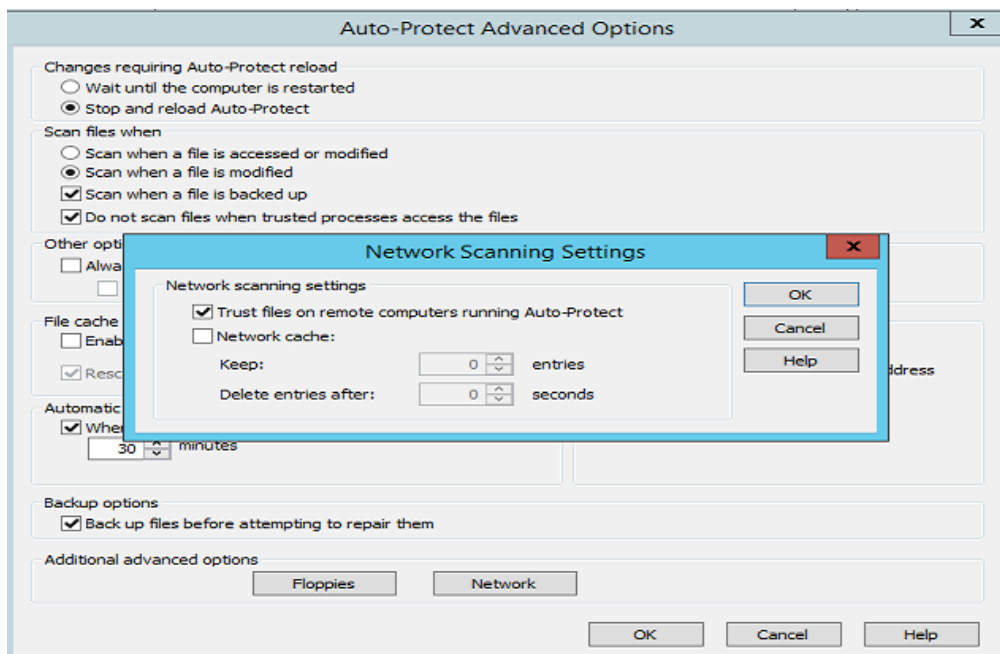


Adjust settings as shown below



Click **Network**

Uncheck **Network cache**



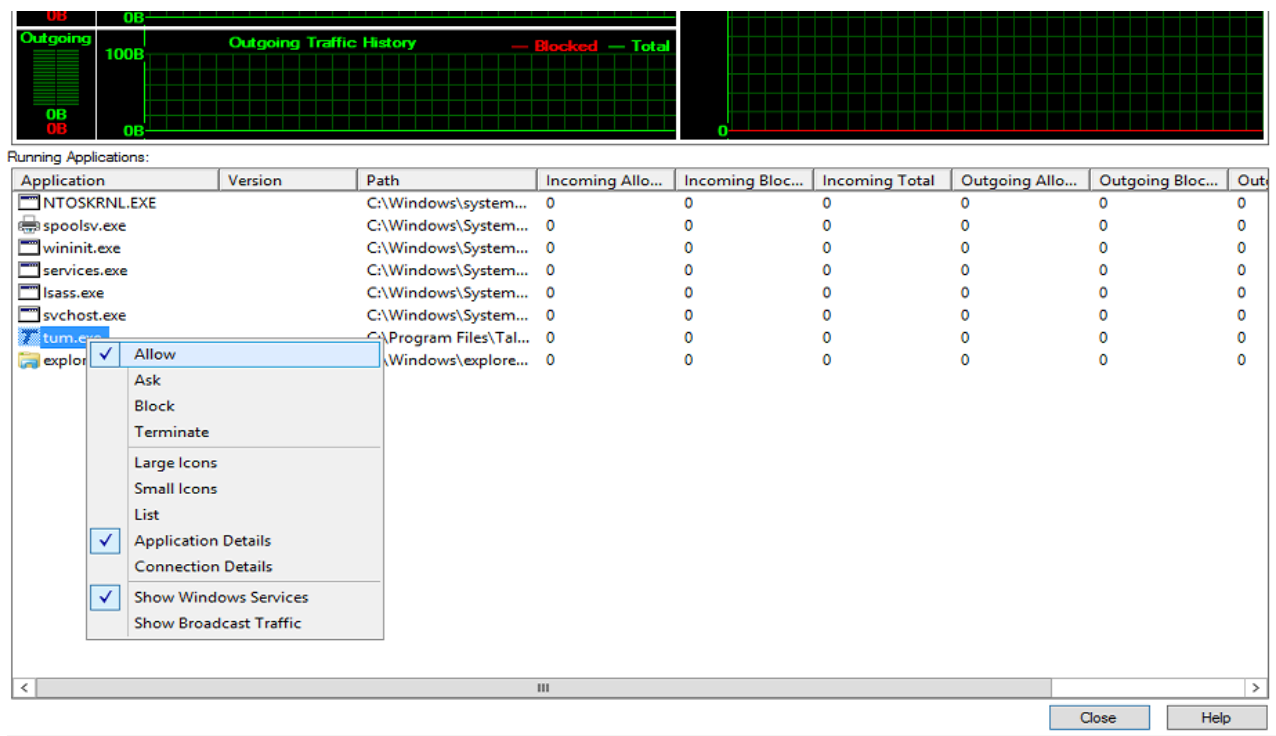
Click **OK**

**Network Threat Protection -> Click Options and select View Network Activity**





Right click **tum.exe** and select **Allow**



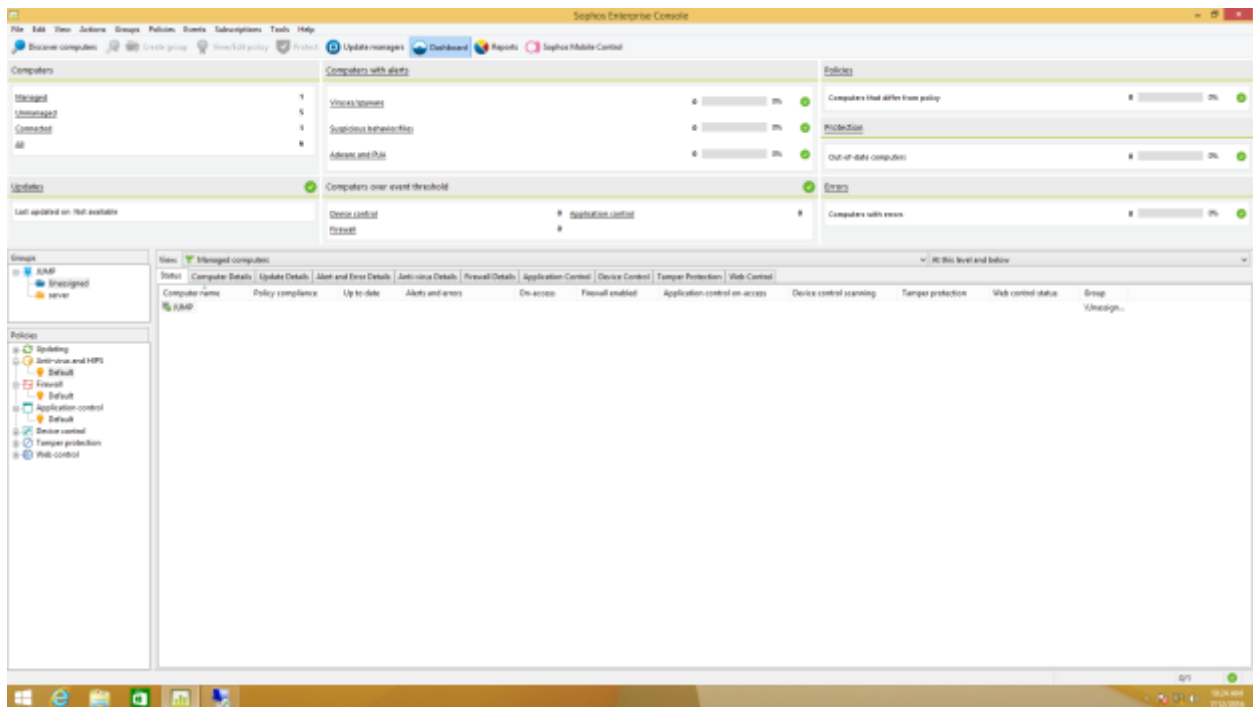
Configuration is complete.

## Sophos Endpoint Security and Control v10.x

This section outlines best practices for Sophos Endpoint Security and Control targeted for Talon FAST™ appliances based on Windows Server 2012 R2.

### 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.



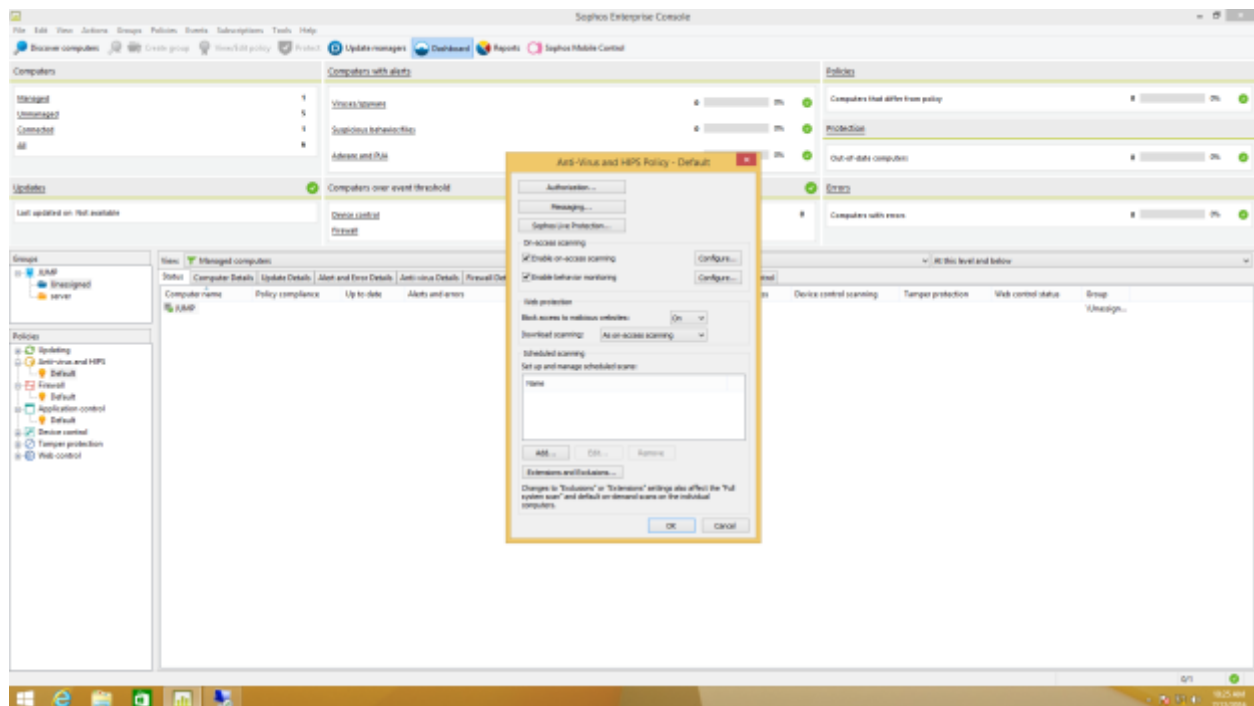
## Excluding Services and Processes using Sophos Enterprise Control

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

**Note:** Ensure that Talon FAST™ processes, services, and drives are excluded from antivirus scanning

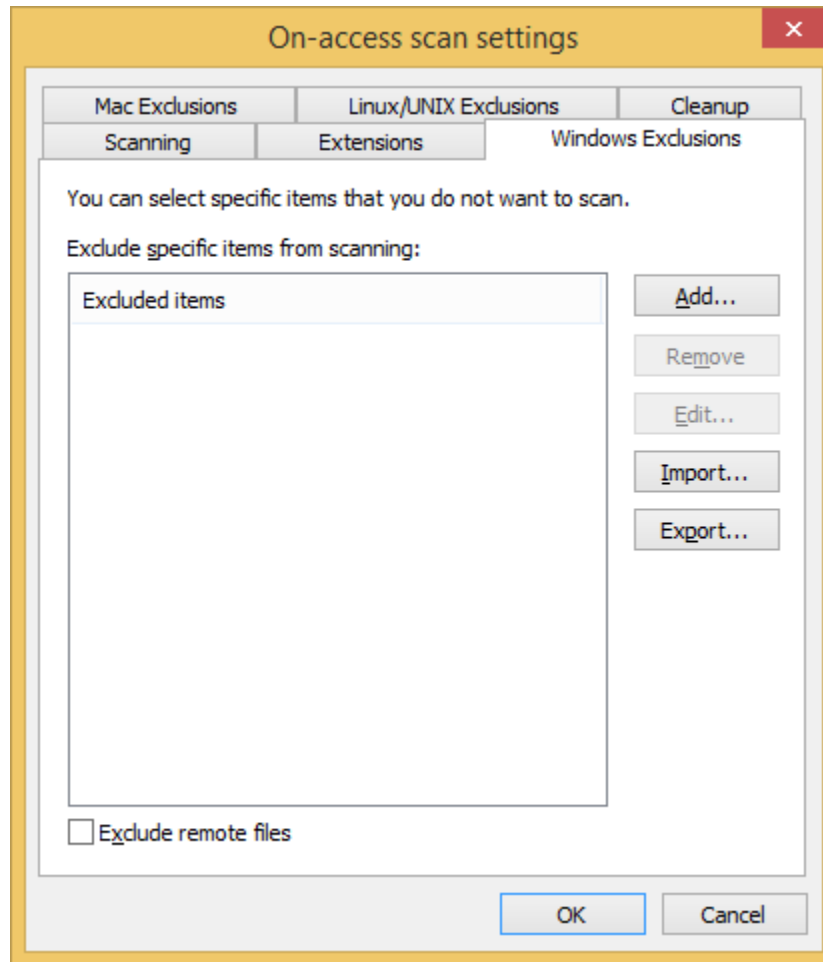
These changes should be made to Server and Client policies as well as group policy for Talon FAST™ users if applicable:

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

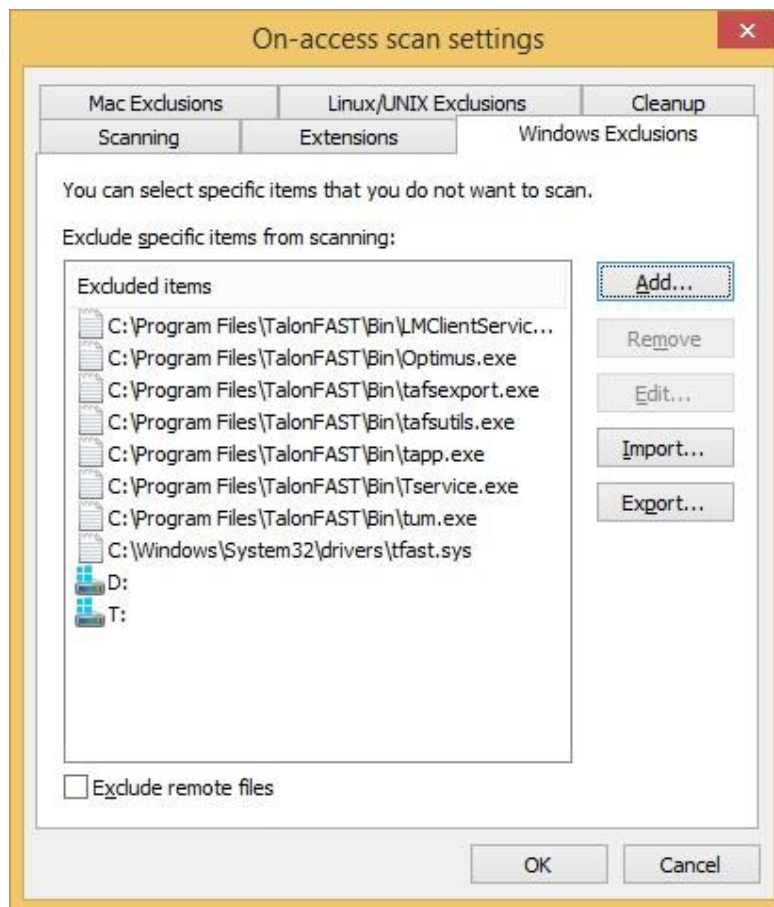


- Click the “Configure...” button next to Enable on-access scanning.

- Click the “Windows Exclusions” tab



- 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\tafsexport.exe
  - C:\Program Files\TalonFAST\Bin\tafsutils.exe
  - C:\Program Files\TalonFAST\Bin\tapp.exe
  - C:\Program Files\TalonFAST\Bin\tfs.exe
  - C:\Program Files\TalonFAST\Bin\TService.exe
  - C:\Program Files\TalonFAST\Bin\tum.exe
  - C:\Windows\System32\drivers\tfast.sys
  - D:\
  - T:\

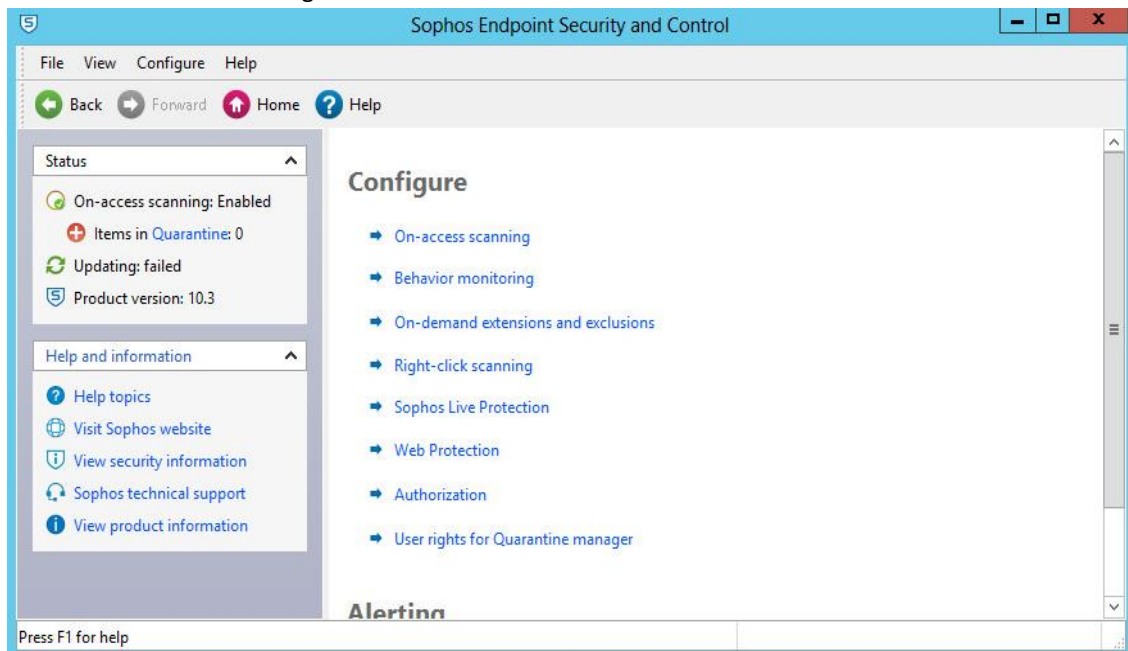


To verify the central configuration results on a connected client machine, we can use the Sophos Endpoint Security and Control panel.

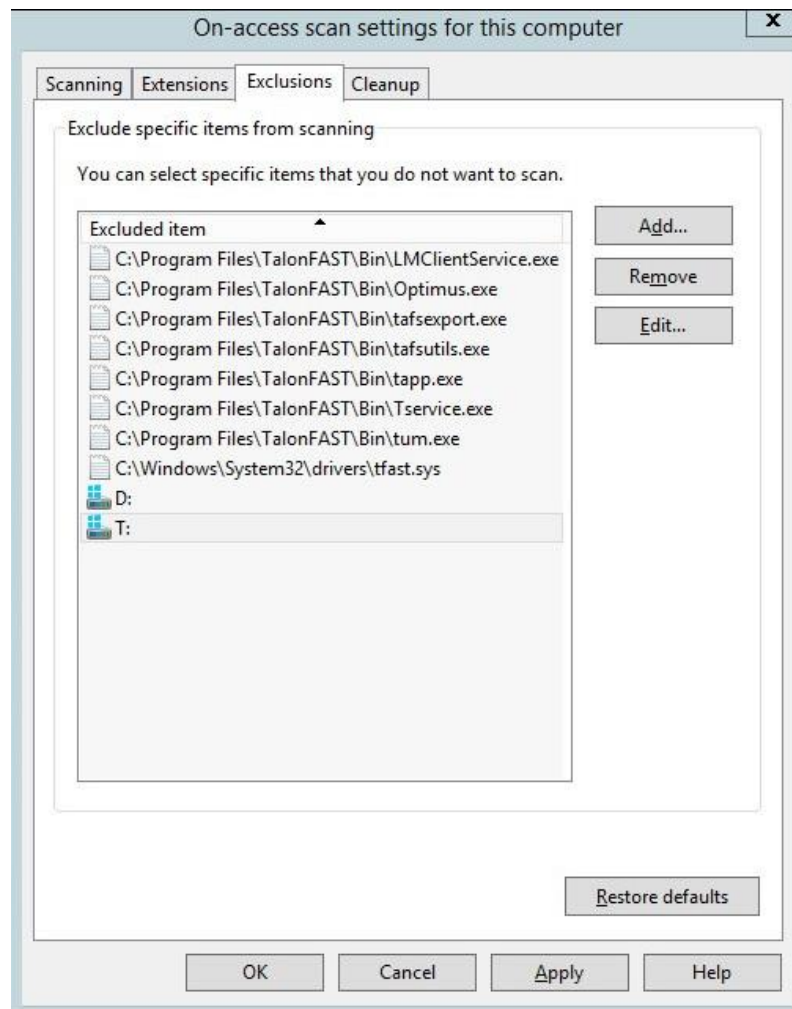
- Click “Configure anti-virus and HIPS”



- Click “On-access scanning”



- 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 2012 R2 by default includes a Microsoft Windows Firewall. Talon FAST™ software automatically provides a script to perform Microsoft Windows firewall maintenance, allowing ports associated with the Talon FAST™ product. Talon recommends the use of the Microsoft Windows firewall.

## Trend Micro Officescan

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

The screenshot displays the Trend Micro OfficeScan Management GUI. The interface includes a left-hand navigation menu with options like 'Summary', 'Security Compliance', 'Networked Computers', and 'Client Management'. The main content area is divided into several sections:

- Summary:** Shows a notification that new widgets are ready to be updated and lists activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, and Damage Cleanup Services.
- Client Connectivity:** A table showing the status of clients.
 

Status	Smart Scan	Conventional Scan	Total
Online	1	0	1
Offline	0	0	0
Remaining	0	0	0
<b>Total</b>	<b>1</b>	<b>0</b>	<b>1</b>
- Security Risk Detections:** A table showing detected security risks.
 

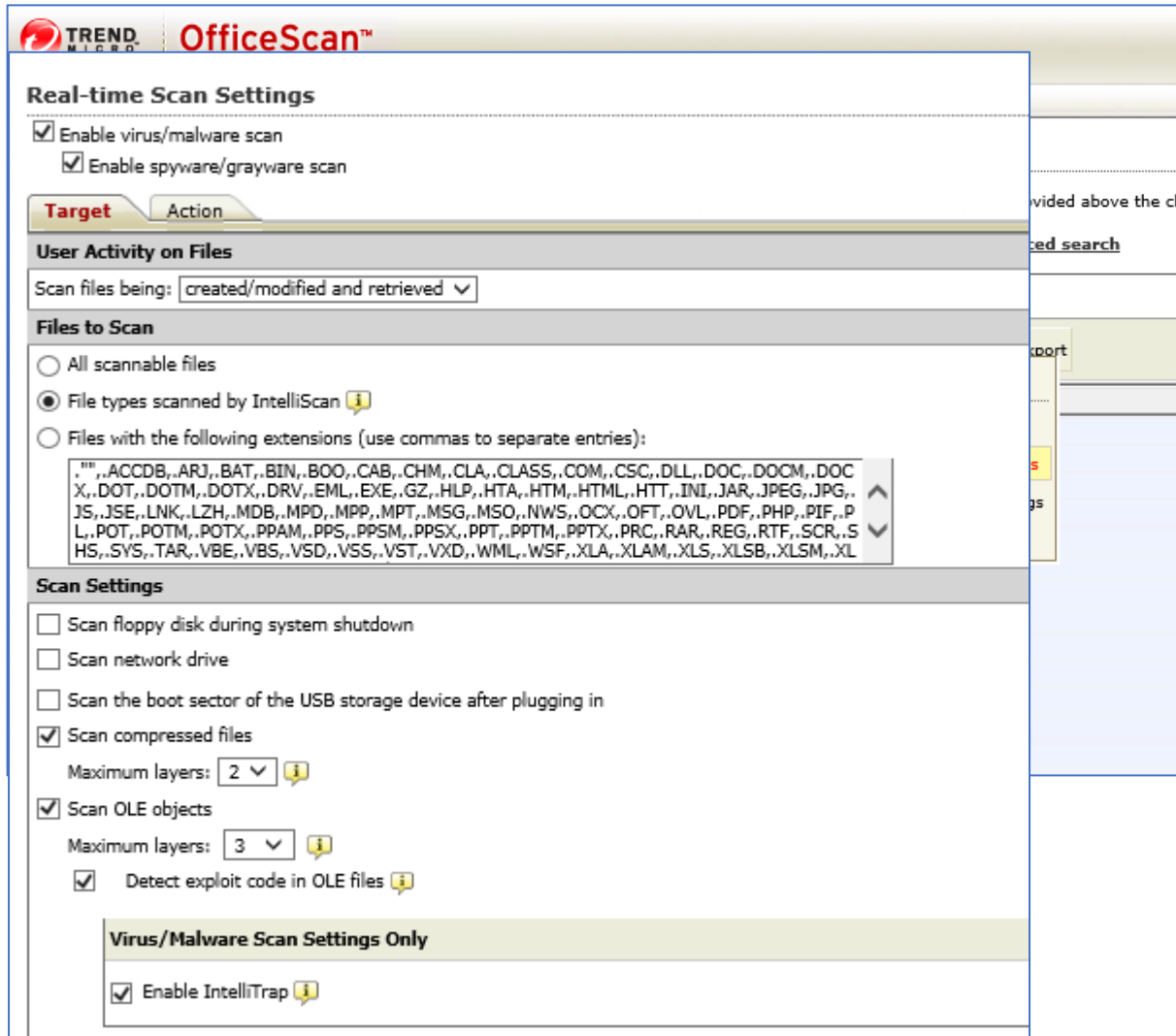
Type	Detections	Infected Computers
Virus/Malware	0	0
Spyware/Grayware	0	0
- Outbreaks:** A table showing the top 10 security risk statistics.
 

Alert Type	Current Outbreak	Last Outbreak
Virus/Malware	None	None
Spyware/Grayware	None	None
- Client Updates:** A table showing the status of client updates.
 

Component	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	9.850.000	0	0	0%
Smart Scan Agent	9.850.000	1	0	100%



- Navigate to “Scan Settings”->”Real-Time Scan Settings”.



- On the “Target” tab, enable “File types scanned by IntelliScan”.
- Directory scanning. Scroll down and add the following exclusions to “Scan Exclusion List (Directories)” to prevent Trend Micro from scanning Talon related directories:
  - C:\Program Files\TalonFAST\bin\\*
  - C:\Program Files\TalonFAST\bin
  - D:\\*
  - D:
  - T:\\*
  - T:



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\tafsexport.exe
- C:\Program Files\TalonFAST\Bin\tafsutils.exe
- C:\Program Files\TalonFAST\Bin\tapp.exe
- C:\Program Files\TalonFAST\Bin\tfs.exe
- C:\Program Files\TalonFAST\Bin\TService.exe
- C:\Program Files\TalonFAST\Bin\tum.exe
- C:\Windows\System32\drivers\tfast.sys

### Real-time Scan Settings

Enable virus/malware scan  
 Enable spyware/grayware scan

**Target**    **Action**

Enable scan exclusion  
 Apply scan exclusion settings to all scan types

#### Scan Exclusion List (Directories)

Enter the directory path (For example, c:\temp\ExcludeDir).

Exclude directories where Trend Micro products are installed

Saving does the following:

Retains client computer's exclusion list  
 Overwrites the client computer's exclusion list  
 Adds path to the client computer's exclusion list  
 Removes path from the client computer's exclusion list

	Add
C:\Program Files\TalonFAST\bin	Remove
C:\Program Files\TalonFAST\bin\*	
D:\	
D:\*	
T:\	
T:\*	

#### Scan Exclusion List (Files)

Enter the file name or the file name with full path (For example, ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp).

Saving does the following:

Retains client computer's exclusion list  
 Overwrites the client computer's exclusion list  
 Adds path to the client computer's exclusion list  
 Removes path from the client computer's exclusion list

	Add
C:\Program Files\TalonFAST\Bin\*.exe	Remove
C:\Windows\System32\Drivers\TFAST.sys	
TFAST.sys	
TService.exe	
Tapp.exe	
tum.exe	



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

Talon 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 2012 R2 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