



# FluidFS Antivirus Integration

Dell Storage Engineering  
July 2014

## Revisions

Date	Description
May 2014	Initial release
July 2014	General updates around FluidFS

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND

AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



# Table of contents

- Revisions..... 2
- Acknowledgements..... 4
- Feedback ..... 4
- Executive summary ..... 4
- 1 Introduction..... 5
  - 1.1 FluidFS antivirus client overview..... 5
    - 1.1.1 Data flow during the virus scanning process..... 6
    - 1.1.2 Detailed file access flow: configuring antivirus scanning and enabling for SMB shares ..... 6
    - 1.1.3 What triggers FluidFS to request a virus scan? ..... 7
    - 1.1.4 When a virus is found ..... 8
  - 1.2 Configuring the virus scan service on FluidFS ..... 8
    - 1.2.1 Configuring antivirus scan on the EqualLogic FS76x0 ..... 8
    - 1.2.2 Configuring antivirus scan on the Compellent FS8600..... 10
    - 1.2.3 Defining virus scanning criteria ..... 10
    - 1.2.4 Antivirus server failure ..... 11
    - 1.2.5 Configure antivirus settings for individual shares..... 11
    - 1.2.6 Configure antivirus scanning from the FluidFS CLI ..... 13
    - 1.2.7 Network topology..... 14
  - 1.3 Antivirus partners for Dell FluidFS ..... 14
- 2 Best practices for antivirus scanning..... 15
- 3 Conclusion..... 16
- A Configuring Trend Micro IWSA virus scanner..... 17
  - A.1.1 Connecting the FluidFS appliance to the virus scan service ..... 22
  - A.1.2 Verifying the virus scan ..... 22



## Acknowledgements

This best practice white paper was produced by the following members of the Dell Storage team:

Engineering: Srikanth Nandigam

Technical Marketing: Chandra Mukhyala

Editing: Margaret Boeneke

Additional contributors: Nimrod Shavit

## Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this information by sending an email to [SISfeedback@Dell.com](mailto:SISfeedback@Dell.com).



[SISfeedback@Dell.com](mailto:SISfeedback@Dell.com)

## Executive summary

To protect themselves from malicious intent, organizations enforce strict security policies regarding virus detection and removal. One common method for implementing a comprehensive virus scan for data repositories stored on NAS volumes is to leverage the Internet Content Adaptation Protocol (ICAP). The Dell Fluid File System (FluidFS), a scale-out NAS solution, has incorporated ICAP to communicate with external scan engines for on-demand virus scanning and detection. ICAP integration allows FluidFS to offload virus scanning to third party antivirus servers such as McAfee, Symantec and Trend Micro, and provides on-demand file scanning upon file read requests from client machines.

This paper provides technical best practices for using FluidFS NAS in conjunction with antivirus client services that can be configured to leverage ICAP-enabled antivirus scanning servers. You will learn how you can implement a scalable and reliable virus scanning solution for protecting valuable files served by FluidFS.



# 1 Introduction

Data housed within any storage system needs to be protected against threats from malware and viruses. Efficient protection against these threats is a very important aspect of a comprehensive data protection strategy for any organization. Computer viruses, spyware and malware, which are growing increasingly numerous and prolific, put data at risk and can have serious business implications if that data becomes compromised.

The Dell Fluid File System helps protect against viruses by integrating with on-demand virus scanning services using the Internet Content Adaptation Protocol (ICAP). A user's external antivirus engine of choice runs on an ICAP server located on the client network. This paper describes the antivirus architecture and explains the steps for configuring antivirus scanning for FluidFS. Appendix A shows an example, outlining the configuration for Trend Micro Interscan Web Security Appliance (IWSA) as the external virus scanning engine.

## 1.1 FluidFS antivirus client overview

The administrator begins by configuring the virus scan on the FluidFS cluster, FluidFS acts as an ICAP client, and the antivirus scan engine acts as an ICAP server. When an end user attempts to read a file using the SMB protocol, FluidFS triggers a virus scan and transmits the files to the ICAP antivirus scanning server, which then scans the requested file for suspicious viruses. Once complete, the ICAP server passes the scan results back to FluidFS, and FluidFS then either makes the clean file accessible to the user or blocks access by quarantining the file. FluidFS antivirus client will not initiate virus scanning while storing (writing) files on the container.

While the scan is in progress, response to the file open request are slightly delayed, which can introduce some latency for read operations, FluidFS antivirus service has a caching feature, which stores a local list of all files that have been scanned. If a user opens a file that has already been scanned (which is listed in the antivirus cache) and the file has not been modified since the last scan, it will provide access to the file without scanning it for a second time. This eliminates redundant scanning and improves read performance when antivirus is enabled

Note: File scan is triggered only when files are accessed using SMB protocol. If files are accessed via NFS, FluidFS does not initiate a virus scan. However, if files were previously blocked by the antivirus scanner, these files are not accessible by NFS. Alternatively, the network share from FluidFS can be scanned by mapping it to a host server running the antivirus client and then scanning it locally, manually or with a scheduled process.



### 1.1.1 Data flow during the virus scanning process



**Step 1:** Client attempts to open and modify an existing file.

**Step 2:** FluidFS determines if the file needs to be scanned based on the file extension, size and scanning cache (checks if previously scanned), then it notifies the antivirus server using ICAP.

**Step 3:** The antivirus server scans the file and sends the result (either *OK* or *Virus*) to the FluidFS cluster.

**Step 4:** Client access to the file is granted or denied based on the scan result.

### 1.1.2 Detailed file access flow: configuring antivirus scanning and enabling for SMB shares

The following steps outline client file access (read) on a SMB file share when using an external ICAP enabled antivirus server:

1. The SMB client accesses the file from the FluidFS container from a mapped drive or via Universal Naming Convention (UNC); for example: \\FluidFS\share1\.
2. FluidFS determines, using file attributes and the file open operation request, if the file needs to be scanned.
  - a. If no scan is needed (the file was scanned before and no updates have been made), the client is granted access and contents are returned.
  - b. If the file needs to be scanned, a scan request is issued to the antivirus scan engine
3. The virus scan engine reads the file and scans it for a virus.
4. The scan engine responds back to FluidFS with one of the following results:
  - a. File OK, no virus found.
  - b. Virus found; file quarantined.
  - c. Virus found; file repaired.
5. FluidFS responds back to the SMB client with the following results:
  - a. Client access is allowed.
  - b. Client access is denied, and FluidFS moves the virus infected file to a quarantine folder.

All files quarantined by the antivirus server are moved under a **.Quarantine\<Date Stamp>** folder on the FluidFS NAS volume.







 eicar.com.800000000000010080000000000...	2/24/2014 1:11 PM	INFECTED File	1 KB
 eicar.com.800000000000010080000000000...	2/24/2014 1:12 PM	INFECTED File	1 KB
 eicar.com.800000000000010080000000000...	2/24/2014 2:57 PM	INFECTED File	1 KB
 eicar.com.800000000000010080000000000...	2/24/2014 4:48 PM	INFECTED File	1 KB
 eicar.com.800000000000010080000000000...	2/24/2014 5:16 PM	INFECTED File	1 KB
 quarantine-list	2/24/2014 5:16 PM	Text Document	1 KB

Figure 1 Sample file list of quarantine folder

A file called **quarantine-list** is created on the on the NAS volume with a folder name **.Quarantine\<Date Stamp>** with information about all viruses found and their quarantine location on FluidFS.

```
SHARE_NAME=test_virus:ORIG_FNAME=\230016\ecar.com:THREAT=Eicar_test_file:QUAR_FNAME=eicar.com.8000000000000100800000000001C8D.infected:QUAR_USER=S-1-5-21-3013153020-774773256-2344179283-500
```

```
SHARE_NAME=test_virus:ORIG_FNAME=\230016\New folder\ecar.com:THREAT=Eicar_test_file:QUAR_FNAME=eicar.com.8000000000000100800000000001CB8.infected:QUAR_USER=S-1-5-21-3013153020-774773256-2344179283-500
```

```
SHARE_NAME=test_virus:ORIG_FNAME=\230016\ecar.com:THREAT=Eicar_test_file:QUAR_FNAME=eicar.com.8000000000000100800000000001DB1.infected:QUAR_USER=S-1-5-21-3013153020-774773256-2344179283-500
```

```
SHARE_NAME=test_virus:ORIG_FNAME=\230016\ecar.com:THREAT=Eicar_test_file:QUAR_FNAME=eicar.com.8000000000000100800000000001E06.infected:QUAR_USER=S-1-5-21-3013153020-774773256-2344179283-500
```

```
SHARE_NAME=test_virus:ORIG_FNAME=\230016\ecar.com:THREAT=Eicar_test_file:QUAR_FNAME=eicar.com.8000000000000100800000000001EF1.infected:QUAR_USER=S-1-5-21-3013153020-774773256-2344179283-500
```

Figure 2 Sample entries of the quarantine-list file

### 1.1.3 What triggers FluidFS to request a virus scan?

- Any read request (file open) from an SMB client on previously unscanned files
- Any read request (file open) from an SMB client on previously scanned files if the antivirus server updated its virus patterns or virus scan engine versions
- Any file operations that involve SMB client reading, such as modifying an existing file
- Copying or moving files triggers a scan request to the external AV server using ICAP

FluidFS does not send a scan request upon the following conditions:

- New files are stored on FluidFS.
- File access using NFS (Files marked as infected cannot be accessed over NFS.)

- If files on FluidFS were previously scanned and no updates were made to the file. In this case, both SMB and NFS clients are granted direct access to files.

### 1.1.4 When a virus is found

FluidFS plays a passive role in the event that a virus is found by the antivirus scan engine. The IT administrator determines how a virus is handled, according to settings in the antivirus software configuration. Typically, if a file is found to be infected, the virus software takes one of two actions: it will clean or quarantine the file.

Actions by the antivirus scanner when a virus is found:

- **Clean the file:** The antivirus software removes the virus and notifies FluidFS that the file is clean and allows client access to that file.
- **Quarantine the file:** The antivirus scanner quarantines the file or moves it to a special location (.quarantine folder on the share), and FluidFS denies the client access.

## 1.2 Configuring the virus scan service on FluidFS

This section describes the sequence of steps for enabling and configuring the antivirus service on the EqualLogic FS76x0 and the Compellent FS8600.

### 1.2.1 Configuring antivirus scan on the EqualLogic FS76x0

1. From the EqualLogic Group manager GUI, select the FluidFS NAS cluster and choose **Advanced settings**. Under **Antivirus Defaults for SMB shares**, check **Enable virus scanning**. Once the virus scanning is enabled, configure the antivirus servers.



Figure 3 Enabling antivirus scanning on the FS76x0

2. Click on **Configure Antivirus servers** to add the IP addresses or hostnames of antivirus scanning servers. Configure the default port for antivirus server, port 1344, to match the configuration on the ICAP antivirus server port.





Figure 4 Antivirus server configured on default port 1344

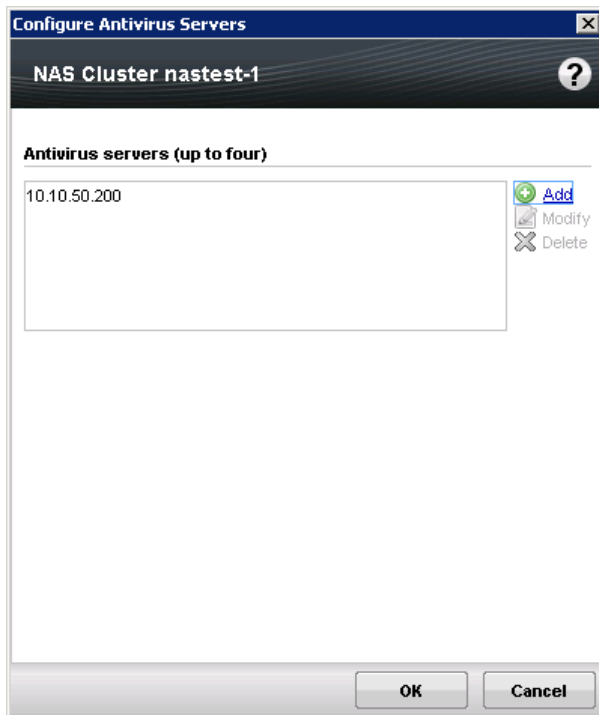


Figure 5 Adding antivirus servers on FS76x0

## 1.2.2 Configuring antivirus scan on the Compellent FS8600

This section describes the sequence of steps involved in enabling and configuring the antivirus service on the Compellent FS86x0

1. From Compellent Enterprise Manager GUI, Select NAS Cluster and choose System. Under Antivirus Hosts Choose Add Antivirus Scanner and configure the Antivirus servers.



Figure 6 Add Antivirus to the FS8600

2. Click Add Antivirus Scanner to add the IP addresses or hostnames of the antivirus scanning servers. Configure the default port for antivirus server, port 1344, to match on the configuration on the ICAP antivirus server port.

A dialog box titled "Add AntiVirus Scanner" with a close button (X) in the top right corner. It contains two input fields: "Name" and "Port". The "Port" field is pre-filled with the value "1344". At the bottom, there are three buttons: "? Help", "X Cancel", and "OK" with an upward arrow icon.

Figure 7 Configure antivirus on FX8600

### AntiVirus Hosts

AntiVirus Hosts			Events
Name	Port	State	
LAB-AV1	1344	Available	

Figure 8 Antivirus list on FS8600

## 1.2.3 Defining virus scanning criteria

The following options provide a way to exclude certain files from scanning based on file extensions, size of files and certain directory paths.

## Antivirus Defaults for CIFS Shares

### Virus scanning

☒ Enable virus scanning

### Large file handling

\* Exclude files larger than: 3 GB (max 2048TB)

☒ Allow user access to unscanned files.

### File extensions to exclude

[Add](#)  
[Modify](#)  
[Delete](#)

### Directory paths to exclude

Figure 9 Defining virus scanning criteria

## 1.2.4 Antivirus server failure

Dell best practices recommend configuring more than one antivirus server on the FluidFS NAS cluster to prevent the antivirus scan engine from becoming a single point of failure. If one or more antivirus scanning servers fail or are unavailable, FluidFS will continue to use the remaining scanning servers for sending the scan requests.

If no scanning servers are available, SMB shares that have antivirus enabled will deny all read requests. Alternatively, the administrator can manually disable antivirus scanning temporarily on a per SMB share basis.

When the antivirus server is back online, FluidFS resumes normal operations with virus scanning enabled.

## 1.2.5 Configure antivirus settings for individual shares

Individual shares can have their own antivirus policies and, by default, they inherit all global settings. However, you can change these settings by going to **NAS volume**, selecting **SMB shares** and modifying its properties. These settings override the default settings for that particular SMB share. This also provides a mechanism to disable antivirus settings for individual shares and manage data protection policies at a more granular level.

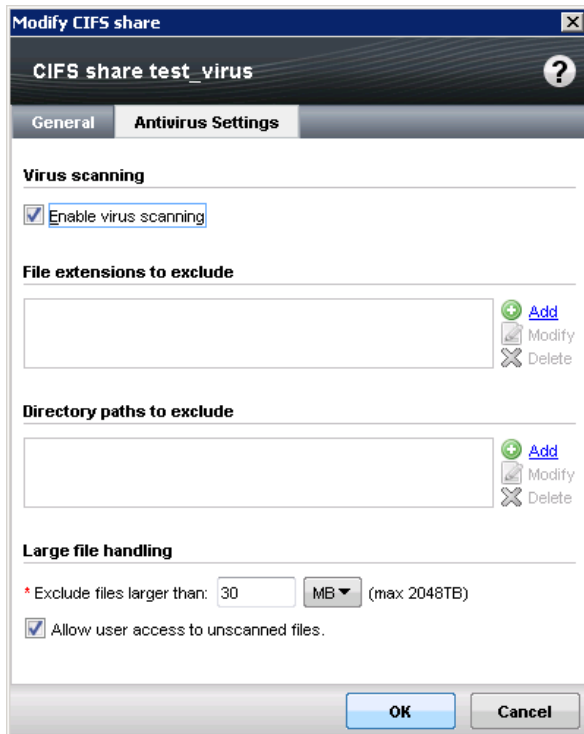


Figure 10 Configuring antivirus setting for individual FluidFS shares on the EqualLogic FS76x0

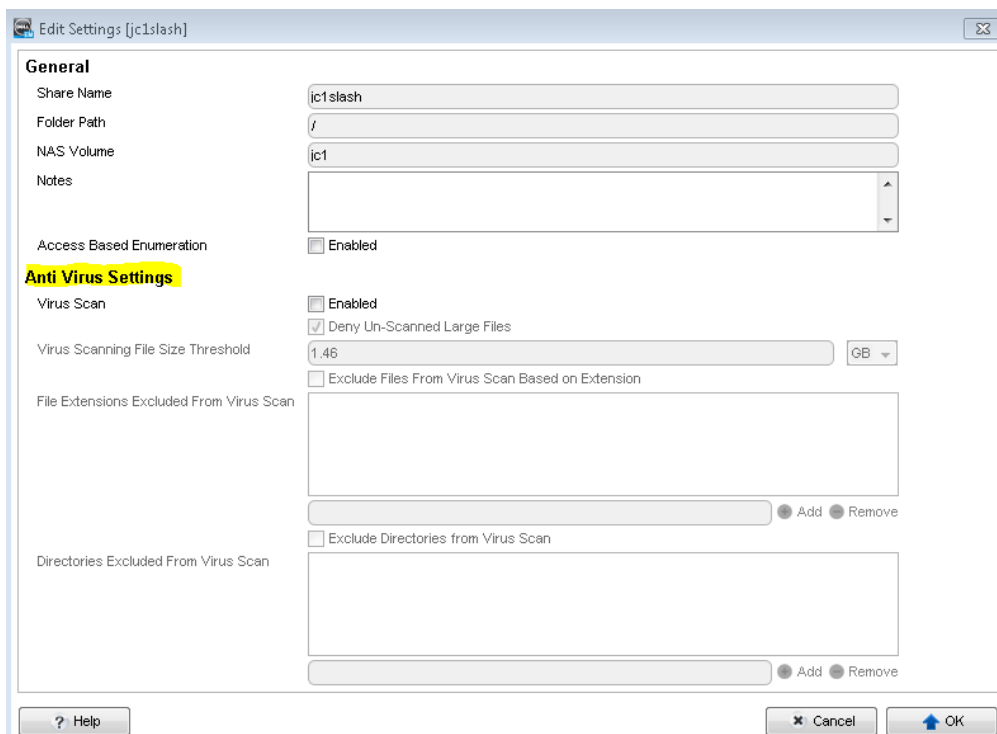


Figure 11 Configuring antivirus setting for individual FluidFS shares on the Compellent FS8600

## 1.2.6 Configure antivirus scanning from the FluidFS CLI

The antivirus scanning servers can also be configured using the native FluidFS CLI. Choose **System -> Data-protection -> Antivirus-scanners** from the CLI to add, modify or view ICAP enabled antivirus servers.

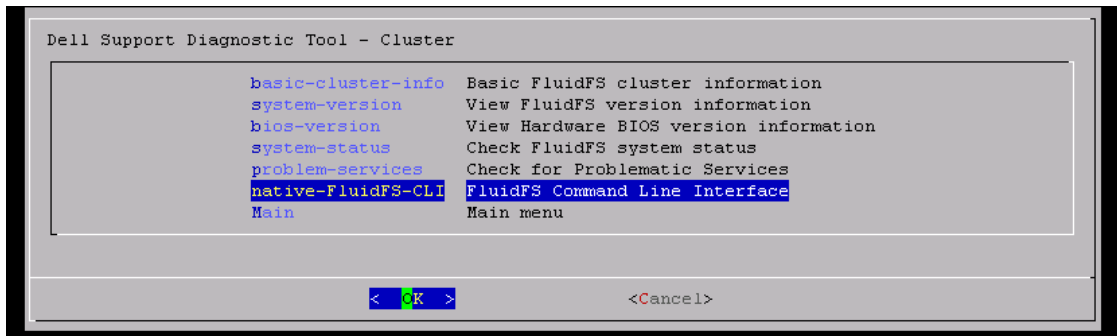


Figure 12 Accessing the native FluidFS CLI

```
CLI> system

Available menus:

    time
    data-protection
    mail-configuration
    administrators
    SNMP
    licenses
    software-updates
    internal
    background-operations
    EQL

CLI/system> data-protection

Available menus:

    antivirus-scanners
    NDMP-configuration
    cluster-partnerships

CLI/system/data-protection> antivirus-scanners

Available commands:

    view
    add
    delete

CLI/system/data-protection/antivirus-scanners> view
Hosts = .-----,-----,
| Name | Port |
|-----|-----|
| 10.10.50.200 | 1344 |
|-----|-----|

CLI/system/data-protection/antivirus-scanners> █
```

Figure 13 Configuring antivirus from the FluidFS CLI

## 1.2.7 Network topology

The FluidFS cluster requires a LAN TCP/IP network connection to access the antivirus servers. For better performance, the external third party server must reside on the FluidFS client network and be accessible without any external routing. For high availability and performance, a minimum of two network interfaces are required to be connected to the same client network as FluidFS client network.

More than one antivirus server is required for high availability and load balancing, so SMB clients may continue to access files from FluidFS shares, even if one of the antivirus servers is unavailable. The FluidFS antivirus service generates extra traffic on the FluidFS client network when the ICAP communication happens between FluidFS nodes and the external third party antivirus server. Dell recommends isolating the management traffic from the ICAP traffic and using the management network for connecting to the internet for virus pattern updates.

## 1.3 Antivirus partners for Dell FluidFS

Dell has partnered with and certified the following external antivirus vendors:

Table 1 Antivirus partners for Dell FluidFS

Partner Name	Product
McAfee	Virus Scan Enterprise
Symantec	Scan Engine Article "How to" URL <a href="http://www.symantec.com/docs/HOWTO83461">http://www.symantec.com/docs/HOWTO83461</a>
Sophos	Endpoint Security and Control
Trend Micro	Interscan Web Security Appliance (IWSA)

**Note:** Always refer to the FluidFS support matrix for the latest information on third party certifications: [http://en.community.dell.com/techcenter/extras/m/white\\_papers/20440246/download.aspx](http://en.community.dell.com/techcenter/extras/m/white_papers/20440246/download.aspx)



## 2 Best practices for antivirus scanning

- Use more than one antivirus scanning server. If one server is unavailable, FluidFS can route the scan requests to other servers and provide client access to the scanned files.
- Use a dedicated antivirus scanner server with adequate CPU and memory, because it will improve the number of antivirus requests that can be processed at a given time. Follow the antivirus partner design guidelines for optimal configuration.
- Connect the FluidFS cluster and antivirus server to the client network using at least a 1 GigE network.
- Measure the read performance impact on scanning large files (greater than 1 GB) and appropriately set the antivirus policies within FluidFS. Bigger files tend to take more time to read and scan and increase the response time to the SMB/NFS clients, so consider setting limits at the FluidFS and ICAP server.
- Use the default ICAP port 1344 if possible. When the ICAP server port is changed, FluidFS requires additional steps to enable communication on the new port. These steps include re-configuring the antivirus service on FluidFS with the new port and re-enabling antivirus for each individual SMB share.



### 3 Conclusion

Antivirus client services on FluidFS can be configured to leverage ICAP-enabled antivirus scanning servers to provide a scalable and reliable virus scanning solution for protecting valuable data stored on FluidFS storage. With this solution, IT administrators can offload the burden of scanning the files from the FluidFS cluster onto an external antivirus scanning platform. This works transparently to FluidFS clients and avoids the need to install antivirus on each client and scanning them locally for viruses. FluidFS is integrated with many antivirus vendors and thus gives users the flexibility to choose the appropriate solution for each environment and provides the best user experience.





## A Configuring Trend Micro IWSA virus scanner

Use the following steps to configure Trend Micro IWSA antivirus server in ICAP mode.

1. Once the Interscan Web Security Appliance (IWSA) server admin is logged on to the console, select **Deployment Wizard** under **Administration**.
2. Configure the ICAP port that the scanner will monitor for scan requests from FluidFS, and set the network configuration properties such as IP addresses, DNS server and gateway.

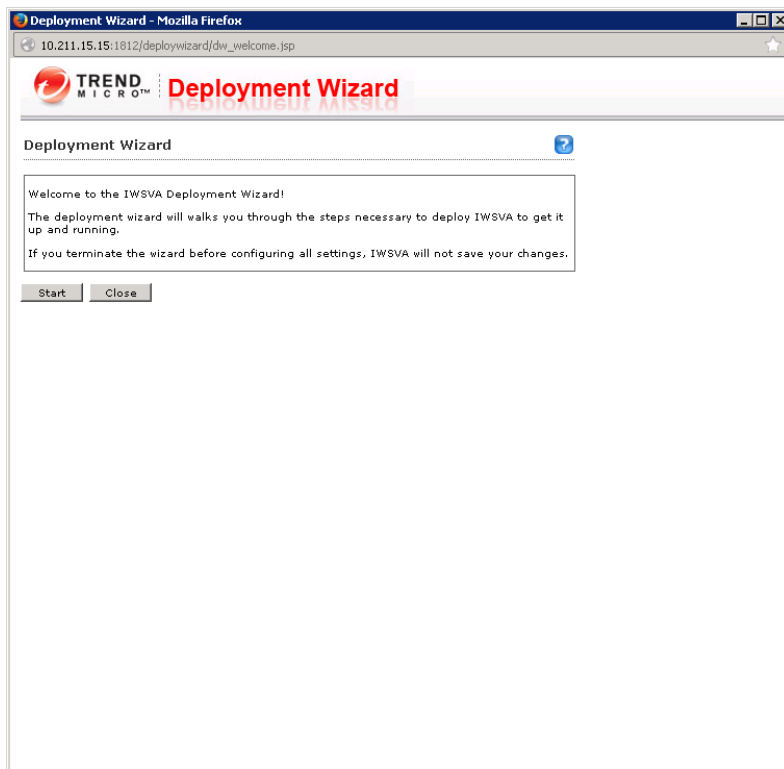


Figure 14 Configuring Trend Micro antivirus server

3. Selecting ICAP mode allows ICAP clients such as FluidFS to communicate for virus scanning. The Deployment Wizard starts by setting the mode of operation for the IWSVA server. Set the IWSVA to **ICAP mode**.

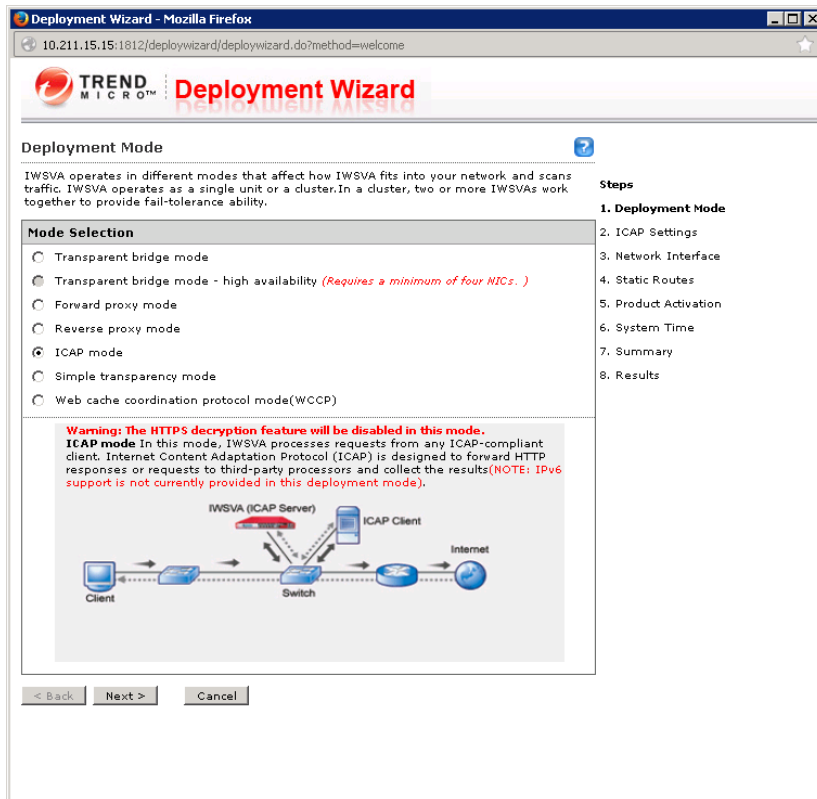


Figure 15 Configuring Trend Micro ICAP server

4. Enable both **X-Virus-ID** and **X-Infection-Found** header options to ensure that FluidFS receives the necessary scan results.
5. The screenshot shows the default value of 1344 for the listening port. This is the same value as the default value used in FluidFS antivirus settings. If the value is changed here, make sure to also change it in the antivirus settings on FluidFS.

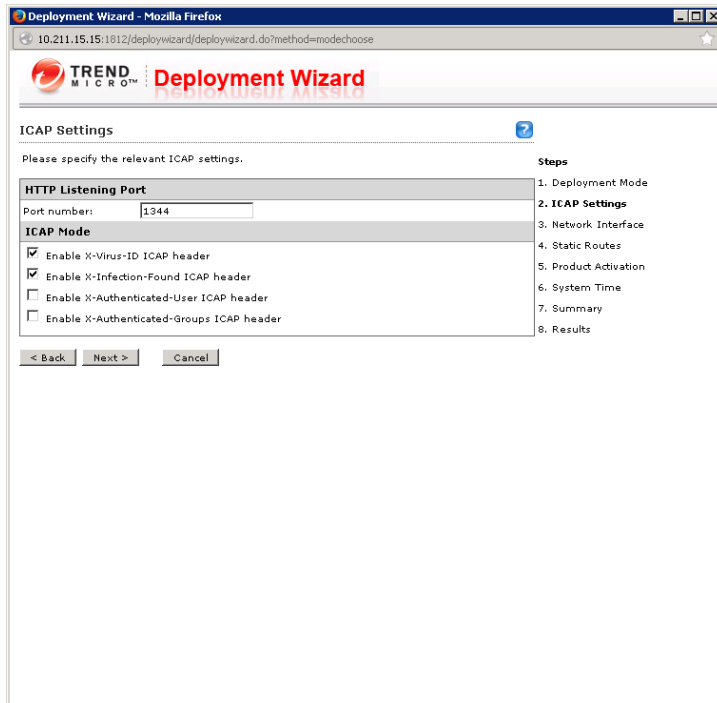


Figure 16 Configuring ICAP headers on Trend Micro Server

6. Select a different management network interface. By doing so, the ICAP communication between IWSA and FluidFS is isolated on a dedicated network, and the management network is dedicated for managing and monitoring the IWSA, including updating virus patterns through the internet.

Figure 17 Configuring Networking on Trend Micro Server

7. Dell recommends keeping FluidFS and IWSA chronologically in sync with each other so that logging information can be easily cross-referenced when needed. To accomplish this, use the same NTP server for both.

**Deployment Wizard - Mozilla Firefox**

10.211.15.15:1812/deploywizard/deploywizard.do?method=staticroutes

**TREND MICRO™ Deployment Wizard**

**System Time** ?

Please specify the system time settings.

**System Time Settings**

☐ Current system time: **03/06/2014** **10:41:06**  
mm/dd/yyyy hh:mm:ss

☒ Synchronize with NTP server

Primary NTP server: \*

Secondary NTP server:

☒ Automatically synchronize every :

☐ Synchronize after deployment

☐ Manually:    
mm/dd/yyyy hh:mm:ss

**Time Zone**

Continent:  City:

< Back Next > Cancel

**Steps**

1. Deployment Mode
2. ICAP Settings
3. Network Interface
4. Static Routes
5. Product Activation
- 6. System Time**
7. Summary
8. Results

Figure 18 Configuring NTP for antivirus server

8. The Summary display allows you to verify that all settings are correct before you submit them.

**Deployment Wizard - Mozilla Firefox**  
 10.211.15.15:1812/deploywizard/deploywizard.do?method=systemtime

**TREND MICRO™ Deployment Wizard**

**Summary** ⓘ

Below is a summary of your configuration. Check these settings and then click Submit to apply them, or click Back to edit them.

**test (ICAP mode)**

**HTTP Listening Port:** 1344

**ICAP Mode**

- ☒ Enable X-Virus-ID ICAP header
- ☒ Enable X-Infection-Found ICAP header
- ☐ Enable X-Authenticated-User ICAP header
- ☐ Enable X-Authenticated-Groups ICAP header

**IPv4 Protocol**

**Data Interface**

Ethernet Interface: eth1 ☒ Enable ping  
 IPv4 address: 10.10.50.200 / 255.255.255.0

**Separate Management Interface**

Ethernet Interface: eth2 ☐ Enable ping  
 IPv4 address: 10.211.15.15 / 255.255.255.192

**Miscellaneous Settings**

Gateway: 10.211.15.62  
 Primary DNS server: 10.10.82.190  
 Secondary DNS server:

☐ Enable IPv6 Protocol

**Settings**

Network ID	Netmask	Router	Interface

**System Time Settings**

**Steps**

1. Deployment Mode
2. ICAP Settings
3. Network Interface
4. Static Routes
5. Product Activation
6. System Time
- 7. Summary**
8. Results

Figure 19 Deployment wizard summary

## A.1.1 Connecting the FluidFS appliance to the virus scan service

Now that the IWSA scan engine is up and running, set FluidFS to connect to the scan engine through the ICAP interface. Follow the steps in Section A.1.2, below.

## A.1.2 Verifying the virus scan

To verify the correct functioning of the virus scan service, you can use virus test files from the web site [www.eicar.org](http://www.eicar.org). Copy those files onto a test machine to access a share from the FluidFS appliance that has been set up for testing.

Create a test SMB share on the FluidFS appliance and enable the virus scan option for that share.

Map the share on a client you can use for copying the virus test files onto the share. Download the EICAR test files and copy them to a directory on the SMB share. Add one or more regular text files as well so you can see the difference in behavior when accessing infected files and non-infected files. After copying, try to access the files and observe that access to files detected as containing a virus is denied.

Check the dashboard and the logging details of the IWSA to see if the files containing viruses were detected.

EqualLogic Group Manager monitoring also logs all entries related to virus detection in its event log.

Severity	Date and Time	Member ID	Message
Info	2/24/2014 5:16:52 PM	eq 204 59.2.24	Virus (Eicar_test_file) was found in file eicar.com on NAS container test_virus during access to CIFS share test_virus. File is moved to quarantine (new path is .Quarantine/2014-2-24/eicar.com.80000000000001008000000000001EF1.infected).
Info	2/24/2014 4:51:22 PM	eq 204 59.2.24	Virus (Eicar_test_file) was found in file eicar.com on NAS container test_virus during access to CIFS share test_virus. File is moved to quarantine (new path is .Quarantine/2014-2-24/eicar.com.80000000000001008000000000001E06.infected).
Info	2/24/2014 1:22:05 PM	eq 204 59.2.21	Virus (AV scan result got from FS cache) was found in file .Quarantine/2014-2-24/eicar.com.80000000000001008000000000001CB8.infected from share test_virus on NAS container test_virus. Quarantine action is not possible for this file, access to file is denied
Info	2/24/2014 1:14:08 PM	eq 204 59.2.24	Virus (Eicar_test_file) was found in file New folder\ecar.com on NAS container test_virus during access to CIFS share test_virus. File is moved to quarantine (new path is .Quarantine/2014-2-24/eicar.com.80000000000001008000000000001CB8.infected).

Figure 20 FluidFS event log entries showing virus files