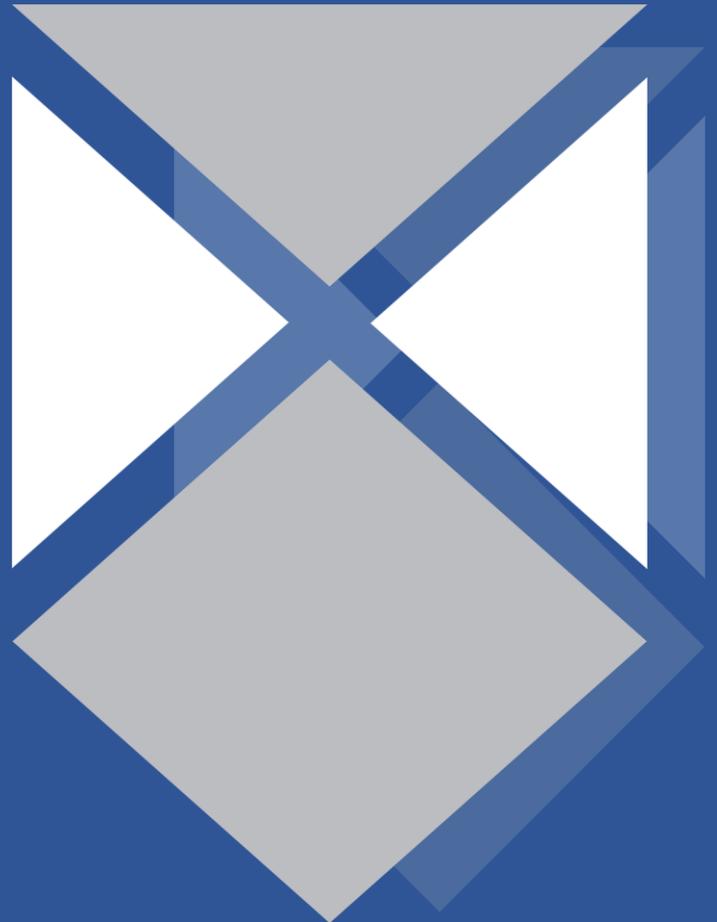# DefendX Software Control-Audit™

Release Notes

Version 5.1

These Release Notes contain supplemental information about Control-Audit Version 5.1

Contents

Using this Product

Product Documentation

This product comes with an Installation/User's Guide that includes introductory information about DefendX Software Control-Audit™, detailed instructions for installing and using DefendX Software Control-Audit™. The Installation and User's Guide exists as an Adobe Acrobat .pdf file on the DefendX Software Support Portal Page (http://www.defendx.com/support-portal/). After installing this product, refer to this guide for complete information on how to use this product.

Installing on networks with multiple domains

DefendX Software Control-Audit™ works within DefendX Software's® Smart Policy Manager™ hierarchical server management environment. As with any enterprise-level application, Smart Policy Manager™ enabled DefendX Software Control-Audit™ servers need to communicate with each other through a Windows® security context that is valid to all nodes in the Smart Policy Manager™ hierarchy. This is because DefendX Software Control-Audit™ and Smart Policy Manager™ work within the established Windows® security environment rather than creating an additional user management system for you to administer.

You can use DefendX Software Control-Audit™ and Smart Policy Manager™ with any Windows® domain model (single, master, multiple-master, complete trust), or with a hybrid model, assuming the service account you specified while installing all DefendX Software Control-Audit™ servers is consistent.

We recommend installing the Smart Policy Manager™ component of DefendX Software Control-Audit™ so it uses a service account that is created in a master domain within the Windows® domain infrastructure. Once the initial Smart Policy Manager™ service is installed, subsequent installations of Smart Policy Manager™ should reference that same account as the service account for that server.

The DefendX Software Control-Audit™ component must have Admin rights in all domains in which users or groups are defined in the Audited Users & Groups, or Exempt Users & Groups for any policy.

New Features:

- Increased the size of the sid fields in the database to accommodate sids that are larger than 64 chars. The fields have been updated to include the max size of 256 characters.

- Feature: The database import processing is now multi-threaded and can be dynamically changed via the registry.

- Feature: Added functionality to allow browsing for directories/shares when adding directories/shares to policies for the NAS versions.

- Enhanced the multi-threaded import. Files that have been queued to be imported have .queued appended to the name for a visual queue as to what is currently queue and what is not.

- Product has been rebranded as DefendX Control-Audit

- Services are now 64bit.

- Support for the contract license has been added.

- NetApp C-mode enhancements on configuration screen to allow for http/https and a specified port for the api communication and allows picking a specific ip address and port for listening for fpolicy notifications.

- TB License enforcement – this is based on the allocated storage of what is being managed.

- Email notifications for license enforcement

- Updated the Reports installer components to use the .net 4.x framework instead of the 2.0 framework. The 2.0 framework is no longer required.

- Updated the cryptography algorithm to use a FIPS compliant algorithm

Some notes:

Notes:

Since Unity uses CEE to send notifications to File Auditor just like the VNX does, the requirement for Unity are the same as VNX. The service account needs to have the EMC Virus
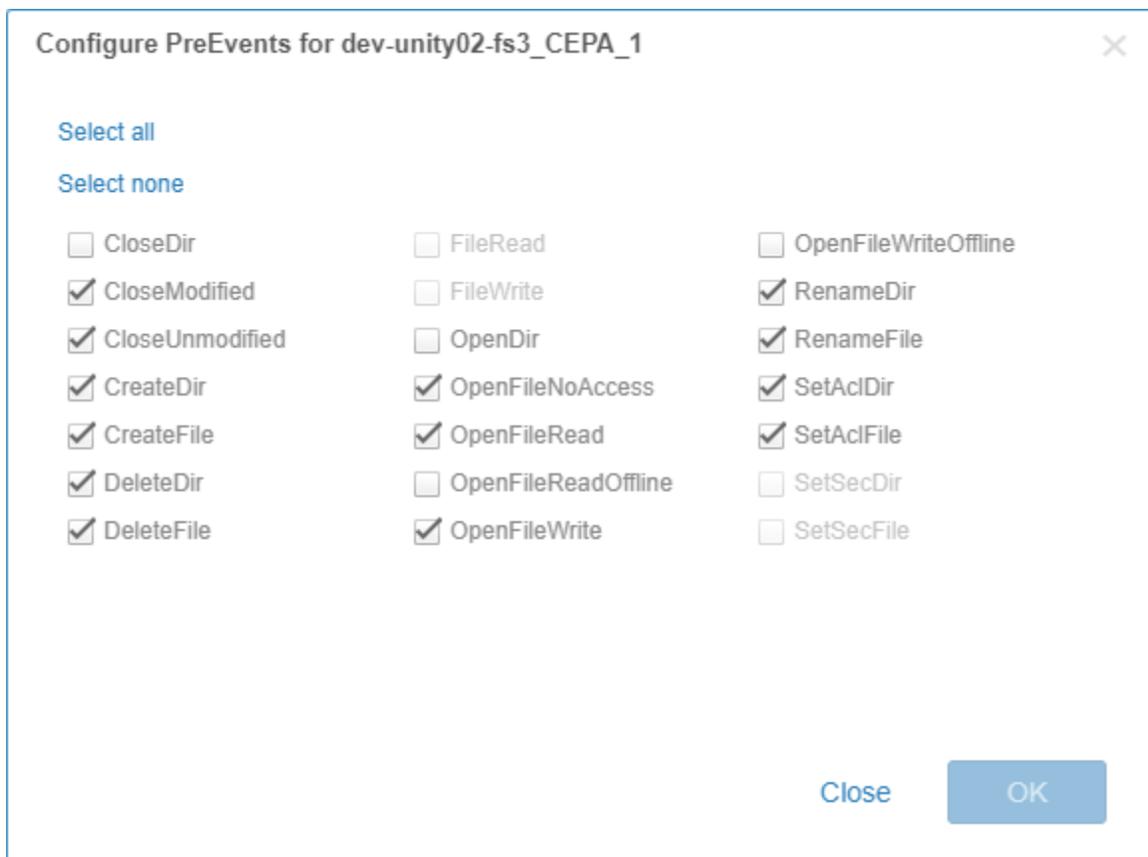
Checking and EMC Event Notification Bypass rights and be a local admin on server being managed. CEE is required.

To enable Event Publishing on the NAS Server.

1. Log into the Unity Unisphere Console

2. Select File in the left menu

3. Select the NAS Servers tab across the top

4. Select the specific NAS Server

5. Click the Edit Icon (pencil)

6. On the Properties page that is displayed, select the Protection & Events tab.

7. Select the Events Publishing menu item on the left

8. Click the checkbox Enable Common Event Publishing
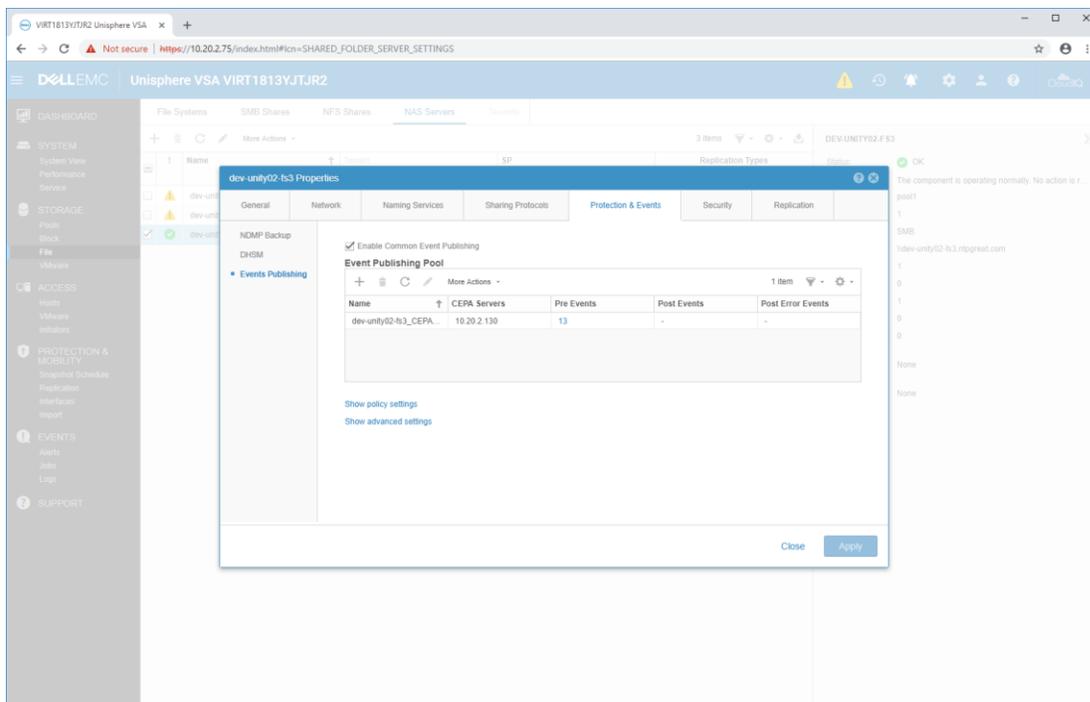
9. Click the + icon to add a new pool.

10. The name will be filled in by default. Click the Add button to add the name/ip address of the CEE server that File Auditor will use

11. Click the Configure link next to Pre Events.

Configure PreEvents for dev-unity02-fs3_CEPA_1

Select all
Select none

☐ CloseDir	☐ FileRead	☐ OpenFileWriteOffline
☑ CloseModified	☐ FileWrite	☑ RenameDir
☑ CloseUnmodified	☐ OpenDir	☑ RenameFile
☑ CreateDir	☑ OpenFileNoAccess	☑ SetAclDir
☑ CreateFile	☑ OpenFileRead	☑ SetAclFile
☑ DeleteDir	☐ OpenFileReadOffline	☐ SetSecDir
☑ DeleteFile	☑ OpenFileWrite	☐ SetSecFile

Close   OK

12. Select the events shown above and click OK.

13. Click Configure. Then click Apply. The settings will be saved and you will be returned to the NAS Servers list.

14. Click on the File Systems link at the top.

15. In order to get events, each file system must have Events publishing enabled.

16. Select a file system on the NAS server, and click the Edit icon.

17. On the properties dialog, select the "Advanced" tab. Check the option for Enable SMB Events publishing

18. Repeat for each file system that will be configured in File Auditor.
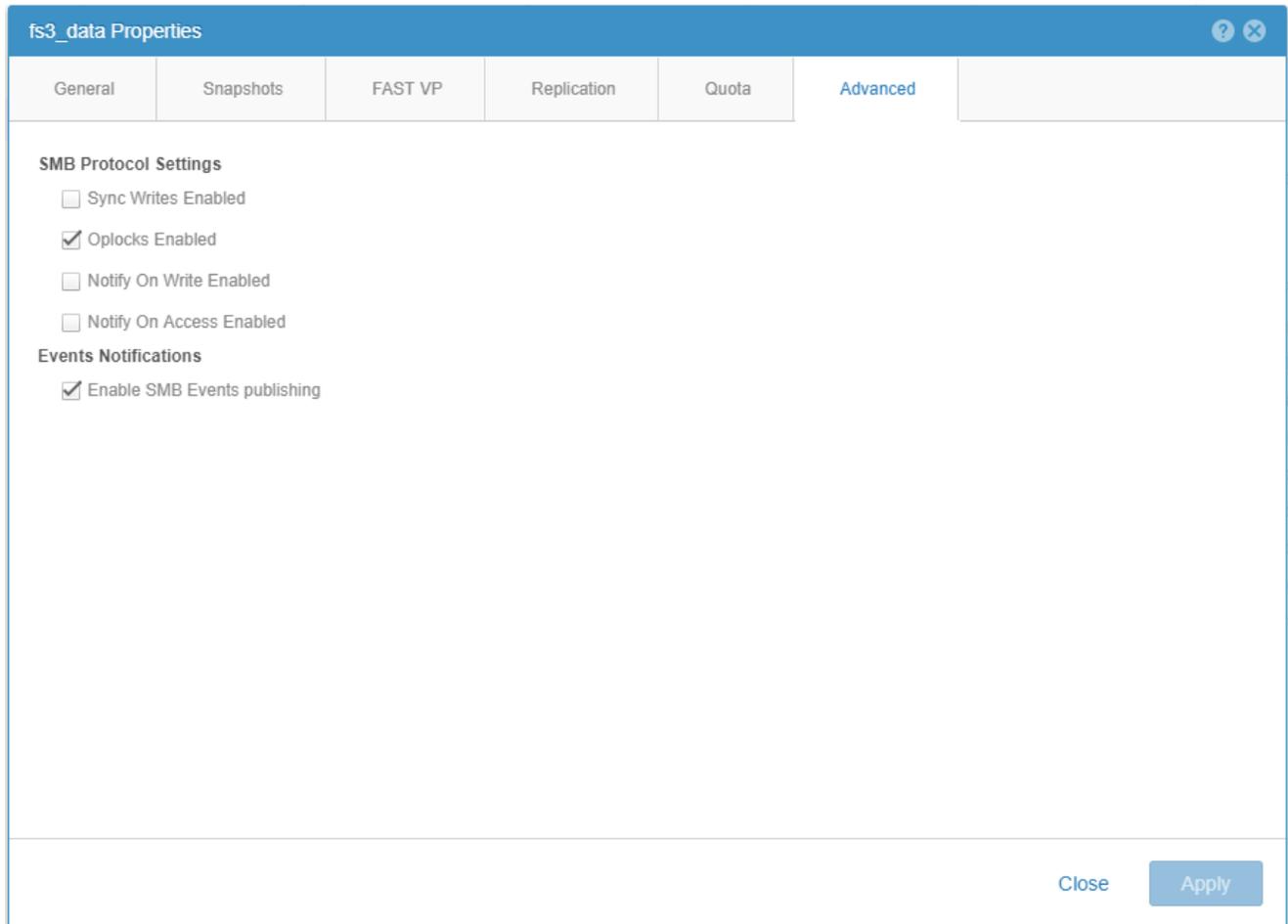
If installing File Auditor into an existing SPM hierarchy or are upgrading an existing File Auditor install, setup will prompt to upgrade SPM. Once SPM has been upgraded, two-way replication with the older servers in the hierarchy will stop. SPM 2.9 will continue to receive updates from SPM 2.8, but not the other way around. Once all servers in the hierarchy have been upgraded to SPM 2.9, replication will resume as normal.

Notes:

The registry DWORD value DBInsertionThreads controls the number of threads that the QFS service and connector services will use to import files into the database. The location of the registry key is as follows:

Windows: HKLM\Software\DefendX Software\Control-Audit\Service

NAS Platforms: HKLM\Software\DefendX Software\Control-Audit\[NAS|HCS|ECS]

The default is 5 with a minimum of 1 and a maximum of 10.

Notes:

Upgrades from prior versions are supported. Registry keys will be migrated to HKLM\Software\DefendX Software\Control-Audit. All configuration keys will be under Control-Audit. The BCS key for Hitachi has been renamed to HCS.

There is a new version of EASE that is required when installing/upgrading. During an upgrade it will recognize this and prompt for the upgrade.

Notes:

If both QFS and FA were installed on the same machine, the QFS admin will no longer load in the UI. This is due to the upgrade to Visual Studio 2017 for Control-Audit and EASE. The QFS Admin dll was built with an older version of Visual Studio and is not compatible. The dlls need to be built with the same version of Visual Studio.

Known issues in Control-Audit

Features the service account does not support

During the DefendX Software Control-Audit™ setup, you can specify an account to use for the system DefendX Software Control-Audit™ service, or you can use the local system account. Since the local system account is not a domain account, the Cross-Domain Resolution of user names and groups in policies feature is not available to DefendX Software Control-Audit™ when using the local system account.

Bug Fixes

- Installer for the reports viewer was not able to correctly identify which version of the .net framework and would display a message that it was required even though it was already installed.

- Fixed an issue with the license manager including non-fixed drives in the storage

- Files opened with the DELETE_ON_CLOSE flag were not being logged in the database for NetApp C-mode filers.

- Setup program not allowing the full contract license key to be pasted in the edit control.

- Setup program not installing the runtime files needed for the connector services.

- Inherited policies were not be inherited

About DefendX Software

DefendX Software helps organizations secure their critical business files and maximize the value of their enterprise file storage resources. From comprehensive intelligence, modeling, costing and chargeback to seamless file movement, protection and archiving, DefendX provides industry-leading capabilities to eliminate waste and align the value of files with the storage resources they consume. With DefendX, important file locations and the users who access them can be monitored to provide governance, protect against theft and enforce compliance policies. For more than 20 years, DefendX Software has been helping public and private sector customers around the world save money and eliminate risk every day.

DefendX Software Professional Services

DefendX Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your DefendX Software Representative at 800-390-6937.

Legal & Contact Information

The information contained in this document is believed to be accurate as of the date of publication. Because DefendX Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of DefendX Software, and DefendX Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. DEFENDX SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

DefendX Software and other marks are either registered trademarks or trademarks of DefendX Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

DefendX Software products and technologies described in this document may be protected by United States and/or international patents.

<div align="center">

DefendX Software
119 Drum Hill Road, #383
Chelmsford MA 01824
Phone: 1-800-390-6937
E-mail: info@DefendX.com
Web Site: http://www.DefendX.com

</div>