



# DefendX Software Control-Audit™

## Installation Requirements

*This guide covers the pre-install items to be considered in preparation for a successful install of DefendX Software Control-Audit™. When the installation is complete, the product is functional. Customers should read through this guide in its entirety for important notes to get the most out of the software.*



## Table of Contents

Executive Summary.....	3
Important Pre-Install Points.....	4
Windows Edition.....	5
NetApp FAS Edition.....	5
EMC VNX/Isilon Edition.....	5
Hitachi Edition.....	7
Things To Remember.....	7
About DefendX Software.....	8
DefendX Software Professional Services.....	8
Legal & Contact Information.....	9

## Executive Summary

Below is a summary of system and other technical requirements in preparation for a successful install of DefendX Software Control-Audit:

### Windows Server Management Host

<b>CPU</b>	2.2GHZ or higher
<b>MEMORY</b>	2-4 GB
<b>DISK SPACE</b>	50 -100MB Available HDD Space (for installation) 1GB per every 1,000,000 I/Os (for database)
<b>OPERATING SYSTEM</b>	Windows Server 2008 or Later
<b>VIRTUAL SUPPORT</b>	VMware (Version 3.5 or higher), MS Hyper-V, XEN
<b>WEB COMPONENTS (OPTIONAL; CAN BE INSTALLED ON SEPARATE SERVER IF DESIRED)</b>	Microsoft IIS (Internet Information Services) version 6.0 or later Microsoft .Net Framework version 4.5.2
<b>DATABASE COMPONENTS (OPTIONAL; CAN BE INSTALLED ON SEPARATE SERVER IF DESIRED)</b>	Microsoft SQL Server version 2005 or Later Mix Mode Authentication (Required) SQL Reporting Services (SSRS) (Required)

### NetApp Filer NAS (required for NetApp installation)

<b>OPERATING SYSTEM</b>	Data OnTap version 7.3 or later
<b>SERVICE ACCOUNT</b>	Domain User & member of local Administrators group on Filer

### EMC VNX NAS (required for EMC installation)

<b>OPERATING SYSTEM</b>	DART version 5.6.36.2 or later
<b>LOGIN CREDENTIALS</b>	Login Credentials to Control Station
<b>SERVICE ACCOUNT</b>	Domain User & member of local Administrators group on CIFS Server
<b>OTHER COMPONENTS</b>	EMC CEE (Common Event Enabler) version 4.2.2 or later (Required) EMC CIFS Management Tools

### Hitachi NAS (required for Hitachi NAS installation)

<b>OPERATING SYSTEM</b>	HOS version 6.1.1684.18 or later
<b>SERVICE ACCOUNT</b>	Domain User & member of local Administrators group on CIFS Server

## Important Pre-Install Points

Below are key items that were discussed to consider in preparation for a successful install of DefendX Software Control-Audit®:

- At the start of the installation, Control-Audit checks that the DefendX Software Smart Policy Manager Service (also referred to as EASE) is present and if not will prompt for that component to be installed before the Control-Audit installation continues. The Smart Policy Manager is responsible for storing and replicating policies in your environment. This component is required prior to continuing with the installation of the Control-Audit Service.
- When the installation is complete the DefendX Software Control-Audit Service and Smart Policy Manager Service will be present on the Server.
- The services require an Active Directory service account that is a member of the Domain Users group and the service account must be a member of the Administrator group on the local server(s) where Control-Audit is installed. This service account must be granted the right to run as a service.
- Policies can be configured to send emails to notify users, but this requires additional inputs to the configuration:
  - In order to resolve user names to emails the system will require access to a directory that maps user names to email addresses. In most organizations this role is fulfilled by Active Directory and only requires the name of the domain or of one or two domain controllers
- When the installation is performed it will create 1 SQL Server database. During this install it helps if the SA account is available to create the database and the required SQL user, after the installation there is no further need for the SA account.
- The Web Server can be running IIS 6.x, 7.x, or 8.x and must have ASP.Net 2.0 and ASP as well as Windows and Basic authentication installed.
- The SQL Server must be running Microsoft SQL Server 2005 or Later.
- The SQL Server should be configured to support Mixed Mode Authentication. This is required by default, but can be worked around if this is not possible.
- The Remote Connection to the SQL Server should be enabled.
- The SQL Server user should have db\_datareader, db\_datawriter, and execute permissions on the Control-Audit database.
- During the installation, the Windows user will need to have access to the Reporting Service on the database server.

## Windows Edition

For the Windows Edition of Control-Audit there is some additional configuration required:

- The Remote Connection to the SQL Server should be enabled.
- The SQL Server user should have db\_datareader, db\_datawriter, and execute permissions on the Control-Audit database.
- The Reporting Service on the database server must grant access to the currently logged Windows user while installing the application.
- Before running DefendX Software Control-Audit for Windows Edition installer, make sure you have the following ready for a smooth installation:
  - The Microsoft SQL Server user name and password for authentication.
  - Access to server.
  - The license key you were given when you purchased the Control-Audit product.

## NetApp FAS Edition

For the NetApp Edition of Control-Audit there is an additional service installed and some additional configuration:

- The NAS Connector Service manages the communication between the Control-Audit Server and the Filer.
  - The NAS Connector Service requires that the service account is a member of the local administrator group on the...
    - 7-Mode - Filer(s) and/or vFiler(s) being managed.
    - CDOT – SVM(s) being managed
  - For CDOT, a cluster account with the ontapi privilege is required
  - The Filer(s) and/or vFiler(s) must have FPolicy enabled. FPolicy is the interface that allows Control-Audit to be notified with file operations
  - The greatest threat to our solution when managing Filers is latency on the connection to the Filer. The Filer will disconnect if our server does not reply quickly enough to screening requests and the most likely cause of this is latency on the connection. For this reason we recommend a dedicated network connection between the Control-Audit Server and the Filer.

## EMC VNX/Isilon Edition

For the EMC Edition of Control-Audit there is an additional service installed and some additional configuration:



## VNX

- The EMC Connector Service manages the communication between the Control-Audit Server and the NAS.
  - There needs to be a CIFS Server that is on the physical data mover (i.e. Server\_2) that our services can use as a bridge to manage CIFS Servers that are on Virtual Data Movers. The CIFS Server that is on the physical data mover does not require a File System assigned to it, but it does help with diagnostics.
  - The EMC Connector Service requires that the service account is a member of the local administrator group on the CIFS Server(s) being managed.
  - The NAS must have the Server\_CEPP service enabled and the CEPP.CONF file must be configured according to the instructions in the installation guide.
  - EMC will need to provide to you the appropriate versions of their Common Event Enabler (CEE) or VNX Event Enabler (VEE) as well as the Data Mover Management MMC.
- EMC account with nasdamin rights to the VNX control station.

## Isilon

- The EMC Connector Service manages the communication between the Control-Audit Server and the NAS.
  - Please refer to the EMC Installation guide for details on preparing the Isilon.

## Hitachi Edition

For the Hitachi Edition of Control-Audit there is some additional configuration required:

- To prepare the HNAS Server, the following must be taken into consideration:
  - For each EVS (Virtual Server) that is managed by DefendX Software Control-Audit, at least one CIFS server name must be created and must join the same domain as the Control-Audit machine.
  - The logon account used to register with the Hitachi NAS Server (the account that will be assigned to the DefendX Software Control-Audit service) needs to be a member of the Hitachi NAS Server's local group Backup Operators. This can be added from the Hitachi NAS Server Command Line Interface (CLI) using the following command:  
**localgroup add "Backup Operators" <FQDomainName\AccountName>**
  - The File-Filtering feature must be enabled in the EVS. To enable the File-Filtering feature, use the following command:  
**fsm set allow-defendx-file-filtering true**

## Things To Remember

- Our software will not affect the system performance on the storage system nor will a reboot be required to complete the installation.
- The storage will not be taken offline or restarted in any way. There will be zero down time for the users accessing the storage.
- When the installation is complete, the product is functional but not enabled. Control-Audit will not manage the environment until policies are configured and enabled.
- The current Installation Guide and User Manual are included in the software that you will download as part of your purchase.

## 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.

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

Copyright © 2018 DefendX Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Doc#DFX1121EF