Varonis Data Security Platform v8.6
Common Criteria Configuration Guide

Document Version: 1.3

2400 Research Blvd
Suite 395
Rockville, MD 20850

Table of Contents

Revision History

Version	Date	Changes
1.0	November 30, 2022	Initial Release
1.1	January 11, 2023	ECR comments addressed
1.2	February 13, 2023	Minor update
1.3	February 23, 2023	Minor update

1 Purpose of this document

This document is a guide for the Varonis Data Security Platform 8.6 implementation of the Common Criteria Application Protection Profile v1.4 (SWAPP v1.4). The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the Varonis DSP 8.6 which runs on Microsoft Windows operating systems.

This document will guide how to install, configure, and operate the Application in a Common Criteria Compliant mode.

- Prerequisite for installing Varonis DSP 8.6
- How to install Varonis DSP 8.6 on Microsoft Windows
- The secure communication mechanisms employed by Varonis
- How to update the Varonis DSP 8.6 application

1.1 TOE Overview

The TOE is a Microsoft Windows-based software application that works with file systems across a network to audit, analyze, and remediate improper or insecure access permissions. The TOE works with a variety of different objects, including files, folders, Active Directory domains, and SharePoint sites. The primary components and features of the TOE included in the evaluation are as follows:

- DatAdvantage (DA)
- Data Classification Engine (DCE)
- DatAlert
- Data Privilege (DP)
- Remediation Engine and Data Transfer Engine (DTE)

DA is the underlying framework that is common across all application components.

DCE provides the facilities to classify sensitive data stored in a number of repositories, tagging of sensitive data, identifying data owners and sensitive data patterns. In conjunction with DatAdvantage, the DCE engineprovides full identification cycle for sensitive data owners.

DatAlert provides real-time alerting for events such as privilege escalations, access on or deletion of sensitive data, permissions or other anomalous behavior related to object access.

Data Privilege is an interface to the application that provides a web-based form providing request and approval workflows for data consumers and owners.

DTE facilitates the secure migration of data between heterogenous file systems by comparing source and target file system access control information and allowing administrators to ensure that the resultant migrated data contains the appropriate permissions in its new location. An additional, complementing part of the suite is the Remediation engine which allows the TOE to identify and correct permissions on data located within the monitored assets.

The TOE is managed remotely via two primary web-based interfaces: DatAdvantage Web and Data Privilege Web. In addition, two locally accessible interfaces are available: DatAdvantage UI and DatAdvantage Management Console. DatAdvantage UI provides the same functionality as DatAdvantage Web, while DatAdvantage Management Console provides initial configuration and maintenance tasks.

2 TOE Description

2.1 Evaluated Configuration

The TOE is an application running on a general-purpose operating system. The TOE consists of a set of application binaries (executable runtimes, DLLs, etc.), web-based UIs, configuration files, and data that correspond with the application components discussed in Section 1.1 above. The TOE leverages the Windows platform to secure connectivity with third-party products using TLS/HTTPS. In addition, the Windows platform provides the secure TLS/HTTPS functionality as necessary to protect the trusted path to TOE administrators.

The TOE is evaluated on the Microsoft Windows Server 2019 build 10 (also known as version 1809) platform.

2.2 Physical Boundaries

The TOE is a software application running on Microsoft Windows Server 2019 build 1809 on a Dell PowerEdge server. The TOE boundary is comprised of the application components described in Section 1.1above, their binary executables and libraries, and the associated configuration data. User data is not considered to be within the scope of the TOE.

2.3 Logical Boundaries

The TOE provides the security functionality required by [SWAPP].

2.4 Other Assumptions

The following assumptions are drawn directly from the [SWAPP]:

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance of the applied enterprise security policy.

3 Secure Installation and Configuration

3.1 Prerequisites

The following steps must be completed before Varonis DSP 8.6 can be installed and configured in Common Criteria mode. This document assumes that any third party monitored systems such as SharePoint and any monitored file systems are installed in the environment and configured for secure TLS access.

3.1.1 Access to Network Resources

As needed for connectivity to management interfaces from an end user as well as connectivity to Active Directory and monitored systems, the DSP applications require access to the Windows platform networking resources. The system must be installed within its own separate network segment to protect the DSP applications from unintended or unauthorized access. In addition, the following network restrictions must be applied on the Windows firewall or an external firewall protecting the DSP server's network segment:

1. For Web UI, allow only port 443 communications to the DSP Server.

2. For DataPrivilege, allow only port 443 communications to the DSP Server.

3. Outbound communications from the Varonis Servers should be restricted to:
    - Monitored Servers
    - Active Directory Servers

For information on configuring the firewall, please refer to the file attached below:

Enable Windows Defender Firewall with

3.1.2 Access to Sensitive Information Repositories

As needed for generating application logs, write access to Windows system logs is required and automatically enabled. Application logs can be viewed using the Windows Event Viewer.

3.1.3 Microsoft SQL Server

Install Microsoft SQL Server 2016 according to the steps mentioned in the following file attached:

Install SQL Server 2016.pdf

3.1.4 Full Disk Encryption

BitLocker **MUST** be installed and active in order for DSP to operate. This will provide the system with the required platform encryption. Please refer to Section 4.3 "Installing and Enabling Bitlocker" in this document for the proper process of running BitLocker on your system.

3.2 Installing Varonis DSP

Once all the prerequisites are completed, follow the below steps to install Varonis DSP 8.6:

1. Please follow the steps provided on the file below (data_security_platform_installation.pdf) to install Varonis DSP 8.6:

Data Security
Platform Installation

2. Follow the steps in the document – they will guide step by step from getting the license to deployment and configuration of the system.

3. Refer to the following section for enabling enhanced cryptography for the Windows platform.

4 Platform Security and Cryptography

4.1 Enabling Enhanced Cryptography

When running the installation (setup.exe) pass the following parameter:

- "-featureToggles=NewCrypto"

Example:

- Setup.exe -featureToggles=NewCrypto

4.2 Cipher Suites, TLS, and LDAP Configurations

The below steps must be followed to configure the Windows platform to support the TLS_RSA, TLS_DHE, and TLS_ECDHE Cipher Suites as necessary to support HTTPS and LDAPs connections.

To enable secure connectivity between the Varonis applications and Active Directory, perform the following steps:

1. Open the Varonis Management Console.

2. Choose the Root/Domains in the Management pane.

3. Edit the domain with which you are working.

4. In the General tab, mark the checkbox "Use LDAPS" for AD Security type.

It must be ensured that the Domain Controller is configured to work with LDAPS. Please follow the steps in the file attached below to configure LDAPS on a Windows Server:

Configure LDAPS on a Windows Server.pdf

Instructions on configuring cipher suites on the Windows platform can be found in the file attached below:

Configure TLSCipherSuites.pdf

4.2.1 Web DA

1. Open the Varonis Management Console

2. Navigate to the following location: Root Level > DSP Server > Service Components > Varonis Web Server

3. Once the certificate has been imported into the DSP/IDU's Computer Certificate store (Personal or Trusted Root), open it and choose the Details tab and highlight Thumbprint

    a. Copy the thumbprint from the certificate and place it in Notepad.
    b. Save the notepad and close it. Open the Notepad document again and you will see a "?" at the beginning - Remove the "?" and copy out the thumbprint.
    c. In the Certificate Thumbprint section, enter the Certificate Thumbprint obtained in Prerequisites. Please ensure that it has no hidden characters.
    d. Verify:
        i. Protocol is set to HTTPS.
        ii. Port is set to 443.

    e. Be sure to press Save before proceeding. Otherwise, changes will not take effect.

4.2.2 DP

a. To configure DP to use SSL:
    a. In IIS manager, click Server Certificates for the main site.
    b. Create a self-signed server certificate by clicking on "Create Self-Signed Certificate". The certificate can be named as you choose.
    c. Add a site binding by clicking on the Default Web Site root, then SSL Settings, Bindings. Add an HTTPS binding and select the previously created SSL certificate.
    d. Browse to the DP site, double-click SSL Settings.
    e. Mark the checkbox for Require SSL. (Do not forget to hit Apply on the right pane.)

4.3 Enabling Bitlocker

Please follow the steps provided on the file below in order to properly install and enable Bitlocker:

Installing
BitLocker.pdf

5 Management Functions

The below steps must be followed in order to perform the functions provided by the Management Console.

5.1 Configuring Various System Users:

1. Open the Management Console and click the Configuration tab.

2. Within the configuration tab, select and open the “Filtered Users/Groups” sub option.

3. When the “Filtered Users/Groups” window is opened, select the green plus button with the “Users/Groups” option next to it.

4. A new window called “Directory Services Search” will populate. Within that window, the operator may search for any user or group of users contained in the Active Directory.

5. Once a desired user or group of users is chosen, click the OK button. Your selection will populate in the “Filtered Users/Groups” tab.

5.2 Configure Monitored File Servers:

1. Open the Management Console and click on the Management tab.

2. Expand the “Root” option and click on “File Servers”.

3. Within the newly opened File Servers window, click on “Add”. A new window called “ResourceWizard” will open.

4. Within the Resource Wizard, select your desired Server Name input the correct administrator credentials, and click “Install”.

5. Your selected server will populate on the “File Servers” window.

5.3 Defining Working Domains:

1. Open the Management Console and click on the Management tab.

2. Expand the “Root” option and click on “Domains”.

3. Within the newly opened Domains window, click on “Add”. A new window called “DomainProperties” will open.

4. Within the Domain Properties window, select your desired Domain Name and Domain Controller Name, then input the correct administrator credentials and click “Install”.

5. Your selected domain will now populate on the “Domains” window.

6 User Roles

Varonis one primary administrative role, “Enterprise Manager”, which enables such user to have access to the Management Console, and manage the Varonis system configuration, as well as a list of roles that enables the user to work within the UI (DA) or the Web UI (but not to do system configuration changes).

1. Defining a user with “Enterprise Manager” role

    a. Login to Varonis Management Console

    b. Go to “Configuration Security”

    c. Click on ‘Add’ to select the user you want to grant access permissions to the Management Console and under “Application Role” field select the following permissions:

        - “Enterprise Manager”

    d. Click on ‘Save’

    e. This user can now logon to the machine with his/her credentials and then access the Management Console

2. Defining a user without Admin rights – for the DA UI, Web UI

    a. Login to Varonis Management Console.

    b. Go to “Configuration Security”.

    c. Click on ‘Add’ to select the user you want to grant access permissions to the DA UI, and Web UI, and under “Application Role” field select the following permissions:

        - User
        - Work Area View User
        - Web UI user
        - Alerts View User
        - Reports View User
        - Review Area View User
        - Statistics View User

    d. Click on ‘Save’

This Windows user can now use the Web UI and DA UI, but cannot modify any system configuration, and will get “access denied” error when trying to use the Management Console.

7 Secure Updates

7.1.1 Checking for Current Version

The following are steps the operator may follow in order to query the system for its currently running version:

1. Management console – it is written in the window title.
2. DatAdvantage UI – Open the help tab and choose the “about” option.
   A popup will be opened with the currently installed version.
3. DataPrivilege UI - Open DataPrivilege page and from the gear icon select “About”.
   Then from the About page click on 'License Details' and you will see the version details.

7.1.2 Configuring the system to notify on new software updates

1. In the Management Console, under **Configuration**, choose “**DatAdvantag Updates**”.
2. Under the **Update Configuration** panel, Choose the checkbox “**Enable Live Update**”.
3. And mark the radio button “**Send me an email for each patch that needs to be installed**”.

When there are new Software updates, beside getting an email, the Administrator can view them and chooseto install by going to the “Root” in the Management Console, and choosing the “Update Manager” tab.

All updates are signed and contain SHA256 Checksum, which is verified by the “Live Update” service.

7.1.3 Installing Updates and Verifying Code Integrity

1. Varonis customers get software updates via the Support Center
2. After logging in, browse to the “Download Center”
3. There, you’ll see list of relevant packages (latest GA versions, or patches)
4. Beside each such package, the customer will find a SHA256 checksum of the package.
5. After downloading the package, the customer shell verify the integrity by using Windows Powershell command Get-FileHash
6. The checksum of the downloaded package can then be compared to the checksum in the Support Site.

7. Once verified, the package can be loaded and used:

    a. In the Management Console, Using the Update Manager tab: select your package and press "Deploy"

    b. Fill all the missing credentials and press next.

    c. Follow the progress until completion

8 Enable exploit protection

The TOE supports Windows Defender Exploit Guard Protection configured with the following mitigations:

- Control Flow Guard
- Randomize memory allocations
- Export address filtering
- Import address filtering
- Data Execution Prevention

Please follow the steps provided on the file below to configure the buffer overflow protectionmechanisms on the environment:

Enable exploit protection.pdf

9 Importing certificates to the TOE

Please follow the steps provided on the file below to import the trusted certificates to the TOE:

Importing certificates.pdf

The trusted Root Certificates should be imported to the 'Trusted Root Certification Authorities' of mmc so that the TOE can use the certificates for validation.

10 Audit logs

All system logs will be located by browsing the installation directory Varonis\DatAdvantage\ and selecting a respective folder of a specific function whose log is desired to be viewed. Logs will be within a sub-folder labeled “Logs”

8.1.1 Trace Logs

The below log shows an example of a trace log generated by a specific function of the Varonis DSP when an applicable function is executed:

Timestamp: 9/2/2022 1:36:22 PM Message:
CreateDefaultInstance<Varonis.Server.Services.IAutomationLargeDataService> been called Category: General, Trace Severity: Information Title: Machine: L1317-DV1 App Domain:
Varonis.UI.ManagementConsole.Shell.exe ProcessId: 38584 Process Name: C:\Program Files (x86)\Varonis\DatAdvantage\Management Console\Varonis.UI.ManagementConsole.Shell.exe Extended Properties:

8.1.2 Error Logs

Below is an example of a log that is generated by a specific function of the Varonis DSP when it detects an error or malfunction:

Timestamp: 9/19/2022 3:11:42 PM Message: HandlingInstanceID: e72204d8-32c9-46c1-b4ca-7253185ad342
An exception of type 'System.InvalidOperationException' occurred and was caught.

11 References

The following documents were created and evaluated as part of the Varonis DSP 8.6 CC evaluation:

- Varonis DSP v8.6 Security Target (ST)
- Varonis DSP v8.6 Common Criteria Configuration Guide (AGD – this document)

End of Document