MetaClean Sync and MetaClean Dashboard

Security Target

v2.0

24/01/2024

Created by

Version control

Version	Comment	Date
0.1	Initial draft version	20/10/2022
1.0	First complete version	07/11/2022
1.1	Minor changes	10/11/2022
1.2	Minor changes	10/11/2022
1.3	Requirements of section *5.4* updated	29/11/2022
1.6	Changes according CPSTIC comments and new TOE functionalities. Minor changes in sections *1.1*, *2.2*, *4.1*, *4.2*, *4.3* and *6*. Sections *2.1*, *2.3* and *3.1* have been modified. Requirements of sections *5.3*, *5.4*, *5.5*, *5.6* and *5.7* have been updated and section *5.2* has been included. Libraries of section *8.1* have been updated.	29/09/2023
1.7	TOE version update in section *1.1* . Version of manuals updated in section *2.2*. Changes in section *2.3* according new TOE functionalities. Assumptions updated in section *4.1*. Assets updated in section *4.2*. Table of section *4.3.1* updated according requirements and threats. Requirements **AUD.1**, **AUD.2** and **AUD.5** of section *5.5* updated according new TOE functionalities.	08/11/2023
1.8	Changes in sections *2.3* and *3.1* according to new TOE functionalities.	14/11/2023
1.9	Minor changes in sections *2.3* and *3.1*. Updates in section *4.3*. Requirement **AUD.5** of section *5.5* modified according TOE functionalities.	22/01/2024
2.0	Changes in section *2.3* for better consistency with the update process. Minor changes in section *3.1*.	24/01/2024

Table of contents

1 Introduction

This document is the Security Target for **MetaClean Sync and MetaClean Dashboard**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Sponsor, TOE and Evaluation Information

Applicant data	Adarsus Technologies S.L.
Developer data	Adarsus Technologies S.L.
Contact information of developer	Avda. Secundino Suazo N-95, C.P.: 28055 Guzmán Rejón (guzman.rejon@adarsus.com)
TOE name	MetaClean Sync and MetaClean Dashboard
TOE version	MetaClean Sync v2.3.0 Professional Version and MetaClean Dashboard v1.3.0
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE Secure Use, Installation and Configuration Guides*
Taxonomy according to CCN-STIC-140	N/A

1.2 Methodology and Evaluation Criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE Description

2.1 TOE Functional Description

The TOE, denominated as **MetaClean Sync and MetaClean Dashboard**, is a software solution that addresses file metadata management. It can be used for automatically deleting metadata or overwriting it with previously defined values, from files in the directories which have been selected to be monitored, in a transparent way for the final user. The TOE can manage metadata from Microsoft Office (Word, Excel, PowerPoint and Visio), OpenOffice/LibreOffice (text documents, spreadsheets and presentations), PDF, image, audio and video files.

The TOE works based on templates, which are used to define which metadata fields will be removed, overwritten with a certain value or kept with the original value. The TOE constantly monitors the directories that have been previously selected by an administrator. When selecting a directory for monitoring, the administrator will have to choose if the subdirectories will also be monitored, the filetypes that will be monitored, the template that will be applied on them and also whether to process electronically signed PDF files or not. As soon as a new file is created or a previous one is saved in a monitored directory, the TOE will immediately modify its metadata following the associated template, if applicable.

The TOE is composed of two main software parts that communicate with each other:

- **MetaClean Sync,** which is to be installed either on a workstation or on a Windows Server in a corporate network, and has the following functionalities:
  - Automatically processes file metadata when files are created or modified in the monitored directories. This functionality can be started and stopped at any time for each monitored directory previously defined by an administrator of the operating system where MetaClean Sync is installed. If it is installed on a workstation, this functionality will only work locally on said machine. However, if it is installed on a Windows Server, this functionality can work on other network units.
  - When starting to monitor a directory, if the option “synchronize” has been previously selected, a recursive search of all files in the directory specified in the monitor will be performed and their metadata will be processed based on the specified configuration. Once the processing of the files that apply is finished, the real-time monitoring of the directory will be started. The following times that the monitor is started, it will detect which files have already been processed and have not changed in order to avoid processing them again.
  - Definition of directories to be monitored. For each monitored directory, the following can be defined:
    - Whether to monitor subdirectories or not.
    - The filetypes to monitor within the directory.
    - Whether to process metadata of electronically signed PDF files or not.
    - The template to apply when processing metadata if no template is received from MetaClean Dashboard.
  - Software update management, which can be initiated manually. This component checks with MetaClean Dashboard for new software versions. If a new version exists, MetaClean Dashboard sends it to MetaClean Sync.

- Registers in a log file all the original metadata that has been processed. This file is then sent to MetaClean Dashboard once the log file reaches a configurable size or after a configurable period of time, if this connection has been configured.
- Connection with MetaClean Dashboard through its URL. Both TOE components can be connected through this parameter.

- **MetaClean Dashboard,** which is designed to be installed on a different machine from the one running MetaClean Sync, and has the following functionalities:
  - Creation of metadata templates for their usage in MetaClean Sync. These templates define how each metadata field will be processed (deleted, overwritten with a certain value or kept with original value) and also allow defining customized metadata fields with a defined value.
  - Associating metadata templates to an Organizational Unit from the LDAP server or to a group of devices.
  - Centralized assignation and distribution of metadata templates to all the instances of MetaClean Sync connected to MetaClean Dashboard, allowing a centralized management of metadata policies. There are two possible ways for distributing templates from MetaClean Dashboard to MetaClean Sync:
    - Distribution to groups of devices defined in MetaClean Dashboard. These groups can be defined from a list of all the devices with MetaClean Sync and connected to MetaClean Dashboard.
    - Distribution to Organizational Units defined in the LDAP server, which is part of the operational environment.
  - Displays statistics for analyzing and monitoring the usage of the TOE, based on the log files received from MetaClean Sync.
  - Distributing updates to MetaClean Sync.

The TOE component MetaClean Dashboard has users provided by the LDAP service. These users are the ones who can perform the dashboard functionalities as well as local users, but these are not under the scope of the evaluation. Any user accessing to MetaClean Dashboard has administrator permissions.

On the other hand, the TOE component MetaClean Sync does not have any kind of users.

When the TOE component MetaClean Sync processes a file, it applies a template received from MetaClean Dashboard. Templates are requested every 15 minutes. The template that MetaClean Dashboard will send is the one from the first condition met out of the following list:

1. The requesting device belongs to a group of devices defined in MetaClean Dashboard with an assigned template.
2. The requesting device or user belongs to an Organizational Unit from the LDAP server and has a template assigned in MetaClean Dashboard.
3. A template assigned in MetaClean Sync to a specific monitored directory.
4. The default template defined in MetaClean Dashboard.

The TOE components have several interfaces which are listed below and shown in the following figure:

- MetaClean Sync:
  - Graphical user interface for administration.
- MetaClean Dashboard:
  - Web interface over HTTPS for administration.

MetaClean Sync communicates with MetaClean Dashboard through HTTPS, using TLS v1.2 or v1.3, for requesting metadata templates, sending logs with the usage of the TOE and requesting updates. The following figure illustrates both components of the TOE:

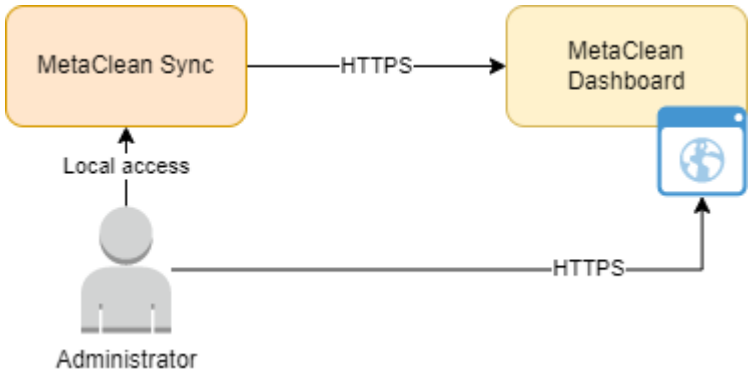

Figure 1: TOE overview.

2.2 Identification of the TOE Secure Use, Installation and Configuration Guides

The following table lists the documents and user guides necessary to carry out the configuration of the TOE properly:

Document type	Document name	Document version (update-history-date)
PDF	MetaClean Sync v.2.3.0 Manual de Instalación y Operación -Sistemas Operativos Windows-	1.4
PDF	MetaClean Dashboard v.1.3.0 Manual de Instalación y Operación -Sistemas Operativos Linux-	1.6

2.3 TOE Usage Description

MetaClean Sync can be installed by following the steps shown on *MetaClean Sync v.2.3.0 Manual de Instalación y Operación -Sistemas Operativos Windows- v1.4*. After installing MetaClean Sync, in order to reach the evaluated configuration, in the "Configuración General" tab the following must be taken into account:

- In the MetaClean Sync deployment, this TOE component has to be running under administrator permissions such as *localsystem* or *administrator*. For the evaluated configuration it will be run as *administrator*.
- MetaClean Sync is capable of requesting updates to MetaClean Dashboard automatically and also has the possibility of requesting them manually. Automatic updates are not part of the evaluated configuration so, in order to reach it, the checkbox "Actualizaciones automaticas" needs to be deactivated.
- MetaClean Sync can keep a backup of the processed files in a configurable directory. However, this functionality is not part of the evaluated configuration. Therefore, the checkbox "Activar Backup" under the "Configuración de Backup de Ficheros Originales" section must be deactivated.
- Under the "Registro de Metadatos" section, set the "*C:\Program Files (x86)\Adarsus\MetaClean Sync Server*" location to save the log file with all the activity regarding metadata processing as well as setting the maximum log capacity (Fichero de log) to 100 KBytes. Check the "Guardar Metadatos" box.
    - In order to view the event results of a given log, first access the *prevMetadataLogFile.log* file, get the *filename* of that log and then search for it in the *MetaClean_Sync_Service.log* file by matching date and time.
    - Set the "Intervalo de envío (Horas)" to 3 hours to send the processed metadata log files to the MetaClean Dashboard.
- Although MetaClean Sync can work without MetaClean Dashboard, the evaluated configuration includes both components working together. In the section "URL de Conexión al Servidor Dashboard", after setting the URL of the MetaClean Dashboard and sending interval (Intervalo de envío), check the box by "Conectar Dashboard".
- MetaClean Sync can send notifications via email to a configurable email address when certain events take place, such as a sudden stop of a monitor. This functionality is not part of the evaluated configuration, and therefore, the checkbox "Activar Notificaciones" under the section "Configuración de Notificaciones" must be deactivated.
- Modify the API key, with at least 32 characters, in the installation folder that will be used to authenticate the MetaClean Sync component against MetaClean Dashboard. The API key is stored in plain text in the following file *C:\Program Files (x86)\Adarsus\MetaClean Sync Server\activation\extra\apiKey.key*. After that, the Administrator of the system must configure the permissions of the file as defined in *3.1 Operational Environment Description*.
- The update process of MetaClean Sync is defined below:
    - The manufacturer sends the MetaClean Sync update to the administrators. This update is uploaded to the MetaClean Dashboard. The administrator shall go to MetaClean Sync and start the update manually. Subsequently, MetaClean Sync will initiate a connection to MetaClean Dashboard to download the update and apply it.

- The administrator shall check the integrity of the MetaClean Sync update, before uploading it to the MetaClean Dashboard, by calculating the SHA256 hash using the "Get-FileHash" command of the Windows PowerShell.
- The obtained hash must be confirmed with the one published in the manufacturer's website (https://www.adarsus.com), as defined in the following screenshot:

Figure 2: Location of the MetaClean Sync update hash in the manufacturer's website

After installing MetaClean Dashboard, in order to reach the evaluated configuration, the following modifications must be applied to the configuration file located at */var/www/html/api/config.json*:

- MetaClean Dashboard allows several authentication methods that include: the use of a local database, an Active Directory and an LDAP server. Although the TOE allows dashboard authentication with local users, the evaluated configuration only includes the authentication against an LDAP server. Therefore, the parameter "*authorizedLDAPUsers*" shall contain the UIDs (defined in the LDAP Server in the operational environment) separated by commas of the users that will be the administrators of MetaClean Dashboard. This setting is mandatory, as LDAP should restrict access to MetaClean Dashboard to users who are not authorized (defined) to access it.
- The parameter "*timeout_minutes*" shall be set to "10".
- The parameter "urlServer" shall be set to "https://dashboard.com/". However, the user is allowed to define another domain if desired.
- To update the hash SHA-256 of the API key stored in the instance running MetaClean Dashboard, change the default value in the *config.json* file. This hash must be the one corresponding to the hash of the API key configured in the installation folder of MetaClean Sync.

Note: The operating system administrator where the TOE component MetaClean Sync is installed and running must be included in the LDAP Server. This ensures that this component can receive templates from the Dashboard based on the configuration options per Organizational Unit (OU).

Besides these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in section *5 Security Functional Requirements* of this document beyond the steps in the TOE guide.

3 Operational Environment

3.1 Operational Environment Description

The TOE, as part of a corporate network, requires of an operational environment as shown in the figure below:

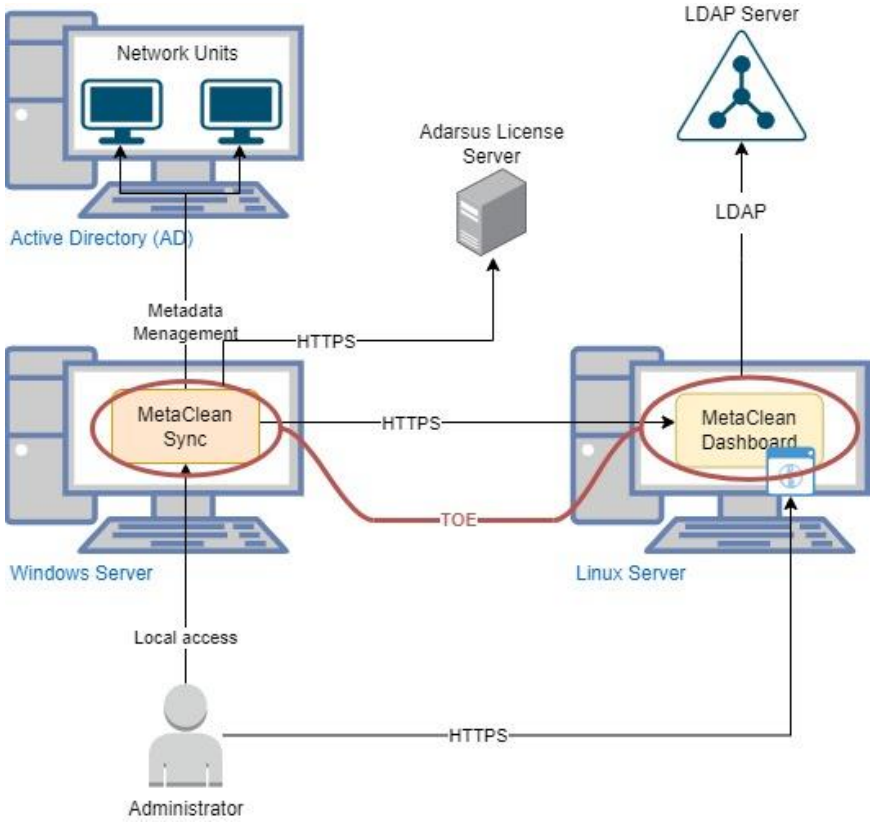

Figure 3: Operational environment.

The components of the operational environment are described below:

- **Windows Server**: This is the machine with the OS Windows Server 2019, where the TOE component MetaClean Sync will be installed and evaluated. MetaClean Sync is capable of running on Windows 10 and newer as well as on Windows Server 2008 and newer but these versions are not considered in this evaluation. When this TOE component is installed in a Windows 10 endpoint, it will only be capable of managing metadata of local files. However, if it is installed in a Windows Server, it will be capable of managing files in network resources as well as local files. The network unit to be monitored will be up through an AD (Active Directory).
- **Linux Server**: This is the machine where the TOE component MetaClean Dashboard will be installed. Although this component can run under both Linux and Windows, this machine will include the Linux OS Ubuntu Server 22.04.1 LTS with the following packages installed: Apache 2.4.52, PHP 8.1.2 and MariaDB 10.6.11.
- **LDAP Server**: This component, that is an OpenLDAP v2.4.47, is required for authentication on the administration web interface of MetaClean Dashboard.

- **AD (Active Directory)**. This component runs on another Windows Server to deploy network units. MetaClean Sync monitors directories that are mounted within an AD.
- **Network Units**: Units on the same local network as the Windows Server. These will contain directories to be monitored by MetaClean Sync.
- **Administrator**: The person in charge of managing both, MetaClean Sync and MetaClean Dashboard. This person must have access to the Windows Server where MetaClean Sync is installed and can use the same machine to access the MetaClean Dashboard management web interface.
    - The Windows Server administrator must change the permissions of the installation folder to limit it only to system administrator. No other non-administrator user of the Windows Server system will be able to manage the API key or access audit logs.
- **Adarsus License Server**: This is the server of the manufacturer that validates the license of MetaClean Sync.

The following communications are defined in the operational environment and make use of HTTPS (HTTP over TLS v1.2 or v1.3):

- Communications between the Administrator and MetaClean Dashboard.
- Communications between MetaClean Dashboard and the LDAP Server.
- Communications between MetaClean Sync and Adarsus License Server.

The LDAP server must be configured as follows:

- Establishment of policies to enforce the complexity of passwords:
    - The password must be able to be set with a minimum or equal length of 12 characters.
    - The password must be able to be composed of lowercase letters, uppercase letters, numbers and special characters ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")”].
- Establishment of a policy to prevent brute force attacks, GPOs regarding a maximum number of attempts and temporal lockout of user accounts should be applied by the administrator. Such policy should define attributes to limit to 3 the number of failed attempts and a 5-minute temporal lockout of account. The attributes are *pwdLockout*, *pwdLockoutDuration* and *pwdLockoutFailure*.

It is necessary to configure the ciphersuites in Apache for communications with the LDAP server. The */etc/apache2/sites-available/default-ssl.conf* file must be configured as follows:

SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1

SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM:ECDHE-ECDSA-CHACHA20-POLY1305:TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHA CHA20_POLY1305_SHA256:TLS_AES_128_CCM_SHA256:TLS_AES_128_CCM_8_SHA256

SSLHonorCipherOrder on

SSLCompression off

SSLSessionTickets off

SSLOpenSSLConfCmd Curves secp256r1:secp384r1:secp521r1:x25519:x448

The operating systems where both TOE components are running have system administrators. Therefore, MetaClean Sync, since it has no users of its own, the users that can exercise its functionalities are the operating system administrators.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.PHYSICAL PROTECTION	The product must be physically protected by its operational environment and not subject to physical attacks that could compromise its security or interfere with its proper operation. In the case of software products, this assumption applies to the physical platform on which the product runs.
A.TRUSTED ADMINISTRATION	The Administrator shall be a fully trusted member of the company/administration's security interests. It is therefore assumed that such person shall be qualified, trained and free from any harmful intent in administering the product. Two types of administrators are distinguished for the TOE: • Operating system administrator of the local computer where MetaClean Sync is installed. • MetaClean Dashboard Administrator.
A.TRUSTED PLATFORM	The product shall run on a trusted platform, including the operating system or any runtime environment on which it is used. The platform versions shall be those recommended by the developer, being admissible but not recommended versions that are in extended support with security patch support and, in any case, unsupported versions. Administrator users of the operating systems on which TOE components are running shall be trusted administrators.
A.PERIODIC UPDATES	The product software will be updated as updates are released to correct known vulnerabilities.
A.TRUSTED UPDATES	The manufacturer shall publish on its official website the update packages together with their SHA256. It is assumed that the website where it is published has a sufficient level of security to ensure that it is an authentic and reliable source.

4.2 Assets to Protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.ADMINISTRATION	Product management interfaces and the information transmitted through them, in both directions.	Confidentiality, Authenticity, Traceability and Integrity.
AS.COMMUNICATIONS	Product communications between its own components and other entities.	Confidentiality, Authenticity and Integrity.
AS.PSS	Configuration data and audit logs which could reveal sensitive information such as usernames, software tools or hardware systems used in an organization.	Integrity
AS.PSC	API key and file metadata before being processed.	Integrity and confidentiality.
AS.UPDATES	Updates of the product that may affect its configuration and functionality.	Integrity

4.3 Threat Descriptions

Threat	Description	Assets
T.NOAUTH	An attacker can gain access as a product administrator by impersonating an administrator to the product, by the product to an administrator, by replaying an administration session, by performing man-in-the-middle attacks.	***AS.PSS, AS.ADMINISTRATION***
T.COM	Weak implementation of standard protocols or use of non-standardized protocols that allow an attacker to compromise the integrity and confidentiality of device communications.	***AS.COMMUNICATIONS***
T.UPD	An attacker can apply a malicious update on the product that compromises its functionalities.	***AS.UPDATES***
T.AUD	An attacker can access, change or modify security functionalities of the product without the consent of the administrator.	***AS.PSS, AS.ADMINISTRATION***
T.MDTEXF	Metadata exfiltration. When transferring documents between different business units of the same corporation or between different corporations, sensitive internal information contained in document metadata, before being processed, could be exfiltrated in an unauthorized way. This information may have been generated by users or automatically and it could include names of business members, business units, usernames, software tools or hardware systems used in an organization. This could enable an attacker to use this internal information as a means to prepare an attack against the organization's systems or users.	***AS.PSC***

4.3.1 Traceability Threats/Security Requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.NOAUTH	T.COM	T.UPD	T.AUD	T.MDTEXF
ADM.2	X			X	
ADM.3	X				
IAU.5	X				
COM.1	X	X	X		X
COM.2	X	X	X		X
COM.3	X	X	X		X
UPD.1			X		
UPD.2			X		
UPD.3			X		
UPD.4			X		
AUD.1				X	
AUD.2				X	
AUD.4				X	
AUD.5				X	
CIF.1		X			
MDT.1					X
MDT.2					X
MDT.3					X
MDT.4					X
MDT.5					X

5 Security Functional Requirements

5.1 SF. Trusted Administration

Requirement	Description
ADM.2	The TOE component MetaClean Sync shall be able to manage the following functionalities: a) Local administration. b) Definition of monitored directories, choosing whether to monitor subdirectories or not, filetypes to monitor in them and associate them with a metadata template. c) Starting and stopping monitors on defined directories. d) Selecting whether to perform an initial sanitization of a monitored directory or not. e) Definition of the URL of MetaClean Dashboard to connect with. f) Set the timeout in hours when log files will be sent to MetaClean Dashboard. The TOE component MetaClean Dashboard shall be able to manage the following functionalities: a) Remote administration. b) Creation of metadata templates. c) Definition of a default metadata template. d) Creation of groups of devices with MetaClean Sync installed and associated to MetaClean Dashboard. e) Association of a metadata template to a group of devices. f) Association of a metadata template to an Organizational Unit from the LDAP server. g) Display statistics regarding the performance of MetaClean Sync.
ADM.3	The TOE component MetaClean Sync shall only allow to be executed with full functionality by administrators of the Windows Server machine in which it is installed. If a non-administrator user tries to execute MetaClean Sync, it shall run with all the administrative functions deactivated. The TOE component MetaClean Dashboard shall restrict the ability of logging in exclusively to administrators before allowing any of the functions described in **ADM.2**.

5.2 SF. Identification and Authentication

Requirement	Description
IAU.5	The TOE component MetaClean Dashboard shall close the user's session after 10 minutes of inactivity.

5.3 SF. Trusted Communication Channels

The ciphersuites listed in this section include the following nomenclature:

- **Recommended (R)**: Refers to the cryptographic algorithms that are considered secure and suitable in the context of HIGH ENS Category.
- **Legacy (L)**: Refers to the cryptographic algorithms, in the context of MEDIUM ENS Category, that are considered with acceptable security in the short term, valid until 2025.

Requirement	Description

COM.1	The TOE shall establish the following communication channels:
	• Communication between MetaClean Sync and MetaClean Dashboard shall be performed through:
	  ○ TLS v1.2:
	  ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)
	• Communication between the Administrator and MetaClean Dashboard shall be performed through:
	  ○ TLS v1.3:
	  ▪ TLS_AES_256_GCM_SHA384 (R)
	  ▪ TLS_CHACHA20_POLY1305_SHA256 (R)
	  ▪ TLS_AES_128_CCM_8_SHA256 (R)
	  ○ TLS v1.2:
	  ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (R)
	• Communication between MetaClean Dashboard and the LDAP Server shall be performed through:
	  ○ TLS v1.2:
	  ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_256_CCM (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_128_CCM (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 (L)
	  ▪ TLS_RSA_WITH_AES_256_CCM (L)
	  ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 (L)
	  ▪ TLS_RSA_WITH_AES_128_CCM (L)
	• Communication between MetaClean Sync and Adarsus License Server shall be performed through:
	  ○ TLS v1.2:
	  ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)
	  ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (R)
	  ▪ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (R)

COM.2	The communication channels in which the TOE is involved shall be started as described below: • MetaClean Sync starts communications with MetaClean Dashboard. • Administrator starts communication with MetaClean Dashboard. • MetaClean Dashboard starts communication with LDAP Server. • MetaClean Sync starts communication with Adarsus License Server.
COM.3	The TOE shall make use of RSA-2048 digital certificates when using the following communication channels: • MetaClean Sync – MetaClean Dashboard • Administrator – MetaClean Dashboard • MetaClean Dashboard – LDAP Server • MetaClean Sync – Adarsus License Server

5.4 SF. Trusted Installation and Updates

Requirement	Description
UPD.1	The TOE component MetaClean Sync, shall display the current software version in the title bar of the window that displays the graphical interface. The TOE component MetaClean Dashboard, shall display the current software version on the top left corner in all the views of the graphical user interface.
UPD.2	The TOE component MetaClean Sync shall verify the integrity of the updates, received from MetaClean Dashboard, through a SHA-256 hash.
UPD.3	The TOE component MetaClean Sync shall allow applying software updates only by environment administrators.
UPD.4	The TOE component MetaClean Sync shall provide the possibility of applying updates manually by environment administrators.

5.5 SF. Audit

Requirement	Description
AUD.1	The TOE component MetaClean Sync shall be capable of registering the following events: • Processed metadata • Monitored directories: creation, modifications (after starting the monitor) and deletion • Changes in general configuration The TOE component MetaClean Dashboard shall be capable of registering the following events: • Login and logout of administrators • Changes in configuration • Creation, modification and deletion of metadata templates • Reception of log files sent by MetaClean Sync
AUD.2	The audit logs shall contain the following information: • Date and time of the event • Type of event identified • Result of the event • User producing the event (if applicable) For processing metadata events, the type of event shall be identified implicitly since they are the only records stored in *prevMetadataLogFile.txt*. The result shall be stored together with the rest of the events identified by the "*processed*" string.
AUD.4	The TOE components MetaClean Sync and MetaClean Dashboard shall be able to store audit logs in the operating system where they are installed.
AUD.5	The TOE component MetaClean Sync shall overwrite the oldest audit log files generating new files of 1MB up to 5 files for the following audit events: • Monitored directories • Changes in general configuration When the number of files is reached, the oldest file shall be deleted. When the processed metadata log file reaches 100KB, the TOE component MetaClean Sync shall rotate the file generating files of 100KB. When the established threshold (3h) is reached, MetaClean Sync shall take up to 5 minutes to send the processed metadata to MetaClean Dashboard, removing them from disk.

5.6 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall only implement the use of cryptographic functions, algorithms and protocols which are included among those authorized for ENS Medium Category according to the CCN-STIC-807 guide**:** • Ciphersuites of communication channels defined in **COM.1**. • RSA-2048 certificates for communications defined in **COM.1**. • SHA-256 hashes for the TOE component MetaClean Sync updates defined in **UPD.2**.

5.7 SF. File Metadata

Requirement	Description
MDT.1	The TOE component MetaClean Sync shall allow starting and stopping a directory monitor previously defined by an administrator. Once started, the monitor can process either local in network units, monitoring in real time, as follows: • If the option "Synchronize" has been selected for a certain monitored directory, MetaClean Sync shall process the metadata of all the files that have not been already processed and that apply, according to the rules defined for such directory. Then, real-time monitoring of the directory shall start. • During successive iterations, MetaClean Sync shall only process files after being saved or created, if they apply according to the rules defined for such directory.
MDT.2	The TOE component MetaClean Dashboard shall allow the creation of templates that define how the file metadata will be processed. Templates shall allow defining how to process each metadata field with one of the following options: • Delete the field contents. • Overwrite field contents with a defined value. • Leave original contents. • Add custom metadata fields with a defined value to the template.
MDT.3	The TOE component MetaClean Sync shall allow administrators to define the following rules for processing file metadata on a given monitored directory: • Whether to monitor subdirectories or not. • The filetypes to monitor within the directory. • Whether to process electronically signed PDF files or not.
MDT.4	The TOE component MetaClean Sync shall delete, overwrite or maintain original file metadata fields, following the template received from MetaClean Dashboard, which shall be requested every 15 minutes. MetaClean Dashboard shall send the template that meets one of the following conditions: • The requesting device belongs to a group of devices defined in MetaClean Dashboard with an assigned template. • The requesting device or user belongs to an Organizational Unit from the LDAP server and has a template assigned in MetaClean Dashboard. • A template assigned in MetaClean Sync to a specific monitored directory. • If none of the previous conditions are met, MetaClean Dashboard shall send the default template.
MDT.5	The TOE component MetaClean Sync shall generate a registry with the original file metadata that has been processed, and periodically send it to the TOE component MetaClean Dashboard, which shall generate and display statistics about the TOE performance regarding processing of file metadata.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
CNI	Centro Nacional de Inteligencia (Spanish National Intelligence Centre).
ENAC	Entidad Nacional de Acreditación (National Accreditation Entity)
ENS	Esquema Nacional de Seguridad (National Security Scheme).
ST	Security Target.
STIC	Seguridad de las Tecnologías de la Información y la Comunicación (Security of Information and Communication Technologies).
TICs	Tecnologías de la Información y la Comunicación (Information and Communication Technologies).
TOE	Target Of Evaluation - Objeto a evaluar.
PDF	Portable Document Format
URL	Uniform Resource Locator
HTTPS	HTTP over TLS
LTS	Long Term Support
LDAP	Lightweight Directory Access Protocol
UID	User ID
OS	Operating System
AD	Active Directory

Table 1 *Abbreviations*

7 Document References

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2004	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 versión 2.0 (Evaluation Technical Report template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022 (National Security Scheme employment cryptology, May 2022).

Table 2 List of document references

8 Annex

8.1 Third Party Libraries Used by the TOE

Library Name	Version	Vendor
org.bouncycastle.bcmail	1.38.0	BouncyCastle.org
org.bouncycastle.bcprov	1.38.0	BouncyCastle.org
org.bouncycastle.bctsp	1.38.0	BouncyCastle.org
Apache Commons Codec	1.10	The Apache Software Foundation
Apache Commons Compress	1.16.1	The Apache Software Foundation
Apache Commons IO	2.5	The Apache Software Foundation
Commons Lang	3.1	The Apache Software Foundation
compress-format	1.7.0_17	Oracle Corporation
org.dom4j	1.5.1	MetaStuff Ltd.
Simple Java API for ODF	0.7-incubating	The Apache Software Foundation
ODFDOM	0.8.8-incubating	The Apache Software Foundation
jakarta.activation	2.0.0	Eclipse Foundation
jakarta.xml.bind-api	3.0.0	Eclipse Foundation
org.apache.xerces.impl.Version	2.9.1	Apache Software Foundation
org.apache.xmlbeans	2.6.0	Apache Software Foundation
Apache Ant	1.9.4	The Apache Software Foundation
ExifTool	12.3.9.0	ExifTool
PHP Anti-XSS Library	1.2	The PHP Group
PHP_XLSXWriter	0.38	The PHP Group
j4mie/idiorm	1.5.6	BSD license
log4net	2.0.8.0	The Apache Software Foundation