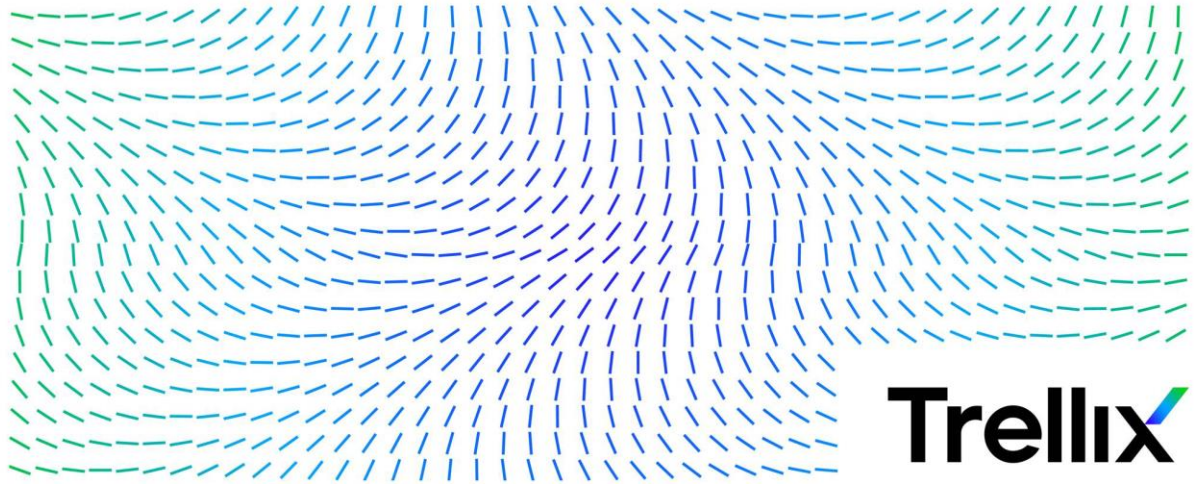
Trellix Endpoint Security (HX) Agent v35.31.31 Common Criteria Guidance Supplement

Release 35.31.31

Document Revision 1.4

Document date: May 21, 2024



Common Criteria Endpoint Agent Addendum Endpoint Agent Addendum

Software Release 35.31.31

Trellix Contact Information:

Website: www.trellix.com

Technical Support: https://www.trellix.com/en-us/support.html

Phone (US):

1.408.321.6300

1.877.347.3393

Table of Contents

1. Introduction

1.1. Scope of Document

This document serves as an administrative guide for the TOE (Target of Evaluation) Trellix Endpoint Security (HX) agent v35.31.31 evaluated for Common Criteria against the Application Software Protection Profile version 1.4 and Functional Package for Transport Layer Security (TLS) version 1.1. It includes the necessary steps to prepare and operate the agent securely within its evaluated configuration.

1.2. References

The following documents were referenced as part of the CC Evaluation of the TOE:

- Trellix Endpoint Security (HX) Agent v35.31.31 Security Target, version 2.3, May 21, 2024.
- Endpoint Security xAgent Deployment Guide Release 35.31.0
- [PP_APP_v1.4] Protection Profile for Application Software, Version 1.4, 2021-10-07
- [PKG_TLS_V1.1] Functional Package for Transport Layer Security, Version 1.1, March 1, 2019

1.3. Terminology

In reviewing this document, readers should be familiar with the following terms:

CC: Common Criteria (CC) is an international set of guidelines and standards used for evaluating and certifying the security features and capabilities of information technology products. The primary goal of Common Criteria is to establish a common framework for evaluating the security attributes of software and hardware products so that customers can make informed decisions about the security of the products they acquire.

TOE: In the context of Common Criteria (CC), the Target of Evaluation (TOE) refers to the specific system, product, or software that is the subject of the security evaluation. The TOE is the entity that undergoes the evaluation process to assess its compliance with the security requirements specified in a Protection Profile (PP) or Security Target (ST). In this document, the TOE is identified as the "Trellix Endpoint Security (HX) Agent v35.31.31.

Endpoint security (HX) server: also called HX server. Trellix Endpoint Security (HX) products include one or more Endpoint Security (HX) Server working with Endpoint Security (HX) Agents (TOE) installed on each device or host in your enterprise. Working together, these products monitor each endpoint device or host and identify threat activity and evidence on them.

1.4. Overview

The TOE is the Trellix Endpoint Security (HX) Agent v35.31.31, a software application residing on a host platform and interacting exclusively with a Trellix Endpoint Security (HX) Server. The TOE is an enterprise-managed agent that runs in the background of a platform of an endpoint to provide protection against common malware as well as advanced attack. Based on a defense in depth model, the TOE uses a modular architecture with default engines and downloadable modules to protect, detect and respond to security events. End users will have no interaction with the software and will

not be alerted of communications with the external Endpoint Security server. As all interactions take place on the Endpoint Security platform. The administrator is expected to deploy the installer with a compliant agent_config.json file (see the section Agent Management Functions).

1.5. Excluded Functionality

The following product functionality is not included in the Common Criteria evaluation:

- SHA-1 is used only in the provisioning of the TOE, not in the digital signature and session authentication functions implemented by the TOE, and
- xAgent to endpoint security (HX) server communication using fast-pooling check on TCP port 80.
- Real-Time Indicator Detection.
- Trellix Exploit Guard Protection.
- Malware Protection.
- The scanning functions, or the specifics of the scanning policies and how they are managed.

1.6. Evaluation Platforms

Common Criteria evaluation has been performed on the following Windows platforms:

- Windows 10 Version 21H2 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1803 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1903 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1909 LTSC 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 2004 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1803 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1903 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1909 LTSC 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 2004 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 11 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2016 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2019 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2012 R2 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2008 R2 (SP1) running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2022 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).

2. Deployment and installation

There are several methods to acquire the TOE's installation images. These include downloading them from the HX server, manually obtaining them from the vendor's cloud servers, or accessing them from the vendor's offline portal. Subsequent updates for the TOE can either be distributed from the HX server or downloaded and installed manually on the host machine. For more details on the deployment and installation of the TOE refer to Endpoint Security xAgent Deployment Release Guide 35.31.0 section titled “Obtaining Agent Installation Software”.

3. Evaluated Configuration

3.1. Operational Environment

Trellix Endpoint Security (HX) Server:

Trellix Endpoint Security (HX) Server is the server from which the TOE and updates thereof are installed on host platforms. For installation on a host platform, the TOE and any updates thereof need to be downloaded from the Trellix Endpoint Security (HX) server. The HX server UI is used to deploy the TOE and configure many of its configurations and settings. Also, the HX server acts as a PKI server, which creates and signs all the used X509 certificates deployed to the TOE.

The TOE collects system events (file, process, registry, network etc.) and processes them as per business logic expressed as scanning rules. It then communicates the results of the scanning to the Trellix Endpoint Security (HX) Server. The Trellix Endpoint Security (HX) Server implements HTTPS TLS for secure communication between itself and the TOE and uses that for all communication.

CRL Server:

The TOE must be associated to a Certificate Revocation List (CRL) Server. The CRL Server contains the revocation list which is communicated to the TOE and used in the validation of the X.509 certificates. The CRL Server is part of the management server associated to the Trellix Endpoint Security (HX) Server.

Host Platform:

The Host Platform may be any computer with an allowed Microsoft Windows operating system. The host platform must have in the minimum 1GB of system memory.

The Host Platform must also implement the necessary network connectivity for the TOE to communicate with the Trellix Endpoint Security (HX) Server. While the TOE implements TLS to protect the content of the communication, the Host Platform must implement the protocol stacks and the physical ports for the connectivity.

3.2. User Roles, Procedures and Operational Guidance for TOE Environment.

The only user roles for configuration of the TOE are administrators defined by the respective customer operational environment. The administrators should have local admin access to the host that the TOE is installed on and admin access to the HX Server.

During configuration, administrators will follow the steps below to facilitate the setup of the TOE and the operational environment:

3.2.1. HX Server FIPS compliance

Enable and verify FIPS compliance on the HX Server through CLI:

- Using an SSH client connect to the IP of the HX Server and login to the HX server with appropriate credentials.
- Enable CLI config mode: *hostname > enable hostname # configure terminal*
- Bring system into FIPS compliance: *hostname (config) # compliance apply standard fips*
- Save your changes: *hostname (config) # write memory*
- Restart the HX server: *hostname (config) # reload*
- Verify FIPS compliance: *hostname (config) # show compliance standard fips*

3.2.2. HX Server Tamper Protection for the Agent.

- Login to the HX Server and navigate to **Admin > Policies** and select **Agent Default Policy**, under **Tamper Protection** toggle “Prevent unauthorized users and processes from tampering with agent files and folders” to off. This allows the admin of the host the TOE is installed on to be able access the install folder of the agent once it is deployed.

3.3. Enabling Encryption

Data written by the TOE is encrypted automatically. This includes all collected data, including data at rest. You cannot enable or disable this encryption.

3.4. Windows BitLocker

In the evaluated configuration, Windows BitLocker must be enabled on the OS Host on which the TOE is installed. BitLocker is available on each of the evaluated platforms.

3.5. Network Connectivity

The TOE requires access to the network to send and receive information from the Endpoint Security server:

- The agent receives requests and updated security information from the Endpoint Security server.
- The agent sends requested data and security information to the Endpoint Security server.

3.6. Assumptions about the TOE

To ascertain that the TOE can effectively fulfil its security requirements in its evaluated configuration, it is imperative for the organization to meet the specified conditions outlined in the claimed Protection Profile:

- 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.
- PROPER_USER: The user of the application software is not wilfully negligent or hostile and uses the software in compliance with the applied enterprise security policy.
- PROPER_ADMINISTRATION: The administrator of the application software is not careless, wilfully negligent, or hostile, and administers the software in compliance with the applied enterprise security policy.

4. Agent Management Functions

Trellix Endpoint Security Agent management functions can be performed by updating the

agent_config.json file, using the HX server GUI or by running commands on the command line.

- Agent Configuration File Management Functions
- Agent Command-Line Management Functions

Prerequisites

- Administrator access

4.1. Agent Configuration File Management Functions

After you have installed agent software, you can configure certain settings for it. These settings are stored in the agent_config.json file.

Trellix does not recommend manually changing many settings in the agent_config.json file. Some of the settings in this file should not be changed without the advice of your Trellix support representative, generally for troubleshooting. In addition, some settings should be updated only using Endpoint Security CLI commands or Web UI settings, as opposed to the text editor.

If you change values in the agent_config.json file without consulting Trellix or in a manner not recommended by Trellix, your agent software functionality may be compromised.

This section lists common settings in the agent_config.json file and describes how and whether they can be changed. It also describes the steps you must take to the edit the agent_config.json file and ensure it is valid after your edits.

- Editing the agent_config.json File
- Channel setting
- Credentials settings
- Events settings
- exploitDetection settings
- Fips settings
- id setting
- Logging settings
- Name
- Process settings
- Serverlist settings
- Service settings
- ts setting
- Type setting
- Version Setting

The frequency at which the agent communicates with the server is set by the user. By default, each agent pools the server every 600 seconds (10 minutes) to obtain information and task requests and pools the server every 30 minutes to obtain the latest indicators. By default, the server requests system information (sysinfo requests) from the agents every four hours.

4.1.1. Editing the agent_config.json File

To edit the agent_config.json file directly:

1. Verify that you are logged in as an administrator of the machine on which the agent is installed.
2. On the command line, navigate to the version 35.31.31 agent installation directory where the xagt.exe file is stored.
3. Export the agent_config.json file from the agent database:
   xagt -x agent_config.json
4. Using a text editor, make changes (as needed) according to the instructions in the rest of this documentation.
5. When all changes have been made, run the file through a JSON validator to ensure the JSON code is valid.
6. When the file has been validated, save it.
7. Import the agent_config.json file back into the agent database:

xagt -i agent_config.json

8. Restart the agent.

   xagt -r

4.1.2. Channel setting

The channel setting identifies the configuration channel to which the agent should subscribe. The default is default. Do not change the value of this setting without the advice of your Trellix support representative.

4.1.3. Credentials settings

The credentials settings consist of certificates related to SSL credential parameters for agent operations. Do not change the values of these certificates without the advice of your Trellix support representative.

4.1.4. Events settings

The events settings control how the agent handles real-time events and intelligence downloads. The keys in this section are listed below in alphabetic order.

Key Name	Edit Manually?	Description
active_ collection_ enabled	Yes	Indicates whether real-time data collection is allowed. Valid values are true(allow real-time data collection) and false(do not allow real-time data collection). The default is true.
intel_poll_ sec	Yes	Specifies the interval (in seconds) at which polling for intelligence occurs. The default is 900 seconds.
intel_uri	Yes	Identifies the URI from which intelligence is downloaded. The default is /content/v1/intel/default/win_iocv2.
max_db_ size	Yes	Specifies the maximum size, in megabytes (MB), of the agent event database.
udp_ send_ events	Yes	Indicates whether UDP (network) events should be captured. Valid values are true (capture UDP events) and false (do not capture UDP events). The default is false.

4.1.5. exploitDetection settings

The exploitDetection settings control how exploit detection is configured. Do not change the value of these keys without the advice of your Trellix support representative.

4.1.6. Fips settings

The FIPS settings consist of a single parameter indicating whether the TOE complies with the cryptographic requirements outlined in the NIAP Common Criteria: Application Software Protection Profile version 1.4 and Functional Package for Transport Layer Security (TLS) version 1.1. Do not change the value of this parameter without the advice of your Trellix support representative.

4.1.7. id setting

The id setting identifies the configuration ID for the agent. This value is supplied by the Endpoint Security server. Do not change the value of this setting without the advice of your Trellix support representative.

4.1.8. Logging settings

The logging settings control how logging occurs for the agent.

Key Name	Edit Manually?	Description
Enabled	Yes	Indicates whether logging is enabled. Valid values are true (logging is enabled) and false (logging is disabled). The default is true.
log_ level	Yes	Specifies the level of data logged. Valid values are debug(the highest volume of log lines), info, notice, warn, err, crit, alert, emerg, and idle(the lowest volume of log lines). The default value is idle.
log_ mask	Yes	Enables component-level logging for any of the following components. When more than one component is specified, separate the component names with colons (:). - UVPROC enables logging of calls to libuv read/write functions. - SSLPROC enables logging of SSL functions. - QUEUE enables logging of internal queue usage. - JOB enables job-related logging.

4.1.9. Name setting.

The name setting identifies the configuration name. This value is supplied by the Endpoint Security server. Do not change the value of this setting without the advice of your Trellix support representative.

4.1.10. Process settings

The process settings control Endpoint Security agent processing.

Key Name	Edit Manually?	Description
cpu_limit	Yes	Specifies the maximum percentage of CPU use allowed by all agent processes. Valid values range from 10 through 100 percent. The default is 100 percent. The CPU usage total of all agent processes must stay within this limit. Non-agent processes do not count towards the limit.
Priority	Yes	Specifies the scheduling priority of the agent process. Valid values are highest, high, above, normal, below, and idle. The default value is idle.
protection_ enabled	Yes	Indicates whether agent protection is activated. Valid values are true (protection is activated) and false (protection is not activated). The default is true. This setting should be set to True to confirm with the CC evaluated configuration.
deny_local_admin_stop	Yes	Allow/disallow local admin from starting/stopping the agent services. The default is true.
detect_unsigned_image_loads	Yes	Prevents loading of unsigned DLLs into Agent process
file_protection_enabled	Yes	Prevent unauthorized users and processes from tampering with Trellix agent files and folders
strict_certificate_validation	Yes	Perform strict certificate validation on agent binaries

4.1.11. Serverlist settings

The serverlist settings define the server address list. Do not manually edit these settings in agent_config.json. Instead, define them using the Web UI or CLI commands. The keys in this section are listed below in alphabetical order.

Key Name	Edit Manually?	Description
disable_ provisioning	No	Indicates whether or not provisioning has been disabled for the server. Valid values are true(provisioning is disabled) and false (provisioning is not disabled). The default is false.
Server	No	Identifies the server IP address and port number.

4.1.12. Service settings

The service settings define the interaction between the server and the agent. Only one key is included in this section.

Key Name	Edit Manually?	Description
config_ pull_ enabled	Yes	Indicates whether the agent configuration file is dynamically pulled from the server. When the configuration file is pulled from the server, configuration updates are applied automatically, overwriting the file on disk. A new configuration file may force the agent service to be restarted, depending on which configuration setting was changed. Valid values are true (the configuration file is dynamically pulled) and false (the configuration file is not dynamically pulled). The default is true.

4.1.13. ts setting

The ts setting identifies the configuration timestamp. This value is supplied by the Endpoint Security server. Do not change the value of this setting without the advice of your Trellix support representative.

4.1.14. Type setting

The type setting must be set to config. Do not change the value of this setting without the advice of your Trellix support representative.

4.1.15. Version Setting

The version setting identifies the JSON version used to parse. Do not change the value of this setting without the advice of your Trellix support representative.

4.2. Agent Command-Line Management Functions

The following command-line parameters can be specified for the xagt command on the command line.

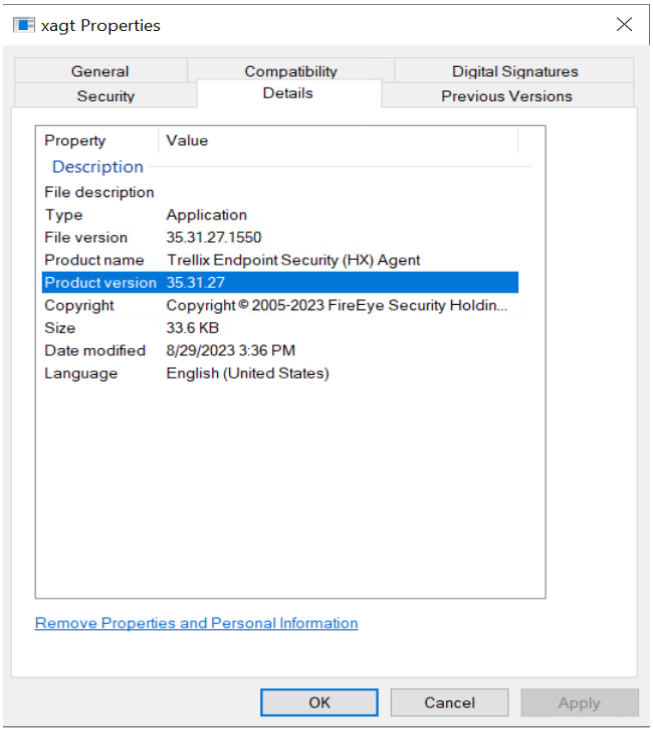
To run the xagt command, you must be logged in as an administrator and you must have navigated to the version 35.31.31 agent installation directory where the xagt.exe file is stored.

Parameter	Shortcut	Description
--help	-h	Lists the command-line parameters and their usage. For example: xagt -h
--log	-l	Sets the log level. Valid values are IDLE, EMERG, ALERT, CRIT, ERR, WARN, NOTICE, INFO, and DEBUG. The default setting is IDLE. For example: xagt -l info
--log-export	-g	Exports the log to the specified file. For example: xagt -g log.txt
--restart	-r	Restarts a running agent. For example: xagt -r
--version	-v	Displays the agent version. For example: xagt -v

5. Verifying the TOE Version

You can determine the agent version in two ways.

1. Run the xagt exe --version command on a command line.
2. Right-click on the agent executable file (xagt.exe), wherever it is installed. Select **Properties** on the drop-down menu and click the **Details** tab of the Properties dialog box.



6. Configuring Certificates

The TOE does not necessitate any form of credentials for communication with the HX server, except for authentication via an x509 certificate. The Trellix Endpoint Security (HX) Server provides a TOE's certificate, in the agent configuration file that is included in agent download packages. Changing any of x509 certificates inputs in the initial TOE's configuration file will result in the failure to install the TOE. The certificates included in the TOE's configuration file are an x509 Certificate authority certificate in addition to the TOE's certificate. If this issue arises, it is recommended to download a fresh copy of the agent software from the HX server and install it on the endpoint. See section 4.1.3 for more details.

Throughout operation, the TOE exclusively communicates with the HX server within a closed environment. Only one certificate is assigned to the TOE for its own use, meaning it will present only this certificate in cases where validation by the HX server is required.

The certificates provided in the initial agent configuration file or in an already provisioned Agent should not be modified. Modifying any of these x509 certificates in an already installed and provisioned TOE will disrupt the connection between the agent and the HX server. The agent automatically receives a renewed certificate from the HX server as part of the routine configuration update scheduled to occur at predefined intervals.

At every startup of the agent, it will start a secure connection to the HX server, to synchronize its clock before doing any other tasks. Before the first-time synchronization, the TOE will not process HX server presented certificates, and it can accept expired HX server certificates until the TOE's clock is synchronized.

7. Updating the TOE

The updates to the TOE are distributed as MSI package files. The MSI package files are signed using certificates with a public trust chain which leads to DigiCert. Some components of the installation package (for instance, RemediationWSC), are signed using certificates with a public trust chain which leads to Sectigo.

When the Endpoint Security (HX) server creates an upgrade job for the agents, the upgrade package is staged and signed. The signature is imbedded in the agent software. Upgrade packages are created using the HX server Web UI.

All downloaded installation executable files include standard *.msi signatures that are verified during installation. If this validation fails, the upgrade fails.

There are two methods to update the agent:

7.1.1. TOE Manual Update

Agent installation images obtained manually must be uploaded to the Endpoint Security (HX) server before they can be deployed to your host endpoints. This ensures that the correct agent configuration file and agent certificates are included in the agent installation package you deploy to your host endpoints.

1. Login to the HX server web console.
2. Navigate to **Admin > Agent versions**, select the version of available upgrade and click **Download agent installer** and copy/move it to the platform that the TOE is currently installed.
3. Login to the TOE's host machine.
4. Extract the package.
5. Run the msi installer package **xagtSetup_xx.xx.xx_universal.msi** to start the upgrade.
6. After the upgrade installation completes, verify that the TOE version is correct (Ref. Section 5).

7.1.2. TOE Update via HX Server

1. Login to the HX Server web console.

2. Navigate to **Admin** > **Host sets** and create a Host set for the machine with the agent installed.
3. Navigate to **Admin** > **Agent Upgrade** and select **Create Upgrade**.
4. Select **"Include Hosts"** for the Host set created earlier and verify if an update/upgrade is available by viewing the "Eligible for Upgrade" display on the page.
5. In the Select Version drop-down, select the Agent version for this upgrade job if one is available.
6. Under Specify installer location, select the default location for the Agent upgrade package (:\Program Files\FireEye\xagt) or enter the URL of an alternate server where the upgrade package resides
7. Under 'Set end date', click 'Set end time' or leave it at 'Never' (the default setting). If you do not specify a time for the upgrade job to stop running, it will keep running, even if all host xAgents have been upgraded. You must manually stop the upgrade job to end it.
8. Click **Create** to finalize the "Create Upgrade" process. View the job details and upgrade process under **Admin > Agent Upgrade.**

8. TLS Common Criteria settings

The TOE generates an RSA 2048-bit key pair and constructs a Certificate Signing Request (CSR) with the public key. The CSR is sent to the Endpoint Security Server to be signed which constructs an X.509 certificate and returns it to the TOE.

The TOE only implements TLS as a sender. The TOE does not support pinned certificates. Wildcards are supported and they only match in the left-most label and do not match with labels featuring an explicit prefix or suffix.

The agent configuration file should be modified as part of the product installation to limit the cipher suites used by the agent to only those used by the Endpoint Security server.

In support of secure communication with the endpoint security server, the agent implements the TLS protocol using mutual authentication mechanism. No configuration is required on the TOE to enable it to participate in mutual authentication during TLS communication. The TOE will automatically transmit its x509 certificate when requested by the HX server during TLS communication. If the HX server does not send the certificate message request, the client will not transmit its certificate.

Follow these steps to configure the TOE into its evaluated configuration:

1. Using a text editor like notepad++ or notepad, edit the agent_config.json configuration file. General information about doing this is described in Editing the agent_config.json File on section 4.1 .
2. To set the cipher suite used to TLS_RSA_WITH_AES_128_CBC_SHA, use a text editor, add an advanced section with an mxs/tls/cipher key to the configuration file, exactly as shown below:
   "advanced": {"mxs/tls/cipher": "!aNULL:!eNULL:!ECDSA:AES128-SHA"},

   This limits the key exchange algorithm to RSA and encryption to AES 128 CBC.

   Note: This is the only cipher suite configured to meet Common Criteria Compliance. The use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

3. Locate the service section of the configuration file and update it exactly as shown below (replacing the existing service section):
   "service": {"config_pull_enabled":false},

   Changing this setting in the Json config file in the TOE, ensures that when the configuration file is automatically pulled from the server, the cipher updates you made in the previous step are not overwritten.

4. When the TLS connection is being established, the agent verifies the reference identifier found in the SAN (Subject Alternative Name) or the CN (Common Name) field in case the SAN is not configured in the X509 presented certificate of the HX server. The TOE supports exact matching and wildcard usage for both types of identifiers, with the condition that the wildcard is the entire left-most label. However, it does not support IP address as reference identifier or certificate pinning.
   Add the following option to the configuration file to enforce verification of the identity of the Endpoint Security server:
   "fips": { "enabled":true,
   "hostnames": "host1.myuid.uid.crt"},

Where “host1.myuid.uid.crt” matches the CN/SAN of the certificate.

9. Other Common Criteria Settings

The TOE can monitor host endpoints for previously unrecognized exploits and other online attacks using a feature called Exploit Guard Protection. However, it's important to note that this feature, while not evaluated or tested, provides both exploit detection and prevention. Additionally, the TOE's Exploit Guard Protection feature is not compatible with Microsoft Defender Exploit Guard Protection, as both offer similar protection mechanisms.

The Common Criteria configuration mandates that Windows Defender Exploit Guard protection be enabled. To achieve this, please ensure that the agent configuration under the 'process' node is configured as follows:

“process”: {

"priority": "idle",
"cpu_limit": 100,
"deny_local_admin_stop": false,
"detect_unsigned_image_loads": true,
"file_protection_enabled": false,
"protection_enabled": false,
"strict_certificate_validation": true

},

Note: Some administrative parameters in this system are modified through editing JSON configuration files. The content of the Json file will be validated during the next restart of the TOE’s services, therefore wrong syntax or modification to protected fields will not be imported to the TOE. Adjustments of parameters through JSON file editing should be ideally under the guidance of vendor support representatives. Administrators should also double check both syntax and semantics of any change before saving the JSON file and directing the system to ingest the change.

10. System Audit Examination

The TOE accesses system RAM, Filesystem and log files on the host machine while it is collecting information. As requested, some of this data may be transferred to the Endpoint Security server for further examination.

The agent monitors its host for host status and alert matches and reports this information to the server. Depending on acquisition parameters, the agent accesses the host file system to gather and deliver data for file and triage collection. It accesses RAM to gather the host full memory and system process memory for examination. It also accesses log files for host events.

The agent retrieves and runs any other server tasks or jobs (such as upgrading and containing hosts). The automatic triage feature allows agents to collect host information surrounding the time of an alert. In addition, the agent can run audit scripts to help diagnose problems on the host endpoint.

The standard diagnostic audit script returns the following host related information:

- agentinfo

- w32processes
- log audit.
- w32rawfile-acquisition
- w32registryraw
- w32network-arp audit
- w32network-dns audit
- w32network-route audit
- w32rawfiles audit
- config key-val, config file acquisition
- exploit detection ETL trace file irrespective of exploit detection status.
- sysinfo audit

11. Technical Support

For technical support, contact Trellix through the Support portal: https://www.trellix.com/en-us/support.html

11.1. Documentation

Documentation for all Trellix products is available on the Trellix Documentation Portal (login required):

https://docs.trellix.com/