Secure Endpoint

Best Practices Guide

Version 2.4
Author: Secure Endpoint TME
Target audience: Beginners, Professionals
Release Date: 2021-06-11

Technical Guide
Cisco public

About This Document

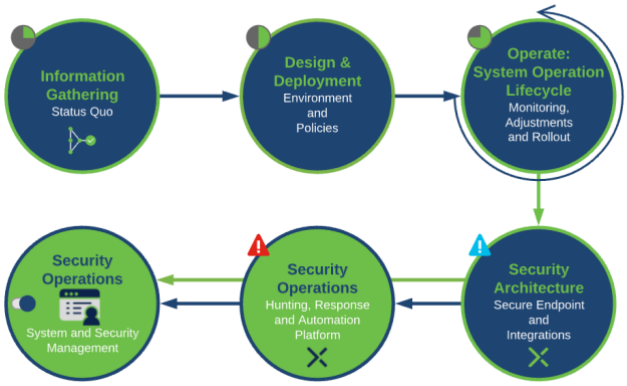
Cisco Secure Endpoint (formerly AMP for Endpoints) is a comprehensive Endpoint Security solution designed to function both as a stand-alone Endpoint Detection & Response (EDR) product, and as an important part of the Cisco SecureX EDR/XDR Architecture®. There are many considerations that customers and partners should be aware of prior to deploying and configuring Secure Endpoint in their environment. The objective of this document is to provide guidance on best practices for deployment methodology, setup and configuration.

Note: The Best Practice Guide is designed as a supplemental document for existing product documentation and does not contain a comprehensive list of all Secure Endpoint configuration options. For more in-depth detailed product settings, please see other official Secure Endpoint documentation located at: https://docs.amp.cisco.com/

This document outlines the recommended stages for successful deploying Cisco Secure Endpoint. The flow chart here serves as a generalized framework for customers to use within their environment.

This includes:

- **Information gathering:** Necessary information about your environment
- **Design & Deployment:** Policy and Rollout planning
- **Operation Lifecycle:** daily product operations, policy adoptions, endpoint updates and upgrades
- **Security Architecture:** Activate included Hunting tools, e.g. SecureX threat response or Real Time Endpoint Search. Activate SecureX including the Ribbon app. Understand the Pivot Menu and add 3rd Party Threat Information. Activate available Post Infection tasks/features included in Secure Endpoint product.
- **Security Operations:** Activate SecureX orchestration to automate and orchestrate security operations. Integrate and enhance existing security Architecture and integrate into existing SOC environments.



During any enterprise-wide deployment, it is recommended to follow these stages in a progressive manner, starting with information gathering and all the way up to integrations setup. Continuous review and improvements are also a part of any successful Secure Endpoint deployment.

They are necessary to ensure a smooth deployment experience, accurate configuration tuning, and timely resolution of any potential performance issues. Cisco recognizes that each customer environment is unique, and this framework should serve as a recommendation only as it may need to be adjusted according to the specifics of the customer use case.

Content

Information Gathering

Introduction

Information gathering is a necessary starting point that ensures the smoothest deployment experience and configuration of Secure Endpoint. This section outlines important considerations around environmental data, security product data, and compliance requirements gathering.

- Endpoint Operating systems (Windows/Linux/macOS)
- Numbers of endpoints
- Existing security products and architecture
- Software deployment process
- Custom applications
- Proxy availability
- Endpoint connectivity information (proxies required, remote (VPN) or local firewalls
- Privacy requirements

Environment Information

The first step is to understand and document the existing security posture. This includes collecting information on the existing environment. The following questions are a good place to start, though it is by no means comprehensive list:

- How many endpoints need to be protected?
- What Operating Systems and Architectures are included in deployment?
- Will Secure Endpoint be installed on endpoints that includes existing EDR software?
    - If so, will it be removed before or after Secure Endpoint is installed?
    - Or will it remain side by side with existing EDR software?
- What endpoints and software are mission critical?
- How is software delivered to endpoints?
- How do endpoints connect with applications/services?
- Do endpoints rely on the use of a proxy?
- Do endpoints roam or connect via VPN?
- Is there inventory of software used on endpoints?
- Is there a Lab environment for testing including the necessary endpoints?
- Are there any Customer defined bandwidth or port restrictions for LAN/WAN links?

The answers to these questions (along with other business process and policies) will provide information helpful for decisions related to deployment. Collecting any other information specific to customer endpoint management needs to be included during this information gathering step.

Security Product Information

Many companies already generated sophisticated documentation for their endpoint security solution, including e.g. business critical software, necessary exclusions and defined deployment processes. This is already a great deal of information regarding what could potentially be transferred to Cisco Secure Endpoint policies. Rather than start from scratch, this information should be compiled, evaluated for current relevance, and used to inform the Secure Endpoint setup process.

The following list is a good place to start, though it is by no means comprehensive:

For the product administrative users:

- Who will need access to the console portal?
- What access should users be granted to the console portal?

What features are used in existing endpoint security? Such as:

- Blocking network activity
- Features that already exist in Secure Endpoint
- Other security features

What configurations exist in existing endpoint security? Such as:

- Exclusions
- Application Block lists
- Application Allow lists
- IP address block lists

While collecting this information, the policies and lists can be refined. Review of the policy lists and features will allow clean up and validation of required endpoint security. Removing policy items will strengthen the security on the endpoint.

Cisco Secure Endpoint is a lightweight connector. Optional, it can operate with other EPP/EDR security products. The existing settings and features will need to be reviewed, in order to ensure that the respective products integrate properly without interfering with each other.

Auditing and Compliance

Many organizations are subject to Auditing and Compliance requirements. These requirements force organizations to maintain data regarding who accessed and made changes, when those changes were made, and historical data related to endpoint security performance. Cisco Secure Endpoint provides detailed user auditing and endpoint historical data with a limit of 30 days. Additional historical retention can be gained by utilizing the Event Streaming functionality.

To ensure that your new Secure Endpoint installation meets these requirements, it is advisable to obtain answers to the following:

- What are your organizational auditing requirements?
- What governmental compliance requirements is your organization subject to?
- PCI DSS, GDPR
- What is your organizational requirement for historical data storage?

Info
Cisco Trust Center: Cisco Trust Center – Privacy Sheets
Cisco GDPR related information • **Product Overview:** https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html • **Secure Endpoint / AMP for Endpoints Privacy Data Sheet:** https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/security/cisco-amp-endpoints-privacy-data-sheet.pdf • **Secure Endpoint / AMP for Endpoints Data Map:** https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatamap/security/amp-privacy-data-map.pdf

Preparation

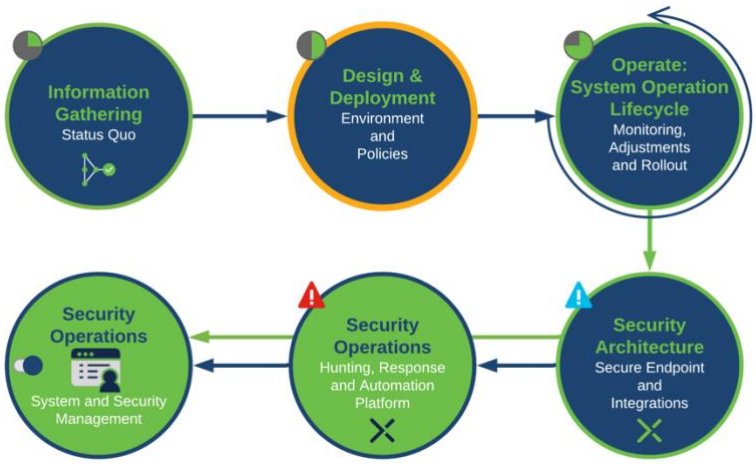
Introduction

Deploy preparation is the next step in the process. This includes deployment planning and policy setup. These steps will depend on the information gathered. While preparing for deployment, there might be some questions that need to be answered before a proper policy can be configured. In some cases, doing testing or engaging with pilot user groups can be used to identify answers that can only be answered in a live environment.

This section outlines background information about Secure Endpoint, which helps to build a well and functioning Cisco Secure Endpoint environment.

Design and Deployment Planning

Design and Deployment Planning stage is the next step in preparation. This stage leverages the data collected in the information gathering section to make deployment relevant decisions around the use of Secure Endpoint, configuration planning, and policy setup.



Cloud infrastructure - Features and Services

Cisco SecureX and Cisco Secure Endpoint follow a Cloud first approach. The endpoints communicate with the cloud infrastructure to receive new policy updates, production updates, file dispositions, live query requests, etc. The cloud architecture provides several features and services.

1. **Secure Endpoint Cloud:** Provides all needed services for the endpoint. As the endpoint fully integrates into SecureX, it is essential to enable SecureX after you have activated your endpoint product.
    a. Endpoint Guides: https://console.amp.cisco.com/docs / https://console.eu.amp.cisco.com/docs /
    b. Required Server Addresses for Proper AMP & Secure Malware Analytics (formerly Threat Grid) Operations: https://www.cisco.com/c/en/us/support/docs/security/sourcefire-amp-appliances/118121-technote-sourcefire-00.html
    c. Cisco Secure Endpoint Support Documentation: https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html
2. **Secure Endpoint Connector:** The software package installed to your endpoints providing protection and generating the telemetry information for the Cloud Detection Engines.
3. **Secure Endpoint Orbital:** Provides Real Time investigation on the endpoint.
4. **SecureX Platform:** The platform provides several services for the Secure Endpoint solution.
    a. **SSO:** Single-Sign-On for all UIs.
    b. **SecureX threat response:** The Investigation tool to query the whole infrastructure for given Observables.
    c. **Orchestration:** Automate Security by building the right workflow.
    d. **Integration Modules:** Integrations into Cisco Secure products and 3rd Party vendors to receive Threat Information. Several vendors are providing a community subscription. http://cs.co/threatresponseintegrations
    e. **SecureX Ribbon:** The Ribbon is an Overlay App, provided by SecureX and is available for SecureX integrated Cisco Secure consoles. The Ribbon includes other apps like the casebook app, incident app or Orbital app to start a Real Time investigation on the endpoint.
    f. **SecureX Pivot Menu:** The Pivot Menu is a security tool, powered by SecureX, that is available in the UIs of many Cisco Secure products. The Pivot Menu provides a very sophisticated and easy way to get immediate, cross-product reputation information on observables, and take common research and response actions on them across your installed Cisco and 3rd party products.
    g. **SecureX Information Sources:** More detailed information about SecureX, features and benefits
    h. **SecureX Documentation:** http://cs.co/SXO_docs
    i. **SecureX Workflow Repo:** http://cs.co/SXO_repo
    j. **SecureX Videos:** http://cs.co/SecureX_videos
    k. **SecureX FAQs:** http://cs.co/SecureX_faq
5. **Cognitive Analytics:** This service analyses standard W3C Log data for malicious traffic. Events are directly posted to the Secure Endpoint Events.
6. **Secure Malware Analytics:** File analysis platform to detonate unknown and unique file to determine malicious behavior indicators.

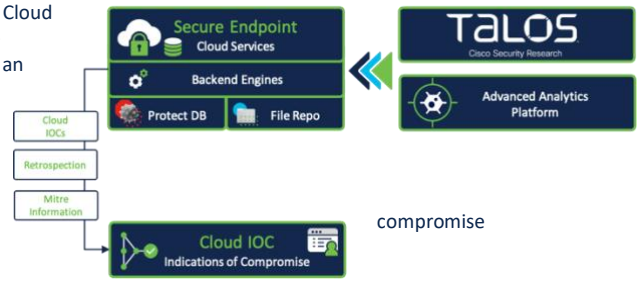
Security Architecture: Secure Endpoint is part of an EDR Architecture including several Threat Hunt and Threat Investigation capabilities beside typical Endpoint Protection capabilities.

Note: For high privacy needs Cisco provides the Secure Endpoint Private Cloud Appliance. This On-premise installation provides highest privacy without integration into other Cloud products and services. Please review **Appendix-A: Secure Endpoint Private Cloud** for more details.

Cloud Infrastructure – Backend Intelligence

The Secure Endpoint backend engines are processing Telemetry data provided by the connector. Based on the connector count, the backend is automatically sized. This data is processed in Real Time and additional retrospective for 7 days. During this period or time, the Secure Endpoint backend receives latest Threat Information, which is correlated with all the Telemetry data from the endpoints.

The outcome from Real Time Processing and Retrospective Analysis are Cloud IOC events. Cloud IOCs are generated by logic and intelligence to detect malicious behavior. This can include malicious files, but in many cases no malicious file is involved in a possible compromise of an endpoint. To raise the Threat context Cisco adds an IOC description and MITRE information. Some main considerations for Cloud IOCs.

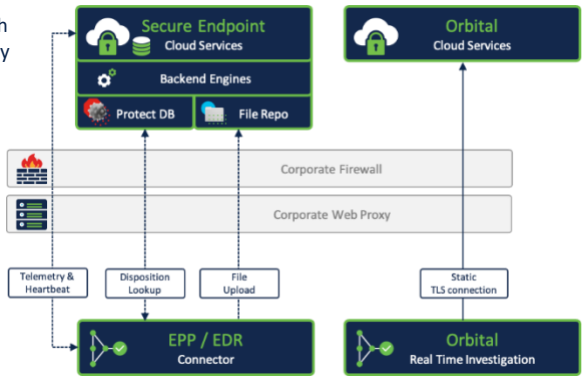


- Real time and retrospective IOC Events
- are used to automate Post infection tasks (automated actions)
- are outlined in the Device Trajectory to show endpoint behavior around the compromise
- regular updates on these intelligences to provide sophisticated detection
- MITRE information directly shown in IOC events

When thinking about a Security Architecture, Cloud IOCs are a very important and useful information to start a Threat Hunt, starting a Threat Investigation or drive security automation.

Cloud Infrastructure - Endpoint Connectivity

Secure Endpoint needs proper configured firewall/proxy systems to be able to communicate with the Public Cloud to query dispositions, send telemetry data for backend processing, receive policy updates, and receive updated definitions. Secure Endpoint uses secure technologies to protect information between the endpoint and cloud. It is recommended that firewalls and proxies are updated to allow communication to the Public Cloud.



Cloud communication

Secure Endpoint Troubleshooting Technotes on cisco.com website:
Required Server Addresses for proper endpoint & malware analytics operations:
http://cs.co/AMP4EP_Required_URLS

Cloud communication: Proxy environments

For environments that use proxies, the proxies must be configured so there is no interception of the TLS communication, which would break communications to the Public Cloud. Policies also need to include proxy configuration that the endpoint can use. Secure Endpoint will only use system defined or policy defined proxies. This prevents communications from being tempered or blocked by sending communications to a malicious proxy.

Best Practice: Disable TLS interception for Secure Endpoint Communication, as it would break the communication.

Cloud communication: Bandwidth consumption

After Secure Endpoint is installed, the AV Signatures are updated. Secure Endpoint does incremental updates for the AV signature, but needs a full initial update after the deployment. For bandwidth saving, you may deploy AMP Update Servers as needed. During EDR operations, where the connector generates the Telemetry Data for Backend Processing, low bandwidth is needed. See the table below for details.

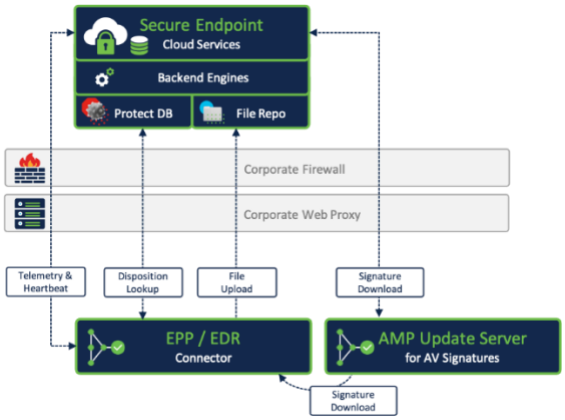
Size per Update per endpoint	Signature Update	Normal Operations (Endpoint Telemetry)
~500MB	initial AV Signature Update	n.a.
< 1MB to 8MB	Incremental Signature Update (~ 4-8 times per day). If the endpoint misses more than 30 incremental updates, a full signature update is done.	n.a.
~540 bytes per Lookup	n.a.	Expected average count per day ~54 queries/day All Engines enabled on the endpoint.

On-Premises Components

AMP Update Server

For environments that have constrained bandwidth requirements, an option to store AV definitions on premises can be made with an Endpoint Update Server. Using this update server is recommended only when Public Cloud with AV scanning is enabled, and bandwidth usage is a concern.

AMP Update Server Configuration Steps:
https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213237-amp-tetra-on-prem-server-configuration-s.html



Best Practice: It is recommended that an AMP Update Server is not used with Public Cloud deployments in high network bandwidth environments or for endpoints that are connected on external networks.

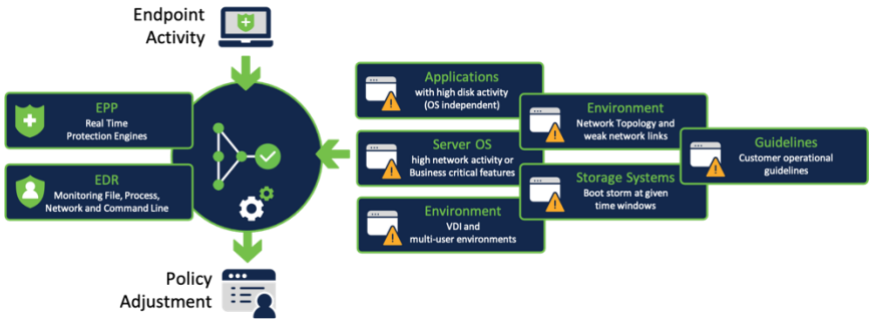
Fundamental Endpoint Connector Design

The Secure Endpoint Connector is a lightweight connector. The goal is to minimize the system load on the endpoint as much as possible. From an EPP/EDR perspective, the connector includes two main areas.

- Real Time Protection Engines (EPP)
- Endpoint Monitoring (EDR - Telemetry Data for Backend processing)

Understanding how the connector works is important and helpful for your Endpoint Security Design and helps to avoid poor usability. There are many circumstances which may have an impact on the connector performance and reliability. A proper configuration is essential for best performance.

As an example, EPP can have an impact on an application with specific characteristics. On the other side, specific application characteristics can result into AMP connector high CPU usage.



Best Practice - Application Impact to connector
Conclusion: There are some common situations which may cause high CPU load:
- High disk activity, where the connector must scan and hash a lot of files.
- Scanning archive files, as unpacking archive file consumes much CPU resources.

File Scanning Sequence

Scanning files is one of the most resource intensive processes on the endpoint. Secure Endpoint does a lot of steps to scan/detect/quarantine files and scripts, or to scan inside compressed files.

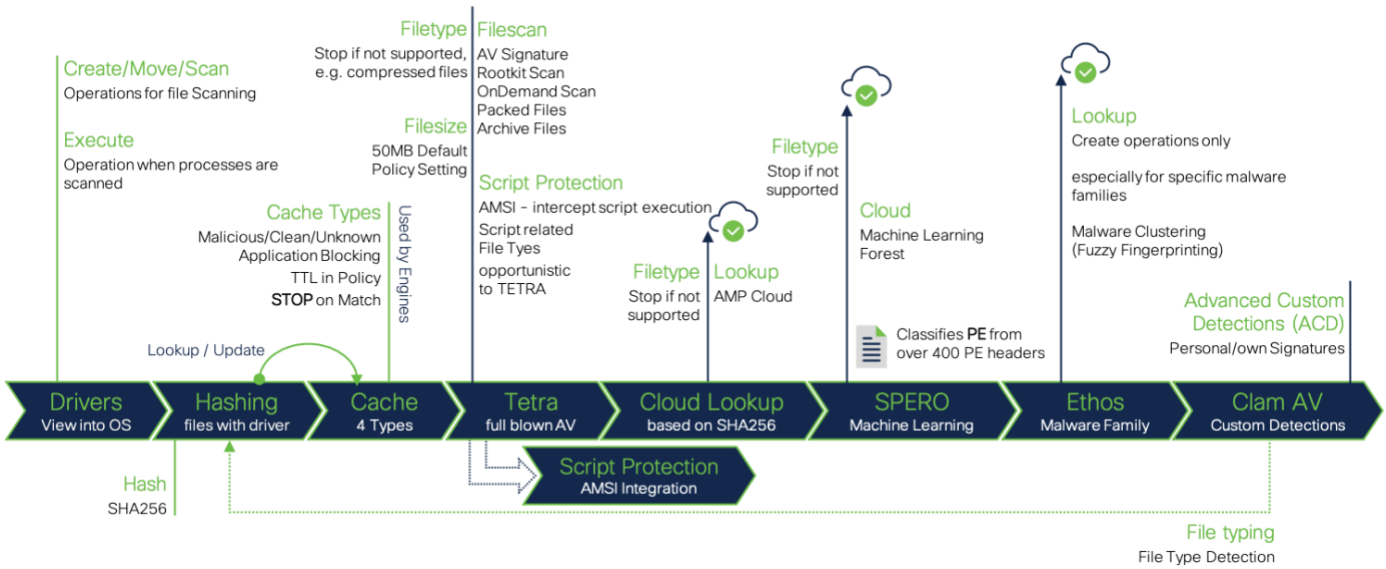
The Secure Endpoint Connector uses the following sequence to scan files on the disk (schematically view). Please keep in mind that many circumstances like file size, file type or policy settings can have an impact on the sequence. In most scenarios, the whole sequence is not processed. Engines like Script Protection, which integrates into Microsoft AMSI, Spero and Ethos are available on Windows Operating System only.

1. **Drivers:** The drivers are the view into the OS. The connector engines are scanning on Create/Move/Scan/Execute operations.
2. **Hashing:** Files are hashed by the driver and added to the local cache. Some parts of Clam AV engine are used for real File Type detection. This is important for all other operations.
3. **Cache:** Secure Endpoint includes 4 different types of Cache. To improve performance, the file scan process stops, if there is a cache hit. The TTL for all cache types can be changed in the policy.
4. **AV-Scan:** If there is no cache hit AV scanning is done. The AV Engine is used for OnAccess Scan, OnDemand Scan, Packet Files Scan, Archive File Scan and Rootkit Scan.
5. **Script Protection:** Secure Endpoint integrates into Microsoft Anti Malware Scanning Interface (AMSI) to scan Script Files processed by the Microsoft Script Interpreters.
6. **Cloud Lookup:** If there is no match so far, the endpoint does a cloud lookup to get threat information for a given hash.
7. **SPERO: Machine Learning:** Analyzing files with Machine Learning techniques.
8. **Ethos, Malware Grouping:** Malware Grouping Engine, which enables the endpoint to detect known malicious activity for unknown files.
9. **ClamAV:** ClamAV is used as an OEM engine on Linux and macOS system. The Windows connector does not use this engine for scanning. ClamAV is used to provide Custom Detection capabilities and file type detection.

Note: A Stop (shown in the graphics below) does not necessarily stop the whole detection sequence, it depends on several circumstances.

Examples:

- If Tetra stops scanning, the sequence may not be stopped.
- If the disposition returned from the Cloud Lookup or a cached result is clean, the sequence terminates early.
- If no detection engine on the endpoint detects a threat, the EDR part still monitors the activity around a file/process and the Cloud Engines are processing this information. This can result into a Cloud Indication of Compromise (IOC) even no endpoint Real Time engine reported a detection.



Best Practice - File Scanning: Finally, for best performance take care about applications generating high disk activity. E.g., Database Servers, Web Servers, development environments, inventory software and so on. This guideline is independent if there is a Server or Workstation operating system installed. Threat Protection and Detection or Threat Risk Mitigation is not a linear process. The Detection Sequence should give you an insight into the product for better understanding how to tune the product as needed.

Note: Please keep in mind, Advanced Custom Detections only work on files of unknown disposition

Supported Operating Systems

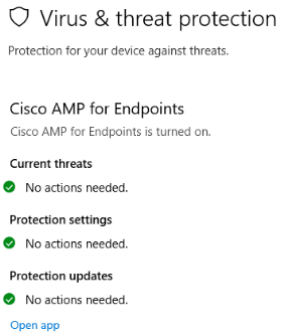
The Secure Endpoint connector is available for Windows, Linux and macOS Operating System. Secure Endpoint Console also provides to integrate iOS and Android devices, as they are in supervised mode.

The official supported versions are listed on the cisco.com website.

- Windows: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214847-amp-for-endpoints-windows-connector-os-c.html
- Linux: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215163-amp-for-endpoints-linux-connector-os-com.html
- macOS: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214849-amp-for-endpoints-mac-connector-os-compa.html
- Security Connector iOS compatibility: https://www.cisco.com/c/en/us/support/docs/security/security-connector/215337-cisco-security-connector-apple-ios-compa.html

Windows Security Center Integration

Secure Endpoint integrates into the Windows Security Center for Virus and Threat Protection after the AV Signatures are fully updated. Keep in mind, this may take some time until the registration process is finished. In this state, the connector already provides protection including all other engines and cloud lookups.



Windows Defender

Since connector version 6.3.1 Secure Endpoint includes a new Service called Cisco Security Monitoring Service. The service is responsible to register Secure Endpoint to the Windows Security Center (WSC). Review details in the Secure Endpoint User guide.

With Version 7.4.1.20439 and later, the integration procedure into WSC has been changed, as the connector registers itself directly after the installation. Previous versions do a full signature update before registering to WSC.

Competitor Products

- **Removal:** Secure Endpoint does not remove any competitor products during the installation process. To replace existing Security products, there are two possible ways to do:
  - Install Secure Endpoint, remove the competitor product. Afterwards reboot the endpoint. This ensures, that the endpoint is protected at any time.
  - If there are any issues or product conflicts, you must remove the competitor product first, reboot the system and install Secure Endpoint after the reboot.
- **Incompatibilities:** There are some known incompatibilities with other security products, which are listed in the Deployment Strategy Guide: https://docs.amp.cisco.com/en/A4E/AMP%20for%20Endpoints%20Deployment%20Strategy.pdf

Endpoint Grouping

Groups are used to categorize the endpoints and the respective policy. It is recommended to define groups to apply a policy on similar endpoints. Attributes to group the endpoints can consist of items such as:

- Type (Server, Desktop, or Laptop)
- Location (Region, Branch or Remote access)
- Application set installed
- Services or Operational functions utilized
- Enabled Security features and options
- User groups (Early adopters, Developers, Power Users, or Regular users)
- Existing grouping

It is recommended that servers and desktops are associated with separate policies because the usage, features, and architectures are different.

Best Practice: Anything related to the endpoint, including the whole policy, Feature Activation like Endpoint Isolation or Orbital Real Time Search are tied to the policy object. A recommended approach is to separate endpoints only if needed. This reduces the necessary administrative effort to manage the endpoints.

Info: Policy Refresh: Cisco Engineering already started a project for Re-Design the Group/Policy handling. The change will provide much more flexibility for policy handling, as components of the policy object will be de-coupled.

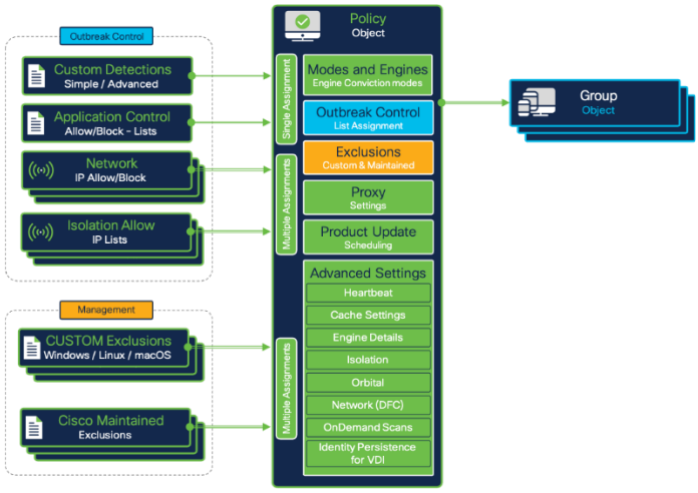
Beside Endpoint grouping based on the info above, it is important to think about how to assign Policies to these groups. These policies can include different types of lists. Lists are assigned to Policies. Based on the List Type, a list can be assigned once to a policy object or multiple times. The settings inside the Policy Object and the assigned lists are generating the policy information for the endpoint. Any change triggers a new policy version. During the next heartbeat, an endpoint sorted into the group receives the new policy.

Policy Configuration Planning

Secure Endpoint policies need to be configured so that the features selected provide the best endpoint security while users are not impacted by functional or performance problems. Policies are associated to groups of endpoints. From the information gathered and endpoint groups, policies can be configured for the desired features and exception lists.

Outbreak Control Lists (Console → Outbreak Control): as shown in the graphics, depending on the list type, it can be assigned once or multiple times to a Policy Object. Each list can be assigned to multiple Policy Objects.

Exclusion Lists (Console → Management → Exclusions): Each List can be assigned multiple times to a policy object. Each List can be assigned to multiple Policy Objects.



Policy Configuration Planning - File Scan

File scanning is the core functionality of Secure Endpoint. This core engine will scan files for malicious signatures and act on malicious files. File scanning will generate a nominal increase in CPU, I/O, and network requests to the cloud. Without file scanning, there is no visibility of file create, move, modification, or execution.

It is recommended that file scanning is enabled to protect files from compromising the endpoint with a malicious file or the ability to retroactively detect a compromise. Endpoints with applications that require heavy file I/O might be impacted by the file scanning. In cases where an application performance is impacted, exclusions can be made on file scanning to reduce any I/O that interferes with the application.

Policy Configuration Planning - File Scan Exclusions

Secure Endpoint provides two different types of exclusion lists. Custom Exclusions and Cisco Maintained Exclusions. Both can be assigned to a policy object multiple time.

Review basic exclusion management: http://cs.co/AMP4EP_Best_Practices_Exclusions

Maintained Exclusions History: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214809-cisco-maintained-exclusion-list-changes.html

Best Practice: Keep your exclusions clean and organized. Defining multiple exclusion lists with the right naming greatly simplifies exclusion management.

Policy Configuration Planning - Network Monitoring

Network monitoring allows Secure Endpoint to collect addresses between the endpoint and other destinations. This information is used to identify and act on malicious destinations. Network monitoring will generate a nominal increase in CPU and network requests to the cloud. Without network monitoring, the information needs to be correlated with external information and would only be visible for internal network resources. Using network monitoring allows a consolidated investigation using Cisco SecureX Architecture®.

It is recommended that network monitoring is enabled for endpoints that do not have a high network load required. This should be enabled for primarily workstations and some servers without a need for high volume of network traffic.

If network monitoring interferes with network operations of an endpoint, either the endpoint can be associated to a policy that doesn't enable network monitoring or install the connector without the DFC component.

Best Practice: Regardless of if there is a Workstation or Server Operating System installed, it is recommended to disable Network Monitoring for Systems with high network load, network teaming or if there are many VLANs configured.

Policy Configuration Planning - Protection Engines

Other protection engines (such as Offline engines, Malicious Activity Protection, etc.) provide protection against additional malicious behaviors. Enabling each engine will improves the efficacy of Secure Endpoint. Depending on the engine or configurations enabled, the efficacy is improved at the cost of performance. When enabling or changing settings on an engine, it is recommended to test changes before deploying them to production endpoints.

Note: When activating a new Engine on a sensitive system which is divergent to the recommended settings, a good option is to start in Audit Mode. In Audit Mode, the connector generates an Event, but does not block in any way.

v1.91 Appendix-B: Non-Standard Environments (VDI) shows more information when activating File Scanning in VDI environments.

It is recommended that engines are enabled and tested. Below are the choices and considerations on how the policy is configured for the engines.

Engine Policy Setting	Efficacy	Performance costs	Other Comments
Enabled	Higher efficacy. This improvement depends on • Engine options enabled • Overzealous Exclusions	Higher cost. This cost depends on: • Application that run on the endpoint • Missing Exclusions	Events sent to Cisco SecureX Architecture® for visibility and central investigation.
Disabled	Lower efficacy	Lower cost on performance.	Only advised for such instances as: • Another product provides equivalent functionality • Performance cost is too high to enable

			• Application incompatibility
Configuration changes	Efficacy change depends on configuration changes.	Performance change depends on configuration changes.	Other configurations such as exclusions can be configured to improve engine performance on the endpoint.

Policy Configuration Planning - Cisco Advanced Search - Orbital

Cisco Advanced Search (Orbital) enables Real Time Investigations on your endpoint. The Orbital Client enables are static connection to the Orbital Cloud Service. It is recommended to enable this feature in the policy to enhance threat hunting or incident response. Testing needs to be done for endpoints that are sensitive to increase in CPU usage. Orbital should be disabled if the increase is too significant.

Getting more value from your endpoint with Orbital: https://blogs.cisco.com/security/getting-more-value-from-your-endpoint-security-tool-2-querying-tips-for-security-and-it-operations

Some considerations regarding Orbital

- Orbital is an additional endpoint component to provide Real-time Queries on an endpoint.
- You need the right license for Orbital: https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/package-comparison.html
- After activated in the policy, Secure Endpoint installs the Orbital client fully automated.
- Orbital Endpoint (orbital.exe) holds a static TLS 1.2 connection to the Orbital cloud.
- Orbital provides generating a Forensic Snapshot, which can be generated manually or automated.
- Orbital uses SQL (Structured Query Language) to query the endpoint like a database.

Preparation Checklist

Take a moment to review the summary for the Secure Endpoint preparation step.

- ☐ Secure Endpoint integrates into the SecureX Architecture. Keep in mind to enable all available feature and functions. Find the list of all Services in the Cloud Architecture Overview in this document
- ☐ The Backend Engines are processing the Endpoint telemetry data in nearly real time and retrospective for 7 days back.
- ☐ Check Proxy/Firewall settings, so the connector can communicate with the Cloud services.
- ☐ There is some bandwidth required for the initial AV Signature update or if there are 30 incremental updates missing. You may deploy AMP Update Server as needed.
- ☐ Secure Endpoint may have an impact on Application performance and specific Application characteristics may impact Connector Resource consumption.
- ☐ Secure Endpoint does not change any setting for Windows Defender and does not remove 3rd Party security products
- ☐ Endpoint Grouping, Policy generation and List Assignment should be well planned to simplify operational work and to raise security.
- ☐ Cisco Advanced Search provides a very simple way to query endpoint information using SQL.

Secure Endpoint - Console Setup

Secure Endpoint Console Setup: This section will provide important information on how to configure User Accounts, create and configure Policies and Groups, set up Prevalence and Outbreak Controls, create Exclusions and activate Automated actions for Post Infection tasks.

This includes:

- User Account Setup
- Create and configure Policies and Groups
- Set up prevalence and outbreak controls
- Create exclusions
- Activate Automated Actions
- Set up AMP Update Server

After you received the activation e-mail for your Secure Endpoint account, click the provided link to do the initial setup of your Cisco Security account. Find detailed information in the Secure Endpoint Entitlement Guide for more details.

Best Practice: Secure Endpoint is an important part of the SecureX EDR/XDR/MDR architecture. Secure Endpoint provides Hunting Features like the Device Trajectory and the File Trajectory. It generates Cloud IOCs by processing the endpoint telemetry data. SecureX is available with any Secure Endpoint license and provides much more Hunting and Investigation capabilities and Security automation. It is highly recommended to connect Secure Endpoint console to SecureX to enable all the provided hunting and investigation capabilities, before configuring the policies and deploying endpoint connectors. Find the list of services in the Cloud infrastructure - Features and Services Section.

The recommended steps are:
- Navigate to security.cisco.com to activate SecureX
- Navigate to visibility.amp.cisco.com to activate SecureX threat response
- Navigate to orbital.amp.cisco.com to activate Secure Endpoint Advanced Search

Find more details in the SecureX - EDR/XDR/MDR Architecture Section of this document.

User Account Setup

User Management is described in detail in the Secure Endpoint User Guide under Accounts. Important, there are several Secure Endpoint features unavailable to user accounts that are not properly configured. To ensure access to all available configuration options, product capabilities and sensitive information, it is important that users enable Two-Factor authentication.

Two-Factor authentication is required for the following features

- remote file fetch
- command line visibility in Events
- prevalence features

Two-factor authentication

To properly configure your user's Two-Factor authentication click your account name in the upper right corner of the Secure Endpoint UI and select My Account. Optional, navigate to Secure Endpoint user management:

- Click **Accounts → Users** and then select your username.
- Click **Enable** next to the **Two-Factor authentication** option and follow the onscreen instructions carefully configuring your Two-Factor authentication using one of the recommended applications (**Duo**, Authy, Google Authenticator).
- Return to the user page and you should now see that Remote File Fetch and Command Line are enabled.

NOTE: Keep your recovery codes in a secure place. If you have already moved to Cisco SecureX SSO, you cannot change Two-Factor authentication in Secure Endpoint backend anymore, as the SSO service has been moved to SecureX platform. To manage your two-factor authentication, navigate to https://me.security.cisco.com/ (User Identity Settings).

Enable SecureX platform and SecureX SSO

The SecureX Platform is available with any license. After you got familiar with the login to Secure Endpoint console, it is highly recommended to **enable the SecureX platform** and to switch to **SecureX Single-Sign-On (SSO)**. Follow the steps outlined in the SecureX Opt-In guide to activate the SecureX platform and SecureX SSO. Review the Cisco SecureX Sign-On Quick Start Guide showing how SecureX SSO (SAML) works.

Note: When logging-in to Secure Endpoint, the account type created is a Cisco Security Account. Do **not** create a new SecureX account directly on the SecureX login page. This will generate a new ORG ID in SecureX, which will be different to your ORG ID for Secure Endpoint. For the first login to SecureX use your Cisco Security Account for SecureX login. This ensures to generate the right SecureX ORG ID, which is identical with your Secure Endpoint ORG ID.

Note: After you have enabled SecureX SSO, the legacy login to Secure Endpoint Console is not available anymore.

Cisco provides several tools to manage your users, SAML and Two-Factor authentication. The table below shows some sources and the configuration options.

Platform and Links	
Secure Endpoint	
https://castle.amp.cisco.com	Manage Secure Endpoint users and your SAML (SSO) configuration.
SecureX	
https://sign-on.security.cisco.com/	Login to Cisco SecureX platform
https://security.cisco.com/	Login to Cisco SecureX platform
https://me.security.cisco.com	SecureX User Identity Settings and Multi-factor Authentication management. Rename Organization and see recent account activity.
https://sso-apps.security.cisco.com/dashboard	SecureX Application Portal
https://www.cisco.com/c/en/us/td/docs/security/secure-sign-on/sso-quick-start-guide/sso-qsg-welcome.html	SecureX Sign-On Quick Start Guide

Console setup checklist

Take a moment to review the summary for the console setup.

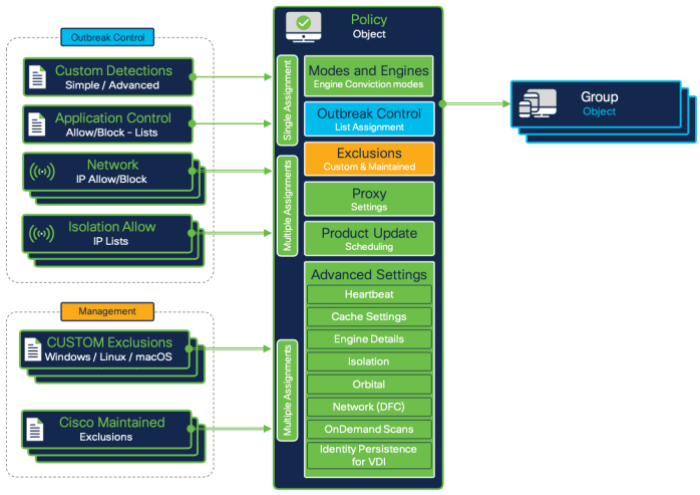
- ☐ Cisco highly recommends activating SecureX as one of the first steps. The SecureX - EDR/XDR/MDR Architecture sections show more details about the SecureX Architecture.
- ☐ Enable Two-Factor authentication for the user to be able to see and configure data sensitive settings.
- ☐ Navigate to security.cisco.com and activate the SecureX platform. Review the guides to enable SecureX platform and moving to SecureX SSO.
- ☐ Build your policies based on the previous chapters Policy Configuration Planning and Secure Endpoint Connector Design. Find the right settings for performance and security in the chapter Policy Design -Performance and Security
- ☐ Enable File Analysis (Prevalence) and post infection tasks as described in chapter SecureX - EDR/XDR/MDR Architecture

Policy Design and Management – Performance and Security

Policy creation and management is the heart of Secure Endpoint. Policies control all configurable aspects of connector function. As such it is important to ensure that all newly created policies are created with the current and future organizational structure in mind. To maintain this flexibility, Cisco recommends creating as few policies as necessary to properly address organizational needs.

The Screenshot shows the Secure Endpoint Policy architecture. This helps to understand the dependencies between the configurable objects and the Policy object itself in the AMP console. This architecture helps you to avoid having multiple lists with duplicate entries. On the left side the Objects (Outbreak Control, Management) are listed which can be used directly in Policy Objects.

Outbreak Control: Custom Detections (Disposition Change), Application Allow/Block Lists (Execution), Network IP Allow/Block and Isolation Allow Lists are assigned to policies. By default, the Secure Endpoint Console provides several policies for administrators to build on-top of. These policies are designed to provide a high level of security while minimizing potential performance impact to the endpoints. When determining policy settings for the various endpoint features, Cisco advises customers to follow the recommended settings provided on the policy page with minimal modification to meet organizational security needs.



There are two primary types of policies provided by default: **Audit** and **Protect**.

- **Audit** policies provide a means of deploying a Secure Endpoint connector while ensuring limited interference on an endpoint. Default Audit policies will not quarantine files or block network connections and as such, they are useful for gathering data for connector tuning during initial deployment and troubleshooting.
- **Protect** policies provide a higher degree of endpoint protection. Connectors utilizing these policies will quarantine known malicious files, block C2 network traffic, and perform other protective actions.

Best practice: Secure Endpoint best practice for policy creation is to create a set of base policies, then duplicate these policies to create the debug and update versions of the same policies. This allows for maintained consistency while gathering debug data and performing connector updates.

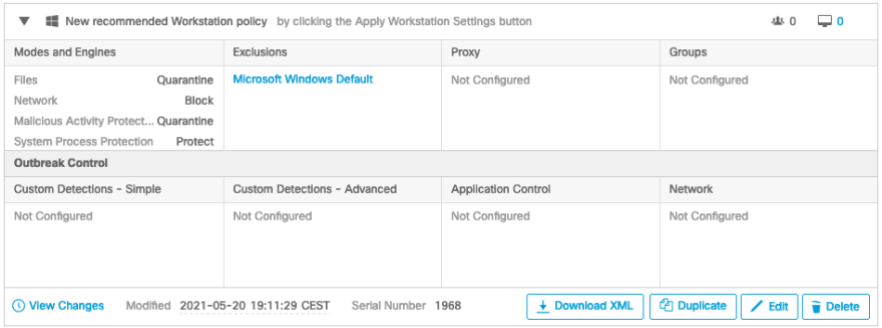
Info: By default, the Secure Endpoint Console provides several policies for administrators to build on-top of. For fast and easy product testing, you can directly use the predefined groups and policies.

The Policy Object

Secure Endpoint provides policies for Windows/Linux/MAC, Mobile Devices like Android and iOS and Network Devices. If no Network device is registered to the AMP cloud, the tab is hidden. The policy Objects are available under Management → Policies.

The policy view shows much information about the policy object.

- Configured mode of the Engines
- Assigned Exclusions
- Proxy Settings
- The groups where the policy is used
- Assigned Detection Lists
- Application Control Lists
- Network Lists (Whitelist/Allow)
- Last modified date
- Serial Number of the Policy (number increased after any change)



Button Download XML: The downloaded file can be added to a broken connector locally in the Secure Endpoint installation directory. This can help, if the connector is not able to communicate with the Secure Endpoint Cloud anymore. To replace the policy.xml file on the connector, stop the connector service → replace policy.xml → start the connector service again.

When generating a new Policy object, the Cisco maintained exclusion list **Microsoft Windows Default** is added to the policy object only.

Policy settings: Best Performance and Security

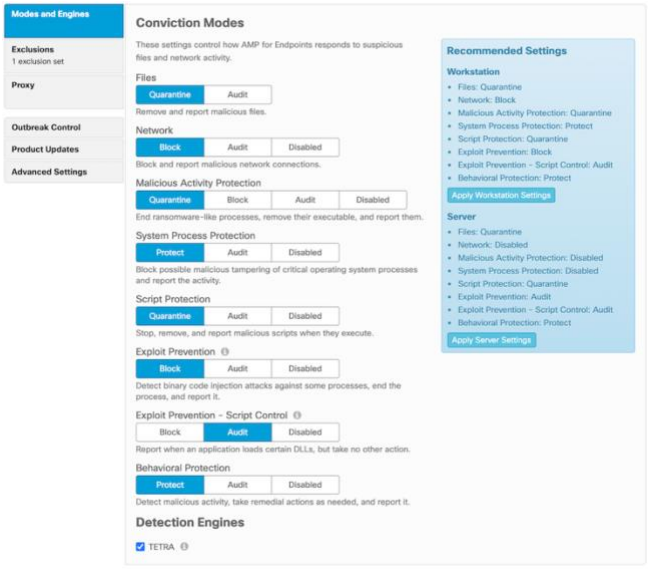
The steps below outline best practice info for Secure Endpoint policy settings. There is no difference if you install Secure Endpoint on a Workstation or Server Operating System, it is the same code base. The previous chapter already gave you some understanding about fundamental Connector Functionality. This section outlines important information and enables you to build a policy which fits your performance and security needs. The section outlines useful information to build your Workstation and Server policy.

Please refer to the **Secure Endpoint product guide** for any setting not explained in this guide: https://console.amp.com/docs. Read this information carefully

Policy Setting: Modes and Engines

The Modes and Engines area gives you an overview about all available engines and its modes. It shows the recommended Settings for Servers and Workstations.

Note: Not all engines are available on all operating systems.



File Scanning: Scanning for malicious files is done by several engines on the endpoint, using different techniques. Even the whole file scanning sequence is not static. Depending on file type, cache info and more, for a file detection more or less scan/detection steps get active. Review the file scanning sequence info for details. By switching File Scanning to Audit, the whole file scanning sequence does not remove a file from the disk.

Recommended Settings: the blue box shows the recommended Engine Settings for Workstation and Server operating systems. These settings are a good choice to start a new policy. Some considerations for Engine Conviction modes.

- When disabling an engine in the policy, the driver is still available on the endpoint. So, the engine can be activated easily at any time.
- When using the installation switches like /skipdfc or /skiptetra, the driver is not installed. This requires a re-install of Secure Endpoint to enable the feature again.
- Automated actions → move computer to group: This automated post infection task moves a computer to a configured group if malicious activity has been detected. This group should have all engines enabled, to ensure the highest possible detection rate. Therefore, all drivers should be available on the system.
- If the AV-Engine driver has not been installed, OnDemand Scans on the system are not available. Review v1.92 Appendix-C: add Tetra manually after /skiptetra was used to add AV-scanning to a system if the /skiptetra switch was used.

Best Practice: When designing File scanning in your environment, review the steps below.
- If you plan to enable AV-scanning later, do not use the /skiptetra installation switch, as this prevents the driver installation. Enabling the policy does not add the driver files to your endpoint. To add drivers to the endpoint again, Secure Endpoint must be re-installed.
- File scanning in VDI environments needs some more granular considerations. Review v1.91 Appendix-B: Virtual Environments (VDI) for details.
- There is a workaround to manually add AV-Scanning to the Windows Endpoint later. Review v1.92 Appendix-C: add Tetra manually after /skiptetra was used for details.

Best Practice Security: Detection and Protection capabilities.
- If AV-scanning detection/quarantine events are missing, the backend engine may generate additional Cloud IOCs. This can happen if the endpoint detects a malicious file, but there is not AV-Engine present to remove the file from the disk.
- You may use the automated action feature to clean up a system where AV-scanning was disabled in the policy. Review v1.80 SecureX - EDR/XDR/MDR Architecture for details to move computers to a configured group to enable highest detection capabilities.
- OnDemand Scans cannot be performed without the AV-scanning engine.
- **Full detection policy:** If there is an indication of compromise where you want to enable highest detection, AV engine should be enabled.

Policy Setting: Define and manage Exclusions

Over time there are often many different Exclusions List defined in the Secure Endpoint console. Exclusions not needed anymore should be removed. Enclosed some guidelines to help you simplifying Exclusion List management.

Cisco-maintained Exclusions: These lists help you to exclude critical files and processes. The Cisco Maintained Exclusion Lists hists is available here: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214809-cisco-maintained-exclusion-list-changes.html

Custom Exclusions: Some guidelines to make Exclusion management easy.

- **Global Exclusions:** Exclusions for Applications which are needed on most of your systems. E.g. an application which is installed on most of your endpoints. Such exclusion lists are assigned to many policies. If you need a new exclusion for this specific application, you just need to update and maintain a single exclusion list.
- **Exclusion List Naming:** This simplifies the Exclusion management. If there are many different versions of an application in place, splitting the exclusions and adding the software version to the exclusion list name helps to simplify exclusion clean up in the future. As seen in the screenshot, the Policy Object is easy to read.

Note: The Secure Endpoint connector includes some exclusions list limits, which cannot be changed (Connector version 6.0.5 and higher). All values are very high and should not be reached during normal operations.

- The limit of process exclusion is 100 across all the exclusions sets
- In policies whit more than 100 process exclusions, only the first 100 are honored
- The exclusions are sorted alphabetically
- The maximum recommended number of exclusions is 300
- The size limit for the policy.xml is 40KB and includes all type of exclusions
- The maximum count for exclusions is 1000

Best Practice: Exclusions: Normally the exclusion list limits should not be reached. Take care if there are many exclusions for specific endpoints. Your group design also helps to reduce the amount of needed exclusion lists. Find additional information in the Best Practices for Secure Endpoint Exclusions guide: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213681-best-practices-for-amp-for-endpoint-excl.html.
- name your exclusion lists right
- multiple exclusion lists help you to cleanup outdated exclusions
- Cisco maintained exclusions help to lower exclusion handling effort

Wildcard Exclusions need more system resources for evaluation than any other exclusion type. If possible, use Wildcard Exclusion as less as possible.

Policy Setting: Exclusions and Security

Exclusions are important for product functionality and reliability. Many customers exclude business critical applications to prevent any possible impact from endpoint security. There are many valid factors to define exclusions. Hashing consumes system resources even before scanning by an engine.

Scan Exclusions also stop the connector from scanning and monitoring. As a result, **excluded areas have the following impact** on your EPP/EDR security level.

- Files are not hashed, not available in the cache, not scanned and no cloud lookup is done.
- Activity is not monitored and sent to the backend.
- Information is missing for the Backend Engines. Malicious activity in an excluded directory will not generate an output (e.g., Cloud IOCs).
- There is no information shown in the Device Trajectory.
- Files will not be uploaded for Advanced Analysis.

Any other activity before and after is monitored and analyzed by all available engines.

Best Practice Security: To reach the highest level of security and to maximize the effectives of Endpoint Engines and Backend Engines, Cisco recommends adding Exclusions only if necessary.
- **Full detection policy:** Remove as much as possible exclusions to enable scanning of most areas on the disk and to enable protection for running processes.

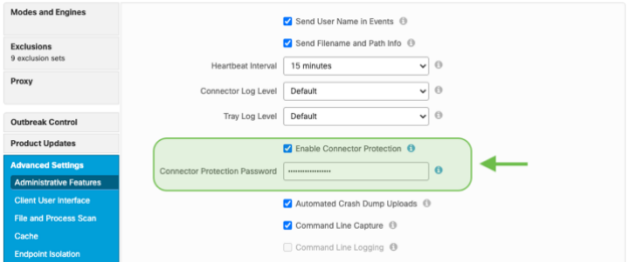
Policy Setting: Proxy

As already explained, the protocol inside the TLS1.2 connection is not HTTP. If TLS is terminated at the proxy, the proxy will drop the packages, because it is not HTTP, and Secure Endpoint communication will stop. The connector still uses the Offline Engines, but all other features like Online Engines, Cloud Lookups and Backend Engines will not work anymore. Finally, there are some guidelines for Proxy Connection.

- Never inspect TLS Traffic on the proxy, it will break the cloud communication.
- When using Proxy authentication, there are some unsupported NTLM authentication scenarios (review the product documentation).
- If a proxy server is configured, any update is done through the proxy.
- The cloud communication is dynamic and switches to direct communication if the proxy is not available.

Policy Setting: Connector Password (Self-protection)

Always set a password, so the Connector is protected against deactivation and uninstall from unauthorized users or malware.



Policy Setting: File and Process Scan

On Execute Mode: Cisco recommends keeping On Execute Mode settings as Passive.
Keep this in mind when changing to Active.

- In Active mode, files and scripts are blocked from being executed until a determination of whether or not it is malicious, or a timeout is reached.
- This also includes the cloud lookup.

Maximum Scan File Size: The Default Value in the Policy is set to 50MB. This value can be lowered, but not raised. Any file bigger than this value will be ignored by the Connector for EPP/EDR functionality. This value is a good compromise between Security and Product functionality. Malware files typically are not bigger in size than 50MB, hashing files up to 50MB does not generate too much CPU load.

Best Practice Security: In case, where **an infected or compromised** endpoint is moved to a defined group using Automated Actions, you may use the following settings:
- Set the maximum scan file size to 50MB, to scan as much as possible files. If a file is bigger than 50MB, any activity around this file is still monitored, scanned and processed by the Backend Engines.
- In any case where security is more important than performance, set the On Execute Mode to Active.

Policy Setting: Cache

The cache speeds up connector performance. If there is a hash already available in the Cache, the connector does not scan a file anymore.

The cache can be cleared on a system as followed:

1. **Stop** the AMP connector **service**.
2. **Delete** the **Cache files** local on the disk (located in the Connector directory)
3. **Start** the AMP connector Service again.

Review Removal of the Secure Endpoint Cache and History Files on Windows in the Troubleshooting Technotes.

Best Practice Security: Cache settings have an impact on performance and security
- Microsoft Office Applications x64 are nearly 50Mb in size. Lowering this value should only be done for endpoints where Microsoft Office is not installed. Microsoft is still a big attack vector on endpoints.
- **Full detection policy:** Set all cache values to the lowest setting.

Policy Setting: File Scanning - Archive Files vs. Packed files

It is important to understand the difference between these two configurable settings.

Archive Files: The AMP connector opens compressed files and scans their contents. Tetra uses the values from the File and Process Scan settings. Default value for File Size is 50MB, and for Archive Files 5MB. Typical compressed files are 7zip, arj, jar (Java Archive), tar or zip files.

Archive Scan uses the following limits to prevent system overload. Enclosed some guidelines.

- Archive File scanning depends on the file sizes as listed above.
- Archive File scanning depends on supported file types.
- Batch of 1000 files, if compressed file includes e.g., 1mio. files.

There's a maximum of 5 levels, however there is no limit for files inside of a zip on the same level unless you want to scan 1 million files at the same time from one compressed file meaning that would be done automatically by batches of 1000.

Packed Files: Having the "Scan Packed Files" option enabled, Tetra Engine detects files which are an ASCII File, but can be executed. Example: a *.JS file is an ASCII File, but can be executed (*.JS files are considered a package in the sense, that the files are executable in that state but are made up of other files/code).

Best Practice: Unpacking Files needs a lot of system resources. Especially Development Environments working with much compiled and compressed code. So, it is highly recommended to group such endpoints and assigning a policy, where special exclusions are configured. Development endpoints are often different to typical endpoints and standard exclusions may not work. To avoid performance detraction, you may disable "Scan Archives" in the policy.

Best Practice Security: Some guidelines for best detection/protection.
- If you deactivate the "Scan Packed Files" Setting, Tetra will no longer detect malicious JS Files.
- **Full detection policy:** Both settings should be enabled to provide highest detection/protection capabilities.

Policy settings: Workstation

Generate a new default policy for Workstation Systems:

- Generate a new policy object under Management → policies by clicking the new policy button.
- Select the Operating System you want to generate the policy for and click new policy.
- Add a meaningful name, optional a description and click the ***Apply Workstation Settings*** Button on the right. This applies the Cisco recommended settings.
- Install the Secure Endpoint **without** any command line switches (default installation), so all engines get installed.

The generated policy object is a very good starting point:

- Files: Quarantine
- Network: Block
- Malicious Activity Protection: Quarantine
- System Process Protection: Protect
- Script Protection: Quarantine
- Exploit Prevention: Block
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

Policy adoptions checklist:

- **Exclusions:** Add additional exclusions only if really needed to provide the best security. Review the Secure Endpoint Installation, Updates and Operational Lifecycle section how to figure out additional needed exclusions. Review Exclusions best practices for Performance and Security when defining additional exclusions.
- **Lists:** In Secure Endpoint console, under Outbreak control generate a list for custom detections simple, custom detections advanced, application control allowed, application control blocked and Network - IP Block & Allow lists. Assign them to your policy. These lists will also be available in the SecureX Pivot Menu. Review the Policy Configuration Planning for best practice.
- **Endpoint Isolation:** Activate this feature as needed. It allows to disconnect your endpoint from the network **manual** or **automated** using Automated Actions. Review the v1.80 SecureX - EDR/XDR/MDR Architecture section for details.
- **Orbital:** Activate Orbital to enable Real Time investigation on the endpoint. Orbital is not available with the standard license. At least Secure Endpoint Advantage license is needed for Orbital.
- **Engine Settings:** Advanced Engine Settings: Under Engines → Common Engine Settings activate Enable Event Tracing for Windows. This enables Windows Event Log information for the Behavioral Protection Engine. This feature may conflict with existing Microsoft Group Policy Settings. Review the info field when enabling this feature and talk to responsible workplace/endpoint designers before activating this feature.
- **Identity Persistence:** This feature is not available per default and must be activated by TAC. If Secure Endpoint is not installed on frequent re-installed endpoints, the feature is not necessary.
- Review the Policy settings: Best Performance and Security section for all other detailed settings.

Policy settings: Server

Generate a new default policy for Server Systems:

- Generate a new policy object under Management → policies by clicking the new policy button.
- Select the Operating System you want to generate the policy for and click new policy.
- Add a meaningful name, optional a description and click the ***Apply Server Settings*** Button on the right. This applies the Cisco recommended settings.
- Install the Secure Endpoint **without** any command line switches (default installation), so all engines get installed.

The generated policy object is a very good starting point:

- Files: Quarantine
- Network: Disabled
- Malicious Activity Protection: Disabled
- System Process Protection: Disabled
- Script Protection: Quarantine
- Exploit Prevention: Audit
- Exploit Prevention - Script Control: Audit
- Behavioral Protection: Protect

Policy adoptions checklist:

- **Exclusions:** Add additional exclusions only if really needed to provide the best security. Review the Secure Endpoint Installation, Updates and Operational Lifecycle section how to figure out additional needed exclusions. Review Exclusions best practices for Performance and Security when defining additional exclusions.
- **Lists:** In Secure Endpoint console, under Outbreak control generate a list for custom detections simple, custom detections advanced, application control allowed, application control blocked and Network - IP Block & Allow lists. Assign them to your policy. These lists will also be available in the SecureX Pivot Menu. Review the Policy Design and Management – Performance and Security section for best practice.
- **Network:** On Server OS most time there is much more network load than Workstation OS. Therefore, some considerations should be done when Network protection should be set to enabled.
    - Disabling the feature instead of installing the connector without network drivers should solve most network issues.
    - Network protection may slow down network operations. If the server application needs high network performance or fastest response times, be carefully when enabling the engine. Detailed testing is highly recommended.
    - Specific network configurations like Network Teaming or several configured VLANs on a Server network card must be tested carefully. Cisco recommends disabling network protection in such scenarios.
    - If there are still network issues, Secure Endpoint should be re-installed using the /skipdfc installation switch to prohibit the network driver installation.
- **System Process Protection:** The engine is designed to protect against "Mimikatz" like attacks. If there are Group policy settings like disabling NTLMv1 or other possible NTLM Security settings configured, the Engine can be set to disabled. If the engine should be enabled, Cisco recommends to carefully test and to monitor server performance.
- **Exploit Prevention:** Exploit Prevention Engine triggers under the following conditions.
  - A Process is listed on the protected processes list. Review the Secure Endpoint User Guide for details.
  - Process was launched by another process in the Exploit Prevention protected list.
  - The process was executed from a directory Exploit Prevention is monitoring.

  If Exploit Prevention triggers, the tiny DLL is loaded into the process and changes are done in the memory for this process. Only this process is aware of the updated memory locations. On Server systems, especially on Domain Controllers, a change in the memory may result into unexpected behavior. Cisco recommends to carefully test and to monitor server performance if this engine gets enabled.
- Review the The Policy settings: Best Performance and Security section for all other detailed settings.
- Activate Real Time Search **Orbital** on supported Server OS.
- Activate **Endpoint Isolation** to disconnect possible compromised Servers from the network.

Policy Setup summary

Take a moment to review the summary for the console setup.

- ☐ Cisco highly recommends activating SecureX as one of the first steps. The SecureX - EDR/XDR/MDR Architecture sections show more details about the SecureX Architecture.
- ☐ Enable Two-Factor authentication for the user to be able to see and configure data sensitive settings.
- ☐ Navigate to security.cisco.com and activate the SecureX platform. Review the guides to enable SecureX platform and moving to SecureX SSO.
- ☐ The guidelines here should enable you to define a policy which works without any interruptions on the endpoint

Info: Cisco started a policy redesign project for Secure Endpoint. This will provide significant improvements for the whole policy management. All changes will happen step-by-step to reduce administrative work to a minimum for the whole transition.

Secure Endpoint Installation, Updates and Operational Lifecycle

Secure Endpoint: Software Rollout

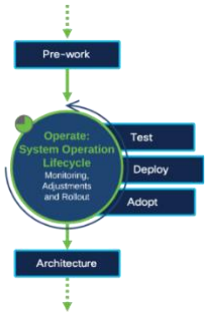
As with any large-scale software deployment, it is always a good practice to deploy in a slow, methodical way. Staged deployments ensure that as we deploy to any environment, if we encounter issues, we are able to resolve them while only impacting a relatively small percentage of endpoints. These concerns are especially relevant with security software, which is why the Cisco Best Practice is to deploy Secure Endpoint using the phased approach. There are some common approaches/examples as outlined in the table.

Planned **Rollout - Scenario 1**	**Planned** **Rollout - Scenario 2**	**Emergency** **Rollout**
Meets the customers deployment strategy	Mostly meets the customers deployment strategy	Outside the Deployment Strategy
Much time for the whole Rollout Project	Limited Time until the Rollout must be finished by a specific date	Emergency, less time, or no time for Project Planning
Testing with the standard Software Images for Endpoints	Testing with the Standard Software Images for Endpoints	Less or no testing
Application Testing and Business critical Systems	Most Application are tested. Some Business-critical Systems are out of scope	Exclude business critical systems (Included in a Worst-Case Scenario)
Rollout: Starting with Standard Image and afterwards deploying sensitive Systems step-by-step. Focus is on a secure Rollout.	**Rollout:** After Testing, the software is rolled out to most of the available systems. Focus is on Rollout End Date and Time.	**Rollout:** Emergency Rollout where the actual Security Solution is not able to protect or missing EDR features during a Security incident. As Fast as possible Rollout is needed.
⌄⌄	⌄⌄	⌄⌄
Each of these deployment scenarios (examples) is possible with Secure Endpoint. For each scenario think about the Best Practices described in the previous chapters.		
Relaxed and Planned Rollout. Lowest risk for any business impact.	Rollout is mostly planned. There can be some noticeable performance impacts. Medium Risk for business impact. Interruptions are part of the whole Deployment strategy.	As fast as possible Rollout. More Security or Visibility is needed. This is a scenario if environment got breached. The Risk of Data loss is much higher than any Risk caused by Software Deployment. This is a common Situation for Cisco Incident Response Services when EPP solutions only are in place at a customer. User interruptions are accepted

Note: These are just a few examples to show the different circumstances for a Security Product Rollout.

Prework - Quick Summary

1. The Secure Endpoint Preparation section outlined much information around the Secure Endpoint architecture, how the connector communicates with the cloud, the fundamental architecture of the connector software and best practices to plan your Secure Endpoint environment. Secure Endpoint fully integrates into the SecureX architecture outlined in the SecureX – EDR/XDR/MDR Architecture section.
2. The Policy Design and Management – Performance and Security section outlined how to enable your Account, how to enable the SecureX platform and useful information to build your Workstation or Server Policy.



Best Practices Secure Endpoint roll-out

The following section should give you some insights and ideas for a successful Secure Endpoint rollout. As already outlined in previous chapters, Cisco recognizes that each customer environment is unique, and this framework should serve as a recommendation only as it may need to be adjusted according to the specifics of the customer use case.

Phase 1: LAB Environment - Testing and Rollout

Step 1: Download the Connector from Secure Endpoint console.
Consider 2 things for Connector downloading:

- If you want to test with a specific Connector version, you have two options:
  - Select the right version under **Accounts → Organization Settings** first (The Default Value is latest which is the latest connector version available).
  - Set the connector version under the policy settings. If product upgrade is not set for a policy, then Organization Setting is used.
- During Download **select the group** the endpoint belongs to. The Group ID is included in the Connector Package. After installation, the Connector will register itself to this specific group.

Best Practice: Set the defined connector version for your environment in the AMP console under **Accounts → Organization Settings**, so everyone is installing the same version. Otherwise generate a download URL under **Management → Download Connector** for any admin which has no access rights to AMP console.

Review the Connector OS Compatibility for Windows, Linux and macOS.

- **Windows**: Document ID:214847
- **Linux:** Document ID:215163
- **MacOS:** Document ID:214849
- Other Secure Endpoint documents on cisco.com website.

Step 2: Install the Connector to the **machines in your LAB**. Start with your standard company image, so you are getting a test result for a high amount of company endpoints. If possible, try to install as much as possible software components.

Testing Procedures:

- If any existing Security Product is to remain, confirm the respective product is functioning as expected
- Login to your endpoint and confirm any login scripts execute
- Open standard applications and confirm applications launch and are functional
- When using a dedicated proxy or transparent proxy, talk to your Proxy Admin
  - If authentication is requested per company policy, use a dedicated user account for AMP for Endpoints proxy authentication. Look into the Secure Endpoint help to see non supported NTLM authentication option
  - The Proxy Admin may exclude Secure Endpoint connections from Proxy Log, especially when they are uploaded to another tool (e.g., splunk), to save Log data and costs.
- Open the Secure Endpoint console to check if the endpoint successfully connects to the AMP cloud and if the right policy as active. Also check the appropriate Events in Secure Endpoint Console
- Identify any issues in functionality or performance. Addressing these issues will be discussed in the Connector Diagnostic section below

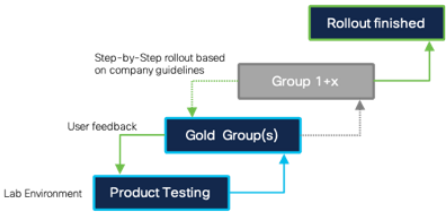
Best Practices: Always test with your existing Deployment Architecture (e.g., Microsoft SCCM, Altiris and others). The Deployment Architecture already provides many Software Packages for testing. During Software Installation and upgrades, there are many files changed on your system by the installer, which will be scanned by Secure Endpoint. Monitor the System Performance during the Software Installation and Upgrade Process. Review the Windows Installer Exit Codes if there is any issue when installing Secure Endpoint.

Software Deployment Agents should be excluded from scanning by process. In secure areas also add the SHA-256 hash to the exclusion.

Phase 2: Gold user Group

Step 3: Define the Gold User Group to test with business-critical applications. There can be situations, where specific application features are generating new files on the disk. Application testing cannot be done by IT.

- Gold Users are testing specific application features and performance.
- Make it easy for gold users to provide feedback.
- Think about a fast solution for the user, e.g., moving the Connector to a group where the Connector is set to Monitoring Mode.



Helpdesk: Instruct the Helpdesk about the software tests with Gold Users. It is always a good choice to involve the Helpdesk in software tests. Add Helpdesk users to the Gold Group as well.

IT department: Members of the IT department may be added to the Gold Group test, as they tend to have greater technical knowledge and can give qualified feedback.

System Owners: Think about the System owners of specific endpoints. Talk to them, inform them and involve them in the system change. Show them how to handle the product, and in a worst case, how they can disable AMP. Define a strategy how the endpoints should be upgraded, when this is possible and how needed exclusions are configured as fast as possible.

Best Practice: Critical Software should be tested by the appropriate User. There can be situations, where a specific feature inside a software product needs a special configuration. Just starting a critical software may not show necessary product adjustments.

Phase 3: Deployment Preparation

Step 4: Generate the deployment packages for the Deployment. Cisco recommends using an existing Deployment Architecture e.g., Microsoft SCCM, Altiris, or others.

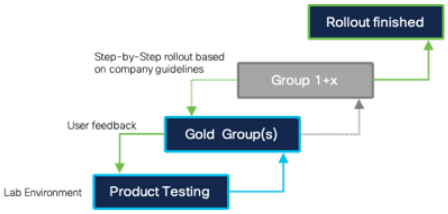
- Define the deployment packages as needed.
- Define Removal Package.
- Test Deployment and Removal.

Best Practice: Review available installer command line switches for the Secure Endpoint connector: http://cs.co/AMP4E_Connector_Install_Switches

Phase 4: Rollout

Step 5: Start the rollout in your Environment based on your internal guidelines, policies and the defined Step-by-Step rollout. Add new exclusions as needed during the Rollout Phase.

- Business Critical System: You may start in Audit mode when deploying Secure Endpoint to Business-Critical Systems.



Best Practice: There can always be an issue when installing new software to endpoints, regardless of if you are installing Secure Endpoint or any other software package. In a Worst-Case-Scenario a stepwise rollout helps you to lower the impact on your infrastructure.

Secure Endpoint: Operational Lifecycle

This section provides strategies to optimize features or functionality in AMP for Endpoints. As new options, features and security fixes are released, it is recommended that a review is conducted of new connector versions to upgrade the endpoints for improved protection.

Testing the installation

- Search the computer name in the Secure Endpoint console if it has registered successfully.

New Engines and Features

With new features released in Secure Endpoint, these features can include new engines or optional configuration settings for existing engines. While testing new releases, it is recommended to enable new features that might not exist in existing products or review the functionality provided in Secure Endpoint. When trying out new features, it can be helpful to enable an audit setting initially. Policy changes can be made, tested, and rolled out without any disruption to the endpoint.

Best Practice: If Secure Endpoint causes high CPU load, a very easy and fast way is to disable Engines step-by-step to identify the engine causing the high load. A specific Secure Endpoint group can be created to allow the engine to be disabled for the impacted endpoints.

Custom Exclusions

Either review of logging from Secure Endpoint or other performance tools can be used to identify custom exclusions.

The steps to identify exclusions from the **Secure Endpoint Diagnostics Package** takes the following steps. The Diagnostic package can be generated directly on the endpoint using the command line, or from the computer properties in the Secure Endpoint console.

Command Line (Windows):

- Start the debug logging on the endpoint. Debug logging can be activated directly on the Endpoint UI (Windows) or in the policy under **Advanced Settings → Administrative Features → Connector Log Level**.
- Start the **ipsupporttool.exe** on the endpoint with the right command line parameter. Use the right time value, so you can replicate the issue. Details using the tool can be found in the Secure Endpoint Troubleshooting Technotes.
- The default location to store the output file is the user desktop.

Secure Endpoint console:

- Navigate to the computer properties under Management → Computers
- Click the Diagnostic Diagnose Button.
- In the Popup window select the length of the Debug Session and click the Create Button.
- Open the Secure Endpoint Tray to pull a new policy. Debug logging will be automatically enabled on the endpoint.
- Replicate the issue on the endpoint.
- Download the Diagnostic package under **Analysis → File Repository**.

Analyze the Diagnostic Package(s)

- Download the Performance Tuning tool from http://cs.co/AMP4E_Tuning_Tool.
- Copy the Diagnostic Package(s) and the Tuning Tool into the same directory.
- Execute the Tuning Tool and review the result

Best Practice: Review the Tuning Tool result and add new exclusions based on the guidelines from the previous chapters. If necessary, repeat the steps to figure out additional needed exclusions.

ƒ

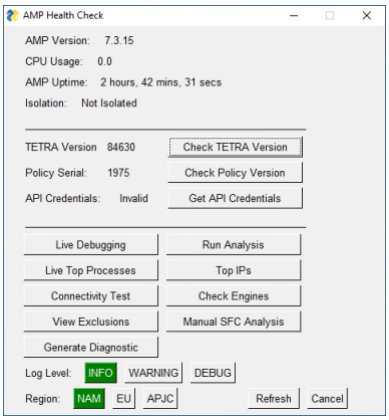
Secure Endpoint: Troubleshooting

The Secure Endpoint Deployment Strategy Guide already includes useful information for troubleshooting This includes:

- Performance
- Outlook performance
- Cloud connectivity
- Missing information in Device Trajectory
- Missing network events in Device Trajectory
- Policy not updating
- Proxy
- Duplicate Connectors
- Simple Custom Detections
- Application Blocking

Health checker Tool

The tool provides a set of tools to investigate issues on the endpoint. It can be downloaded from https://github.com/CiscoSecurity/amp-05-health-checker-windows. The Live Debugging option can also be used to determine necessary scan exclusions.

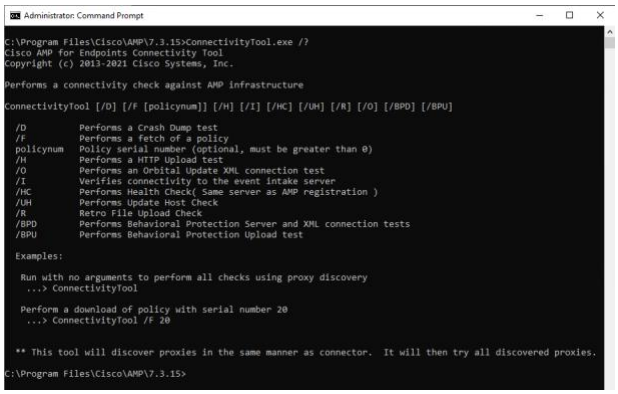


Connectivity Tool

The tool provides several connection tests including policy pull, event upload, orbital update check and checks for Behavioral Protection Engine.
To show all possible options

1. open a command prompt (cmd) window
2. navigate to the Connector installation directory
3. type ConnectivityTool.exe /? and press enter

Review the help output for available options.



Analyze AMP Diagnostic Bundle for High CPU on Windows and macOS

Find a detailed description how to troubleshoot High CPU condition on the cisco.com website:

- Windows: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215261-analyze-amp-diagnostic-bundle-for-high-c.html
- macOS: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215570-analize-macos-amp-diagnostic-bundle-for.html

Processes secured by Exploit Prevention

In rare cases applications show unexpected behavior if Exploit prevention injected the tiny DLL for the memory changes. To list all running processes where Exploit Prevention tiny DLLs has been injected, you can use Orbital to query the endpoint.

- Open the Orbital console and start a new query
- Select the host you want to query using **host:hostname** as the search target
- Copy the following Custom SQL and click the Live Query button

```
select DISTINCT p.pid, p.name AS "Process Name",
p.path AS "Process Path",
pm.path AS "DLL-Loaded-path",
sha256,
a.issuer_name AS "DLL-Cert-Issuer_Name",
a.subject_name AS "DLL-Cert-Subject_Name",
a.result
from processes p
LEFT JOIN process_memory_map pm ON p.pid=pm.pid
LEFT JOIN authenticode a ON pm.path = a.path
LEFT JOIN hash h ON pm.path = h.path
WHERE pm.path != ""
AND pm.path NOT LIKE "%windows\system32%"
AND pm.path LIKE "%.dll"
AND pm.path LIKE "%Protector64.dll%"
ORDER BY p.pid;
```

SecureX – EDR/XDR/MDR Architecture

Secure Endpoint fully integrates into the SecureX platform. SecureX enhances the endpoint product with sophisticated hunting tools and security automation. The architecture provides features listed in the Cloud infrastructure - Features and Services section of this document. Cisco highly recommends enabling SecureX as one of the first tasks. Follow the steps outlined in the SecureX Opt-In guide to activate the SecureX platform and SecureX SSO. Review the Cisco SecureX Sign-On Quick Start Guide showing how SecureX SSO works.

Review additional sources for SecureX

- SecureX Documentation: http://cs.co/SXO_docs
- SecureX FAQs: http://cs.co/SecureX_faq
- SecureX Youtube Playlist: http://cs.co/SecureX_videos
- SecureX Orchestration Workflows: http://cs.co/SXO_repo

Best Practice: Think about how the SecureX architecture enhances your security and simplifies security investigations. SecureX and all features provided by SecureX are available with any Secure Endpoint license.

Secure Endpoint: automated actions

Secure Endpoint provides 4 different types of automated actions. Any feature is described in detail in the Secure Endpoint product guide. The automated actions are

- Take a Forensic Snapshot upon compromise
- Isolate a Computer upon Compromise
- Submit to Threat Grid upon Detection
- Move Computer to Group upon Compromise

Automated Post Infection: Move Computer to Group

Move computer to group needs some preparation. As this is a post infection task, there should be policy defined, which provides the highest detection/protection capabilities.

- Enable all Engines and set them to Protect/Quarantine. Review the Policy settings: Best Performance and Security section for additional info
- Reduce the cache setting to the lowest setting
- Remove as much as possible exclusions
- Activate On-Demand Scanning in the policy

Best Practice: Prepare the right policy for the group systems will be sorted to.

Automated Post Infection: Isolate the endpoint from the network

Isolate the computer from the network: Secure Endpoint communication is excluded in the product, and is always functioning, even the endpoint gets isolated. Before activating this feature, think about which communication should still be possible, e.g., communication to central systems for logging or remote access.

Best Practice: Define Isolation IP-Allow lists to provide necessary communication for endpoints before activating the feature.

Secure Endpoint: File Analysis

Secure Endpoint backend does not request files automatically. Prevalence must be enabled in Secure Endpoint under **Analysis -> Prevalence -> Configure Automatic Analysis**.

SecureX: Integration Modules

Cisco provides out-of-the-box integrations into Cisco and 3rd Party products. These integrations greatly enhance the hunting experience.

- Configure integration modules for available Cisco products. Review SecureX supported products.
- Configure 3rd party Integrations using Cisco hosted modules. These modules automatically provide data translation between Cisco and 3rd party vendors.

Best Practice: During an investigation all configured modules are queried for information. Cisco highly recommends configuring all available integration modules.

SecureX: Pivot Menu

The Pivot Menu is a security tool, powered by SecureX, that is available in the UIs of many Cisco Security products (with more to come!) The Pivot Menu provides a very sophisticated and easy way to get immediate, cross-product reputation information on observables, and take common research and response actions on them across your installed products.

SecureX: Threat Response

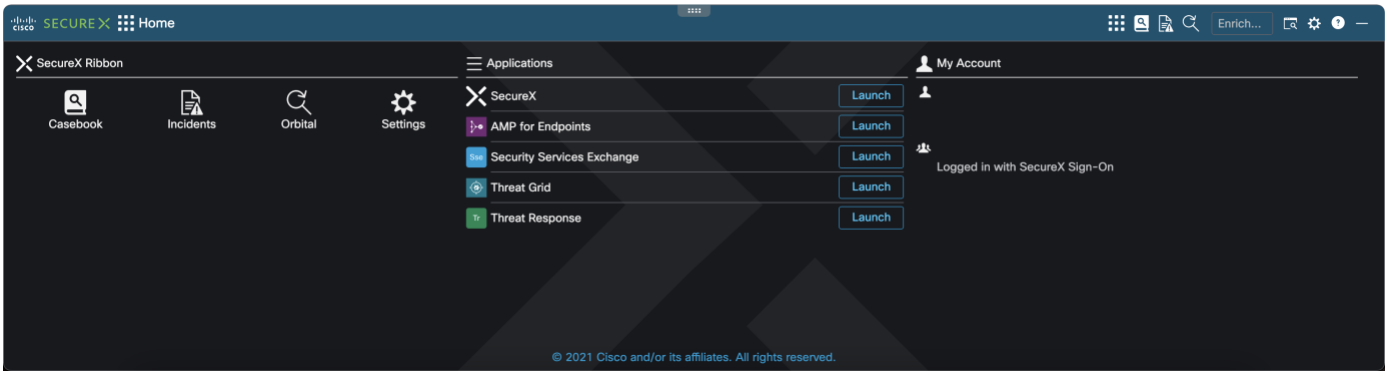
SecureX Threat Response enables an investigation from many areas of the SecureX integrated products. Any time a UI shows observables with type hash, IP, domain and more enables a direct investigation with SecureX threat response.

Best Practice: SecureX threat response simplifies threat investigation and should be enabled in any way.

SecureX: Ribbon

Cisco SecureX is both a centralized console and a distributed set of capabilities that unify visibility, enable automation, accelerate incident response workflows, and improve threat hunting. These distributed capabilities are presented in the form of applications (apps) and tools in the SecureX ribbon. Review SecureX Ribbon details in the SecureX help

- SecureX Ribbon - Introduction
- SecureX Ribbon – Casebook app
- SecureX Ribbon - Incident app
- SecureX Ribbon - Orbital app



Appendix-A: Secure Endpoint Private Cloud

The major differences between the two are:

Infrastructure	Pro	Con
Public Cloud	• Endpoint features are deployed here first • Roaming endpoints can remain connected to the cloud	• Internal network needs allowances to Public Cloud servers
Private Cloud	• Better data privacy for the endpoint with cloud servers on premises • Dedicated resources are used to service endpoints	• Hardware limits the number of active endpoints supported

Consideration: Public Cloud vs. Private Cloud Appliance

Secure Endpoint provides two options for deployment: **Public Cloud** and **Private Cloud Appliance**. It is important to understand the differences between the two options to ensure that you choose the best fit for your organization.

Public Cloud:

- Secure Endpoint Public Cloud (cloud native approach) is the most common option chosen by customers. This method of deployment ensures that new features are immediately available while requiring no server resources to manage endpoint deployments. As such, this method is more flexible and recommended by Cisco.

Private Cloud Appliance:

- The Secure Endpoint Private Cloud Appliance is hosted in your environment. This deployment option provides more privacy for your organization by keeping all endpoint telemetry data under your direct control.
- The Secure Endpoint Private Cloud Appliance comes in two forms, a virtual appliance and a physical UCS appliance. Each option has its own set of requirements which should be carefully evaluated before purchasing decisions are made.
- Both versions of Secure Endpoint Private Cloud appliance offer two primary modes of operation:
    a. **Proxy Mode:** Connection to cloud using the companies web proxy.
    b. **Air-Gap Mode:** No connection to cloud in any way.
- Most Secure Endpoint Private Cloud customers run their appliance in Proxy Mode, as this is the recommended configuration for Private Cloud deployments.
- Air-Gap Mode is deprecated for virtual Private Cloud deployments, however still available for customers deploying a physical UCS HW and provided for customers with extreme privacy requirements or for customers who are unable to have external network connectivity.

Review the Secure Endpoint Private Cloud Documentation on the cisco.com website: https://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/series.html#~tab-documents

Details: Public Cloud vs. Private Cloud

The table shows some main differentiators between Secure Endpoint Public Cloud and Secure Endpoint Private Cloud Appliance.

Feature	Public Cloud	Private Cloud	Info
Deployment			
Location	Regional Cloud DC	Virtual Appliance or Hardware Appliance	Deployment Strategy Guide
Privacy	Managed Cloud Service	Proxy Mode or Air-gaped Mode	Cisco Trust Portal
Sizing	Managed Cloud Service	100.000 endpoints supported on HW appliance	Virtual Appliance Sizing
High Availability	Managed Cloud Service	Cold Standby	
Reliability	Managed Cloud Service	Backup / Restore Procedure	
MSSP Portal	Available	n.a.	
Policy and Features			
Connector Policy	Latest available features	Yes	
Endpoint Engines	Latest available features	Yes	
OS Support	Win/Linux/macOS/iOS/Android	Win/Linux/macOS/iOS/	See release notes
Identity Persistence	Yes	Yes	
Endpoint isolation	Yes	Yes	
Automated actions	Yes	Yes	
→ move to group	Yes	Yes	
→ Isolate endpoint	Yes	Yes	
→ Submit file for analysis	Yes	Yes	
→ Forensic Snapshot	Yes	No	Orbital needed *1
Integrations into SecureX and Hunting Services			
SecureX	Yes	No	
Cognitive Analytics	Yes	No	
Threat Response	Yes	No	
Advanced Search (Orbital)	yes	No	
Secure Malware Analytics			
Cloud	Yes	No	
On-Premises Appliance	No	Yes	

*1: Forensic Snapshot depends on Orbital Cloud Service which is not available for On-premises deployment.

Appendix-B: Virtual Environments (VDI)

Introduction - VDI and Multi-User Environments

Virtual Desktop Infrastructure (VDI) and Multi-User Environments like Terminal Servers, Hyper-V, VMware and others need some granular planning, so Secure Endpoint can be installed without interruption or performance degrade of the virtualization platform. There are so many different virtualization options available on the market, so we cannot list them all here. The following section may give you a short insight into virtualization environments and why adding Endpoint must be planned carefully.

Note: Review the best practices guides provided by Virtualization vendors like Microsoft, VMware, Citrix, Open Stack and others.

Best Practice: Virtual Environments OS Support
Secure Endpoint is VDI vendor agnostic if the Virtual Desktop operating system is supported. Virtual Environments need some special configuration so Secure Endpoint is working without interruptions to the VDI environment.

Endpoint virtualization vs. application virtualization

- **Endpoint: Virtualization:** The Virtualization platform provides a **complete virtual desktop** for a user. The benefit for an IT department is, that any desktop can be easily rebuilt. With a few steps an admin can re-deploy a whole virtual endpoint from a **golden image**.

  The virtualization platform is often a part of the **deployment strategy** at a customer. If there is a new application needed, a new golden image with a new version number is created. IT department can test the new image, especially if there is any bad impact based on the recent changes. After testing, a rollout is started to re-deploy all end-user virtual systems. It there are any issues, the IT department can switch back to the previous image.

  To prevent the loss of the user **settings**, stored in the **user profile**, and to provide all the settings regardless of where the user does a logon, features like **roaming user profiles** are used. These profiles include data like application settings, Browser favorites and cache, the desktop icons and much more. During Logon, the profile is copied from a network share to the local machine. During user logoff, the profile is copied back to the network share. The challenge with user profiles is the **high number of files** stored in the user directory. In many cases **SMB protocol** is used to access the network share where the roaming profile is stored.

  End-users can access the virtual desktop using a proper configured Windows 10 endpoint (just used as the access device) without local installed applications. Another option is using a small Terminal, which is booting a small Linux image including a client to access the virtual desktop.

  Summary: For the end-user it looks like e.g., a typical Windows 10 endpoint, but the backend architecture is completely different than a physical desktop or notebook.

- **Application Virtualization:** This approach is divergent to Endpoint Virtualization because the application only is "virtual". This means, the application is not installed on the user endpoint, it is "streamed" from the virtualization platform
  As an example:
  1. The user starts an application from the icon on the desktop.
  2. In the virtualization backend, the user is logged on to another host. This can be e.g., a Windows Terminal server. This is completely transparent for the end-user starting the application.
  3. After logon in the backend, the application is started and is streamed to the user desktop.

- **Commonalities between both approaches:** There are many different approaches available today. Just high-lighting two examples. Both scenarios are using a **Storage System** in the backend. Where during user Logon **SMB protocol** may be used, a common approach to connect Storage to a Virtualization host is **iSCSI**.
  In any case, there is some **Network layer communication**. The **average access time** from a local disk and a network layer is quite different. Virtualization environments and Storage systems are providing different features to reduce problems with access time.
  Finally, in such a scenario, the **goal of a proper AMP configuration**, is to avoid degrading the performance by scanning specific files.

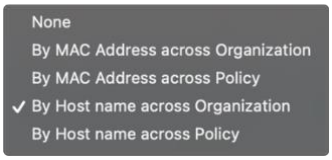
Recommended guidance is to meet with the responsible IT-admins at a customer site to obtain a thorough understanding of their virtualization environment before attempting the deployment. Note: It´s common that different teams at the Customer site handle the Virtual environment vs the team that Administrate the Cisco Secure Endpoint solution.

Secure Endpoint installed in VDI and Multiuser Environments

Today there are no known incompatibilities between Secure Endpoints and Virtualization products. As long the OS is supported, Secure Endpoint can be installed. For proper functionality Endpoint provides several features and options. The next section shows possible options, starting with the backend preparation.

Identity persistence

There is often the case where systems are frequently re-deployed for VDI, or IT-support is re-installing endpoints. In both cases the system name may not be changed and the Secure Endpoint connector GUID in the registry is generated new. Based on this new Connector GUID the Endpoint backend will generate a new Computer Object. This issue can be solved by activating the Identity persistence feature in Endpoint Backend. The feature must be **enabled by TAC**. After the feature is enabled, a new option is available in your **Endpoint policy**.



Deployment of Cisco Secure Endpoint with Identity Persistence:
https://www.cisco.com/c/en/us/support/docs/security/advanced-malware-protection-endpoints/200318-Deployment-of-Cisco-AMP-for-Endpoints-wi.html

Identity persistence configuration

- Go to Management → Policies and select the appropriate policy.
- In your policy navigate to Advanced Settings → Identity Persistence to configure the proper settings

DO NOT activate the feature if not needed.

Best Practice: Always take care when moving endpoints between groups where Identity Persistence is enabled in one group and disabled in the other group. This may result in duplicate computer accounts.
When using Automated Actions, where an Endpoint is automatically moved to different group, or Endpoints are frequently reinstalled, it is highly advised to enable **Identity Persistence in all groups**.

Best Practice: Identity Persistence is not related to VDI only, it is most time used when Secure Endpoint is installed on virtual systems. Frequently re-imaging of endpoints commonly happens in VDI environments. This feature can be used at any time, where systems are frequently re-deployed. Take a few moments to think about what the better approach is for your environment, identifying systems by MAC Address or Hostname.

Golden Image and Endpoint cloning

- If there is a need to create a golden image use the **/goldenimage** command line switch for connector installation. Find details here: https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214462-how-to-prepare-a-golden-image-with-amp-f.html
- To clone a system where Secure Endpoint is already installed, the needed steps are different and described here: https://www.cisco.com/c/en/us/support/docs/security/advanced-malware-protection-endpoints/118749-technote-fireamp-00.html

Note: Secure Endpoint does an incremental signature update for 30 signatures. Afterwards the whole signature set is downloaded. A golden image is often used for a longer period, which exceeds the incremental update limit. In this case, at any time, a new VDI system gets deployed from that golden image, Secure Endpoint will download the whole signature set. For such scenarios a Tetra Update Server should be in place, to speed up the update process and to safe bandwidth consumption to the cloud.

Endpoint Tray Icon

The Secure Endpoints process sfc.exe allows a single Tray Icon connection. In a Multi-User Environment, e.g., Terminal Servers, disable the Tray Icon completely in the policy. If not, the Tray Icon will show wrong information, as the sfc.exe process cannot connect to the tray icon process.

Best Practices: In any environment where multiple User are logging into a system, e.g., Terminal server, the Tray Icon should be disabled by policy.

Exclusion and Feature deactivation

Exclude specific types of applications as listed below. As explained in the previous chapter, exclude any process with high disk activity to prevent any degrade of performance on the backend storage system. In addition, turn off Secure Endpoint features generating high disk activity as listed below.

- Startup intensive applications must be excluded.
- Profiling/Inventory tools must be whitelisted.
- No OnDemand Scans / disable flash scan on install.
- No Endpoint IOC Scans.
- Exclude all processes which are provided by the Virtualization Vendor. E.g., all Citrix processes for Application Virtualization.

Tetra Engine: Cisco recommends not to use Tetra AV in virtual environments by installing Secure Endpoint using the command line argument **/skiptetra 1**. If there is a need for AV Scanning, install Tetra Step-by-Step on systems. Monitor system and storage performance before installing on additional endpoints.

Network (DFC): Systems providing Virtualization in any way are needing high network bandwidth. Install Secure Endpoint without Network DFC using the **/skipdfc 1** command line.

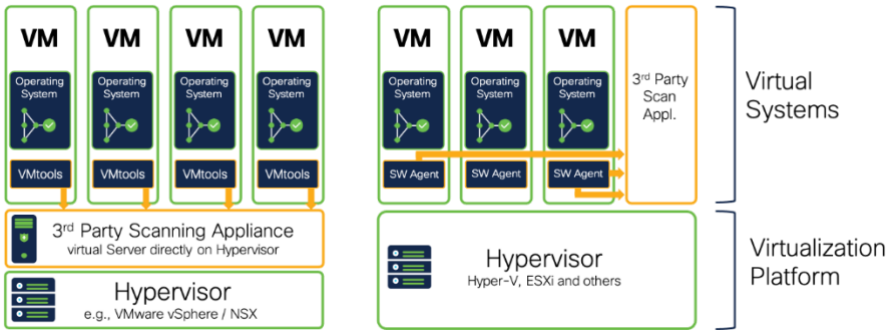
Boot storm - Note: When installing Tetra AV on a Multiuser Environment, think about the Boot storm when endpoints are started, and the users are logging in.

Best Practice: Disk Performance and Secure Endpoint Features
→ **Best Practice - Performance:** Avoid any configuration which generates high disk activity caused by scanning many files.
→ **Best Practice - Network Performance and stability:** Install the Secure Endpoint connector without the network drivers.

Native Hypervisor Integrations and Secure Endpoint

Native Virtualization Integration: Secure Endpoint can be installed in a virtual environment, as long the Guest OS is supported by Secure Endpoint. There are three common integrations/approaches to scan files in virtual environments. Each system provides advantages/disadvantages, based on the point of view.

- **Option:** Scanning directly on Hypervisor level (e.g., VMware NSX).
- **Option:** Virtual Scanning Appliance, scan process is moved to a scanning appliance by an agent inside the VM.
- **Option:** Endpoint Security running directly in the VM.



For many customers resource consumption for File Scanning is an important factor for implementation. In many cases, the goal is to move the scan process to a dedicated appliance. Such approach is for scanning only, but based on this design, EDR features, or behavior-based engines are missing. Therefore, many vendors, once again, are installing a software agent into the virtual machine.

Note: Secure Endpoint is always installed inside the virtual machine. Today Cisco does not provide file scanning directly on the Hypervisor level.

The tables below show some key differentiations between the virtualization scenarios. Cisco is not aware about the latest product changes/approaches of competitor products and features. The table should help you to understand key features. Always investigate latest product documentation and plan carefully with the customers IT Team. In addition, the following tables do not include Hybrid solutions where a Service Appliance and an additional endpoint is in place. It should give you a basic understanding about the differences of each approach.

	Hypervisor Level Scanning	Service Appliance Scanning	Scanning inside the VM	Info
Deployment				
Secure Endpoint Placement	no	no	yes	
Endpoint Software	VMware Tools	Software Agent	Secure Endpoint	
Scan Appliance Inst. Count	1x per Hypervisor	1x per x endpoints	n.a.	
Scan Engine Location	Hypervisor (VM)	Service Appliance (VM)	Inside VM	
Scan Count per file (worst-case)	once per hypervisor	once per appliance	once per host	← Scanning the same file multiple times can cause high load and latencies on Storage Systems
Communication to Scan Service	IP based	IP based	Drivers inside VM	Communication between the VM and the Scan Service
High availability	No	Yes	n.a.	
Impact on Outage	All VMs on Hypervisor	All VMs connected to Appliance	Single VM	
Resource consumption	100 – 200B per Hypervisor	100-200MB per x endpoints	100MB per endpoint	Resource saving depends on the Architecture, e.g., how many endpoints are hosted by one Hypervisor. Effectiveness of resource savings is often important for customers. The resource consumption has an impact on the VM density per Hardware.
Example 1000 VMs (RAM consumption)	1-2 GB RAM (100VMs per hypervisor)	100-200 MB for appliance. 1GB (10 MB per endpoint)	10 GB (100MB per VM)	RAM consumption for File Scanning Resources over virtual infrastructure

	Hypervisor Level Scanning (EDR)	Service Appliance Scanning (EDR)	Scanning inside the VM (EDR)	Info
Protection and EDR				
File Scanning	Yes	Yes	Yes	
Process Information	No	Partial	Yes	
OnDemand Scan	No	No	Yes	
Machine Learning	No	No	Yes	
Behavior Engines	No	No	Yes	Needs endpoint behavior details
Post infection tasks	No	No	Yes	
High availability	No	Yes	n.a.	
Real Time Forensic	No	No	Yes	
Resource consumption	100 – 200B per Hypervisor	100-200MB per x endpoints	100MB per endpoint	Resource saving depends on the Architecture, e.g., how many endpoints are hosted by one Hypervisor. Effectiveness of resource savings is often important for customers. The resource consumption has an impact on the VM density per Hardware.
Example 1000 VMs (RAM consumption)	1-2 GB RAM (100VMs per hypervisor)	100-200 MB for appliance. 1GB (10 MB per endpoint)	10 GB (100MB per VM)	RAM consumption for File Scanning Resources over virtual infrastructure

Summary: Various Integrations into virtualization environments are useful for resource savings for RAM and CPU by moving Scanning Resources to a dedicated system. Without an additional endpoint component, such solutions are missing endpoint protection and EDR functionality and do not provide post infection task like
- isolating the endpoint from the network
- generating forensic snapshot
- advanced file analysis triggered by endpoint behavior

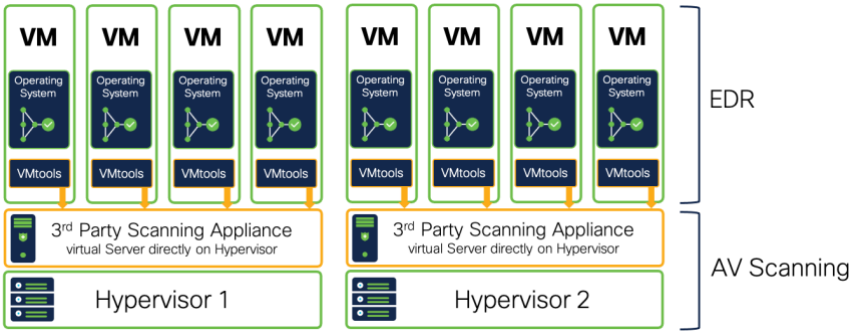
Best Practice: If a product for Agentless Scanning is already in place, you may install the Secure Endpoint connector without Tetra Engine using the /skiptetra 1 installation switch. Second option is using a policy where Tetra is disabled, so you can enable AV scanning in Secure Endpoint without re-installing the product.

Integration: Scanning per Hypervisor (e.g., VMware)

Description: A 3rd Party Scanning appliance is installed on the Hypervisor. This Appliance is responsible for AV Scanning only.

AV Scanning done by Hypervisor insights:

- No Process information available for the Scanning Appliance.
- OnDemand Scans are not possible.
- Path Exclusions only are available, no process exclusions possible.
- Automated Deployment of a Scanning Appliance possible (vendor dependent)
- VMware Tools must be installed.
- Additional Software Component inside VM needed providing protection beyond AV scanning and EDR.



Secure Endpoint Deployment:

- Install Secure Endpoint s without Tetra with the /skiptetra 1 installation switch.
  - (Duplicate Scanning possible, but needs more system Resources, not recommended)
- All other engines can be installed based on the guidelines in the previous sections.

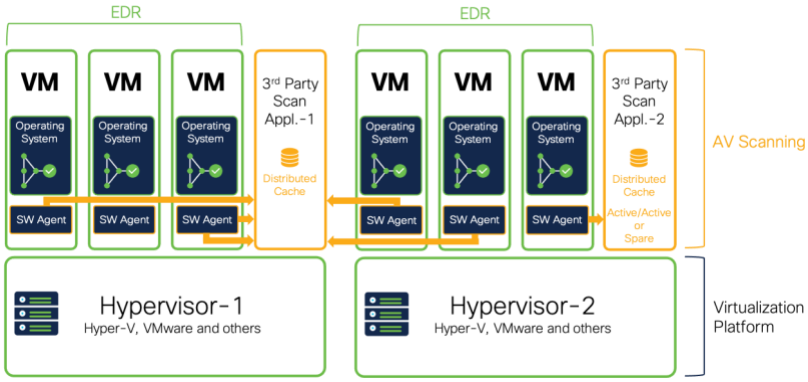
Info: VMware acquired Carbon Black and Lastline. New features provided by the acquisitions are not part of this document.

Integration: Scanning with dedicated Scanning Node (e.g., Hyper-V, Citrix, OpenStack)

Description: A dedicated Scanning Appliance is used to scan Content for virtual systems across multiple Hypervisors. One appliance can also be used serving the scanning service for virtual endpoints hosted on different Hypervisors and versions.

AV scanning done by dedicated Appliance.

- Can handle many endpoints across Hypervisor Platforms
- Distributed Cache (Vendor dependent)
- SW-Agent in VM sends file for scanning.
- Exclusions possible based on Process (vendor dependent)
- No OnDemand Scans



Secure Endpoints Deployment:

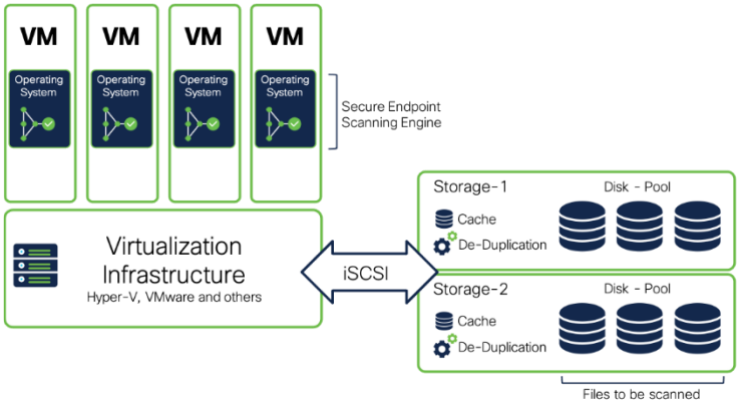
- Install Secure Endpoint without Tetra with the /skiptetra 1 installation switch.
  - (duplicate Scanning possible, but needs more system Resources, not recommended)
- All other engines can be installed based on the guidelines in the previous sections.
- Configure Exclusions for the SW Agents, which forwards files to the Scanning Appliance.

OnDemand/IOC Scanning in virtual Environments

The drawing shows an easy example of a virtual environment. One or more storage systems are connected to the Hypervisor using iSCSI. Several virtual systems are hosted by the Hypervisor.

- Secure Endpoint is running in the memory of the virtual machine.
- The Operating System files are located on the storage system.

To scan a file, it must be fully copied from the storage system to the virtual machine. If the same file is available on multiple virtual systems, the file must be copied several times.



Best Practice: OnDemand Scan: Avoid OnDemand Scanning (File Scanning and IOC Scanning) in virtual environments. If a customer requests OD-Scans as part of the Security Guidelines, separate the endpoints in different groups, so not all endpoints start the scan at the same time.

Recommended Settings for Microsoft Windows Terminal Server

Microsoft Terminal Server have some special characteristics and therefore a proper Secure Endpoint configuration is important.

Characteristics:

- Multiple user sessions at once.
- Roaming Profiles are often used and stored on a remote network drive. This results into high network bandwidth usage during user logon and logoff. Roaming profiles include thousands of files, which are copied to the local drive.
- Login/Logout storms are generating high load on the Terminal Server system.
- A lot of running Applications in the memory.
- High disk activity generated by the running applications.

Recommended Settings

- Define an own Group and Policy Template for Terminal Servers.
- Assign the Cisco Maintained Exclusion List for Microsoft Windows.
- Exclude Processes which are related to the virtualization system. Review the recommended Terminal Server AV exclusions from Microsoft website: https://social.technet.microsoft.com/wiki/contents/articles/18439.terminal-server-antivirus-exclusions.aspx
- Disable the Tray icon for Secure Endpoint in the policy as outlined above.
- Disable the Network Protection in the Policy. If there are still issues with the network performance, re-install the endpoint using the **/skipdfc** install switch. Review the Deployment Guide for details, outlines in the Secure Endpoint Preparation and operational Lifecycle section of this guide.
- Malicious Activity Protection Engine and Exploit-Protection Engine must be tested carefully, as changes to the memory may generate issues in a Terminal Server environment. Start in Audit Mode and switch to protection mode Step-by-Step.
- Do not use On-Demand Scans for Terminal Servers to avoid disk performance issues. If required by the customer, do the OnDemand scan during times where no users are logged on to the Terminal server. Use different smaller OnDemand scans, where parts of the disk are scanned, to speed up the scanning process.

Recommended Settings for Microsoft Hyper-V

Microsoft Hyper-V provides virtualization of other Operating Systems. Secure Endpoint is VDI vendor agnostic if the Virtual Desktop operating system is supported. For performance reason the Hyper-V Platform has no Endpoint Security installed, as the virtual VMs are already protected. In cases where protecting the Hypervisor platform is a customer requirement, Secure Endpoint needs a proper configuration.

Building a policy for Microsoft Hyper-V.

- Define an own Group and Policy Template for Microsoft Hyper-V systems.
- Assign the Cisco Maintained Exclusion List for Microsoft Windows.
- Add additional necessary exclusions recommended by Microsoft: https://docs.microsoft.com/en-us/troubleshoot/windows-server/virtualization/antivirus-exclusions-for-hyper-v-hosts
- If the Hypervisor is clustered, add Microsoft Cluster Exclusions based on the Microsoft recommendations: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-exclusions-microsoft-defender-antivirus?view=o365-worldwide
  - If there is a quorum disk configured, the whole path must be excluded from scanning. Review Microsoft Information for quorum disk: https://docs.microsoft.com/en-us/windows-server/failover-clustering/manage-cluster-quorum
- **Disable** Exploit Prevention and Malicious Activity Protection in the Policy.
- **Disable/Remove** any OnDemand Scan on the Hyper-V System.
- Network Performance is essential for a Hyper-V system. Install Secure Endpoint using the **/skipdfc** installation switch to stop the Secure Endpoint network driver installation.
  - **Disable** Secure Endpoint product update in the policy. If the connector is updated using the internal feature, the standard installation command line is used.

Best Practice: Always test carefully when installing Secure Endpoint on a Microsoft Hypervisor System. Do not install on a system with running VMs.

Threat Hunt with SecureX: If the customer is using Microsoft Defender on the Virtualization platform you may activate the SecureX Microsoft Graph Security API module. This allows the customer to display Microsoft Security Information during a Threat Hunt in SecureX threat response. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWm9G4.

Virtual Systems in public cloud environments

Secure Endpoint can be installed on any virtualization platform if the OS in the virtual workload is supported. In public cloud environments like Amazon Web Services (AWS) and others, performance generates costs. A proper Secure Endpoint configuration helps to save costs-

- Review if the virtual OS in the public cloud environment is supported by Secure Endpoint. Review the Supported Operating Systems section of this document. Review the official supported OS information from the cisco.com website.
- Review the Policy Design and Management – Performance and Security section to build a Secure Endpoint policy with a low resource impact on the
- Activate On-Demand scanning **only** if necessary or if you are expecting a compromise. In such cases you may activate Automated Actions feature to move a computer to the appropriate group, after a Cloud IOC was generated.
  Endpoint IOC scans are very resource and time intensive. Run Endpoint IOC scans only if needed.
- In cloud where system resources generate costs, check system performance in regular intervals. Review the Secure Endpoint: Troubleshooting section to figure out high CPU problems.

VDI Checklist/Summary

Take a moment to review the summary to install Secure Endpoint in a VDI environment.

- ☐ Open a TAC case to enable Identity persistence.
- ☐ Verify the type of the virtualization platform.
- ☐ Use the **/goldenimage** command line switch to generate a golden image. Take care, that the image does not connect to Secure Endpoint backend before freezing.
- ☐ Incremental Updates are available for a max. count of 30 Signature updates, afterwards the whole Signature package will be downloaded. Deploy an AMP Update Server to store the Signature Files in the local network.
- ☐ The sfc.exe process supports one Tray Icon connection. Disable the Tray Icon in the Policy for Multi-User deployments.
- ☐ If enabling Tetra, be carefully and enable step-by-step to prevent Storage overload. Review the guidelines for Exclusion and Feature deactivation
- ☐ Do not install the network driver on systems with high network load or if many VLANs are configured on the network interface.
- ☐ Secure Endpoint always runs inside the virtual OS.
- ☐ OnDemand Scan can degrade the Storage Performance. Avoid ODScanning/IOC Scans for daily operations.
- ☐ When integrating a VDI environment into an EDR/XDR/MDR architecture, plan, and test carefully.
- ☐ Review the recommendations for specific environments like Microsoft Terminal server, Hyper-V and public cloud infrastructure environments.

Appendix-C: add Tetra manually after /skiptetra was used

As this is a **workaround**, always test in a non-productive environment before doing a global rollout!

Adding Tetra manually to an endpoint

tested with connector version 7.3.15

Perform the following steps to add Tetra again to your endpoint, if the /skiptetra 1 installation switch has been used.

1. Stop the Connector
2. Copy trufos.sys from C:\Program Files\Cisco\AMP\tetra to C:\Windows\System32\drivers
3. Created registry entries at location HKLM\System\ControlSet001\Services\Trufos. See Registry Key values below.
4. Ensure tetra is enabled in the Policy on the portal:
    a. Advanced Settings → TETRA → TETRA checkbox should be checked
    b. Models and Engines → TETRA checkbox should be checked
5. Start the Connector

There is one side effect: - if after performing these steps, in the future if Secure Endpoint is uninstalled, then trufos.sys and registry entries created above will have to be manually removed. If you do not remove the files/registry keys, this does not have any impact on the endpoint.

Batch File to generate Registry Key values

Copy the following text into a .bat file to add all registry key at once.

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v DependOnService /t REG_MULTI_SZ /d FltMgr
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v DisplayName /t REG_SZ /d Trufos
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v ErrorControl /t REG_DWORD /d 1
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Group /t REG_SZ /d "FSFilter Anti-Virus"
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v ImagePath /t REG_EXPAND_SZ /d "\??\C:\WINDOWS\System32\Drivers\trufos.sys"
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Start /t REG_DWORD /d 3
reg add HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Trufos /v Type /t REG_DWORD /d 2
```

Best Practice: if you are using a newer connector version than 7.3.15, always test carefully if there was any change with the registry keys!!

Appendix-D: 3rd Party Integrations with Secure Endpoint

Several 3rd party security companies developed integrations with Secure Endpoint. The latest list can be found at:
https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/AMP-endpoints-partners-integrations.html#~third-party-solutions

List of available integrations:

- Alert Logic
- Arctic Wolf Networks
- Blackpoint
- Cigent D3E
- Empow Cybersecurity
- Exabeam
- Fortinet FortiSOAR
- IBM BigFix
- IBM MaaS360
- IBM QRadar
- IBM Resilient
- Jask (Sumo Logic)
- LogicHub
- LogRhythm
- Palo Alto Networks Cortex XSOAR
- Panaseer
- Perch Security
- RSA NetWitness SIEM
- ServiceNow ITSM
- Siemplify
- Splunk Phantom
- Splunk SIEM
- Swimlane
- Syncurity
- TheHive SOAR

Integrate Secure Endpoint using API Code Examples

The API documentation can be found at: https://developer.cisco.com/amp-for-endpoints/

Cisco Security on GitHub – sample integration code

Sample integration code at: https://github.com/CiscoSecurity?q=amp&type=&language=&sort=

Appendix-E: Exclusions in depth

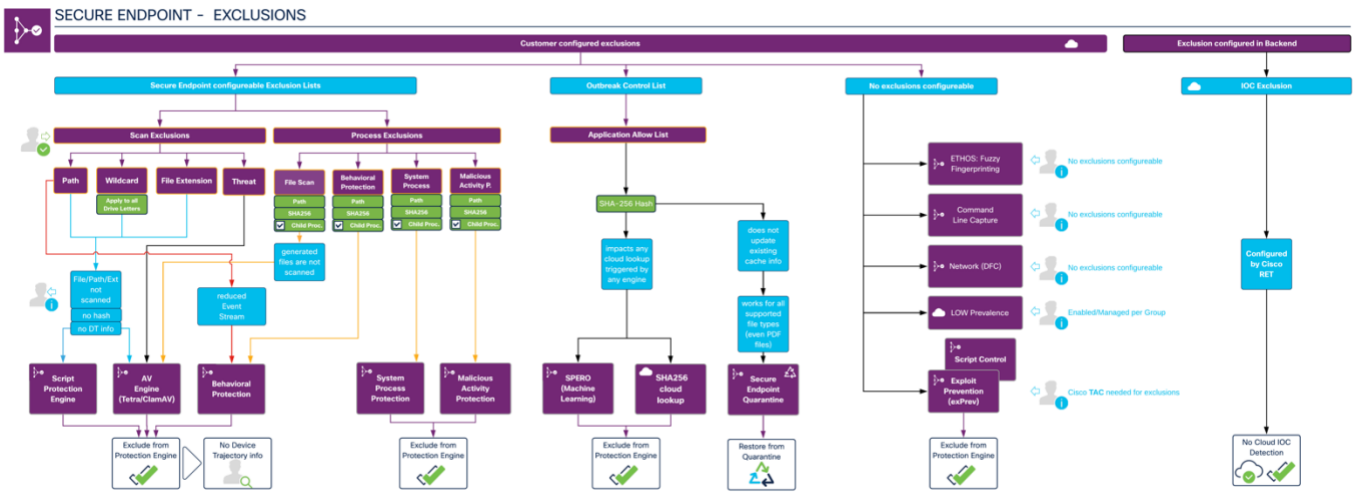
The guide outlines a lot of useful information around exclusion management for Secure Endpoint.

- Policy Configuration Planning section showing how the policy object looks like and how list objects are assigned to policies.
- Known limits for exclusions in the Policy Setting: Define and manage Exclusions section. Best Practices for List management and assignment.
- Troubleshooting the endpoint to determine necessary exclusions. Use the Device Trajectory to show which engine detected a threat.
- Clean-up exclusion on a regular base to provide the highest security level.
- Use as less as possible exclusions to provide the highest security level.

File Analysis and other Endpoint Protection areas with Secure Endpoint are not a linear process. As an example, File scanning is using several stages based on thy file type, cache status and more. Review the File Scan Sequence for details.

Insights into the drawing below.

- **Scan Exclusions** (Path/Wildcard/File Extension/Threat) are having an impact on AV-Scanning and the Script Protection Engine. The exclusion impacts the System Activity Monitor of Behavioral Protection Engine. Excluded files are not hashed and no telemetry for the backend engines is generated. Excluded processes are not visible in the Device Trajectory, except command line activity.
- **Process exclusions** are more related to single engines.
  - Process → File Scan: The process is not scanned. Any file generated by this process is also not scanned.
  - Process → Behavioral Protection: The process is excluded from the Attack Pattern Engine.
  - Process → System Process Protection or Malicious Activity Protection: The process is excluded from the specific engine
- **Application Allow Lists:** Entries have an impact on the following areas of the endpoint connector.
  - **File Type:** Entries are processed for Portable Executables and other file types, e.g., PDF files.
  - SPERO (Machine Learning): Allowed hashes are excluded from machine learning detection.
  - Cloud Lookups: Allowed hashes are excluded from cloud lookups. Cloud lookup detections are shown in Device Trajectory as **SHA engine**.
  - Files from the **quarantine folder** are restored to the original location on the disk if a hash has been added to the application allow list.
- Cloud IOC exclusions are not available today. Exclusions are added to the backend by Cisco. Please open a TAC case to add necessary Cloud IOC detection exclusions.



Best Practice: Use exclusions as less as possible to provide the highest security level and to maximize the detection of the Backend Detection Engines.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.