AMP for Endpoints Deployment Methodology and Best Practices

Contents

AMP for Endpoints

Deployment Best Practices

About This Document

AMP for Endpoints is a comprehensive Endpoint Security solution designed to function both as a stand-alone tool, and as a part of the architecture of natively integrated Cisco and 3rd party solutions. As such, there are many considerations that customers and partners should be aware of prior to deploying and configuring AMP for Endpoints in their environment. The objective of this document is to provide guidance around deployment methodology, setup and configuration, and general best practices.

Please be aware that this document focuses primarily on deployment strategies and best practices. It is designed as a supplemental document and does not contain a comprehensive list of all AMP for Endpoints features or configuration options. For more in-depth detailed information on specific product features or integrations, please see the other official AMP for Endpoints documents located here:

- [https://docs.amp.cisco.com/](https://docs.amp.cisco.com/)

Table of Contents

About This Document. 2

Deployment Journey. 6

Stage 1: Information Gathering. 7

Consideration: Environmental Data Gathering.. 7

Consideration: Security Product Data Gathering.. 7

Consideration: Auditing and Compliance. 8

Stage 2: Deployment Planning. 8

Consideration: Public Cloud vs. Private Cloud. 8

Consideration: AMP for Endpoints Configuration Planning.. 9

Consideration: Firewall and Proxy Settings. 10
Deployment Journey

This section outlines the recommended stages for deploying AMP for Endpoints in an enterprise environment successfully. The flow chart below serves as a generalized framework for customers to use within their environment.
The stages are: information gathering, deployment planning, console setup, alpha deployment, beta deployment, general deployment, and integrations setup. 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. Repeat cycles are also a part of any successful AMP for Endpoints 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.

**Stage 1: Information Gathering**

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

- Operating systems and versions
- Numbers of endpoints
- Existing security products
- Software deployment process
- Custom applications
- Proxy settings
- Privacy requirements
Consideration: Environmental Data Gathering

The first step is to understand and document the existing security posture. At a minimum, this should include:

- How many endpoints AMP for Endpoints will be installed on?
- What Operating Systems AMP for Endpoints will be installed on?
- Will the existing endpoint security product be removed before or after AMP for Endpoints is installed?
- Will AMP for Endpoints be cohabitating with the existing security product?
- What are the mission critical systems and software?
- What is the current software deployment process?
- Is there a HTTP/S Proxy in the environment?
- What are the organizational privacy requirements?

Consideration: Security Product Data Gathering

Most organizations deploy AMP for Endpoints into an environment where an existing endpoint security product is already installed. As such, there is already a great deal of information regarding what could potentially be transferred to AMP for Endpoints. Rather than start from scratch, this information should be compiled, evaluated for current relevance, and used to inform the AMP for Endpoints setup process. The following list is a good place to start, though it is by no means comprehensive:

- What exclusions are already included in the existing endpoint security product?
- Is there an existing application block list or an application white list?
- Is the current endpoint security software being used to block IP addresses?
- Are the exclusions, block lists, and blocked IP addresses still relevant to the current security posture?
- What security features are currently in use with the existing endpoint security product? Do these features exist in AMP for Endpoints? Can we transition the existing settings to the AMP for Endpoints console?

Consideration: Auditing and Compliance

Many organizations are subject to Auditing and Compliance requirements. Often times 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. AMP for Endpoints provides detailed user auditing and endpoint historical data with a limit of 30 days. Additional historical retention can be gained by utilizing the AMP for Endpoints Event Streaming functionality. To ensure that your new AMP for Endpoints 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?

Stage 2: Deployment Planning

Deployment Planning phase is the next step of preparation. This stage leverages the data collected in the information gathering section to make deployment relevant decisions around the use of public or private cloud, configuration planning, and console setup.

Consideration: Public Cloud vs. Private Cloud

AMP for Endpoints has two options for deployment: Public Cloud and Private Cloud. It is important to understand the differences between the two options to ensure that you choose the best fit for your organization.

• Public Cloud: AMP for Endpoints Public Cloud deployment 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: The AMP for Endpoints Private Cloud 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 AMP for Endpoints 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 AMP for Endpoints Private Cloud offer two primary modes of operation: Proxy Mode and Air-Gap Mode. Most AMP for Endpoints Private Cloud customers run their appliance in Proxy Mode, and this is the recommended configuration for Private Cloud deployments. Air-Gap Mode is deprecated for virtual Private Cloud deployments (will be available for physical UCS) and is provided for customers with extreme privacy requirements.
or for customers who are unable to have external network connectivity.<Link to specific information regarding private cloud options and requirements>

- Endpoint Connector Requirements: Specifics regarding endpoint connector requirements for all supported operating systems can be found here: <Link>

**Consideration: AMP for Endpoints Configuration Planning**

The primary means of organizing and managing batches of endpoints in the AMP for Endpoints console is via Groups. They allow the computers in an organization to be managed according to their function, location, or other criteria, as well as create parent and child groups to manage the overall environment at a granular level. In order to accomplish this, it is important to consider the following questions and plan your group and policy schema carefully:

- How will Groups of endpoints be organized?
- How will Policies be organized?
- How will Exclusions be organized?
- Will the selected structure fulfill the business needs a year from now?
- Will TETRA (Windows) / ClamAV (MacOS) be utilized as an AV engine?
- Will the AMP Update Server be deployed in your organization?
- Will the Cognitive Intelligence integration be enabled?

**Consideration: Firewall and Proxy Settings**

AMP for Endpoints Public Cloud required specific firewall rules and/or proxy settings to ensure proper endpoint connector functionality. Organizations using the Public Cloud option must allow outbound HTTP/TLS communication (TCP/443). This outbound communication can be limited to specific IP addresses and server URLs. Additional details can be found in the following TechNote article:

- Required Server Addresses for Proper AMP Operations:

**Stage 3: Console Setup**

This section will provide information on how to configure User Accounts, create and configure Policies and Groups, set up Prevalence and Outbreak Controls, create Exclusions, and set up an AMP Update Server.
User Setup

Several AMP for Endpoints features are unavailable to user accounts that are not properly configured. To ensure access to all available configuration options and product capabilities, it is important that users enable Two-Step Verification, Casebooks, and the Time Zone. Additional options available to users are Opting out of Google Analytics and Receive Announcements by Email.

**NOTE:** Two-Step Verification is required to use Remote File Fetch, Command Line Visibility, and Prevalence features. AMP for Endpoints Two-Step Verification has been tested and is compatible with Duo, Google Authenticator, and Authy for your iOS or Android device.

Steps

In order to properly configure your user’s Two-Step Verification, you will first need to log into your account with the credentials provided by your sales representative.

1. Click **Accounts à Users** and then select your username.
2. Click **Enable** next to the Two-Step Verification option and follow the onscreen instructions carefully configuring your two-step verification using one of the recommended applications (Duo, Authy, Google Authenticator)
3. Return to the user page and you should now see that Remote File Fetch and Command Line are enabled. Proceed with setting up the **Time Zone**, authorizing **Casebook**, and checking the **Receive Announcements by email**

When properly configured the user-page should look like this.
Policy Management

Policy creation and management is the heart of AMP for Endpoints. 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.

By default, the AMP for Endpoints Console provides a number of 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 in order 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 an AMP for Endpoints 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
BEST PRACTICE: AMP for Endpoints 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.

Steps

The steps below outline the recommended settings for an Audit, Protect, and Server policies.

1. While in the AMP for Endpoints Console, navigate to Management à Policies and click on the Windows tab, then click on Audit policy record to toggle expand settings and then click Edit.

2. While in the Modes and Engines tab of Audit policy, change the Malicious Activity Protection and System Process Protection engines to Audit and remove the checkbox in front of the Exploit Prevention

NOTE: Exploit Prevention engine does not allow monitoring, it always blocks/protects. Therefore, it is recommended to completely disable it for Audit policy.

3. Navigate to the Advanced Settings à Administrative Features page of the Audit policy and set up a Connector Protection Password to prevent unauthorized users (or malware) from starting/stopping or uninstalling the AMP
4. Navigate to the **Advanced Settings** à **Client User Interface** page of the **Audit** policy and choose whether you want end users to see the user interface or not.

**NOTE:** Cisco recommends disabling the client interface for simplicity however, this is an organization specific decision to make. If you decide to keep the Client User Interface, Cisco recommends using most of the default settings, while checking the Hide Exclusions checkbox to minimize user visibility of security settings.
5. Navigate to the Advanced Settings à File and Process Scan page of the Audit policy and ensure that On Execute Mode is set to Passive.

**NOTE:** Cisco recommends keeping the On Execute Mode settings as Passive. Changing that setting to Active mode may result in significant performance issues.
6. Familiarize yourself with the other policy configuration settings without making any further changes and then click **Save**. Below is what the Windows **Audit** policy should look like.

7. Next step is to create **Audit** policy duplicates for the purposes of debugging and triggering updates. While in the **Windows** tab of the **Policies** configuration, click on the **Audit** policy record and in the expanded settings view click on the **Duplicate** button (bottom right of the record view). That will create a duplicate policy named **Copy of Audit**.

8. Rename the newly created copy to **Audit - Debug** by first clicking on the **Edit** (bottom right of the record view), then changing the entry in the **Name** view, and finally clicking on **Save** (button on the bottom right of the policy configuration).

9. Create one more duplicate of the Windows **Audit** policy and rename it to **Audit – Update** We will configure audit and debug settings later.
10. Repeat the steps above for default **Protect** and **Server** policies, start with the provided settings. The main difference will be in the **Modes and Engines** For **Protect** policies, below is what **Modes and Engines** should look like.

**Modes and Engines**

**Conviction Modes**

These settings control how AMP for Endpoints responds to suspicious files and network activity.

- **Files**
  - **Quarantine**
  - **Audit**

- **Network**
  - **Block**
  - **Audit**
  - **Disabled**

- **Malicious Activity Protection**
  - **Quarantine**
  - **Block**
  - **Audit**
  - **Disabled**

- **System Process Protection**
  - **Protect**
  - **Audit**
  - **Disabled**

**Detection Engines**

- **TETRA**
- **Exploit Prevention**

**NOTE:** Other settings, including Administrative Features, Client User Interface, File and Process Scan, and others are the same as with the Audit policies.

1. For **Server** policies, below is what **Modes and Engines** should look like.

**Conviction Modes**

These settings control how AMP for Endpoints responds to suspicious files and network activity.

- **Files**
  - **Quarantine**
  - **Audit**

- **Network**
  - **Block**
  - **Audit**
  - **Disabled**

- **Malicious Activity Protection**
  - **Quarantine**
  - **Block**
  - **Audit**
  - **Disabled**

- **System Process Protection**
  - **Protect**
  - **Audit**
  - **Disabled**

**Recommended Settings**

**Workstation**
- Files: Quarantine
- Network: Block
- Malicious Activity Protection: Quarantine
- System Process Protection: Protect

**Server**
- Files: Quarantine
- Network: Disabled
- Malicious Activity Protection: Disabled
- System Process Protection: Disabled

**NOTE:** Network engine (DFC) should be completely disabled for most server deployments.
Furthermore, make sure to install server connectors with appropriate command line switches to disable installation of Device Flow Correlation. Keep Files in Audit for initial deployment and switch to Quarantine after initial tuning and review. Other settings, including Administrative Features, Client User Interface, File and Process Scan, and others are the same as with the Audit policies. Command Line Switches: [http://cs.co/AMP4EP_CLI_Switches](http://cs.co/AMP4EP_CLI_Switches)

11. Create additional debug (Protect – Debug and Server – Debug) and update (Protect – Update and Server – Update) policy versions. We will configure audit and debug settings later. Do not modify the Domain Controller and Triage policies for now.

When configured accordingly the Windows policies page should look like this:

![Policies Page](image)

**Groups**

Groups are the link between the endpoint connectors and the associated policies. As such, the top level of groups should have associated policies for all Operating Systems. For example, Audit Parent Group would have Audit policies assigned for Windows, Mac, Linux, iOS, and Android. However, connectors should not be placed directly into the parent groups. Rather, it is highly advisable to create child groups based on the standards a company uses to organize their endpoints. Utilizing child groups for endpoint organization allows for more granular management.

The AMP for Endpoints Console comes pre-populated with five default parent groups which are meant to act as a template. You can create as many parent or child groups as needed for your environment. The child group will inherit all of the policies of the parent group. Additionally, child groups can be moved between parent groups. When a child group is moved to a new parent group, it will inherit all of the policies associated with the new parent group.
The creation of parent groups should match your policies and be named identically. For example, if you have the following Policies:

- Audit
- Audit Debug
- Audit Update

You should have Parent Groups that correspond to each of these Policies:

- Audit Parent Group
- Audit Debug Parent Group
- Audit Update Parent Group

**NOTE:** The name of the group is only a descriptor for the devices within the group, it does not dictate the behavior of the group. It is always the policy that dictates how the connector will behave. For instance, you could have a group named Audit with a Protect policy attached. It is recommended to keep naming of groups and policies consistent to avoid confusion.

Once your endpoints are organized into their child groups, granular management becomes a simple task of moving the child group between parent groups. For example, when a new connector version is released, simply change the product update settings in the policy and move child groups into the associated Update Parent Group one at a time. This allows for granular
phased updates for your endpoint connectors without the need to create additional groups or policies.

**BEST PRACTICE:** Distribute your connectors across multiple child groups organized by commonalities. Example organization include region, time zone, office, business unit, functional similarities, etc. Then associate the child group with the appropriate parent group. Do not put all of your endpoint connectors into one group and do not put connectors into parent groups directly.

## How to Create Parent and Child Groups

The steps below outline how to create parent and child groups. These steps are meant to serve as an example for how to organize your AMP for Endpoints group structure.

1. While in the AMP for Endpoints Console, navigate to **Management à Groups** and click on the **Edit** button next to the **Audit** group and change the name to **Audit Parent Group**. Ensure that the Windows policy assigned is **Audit** (according to the name selected in the Policy Creation exercise). Click **Save**.

2. Create two new groups named **Audit Debug Parent Group** and **Audit Update Parent Group** using the **Create Group** button on the right side of the Groups page. Ensure that the Windows policies assigned to these groups are **Audit – Debug** and **Audit – Update**.

3. Repeat the same steps for the **Protect** and **Server** groups - create four new groups in total and ensure the Windows policies are assigned accurately to reflect the purpose of each group. For example, **Protect Debug Parent Group** should have **Protect - Debug** policy assigned for Windows and **Server Update Parent Group** should have **Server - Update** policy assigned for Windows).

4. Finally, create child groups based on whatever organizational schema your company uses for endpoint management.

**NOTE:** You can choose the Parent Group for a newly created group at the time of creation.
This is what the top of the Groups page should look like after completing the steps outlined above. Keep in mind, that some of the newly created parent groups do not fit on a single screenshot.

Prevalence

The AMP for Endpoints Prevalence feature is the built-in link to the Threat Grid file analysis environment. This feature monitors the selected AMP for Endpoint groups of endpoints for unknown executable files with low prevalence. When an unknown executable file is detected, the AMP for Endpoints cloud service can request the endpoint connector to upload the file for analysis if certain conditions are met. Once the file has been successfully uploaded to AMP for Endpoints Console, it is submitted to Threat Grid for further static and dynamic analysis. If the file returns a high threat score, then the AMP cloud is updated and the file is quarantined on the endpoint.

NOTE: By default, all AMP for Endpoints accounts come with a 24-hour rolling window submission limit of 100 files. Additional Threat Grid ‘Advanced File Analysis’ submission packs can be
purchased to increase the limit if needed.

Prevalence Configuration Steps

The steps below will demonstrate how to properly configure the prevalence feature.

1. While in the AMP for Endpoints Console, navigate to Analysis à Prevalence and click on the Configure Automatic Analysis button on the right side of the page.
2. Select the groups that will submit files for analysis and click Apply.

**BEST PRACTICE:** Prevalence should be configured for all endpoint groups but exceptions should be made for groups responsible for software development and groups with high privacy requirements (Automatic file submission may violate company confidentiality policy).

3. You should see the Current Automatic Analysis Status displaying the number of groups selected and the number of endpoints within these groups. At this point, we have not deployed any endpoint connectors and so the number is still zero.

Exclusions

Creating and managing exclusions within AMP for Endpoints is necessary to ensure minimal performance impact and proper application compatibility. AMP for Endpoints provides a large number of exclusions maintained by Cisco to assist organizations in getting setup rapidly. However, in most instances, at least some custom exclusions will be needed. In order to properly identify needed custom exclusions, it is necessary to obtain debug diagnostic data while the endpoint is under normal operational load. These diagnostic files are then parsed by the Tuning Tool, resulting in file frequency data. Additional resources for exclusions can be found in vendor documentation for existing endpoint security products and other popular software. For information on how to obtain diagnostic files and Tuning Tool usage please see Identifying New Exclusions in the Alpha Deployment section of this document.

**NOTE:** Exclusions should be re-evaluated carefully before porting them from one product to another to ensure they are still relevant for the environment, as well as to limit unnecessary gaps in security coverage. An overview of exclusions is available in the AMP for Endpoints user guide, as well as in the document:

http://cs.co/AMP4EP_Best_Practices_Exclusions
Outbreak Controls

AMP for Endpoints provides a wide variety of controls to manage and mitigate the spread of malicious software within customer environments. These controls include Simple Custom Detections (quarantine of files based on SHA256 matching), Advanced Custom Detections (matching on custom Clam AV rules), Application Controls (blocking and white lists to control application execution), Network (black and white IP address lists), and Endpoint IOC’s (custom OpenIOC formatted detection rules imported by customers for scanning).

Before importing data into outbreak controls from existing security products, the SHAs, IPs, and Rules should be re-evaluated carefully to ensure they are still relevant for the environment. Additionally, custom detections need to be applied for all relevant policies that require a particular custom detection to be honored. That is one of the reasons why accurate planning of your group and policy layout is so important.

NOTE: You can add SHA256 entries to the AMP for Endpoints Console one by one or you can upload a file containing a set of SHA256 entries at once. You can also upload a file itself to calculate a hash. Keep in mind that AMP for Endpoints won’t let you add a hash of a legitimate clean file (marked as such in the AMP Cloud) to a Simple Custom Detection list. This is a guardrail in place to prevent accidental convictions of legitimate files. Clean files can be added to Application Blocking lists to prevent execution though.

AMP Update Server

AMP for Endpoints contains a traditional AV engine called TETRA. TETRA is designed to work alongside the other AMP for Endpoints engines, providing enhanced security for static and mobile platforms. Since TETRA is designed to work in an offline capacity, it requires the download of signature files to operate properly. Given the bandwidth overhead inherent in downloading the initial signature files, AMP Update Server can be used to reduce WAN bandwidth overhead. Additionally, the AMP Update Server provides a local copy of the signature files, which helps ensure that network disruptions cannot prevent signature file updates.

To ensure maximum flexibility, the AMP Update Server has been designed to work on IIS, Nginx, and Apache.

NOTE: For more information on how to setup the AMP Update Server please see the following TechZone Article: http://cs.co/AMP_Update_server
BEST PRACTICE: In environments where the TETRA engine is to be used with desktops, virtual environments, and servers, it is advisable to configure an AMP Update Server. An organization may have multiple AMP Update Servers serving definitions to regional offices (a server is configured per policy). Keep in mind that it is recommended that remote workstations and roaming systems download updates directly from the AMP Cloud and NOT the AMP Update Server.

Stage 4a: Alpha Deployment

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 AMP for Endpoints using the phased approach outlined in Stage 4a, Stage 4b, and Stage 5.
Audit Deployment (Alpha group)

In stages 1 through 3, we gathered information regarding our current setup and configured our console with known exclusions, groups, and policies. With that information in hand and the configuration complete, we are ready to begin deploying to the Alpha round of endpoints. The Alpha deployment endpoints should be deployed to a group under the Audit – Debug Parent group. This will ensure that the connector maintains a useful data set for tuning purposes.

**BEST PRACTICE:** Alpha deployment should consist of a very small subset of your organization. Depending on organization size, this may consist of between 1 and 10 percent of your workstations. With real-world deployments, it is highly recommended to begin the deployment process with the IT staff, as they will have the skills to help diagnose the issue while avoiding unnecessary tickets for your helpdesk. It is recommended to deploy the AMP for Endpoints connector with an Audit policy that has debug enabled as it will help reduce the potential for negative impact on the user endpoints while providing valuable data that will be used for tuning purposes.

**NOTE:** Default and additional command line switches for the AMP Connector:
http://cs.co/AMP4E_Connector_Install_Switches

Connector Tuning (Alpha group)

Once the connector has been deployed and has registered with the AMP for Endpoints console, it should be allowed to collect data for a period of time as this will allow the connector to obtain the data we can use to create additional exclusions. In a real-world deployment, the connector should be registered and active for a minimum of 30 minutes (preferably 1 hour) before we are ready to retrieve diagnostic packages from the endpoints.

**BEST PRACTICE:** It is advisable to run this process at least two times or more during business hours to ensure that any needed exclusions are identified and implemented.

Identifying New Exclusions
The steps below will walk through the Cisco Maintained Exclusions and Custom Exclusions dashboards, triggering a diagnostic upload to the AMP for Endpoints console, downloading the resulting diagnostic file, and running the Tuning Tool.

**NOTE:** The Windows Connector Tuning Tool is not supported by Cisco TAC. Customers are free to use this tool, however, if any issues are encountered, they should be reported as an issue on Github. Cisco TAC will not assist customers with the use of this tool, if a tuning case is opened, TAC will assist with tuning the endpoints directly.

1. Log into AMP for Endpoints and navigate to **Management à Exclusions**. Two categories will be visible: **Custom** and **Cisco-Maintained**

   **A. Custom Exclusions** are created by your organization to address specific non-standard cases. Such exclusions are often created after initial tuning. You can exclude Paths, File Extensions, Wildcards, Threats, and Processes.

   **BEST PRACTICE:** The recommended best practices for exclusions are described in the following document: [http://cs.co/AMP4E_Exclusions_Best_Practices](http://cs.co/AMP4E_Exclusions_Best_Practices)

   **B. Cisco-Maintained Exclusions** are created and maintained by Cisco to provide better compatibility between the AMP for Endpoints Connector and antivirus, security, and other software.

   **NOTE:** Cisco-Maintained exclusions cannot be deleted or modified. You can see which files and directories are being excluded for each application. These exclusions may also be updated over time with improvements and new versions of applications.

2. Navigate to **Management à Filter** for one of the Alpha group endpoints.
3. Click the **Diagnose**
4. Set the **Debug Session -> 15 minutes** and click Historical Data and Kernel Log buttons.
5. Wait 20-30 minutes for the diagnostic to run and upload to the AMP for Endpoints file repository.
6. Click Analysis à File Repository.
7. Click Type à Connector Diagnostics.
8. Expand the connector record and click Download.
9. Navigate to: http://cs.co/AMP4E_Tuning_Tool
10. Download the Diag_Analyzer_<version>.exe
11. Place the Diagnostic and the Diag_Analyzer in the same folder.
12. Double-click: Diag_Analyzer_<version>.exe file. This will result in the decompression of the diagnostic file, and the creation of a text file containing file and directory frequency information.
13. Evaluate the resulting text file for potential new exclusions.

**NOTE:** With the output of the tuning tool, identify the busiest, most accessed files and processes. Verify the validity to your business environment and vulnerability to external environments. Ensure
you are aware of the files and processes vulnerabilities if any exist.

**NOTE:** Exclusion lists must be added to the relevant policies in order for the exclusions to be passed to endpoint connectors.

Carefully review the output and determine which exclusions need to be implemented while keeping possible security loopholes in mind. Add the resulting exclusion to your AMP for Endpoints Console. It is highly recommended to review the Exclusion Best Practices document step 1a of this exercise.

**BEST PRACTICE:** Connector tuning should be performed as often as necessary, with as large an endpoint sample set as practical, to ensure stable, low resource performance of the AMP for Endpoints Connector.

**Connector Activation (Alpha group)**

Once the connector has been deployed to the initial Alpha group, tuning has been performed, and possible performance issues mitigated through addition of new exclusions, you are ready to activate the endpoint connectors by moving them to a different parent group with Protect policy enabled. At this stage, continue to monitor for performance issues and help desk tickets.

**BEST PRACTICE:** Before moving the endpoints to Protect mode, ensure that exclusions are configured properly and any custom software is added to application whitelists to avoid false detections. If additional issues are encountered and a return to the Audit posture is needed, simply move the child group back to the Audit Parent Debug Group. However, also consider collecting diagnostic packages while the endpoint is running in Protect mode. If several rounds of exclusions tuning are unable to resolve your issue, open a case with Cisco TAC support as you may be encountering a previously unknown issue that requires a more detailed analysis.

**Stage 4b: Beta Deployment**

Unlike the relatively small Alpha deployment, the initial round of Beta deployments should be a larger group of endpoints but still restricted to only a small percentage of the organization as a whole. The Beta deployment stage may be repeated several times, expanding the install base during each integration to ensure a steady and thorough growth in the install base. Beta deployments should begin in an Audit Debug configuration and move into a Protect Debug stage after initial tuning. Once tuning has been finalized and endpoint issues have been resolved, these systems can be moved out of Debug into the standard Protect Group.
BEST PRACTICE: If there are test environments for mission critical systems (such as server and others), they should be targeted during a round of beta deployments. When choosing target endpoints for Beta deployment, choose a limited cross section of all departments or endpoint roles. This provides a better overall understanding of the target environment and allows for smoother diagnostics and tuning based on feedback from the field. The Beta deployment stage should be repeated several times to ensure maximum compatibility and performance across all target endpoint groups.

Audit Deployment (Beta group)

This is where it starts to get repetitive. Just like with the Alpha deployment stage, we start by deploying the AMP Connector in Audit mode to more endpoints. That should expand the initial deployment to cover other departments with different roles and functions, different software sets, and different user behaviours.

Connector Tuning (Beta group)

The tuning exercise for the Beta group is practically the same as it was for the Alpha group. The only difference is that we now target endpoints that were deployed during the Beta stage. As there are different endpoint roles and organizational departments involved at that stage, they are likely to produce a different set of exclusion requirements that we need to account for.

Connector Activation (Beta group)

Once the connector has been deployed to the broader Beta group, the tuning has been done, and exclusions added, it is time to activate the endpoint connectors by moving them to Protect mode. Continue to monitor for performance issues and help desk tickets. The same set of best practices applies for the Beta group in regard to exclusions, application whitelisting, and tuning.

Stage 5: General Deployment
With the success of both Alpha and Beta deployment stages, General deployment becomes practically feasible. Endpoints should be installed using an active Protect mode which means there is no connector activation step. At this stage, policies, groups, and exclusions should be properly configured and tuned for their target environments. Configuration and performance issues should be minimal, and administrators should generally have a feel for what to expect.

**BEST PRACTICE:** Plan the General Deployment to reach 100% of compatible endpoints. Deploy to these endpoints in as many stages as the deployment team is comfortable with. It is recommended to deploy starting with the least important systems, through moderately important, and finish with critical systems. Allow time between each round of deployments to complete the feedback loop and tune if needed.

### General Deployment

Having completed stages 4a, and 4b successfully AMP for Endpoints should be ready for General Deployment to the broader enterprise. To ensure success, the administrator should be convinced that they have 90+% of the exclusions and issues dealt with and confident in deploying the AMP Connector to remaining systems in Protect mode, directly bypassing Audit mode deployment. This stage will typically not include new organizational units, system groups, and user roles.

### Steps

General Deployment, by its definition, would typically assume practicing the skills obtained in Alpha and Beta deployment phases up to the point of covering 100% of compatible endpoints.

### Consideration: Connector Tuning

Conduct connector tuning until all performance and compatibility issues have been eliminated. If adequate attention has been paid to exclusions during stage 4a and 4b, minimal additional tuning should be required. However, as most environments are dynamic in nature these days, it is recommended to establish a repeatable process that can help quickly eliminate problems as they arise. That involves not only monitoring the broader enterprise with all of its departments for help...
desk calls, but also collecting diagnostic packages for new endpoint roles as they are introduced. At this point, there should be a deployment process that works as a repeatable loop: Deploy – Diagnose – Tune.

Stage 6: Integrations

AMP for Endpoints has been designed as a part of an architectural security solution. As such, it natively integrates with a large number of Cisco Security products. Additionally, AMP for Endpoints has pre-built plugins for both Splunk and Q-Radar with API functionality that allows integration with the majority of SIEM products and alerting systems. These integrations form an architecture allowing for cross platform detection and response capabilities.

**STAGE 6: Integrations Setup**

- Configure native Cisco integrations
- Create API Credentials
- Configure 3rd party integrations

Threat Response

Cisco Threat Response is an innovative platform that brings together security-related information from Cisco and third-party sources into a single, intuitive investigation and response console. Modules allow for rapid correlation of data by building relationship graphs that enable security teams to obtain a clear view of the attack and quickly make effective response actions. The daily workflow is also streamlined through the integrated case management tool named “Casebook” that was enabled in the User Setup section.

Enable Threat Response Integration

Many Security Operations teams will want to take advantage of the Cisco Threat Response integration, which is already equipped for AMP for Endpoints. By adding the AMP for Endpoints module to Cisco Threat Response, investigators will be able to search for IP addresses, domains, URLs, and file hashes that have been recorded by AMP for Endpoints.

1. Log into the AMP for Endpoints console, then open a new browser tab and navigate to visibility.cisco.com. Proceed by clicking Log In with Cisco Security button and enter the same credentials that you have used to login to AMP for Endpoints.
NOTE: At the time of writing this guide, Threat Response requires that your AMP for Endpoints user account has administrative privileges to access and leverage the platform.

2. After you have logged into Threat Response, click on Modules. You will see that multiple modules including AMP Global Intel, Private AMP Global Intel, AMP File Reputation, Talos Intelligence are already enabled by default.

3. On the same page click Add New Module. That is where we will add a module for AMP for Endpoints. Follow the instructions in the open dialogue window. After populating the 3RD PARTY API CLIENT ID and the API KEY fields confirm by clicking Create Module.

NOTE: The URL field should be specified according to location of your AMP for Endpoints instance (NA, EU or APJC). Keep it as default for now.

4. You should then see the newly created AMP for Endpoints module on the Modules page. We do not configure any other modules as a part of this guide however, you may find relevant instructions for configuration of other modules and Threat Response APIs by clicking the How do I configure modules? and API Clients buttons on the Modules page accordingly.

Threat Grid

Threat Grid is Cisco’s malware analysis and threat intelligence platform that improves security through static and dynamic sample analysis and threat intelligence generation and sharing. AMP for Endpoints provides a limited integration with Threat Grid via the Prevalence feature. However, a full Threat Grid account allows for broader integration and sample management across the Cisco Security Portfolio. Being completely API-driven, Threat Grid is designed to enrich the overall security infrastructure and as such, it integrates with most of the Cisco security portfolio as well as with a growing number of 3rd party products.

Steps

If you already have a Threat Grid account, you can integrate your AMP for Endpoints account with
your Threat Grid account by simply obtaining your Threat Grid API key and installing it in AMP for Endpoints Console. This will allow for centralized sample management, ensuring that any sample runs utilize your organizational settings. Additionally, the Threat Grid integration with AMP for Endpoints will allow users to leverage a unified Cisco Security account to login to both tools. This will tie your AMP for Endpoints file analysis submissions (originating from Prevalence or submitted manually) to your Threat Grid Cloud portal.

1. Log into Panacea.threatgrid.com
2. Click on your username in the top right corner and go to My Account page where you will copy your Threat Grid API key by clicking on a tiny button on the right side from the API Key

![API Key Copy](image)

1. Now open your AMP for Endpoints Console and navigate to Accounts à Business, click Edit on the top right corner of that page, and scroll down to the Cisco Threat Grid API Paste the key that you have copied from Threat Grid into the API Key field and click Save.

**NOTE:** This setup will allow you to see your file analysis submissions originating from AMP for Endpoints in your Threat Grid Cloud account, which offers more robust view into analysis results, as well as allows to perform more in-depth threat research and investigations.

**Cognitive Intelligence**

Cognitive Intelligence (previously known as Cognitive Threat Analytics) detects malicious activity that was able to successfully bypass other security controls or entered through unmonitored channels (including removable media) and is actively operating inside an organization’s environment. Cognitive Intelligence is a cloud-based service that uses machine learning and statistical modelling of networks to detect malicious C2 traffic tied back to compromised endpoints. More specifically, it analyses user and device behaviour from web traffic and NetFlow to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in the infrastructure. The backend algorithms of Cognitive Intelligence also allow to improve detection of yet unknown malicious files by looking at command lines arguments associated with binary executions and by correlating files with their destination servers. As such, Cognitive Intelligence is a major contributor to the efficacy of AMP for Endpoints and it’s considered a best practice to leverage it whenever possible.

**Steps**

Below is an example of how to configure Cognitive Intelligence from within AMP for Endpoints and configure Cisco Web Security Appliance as a telemetry source.

1. While in the AMP for Endpoints Console, navigate to Accounts à Business, click Edit and scroll down to the Cognitive Threat Analytics section of the page.
2. Click Enable and then click Configure. You should be redirected to the page that allows configuring your first telemetry source. Click on Let’s Get Started button, then on SCP, and finally provide a suitable Device name (anything will work, just make sure it identified your
NOTE: This example shows how to configure a Cisco Web Security Appliance (WSA) as a web log telemetry source. However, Cognitive Intelligence can also leverage 3rd party tools as telemetry sources, as long as the logs are provided in the required W3C format over HTTPS or SCP (McAfee, BlueCoat, Squid, ZScaler,...). Stealthwatch Enterprise (NetFlow) is also among the most common telemetry sources for Cognitive.

3. Leverage the following step-by-step configuration guide to complete and verify the pairing of your WSA with Cognitive.


General Best Practices

This section explains additional generalized best practices that should be considered when deploying and operating Cisco AMP for Endpoints.

Connector Updates

If you followed best practices with regards to the creation of policies and groups, then connector updates are trivial tasks that can be performed as granularly as your staff would like. You can execute it by simply moving the child group for the endpoints you wish to target into the update version of their current parent group.

BEST PRACTICE: After upgrading from one version of the endpoint connector to another, always reboot the endpoint. In many cases failure to reboot an endpoint after a connector update will prevent the connector from functioning properly. It is recommended to schedule connector updates to coincide with maintenance windows.

Exercise: Troubleshooting
AMP for Endpoints is a robust product with a number of different scanning and security engines. As such, troubleshooting AMP for Endpoints Connectors can be a daunting task to those not familiar with its intricacies. However, there are some basic trouble shooting steps that you can take that resolve the majority of problems.

## Connectivity Test

One standard issue many admins encounter is a problem validating that their firewall and proxy rule sets are fully implemented. To assist with troubleshooting this issue AMP for Endpoints includes a connectivity test tool as part of the windows connector install on every endpoint. Running the tool is simple and the results will help immediately identify if the endpoint has proper connectivity to the AMP for Endpoints cloud infrastructure.

### Steps

To run the connectivity test first choose an endpoint with a potential connectivity issue:

1. Browse to the local AMP for Endpoints directory: `C:\Program Files\Cisco\AMP\<version number>`
2. Execute the connectivity tool by right-clicking the `exe` and selecting the `Run as administrator` option.
3. Open the resulting `exe.txt` file and scroll to the bottom. The summary data will tell you if you have a connectivity problem. If you do discover an issue using the connectivity tool, scrolling up and identifying the failed curl call will help determine where that problem lies within network.

![Connectivity Test Result](image)

### Device Trajectory Test

In some instances, we may be uncertain if a connector is communicating with the AMP for Endpoints Cloud Infrastructure. Many times, we will have endpoints that do not report an “event” for a significant period of time. In these cases, admins often wonder if the endpoint is functioning properly. One quick and easy method to determine if a connector is reporting data to the backend is to simply open the Device Trajectory view for that endpoint.

### Steps

In this exercise, you will use Device Trajectory to determine if an endpoint is reporting data to the cloud.
1. While in the AMP for Endpoints Console navigate to Management -> Computers and use Filters to locate the endpoint in question. Last Seen value is usually a great indicator if the endpoint is communicating with the AMP Cloud.

NOTE: For this simple exercise, choose any of your endpoints installed.

2. Expand the endpoint record and click the Device Trajectory. You should be taken to the view with historical representation of process, file, and network events on that system.

3. If the endpoint has device trajectory data in the last few minutes then the endpoint is reporting properly and event data will appear if a detection is triggered. You can also run a simple check by downloading pdf test file on that endpoint and reviewing if it shows up on Device Trajectory. (https://mysite.science.uottawa.ca/rsmith43/Zombies.pdf)

Improper Exclusions Check

Performance problems are one of the more common issues that admins encounter when running security products and are typically tied to missing exclusions. However, in some instances, improperly formatted exclusions can lead to significant performance overhead. One way to identify some of these exclusions is to use the Windows Tuning tool from Github (downloaded during Connector Tuning exercises). This tool is capable of pointing out improperly formatted exclusions to assist in resolving these performance issues.

Steps

In this exercise, you will use the Windows Tuning tool to check for improper exclusions.

1. While on the Management à Computers page of the AMP for Endpoints Console, request a support diagnostic package from an endpoint by expanding the record and clicking.
2. Wait for the diagnostic package to upload to the console (7-10 minutes) and download it from Analysis à File Repository. Make sure to select Connector Diagnostics as the Type.
3. Place the diagnostic package in the AMP Diagnostics network folder (shortcut on your Student_Win desktop), make sure you still have the exe tool in that folder.
4. Run the tool against the diagnostics package and carefully observe the results in the newly created txt file.

NOTE: When you run the tool from the CLI, make sure to respond “y” to the question about viewing exclusions from your policy or specify the “-e 1” option.

When evaluating the results of the tuning tool and the exclusions listed in the AMP for Endpoints Console, it is important to evaluate the exclusions for performance as well. Performance exclusion checks consist of 2 parts:

1. Is the exclusion the proper type: Wildcard, Path, Process, File Extension, Threat.

Wildcard Exclusions: C:\Program Files\MyApplication\*.logC:\Users\MyApplication\C:\ProgramData\MyApplication\*.log

If an exclusion has a leading wildcard, the tool will throw a Warning like the one below.
NOTE: Exclusions with leading wildcards are likely to cause performance issues. These exclusions should be reformatted to remove the leading wildcard using CSIDL paths or drive letters.

Regardless of the methodology used, issues will often occur that require troubleshooting beyond simple tuning. When this occurs, the best approach is to obtain debug diagnostics from the endpoint while the issue is occurring and submit the diagnostic data to TAC. This will greatly reduce the time it takes to identify and resolve any issues that you encounter.

Consideration: Virtual Desktop Infrastructure

AMP for Endpoints is VDI vendor agnostic. The virtualization host operating system does not need to be supported in order for AMP for Endpoints to function in the virtualized environment.

AMP for Endpoints supports both Persistent and Non-Persistent VMs.

- Persistent VM’s are treated like any other desktop or laptop. Persistent VDI environment should focus on correctly creating the deployment gold image.
- Non-Persistent VM’s require additional configuration and tuning prior to deployment.

NOTE: Both configurations require access to the Identity Persistence feature of AMP for Endpoints. To enable this feature, open a case with Cisco TAC and request feature enablement.

Identity Persistence allows AMP for Endpoints to properly map endpoint UUID’s to existing computer records within the console. Identity persistence is used to prevent the creation of duplicate connector records in the AMP for Endpoints dashboard. This feature also helps to maintain the consistency of endpoint connector records by providing continuity of the historical record. Additionally, it prevents one endpoint from using more than one connector license. If duplicate records appear in your console, open a TAC case to get this resolved. TAC will help identify the cause of the duplication and can help clean up the duplicate records.

BEST PRACTICE: When using Identity Persistence configure it across all policies uniformly, non-
uniform settings may result in the creation of duplicate connector records. The recommended configuration for Identity Persistence is “By Hostname across Business”.

Appendix. AMP for Endpoints Overview

This appendix provides a brief introduction of Cisco AMP for Endpoints solution, its protection capabilities, and deployment use cases.

Solution Overview

Cisco AMP for Endpoints overview is a cloud-managed endpoint security solution which combines the capabilities of preventing attacks at the point of entry, detecting threats that land on the endpoint, and responding to advanced threats that were able to circumvent other preventative security layers of defence. AMP for Endpoints implements continuous monitoring and retrospective analysis of all file and process activity happening on the disk of the endpoint system, allowing it to identify malware retrospectively as well as perform forensic, threat hunting, and incident response functions.

AMP for Endpoints provides robust incident response workflows to help facilitate daily routine by cyber teams. The Inbox tab of the Dashboard helps quickly identify endpoints that require attention in your environment in order to begin working on remediation. While Inbox is not a full replacement of ticket management systems, it provides solid augmentation to the capabilities of such tools to make managing incidents easier.

Device Trajectory is a visual capability that represents a historical view of processes and file executions on your endpoints. It gives you tremendous insight into how files are behaving in your environment: how and when they execute, whether they make network connections, whether they introduce other files as a result of these connections, and so on. AMP for Endpoints assigns a
disposition to files based on the global threat intelligence produced by Talos: clean, malicious or unknown. Yellow overlays get your attention where it needs to be, the starting point of infection that helps explain how the threat was introduced.

File Trajectory displays information related to a specific file. It helps understand where the file was observed across your AMP for Endpoints environment. Through a native integration of AMP for Endpoints with Cisco’s Email Security, Web Security and Network Security (Firepower) devices called AMP Unity, File Trajectory displays if a file was also observed in transit through any of these inspection points in a single unified view, which reduces the lag of pivoting from one user interface to another, and as a result makes security teams more efficient. AMP Unity provides other significant benefits such as black/white listing unification across platforms.

AMP for Endpoints supports a variety of operating systems including Microsoft Windows (Desktop and Server), Linux (RedHat and Centos), MacOS, Android, and iOS (official product name for iOS is Clarity, a part of Cisco Security Connector).
Protection Lattice

Cisco AMP for Endpoints protection capabilities comprise several technologies that work together to prevent, detect, and remediate malicious code at the endpoint. The following describes the security stack of the AMP for Endpoints connector for Windows.

The core In Memory prevention engines include:

- **Exploit Prevention** defends endpoints from memory attacks commonly used by obfuscated malware, exploits, and post-exploitation tools targeting software vulnerabilities of protected processes.
- **System Protection (System Process Protection engine)** defends critical Windows system processes from being tampered or compromised through memory injection attacks by other offending processes.

The core On-Disk Detection technologies include:

- **AMP Cloud** blocks malware using the global threat intelligence that is constantly augmented with new threat knowledge from Cisco Talos, Threat Grid, and Cognitive Intelligence (machine learning) research.
- **Behavioural Analysis (Malicious Activity Protection engine)** offers run-time detection and blocking of abnormal behaviour associated with a running file or process (eg. ransomware-related behaviours).
- **Anti-Virus and Blocklist (TETRA for Windows and Custom Detections)** is a traditional signature-based antivirus engine, which resides on the endpoint and provides on disk malware detection capabilities; Custom Detections serve the goal of delivering robust control capabilities to the security analyst by allowing to define custom signatures and enforce blacklists using industry standard formats.

The core Post-Infection detection technologies include:

- **Network (Device Flow Correlation or DFC)** inspects incoming and outgoing network
communications of a process/file on the endpoint, allows to enforce a restrictive action according to the policy (IP reputation and custom IP block lists).

- **Cloud IOCs** help surface suspicious activity observed on the endpoints through pattern recognition, related alerts serve as the trigger for more in-depth investigations and response.
- **Endpoint IOCs** is a powerful threat hunting capability for scanning endpoints for post-compromise indicators across the enterprise. The scanning can be imported from custom or Cisco-created open IOC XML files.

**Cognitive Intelligence** further enhances AMP for Endpoints efficacy through the efforts of Cisco’s Machine Learning research team (12+ years of research experience, 80+ ML data scientists and engineers, 60+ patents and fillings, 200+ publications on the subject). With that, the product is enriched with file-less and agent-less detection capability based on the analysis of network (web logs, Netflow) telemetry. The result of that analysis is context-rich threat knowledge tailored to a particular organization. Cognitive Intelligence also leverages backend intelligence for correlation of threat behaviours and activity across multiple monitored datasets (Network, Endpoint, Attacker Model), thereby providing an increased level of security efficacy. On top of that, other dedicated models operate embedded inside the AMP and Threat Grid products to deliver ML-based Static File Analysis capability.

These security capabilities are the foundation of the overall approach to pervasive advanced malware protection. While Cisco recommends using all of these engines in conjunction with each other to leverage the full value of the solution, customers can select whether to enable or disable one or another engine through a Policy. While listed separately, these technologies work together as a protection lattice to provide improved visibility and increased control across the entire attack continuum.

**Online and Offline Engines**

An important consideration for most enterprise deployments is the requirement to have always-on cloud connectivity for continued protection. AMP for Endpoints engines provide endpoint protection with or without AMP Cloud connectivity (depending on the engine). Below is a table that breaks down the engines into two groups: online (require AMP Cloud connectivity to provide threat protection and detection) and offline (do not require AMP Cloud connectivity to perform security related functions).

<table>
<thead>
<tr>
<th>Online</th>
<th>Offline</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP Cloud</td>
<td>Exploit Prevention</td>
</tr>
<tr>
<td>Cloud IOCs</td>
<td>System Process Protection</td>
</tr>
<tr>
<td>Endpoint IOCs</td>
<td>Malicious Activity Protection</td>
</tr>
<tr>
<td>Threat Grid</td>
<td>Anti-Virus Signatures*</td>
</tr>
<tr>
<td>Simple Custom Detections</td>
<td>Advanced Custom Detections*</td>
</tr>
</tbody>
</table>

*Initial deployment of Advanced Custom Detections/AV sigs requires AMP Cloud connectivity.
Use Cases

Cisco AMP for Endpoints can be installed alongside other endpoint security solutions or could be leveraged as a standalone tool. When deployed alongside other products accurate baselining and tuning is recommended to ensure two products co-exist well and do not cause performance and compatibility issues.

While the appendix provided for this hands-on training covers a high-level overview of AMP for Endpoints, it should not be considered as a replacement to the official product documentation available at https://console.amp.cisco.com/docs