

思科电邮安全高级恶意软件防护(AMP)最佳实践指南

目录

[简介](#)

[验证功能密钥](#)

[启用高级恶意软件防护\(AMP\)](#)

[自定义高级恶意软件防护\(AMP\)全局设置](#)

[文件分析阈值设置](#)

[将ESA与面向终端的AMP集成控制台](#)

[启用邮箱自动补救\(MAR\)](#)

[在邮件策略中配置高级恶意软件防护\(AMP\)](#)

[将SMA与思科威胁响应\(CTR\)集成](#)

[结论](#)

简介

高级恶意软件防护(AMP)是一个全面的解决方案，可实现恶意软件检测和拦截、持续分析和追溯性警报。利用思科电邮安全的AMP，可在攻击前、攻击中和攻击后的整个攻击过程中提供卓越的保护，并采用最经济高效且易于部署的高级恶意软件防御方法。

本最佳实践文档将介绍思科邮件安全设备(ESA)上AMP的主要功能，如下所列：

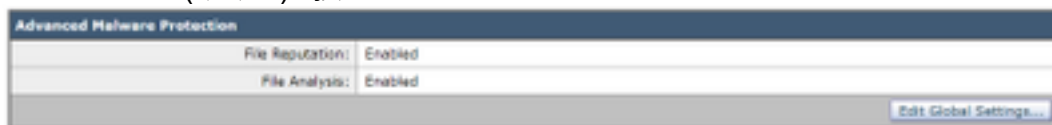
- **文件信誉** — 在每个文件经过ESA时捕获其指纹，并将其发送到AMP的基于云的情报网络，以进行信誉判定。根据这些结果，您可以自动阻止恶意文件并应用管理员定义的策略。
- **文件分析** — 提供分析流经ESA的未知文件的功能。高度安全的沙盒环境使AMP能够收集有关文件行为的精确详细信息，并将这些数据与详细的人机分析相结合，以确定文件的威胁级别。然后，此配置将输入到基于AMP云的情报网络，并用于动态更新和扩展AMP云数据集以增强保护。
- **邮箱自动补救(MAR)** — 对于Microsoft Office 365和Exchange 2013/2016，使用在初始检测点后变为恶意的文件自动删除电子邮件。这可节省管理员的工作时间，并有助于遏制威胁的影响。
- **Cisco AMP Unity** — 允许组织在面向终端的AMP控制台中注册其支持AMP的设备（包括ESA）和AMP订阅。通过这种集成，可以查看和查询思科电邮安全，以获取示例观察结果，就像面向终端的AMP控制台已经为终端提供的一样，并允许将文件传播数据关联到单个用户界面中的所有威胁媒介。
- **Cisco Threat Response** — 是一个协调平台，可将来自思科和第三方来源的安全相关信息整合到一个直观的单一调查和响应控制台中。它通过模块化设计来实现此目的，该设计用作事件日志和威胁情报的集成框架。模块通过构建关系图实现数据的快速关联，从而使安全团队能够清楚地了解攻击，并快速做出有效的响应操作。

验证功能密钥

- 在ESA上，导航至“System Administration”>“Feature Keys”。
- 查找“文件信誉和文件分析”功能键，并确保状态为“活动”

启用高级恶意软件防护(AMP)

- 在ESA上，导航至“安全服务”>“高级恶意软件防护 — 文件信誉和分析”
- 单击“Advanced Malware Protection Global Settings(高级恶意软件防护全局设置)”上的“Enable (启用)”按钮：



- 提交更改。

自定义高级恶意软件防护(AMP)全局设置

- AMP现在已启用，请单击“编辑全局设置”以自定义全局设置。
- 文件扩展名列表将不时自动更新，因此请始终访问此设置并确保已选择所有文件扩展名：



- 展开文件信誉的高级设置
- 文件信誉服务器的默认选择是AMERICA(cloud-sa.amp.cisco.com)
- 点击下拉菜单并选择最近的文件信誉服务器（尤其是对APJC和欧洲客户）：



- 展开文件分析的高级设置
- 文件分析服务器URL的默认选择是AMERICAS(<https://panacea.threatgrid.com>)
- 点击下拉菜单并选择最近的文件信誉服务器（尤其对于欧洲客户）：



文件分析阈值设置

(可选) 允许您设置可接受文件分析分数的上限阈值。根据阈值设置被阻止的文件在高级恶意软件

防护报告的传入恶意软件威胁文件部分中显示为自定义阈值。

- 在AMP全局设置页中，展开**Threshold Settings**。
- 云服务的默认值为**95**。
- 选择“**输入自定义值**”单选按钮并更改值（例如**70**）：



- 单击**提交并提交更改**

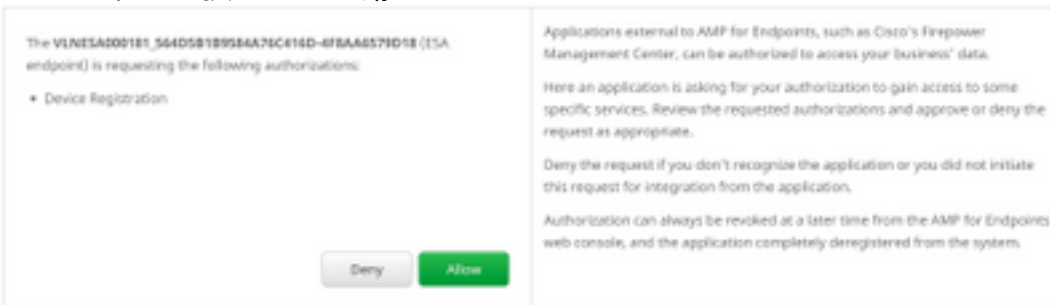
将ESA与面向终端的AMP集成控制台

(仅适用于面向终端的AMP客户)统一的自定义文件阻止列表（或文件允许列表）可通过面向终端的AMP控制台创建，并且可以在包括ESA在内的安全架构中无缝分配遏制策略。

- 在AMP全局设置页面中，展开**文件信誉的高级设置**
- 单击按钮 — 向面向终端的AMP注册设备：



- 单击**OK**重定向到面向终端的AMP控制台站点以完成注册。
- 使用您的用户凭证登录到面向终端的AMP控制台
- 单击**Allow**授权ESA注册：



- 面向终端的AMP控制台会自动将页面转回ESA。
- 确保注册状态显示为**SUCCESS**：



- 单击**提交并提交更改**

启用邮箱自动补救(MAR)

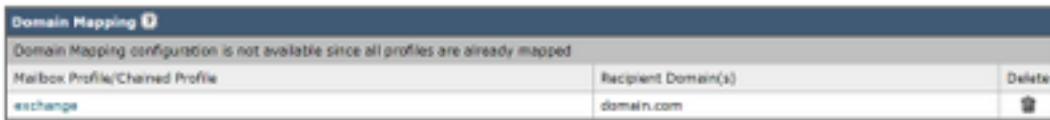
如果您有O365个邮箱或Microsoft Exchange 2013/2016，则邮箱自动补救(MAR)功能将允许在文件信誉判定从Clean/Unknown更改为Malicious时执行该操作。

- 导航至“**系统管理**”>“**帐户设置**”
- 在“**帐户配置文件**”下，单击**创建帐户配置文件**以使用您的Office 365和/或Microsoft Exchange的邮箱创建API连接配置文件：



- 单击**提交并提交更改**

- **(可选)** 链接配置文件是配置文件的集合，仅当要访问的帐户驻留在不同类型部署的不同租户时，才配置链接配置文件。
- 单击**Create Domain Mapping**按钮，将帐户配置文件与收件人域进行映射。建议的设置如下所示：



The screenshot shows a table titled "Domain Mapping" with a message: "Domain Mapping configuration is not available since all profiles are already mapped". The table has three columns: "Mailbox Profile/Chained Profile", "Recipient Domain(s)", and "Delete". There is one row with "exchange" in the first column and "domain.com" in the second column. A delete icon is visible in the third column.

Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
exchange	domain.com	

- 单击**提交并提交更改**

在邮件策略中配置高级恶意软件防护(AMP)

在全局配置AMP和MAR后，您现在可以启用服务以发送邮件策略。

- 导航至**邮件策略>传入邮件策略**
- 单击**要自定义的策略**的“高级恶意软件防护”(Advanced Malware Protection)下的蓝色链接，为传入邮件策略自定义高级恶意软件防护设置。
- 为此最佳实践文档的目的，请单击启用文件信誉旁的单选按钮，然后选择启用文件分析：



The screenshot shows the "Advanced Malware Protection Settings" interface. It includes a "Policy" dropdown set to "DEFAULT". Under "Enable Advanced Malware Protection for This Policy:", there are three radio button options: "Enable File Reputation" (selected), "Enable File Analysis", and "No".

Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input type="radio"/> Enable File Analysis <input type="radio"/> No

- 建议在AMP结果中包含X报头，以生成消息。
- 接下来的三个部分允许您选择在附件因邮件错误、速率限制或AMP服务不可用而被视为不可扫描时ESA必须执行的操作。建议的操作是**将警告文本预置在消息主题上**：

Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is ▾
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is ▾
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is ▾
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>

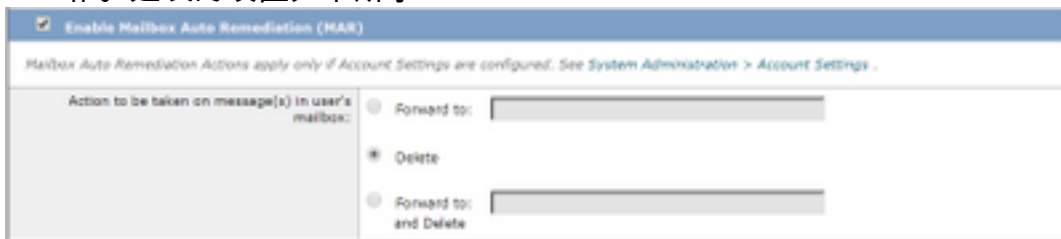
- 下一节将配置ESA，以在附件被视为恶意时丢弃邮件：

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: MALWARE DETECTED]
» Advanced	Optional settings.

- 建议的操作是隔离邮件(如果附件发送用于文件分析)：

Messages with File Analysis Pending:	
Action Applied to Message:	Quarantine ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT(S) MAY CONTAIN]
» Advanced	Optional settings.

- (仅适用于传入邮件策略) 配置在威胁判定变为恶意时对发送给最终用户的邮件执行的补救操作。建议的设置如下所示：

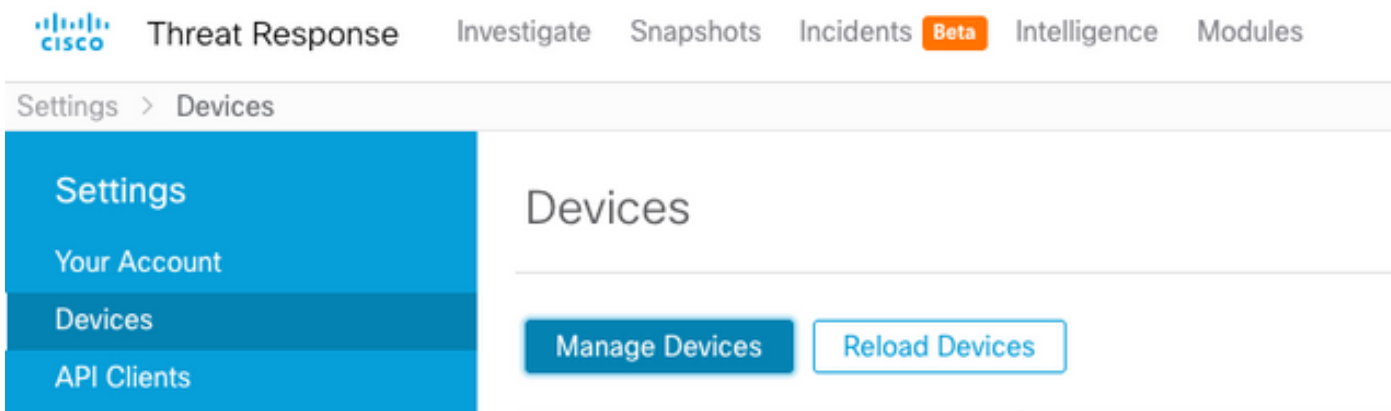


- 单击提交并提交更改

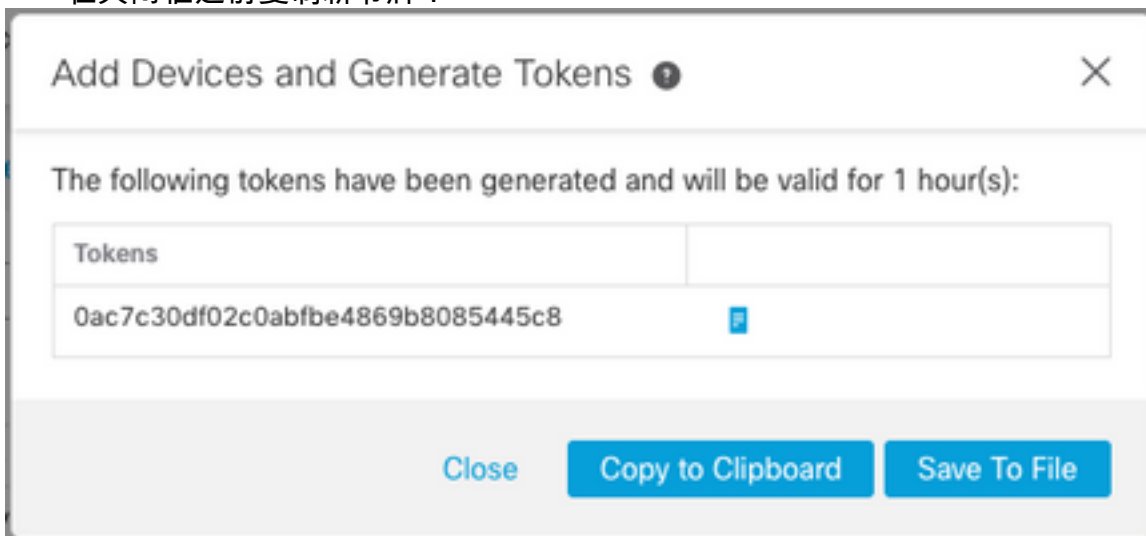
将SMA与思科威胁响应(CTR)集成

集成SMA电子邮件模块需要通过CTR使用安全服务交换(SSE)。SSE允许SMA向Exchange注册，并且您为思科威胁响应提供访问注册设备的明确权限。该过程包括通过令牌将SMA链接到SSE，该令牌在您准备好链接时生成。

- 在CTR门户(<https://visibility.amp.cisco.com>)上，使用您的用户凭证登录。
- CTR使用模块与包括ESA在内的其他思科安全产品集成。单击“Modules(模块)”选项卡。
- 选择“Devices”，然后单击“Manage Devices”：



- CTR将透视页面到SSE。
- 单击+图标生成新标记，然后单击继续。
- 在关闭框之前复制新令牌：



- 在您的SMA上，导航至**Management Appliances**选项卡 > **Network** > **Cloud Service Settings**
- 单击**Edit Setting**，确保Threat Response选项为**Enable**。
- 威胁响应服务器URL的默认选择是**AMERICAS**(api-sse.cisco.com)。对于欧洲客户，单击下拉菜单并选择**EUROPE**(api.eu.sse.itd.cisco.com):

- 单击**提交**并**提交更改**
- 将令牌密钥（您已从CTR门户生成）粘贴到云服务设置中，然后单击**注册**：

- 完成注册过程需要一段时间，请在几分钟后导航回此页面以再次检查状态。
- 返回**CTR > Modules > Device**，然后单击**Reload Device**按钮，确保SMA显示在列表中：

Name	Type	Version	Description	ID	IP Address
sma1	SMA	13.0.0-187	SMA	1	127.0.0.1

结论

本文档旨在说明邮件安全设备中思科高级恶意软件防护(AMP)的默认或最佳实践配置。其中大多数设置在入站和出站邮件策略中都可用，建议在两个方向上进行配置和过滤。