



## 监控系统状态

本章包含以下部分：

- [关于安全管理设备状态, on page 1](#)
- [在设备的新 Web 界面上监控服务状态, 第 2 页](#)
- [监控安全管理设备容量, on page 3](#)
- [监控受管设备的数据传输状态, on page 4](#)
- [查看受管设备的配置状态, on page 5](#)
- [监控报告数据可用性状态, on page 5](#)
- [监控邮件跟踪数据状态, 第 6 页](#)
- [监控受管设备的容量, on page 6](#)
- [识别有效的 TCP/IP 服务, on page 7](#)
- [在硬件故障期间更换托管设备, 第 7 页](#)

## 关于安全管理设备状态

默认情况下，从浏览器访问思科 安全邮件和 Web 管理器设备时会首先显示“系统状态 (System Status)”页面。（要更改登录页面，请参阅[设置首选项](#)。）

要在任何其他时间访问“系统状态” (System Status) 页面，请依次选择**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

在您启用监控服务并添加受管设备之前，只有“系统信息” (System Information) 部分提供状态信息。如果您运行了“系统设置向导” (System Setup Wizard)，启用了集中服务，并添加了受管设备，则“集中服务” (Centralized Services) 部分和“安全设备数据传输状态” (Security Appliance Data Transfer Status) 部分会填充数据。

状态信息包括以下内容：

- **集中服务：** 每项集中服务的状态，包括处理队列使用情况
- **系统正常运行时间：** 设备已持续运行多长时间
- **CPU 利用率：** 每项监控服务使用的 CPU 容量百分比
- **系统版本信息：** 型号、AsyncOS（操作系统）版本、构建日期、安装日期和序列号

### 相关主题

- [监控处理队列](#) , on page 3
- [监控 CPU 利用率](#) , on page 3
- [监控受管设备的数据传输状态](#) , on page 4

## 在设备的新 Web 界面上监控服务状态

现在，您可以在安全管理设备的新 Web 界面上监控受管设备的状态并管理集中服务。

您可以使用设备新 Web 界面上的**服务状态 (Service Status)** 选项卡来启用和禁用集中服务，例如邮件报告、邮件跟踪和隔离。

**邮件功能状态 (Email Feature Status)** 部分会显示已启用的服务，以及您为每项服务使用的许可证数量。单击**查看设备 (View Appliances)**，查看已添加的设备数量。这样会重定向至设备的旧版 Web 界面。有关详细信息，请参阅[关于添加受管设备](#)

您可以在设备的新 Web 界面的“服务状态” (Service Status) 页面上查看“文件分析” (File Analysis) 详细信息。要让组织中的所有内容安全设备都可以在云中显示有关从组织中的任何思科邮件安全设备或思科网络安全设备送交分析的文件的详细结果，您必须将所有受管设备加入到同一设备组。

您可以在“服务状态” (Service Status) 页面上启用和禁用以下集中服务：

- 集中报告

有关详细信息，请参阅 [在新 Web 界面上启用集中邮件报告](#)。

- 集中邮件跟踪

有关详细信息，请参阅 [在新 Web 界面上启用集中邮件跟踪](#)。

- 集中垃圾邮件隔离区

有关详情，请参阅：

- [在新 Web 界面上启用和配置垃圾邮件隔离区](#)。
- [通知最终用户被隔离的邮件](#)。
- [配置最终用户访问垃圾邮件隔离区的权限](#)。
- [在新 Web 界面上启用安全列表和阻止列表](#)。

- 集中策略、病毒和病毒爆发隔离区

有关详细信息，请参阅 [在设备的新 Web 界面上启用集中策略、病毒和隔离区功能](#)。

- 安全列表和阻止列表

有关详细信息，请参阅 [在新 Web 界面上启用安全列表和阻止列表](#)。

# 监控安全管理设备容量

- [监控处理队列](#) , on page 3
- [监控 CPU 利用率](#) , on page 3

## 监控处理队列

您可以定期检查用于邮件和 Web 报告的处理队列百分比，以确定设备是否以最佳容量运行。

在等待安全管理设备处理时，处理队列会存储集中报告和跟踪文件。通常，安全管理设备会收到批量报告和跟踪文件以进行处理。处理队列中的报告和跟踪文件百分比通常随着从托管设备发送文件并且由安全管理设备进行处理而浮动。



**Note** 处理队列百分比衡量队列中的文件数。不考虑文件大小。百分比只是大概估计的安全管理设备的处理负载。

- 步骤 1** [仅限新 Web 界面] 在安全管理设备上，从产品下拉列表中选择**邮件 (Email)**，然后选择**服务状态 (Service Status)**。
- 步骤 2** 在安全管理设备上，选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **系统状态 (System Status)**。
- 步骤 3** 在页面顶部的**集中服务**部分中，查看以下各项的处理队列百分比：
  - a) 集中报告（“邮件安全”子部分）
  - b) 集中邮件跟踪
  - c) 集中报告（“网络安全”子部分）
- 步骤 4** 如果处理队列使用百分比连续几小时或几天一直保持较高，则系统将满容量或超容量运行。  
这种情况下，请考虑从安全管理设备移除一些托管设备，安装额外的安全管理设备，或同时实施这两种措施。

## 监控 CPU 利用率

要查看安全管理设备针对每项集中服务使用的 CPU 容量百分比，请执行以下操作：

- 步骤 1** [仅限新 Web 界面] 在安全管理设备上，从产品下拉列表中选择**邮件 (Email)**，然后选择**服务状态 (Service Status)**。
- 步骤 2** 依次选择**管理设备 (Management Appliance)** > **集中服务 (Centralized Services)** > **系统状态 (System Status)**。
- 步骤 3** 滚动到系统信息 (**System Information**) 部分并查看 **CPU 利用率 (CPU Utilization)** 子部分。

CPU 利用率百分比表示安全管理设备的 CPU 处理投入到每个主要集中服务的部分。某些服务的利用率百分比可以合并。例如，邮件报告合并并在“报告服务”下，而垃圾邮件、策略、病毒和病毒爆发隔离区合并并在“隔离区服务”下。安全管理设备的其他操作组合在常规标题“安全管理设备 (Security Management appliance)”下。

步骤 4 刷新浏览器显示可查看最新数据。

CPU 利用率会不断变化。

## 监控受管设备的数据传输状态

要执行集中管理功能，安全管理设备需要将托管设备中的数据成功传输到安全管理设备。“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分提供有关安全管理设备管理的每台设备的状态信息。

默认情况下，“安全设备数据传输状态 (Security Appliance Data Transfer Status)”部分最多显示十台设备。如果安全管理设备管理的设备数量超过十台，可以使用“显示的项目 (Items Displayed)”菜单选择要显示的设备数量。



### Note

“系统状态 (System Status)”页面顶部的“服务 (Services)”部分显示有关数据传输状态的摘要信息。“安全设备数据传输状态” (Security Appliance Data Transfer Status) 部分提供特定于设备的数据传输状态。

在“系统状态” (System Status) 页面的“安全设备数据传输状态” (Security Appliance Data Transfer Status) 部分，您可以查看特定设备的连接状态问题。有关设备上每项服务的状态的详细信息，请单击设备名称以查看设备的“数据传输状态” (Data Transfer Status) 页面。

“数据传输状态: *Appliance\_Name*” (Data Transfer Status: *Appliance\_Name*) 页面显示每项监控服务发生最后一次数据传输的时间。

邮件安全设备的数据传输状态可以是下列值之一：

- **未启用**：邮件安全设备上未启用监控服务。
- **从未连接**：在邮件安全设备上启用了监控服务，但邮件安全设备和安全管理设备之间尚未建立连接。
- **正在等待数据**：邮件安全设备已连接到正在等待接收数据的安全管理设备。
- **已连接和传输数据**：已在邮件安全设备和安全管理设备之间建立连接，并且数据已成功传输。
- **文件传输失败**：已在邮件安全设备和安全管理设备之间建立连接，但数据传输失败。

网络安全设备的数据传输状态可以是下列值之一：

- **未启用**：未为网络安全设备启用集中配置管理器。
- **从未连接**：为网络安全设备启用了集中配置管理器，但网络安全设备和安全管理设备之间尚未建立连接。
- **正在等待数据**：网络安全设备已连接到等待接收数据的安全管理设备。
- **已连接和传输数据**：已在网络安全设备和安全管理设备之间建立连接，并且数据已成功传输。

- **配置推送失败**: 安全管理设备已尝试将配置文件推送到网络安全设备, 但传输失败。
- **等待配置推送 (Configuration push pending)**: 安全管理设备正在向网络安全设备推送配置文件。
- **等待配置推送 (Configuration push pending)**: 安全管理设备已成功地将配置文件推送到网络安全设备。

数据传输问题可以反映临时网络问题或设备配置问题。第一次向安全管理设备添加托管设备时, “从未连接 (Never connected)” 和 “正在等待数据 (Waiting for data)” 状态是正常的临时状态。如果状态最终没有变为 “已连接和传输数据 (Connected and transferred data)”, 则数据传输状态可能指示配置问题。

如果设备出现 “文件传输失败” (File transfer failure) 状态, 请监控设备以确定故障是由网络问题还是设备配置问题导致。如果没有网络问题阻止数据传输, 但是状态未变成 “已连接并已传输数据” (Connected and transferred data), 则您可能需要更改设备配置以启用数据传输。

## 查看受管设备的配置状态

您可以通过以下方式之一查看受管设备的配置状态:

- [仅限新 Web 界面] 在安全管理设备上, 从产品下拉列表中选择 **邮件 (Email)**, 然后选择 **服务状态 (Service Status)**。
- 在安全管理设备上, 选择 **管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)**。

“集中服务状态 (Centralized Service Status)” 部分显示启用的服务, 以及用于每项服务的许可证数量。“安全设备” (Security Appliances) 部分列出您已添加的设备。复选标记表示已启用的服务, “已建立连接?” (Connection Established?) 列显示是否已正确配置文件传输访问权限。

### 相关主题

- [指定处理所放行邮件的备用设备](#)
- [关于添加受管设备](#)

## 网络安全设备的其他状态信息

有关网络安全设备的其他状态信息, 请参阅 [查看各台网络安全设备的状态](#)。

## 监控报告数据可用性状态

通过安全管理设备, 可以监控指定期间报告数据的可用性。请参阅设备适当的部分:

- [监控邮件安全报告数据可用性, on page 6](#)

## 监控邮件安全报告数据可用性

要在安全管理设备上监控来自邮件安全设备的报告数据，请依次查看**邮件 > 报告 > 报告数据可用性**页面。

在**报告数据可用性**页面中，您可以查看在指定的时间段安全管理设备从邮件安全设备收到的报告数据百分比。条形图表示在该时间范围内收到的数据的完整度。

可以监控前一天、前一周、前一个月或前一年的报告数据可用性。如果安全管理设备从邮件安全设备接收的报告数据少于 100%，可以立即得知您的数据不完整。使用数据可用性信息可验证报告数据，并解决系统问题。

## 监控网络安全报告数据可用性

要在安全管理设备上监控来自网络安全设备的报告数据，请依次查看**网络 > 报告 > 数据可用性**页面。

在“数据可用性 (Data Availability)”页面，可以更新和排序数据，以便您实时了解资源利用率和网络流量问题点。



### Note

在“Web 报告数据可用性” (Web Reporting Data Availability) 窗口中，仅当“Web 报告” (Web Reporting) 和“邮件报告” (Email Reporting) 均被禁用时，“Web 报告” (Web Reporting) 才会显示为已禁用。

所有数据资源利用率和网络流量问题所在均会在该页面上显示。通过单击其中一个列出的网络安全设备链接，您可以查看该设备的报告数据可用性。

可以监控前一天、前一周、前一个月或前一年的报告数据可用性。如果安全管理设备从网络安全设备接收的报告数据少于 100%，可以立即得知您的数据不完整。使用数据可用性信息可验证报告数据，并解决系统问题。

如果在计划报告内为 URL 类别使用“数据可用性” (Data Availability)，并且在任意设备之间存在着数据差异，则会在页面底部显示以下信息：“Some data in this time range was unavailable”。如果没有数据差异，则不会显示任何内容。

有关网络安全设备上的“数据可用性”页面的详细信息，请参阅“[数据可用性](#)”页面。

## 监控邮件跟踪数据状态

要监控邮件跟踪数据的状态，请依次查看**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪数据可用性 (Message Tracking Data Availability)**页面。

## 监控受管设备的容量

您可以从安全管理设备监控托管设备的容量。可以检查所有邮件或网络安全设备的统一容量，也可以查看单个设备的容量。

查看容量	请参阅
托管网络安全设备	<a href="#">系统容量页面</a>
托管邮件安全设备	<a href="#">系统容量页面</a>

## 识别有效的 TCP/IP 服务

要识别安全管理设备使用的有效 TCP/IP 服务，请在命令行界面中使用 `tcp services` 命令。

## 在硬件故障期间更换托管设备

如果由于硬件故障或其他原因必须更换托管设备，则被替换的设备中的数据不会丢失，但数据在安全管理设备上无法正确显示。

更换托管设备后，将新设备添加到 SMA 上的主机列表中，并将其连接到新设备。如果 IP 地址保持不变，请将旧主机条目上的 IP 地址更改为非现有值。

