

目录

[简介](#)

[什么是级别在ESA的管理访问联机？](#)

[相关信息](#)

简介

本文描述多种管理访问访问级别或者预定义的用户角色，是可行的在电子邮件安全工具(ESA)。

什么是级别在ESA的管理访问联机？

当您创建新用户帐户时，您分配用户到一个预定义的或一个自定义用户角色。每个用户角色包含不同的级别在OS和设备访问内的权限，如下：

管理员

与管理员角色的用户帐户有对系统的所有配置设置的完全权限。然而，只有管理员用户访问与操作员角色的用户帐户限制从：

- 创建或编辑用户帐户。
- 发出resetconfig命令。
- 升级设备。

操作员

- 发出systemsetup命令或运行系统设置向导。
- 发出adminaccessconfig命令。
- 执行一些检疫功能(包括创建，编辑，删除和集中的检疫)。
- 除用户名和密码之外的正在修改的LDAP服务器配置文件设置，如果LDAP为外部验证

否则，他们有权限和管理员角色一样。

与只读操作员角色的用户帐户访问查看的配置信息。有只读操作员角色的用户能做和提交有此角色的用户不能访问以下：

只读操作员

- 文件系统、FTP或者SCP。
- 创建，编辑，删除或者集中的检疫的设置。

访客

与访客角色的用户帐户能只查看状态信息。如果访问在检疫，启用有访客角色的用户能也与技术人员角色的用户帐户能执行系统升级，重新启动设备和管理功能键。技术人员可也

- 挂起电子邮件交付和接收。
- 查看workqueue和监听程序状态。
- 保存并且给配置文件发电子邮件。
- 备份safelists和blocklists。技术人员不能恢复这些列表。
- 从集群断开设备。
- 启用或禁用思科技术支持的远程服务访问。
- 提高支持请求。

技术人员

与支持中心用户角色的用户帐户限制对：

支持中心用户

- 消息跟踪。
- 管理在检疫的消息。

有此角色的用户不能对系统的其余的访问，包括CLI。在有此角色的一个用户能管理他们前与一个自定义用户角色的用户帐户能只访问电子邮件安全功能分配到角色。这些功能可以

自定义用户角色

注意： 用户分配到自定义角色不能访问CLI。

系统的默认用户用户帐号， admin，有所有管理权限。管理员用户用户帐号不可能删除，但是您能更改密码和锁定帐户。

虽然没有限制到您在设备能创建用户帐户的数量，您不能创建与由系统保留的名称的用户帐户。例如，您不能创建名为“操作员的”用户帐户或“请根源”。

每上述定义的所有角色能访问GUI和CLI，除了支持中心用户角色和自定义用户角色，能只访问GUI。

相关信息

- [思科电子邮件安全工具-最终用户指南](#)
- [技术支持和文档 - Cisco Systems](#)