



## 用户角色

- [CDO中的用户角色, on page 1](#)

### CDO中的用户角色

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户 ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当接口或文档提及只读用户、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

### 多云防御 中的角色

在用户通过 多云防御 门户访问 多云防御 租户时，角色扮演着重要角色。角色是授予用户一组权限的权限。

有三个可用的角色：

- 超级管理员 (admin\_super)。
- 仅编辑管理员 (admin\_rw)。
- 只读管理员 (admin\_read-only)。

有两个权限定义：

- 修改 - 读取、写入、编辑和删除。
- 读 - 只读。

下表概述了与每个角色关联的每个设置的权限：

设置	超级管理员 (admin_super)	仅编辑 (admin_rw)	只读 (admin_read-only)
管理			

设置	超级管理员 (admin_super)	仅编辑 (admin_rw)	只读 (admin_read-only)
用户	修改	修改 (超级管理员除外)	读
MFA 启用/禁用	修改	修改 (超级管理员除外)	读
重置 MFA	修改	修改 (超级管理员除外)	读
API 密钥	修改	修改	已读
角色	读	读	读
账户 > 应用标签	修改	修改	已读
账户 > 邮件域	修改	已读	读
系统	读	读	读
电表	读	读	读
<b>警报配置文件</b>			
服务	修改	修改	已读
警报	修改	修改	已读

只能为多云防御租户中的一(1)位用户分配超级管理员角色。此用户被视为账户的**所有者**，与AWS账户或Linux根账户的所有者同义。应为所有其他用户分配读/写管理员或只读管理员角色。

超级管理员角色由多云防御分配，并授予在创建多云防御租户时创建的第一个用户。如果需要对超级管理员用户进行任何更改，请联系[多云防御支持人员](#)。

## 当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。