配置FMC域用户访问和角色(&N)

问题

本文档介绍如何为FMC中跨全局域和子域的多个用户配置不同的用户权限。

环境

- 思科安全防火墙管理中心(FMC)- 7.6.4（适用于所有FMC）
- 具有全局域和子域的多域部署
- 多个FTD设备分配给不同的子域
- 多个用户需要不同的权限级别

分辨率

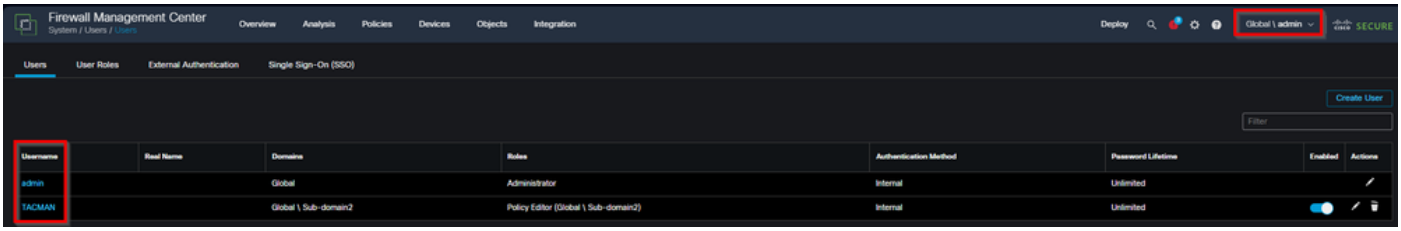
本文档解决了如何在FMC中跨全局域和子域为多个用户配置不同的用户权限，从而能够限制域之间的访问并限制特定用户的全局域访问。Cisco FMC支持跨多个域的精细用户角色分配，并能够限制域之间的访问。该配置涉及在特定域中创建用户，并分配适当的角色来控制访问级别。

创建用户和域访问行为

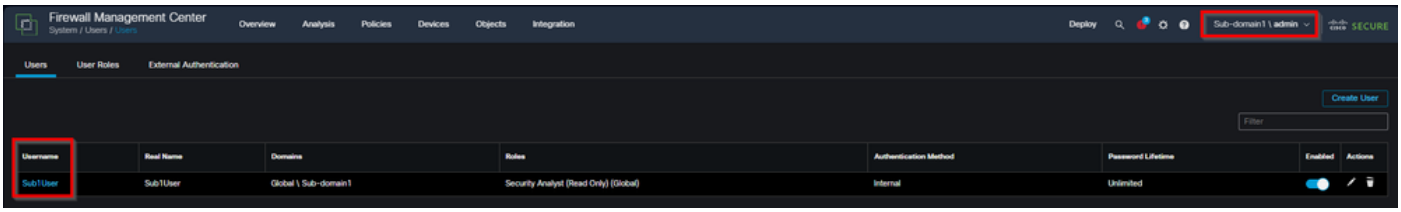
FMC用户管理系统根据用户的创建位置以不同方式运行：

在子域中创建的用户

- 在子域中直接创建的用户仅在特定域中可见：

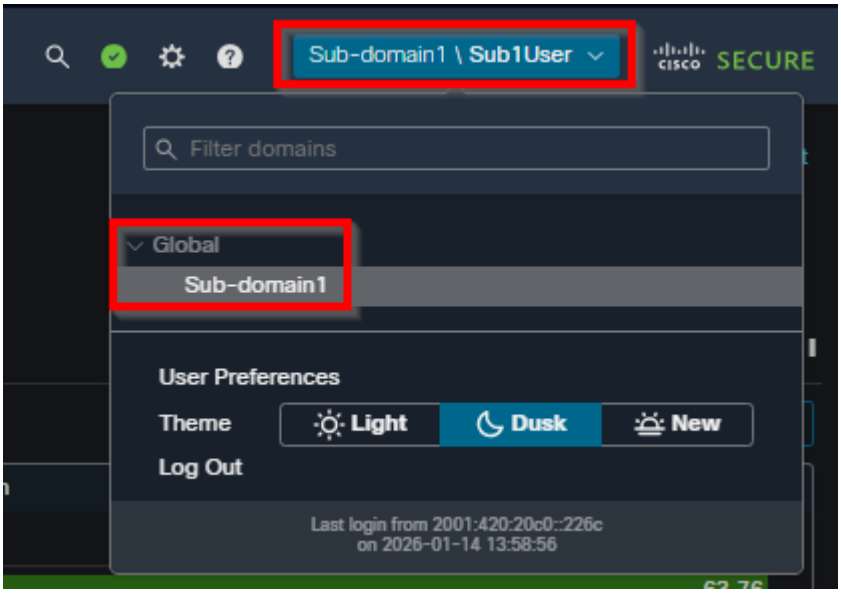


inline_image_0.png



inline_image_1.png

- 这些用户必须使用域规范格式subdomain\username登录。
- 访问自动限制到创建用户的域：

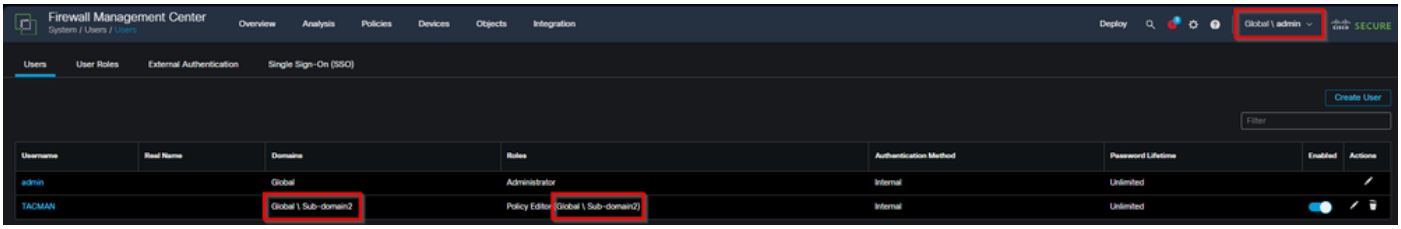


inline_image_2.png

- 在子域中创建的自定义角色仅适用于该域。

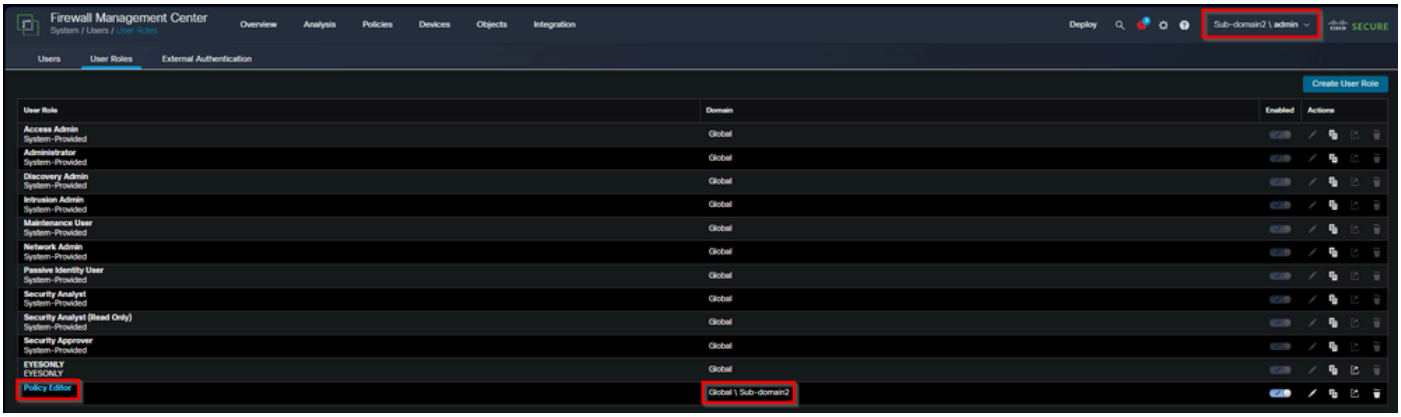
在全局域中创建的用户：

- 从全局域创建的用户仅可使用其用户名登录，即使其角色仅在子域中也是如此。
- 这些用户在“全局域用户”列表中保持可见：



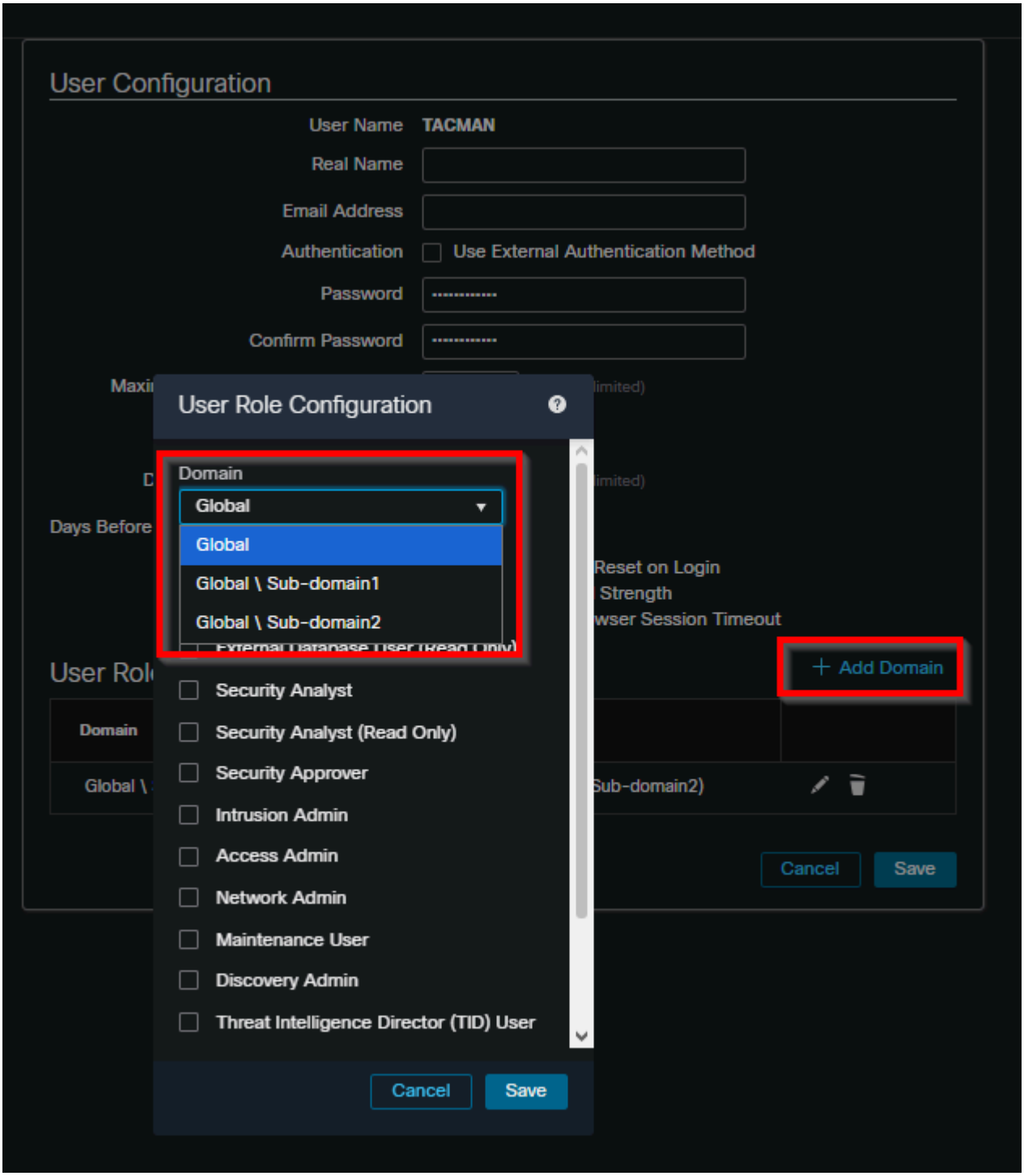
inline_image_3.png

- 可以为任何后代域分配角色：



inline_image_4.png

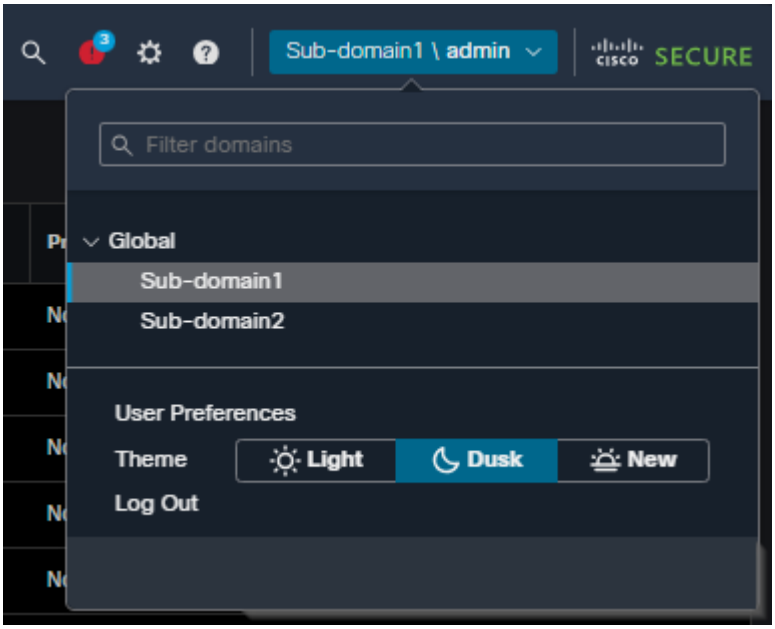
- 可通过角色分配限制对特定子域的访问：



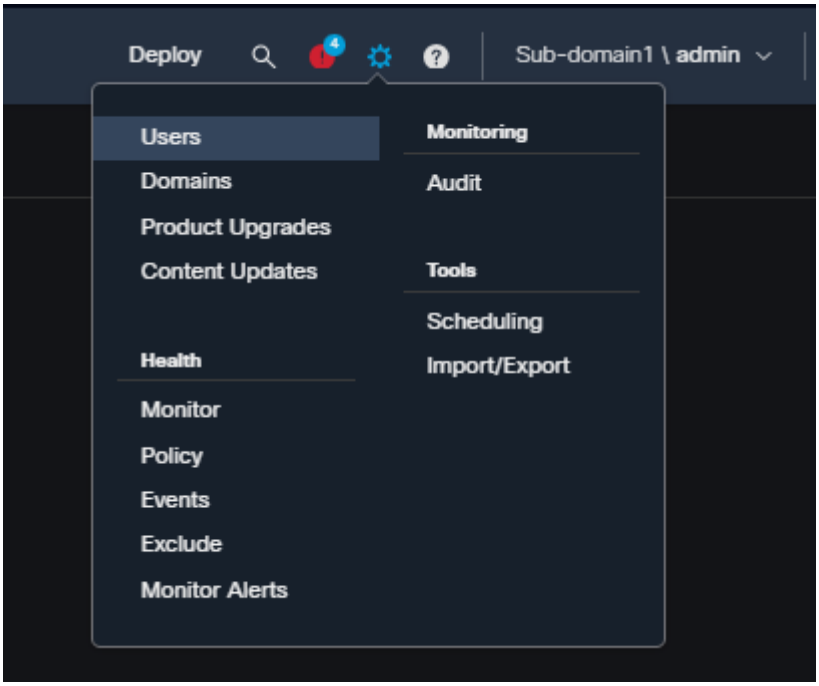
inline_image_5.png

子域用户限制的配置步骤

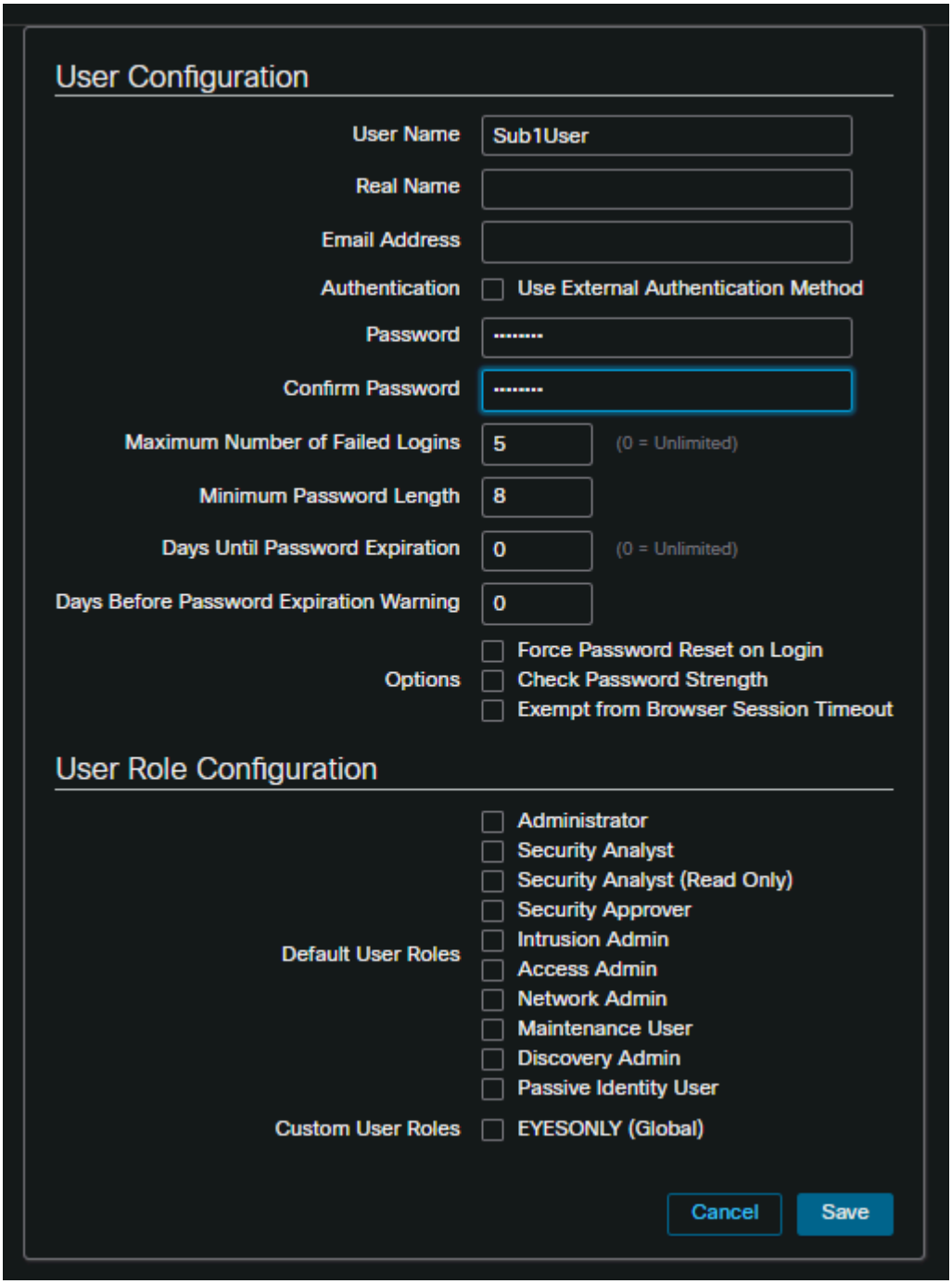
- 导航到必须限制访问的特定子域，并在系统/用户下创建用户帐户。



inline_image_6.png

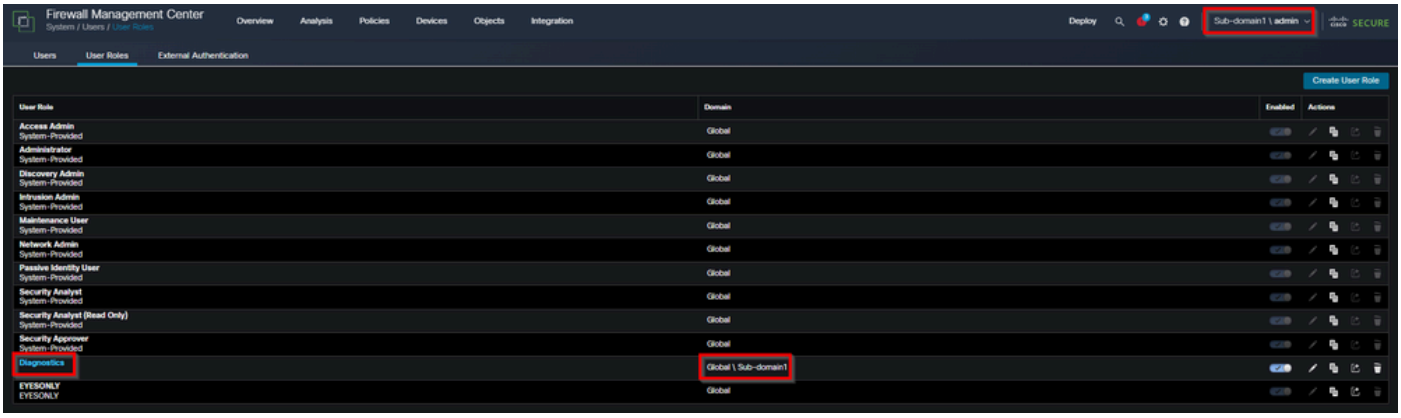


inline_image_7.png



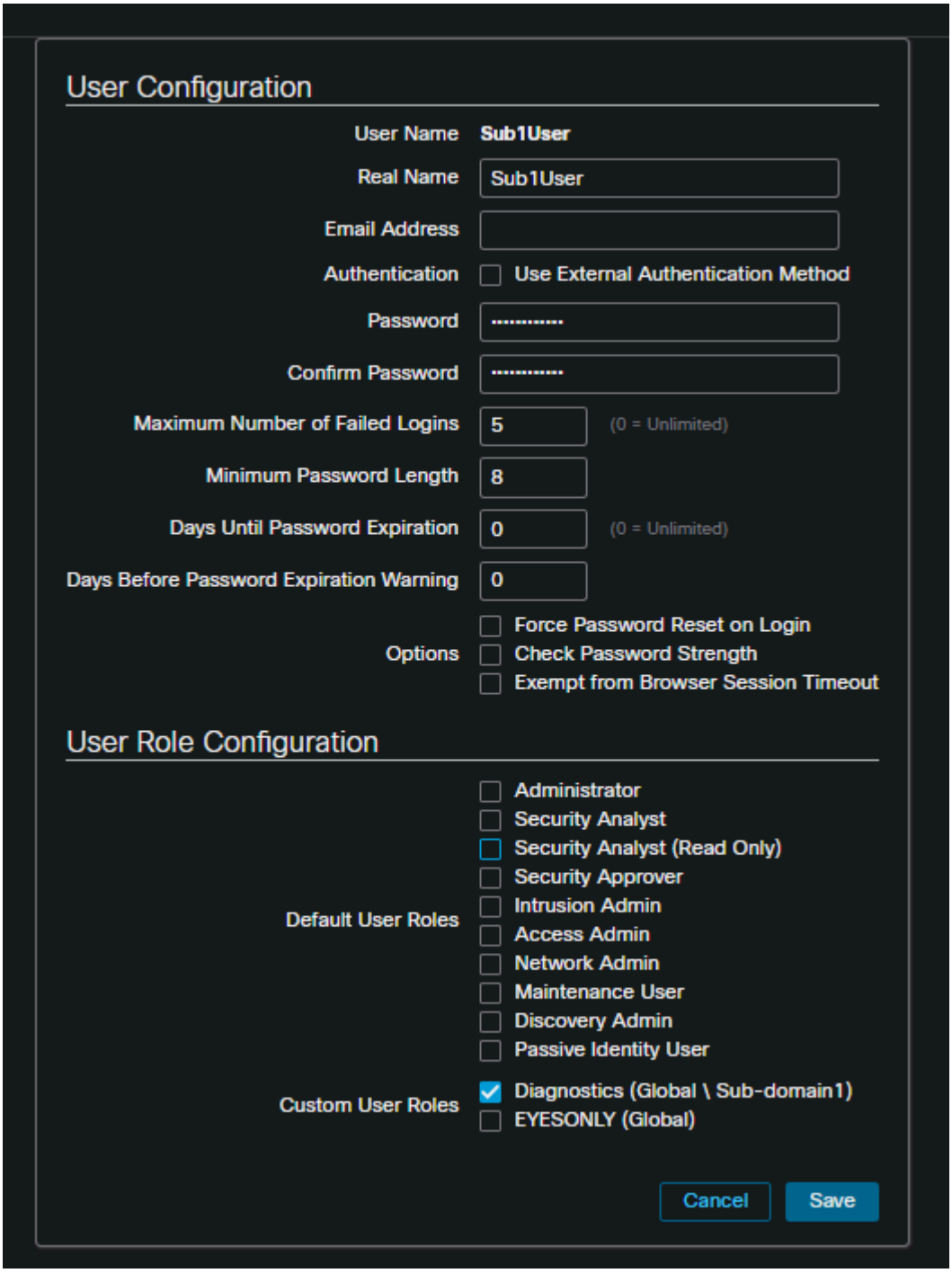
inline_image_8.png

- 在系统/用户角色下的子域中创建自定义角色。在子域中创建的自定义用户角色仅在该域中可用，不能从其他域访问。



inline_image_9.png

- 将自定义角色分配给用户。用户仅继承对创建用户和角色的域的权限。



inline_image_10.png

- 子域用户的用户登录格式。在子域中创建的用户必须使用此登录格式：

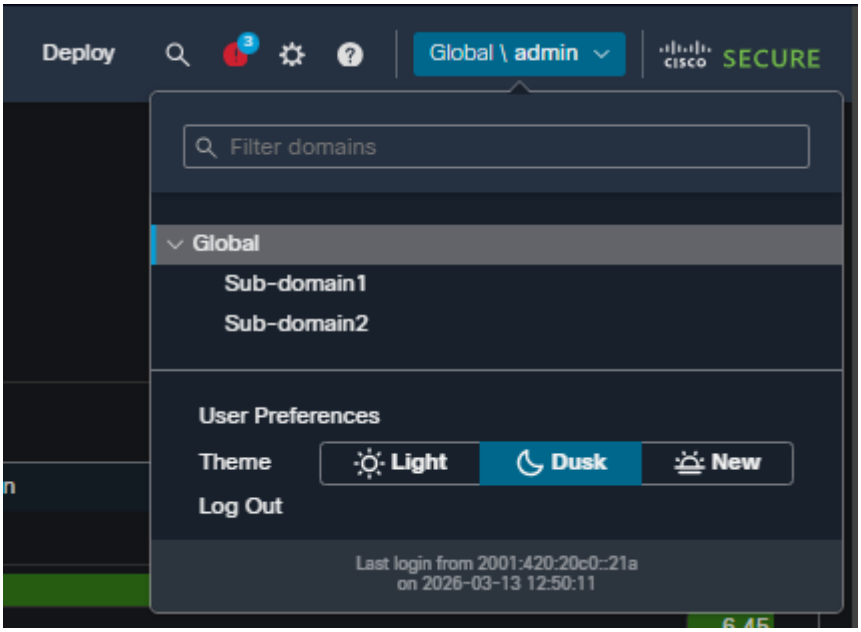
用户名：子域\用户名

密码：[用户密码]

inline_image_11.png

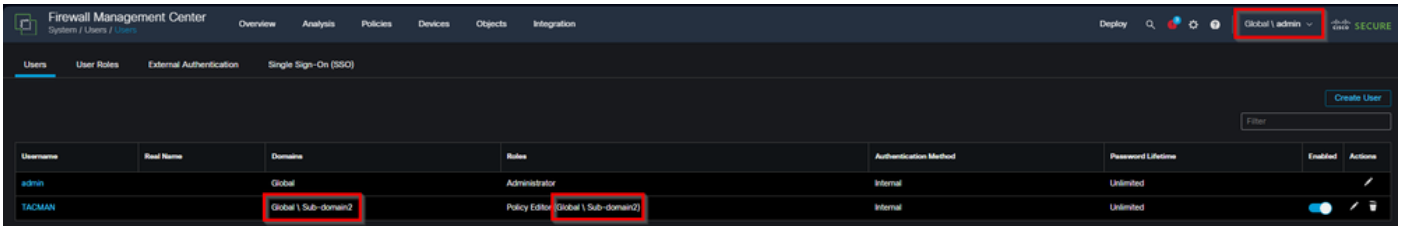
具有子域限制的全局域用户的配置步骤

- 在“系统/用户”下的“全局域”中创建用户。使用具有“全局域”访问权限的管理帐户创建用户。

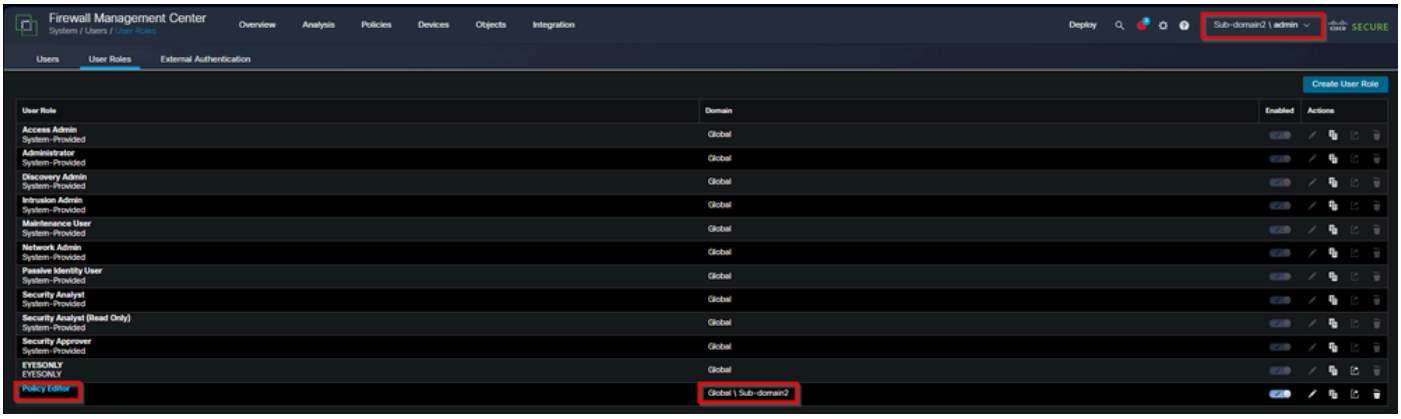


inline_image_12.png

- 仅为“系统/用户”下的特定子域分配角色。在用户配置中，只为目标子域分配角色，而不提供任何全局域权限。



inline_image_3.png



inline_image_14.png

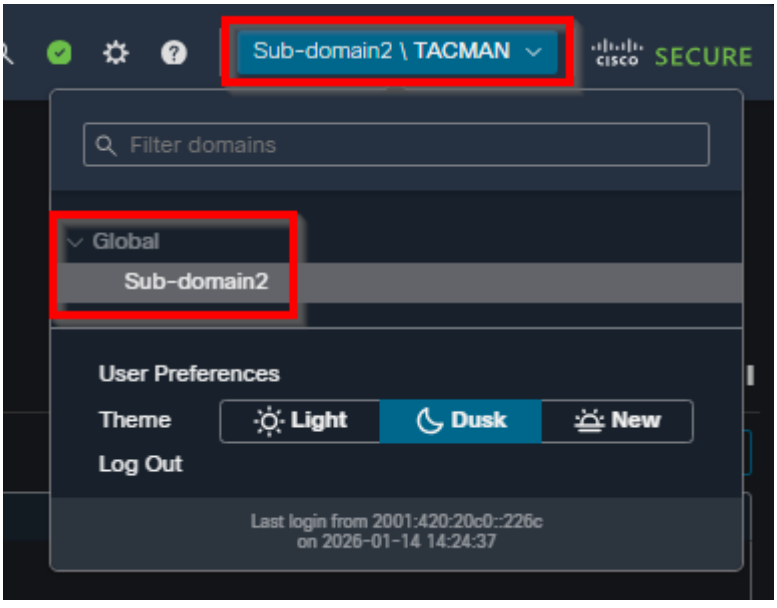
- 这些用户只能使用其用户名登录，无需指定域：

用户名：username

密码：[用户密码]

inline_image_15.png

- 用户仅有权访问专门分配了角色的子域，无权访问全局域或其他子域。



inline_image_16.png

角色分配灵活性

用户可以在每个域中具有不同的权限：

- 全局域中的只读权限和后代域中的管理员权限
- 在特定子域中没有具有完全管理员权限的全局域访问
- 一个子域中的策略编辑器权限，无法访问其他子域

外部用户注意事项

对于外部用户（LDAP或RADIUS身份验证）：

- 如果通过组成员资格或用户属性分配用户角色，则无法删除最低访问权限。
- 可以分配比默认用户角色更大的范围的其他权限。
- 外部身份验证对象仅在创建它们的域中可用。
- 单个用户权限的配置范围必须大于默认用户角色，才能进行适当的限制。

限制和注意事项

- 祖先域中创建的自定义用户角色不能从后代域中编辑。
- 外壳身份验证仅在全局域中可用，在子域中不可用。
- 用户首选项和控制面板设置适用于帐户有权访问的所有域。
- 对用户的权限修改单独配置，而不是分组或批量方式配置。

原因

这一要求源于在多域FMC部署中实施精细访问控制的需要，在该部署中，用户需要对全局域和子域进行不同级别的访问，并在域之间实施特定限制以维护安全边界。

相关内容

- 思科安全防火墙管理中心管理指南7.6:用户
- 思科安全防火墙管理中心管理指南7.6:创建自定义用户角色
- 思科安全防火墙管理中心管理指南7.6:添加或编辑内部用户
- 思科安全防火墙管理中心管理指南7.6:用户和域
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。