管理用户访问

- 用户访问概述， 第 1 页
- 用户访问先决条件， 第 5 页
- 用户访问配置任务流程 ， 第 5 页
- 禁用非活动用户帐户 ， 第 13 页
- 设置远程帐户， 第 14 页
- 标准角色和访问控制组， 第 14 页

用户访问概述

通过配置以下项目，管理用户对 Cisco Unified Communications Manager 的访问：

- 访问控制组
- 角色
- 用户等级

访问控制组概述

访问控制组是分配给这些用户的用户和角色的列表。当您将最终用户、应用程序用户或管理员用户分配给访问控制组时，用户将获得与组关联的角色的访问权限。您可以通过将具有相似访问需求的用户分配给仅具有他们所需角色和权限的访问控制组来管理系统访问。

有两种类型的访问控制组：

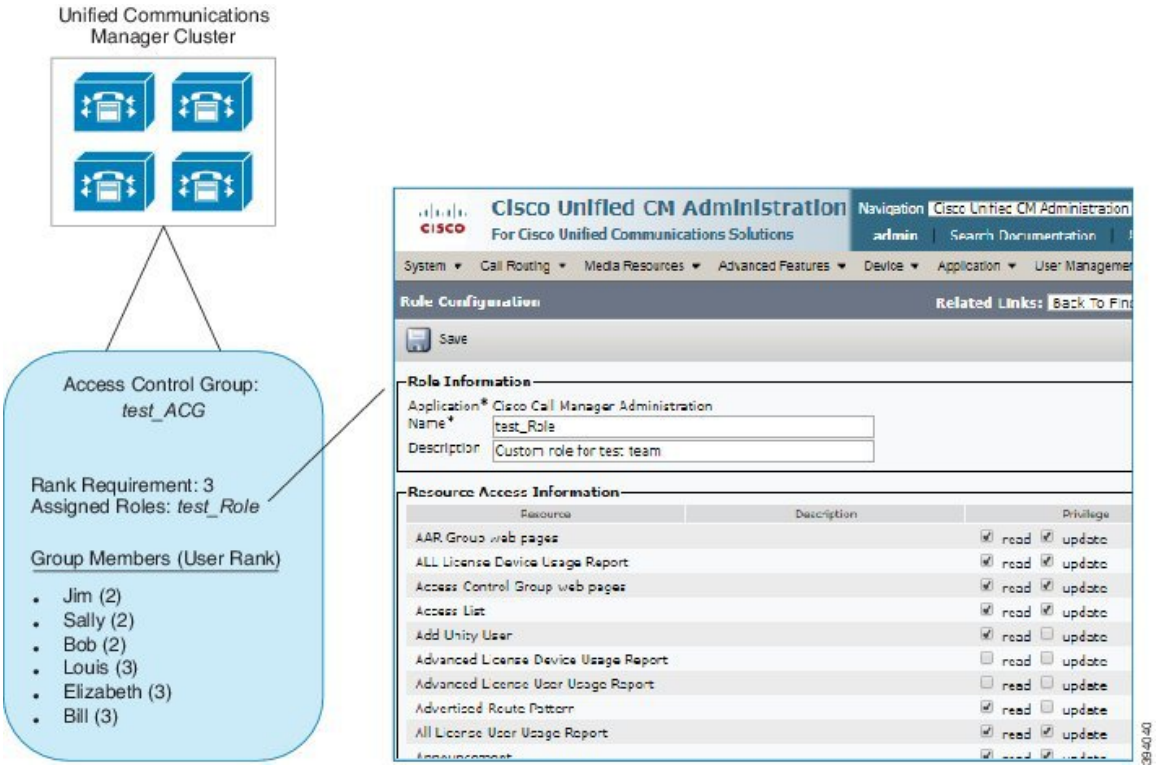
- 标准访问控制组—这些是预定义的默认组，其角色分配能够满足一般的部署需求。您不能编辑标准组中的角色分配。不过，除了编辑用户等级要求之外，还可以添加和删除用户。有关标准访问控制组及其关联角色的列表，请参阅标准角色和访问控制组， 第 14 页。
- 自定义访问控制组—当所有标准组都不包含满足您需求的角色权限时，可以创建自己的访问控制组。

用户等级框架提供一组对可以分配给用户的访问控制组的控制。要分配给访问控制组，用户必须满足该组的最低等级要求。例如，如果最终用户的用户等级为 4，则该用户只可以分配到最低等级要求介于 4 到 10 之间的访问控制组。不能将他们分配给最低等级为 1 的组。

示例 - 访问控制组的角色权限

以下示例说明了测试团队的成员被分配给访问控制组 **test_ACG** 的群集。右侧的屏幕截图显示了 test_Role（即与访问控制组关联的角色）的访问设置。另请注意，访问控制组的最低等级要求为 3。所有组成员的等级必须介于 1-3 之间，才能加入组。

图 *1:* 访问控制组的角色权限



角色概述

用户通过与用户所属的访问控制组相关联的角色获得系统访问特权。每个角色包含一组附加到特定资源或应用程序的权限，例如 Cisco Unified CM 管理或 CDR 分析和报告。对于 Cisco Unified CM 管理之类的应用程序，角色可能包含允许您在应用程序中查看或编辑特定 GUI 页面的权限。您可以分配给资源或应用程序的权限级别有三个：

- 读取—允许用户查看资源的设置。
- 更新—允许用户编辑资源的设置。
- 无权限—如果用户既没有读取权限，也没有更新权限，则其无权查看或编辑给定资源的设置。

角色类型

在预配置用户时，您必须确定要应用的角色，然后将用户分配到包含该角色的访问控制组。Cisco Unified Communications Manager 中有以下两种主要类型的角色：

- 标准角色—这些是预先安装的默认角色，旨在满足常见部署的需求。您无法编辑标准角色的权限。
- 自定义角色—当没有标准角色拥有您所需的权限时，可创建自定义角色。此外，如果需要更精细级别的访问控制，可以应用高级设置来控制管理员编辑关键用户设置的能力。请参阅以下部分了解详细信息。

高级角色设置

对于自定义角色，您可以将详细的控制级别添加到**应用程序用户配置**和**最终用户配置**窗口上的所选字段。

在**高级角色配置**窗口中，您可以配置对 Cisco Unified CM 管理的访问权限，同时限制对以下任务的访问：

- 添加用户
- 编辑密码
- 编辑用户等级
- 编辑访问控制组

下表详细说明您可以通过此配置应用的更多控制：

表 *1:* 高级资源访问信息

高级资源	访问控制
权限信息	控制添加或编辑访问控制组的能力： • **查看** - 用户可以查看访问控制组，但不能添加、编辑或删除访问控制组。 • **更新** - 用户可以添加、编辑或删除访问控制组。 **注释** 当两个值都不选时，**权限信息**部分不可用。 **注释** 如果选择**查看**，**用户可以更新自己的权限信息**字段设置为**否**并禁用。如果希望能够编辑此字段，必须将**权限信息**字段设置为**更新**。

高级资源	访问控制
用户可以更新自己的权限信息	控制用户编辑自己的访问权限的能力： • **是** - 用户可以更新自己的权限信息。 • **否** - 用户无法更新自己的权限信息。不过，用户可以查看或修改等级相同或较低的用户的权限信息。 **注释** 如果未选中**权限信息更新**复选框，则**用户可以更新自己的权限信息**字段设置为**否**并禁用。
用户等级	控制更改用户等级的能力： • **查看** - 用户可以查看用户等级但不能进行更改。 • **更新** - 用户可以更改用户等级。 **注释** 当两个值都不选时，**用户等级**部分不可用。 **注释** 如果选择**查看**，**用户可以更新自己的用户等级**字段设置为**否**并禁用。如果希望能够编辑此字段，必须将**用户等级**字段设置为**更新**。
用户可以更新自己的用户等级	控制用户编辑自己用户等级的能力： • **是** - 用户可以更新自己的用户等级。 • **否** - 用户无法更新自己的用户等级。不过，用户可以查看或修改等级相同或较低的用户的等级。 **注释** 如果未选中**用户等级更新**复选框，则**用户可以更新自己的用户等级**字段设置为**否**并禁用。
添加新用户	控制添加新用户的能力： • **是** - 用户可以添加新用户。 • **否** - **新增**按键不可用。
密码	控制更改密码的能力： • **是** - 用户可以在**应用程序用户信息**部分更改用户密码。 • **否** - **应用程序用户信息**部分的**密码**和**确认密码**不可用。

用户等级概述

用户等级分层结构提供了一组控制机制，管理员可以通过访问控制组分配给最终用户或应用程序用户。

在预配置最终用户或应用程序用户时，管理员可以为用户分配用户等级。管理员还可以为每个访问控制组分配用户等级要求。添加用户以访问控制组时，管理员只能将用户分配给用户的用户等级符合等级要求的组。例如，管理员可以将用户等级为 3 的用户分配给用户等级要求介于 3 到 10 之间的访问控制组。但是，管理员无法将该用户分配给用户等级要求为 1 或 2 的访问控制组。

管理员可以在**用户等级配置**窗口中创建自己的用户等级分层结构，并可在预配置用户和访问控制组时使用该分层结构。请注意，如果未配置用户等级分层结构，或者您在预配置用户或访问控制组时不指定用户等级设置，则系统会为所有用户和访问控制组分配默认的用户等级 1（可能的最高等级）。

用户访问先决条件

确保查看您的用户需求，了解用户所需的访问级别。您需要分配具有用户所需访问权限的角色，但这些角色不提供对用户不应访问的系统的访问权限。

在创建新角色和访问控制组之前，查看标准角色和访问控制组的列表，以验证现有访问控制组是否具有所需的角色和访问权限。有关详细信息，请参阅标准角色和访问控制组 ， 第 14 页。

用户访问配置任务流程

执行以下任务以配置用户访问。

开始之前

如果要使用默认角色和访问控制组，可以跳过创建自定义角色和访问控制组的任务。您可以将用户分配给现有的默认访问控制组。

过程

	命令或操作	目的
步骤 1	配置用户等级分层结构 ， 第 6 页	设置用户等级分层结构。请注意，如果跳过此任务，所有用户和访问控制组将分配给默认的用户等级 1（最高等级）。
步骤 2	创建自定义角色 ， 第 6 页	如果默认角色没有您所需的访问权限，请创建自定义角色。
步骤 3	为管理员配置高级角色 ， 第 7 页	可选。自定义角色中的高级权限可让您控制管理员编辑关键用户设置的能力。
步骤 4	创建访问控制组 ， 第 8 页	如果默认组没有您所需的角色分配，可以创建自定义访问控制组。
步骤 5	向访问控制组分配用户 ， 第 8 页	从标准或自定义访问控制组添加或删除用户

	命令或操作	目的
步骤 6	为访问控制组配置重叠权限策略，第 9 页	可选。如果用户被分配到权限相互冲突的多个访问控制组，则使用此设置。

配置用户等级分层结构

此程序用于创建自定义用户等级分层结构。

注释 如果未配置用户等级分层结构，则默认情况下系统会为所有用户和访问控制组的用户等级分配1（可能的最高等级）。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户等级**。

步骤 2 单击**新增**。

步骤 3 从**用户等级**下拉菜单中，选择一个介于 1 到 10 之间的等级设置。最高等级为 1。

步骤 4 输入**等级名称**和**说明**。

步骤 5 单击**保存**。

步骤 6 重复此程序以添加其他用户等级。
您可以将用户等级分配给用户和访问控制组，以控制用户可分配到的组。

创建自定义角色

此程序用于创建具有自定义权限的新角色。如果没有符合您所需权限的标准角色，则需要执行此操作。可以通过两种方式来创建角色：

- 使用**新增**按钮从头开始创建和配置新角色。
- 如果现有角色的访问权限与您所需的权限接近，请使用**复制**按键。可以将现有角色的权限复制到可编辑的新角色。

过程

步骤 1 在 Cisco Unified CM 管理中，单击**用户管理** > **用户设置** > **角色**。

步骤 2 执行以下任一操作：

- 要创建新角色，请单击**新增**。选择此角色关联的**应用程序**，然后单击**下一步**。

- 要从现有角色复制设置，请单击**查找**并打开现有的角色。单击**复制**，然后输入新角色的名称。单击**确定**。

步骤 3 输入角色的**名称**和**说明**。

步骤 4 对于每个资源，选中适用的复选框：

- 如果希望用户能够查看资源的设置，选中**读取**复选框。
- 如果希望用户能够编辑资源的自动，选中**更新**复选框。
- 要限制对资源的访问，将两个复选框都保留未选中状态。

步骤 5 单击**授予所有访问权限**或**拒绝所有访问权限**按钮，以授予或删除此角色访问页面上显示的所有资源的权限。

注释 如果资源列表包含多个页面，则此按键仅适用于当前页面上显示的资源。要更改对其他页面上所列资源的访问权限，必须显示这些页面并在各页面上单击此按钮。

步骤 6 单击**保存**。

为管理员配置高级角色

借助高级角色配置，您可以更细致地编辑自定义角色的权限。您可以在**最终用户配置**和**应用程序用户配置**窗口中控制管理员编辑以下关键设置的能力：

- 编辑用户等级
- 编辑访问控制组分配
- 添加新用户
- 编辑用户密码

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **角色**。

步骤 2 单击**查找**并选择一个自定义角色。

步骤 3 从**相关链接**中选择**高级角色配置**，然后单击**前往**。

步骤 4 从**资源网页**中，选择**应用程序用户网页**或**用户网页**。

步骤 5 编辑设置。有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 6 单击**保存**。

创建访问控制组

如果需要创建新的访问控制组，请遵照此程序执行。如果所有标准组都没有所需的角色和访问权限，您可能需要执行此操作。有两种方法可以创建自定义的组：

- 使用**新增**按钮从头创建和配置新的访问控制组。
- 如果现有组的角色权限与您的需求接近，请使用**复制**按钮。您可以将现有组的设置复制到可编辑的新组。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 执行以下任一操作：

- 要从头创建新组，请单击**新增**。
- 要从现有组复制设置，请单击**查找**并打开现有的访问控制组。单击**复制**，然后输入新组的名称。单击**确定**。

步骤 3 输入访问控制组的**名称**。

步骤 4 从**可用于具有以下用户等级的用户**下拉列表中，选择要分配给该组的用户必须满足的最低用户等级。默认用户等级为 1。

步骤 5 单击**保存**。

步骤 6 向访问控制组分配角色。您选择的角色将分配给组成员：

a) 从**相关链接**中，选择**分配角色至访问控制组**，并单击**转至**。
b) 单击**查找**以搜索现有的角色。
c) 选中要添加的角色，然后单击**添加选定项**。
d) 单击**保存**。

下一步做什么

向访问控制组分配用户 ，第 8 页

向访问控制组分配用户

从标准或自定义访问控制组添加或删除用户.

注释 您只能添加那些用户等级与访问控制组的最低用户等级相同或更高的用户。

注释 如果要从公司 LDAP 目录同步新用户，并且使用适当的权限创建了等级分层结构和访问控制组，则可以将组分配给已同步的用户，作为 LDAP 同步的一部分。有关如何设置 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》。

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。

此时将出现**查找并列出访问控制组**窗口。

步骤 2 单击**查找**并选择要为其更新用户列表的访问控制组。

步骤 3 从**可用于具有以下用户等级的用户**下拉列表中，选择要分配给该组的用户必须满足的等级要求。

步骤 4 在**用户**部分，单击**查找**以显示用户列表。

步骤 5 如果想要将最终用户或应用程序用户添加到访问控制组，请执行以下操作：

a) 单击**将最终用户添加到访问控制组**或**将应用程序用户添加到访问控制组**。
b) 选择要添加的用户。
c) 单击**添加选定项**。

步骤 6 如果想要从访问控制组删除用户：

a) 选择要删除的用户。
b) 单击**删除选定项**。

步骤 7 单击**保存**。

为访问控制组配置重叠权限策略

配置 Cisco Unified Communications Manager 如何处理可能由访问控制组分配导致的重叠用户权限。这是为了涵盖最终用户被分配到多个访问控制组，而每个访问控制组都有冲突的角色和权限设置的情况。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**下方，如下所示为**重叠用户组和角色的有效访问权限**配置以下值之一：

- **最大值** — 有效权限代表所有重叠访问控制组的最大权限。这是默认选项。
- **最小值** — 有效权限代表所有重叠访问控制组的最小权限。

步骤 3 单击**保存**。

查看用户权限报告

执行以下程序以查看现有最终用户或现有应用程序用户的用户权限报告。用户权限报告会显示访问控制组、角色和分配给最终用户或应用程序用户的访问权限。

过程

步骤 1 在 Cisco Unified CM 管理中，执行以下步骤之一：

- 对于最终用户，选择**用户管理** > **最终用户**。
- 对于应用程序用户，选择**用户管理** > **应用程序用户**。

步骤 2 单击**查找**并选择您要为其查看访问权限的用户

步骤 3 从**相关链接**下拉列表中，选择**用户权限报告**，然后单击**转至**。
随即会出现“用户权限”窗口。

创建自定义帮助台角色任务流程

有些公司希望其技术支持人员拥有能够执行某些管理任务的权限。按照此任务流程中的步骤为技术支持团队成员配置角色和访问控制组，以允许他们执行一些任务，例如添加电话和添加最终用户。

过程

	命令或操作	目的
步骤 1	创建自定义技术支持角色，第 10 页	为技术支持团队成员创建自定义角色，并为添加新电话和添加新用户等项目分配角色权限。
步骤 2	创建自定义技术支持访问控制组，第 11 页	为技术支持角色创建新的访问控制组。
步骤 3	将技术支持角色分配到访问控制组，第 11 页	将技术支持角色分配到技术支持访问控制组。分配到此访问控制组的任何用户都将分配到技术支持角色的权限。
步骤 4	将技术支持成员分配到访问控制组，第 12 页	为技术支持团队成员分配自定义技术支持角色的权限。

创建自定义技术支持角色

执行此程序以创建自定义技术支持角色，您可以将该角色分配给组织内的技术支持成员。

过程

步骤 1 在 Cisco Unified Communications Manager 管理中，选择**用户管理** > **用户设置** > **角色**。

步骤 2 单击**新增**。

步骤 3 从“应用程序”下拉列表中，选择要分配给此角色的应用程序。例如，**Cisco CallManager 管理**。

步骤 4 单击**下一步**。

步骤 5 输入新角色的**名称**。例如，**Help Desk**。

步骤 6 在**读取和更新权限**下方，选择您要为技术支持用户分配的权限。例如，如果您希望技术支持成员能够添加用户和电话，请在“用户”网页和“电话”网页上选中**读取**和**更新**复选框。

步骤 7 单击**保存**。

下一步做什么

创建自定义技术支持访问控制组，第 11 页

创建自定义技术支持访问控制组

开始之前

创建自定义技术支持角色，第 10 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**新增**。

步骤 3 输入访问控制组的名称。例如，**Help_Desk**。

步骤 4 单击**保存**。

下一步做什么

将技术支持角色分配到访问控制组，第 11 页

将技术支持角色分配到访问控制组

执行以下步骤为技术支持访问控制组配置来自技术支持角色的权限。

开始之前

创建自定义技术支持访问控制组，第 11 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您为技术支持创建的访问控制组。
此时将显示**访问控制组配置**窗口。

步骤 3 在**相关链接**下拉列表框中，选择**将角色分配到访问控制组**选项，然后单击**转至**。
随即将显示**查找并列出角色**弹出窗口。

步骤 4 单击**将角色分配到组**按钮。

步骤 5 单击**查找**并选择技术支持角色。

步骤 6 单击**添加选定项**。

步骤 7 单击**保存**。

下一步做什么

将技术支持成员分配到访问控制组 ， 第 12 页

将技术支持成员分配到访问控制组

开始之前

将技术支持角色分配到访问控制组 ， 第 11 页

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **访问控制组**。

步骤 2 单击**查找**并选择您创建的自定义技术支持访问控制组。

步骤 3 请执行以下步骤之一：

- 如果您的技术支持团队成员被配置为最终用户，请单击**将最终用户添加到组**。
- 如果您的技术支持团队成员被配置为应用程序用户，请单击**将应用程序用户添加到组**。

步骤 4 单击**查找**并选择您的技术支持用户。

步骤 5 单击**添加选定项**。

步骤 6 单击**保存**。
Cisco Unified Communications Manager 会向您的技术支持团队成员分配您创建的自定义技术支持角色的权限。

删除访问控制组

使用以下程序完全删除访问控制组。

开始之前

删除访问控制组时，Cisco Unified Communications Manager 会从数据库中删除所有访问控制组数据。确保您了解哪些角色正在使用访问控制组。

过程

步骤 1 选择**用户管理** > **用户设置** > **访问控制组**。

此时将显示**查找并列出访问控制组**窗口。

步骤 2 找到您要删除的访问控制组。

步骤 3 单击要删除的访问控制组的名称。

此时将显示所选的访问控制组。列表按字母顺序显示此访问控制组中的用户。

步骤 4 如果要完全删除访问控制组，请单击**删除**。

此时将显示一个对话框，警告您无法撤消访问控制组的删除。

步骤 5 要删除访问控制组，请单击**确定**；要取消该操作，请单击**取消**。如果单击**确定**，Cisco Unified Communications Manager 将从数据库中删除访问控制组。

撤销现有的 OAuth 刷新令牌

使用 AXL API 撤销现有的 OAuth 刷新令牌。例如，如果一名员工离开了您的公司，您可以使用此 API 撤销该员工当前的刷新令牌，以使他们不能获得新的访问令牌，并且将不能再登录到公司帐户。该 API 是一个基于 REST 的 API，受 AXL 凭证保护。您可以使用任何命令行工具来调用 API。下面的命令提供了一个可用于撤销刷新令牌的 cURL 命令的示例：

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

其中：

- `admin:password` 是登录 ID 和 Cisco Unified Communications Manager 管理员帐户的密码。
- `UCMaddress` 是 Cisco Unified Communications Manger 发布方节点的 FQDN 或 IP 地址。
- `end_user` 是您要对其撤销刷新令牌的用户的用户 ID。

禁用非活动用户帐户

遵照以下程序使用 Cisco 数据库层监控器服务禁用非活动用户帐户。

如果您在指定的天数内未登录 Cisco Unified Communications Manager，Cisco 数据库层监控器将在预定的维护任务期间将用户帐户状态改为非活动。在后续的审核日志中，系统会自动审核禁用的用户。

开始之前

在 Cisco 数据库层监控器服务（**系统** > **服务参数**）中输入所选服务器的**维护时间**。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **服务参数**。

步骤 2 从**服务器**下拉列表框中选择服务器。

步骤 3 从**服务**下拉列表框中，选择 **Cisco 数据库层监控器**参数。

步骤 4 单击**高级**。

步骤 5 在**禁用未使用用户帐户的天数**字段中，输入天数。例如 90。系统使用输入的值作为阈值，将帐户状态声明为非活动。要关闭自动禁用，请输入 0。

注释 这是必填字段。默认值和最小值为 0，单位为天。

步骤 6 单击**保存**。
如果在配置的天数（例如 90 天）内保持非活动状态，则用户将被禁用。审核日志中会输入一个条目，其将显示如下消息：“<userID> 用户被标记为非活动”。

设置远程帐户

在 Unified Communications Manager 中配置一个远程帐户，以便 Cisco 支持人员能够暂时访问您的系统进行故障诊断。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**服务** > **远程支持**。

步骤 2 在**帐户名**字段中，输入远程帐户的名称。

步骤 3 在**帐户期限**字段中，输入帐户期限，以天为单位。

步骤 4 单击**保存**。
系统将生成加密的密码短语。

步骤 5 与 Cisco 支持人员联系，向其提供远程支持帐户名和密码短语。

标准角色和访问控制组

下表总结了标准角色和在 Cisco Unified Communications Manager 上预先配置的访问控制组。标准角色的权限是默认配置的。此外，与标准角色关联的访问控制组也是默认配置的。

对于标准角色和关联的访问控制组，您都无法编辑任何权限或角色分配。

表 2: 标准角色、权限和访问控制组

标准角色	角色的权限/资源	关联的标准访问控制组
标准 AXL API 访问	允许访问 AXL 数据库 API	标准 CCM 超级用户
标准 AXL API 用户	授予登录权限以执行 AXL API。	
标准 AXL 只读 API 访问	默认情况下允许您执行 AXL 只读 API（list API、get API、executeSQLQuery API）。	
标准管理员报告工具管理	允许您查看和配置 Cisco Unified Communications Manager CDR 分析和报告 (CAR)。	标准 CAR 管理员用户、标准 CCM 超级用户
标准审核日志管理	允许您执行审核日志记录功能的以下任务： • 在 Cisco Unified 功能配置的“审核日志配置”窗口中查看和配置审核日志记录 • 在 Cisco Unified 功能配置中查看和配置跟踪并在实时监控工具中收集审核日志功能的跟踪 • 在 Cisco Unified 功能配置中查看和启动/停止 Cisco Audit Event 服务 • 在 RTMT 中查看和更新关联的警告	标准审计用户
标准 CCM 管理员用户	授予 Cisco Unified Communications Manager 管理的登录权限。	标准 CCM 管理员用户、标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器监控、标准 CCM 超级用户、标准 CCM 服务器维护、标准信息包探查器用户
标准 CCM 最终用户	授予 Cisco Unified Communications Self Care 门户网站的最终用户登录权限	标准 CCM 最终用户

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 功能管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 使用批量管理工具查看、删除和插入以下项目：
	  • 客户码和强制授权码
	  • 呼叫代答组
	• 在 Cisco Unified Communications Manager 管理中查看和配置以下项目：
	  • 客户码和强制授权码
	  • 呼叫暂留
	  • 呼叫代答
	  • Meet-me 号码/模式
	  • 留言通知
	  • Cisco Unified IP 电话服务
	  • 语音信箱引导、语音信箱端口向导、语音信箱端口和语音信箱配置文件
		标准 CCM 服务器维护

标准 CCM 网关管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 在批量管理工具中查看和配置网关模板 • 查看和配置网守、网关和干线	标准 CCM 网关管理

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 电话管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 在批量管理工具中查看和导出电话
	• 在批量管理工具中查看和插入用户设备配置文件
	• 在 Cisco Unified Communications Manager 管理中查看和配置以下项目：
	  • BLF 快速拨号
	  • CTI 路由点
	  • 默认设备配置文件或默认配置文件
	  • 目录号码和线路显示
	  • 固件加载信息
	  • 电话按键模板或软键模板
	  • 电话
	  • 特定电话的电话按键重新排序信息（通过单击“电话配置”窗口中的“修改按键项”按钮）
		标准 CCM 电话管理

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCM 路由计划管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务： • 查看和配置应用程序拨号规则 • 查看和配置呼叫搜索空间和分区 • 查看和配置拨号规则，包括拨号规则模式 • 查看和配置寻线列表、寻线引导和线路组 • 查看和配置路由过滤器、路由组、路由寻线列表、路由列表、路由模式和路由计划报告 • 查看和配置时段和时间表 • 查看和配置转换模式	

标准 CCM 服务管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 查看和配置以下项目：
	  • 信号器、会议桥和转码器
	  • 音频来源和 MOH 服务器
	  • 媒体资源组和媒体资源组列表
	  • 媒体终结点
	  • Cisco Unified Communications Manager Assistant 向导
	• 在批量管理工具中查看和配置“删除经理”、“删除经理/助理”和“嵌入经理/助理”窗口
		标准 CCM 服务器维护

标准角色	角色的权限/资源	关联的标准访问控制组

标准 CCM 系统管理	允许您在 Cisco Unified Communications Manager 管理中执行以下任务：
	• 查看和配置以下项目：
	  • 自动路由迂回 (AAR) 组
	  • Cisco Unified Communications Manager (Cisco Unified CM) 和 Cisco Unified Communications Manager 组
	  • 日期和时间组
	  • 设备默认值
	  • 设备池
	  • 企业参数
	  • 企业电话配置
	  • 位置
	  • 网络时间协议 (NTP) 服务器
	  • 插件
	  • 用于运行信令呼叫控制协议 (SCCP) 或会话发起协议 (SIP) 的电话的安全性配置文件；用于 SIP 干线的安全性配置文件
	  • 可存活远程站点电话 (SRST) 引用
	  • 服务器
	• 在批量管理工具中查看和配置“作业计划程序”窗口
		标准 CCM 服务器维护

标准 CCM 用户权限管理	允许您在 Cisco Unified Communications Manager 管理中查看和配置应用程序用户。	
标准 CCMADMIN 管理	允许您访问 CCMAdmin 系统的所有方面	

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CCMADMIN 管理	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看和配置所有项目。	标准 CCM 超级用户
标准 CCMADMIN 管理	允许您在被叫号码分析器中查看和配置信息。	
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	
标准 CCMADMIN 只读	允许您在 Cisco Unified Communications Manager 管理和批量管理工具中查看配置。	标准 CCM 网关管理、标准 CCM 电话管理、标准 CCM 只读、标准 CCM 服务器维护、标准 CCM 服务器监控
标准 CCMADMIN 只读	允许您在被叫号码分析器中分析路由配置。	
标准 CCMUSER 管理	允许访问 Cisco Unified Communications Self Care 门户网站。	标准 CCM 最终用户
标准 CTI 允许呼叫监控	允许 CTI 应用程序/设备监控呼叫	标准 CTI 允许呼叫监控
标准 CTI 允许呼叫暂留监控	允许CTI应用程序/设备使用呼叫暂留。 **重要事项** 开放线路和暂留线路的最大数不得超过 65000。 如果总数超过65,000，请从应用程序用户中删除“标准CTI允许呼叫暂留监控”角色或减少配置的暂留线路数。	标准 CTI 允许呼叫暂留监控
标准 CTI 允许呼叫录音	允许 CTI 应用程序/设备录音呼叫	标准 CTI 允许呼叫录音
标准 CTI 允许主叫号码修改	允许CTI应用程序在通话期间转换主叫方号码	标准 CTI 允许主叫号码修改
标准 CTI 允许控制所有设备	允许控制所有 CTI 可控制设备	标准 CTI 允许控制所有设备
标准CTI允许控制支持已连接转接和会议的电话	允许控制支持已连接转接和会议的所有 CTI 设备	标准CTI允许控制支持已连接转接和会议的电话
标准CTI允许控制支持跳转模式的电话	允许控制支持跳转模式的所有CTI设备	标准CTI允许控制支持跳转模式的电话
标准 CTI 允许接收 SRTP 重要材料	允许 CTI 应用程序访问和分发 SRTP 重要材料	标准 CTI 允许接收 SRTP 重要材料
标准 CTI 已启用	启用 CTI 应用程序控制	标准 CTI 已启用

标准角色	角色的权限/资源	关联的标准访问控制组
标准 CTI 安全连接	启用到 Cisco Unified Communications Manager 的安全 CTI 连接	标准 CTI 安全连接
标准 CU 报告	允许应用程序用户生成各种来源的报告	
标准 CU 报告	允许您在 Cisco Unified 报告中查看、下载、生成和上传报告	标准 CCM 管理用户、标准 CCM 超级用户
标准 EM 验证代理权限	管理应用程序的 Cisco 分机移动 (EM) 验证权限；与 Cisco 分机移动交互的所有应用程序用户（例如，Cisco Unified Communications Manager Assistant 和 Cisco Web Dialer）必需	标准 CCM 超级用户、标准 EM 验证代理权限
标准信息包探查	允许您访问 Cisco Unified Communications Manager 管理以启用数据包探查（捕获）。	标准信息包探查器用户
标准实时和跟踪收集	允许您访问 Cisco Unified 功能配置和实时监控工具视图并使用以下项目： • 简单对象访问协议 (SOAP) 功能配置 AXL API • SOAP 呼叫记录 API • SOAP Diagnostic Portal (Analysis Manager) 数据库服务 • 配置审核日志追踪功能 • 配置实时监控工具，包括收集跟踪	标准实时和跟踪收集

标准角色	角色的权限/资源	关联的标准访问控制组
标准功能配置	允许您在Cisco Unified 功能配置或实时监控工具中查看和配置以下窗口： • “警报配置”和“警报定义”（Cisco Unified 功能配置） • 审计追踪（标记为只读/仅查看） • SNMP 相关窗口（Cisco Unified 功能配置） • “跟踪配置”和“跟踪配置故障诊断”（Cisco Unified 功能配置） ） • 日志分区监控 • 警告配置 (RTMT)、配置文件配置 (RTMT)，以及跟踪收集 (RTMT) 允许您查看和使用 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。 对于 SOAP 呼叫记录 API，RTMT Analysis Manager 呼叫记录权限通过此资源进行控制。 对于 SOAP Diagnostic Portal 数据库服务，RTMT Analysis Manager 托管数据库通过此资源控制访问。	标准 CCM 服务器监控、标准 CCM 超级用户
标准功能配置管理	功能配置管理员可在 Cisco Unified Communications Manager 管理中访问“插件”窗口并从此窗口中下载插件。	
标准功能配置管理	允许您管理被叫号码分析器功能配置的所有方面。	
标准功能配置管理	允许您在Cisco Unified 功能配置和实时监控工具中查看和配置所有窗口。（审计追踪仅支持查看） 允许您查看和使用所有 SOAP 功能配置 AXL API。	
标准功能配置只读	允许您查看被叫号码分析器中组件的所有功能配置相关数据。	标准 CCM 只读

标准角色	角色的权限/资源	关联的标准访问控制组
标准功能配置只读	允许您在Cisco Unified 功能配置和实时监控工具中查看配置。（“审计配置”窗口除外，该窗口由“标准审核日志管理”角色代表） 允许您查看所有 SOAP 功能配置 AXL API、SOAP 呼叫记录 API 和 SOAP Diagnostic Portal (Analysis Manager) 数据库服务。	
标准系统服务管理	允许您在 Cisco Unified 功能配置中查看、激活、启动和停止服务。	
标准 SSO 配置管理员	允许您管理 SAML SSO 配置的所有方面	
标准保密访问级别用户	允许您访问所有保密访问级别页面	标准 Cisco Call Manager 管理
标准 CCMADMIN 管理	允许您管理 CCMAdmin 系统的所有方面	标准 Cisco Unified CM IM and Presence 管理
标准 CCMADMIN 只读	允许所有 CCMAdmin 资源的读取访问权限	标准 Cisco Unified CM IM and Presence 管理
标准 CU 报告	允许应用程序用户生成各种来源的报告	标准 Cisco Unified CM IM and Presence 报告