管理凭证策略

- 凭证策略和验证， 第 1 页
- 配置凭证策略， 第 2 页
- 配置凭证策略默认设置， 第 2 页
- 监控验证活动， 第 3 页
- 配置凭证缓存， 第 4 页
- 管理会话终止， 第 4 页

凭证策略和验证

验证功能会验证用户、更新凭证信息、跟踪和记录用户事件和错误、记录凭证更改历史记录，以及加密或解密数据存储的用户凭证。

系统始终根据 Unified Communications Manager 数据库验证应用程序用户密码和最终用户个人识别码。 系统可以根据公司目录或数据库验证最终用户密码。

如果系统与公司目录同步，Unified Communications Manager或轻量级目录访问协议 (LDAP) 中的验证功能可以验证密码：

- 启用 LDAP 验证时，用户密码和凭证策略不适用。 这些默认值会应用于通过目录同步（DirSync 服务）创建的用户。
- 禁用 LDAP 验证后，系统根据数据库验证用户凭证。 通过此选项，您可以分配凭证策略、管理验证事件和管理密码。 最终用户可以通过电话用户界面更改密码和个人识别码。

凭证策略不适用于操作系统用户或 CLI 用户。 这些管理员使用操作系统支持的标准密码验证程序。

在数据库中配置用户后，系统将在数据库中存储用户凭证的历史记录，以防用户在收到提示其更改其凭证的消息时输入之前用过的信息。

凭证策略的 JTAPI 和 TAPI 支持

由于 Cisco Unified Communications Manager Java 电话应用程序编程接口 (JTAPI) 和电话应用程序编程接口 (TAPI) 支持分配给应用程序用户的凭证策略，所以开发者必须创建应用程序以应对凭证策略执行时的密码过期、个人识别码过期以及锁定返回码。

应用程序使用 API 验证数据库或公司目录，而不管应用程序使用何种验证模型。

有关开发人员 JTAPI 和 TAPI 的详细信息，请参阅开发人员手册，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html。

配置凭证策略

凭证策略适用于应用程序用户和最终用户。 可将密码策略分配给最终用户和应用程序用户，将个人识别码策略分配给最终用户。“凭证策略默认值配置”列出这些组的策略分配。 向数据库添加新用户时，系统会分配默认策略。 您可以更改分配的策略并管理用户验证事件。

注释 确保 CTI 应用用户的凭证策略设置下的允许非活动天数参数设置为 0（无限制）。 否则，应用程序用户会意外地变为非活动状态，并且 CTI 应用在重新启动后可能无法连接到 Unified CM。

过程

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

步骤 2 请执行以下步骤之一：

- 单击**查找**并选择一个现有的凭证策略。
- 单击**新增**以创建新的凭证策略。

步骤 3 填写**凭证策略配置**窗口中的字段。 请参阅联机帮助，了解有关字段及其配置设置的更多信息。

步骤 4 单击**保存**。

配置凭证策略默认设置

安装时，Cisco Unified Communications Manager 将静态默认凭证策略分配给用户组。 它不提供默认凭证。 您的系统提供了一些选项来分配新的默认策略，以及为用户配置新的默认凭证和凭证要求。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **凭证策略默认设置**。

步骤 2 从**凭证策略**下拉列表框中，选择此组的凭证策略。

步骤 3 在**更改凭证**和**确认凭证**配置窗口中输入密码。

步骤 4 如果您不希望用户可以更改此凭证，请选中**用户无法更改**复选框。

步骤 5 如果您想将此凭证用作临时凭证，最终用户必须在下次登录时更改，请选中**用户必须在下次登录时更改**复选框。

注释 请注意，如果选中此复选框，您的用户将无法使用个人目录服务更改个人识别码。

步骤 6 如果您不希望凭证过期，请选中**没有过期**复选框。

步骤 7 单击**保存**。

监控验证活动

系统显示最近的验证结果，例如上次黑客尝试时间以及登录尝试失败计数。

系统将为以下凭证策略事件生成日志文件条目：

- 验证成功
- 验证失败（密码错误或未知）
- 由于以下原因验证失败：
  - 管理锁定
  - 黑客行为锁定（登录失败锁定）
  - 过期软锁定（过期的凭证）
  - 非活动锁定（凭证有一段时间未使用）
  - 用户必须更改（凭证设置为“用户必须更改”）
  - LDAP 非活动（切换到 LDAP 验证且 LDAP 非活动）
- 用户凭证更新成功
- 用户凭证更新失败

注释 如果对最终用户密码使用 LDAP 验证，LDAP 仅跟踪验证成功和失败。

所有事件消息都包含字符串 “ims-auth” 和尝试验证的用户 ID。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**用户管理** > **最终用户**。

步骤 2 输入搜索条件，单击**查找**，然后从结果列表中选择用户。

步骤 3 单击**编辑凭证**以查看用户的验证活动。

下一步做什么

您可以通过 Cisco Unified 实时监控工具 (Unified RTMT) 查看日志文件。还可以将捕获的事件收集到报告中。有关如何使用 Unified RTMT 的详细步骤，请参阅《*Cisco Unified* 实时监控工具管理指南》，位于 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

配置凭证缓存

启用凭证缓存以提高系统效率。 您的系统不必为每一个单点登录请求执行数据库查找或调用存储的程序。 关联的凭证策略不会执行，直至缓存时间到期。

此设置适用于所有调用用户验证的 Java 应用程序。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 根据需要执行以下任务：

- 将**启用缓存**企业参数设置为**真**。 启用此参数后，Cisco Unified Communications Manager 会使用缓存的凭证最多 2 分钟。
- 将**启用缓存**企业参数设为**假**以禁用缓存，这样系统就不会使用缓存的凭证进行验证。 对于 LDAP 验证，系统会忽略此设置。 凭证缓存要求每位用户具备最小额外内存量。

步骤 3 单击**保存**。

管理会话终止

管理员可以遵照此程序终止特定于每个节点的用户的活动登录会话。

注释

- 权限级别为 4 的管理员才可终止会话。
- 会话管理终止特定节点上的活动登录会话。 如果管理员想要终止跨不同节点的所有用户会话，则管理员必须登录每个节点并终止会话。

这适用于以下接口：

- Cisco Unified CM 管理

- Cisco Unified 功能配置
- Cisco Unified 报告
- Cisco Unified Communications Self Care 门户网站
- Cisco Unified CM IM and Presence 管理
- Cisco Unified IM and Presence 功能配置
- Cisco Unified IM and Presence 报告

过程

步骤 1 从 Cisco Unified 操作系统管理或 Cisco Unified IM and Presence 操作系统管理中，选择**安全** > **会话管理**。
此时“会话管理”窗口将显示。

步骤 2 在**用户 ID** 字段中输入活动登录用户的用户 ID。

步骤 3 单击**终止会话**。

步骤 4 单击**确定**。

如果终止的用户刷新登录的界面页面，用户将被注销。 审核日志中会输入一个条目，其中显示终止的用户 ID。

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。