



Informatica® Multidomain MDM
10.3

安全指南

Informatica Multidomain MDM 安全指南

10.3

2018 年 9 月

© 版权所有 Informatica LLC 2014, 2019

本软件和文档仅根据包含使用与披露限制的单独许可协议提供。未事先征得 Informatica LLC 同意，不得以任何形式、通过任何手段（电子、影印、录制或其他手段）复制或传播本文档的任何部分。

美国政府权利交付给美国政府客户的程序、软件、数据库及相关文档和技术数据是指适用的联邦采购条例和政府机构特定补充条例中定义的"商业计算机软件"或"商业技术数据"。因此，使用、复制、披露、修改和改编应遵循适用的政府合同中规定的限制和许可条款、政府合同条款的适用范围以及 FAR 52.227-19 商用计算机软件许可中规定的额外权利。

Informatica 和 Informatica 标志是 Informatica LLC 在美国和世界其他许多司法管辖区的商标或注册商标。欲获得 Informatica 商标的最新列表，请访问 <https://www.informatica.com/trademarks.html>。其他公司和产品名称可能是其各自所有者的商业名称或商标。

本软件和/或文档中的若干部分受第三方所拥有的版权约束。所需的第三方声明随产品一起提供。

本文档中的信息如有更改，恕不另行通知。如发现本文档中有什么问题，请通过以下电子邮件地址向我们报告：infa_documentation@informatica.com。

Informatica 产品根据对应协议的条款和条件进行担保。INFORMATICA 按"原样"提供本文档中的信息，无任何明示或暗示的担保，包括但不限于任何适销性和特定用途适用性担保，也没有任何非侵权担保或条件。

发布日期: 2019-05-28

目录

前言	7
Informatica 资源	7
Informatica Network	7
Informatica 知识库	7
Informatica 文档	7
Informatica 产品可用性矩阵	8
Informatica Velocity	8
Informatica Marketplace	8
Informatica 全球客户支持部门	8
第 1 章：MDM Hub 安全简介	9
MDM Hub 安全概览	9
MDM Hub 控制台	9
Dynamic Data Masking	10
安全访问管理器	11
身份验证	11
授权	11
保护资源和特权	12
角色	12
安全实施方案	13
内部策略判定点	13
外部用户目录	13
基于角色的集中策略判定	14
全面集中的策略判定	15
安全方案的配置任务	15
第 2 章：资源	16
资源概览	16
安全资源和专用资源	17
资源组	17
资源组层次结构	17
安全资源	17
“安全资源”工具	18
安全资源的配置	18
设置 MDM Hub 资源的状态	18
筛选资源	18
资源组配置	19
添加资源组	19
编辑和删除资源组	19
刷新资源列表	20

刷新其他安全更改.	20
第 3 章：角色.	21
角色概览.	21
角色配置.	21
添加角色.	22
编辑和删除角色.	22
特权.	22
内部角色和外部角色.	23
将资源特权分配给角色.	23
将角色分配给其他角色.	24
为角色生成资源特权的报告.	24
将生成的报告另存为 HTML 文件.	24
第 4 章：用户和用户组.	25
用户和用户组概览.	25
用户配置.	25
用户对 MDM Hub 资源的访问权限.	26
添加用户帐户.	26
编辑和删除用户帐户.	26
编辑用户补充信息.	27
更改用户帐户的密码设置.	27
配置用户访问操作引用存储的权限.	28
密码策略配置.	28
密码策略设置.	28
管理全局密码策略.	29
管理专用密码策略.	29
JDBC 数据源安全配置.	30
安全 JDBC 数据源的用户名和密码.	30
Oracle SID 连接类型的数据库 ID.	30
Oracle 服务连接类型的数据库 ID.	30
IBM DB2 连接类型的数据库 ID.	30
Microsoft SQL Server 连接类型的数据库 ID.	31
主数据库的数据库 ID.	31
密码加密.	31
用户组配置.	31
启动“用户和组”工具.	31
添加用户组.	32
编辑和删除用户组.	32
将用户和用户组分配给用户组.	33
将用户分配给当前 ORS 数据库.	33
角色与用户和用户组之间的关联.	33
将用户和用户组分配给角色.	33

向用户和用户组分配角色.	34
第 5 章：安全提供程序.	35
安全提供程序概览.	35
安全提供程序管理.	35
提供程序文件管理.	36
上传提供程序文件.	36
删除提供程序文件.	37
安全提供程序设置.	37
更改安全提供程序设置.	37
启用和禁用安全提供程序.	37
移动安全提供程序的处理顺序.	38
提供程序属性.	38
添加提供程序属性.	38
编辑提供程序属性.	39
自定义提供程序.	39
providers.properties 文件示例.	40
外部身份验证.	40
添加登录模块.	40
删除登录模块.	41
第 6 章：应用程序级别安全.	42
应用程序级别的安全性概览.	42
Informatica Data Director.	43
置备工具.	44
ActiveVOS.	44
Dynamic Data Masking.	44
在 Dynamic Data Masking 与 MDM HU 币 之间集成.	45
适用于 MDM Hub 的 Dynamic Data Masking 最佳实践.	45
为操作引用存储设置 Dynamic Data Masking.	46
在 Linux 上设置 WebLogic T3S 通道.	46
第 7 章：密码哈希.	48
密码哈希概览.	48
密码哈希选项.	49
自定义哈希算法.	49
基于证书的身份验证.	49
基于证书的身份验证和外部客户端.	50
受信任的应用程序.	50
将外部应用程序添加为可信应用程序.	50
证书和密钥的管理.	51
密码重置过程.	51
安全配置实用程序.	51

故障排除.....	52
附录 A: 词汇表.....	53
索引.....	57

前言

《Informatica MDM Hub 安全指南》面向数据库管理员、系统管理员以及负责安装和设置 Informatica^(R) MDM Hub 的实施人员。本指南假定您具备操作系统、数据库环境和应用程序服务器的相关知识。

Informatica 资源

Informatica 通过 Informatica Network 和其他在线门户为您提供一系列产品资源。使用这些资源，可以充分利用 Informatica 产品和解决方案，并向其他 Informatica 用户和主题专家学习。

Informatica Network

在 Informatica Network 中可以获得许多资源，包括 Informatica 知识库和 Informatica 全球客户支持。要进入 Informatica Network，请访问 <https://network.informatica.com>。

作为 Informatica Network 成员，您可以选择以下服务：

- 在知识库中搜索产品资源。
- 查看产品可用性信息。
- 创建并检查您的支持案例。
- 查找当地的 Informatica 用户组网络并与您的伙伴进行协作。

Informatica 知识库

使用 Informatica 知识库可查找产品资源，例如操作方法文章、最佳实践、视频教程以及常见问题的答案。

要搜索知识库，请访问 <https://search.informatica.com>。如果您对知识库有任何疑问、意见或建议，请与 Informatica 知识库团队联系，电子邮件地址为 KB_Feedback@informatica.com。

Informatica 文档

使用 Informatica 文档门户可浏览大量当前与最近产品版本的文档库。要浏览文档门户，请访问 <https://docs.informatica.com>。

除文档门户之外，Informatica 还在 Informatica 知识库中维护了许多产品的文档。如果在文档门户上找不到您产品或产品版本的文档，可以搜索知识库，网址为 <https://search.informatica.com>。

如果您对产品文档有任何疑问、意见或建议，请与 Informatica 文档团队联系，电子邮件地址为 infa_documentation@informatica.com。

Informatica 产品可用性矩阵

产品可用性矩阵 (PAM) 指明了产品版本支持的操作系统版本、数据库以及数据源和目标的类型。您可以在以下网址中浏览 Informatica PAM:

<https://network.informatica.com/community/informatica-network/product-availability-matrices>。

Informatica Velocity

Informatica Velocity 是由 Informatica 专业服务根据数百个数据管理项目的实际经验所开发出来的，其中汇集了大量使用技巧和最佳实践。Informatica Velocity 代表了 Informatica 顾问的集体知识，这些顾问与世界各地的组织合作，共同计划、开发、部署和维护成功的数据管理解决方案。

您可以在以下网址中找到 Informatica Velocity 资源：<http://velocity.informatica.com>。如果您对 Informatica Velocity 有任何疑问、意见或建议，请通过 ips@informatica.com 与 Informatica 专业服务联系。

Informatica Marketplace

Informatica Marketplace 是一个论坛，该论坛中提供的解决方案可扩展和增强您的 Informatica 实施。利用 Informatica 开发人员和合作伙伴在 Marketplace 中提供的数以百计的解决方案，可提高您的工作效率并加快项目实施时间。您可以在以下网址中找到 Informatica Marketplace：<https://marketplace.informatica.com>。

Informatica 全球客户支持部门

您可以通过电话或 Informatica Network 与全球支持中心联系。

要查找您当地的 Informatica 全球客户支持部门电话号码，请访问 Informatica 网站，链接为：<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>。

要在 Informatica Network 上查找在线支持资源，请访问 <https://network.informatica.com>，然后选择 eSupport 选项。

第 1 章

MDM Hub 安全简介

本章包括以下主题：

- [MDM Hub 安全概览, 9](#)
- [MDM Hub 控制台, 9](#)
- [Dynamic Data Masking, 10](#)
- [安全访问管理器, 11](#)
- [身份验证, 11](#)
- [授权, 11](#)
- [保护资源和特权, 12](#)
- [角色, 12](#)
- [安全实施方案, 13](#)

MDM Hub 安全概览

MDM Hub 可使数据免遭未经授权的访问和篡改，从而保护信息隐私和数据完整性。

您可以在 Hub 控制台中使用安全访问管理器来保护 MDM Hub 资源并强制实施操作安全策略，包括用户身份验证和授权。

您可以使用 Dynamic Data Masking 避免对敏感数据的访问。例如，您可以使用 Dynamic Data Masking 对没有管理权限的所有用户隐藏信用卡号。

您可以通过多种方式在 MDM Hub 实施中配置安全。您可以使用第三方安全提供程序来处理组织的特定安全元素，或者可以配置 MDM Hub 来管理所有安全方面。有关使用 服务集成框架 (SIF) 来配置安全的详细信息，请参阅《*Multidomain MDM 服务集成框架指南*》。

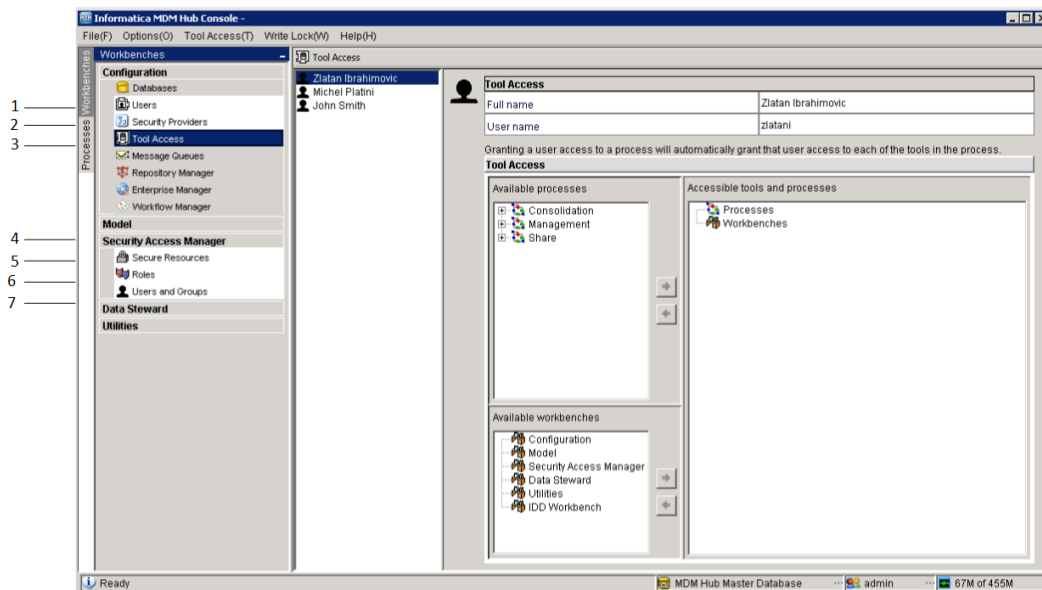
重要说明: 在开始保护 Multidomain MDM 之前，请确保您的应用程序服务器和缓存设备受到保护。

MDM Hub 控制台

使用 Hub Console：Hub 控制台在 MDM Hub 中配置安全。

要控制对 Hub Console：Hub 控制台工具的访问特权，可以使用“配置”工作台中的“工具访问”工具。例如，可以使用“工具访问”工具拒绝数据管理者访问除“数据管理器”和“合并管理器”工具之外的所有 Hub Console：Hub 控制台工具。

下图显示了 Hub Console：Hub 控制台界面：



Dynamic Data Masking

Informatica Dynamic Data Masking 是一款数据安全产品，可在客户端与数据库之间运行来防止未经授权访问敏感信息。Dynamic Data Masking 可侦听发送到数据库的请求并将数据屏蔽规则应用到请求，以在数据发送回客户端之前将其屏蔽。

您可以使用 Dynamic Data Masking 屏蔽或阻止对存储在由 MDM Hub 管理的生产和非生产数据库中的敏感数据进行的访问。设置连接规则以标识传入请求和安全规则，从而定义屏蔽数据的方式。Dynamic Data Masking 会监控来自 MDM Hub 的传入数据库请求，并在将请求发送到数据库之前修改数据库请求。数据库会处理修改的请求，并将屏蔽结果返回到 Dynamic Data Masking。然后，Dynamic Data Masking 将结果发送到 MDM Hub。

您可以使用 Dynamic Data Masking 为特定类型的数据库请求屏蔽数据，或者可以将访问限制为组织中特定组中的数据。例如，您可以创建规则以在数据库请求来自支持团队成员时，对信用卡号应用屏蔽函数。Dynamic Data Masking 将数据发送回 MDM Hub 时，支持团队成员会看到屏蔽的号码而不是真正的信用卡号。

注意: 要在 MDM Hub 中使用 Dynamic Data Masking，需要安装 Dynamic Data Masking 9.6.0 和紧急错误修复 14590。较早版本的 Dynamic Data Masking 与 MDM Hub 不兼容。

有关 Dynamic Data Masking 的详细信息，请参阅 Dynamic Data Masking 文档。

安全访问管理器

安全访问管理器是 MDM Hub 的安全模块。安全访问管理器 会保护 MDM Hub 资源，使其免遭未经授权的访问。

安全访问管理器会在 MDM Hub 实施中强制执行组织的安全策略。安全访问管理器根据安全配置管理用户身份验证和授权。

注意: 您可以使用安全访问管理器配置用户从第三方应用程序对 MDM Hub 资源的访问权限。但是，不能通过安全访问管理器为 Hub Console: Hub 控制台工具和资源配置安全。Hub Console: Hub 控制台会通过单独的安全机制对用户进行身份验证，并授予用户对 Hub Console: Hub 控制台工具和资源的访问权限。

身份验证

身份验证是验证用户身份的过程。

MDM Hub 根据用户提供的凭据（例如用户名和密码或安全负载中的原始二进制数据）对其进行身份验证。

MDM Hub 会使用以下类型的身份验证：

内部

在 MDM Hub 中会对用户进行身份验证，用户通过用户名和密码登录。

外部目录

通过外部用户目录对用户进行身份验证，对启用了 LDAP 的目录服务器、Microsoft Active Directory 和 Kerberos 提供本机支持。

外部身份验证提供程序

使用第三方身份验证提供程序对用户进行身份验证。

MDM Hub 实施可以仅使用其中一种类型的身份验证，或者实施可以将多种身份验证结合使用。使用的身份验证类型取决于配置安全的方式。

授权

授权是确定用户是否拥有足够特权来访问请求的 MDM Hub 资源的进程。

在 MDM Hub 中，可以使用内部和外部授权：

内部

通过 MDM Hub 授权。MDM Hub 通过检查与分配给您用户帐户的任何角色关联的特权，确定您是否可访问安全资源。

外部

通过第三方授权提供程序授权。

您可以将 MDM Hub 配置为使用任一类型的授权，或者可以将其配置为同时使用两种类型的授权。

保护资源和特权

您可以将多个 MDM Hub 资源配置为安全资源。

以下资源可配置：

- 基础对象
- 映射
- 包
- 清理函数
- 匹配规则集
- 元数据
- 配置文件
- 用户表

您可以根据特权授予对 MDM Hub 资源的访问权限。MDM Hub 可以分配以下特权：

- 读取
- 创建
- 更新
- 合并
- 执行
- 删除

资源可以为专用资源或安全资源。默认情况下，资源为安全资源。MDM Hub 仅可授予对安全资源的特权。

在 MDM Hub 中配置安全时，请考虑以下因素：

- 特定资源会配置为安全。
- 特定角色会配置为能够访问一个或多个安全资源。
- 每个安全资源可配置有特定的特权（例如读取或写入），从而为角色定义对安全资源的访问权限。

要运行 服务集成框架 请求，登录用户拥有的角色必须具有访问请求中涉及的资源所需的特权。

角色

角色代表用于访问安全 MDM Hub 资源的一组特权。为用户分配角色使该用户获得特权。

您可以使用安全访问管理器工作台上的“角色”工具为用户和用户组分配角色。分配给用户或用户组的角色会确定用户或用户组的资源特权。不能直接为用户分配特权。

安全访问管理器将针对外部应用程序用户发出的请求强制执行资源授权。使用 Hub Console：Hub 控制台访问 MDM Hub 资源的管理员和数据管理者受资源特权的影响程度不同。

安全实施方案

您可以通过多种方式在 MDM Hub 实施中配置安全。

策略判定点是在运行时确定用户身份的特定安全检查点。它称为身份验证。策略判定点还确认用户可以访问哪些 MDM Hub 资源。它称为授权。策略判定点是由 MDM Hub 在内部进行处理还是由第三方安全提供程序或其他安全服务在外部进行处理取决于 MDM Hub 实施。

以下场景是可在 MDM Hub 实施中配置安全的高级方式示例：

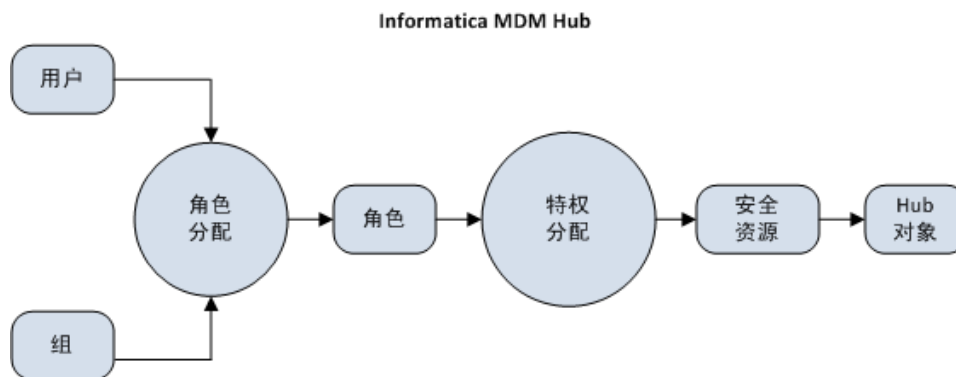
- 仅限内部的策略判定点
- 外部用户目录
- 基于角色的集中策略判定点
- 全面集中的策略判定点

注意：MDM Hub 不会反映外部安全提供程序对资源特权所做的更改。如果使用外部安全提供程序对资源特权进行更改，请使用其他方式将更改与 MDM Hub 同步。

内部策略判定点

MDM Hub 可以在内部处理所有策略判定。

下图显示了使 MDM Hub 在内部处理所有策略判定的安全部署：



在此方案中，MDM Hub 基于使用 Hub Console：Hub 控制台配置用户、组、角色、特权和资源的方式来决定所有策略。

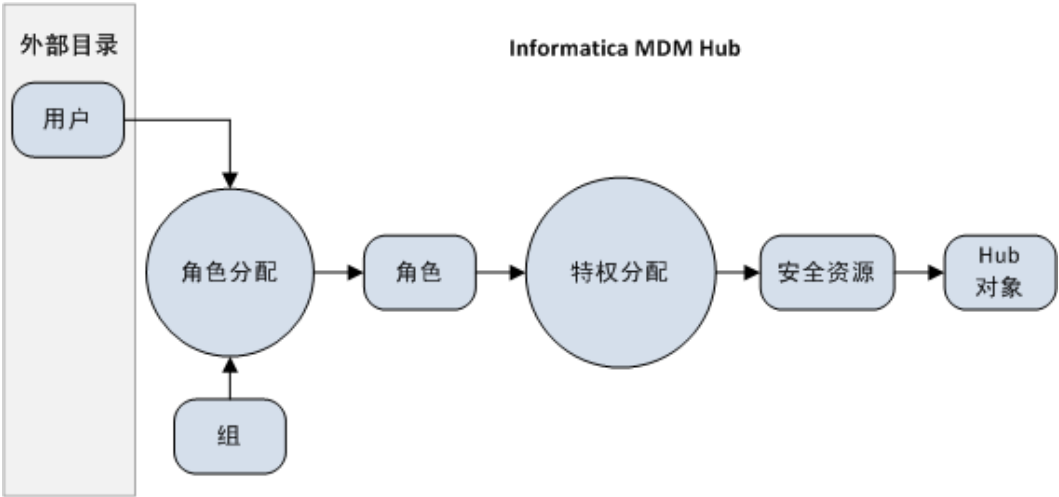
外部用户目录

MDM Hub 可以与外部用户目录集成。

在外部用户目录中维护的用户或用户组必须仍在 MDM Hub 中注册。需要先进行注册，然后 MDM Hub 才可为这些用户和组分配角色及其关联的特权。

将来自外部目录的用户分配给 MDM Hub 中的组。即使要通过轻量级目录访问协议维护关系，也必须维护 MDM Hub 中的用户与组之间的关系。

下图显示了一个安全部署，在该部署中，您管理外部目录中的用户，同时管理 MDM Hub 中的组、角色分配和特权分配。

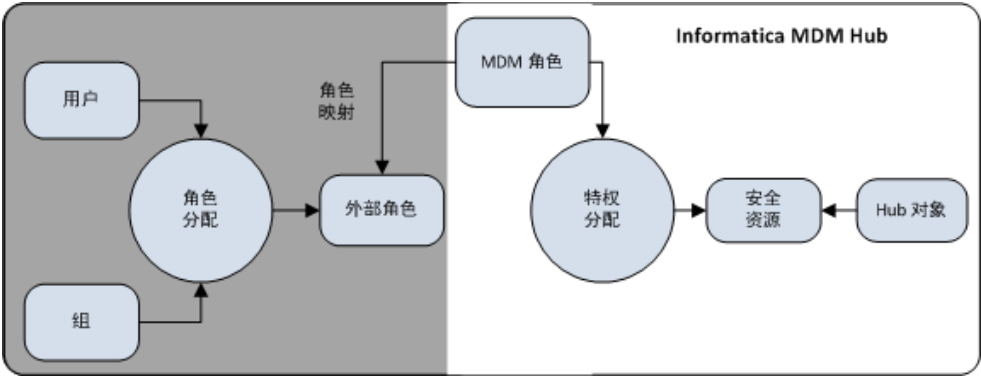


在这种情况下，外部用户目录将负责管理用户帐户、组以及用户配置文件。外部用户目录可以对用户进行身份验证，并向 MDM Hub 提供有关组成员关系和用户配置文件的信息。

基于角色的集中策略判定

MDM Hub 可以在内部处理一些策略判定，并接收外部角色分配。

下图显示了在 MDM Hub 外部进行角色分配（除用户帐户、组和用户配置文件之外）的安全部署：

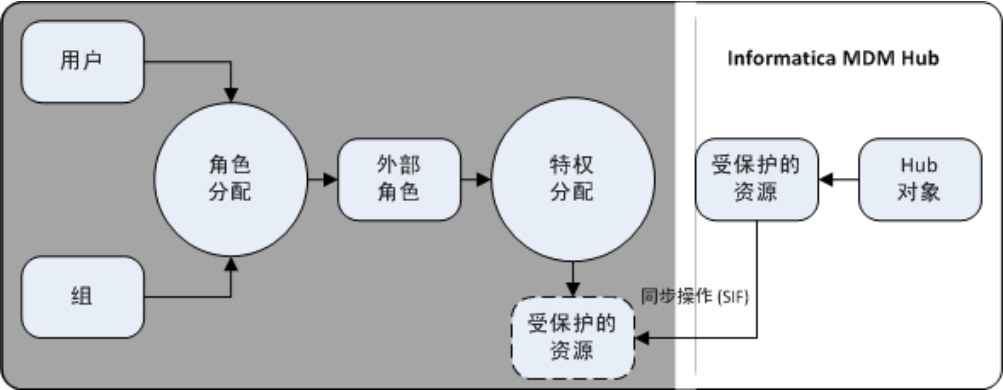


在此方案中，外部角色将被显式映射到 MDM Hub 角色。

全面集中的策略判定

MDM Hub 可以在内部控制受保护的资源，但是接受从外部目录分配的角色和特权。

下图显示了角色定义和特权分配在 MDM Hub 外部进行的安全部署。该图还显示用户帐户、组、用户配置文件和角色分配在 MDM Hub 的外部进行：



在此方案中，MDM Hub 只公开使用外部代理的受保护资源，这些资源可以与 服务集成框架 请求的内部受保护资源保持同步。所有策略均在 MDM Hub 外部判定。

安全方案的配置任务

下表显示了适合每种安全实施方案的安全配置任务。如果单元格包含“是”，则关联的任务在 MDM Hub 中进行。如果单元格包含“否”，则关联的任务在 MDM Hub 外部进行。

服务/任务	内部策略判定点	外部用户目录	基于角色的集中策略判定点	全面集中的策略判定点
配置 MDM Hub 用户	是	是	否	否
使用外部身份验证	否	是	否	否
将用户分配给当前 操作引用存储 数据库	是	是	否	否
管理全局密码策略	是	否	否	否
配置用户组	是	是	否	否
保护 MDM Hub 资源	是	是	是	是
设置 MDM Hub 资源的状态	是	是	是	是
配置角色	是	是	是	否
将内部角色映射到外部角色	否	否	是	否
将资源特权分配给角色	是	是	是	否
管理安全提供程序	否	是	是	是
将角色分配给用户和用户组	是	是	否	否

注意: 如果使用第三方安全提供程序处理 MDM Hub 实施中的任何安全部分，请参阅安全提供程序中的配置说明。

第 2 章

资源

本章包括以下主题：

- [资源概览, 16](#)
- [安全资源和专用资源, 17](#)
- [资源组, 17](#)
- [“安全资源”工具, 18](#)
- [安全资源的配置, 18](#)
- [资源组配置, 19](#)

资源概览

Hub Console：Hub 控制台允许您对外部应用程序公开或隐藏 MDM Hub 资源。

安全资源是向“角色”工具公开的受保护 MDM Hub 资源，从而允许将资源添加到具有特定特权的角色。资源组是安全资源的集合，简化了特权分配。可以使用“安全资源”工具定义资源组以及创建资源的层次结构。

您可以将以下 MDM Hub 资源配置为安全资源：

基础对象

用户有权访问所有安全基础对象、列和内容元数据。

清理函数

用户可以运行所有安全清理函数。

层次结构管理器配置文件

用户有权访问所有安全 层次结构管理器 配置文件。

映射

用户有权访问所有安全映射及其列。

包

用户有权访问所有安全包及其列。

远程包

用户有权访问所有安全远程包。

默认情况下批处理组是安全的。您不能将批处理组的状态改为专用。批处理组具有读取和执行权限。

此外，可以使用 Hub Console：Hub 控制台保护可通过 SIF 请求访问的其他资源，包括元数据、匹配规则集、审计表和用户表。

注意: 如果您使用的是 Informatica Data Director, 可以使用 HTTP 方法 GET 或 POST 访问 Hub 服务器。其他 HTTP 方法, 如 DELETE 或 PUT, 将返回 HTTP 错误。

安全资源和专用资源

您可以将受保护的 MDM Hub 资源配置为安全或专用。

安全

向“角色”工具公开此 MDM Hub 资源, 从而允许将此资源添加到具有特定特权的角色。为用户分配特定角色时, 该用户可以使用 SIF 请求根据与该角色关联的特权访问安全资源。默认情况下, MDM Hub 会将新资源 (例如基础对象) 指定为安全。

专用

在“角色”工具中隐藏 MDM Hub 资源。阻止通过 SIF 请求访问资源。

必须先将资源设置为安全, 然后外部应用程序才可使用 SIF 请求访问 MDM Hub 资源。

您可能不希望向外部应用程序公开某些 MDM Hub 资源。例如, 您的 MDM Hub 实施可能包含仅在批处理作业中 (而不是在 SIF 请求中) 使用的映射或包, 因此这些资源仍可保留为专用。

注意: MDM Hub 不将包列视为安全资源。包列会从父基础对象那里继承安全状态和特权。如果包列基于系统表列, 则无需为它们设置安全, 因为默认情况下它们可供访问。

资源组

资源组是安全资源的逻辑集合。

可以使用“安全资源”工具定义资源组, 然后向资源组分配相关的资源。资源组简化了特权分配, 使您可以为多个资源分配特权并为角色分配资源组。

为简化管理, 可以考虑创建以下类型的资源组:

- 定义一个包含所有安全资源的 ALL_RESOURCES 资源组, 允许您全局设置最低特权。
- 按资源类型定义资源组, 以便可以设置这些类型资源的最低特权。
- 按功能区 (例如 TRAINING_RESOURCES) 定义资源组。
- 定义一个全方位的资源组, 然后将其分配给具有类似特权的多个不同角色。

资源组层次结构

资源组还可以包含其他资源组, 其所属的资源组除外。这意味着您可以构建资源组层次结构, 并简化对大型资源集合的管理。

安全资源

只有安全资源可以属于资源组。专用资源不能属于资源组。

如果将资源的状态更改为专用, 则 MDM Hub 会从任何其所属的资源组中删除该资源。将某个资源的状态设置为安全时, MDM Hub 会将该资源添加到相应的资源组。

“安全资源” 工具

使用 Hub Console：Hub 控制台 中的“安全资源”工具详细管理 MDM Hub 资源的安全，包括将任何 MDM Hub 资源的状态设置为安全或专用。还可以使用资源组配置资源的层次结构。

“安全资源”工具包含以下选项卡：

资源

用于将单个 MDM Hub 资源的状态设置为安全或专用。MDM Hub 以层次结构的形式显示资源，从而显示资源之间的关系。全局资源将显示在层次结构的顶部。

资源组

用于配置资源组。

您可以使用“安全资源”工具向“角色”工具和 SIF 请求公开或隐藏资源。在使用该工具之前，必须先连接到操作引用存储。

安全资源的配置

要浏览和配置 MDM Hub 资源，请使用“安全资源”工具中的“资源”选项卡。

设置 MDM Hub 资源的状态

可以为任何 MDM Hub 资源将资源状态配置为安全或专用。

注意：此状态设置不会应用到仅包含安全资源的资源组或全局资源。

1. 启动“安全资源”工具。
2. 获取写入锁定。
3. 在“资源”选项卡中，浏览“资源”树以找到要配置的资源。
4. 双击资源名称，以在安全和专用之间进行切换。要一次更改多个资源的状态，请执行步骤 5 和 6。
5. 选中需要更改状态的资源。可以根据需要选择多个资源。
6. 更新选定资源的状态。
 - 单击**安全**按钮将选定资源的状态更改为安全。
 - 单击**专用**按钮将选定资源的状态更改为专用。
7. 单击**保存**按钮以保存更改。

筛选资源

要简化更改 MDM Hub 资源集合状态的过程，可以指定筛选器以仅显示要更改的资源。

1. 启动“安全资源”工具。
2. 获取写入锁定。
3. 单击**筛选资源**按钮。

“安全资源”工具将显示“资源筛选器”对话框。

4. 选择资源类型。
 - 选择要包含在筛选器中的资源类型。
 - 清除要从筛选器排除的资源类型。
5. 单击**确定**。

“安全资源”工具将显示已筛选的资源树。

资源组配置

可以使用“安全资源”工具定义资源组以及创建资源的层次结构。然后可以使用“角色”工具将特权分配给单个操作中的多个资源。

“安全资源”工具可直观地区分直接属于当前资源组的资源与间接属于当前资源组的资源。显式添加到资源组的资源具有直接成员关系。属于添加到资源组的某个资源组的资源具有间接成员关系。

例如，您有两个资源组：

- 资源组 A 中包含“使用者”基础对象，即“使用者”基础对象是资源组 A 的直接成员。
- 资源组 B 中包含“地址”基础对象。
- 资源组 A 中包含资源组 B，即“地址”基础对象是资源组 A 的间接成员。

在此示例中，“地址”基础对象在您编辑资源组 A 时不可用。您必须编辑资源组 B 才能编辑“地址”基础对象。

添加资源组

使用“安全资源”工具将资源组添加到资源列表。

1. 启动“安全资源”工具。
2. 获取写入锁定。
3. 单击**资源组**选项卡。

“安全资源”工具将显示“资源组”选项卡。
4. 单击**添加**按钮。

“安全资源”将显示“将资源添加到资源组”对话框。
5. 为资源组输入一个唯一的描述性名称。
6. 根据需要，单击加号 (+) 展开资源层次结构。

每个资源都有一个指示资源组中的成员身份的复选框。如果选择父项，则还会显示所有子项。例如，如果在树中选定基础对象项，则将选定所有基础对象及其子资源。
7. 选择要分配给此资源组的资源。
8. 单击**确定**。

“安全资源”工具会将新资源添加到“资源组”节点中。

编辑和删除资源组

可以使用“安全资源”工具编辑或删除资源组。

1. 启动“安全资源”工具。

2. 获取写入锁定。
3. 单击**资源组**选项卡。
4. 选择要编辑或删除其属性的资源组。
 - 单击**编辑**按钮编辑资源组。
 - 单击**删除**按钮删除资源组。

“安全资源”工具将显示“将资源分配给资源组”对话框。或者“安全资源”工具将从“资源组”节点中移除已删除的资源。
5. 编辑资源组名称。
6. 单击加号 (+) 展开资源层次结构。
7. 选中**仅显示为此资源组选择的资源**复选框。
8. 选择要分配给此资源组的资源。
9. 清除要从此资源组中删除的资源。
10. 单击**确定**。

刷新资源列表

添加资源后，可以刷新资源列表以对其进行更新。

要刷新“资源”列表，请从“安全资源”菜单中选择**刷新**。

“安全资源”工具将更新资源列表。

刷新其他安全更改

您还可以更改刷新所有其他安全更改的时间间隔。

要设置安全更改的刷新频率，请设置 `cmxserver.properties` 文件中的以下参数：

```
cmx.server.sam.cache.resources.refresh_interval
```

注意：默认刷新间隔为 5 个时钟节拍（1 个时钟节拍为 60,000 毫秒），即相当于 5 分钟。

第 3 章

角色

本章包括以下主题：

- [角色概览, 21](#)
- [角色配置, 21](#)
- [特权, 22](#)
- [内部角色和外部角色, 23](#)

角色概览

角色是指向用户或组分配的一组特权。角色代表用于访问安全 MDM Hub 资源的一组特权。

对于要查看或操作安全 MDM Hub 资源的用户，必须向这些用户分配授予其足够特权以访问该资源角色。角色可确定向用户授权访问的内容以及可以在 MDM Hub 中执行的任务。

MDM Hub 角色非常精细且灵活，可使管理员根据组织的安全策略实施复杂的安全保护措施。一些用户（例如管理员）可能被分配对一切内容都有访问权限的单个角色。其他用户（例如数据管理者）可能具有显式受限制特权的单个角色。

还可以向一个角色分配其他角色，从而继承为这些角色配置的访问特权。特权是累加性的，这表示在合并角色时，还会合并这些角色的特权。例如，角色 A 对“地址”基础对象具有读取特权，而角色 B 对其具有创建和更新特权。如果向用户帐户分配了角色 A 和角色 B，该用户帐户将对“地址”基础对象具有读取、创建和更新特权。用户帐户会继承为向用户帐户分配的所有角色配置的特权。

角色配置

您可以在 MDM Hub 中创建、编辑和删除角色。

注意：如果使用全面集成的安全部署（在外部对用户授权），则无需配置角色。

资源特权因用户执行工作所需的访问权限范围而异。对于管理员来说，最佳实践是遵循最少特权原则。为用户分配执行工作所需的最低级别的特权。

添加角色

要配置角色并分配对 MDM Hub 资源的访问特权，请使用安全访问管理器工作台中的“角色”工具。

提示: 避免角色名称中出现空格。当 MDM Hub 与 ActiveVOS 通信时，空格会导致出现错误。

1. 启动“角色”工具。
2. 获取写入锁定。
3. 指向导航窗格中的任意位置，右键单击，然后选择**添加角色**。
“角色”工具会显示“添加角色”对话框。
4. 输入角色的名称。
5. 输入角色的可选说明。
6. 输入角色的外部名称或别名。
7. 单击**确定**。

新角色显示在角色列表中。

编辑和删除角色

要编辑或删除现有角色，请使用安全访问管理器工作台中的“角色”工具。

1. 启动“角色”工具。
2. 获取写入锁定。
3. 滚动浏览角色列表并选择要编辑的角色。
 - 对于要编辑的每个属性，单击其旁边的**编辑**按钮，并指定新值。
 - 指向导航窗格中的任意位置，右键单击，然后选择**删除角色**，在系统提示确认时单击**是**。
4. 单击**保存**按钮以保存更改。

特权

通过 MDM Hub 内部授权，您可以为角色分配特权。

可以为角色分配以下特权：

读取

用户可以查看数据，但不可更改数据。

创建

用户可以在 Hub 存储中创建数据记录

更新

用户可以在 Hub 存储中更新数据记录。

删除

用户可以在 Hub 存储 中删除数据记录。

合并

用户可以合并及取消合并数据。

执行

用户可以运行清理函数和批处理组。

特权决定了外部应用程序用户是否具有 MDM Hub 资源的访问权限。例如，您可以将角色配置为具有对特定包的读取、创建、更新与合并特权。

注意：每种特权均相异，并且必须显式分配。特权不会汇总其他特权。例如，对资源具有更新权限的某个用户不一定对其具有读取权限。两个特权必须单独分配。

在使用 Hub 控制台 时，尽管设置仍影响 Hub 控制台的使用，但不会强制实施特权。例如，数据管理者无法查看合并管理器和数据管理器中的任何包（具有读取特权的包除外）。数据管理者要编辑和保存对特定包中数据的更改，必须具有该包的更新和创建特权。

如果数据管理者没有更新或创建特权，则无法在 数据管理器 中更改任何数据。同样，数据管理者必须具有合并特权才能使用 合并管理器 来合并或取消合并记录。要了解有关合并管理器和数据管理器工具的详细信息，请参阅《*Multidomain MDM 数据管理者指南*》。

内部角色和外部角色

在基于角色的集中安全实施中，必须在 MDM Hub 内部角色与通过 MDM Hub 单独管理的外部角色之间创建映射。

外部角色名称可能与 MDM Hub 环境中使用的内部角色名称不同。

配置详细信息依赖于安全提供程序的角色映射实现。在配置文件中映射角色。可以将一个外部角色映射到多个内部角色。

注意：尽管映射通常以 XML 形式创建，但是配置文件没有预定义的格式。它可能不是 XML 文件，甚至不是一个文件。映射属于自定义用户配置文件或身份验证提供程序实现的一部分。映射的作用是在用户配置文件对象角色列表中填充内部角色 ID。

将资源特权分配给角色

您可以使用安全访问管理器工作台上的“角色”工具为角色分配和编辑资源特权。

1. 启动“角色”工具。
2. 获取写入锁定。
3. 滚动角色列表并选择要为其分配资源特权的角色。
4. 单击**资源特权**选项卡。
5. 展开“资源”层次结构以显示要为此角色配置的安全资源。
6. 对于要配置的每个资源，请执行以下操作：
 - 选择要授予此角色的任何特权。
 - 清除要从此角色中删除的任何特权。
7. 单击**保存**按钮以保存更改。

将角色分配给其他角色

角色还可以继承除其所属的任何角色之外的其他角色。例如，如果将角色 B 分配给角色 A，则角色 A 会继承角色 B 的访问特权。

1. 启动“角色”工具。
2. 获取写入锁定。
3. 滚动角色列表，然后选择要向其分配其他角色的角色。
4. 单击**角色**选项卡。
 - “角色”工具会显示可分配给所选角色的任何角色。
5. 选择要分配给所选角色的任何角色。
6. 清除要从此角色中删除的任何角色。
7. 单击**保存**按钮以保存更改。

为角色生成资源特权的报告

您可以生成一个报告，该报告说明向特定角色授予的资源特权。

1. 启动“角色”工具。
2. 获取写入锁定。
3. 滚动角色列表并选择要为其生成报告的角色。
4. 单击**报告**选项卡。
5. 单击**生成**。
 - “角色”工具将生成报告，并将报告显示在“报告”选项卡中。

将生成的报告另存为 HTML 文件

1. 单击**保存**。
 - “角色”工具将提示您为已保存的报告指定目标位置。
2. 导航至目标位置。
3. 单击**保存**。
 - 安全访问管理器将使用以下命名约定保存报告：
`<ORS_Name>-<Role_Name>-RolePrivilegeReport.html`
其中：
 - `ORS_Name` 是目标数据库的名称。
 - `Role_Name` 是与生成的报告关联的角色。
 - “角色”工具会将当前报告以 HTML 文件的形式保存在目标位置上。随后，您即可使用浏览器显示此报告。

第 4 章

用户和用户组

本章包括以下主题：

- [用户和用户组概览, 25](#)
- [用户配置, 25](#)
- [密码策略配置, 28](#)
- [JDBC 数据源安全配置, 30](#)
- [用户组配置, 31](#)
- [角色与用户和用户组之间的关联, 33](#)

用户和用户组概览

MDM Hub 用户是可以访问 MDM Hub 资源的个人。

在 Hub 存储的主数据库中定义的用户帐户。有关 MDM Hub 用户的说明，请参阅 《*Multidomain MDM 概览指南*》。

用户帐户使用所分配的角色获得对 MDM Hub 资源的访问权限，并继承为每个角色所配置的特权。

您可以使用“配置”工作台中的“用户”工具为 MDM Hub 用户配置用户帐户，以及更改密码和启用外部身份验证。具有足够授权的外部应用程序也可以使用 SIF 请求注册用户帐户，如 《*Multidomain MDM 服务集成框架指南*》中所述。

用户配置

您可以在 MDM Hub 中创建、编辑和删除用户。

根据部署安全的方式，MDM Hub 实施可能要求将用户添加到主数据库。

在以下方案中，必须在主数据库中配置用户：

- 正在使用 MDM Hub 中的内部授权。
- 正在将外部授权与 MDM Hub 配合使用。
- 多个用户使用不同的帐户访问 Hub Console：Hub 控制台。

仅需要定义一次用户，即使同一用户将访问与主数据库关联的多个操作引用存储也是如此。

用户对 MDM Hub 资源的访问权限

用户（包括管理员和数据管理者）可以通过以下方式访问 MDM Hub 资源：

MDM 应用程序

用户可以通过登录 Hub Console：Hub 控制台并使用有权访问的工具与 MDM Hub 进行交互。另外，用户还可以使用 IDD 或置备工具访问基础对象和业务实体中的数据。

第三方应用程序

用户可以通过采用 SIF 类的第三方应用程序与 MDM Hub 数据间接进行交互。这些用户从不登录 Hub Console：Hub 控制台。他们使用可以调用 SIF 类的应用程序登录 MDM Hub。这些用户称为外部应用程序用户。要了解有关开发人员可以调用的 SIF 请求的更多信息，请参阅《*Multidomain MDM 服务集成框架指南*》。

添加用户帐户

使用“安全访问管理器”工作台中的“用户”工具向 MDM Hub 中添加用户帐户。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**用户**选项卡。
4. 单击**添加用户**按钮。
“用户”工具将显示**添加用户**对话框。
5. 输入用户的名字、中间名和姓氏。
6. 输入用户的用户名。这是用户登录 Hub Console：Hub 控制台时输入的名称。
7. 为用户输入一个有效的电子邮件地址。MDM Hub 会将此用户帐户的密码发送到此电子邮件地址。
8. 输入用户的默认数据库。这是用户登录 Hub Console：Hub 控制台时默认选择的数据库。
9. 如果用户帐户针对的是应用程序，选中**应用程序用户**复选框。
注意：应用程序用户用于对受信任的应用程序代表用户生成的请求进行基于证书的身份验证。
10. 输入并验证用户的密码。
11. 选择身份验证的类型。
 - 如果您的 MDM Hub 实施使用经由第三方安全提供程序的身份验证，请选中**使用外部身份验证**复选框。
 - 如果您要在 MDM Hub 中使用内部身份验证，请清除**使用外部身份验证**复选框。
12. 浏览并找到用户的公共证书。MDM Hub 可使用此证书对用户请求进行身份验证。
注意：如果用户帐户针对的是应用程序用户，则必须选择一个证书。
13. 单击**确定**。
“用户”工具会将新用户添加到**用户**选项卡上的用户列表中。

编辑和删除用户帐户

您可以使用“安全访问管理器”工作台中的“用户”工具编辑或删除用户帐户。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**用户**选项卡。
4. 如果要删除用户，请选择要删除的用户帐户。

5. 单击**删除**按钮。
“用户”工具会提示您确认删除。
6. 单击**是**确认删除。
“用户”工具会从用户列表中将已删除的用户帐户移除。
7. 如果要编辑用户，请选择要配置的用户帐户。
8. 要更改姓名，可双击单元格并键入不同的姓名。
9. 选择不同的登录数据库和服务器（如果需要）。
10. 选中**管理员**复选框，为此用户提供管理访问权限，从而使他们可以访问所有 Hub Console：Hub 控制台工具和所有数据库。
11. 选中**启用**复选框以激活此用户帐户并允许此用户登录。
注意：如果对用户使用外部身份验证，则无法通过 Hub Console：Hub 控制台禁用用户帐户。
12. 单击**保存**按钮。
“用户”工具会将您所做的更改保存到用户帐户。

编辑用户补充信息

您可以使用 MDM Hub 管理每个用户的补充信息，例如电子邮件地址或电话号码。MDM Hub 不要求您提供此信息，而且 MDM Hub 也不以任何特殊方式使用此信息。

注意：您不能在 Hub 控制台中更改 admin 用户的电子邮件地址。要更改 admin 用户的电子邮件地址，请直接在 CMX_SYSTEM 架构下的 C_REPOS_USER 表中更新 admin 用户条目。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**用户**选项卡。
4. 选择要编辑其属性的用户。
5. 单击**编辑**按钮。
“用户”工具会显示**编辑用户**对话框。
6. 指定用户的任何属性，例如职位、电子邮件地址或登录消息。登录消息是 Hub Console：Hub 控制台在此用户登录后显示的消息。
7. 单击**确定**。
8. 单击**保存**按钮以保存更改。

更改用户帐户的密码设置

您可以更改用户的密码设置。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**用户**选项卡。
4. 选择要更改其密码的用户。
5. 单击**更改密码**按钮。
“用户”工具会为选定用户显示**更改密码**对话框。
6. 指定并验证新密码。

7. 选择身份验证的类型。
 - 如果 MDM Hub 实施通过第三方安全提供程序使用身份验证，请选中**使用外部身份验证**复选框。
 - 如果您要在 MDM Hub 中使用内部身份验证，请清除**使用外部身份验证**复选框。
8. 单击**确定**。

配置用户访问操作引用存储的权限

您可以配置用户对 操作引用存储 数据库的访问权限。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**目标数据库**选项卡。

“用户”工具将显示“目标数据库”选项卡。
4. 展开每个数据库节点以查看可以访问该数据库的用户。
5. 要将用户分配更改为数据库，请右键单击数据库名称并选择**分配用户**。

“用户”工具会显示**将用户分配给数据库**对话框。
6. 选择您希望分配到选定数据库的任何用户的名称。
7. 清除您不希望分配到选定数据库的任何用户的名称。
8. 单击**确定**。

密码策略配置

您可以为所有用户定义全局密码策略。为各个用户配置可替代全局密码策略的专用密码策略。所有密码都区分大小写。

注意: 如果在启用了安全的 JBoss 应用程序服务器上部署 MDM Hub，请确保您设置的密码符合 JBoss 密码策略。您的密码还必须符合 MDM Hub 全局密码策略。这非常重要，因为 Hub Console：Hub 控制台的密码和 JBoss 的密码必须匹配。

密码策略设置

您可以为 MDM Hub 用户指定密码策略设置。

MDM Hub 允许您按照专用密码策略设置用户：

密码长度

密码的最小和最大长度（字符数）。

密码过期

指定密码是否过期以及密码有效的天数。

选中**密码过期**复选框以设置密码的过期时间段。清除**密码过期**复选框以设置不会过期的密码。

如果选中**密码过期**复选框，请指定一个天数，密码在此天数后必须到期。可以设置的密码到期时间段最小值为 10。

登录设置

宽限登录次数和允许的失败登录最大次数。

密码历史记录

可以重用密码的次数。

密码要求

选中**密码模式验证已启用**复选框以实施密码模式。可以为密码模式指定以下条件：

- 唯一字符的最小数量
- 密码开头必须为
- 密码必须包含
- 密码结尾必须为

管理全局密码策略

全局密码策略适用于未指定专用密码策略的用户。

1. 启动**用户**工具。
2. 获取写入锁定。
3. 单击**全局密码策略**选项卡。
此时将显示“全局密码策略”窗口。
4. 指定密码策略设置。
5. 单击**确定**。
6. 单击**保存**按钮保存全局设置。

管理专用密码策略

可以为任何用户指定替代全局密码策略的专用密码策略。

注意：密码策略管理的最佳实践是确保大多数用户密码由全局策略而不是许多专用策略进行管理。

1. 启动“用户”工具。
2. 获取写入锁定。
3. 单击**用户**选项卡。
4. 选择要为其设置专用密码策略的用户。
5. 单击**管理密码策略**按钮。
此时将显示所选用户的**专用密码策略**窗口。
6. 启用**专用密码策略已启用**选项。
7. 为用户指定密码策略设置。
8. 单击**确定**。
9. 单击**保存**按钮以保存更改。

JDBC 数据源安全配置

在 MDM Hub 实施中，如果 JDBC 数据源使用应用程序服务器安全，则必须配置 `cmxserver.properties` 文件中的设置。

您必须在 `cmxserver.properties` 文件中存储用于 JDBC 数据源的应用程序服务器的用户名和密码。密码不能以明文形式显示。您必须先将密码保存在 `cmxserver.properties` 文件中，然后再对其进行加密。

要了解有关受保护 JDBC 数据源的详细信息，请参阅应用程序服务器文档。

安全 JDBC 数据源的用户名和密码

要在 `cmxserver.properties` 文件中为安全 JDBC 数据源配置用户名和密码，请使用以下参数：

```
databaseId.username=username  
databaseId.password=encryptedPassword
```

其中 `databaseId` 是 JDBC 数据源的唯一标识符。

Oracle SID 连接类型的数据库 ID

对于 Oracle SID 连接类型，数据库 ID 由以下字符串组成：

<数据库主机名>-<Oracle SID>-<架构名称>

例如，通过以下设置：

- <数据库主机名> = localhost
- <Oracle SID> = MDMHUB
- <架构名称> = Test_ORS

用户名和密码属性为：

```
localhost-MDMHUB-Test_ORS.username=weblogic  
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Oracle 服务连接类型的数据库 ID

对于 Oracle 服务连接类型，数据库 ID 由以下字符串组成：

<服务名称>-<架构名称>

例如，通过以下设置：

- <服务名称> = MDM_Service
- <架构名称> = Test_ORS

用户名和密码属性为：

```
MDM_Service-Test_ORS.username=weblogic  
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

IBM DB2 连接类型的数据库 ID

对于 IBM DB2 连接类型，数据库 ID 由以下字符串组成：

<数据库主机名>-<数据库名称>-<架构名称>

例如，通过以下设置：

- <数据库主机名> = localhost

- <数据库名称> = dsui2
- <架构名称> = DS_UI2

用户名和密码属性为：

```
localhost-dsui2-DS_UI2.username=weblogic
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Microsoft SQL Server 连接类型的数据库 ID

对于 Microsoft SQL Server 连接类型，数据库 ID 由以下字符串组成：

<数据库主机名>-<数据库名称>

例如，通过以下设置：

- <数据库主机名> = localhost
- <数据库名称> = ds_ui1

用户名和密码属性为：

```
localhost-ds_ui1.username=weblogic
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

主数据库的数据库 ID

如果要确保访问主数据库的 JDBC 数据源安全，则 databaseId 为 CMX_SYSTEM。在此情况下，属性应为：

```
CMX_SYSTEM.username=weblogic
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

密码加密

要为数据库架构生成加密的密码，请使用以下命令：

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password
Plaintext Password: password
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

用户组配置

用户组是用户帐户的逻辑集合。

用户组可简化安全管理。例如，您可以将外部应用程序用户合并在一个用户组中，然后向该用户组而不是每个单独的用户授予安全角色。除了用户之外，用户组还可以包含其他用户组。

使用安全访问管理器工作台“用户和组”工具的“组”选项卡配置用户组。

启动“用户和组”工具

在 Hub Console：Hub 控制台中启动“用户和组”工具。

1. 在 Hub Console：Hub 控制台中，连接到 操作引用存储（如果您尚未连接）。

2. 展开安全访问管理器工作台，然后单击**用户和组**。

Hub Console：Hub 控制台会显示“用户和组”工具。

“用户和组”工具包含以下选项卡：

组

用于定义用户组和将用户分配给用户组。

分配给数据库的用户

用于将用户帐户与数据库相关联。

将用户/组分配给角色

用于将用户和用户组与角色相关联。

将角色分配给用户/组

用于将角色与用户和用户组相关联。

添加用户组

您可以使用“安全访问管理器”工作台中的“用户和组”工具添加用户组。

1. 启动“用户和组”工具。
 2. 获取写入锁定。
 3. 单击**组**选项卡。
 4. 单击**添加**按钮。
“用户和组”工具会显示**添加用户组**对话框。
 5. 输入用户组的描述性名称。
 6. 或者，输入用户组的说明。
 7. 单击**确定**。
- 此时“用户和组”工具会将新的用户组添加到列表中。

编辑和删除用户组

还可以使用“用户和组”工具编辑或删除用户组。

1. 启动“用户和组”工具。
2. 获取写入锁定。
3. 单击**组**选项卡。
4. 滚动用户组列表并选择要编辑的用户组。
5. 如果要删除用户组，请单击**删除**按钮。
“用户和组”工具将提示您确认删除。
6. 单击**是**。
“用户和组”工具将从列表中移除已删除的用户组。
7. 如果要编辑用户组，请单击您要编辑的每个属性旁边的**编辑**按钮，然后指定新值。
8. 单击**保存**按钮以保存更改。

将用户和用户组分配给用户组

要将成员分配给用户组，请执行以下操作：

1. 启动“用户和组”工具。
2. 获取写入锁定。
3. 单击**组**选项卡。
4. 滚动用户组列表并选择要编辑的用户组。
5. 右键单击刚创建的用户组，然后选择**分配用户和组**。
“用户和组”工具会显示**分配给用户组**对话框。
6. 选择要分配给选定用户组的任何用户和用户组的名称。
7. 清除不希望分配给选定用户组的任何用户和用户组的名称。
8. 单击**确定**。

将用户分配给当前 ORS 数据库

要将用户分配给当前 操作引用存储 数据库，请执行以下操作：

1. 启动“用户和组”工具。
2. 获取写入锁定。
3. 单击**分配给数据库的用户**选项卡。
4. 单击**将用户分配给数据库**按钮将用户分配给 操作引用存储 数据库。
“用户和组”工具会显示**将用户分配给数据库**对话框。
5. 选择您希望分配到选定 操作引用存储 数据库的任何用户的名称。
6. 清除您不希望分配到选定 操作引用存储 数据库的任何用户的名称。
7. 单击**确定**。

角色与用户和用户组之间的关联

可以将角色与用户和用户组相关联。可以使用**用户和组**工具来通过以下方式将角色与用户关联：

- 向角色分配用户和用户组。
- 向用户和用户组分配角色。

选择最适合您的实现的方式。

将用户和用户组分配给角色

要将用户和用户组分配给角色，请执行以下操作：

1. 启动“用户和组”工具。
2. 获取写入锁定。
3. 单击**将用户/组分配给角色**选项卡。
4. 选择要向其分配用户和用户组的角色。
5. 单击**编辑**按钮。

“用户和组”工具会显示**将用户分配给角色**对话框。

6. 选择要分配给选定角色的所有用户和用户组的名称。
7. 清除不希望分配给选定角色的任何用户和用户组的名称。
8. 单击**确定**。

向用户和用户组分配角色

要将角色分配给用户和用户组，请执行以下操作：

1. 启动“用户和组”工具。
2. 获取写入锁定。
3. 单击**将角色分配给用户/组**选项卡。
4. 选择要向其分配角色的用户或用户组。
5. 单击**编辑**按钮。

“用户和组”工具会显示**将角色分配给用户**对话框。

6. 选择要分配给选定用户或选定用户组的角色。
7. 清除不希望分配给选定用户或用户组的角色。
8. 单击**确定**。

第 5 章

安全提供程序

本章包括以下主题：

- [安全提供程序概览, 35](#)
- [安全提供程序管理, 35](#)
- [提供程序文件管理, 36](#)
- [安全提供程序设置, 37](#)
- [提供程序属性, 38](#)
- [自定义提供程序, 39](#)
- [外部身份验证, 40](#)

安全提供程序概览

安全提供程序是为访问 MDM Hub 的用户提供诸如身份验证和授权等安全服务的第三方应用程序。安全提供程序是某些 MDM Hub 安全部署方案的一部分。

提供程序文件包含安全提供程序的配置文件信息。如果要使用其他第三方安全提供程序，请使用“安全提供程序”工具将提供程序文件上传到 MDM Hub。还可以使用“安全提供程序”工具修改、删除、启用或禁用“提供程序”列表中的安全提供程序。

MDM Hub 附带了一组默认的内部安全提供程序。也可以添加第三方安全提供程序。内部安全提供程序无法删除。

安全提供程序管理

您可以通过 Hub Console：Hub 控制台的“配置”工作台中的“安全提供程序”工具管理 MDM Hub 实施中的安全提供程序。

可以从 MDM Hub 内部的默认选择或从您自己的自定义添加提供程序选择中添加安全提供程序。内部安全提供程序无法删除。

MDM Hub 支持以下类型的安全提供程序：

身份验证提供程序

通过验证用户的身份对其进行身份验证。通知 MDM Hub 用户其身份属实。此类型的安全提供程序不验证用户是否具有所需的特权来访问特定 MDM Hub 资源。

授权提供程序

通知 MDM Hub 用户是否具有所需的特权来访问特定 MDM Hub 资源。

用户配置文件提供程序

通知 MDM Hub 有关个人用户的信息，如用户特定的属性和用户所属的角色。

内部提供程序表示身份验证、授权和用户配置文件服务的内部 MDM Hub 实施。

一些 MDM Hub 默认提供程序是父提供程序。父提供程序始终为身份验证和授权请求返回肯定的响应。不希望配置用户、角色和特权时，在开发环境中使用父提供程序。父提供程序还可以用于生产环境，即基于 SIF 请求以层的形式提供安全性，以便提高环境的性能。

提供程序文件管理

提供程序文件包含安全提供程序的配置文件信息。

如果要使用您自己的第三方安全提供程序，必须通过“安全提供程序”工具明确注册它们。要注册安全提供程序，可上载包含注册所需的配置文件信息的提供程序文件。

提供程序文件是包含以下数据的 JAR 文件：

- 描述一个或多个外部安全提供程序的清单。每个安全提供程序具有以下设置：
 - 提供程序名称
 - 提供程序说明
 - 提供程序类型
 - 提供程序工厂类名称
 - 指定提供程序配置详细信息的属性。它可以是名称-值对的列表：属性名称和默认值。
- 提供程序实施和任何所需的第三方库。

Informatica 资源工具包在 Hub 服务器上复制提供程序文件的示例实施。有关示例提供程序文件的详细信息，请参阅《*Multidomain MDM 资源工具包指南*》。

上载提供程序文件

上载提供程序文件以添加或更新提供程序信息。

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 在左侧导航窗格中，右键单击“提供程序文件”，然后选择**上载提供程序文件**。
“安全提供程序”工具提示您为此提供程序选择 JAR 文件。
4. 指定 JAR 文件，根据需要导航文件系统，然后选择要上载的 JAR 文件。
5. 单击**打开**。
“安全提供程序”工具将检查选定的文件，以确定其是否为有效的提供程序文件。
6. 如果您上载的提供程序文件具有与现有提供程序文件相同的名称，则“安全提供程序”工具将询问您是否要覆盖现有提供程序文件。单击**是**进行确认。
“安全提供程序”工具通过其他提供程序信息填充“提供程序”列表。上载提供程序文件后，可以从文件系统中删除原始文件。

删除提供程序文件

如果您不再使用某个安全提供程序，可以删除提供程序文件。

1. 启动“安全提供程序”工具。
 2. 获取写入锁定。
 3. 在左侧导航窗格中，右键单击要删除的提供程序文件，然后选择**删除提供程序文件**。
“安全提供程序”工具将提示您确认删除。
 4. 单击**是**。
“安全提供程序”工具会将删除的提供程序文件从列表中移除。
- 注意：**不能删除 MDM Hub 附带的内部提供程序文件。

安全提供程序设置

“安全提供程序”工具会显示已注册提供程序的列表。

已注册提供程序的列表按提供程序类型排序。“提供程序”列表中的提供程序序列还表示调用它们的顺序。用户需要至少按照“提供程序”列表中的一个提供程序进行身份验证。

例如，尝试登录并提供您的用户名和密码时，MDM Hub 会将您的登录凭据提供给身份验证列表中的每个身份验证提供程序。MDM Hub 会按照顺序对整个列表执行操作。如果通过列表中的一个提供程序成功进行身份验证，MDM Hub 就认为您已通过身份验证。如果通过任何身份验证提供程序进行身份验证均失败，则您未通过身份验证。

更改安全提供程序设置

要更改安全提供程序的设置，请执行以下步骤：

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 选择您要修改的安全提供程序。
4. 在“属性”面板中，单击要编辑的任何设置旁边的**编辑**按钮。
5. 单击**保存**按钮以保存更改。

启用和禁用安全提供程序

1. 获取写入锁定。
2. 选择要启用或禁用的安全提供程序。
 - 选中**启用**复选框以启用禁用的安全提供程序。
 - 清除**启用**复选框以禁用安全提供程序。

一旦禁用，提供程序名称将不可用，并移至“提供程序”列表的末尾。不能在“提供程序”列表中重新排列已禁用的提供程序。

3. 单击**保存**按钮以保存更改。

移动安全提供程序的处理顺序

MDM Hub 会根据安全提供程序在“提供程序”列表中显示的顺序来处理安全提供程序。您可以重新排列安全提供程序的显示顺序。

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 要上移提供程序，请右键单击要移动的提供程序，然后选择**上移提供程序**。
“安全提供程序”工具会将此提供程序移动到该“提供程序”列表中上一个提供程序的前面，然后刷新导航窗格。
4. 要下移提供程序，请右键单击要移动的提供程序，然后选择**下移提供程序**。
“安全提供程序”工具会将此提供程序移动到该“提供程序”列表中上一个提供程序的下方，然后刷新导航窗格。

提供程序属性

“提供程序”面板包含以下字段：

名称

此安全提供程序的名称。

说明

此安全提供程序的说明。

提供程序类型

安全提供程序的类型。类型可以是以下值之一：

- 身份验证
- 授权
- 用户配置文件

提供程序文件

与此安全提供程序关联的提供程序文件的名称，或者对于内部提供程序，该字段为**内部提供程序**。

启用

指示此安全提供程序是否已启用。启用的安全提供程序处于选中状态。禁用的安全提供程序处于未选中状态。请注意，不能禁用内部提供程序。

属性

此安全提供程序所定义的其他属性。每个属性均为一个名称 - 值对。安全提供程序可能需要或允许使用一些唯一属性，您可以在此处进行指定。

添加提供程序属性

要添加提供程序属性，请执行以下步骤：

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 在导航窗格中，选择要向其添加属性的身份验证提供程序。

4. 单击**添加**按钮。
“安全提供程序”工具将显示“添加提供程序属性”对话框。
5. 指定属性的名称。
6. 指定要分配给此属性的值。
7. 单击**确定**。

编辑提供程序属性

要编辑现有提供程序属性，请执行以下步骤：

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 在导航窗格中，选择要为其编辑属性的身份验证提供程序。
4. 对于要编辑的每个属性，单击其旁边的**编辑**按钮，并指定新值。
5. 单击**保存**按钮以保存更改。

自定义提供程序

您可以将自定义提供程序类打包在构成提供程序文件的 JAR 或 ZIP 文件中。

在 `providers.properties` 文件中指定自定义提供程序的设置。然后，将该文件放置在 `META-INF` 目录下的 JAR 文件中。这些设置随后将被加载器转换为 Hub 控制台中显示的内容。

`provider.properties` 文件具有以下元素：

`ProviderList`

所包含的提供程序名称的列表（以逗号分隔）。

`File-Description`

包的说明。

`XXX-Provider-Name`

提供程序 `XXX` 的显示名称。

`XXX-Provider-Description`

提供程序 `XXX` 的说明。

`XXX-Provider-Type`

提供程序 `XXX` 的类型。可能的值为 `USER_PROFILE_PROVIDER`、`JAAS_LOGIN_MODULE` 和 `AUTHORIZATION_PROVIDER`。

`XXX-Provider-Factory-Class-Name`

提供程序的实施类，其也在同一 JAR 或 ZIP 文件中。

`XXX-Provider-Properties`

定义提供程序属性的名称/值对的列表（以逗号分隔）。

注意：提供程序存档文件中必须包含要使自定义提供程序起作用所需的所有类，以及所需的资源。这些资源是您的实施特有的。

providers.properties 文件示例

注意: 除了 XXX-Provider-Properties 之外的所有设置都是必需的。

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name:
com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

外部身份验证

可以通过 Java 身份验证和授权服务 (JAAS)，对用户配合使用外部身份验证与 MDM Hub。

MDM Hub 为以下类型的身份验证标准提供了模板：

- 轻型目录访问协议 (LDAP)
- Microsoft Active Directory
- 使用 Kerberos 协议的网络身份验证

这些模板提供了这些身份验证标准所需的设置（如协议、服务器名称和端口）。您可以使用这些模板添加新的登录模块以及所需的设置。有关这些身份验证标准的详细信息，请参阅相应的供应商文档。

添加登录模块

要在 MDM Hub 中设置外部身份验证，必需创建登录模块。

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 右键单击“身份验证提供程序(登录模块)”，然后选择**添加登录模块**。
“安全提供程序”工具将显示“添加登录模块”对话框。
4. 单击向下箭头并选择登录模块的模板。

OpenLDAP 模板

基于 LDAP 身份验证属性。

MicrosoftActiveDirectory 模板

基于 Active Directory 身份验证属性。

Kerberos 模板

基于 Kerberos 身份验证属性。

5. 单击**确定**。
“安全提供程序”工具会将新的登录模块添加到列表。
6. 在“属性”面板中，单击要编辑的任意属性旁边的**编辑**按钮。为要创建的登录模块的类型指定设置。
7. 单击**保存**按钮以保存更改。

删除登录模块

如果需要，可以删除登录模块。

1. 启动“安全提供程序”工具。
2. 获取写入锁定。
3. 在导航窗格中，右键单击“身份验证提供程序(登录模块)”下的某个登录模块，然后选择**删除登录模块**。
“安全提供程序”工具将提示您确认删除。
4. 单击**是**。
“安全提供程序”工具将从列表中移除已删除的登录模块，并刷新左侧导航窗格。

第 6 章

应用程序级别安全

本章包括以下主题：

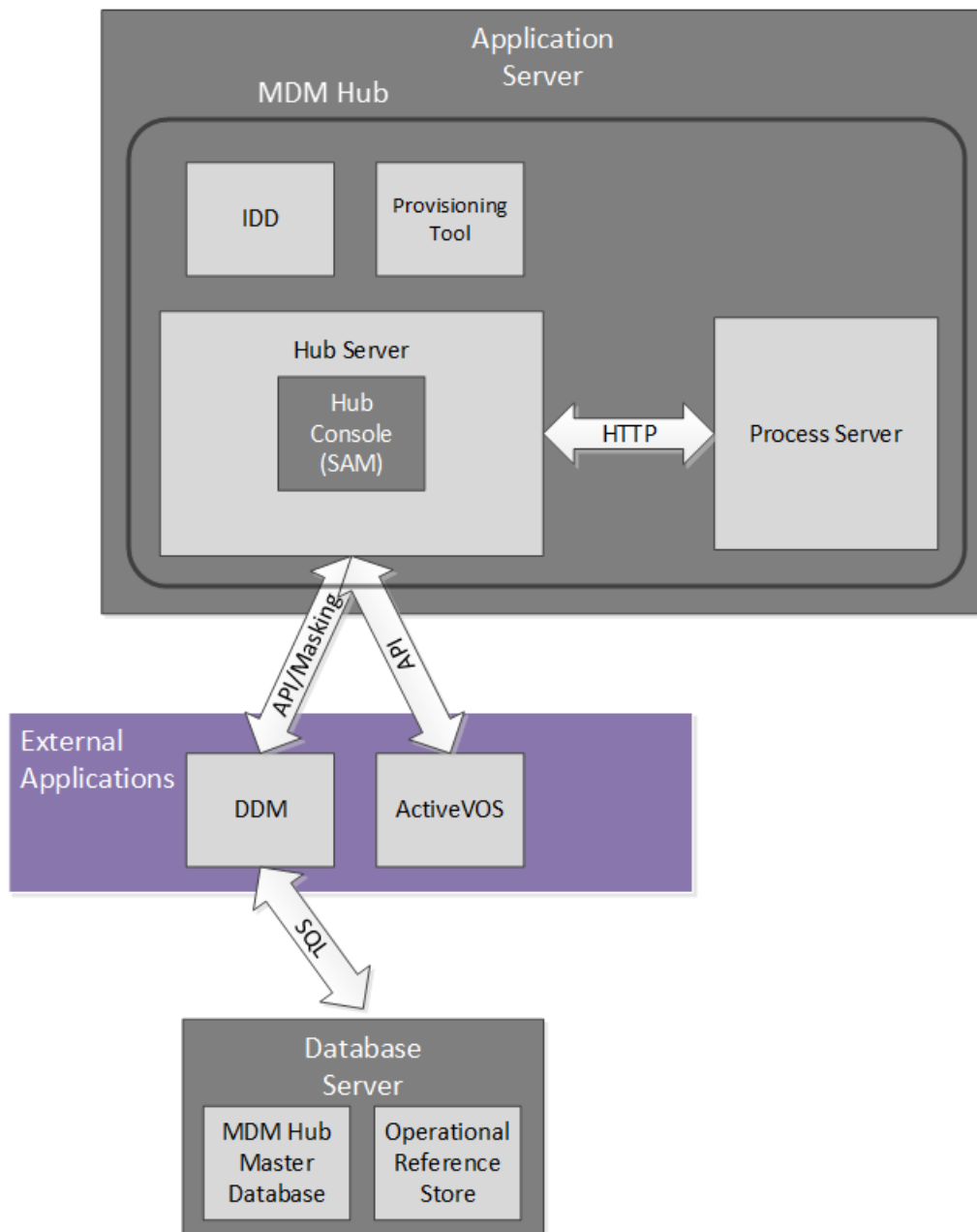
- [应用程序级别的安全性概览, 42](#)
- [Informatica Data Director, 43](#)
- [置备工具, 44](#)
- [ActiveVOS, 44](#)
- [Dynamic Data Masking, 44](#)
- [在 Linux 上设置 WebLogic T3S 通道。 , 46](#)

应用程序级别的安全性概览

安全访问模块 (SAM) 是 MDM Hub 的安全模块，可控制用户凭据和角色。MDM Hub 实施中的其他应用程序和组件也具有安全设置，这些安全设置可确保应用程序和组件与 MDM Hub 安全通信。例如，您可以为 Informatica Data Director 配置数据级别安全。

Informatica 对 Informatica 产品开展了内部安全测试。例如，Informatica 使用行业标准扫描应用程序来测试产品是否存在安全漏洞（例如 SQL 注入攻击）。与 SAM 结合使用的其他 Informatica 安全应用程序可为 MDM Hub 实施增添额外一层安全。Informatica Dynamic Data Masking (DDM) 可对数据进行屏蔽，以防止敏感信息受到未经授权的访问。Informatica MDM 置备工具和 Informatica ActiveVOS 并非安全应用程序，但它们仍能与 MDM Hub 安全通信。

下图显示了一个 MDM Hub 实施示例以及各组件如何彼此连接：



Informatica Data Director

Informatica Data Director 是一款适用于 MDM Hub 且基于 Web 的数据管理应用程序。配置 Data Director 应用程序时，业务用户可以创建、管理、消费和监视主数据。

Informatica Data Director 遵循开放式 Web 应用程序安全项目 (Open Web Application Security Project, OWASP) 提出的十大安全建议。Informatica 使用 IBM Security AppScan 来测试安全漏洞 (例如 SQL 注入攻击)。HTTP 方法 GET 或 POST 可以从 IDD 检索信息，而其他 HTTP 方法 (例如，DELETE 或 PUT) 将返回 HTTP 错误。

配置 Data Director 应用程序时，可以将操作引用存储中的表组织到业务实体或主题区域中。两种方法均可以将您要视为一个单元的相关数据（例如关于某个客户的所有数据）分为一组。自 Multidomain MDM 10.1 版开始，业务实体是建议的组织方式。业务实体是 Entity 360 框架的核心，包括业务实体服务和现代实体视图。

对于数据安全，Data Director 应用程序使用在操作引用存储上设置的用户角色和资源特权。请记住，MDM 管理员在 Hub 控制台 中使用安全访问管理器工作台定义每个用户角色的资源特权。在 Data Director 应用程序中，用户可以执行其用户角色允许的操作。

业务实体的角色特权和主题区域以不同方式派生自资源特权，因此安全可能会略有不同。但是，两种方式同样安全。有关业务实体的安全的详细信息，请参阅《《Multidomain MDM 置备工具指南》》。有关主题区域的安全配置和数据安全的详细信息，请参阅《《Multidomain MDM Data Director 实施指南》》。

置备工具

您可以使用置备工具，基于在操作引用存储 (Operational Reference Store, ORS) 中定义的架构信息创建业务实体模型。业务实体模型是 Data Director 中的 Entity 360 框架的基本组成部分。

您必须登录到置备工具才能配置业务实体。

当您在处理配置文件时，应将所做更改保存到临时工作区。发布更改之前，置备工具不会应用更改。如果多个用户同时更改 ORS 的业务实体配置，则会使用最近发布的配置更新 MDM Hub。

置备工具和 Hub 服务器必须在同一个应用程序服务器上运行。

有关详细信息，请参阅《《Multidomain MDM 置备工具指南》》。

ActiveVOS

Informatica ActiveVOS[®] 是一款业务流程管理 (BPM) 工具，可帮助您实现业务流程自动化。您可以创建集成了人员、流程和系统的流程模型，并借此提高业务效率。

使用 ActiveVOS 可以确保更新的实体数据先经过变更-批准工作流，然后再将更新的记录用于最佳数据版本 (BVT) 记录。例如，业务流程可能需要高级经理先审阅并批准客户数据更新，然后再将相关数据变为主数据。

为支持变更-批准工作流，MDM Hub 和 Data Director 与 ActiveVOS Server 集成。预定义的 MDM 工作流、任务类型以及角色可保证组件彼此同步。您可以对 MDM 实施进行配置，使其与嵌入式 ActiveVOS Server 配合工作。或者，您也可以在环境中运行 ActiveVOS 的独立实例。

嵌入式 ActiveVOS 可对同时受 MDM 和 ActiveVOS 信任的特定主体从 Data Director 和 MDM Hub 发出的请求进行身份验证。该主体称为受信任用户。系统管理员可以在应用程序服务器中为受信任用户创建凭据和角色。

ActiveVOS Server 和 MDM Hub 必须在同一个应用程序服务器上运行。有关详细信息，请参阅《《Multidomain MDM 配置指南》》。

Dynamic Data Masking

Informatica Dynamic Data Masking 是一款数据安全产品，可在客户端与数据库之间运行来防止未经授权访问敏感信息。Dynamic Data Masking 可侦听发送到数据库的请求，并在将请求结果发送回客户端之前对数据应用屏蔽。

Dynamic Data Masking 为 MDM Hub 管理的数据库提供了额外级别的数据安全。使用 Dynamic Data Masking 管理控制台配置 Dynamic Data Masking 与操作引用存储的连接，并设置用于数据的屏蔽规则。在注册操作引用存储时，配置 MDM Hub 与 Dynamic Data Masking 的连接。

MDM 安装程序不会将 Dynamic Data Masking 与 MDM Hub 一起安装。必须单独安装 Dynamic Data Masking。有关 Dynamic Data Masking 安装的详细信息，请参阅 Dynamic Data Masking 文档。

注意: 要在 MDM Hub 中使用 Dynamic Data Masking，必须安装有 Dynamic Data Masking 9.6.0 以及紧急错误修复 14590。较早版本的 Dynamic Data Masking 与 MDM Hub 不兼容。

在 Dynamic Data Masking 与 MDM Hub 之间集成

安装 Dynamic Data Masking 并正确进行设置后，可以将 Dynamic Data Masking 与 MDM Hub 集成在一起。

以下步骤介绍了集成过程：

1. 在 Dynamic Data Masking 管理控制台中，创建 Dynamic Data Masking 服务。配置侦听器端口号以匹配客户端用于向数据库发送请求的端口号。
2. 为需要数据屏蔽的数据库定义数据库连接属性。
3. 创建连接规则。配置规则以标识必须屏蔽的数据库请求。为连接规则集分配数据库和安全规则集。
4. 创建安全规则集。定义规则来屏蔽发回 MDM Hub 的数据。
5. 在 Hub 控制台中，配置与 Dynamic Data Masking 的连接。

为操作引用存储运行进程时，Dynamic Data Masking 会先对数据库应用规则，然后再将数据返回到 MDM Hub。

注意: 如果不添加 Dynamic Data Masking 与操作引用存储的连接，则 MDM Hub 会绕过您定义的 Dynamic Data Masking 规则。

有关如何配置 Dynamic Data Masking 的详细信息，请参阅《*Informatica Dynamic Data Masking 管理员指南*》。

适用于 MDM Hub 的 Dynamic Data Masking 最佳实践

您可以借助建议的最佳实践，在 MDM Hub 中有效地使用 Dynamic Data Masking。

在规则编辑器中创建 Dynamic Data Masking 规则的最佳实践

Dynamic Data Masking 在规则编辑器中按照从上到下的顺序评估规则。因此，如果创建非屏蔽规则，则必须将它们放置在您创建的任何屏蔽规则之上以使它们生效。

允许用户查看未屏蔽数据的最佳实践

Dynamic Data Masking 不会屏蔽数据库中的数据。查看 MDM Hub 中的数据时，数据会以屏蔽的形式显示。在 Dynamic Data Masking 中使用创建视图语句为用户提供查看未屏蔽数据的特权。

阻止用户的最佳实践

要阻止用户添加应用了屏蔽的记录，必须为每个受影响的基础对象创建单独的规则。定义文本匹配项 %INSERT %<BO_NAME>%<ROLE NAME>% 和阻止语句处理操作。

允许用户更新屏蔽数据的最佳实践

默认情况下，Dynamic Data Masking 引擎会阻止用户编辑具有屏蔽数据的表。如果要更新 MDM Hub 中的屏蔽数据，可以在 Dynamic Data Masking 规则编辑器中创建规则以允许用户更新屏蔽的列。

通过 MDM_SYSTEM 指示器创建规则的最佳实践

在 MDM Hub 中，用户 MDM_SYSTEM 是用于系统调用的内部指示器。MDM_SYSTEM 不会显示在 Hub 控制台的角色列表中。Dynamic Data Masking 根据用户所具有的 MDM Hub 角色应用屏蔽。在规则编辑器中创建 Dynamic Data Masking 规则时，不要仅为 MDM_SYSTEM 指示器创建规则。帐户图表安装和配置指南必

须将 MDM_SYSTEM 与用户名或属于用户的角色组合在一起。可以将 MDM_SYSTEM 指示器与任何其他规则组合在一起以在 Dynamic Data Masking 中创建精细规则。

为操作引用存储设置 Dynamic Data Masking

通过 Hub 控制台注册操作引用存储时，配置 Dynamic Data Masking 与 MDM Hub 的连接。

1. 启动 Hub 控制台。
此时将显示**更改数据库**对话框。
2. 选择 MDM Hub 主数据库，然后单击**连接**。
3. 在“配置”工作台上，启动**数据库工具**。
4. 获取写入锁定。
5. 单击**注册数据库**按钮。
此时将显示 **Informatica MDM Hub 连接向导**，并提示您选择数据库类型。
6. 选择数据库的类型，然后单击**下一步**。
7. 配置数据库的连接属性。
8. 在**端口**字段中，输入的端口必须与数据库的 Dynamic Data Masking 侦听器端口匹配。
9. 在 **DDM 连接 URL** 字段中，输入 Dynamic Data Masking 服务器的 URL。
10. 单击**完成**。
此时将显示**注册数据库**对话框。
11. 单击**确定**。
MDM Hub 会注册操作引用存储。
12. 选择注册的操作引用存储，然后单击**测试数据库连接**按钮以测试数据库设置。
如果使用 WebSphere，请在测试数据库连接之前重新启动 WebSphere。
“测试数据库”对话框将显示数据库连接测试的结果。
13. 单击**确定**。
Dynamic Data Masking 会连接到您注册的操作引用存储。

在 Linux 上设置 WebLogic T3S 通道。

WebLogic T3S 是可为 MDM Hub 设置的基于 SSL 的协议。

以下步骤假设您已熟悉如何创建和使用密钥库、为 SSL 配置服务器实例以及创建通道。有关详细信息，请参阅 WebLogic 文档。

1. 在开始之前，您必须具有要用于标识的密钥库。
2. 在 WebLogic 管理控制台中，导航到用于 MDM 的服务器实例，然后使用以下属性配置 SSL：
 - **标识和信任位置** = 密钥库
 - **私钥位置** = 来自自定义标识密钥库
 - **私钥别名** = <密钥库中定义的别名>
 - **私钥密码短语** = <密钥库中定义密码短语>

- 证书位置 = 来自自定义标识密钥库
 - 受信任的证书机构 = 来自 Java 标准信任密钥库
3. 打开管理员命令提示 (cmd) 窗口, 然后使用 keytool 命令将密钥库导入 lib/security/cacerts 下的 JDK 和 JRE 目录。
以下示例代码显示了相关语法:


```
keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation directory>/jre/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/wls12c_server.cer" -v

keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation directory>/lib/security/cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/<WebLogic server instance>/keystores/wls12c_server.cer" -v
```

注意: 如果需要 keytool 命令的帮助, 请参阅 Java 文档。
 4. 导航到 <WebLogic domain>/bin/startWebLogic.sh 文件, 并设置以下 Java 选项:


```
-Doracle.jdbc.J2EE13Compliant=true
```
 5. 在 WebLogic 管理控制台中, 创建与 SSL 配置匹配的 T3S 通道。设置以下属性:
 - 名称 = <通道名称>
 - 协议 = t3s
 - 侦听地址 = <密钥库中定义的主机名>
 - 侦听端口 = <密钥库中定义的端口>
 - 选择已启用隧道
 - 选择双向 SSL
 - 验证服务器私钥别名是否显示您在配置 SSL 时指定的别名。
 6. 保存通道, 然后验证该通道是否显示在网络通道的列表中。
 7. 如果通过 Entity 360 视图使用 Informatica Data Director, 则导航到 <WebLogic 域>/bin/setDomainEnv.sh 文件, 然后设置以下 MDM 选项:
 - e360.mdm.protocol=t3s
 - e360.mdm.host=<T3S 通道侦听地址>
 - e360.mdm.host=<T3S 通道侦听端口>
 8. 重新启动 WebLogic。
 9. 通过对通道进行 ping 测试该通道是否正常工作。


```
java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen Port> -username <WebLogic username> -password <WebLogic password> PING
```
 10. 现在可以使用 HTTPS 和安全端口启动 Hub 控制台。


```
https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
```

第 7 章

密码哈希

本章包括以下主题：

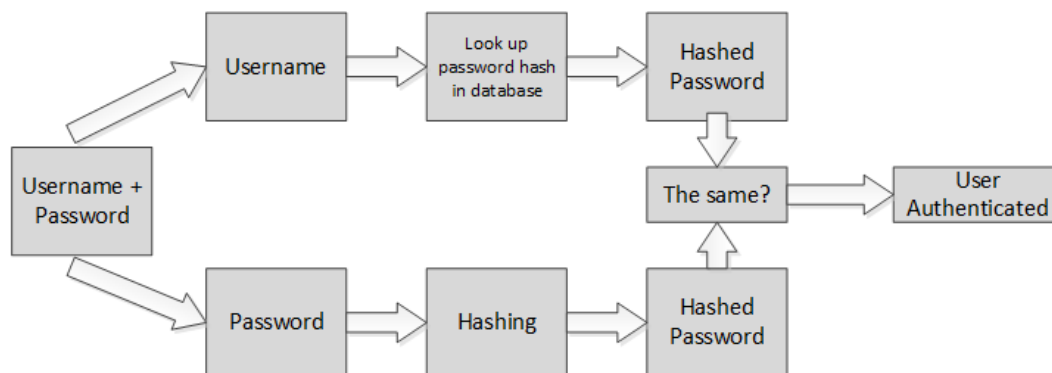
- [密码哈希概览, 48](#)
- [密码哈希选项, 49](#)
- [受信任的应用程序, 50](#)
- [证书和密钥的管理, 51](#)
- [密码重置过程, 51](#)
- [安全配置实用程序, 51](#)
- [故障排除, 52](#)

密码哈希概览

密码哈希是一种通过加密哈希函数对密码进行加密的方法。MDM Hub 使用密码哈希方法保护用户密码的安全，并确保密码绝不会以明文形式存储在数据库中。MDM Hub 管理员在安装 Hub 服务器过程中配置密码哈希选项，例如使用的算法和证书。

Informatica 提供了一个安全配置实用程序，用来管理 MDM Hub 实施中的某些安全设置，其中包括更改哈希算法或重置 MDM Hub 用户密码。

下图显示了 MDM Hub 如何使用经过哈希运算的密码对用户进行身份验证：



相关主题：

- [“安全配置实用程序” 页面上 51](#)

密码哈希选项

在安装 Hub 服务器期间，您可以配置以下密码哈希选项：

- 是否要创建自己的客户哈希键作为哈希算法的一部分。
- 是使用默认的 SHA3 哈希算法还是创建自定义哈希算法。
- 是使用默认的证书提供程序还是使用自定义证书提供程序。

SHA3 哈希算法和自定义哈希算法都可以确保 MDM Hub 用户的密码受到加密保护，并且绝不会以明文方式存储在数据库中。无论您使用哪种哈希算法，该算法都具有以下组成部分：

- 哈希函数
- 为每个 MDM Hub 用户随机生成的值
- 可选的客户哈希键（在 MDM Hub 安装期间设置）。MDM Hub 管理员负责生成此键并安全地存储它。

如果您自己创建客户哈希键，Informatica 建议使用最多包含 32 个十六进制字符（无分隔符）的键。

重要说明：请确保键的保密性。如果客户哈希键的值丢失，您必须重置所有密码。

密码哈希算法和算法的基础实施存储在 Hub 服务器属性中。有关 Hub 服务器属性的详细信息，请参阅《*Multidomain MDM 配置指南*》。

自定义哈希算法

您可以为 MDM Hub 中的密码哈希处理使用自定义哈希算法。

您可以在安装 MDM Hub 的过程中配置自定义哈希实现类。或者，也可以通过安全配置实用程序更改哈希算法。

要实现自定义哈希算法，必须在位于以下目录的 `siperian-server-hash.jar` 文件中实现 Java 抽象类 `com.siperian.sam.security.hashing.algorithms.HashAlgorithm`：

<MDM Hub 安装目录>/server/lib/hashing

基于证书的身份验证

MDM Hub 将密码哈希技术与基于证书的身份验证结合使用。证书为那些不想在访问受信任的应用程序时输入密码的用户提供另一层安全保护。默认情况下，证书登录模块将 IDD 等 Informatica 应用程序视为受信任的应用程序。

要使用外部应用程序进行基于证书的身份验证，该外部应用程序会向 MDM Hub 传递串联在一起的应用程序名称和用户名。例如，IDD/admin。该外部应用程序还必须传递安全有效负载。要生成安全有效负载，请使用资源工具包中的安全有效负载生成器实用程序。应用程序用户还需要一个私钥，这个私钥必须由客户端维护。有关安全负载生成器实用程序的详细信息，请参阅《*Multidomain MDM 资源工具包指南*》。

MDM Hub 会创建可供基于证书的身份验证使用的公共证书，但是您也可选择实施自定义证书提供程序。要实施自定义证书提供程序，必须在位于以下目录的 `siperian-server-pkiutil.jar` 文件中实现 `PKIUtil.java` 接口：

<MDM Hub 安装目录>/server/lib/pkiutils

基于证书的身份验证和外部客户端

MDM Hub 外部的客户端（例如 SiperianClient API）会通过用户凭据身份验证触发请求。但是，如果用户凭据身份验证不可行，外部客户端也可以使用基于证书的身份验证。

要为 MDM Hub 外部的客户端配置基于证书的身份验证，请执行以下步骤：

1. 实施自定义证书提供程序。
2. 提供 PKIUtil.java 实现来从以下用户检索私钥：
 - 与外部客户端关联的用户
 - 与 MDM Hub 关联的应用程序用户
3. 在 Hub 控制台中，为与外部客户端关联的用户注册公共证书。
4. 使用外部客户端触发请求。

受信任的应用程序

在 MDM Hub 中，受信任的应用程序是一种用户类型，称为应用程序用户，可代表任何常规的 MDM Hub 用户（包括 admin 用户）运行请求。可信应用程序属于 MDM Hub 可信应用程序框架。

受信任的应用程序在 CMX_SYSTEM 架构下的 C_REPOS_USER 表中的 APPLICATION_IND 列中进行定义。每个受信任的应用程序在 Hub 控制台都注册为一个应用程序用户。默认情况下，MDM Hub 将 MDM Hub 实施中广泛使用的 Informatica 应用程序视为受信任的应用程序。例如，Informatica Data Director 和 ActiveVOS 就是受信任的应用程序。

默认情况下，每个受信任的应用程序都配置了一套公钥和私钥。MDM Hub 通过以下方式之一对来自受信任应用程序的请求进行身份验证：

- 用户凭据身份验证
- 基于证书的身份验证

要将另一应用程序配置为受信任的应用程序，请参阅[“添加用户帐户” 页面上 26](#)。

将外部应用程序添加为可信应用程序

您也可以添加 MDM Hub 可信应用程序框架之外的外部应用程序。

1. 实施和配置自定义证书提供程序。
注意：您可以在安装或升级 MDM Hub 时配置自定义证书提供程序。否则，请使用安全配置实用程序更改证书提供程序配置。
2. 提供 PKIUtil.java 实现来从以下用户检索私钥：
 - 与外部客户端关联的应用程序用户
 - 与 MDM Hub 关联的应用程序用户
3. 在 Hub 控制台中，为与外部应用程序对应的应用程序用户添加一个用户帐户。
注意：确保在添加用户对话框中选择应用程序用户复选框，同时确保仅使用小写字符作为用户帐户名称。
4. 为应用程序用户帐户注册公共证书。

5. 使用外部应用程序触发请求。

注意: 如果要使用基于证书的身份验证, 请将请求名称设置为 <应用程序名称>/<用户名>。<应用程序名称> 必须与步骤 3 中使用的名称相同。<用户名> 是触发请求的 MDM Hub 用户的名称。

证书和密钥的管理

如果您使用自定义证书提供程序进行基于证书的身份验证, 必须在安全的位置为每个用户维护证书和私钥对。

默认情况下, MDM Hub 将私钥和证书保留在以下位置:

<MDM Hub 安装目录>/server/resources/certificates

您可以在安装 MDM Hub 的过程中配置自定义证书提供程序。或者, 也可以通过安全配置实用程序更改证书提供程序。

要实施自定义证书提供程序, 必须在位于以下目录的 siperian-server-pkiutil.jar 文件中实施 PKIUtil.java 接口:

<MDM Hub 安装目录>/hub/server/lib/pkiutils

注意: 如果您使用自定义证书提供程序, 必须维护密钥库和公共证书, 以供 PKIUtil 实施使用。

相关主题:

- [“安全配置实用程序” 页面上 51](#)

密码重置过程

如果您忘记了密码, 或者认为自己的哈希算法的加密内容泄漏, 可以重置您的密码。要重置密码, 请联系 Informatica 全球客户支持部门。

重置密码时, 您会收到一封电子邮件, 其中包含一个临时密码。使用此密码登录到 MDM Hub, 然后将密码更改为您认为有意义的密码。您可以通过 Hub 控制台或 Informatica Data Director 更改您的密码。

安全配置实用程序

您可以向 Informatica 全球客户支持部门索取安全配置实用程序, 以帮助您管理 MDM Hub 实施中的某些安全设置。使用安全配置实用程序, 您可以执行以下任务:

1. 在 MDM Hub 中为用户重置密码。
2. 更改密码哈希运算使用的哈希算法。
3. 更改身份验证使用的证书提供程序。
4. 更改用于创建哈希算法的客户哈希键。

注意: 要获取安全配置实用程序, 请联系 Informatica 全球客户支持部门。

故障排除

如果遇到问题，请使用以下信息来排除故障。

MDM Hub 用户无法登录

如果 MDM Hub 在安装 Hub 服务器后重新创建了 CMX_SYSTEM 架构，MDM Hub 将无法识别哈希密码。结果是，用户将无法登录 MDM Hub。

要解决此问题，请手动重新运行 postInstallSetup 脚本。此脚本可确保 MDM Hub 用户的密码重新进行哈希，随后用户便可以登录。

有关 postInstallSetup 脚本的详细信息，请参阅《《*Multidomain MDM 安装指南*》》。

附录 A

词汇表

batch group：批处理组

由可以使用单个命令执行的各个批处理作业（例如，暂存、加载和匹配作业）组成的集合。组中的每个批处理作业可按顺序执行，也可与其他作业并行执行。

database：数据库

位于 Hub 存储中的有组织的数据集合。Informatica MDM Hub 支持两种类型的数据库：主数据库和操作引用存储 (ORS)。

Data Manager：数据管理器

该工具用来查看所有合并（包括自动合并）的结果并在必要时更正数据内容。可让您查看每条基础对象记录的数据沿革。数据管理器还允许您取消合并以前合并的记录，并查看每条合并记录的不同类型的历史记录。

使用“数据管理器”工具可以搜索记录、查看记录的交叉引用、取消合并记录、取消链接记录、查看历史记录、创建新纪录、编辑记录以及替代信任设置。数据管理器显示符合您所定义的搜索条件的所有记录。

data steward：数据管理者

Informatica MDM Hub 用户，主要负责数据质量。数据管理者通过 Hub Console：Hub 控制台访问 Informatica MDM Hub，并使用 Informatica MDM Hub 工具配置 Hub 存储中的对象。

Dynamic Data Masking

在客户端和数据库之间操作的数据安全产品，用于防止未经授权访问敏感信息。Dynamic Data Masking 可拦截发送到数据库的请求，并在将请求发回客户端前对该请求应用数据屏蔽规则以屏蔽数据。

hierarchy：层次结构

层次结构是层次结构管理器中的一组关系类型。这些关系类型不会根据实体在层次结构中的位置划分等级，也不一定彼此相互关联。它们仅仅是分为一组的关系类型，以便于分类和识别。

Hub Console：Hub 控制台

Informatica MDM Hub 用户界面，由一组工具所组成，用于管理员和数据管理者。每个工具都允许用户执行一个特定操作或一组相关操作，如建立数据模型、运行批处理作业、配置数据流、运行批处理作业、配置外部应用程序访问 Informatica MDM Hub 资源的权限以及其他系统配置和操作任务。

Hub Server：Hub 服务器

一个位于中间层（应用程序服务器）的运行时组件，用于提供核心服务和常见服务（包括访问、安全及会话管理）。

Hub 存储

在 Informatica MDM Hub 实现中，指的是包含主数据库以及一个或多个操作引用存储 (ORS) 数据库的数据库。

Kerberos

一种计算机网络身份验证协议，该协议允许通过非安全网络通信的节点以一种安全的方式向对方证明自己的身份。Kerberos 协议由美国麻省理工学院开发，可供用户免费实施。

Operational Reference Store (ORS)：操作引用存储 (ORS)

数据库包含主数据以及对主数据起作用的规则。规则包括用于处理主数据的规则、用于管理主数据对象集的规则以及 MDM Hub 用来定义最佳数据版本的处理规则和辅助逻辑。MDM Hub 配置可以具有一个或多个操作引用存储。ORS 的默认名称是 CMX_ORS。

policy enforcement points (PEPs)：策略强制点(PEP)

运行时强制执行身份验证和授权请求安全策略的特定的安全检查点。

Security Access Manager (SAM)：安全访问管理器 (SAM)

安全访问管理器 (SAM) 是用来防止 MDM Hub 资源被未经授权访问的安全模块。运行时，SAM 将强制执行组织针对 MDM Hub 实施的安全策略判定，根据您的安全配置处理用户身份验证和访问授权。

专用资源

“角色”工具中隐藏的 Informatica MDM Hub 资源，可通过服务集成框架 (SIF) 操作阻止访问。在 Hub 控制台中添加新资源（如新基础对象）时，默认情况下将其指定为“专用”资源。

元数据

一种用于描述其他数据的数据。在 Informatica MDM Hub 中，元数据用于描述 Informatica MDM Hub 实现过程中使用的架构（数据模型）以及相关的配置设置。

写入锁定

在 Hub Console：Hub 控制台中，写入锁定是指更改底层架构时必需使用的锁定。所有非数据管理者工具（操作引用存储 安全工具除外）都将处于只读模式，除非您获取了一个写入锁定。写入锁定允许多个并发用户更改架构。

包

包是指 Informatica MDM Hub 中的一个或多个基本表的公共视图。包表示某些表以及加入这些表的其他表中的列的子集。包基于查询。基本查询可以从表或其他包中选择一个记录子集。

基础对象

一种包含关于业务相关实体（如客户或帐户）的信息的表。

安全

防止 Informatica MDM Hub 实施中的数据和其他资源遭受未经授权的访问或篡改，从而保护信息隐私性、机密性和数据完整性的功能。

安全提供程序

为访问 Informatica MDM Hub 的用户提供安全服务（身份验证、授权和用户配置文件服务）的一种第三方应用程序。

安全访问管理器工作台

包括用于管理用户、组、资源和角色的工具。

安全负载

为 MDM Hub 操作请求提供的行二进制数据，可包含进一步身份验证或授权所需的追加数据。

密码策略

为 Informatica MDM Hub 用户帐户指定密码特性，如密码长度、到期时间、登录设置、密码重用及其他要求。可以为 Informatica MDM Hub 实施中的所有用户帐户定义全局密码策略，并且可以覆盖各个用户的这些设置。

层次结构管理器

用户可以通过 层次结构管理器 管理与在 MDM Hub 中管理的记录相关联的层次结构数据。有关详细信息，请参阅《*Multidomain MDM 配置指南*》和《*Multidomain MDM 数据管理者指南*》。

工作台

在 Hub Console：Hub 控制台中，指对类似工具进行分组的一种机制。工作台是相关工具的逻辑集合。例如，模型工作台包含用于数据建模的工具（如架构、查询、包和映射）。

授权

确定用户是否拥有足够特权来访问请求的 Informatica MDM Hub 资源的进程。在 Informatica MDM Hub 中，资源特权将分配给角色。用户和用户组将分配给角色。用户的资源特权由分配了这些特权的角色以及分配给该用户所属用户组的角色确定。

提供程序

请参阅[安全提供程序页面上 54](#)。

特权

MDM Hub 资源的访问权限。通过 MDM Hub 内部授权，每个角色均可获得以下特权之一。

特权	允许用户……
读取	查看数据。
创建	在 Hub 存储中创建数据记录。
更新	在 Hub 存储中更新数据记录。
合并	合并与取消合并数据。
执行	执行清理函数和批处理组。
删除	删除 Hub 存储中的数据记录。

特权决定了外部应用程序用户是否具有 MDM Hub 资源的访问权限。例如，可将一个角色配置为对特定包和包列具有“读取”、“创建”、“更新”和“合并”特权。尽管这些设置在一定程度上仍会影响 Hub 控制台的使用，但在使用 Hub 控制台时并不强制实施这些特权。

策略判定点 (PDP)

验证用户身份并授权用户访问 MDM Hub 资源的特定安全检查点。

角色

定义了用于访问安全 Informatica MDM Hub 资源的一组特权。

身份验证

核实用户身份以确保其身份属实的过程。在 Informatica MDM Hub 中，基于用户提供的凭据（用户名/密码、安全负载或两者的组合）对用户进行身份验证。Informatica MDM Hub 提供了内部身份验证机制，还支持使用第三方身份验证提供程序对用户进行身份验证。

配置工作台

包括配置各种 MDM Hub 对象（包括操作引用存储、用户、安全、消息队列和元数据验证）的工具。

配置文件

在层次结构管理器中，介绍了 HM 用户可显示、编辑或添加的字段和记录。例如，一个配置文件可以允许对所有实体和关系具有完全读取/写入访问权限，而另一个配置文件则只允许具有读取访问权限（不允许执行添加或编辑操作）。

索引

A

- 安全访问管理器 (SAM) [11](#)
 - “安全提供程序” 工具
 - 关于安全提供程序 [35](#)
 - 提供程序文件 [36](#)
- 安全提供程序文件
 - 关于安全提供程序文件 [35](#)
 - 删除 [37](#)
 - 上载 [36](#)
- 安全
 - JDBC 数据源, 配置 [30](#)
 - 身份验证 [11](#)
 - 授权 [11](#)
 - 配置 [9](#)

C

- 操作引用存储 (ORS)
 - 将用户分配给 [33](#)
- 词汇表 [53](#)

D

- Dynamic Data Masking
 - 概览 [10](#)

G

- 故障排除
 - 密码哈希 [52](#)

J

- JDBC 数据源
 - 安全, 配置 [30](#)
- 角色
 - 编辑 [22](#)
 - 将资源特权分配给角色 [23](#)

M

- 密码
 - 全局密码策略 [29](#)
 - 专用密码 [29](#)
- 密码策略
 - 全局密码策略 [29](#)
 - 专用密码策略 [29](#)

P

- providers.properties 文件
 - 示例 [40](#)

Q

- 全局
 - 密码策略 [29](#)

S

- 身份验证
 - 关于身份验证 [11](#)
 - 内部身份验证 [11](#)
 - 外部目录身份验证 [11](#)
 - 外部身份验证提供程序 [11](#)
- 授权
 - 关于授权 [11](#)
 - 内部授权 [11](#)
 - 外部授权 [11](#)
- 数据库
 - 用户访问权限 [28](#)

T

- 提供程序
 - 自定义添加 [39](#)

W

- 外部应用程序用户 [26](#)

Y

- 用户
 - 补充信息 [27](#)
 - 分配给操作记录存储 (ORS) [33](#)
 - 密码设置 [27](#)
 - 全局密码策略 [29](#)
 - 数据库访问 [28](#)
 - 外部应用程序用户 [26](#)
 - 专用密码策略 [29](#)
- 用户组
 - 将用户分配给 [33](#)

Z

- 专用密码策略 [29](#)
- 资源特权, 分配给角色 [23](#)

资源组
编辑 [19](#)

资源组 (续)
添加 [19](#)