



运维审计平台系统 (PSM)

用户指南

Version 1.0

安讯奔
安全认证 超越云端

日期：2014 年 09 月 18 日

版权声明

版权所有，保留一切权利。© 2013-2015 北京安讯奔科技有限责任公司。

未经北京安讯奔有限责任公司的书面许可，任何单位和个人不得对本文档内的任何部分擅自进行摘录、复制，并不得以任何形式传播。

商标和免责声明

USO、PSM、UAS、UAM、UIM、DB Guard、DB Secure、VM Guard 以及 YESsafe、YESsafe ID、YESsafe Token 及其他安讯奔产品标识均为北京安讯奔科技有限责任公司所有。

本文档中出现的其他公司的商标、产品标识，均属各自权利人所有。

本文档提及的信息仅供参考。有关信息会随时更新，安讯奔恕不承担另行通知的义务。

本文档中提及的信息，安讯奔不做任何形式的明示或暗示的担保。

若因本文档或其提到的任何信息引起的意外损失、间接损失，安讯奔对此恕不承担任何责任。

联系方式

北京安讯奔科技有限责任公司

地址：北京市海淀区西直门北大街 60 号北京首钢国际大厦 1509 室

电话：400-910-2668

邮箱：enquiry@axbsec.com

传真：(86) 010-8273 6009 ext 623

网站：<http://www.axbsec.com>

目 录

1	介绍	1
1.1	简介	1
1.2	本用户指南的结构	1
2	PSM 角色、管理和配置	2
2.1	PSM 角色	2
2.1.1	PSM 管理角色	2
2.1.2	PSM 凭证管理角色	3
2.2	PSM 管理和配置	3
2.3	PSM 管理界面	3
3	PSM 配置管理	4
3.1	简介	4
3.2	查看 PSM 配置	4
3.3	编辑 PSM 配置	6
4	目标资源管理	16
4.1	简介	16
4.2	为 PSM 目标资源启用 TCP 端口	16
4.3	管理 Windows 目标资源	17
4.3.1	创建 Windows 目标资源	17
4.3.2	查找和查看 Windows 目标资源	18
4.3.3	管理 Windows 目标资源	20
4.4	管理基于 Telnet 的 UNIX 目标资源	21
4.4.1	创建基于 Telnet 的 UNIX 目标资源	21
4.4.2	查找和查看基于 Telnet 的 UNIX 目标资源	24
4.4.3	管理基于 Telnet 的 UNIX 目标资源	26
4.5	管理基于 SSH 的 UNIX 目标资源	26
4.5.1	创建基于 SSH 的 UNIX 目标资源	26
4.5.2	查找和查看基于 SSH 的 UNIX 目标资源	28
4.5.3	管理基于 SSH 的 UNIX 目标资源	28
4.6	管理基于 Telnet 通用类的目标资源	29
4.6.1	创建基于 Telnet 通用类的目标资源	29
4.6.2	查找和查看基于 Telnet 通用类的目标资源	33
4.6.3	管理基于 Telnet 通用类的目标资源	33
4.7	管理基于 SSH 通用类的目标资源	34

4.7.1	创建基于 SSH 通用类的目标资源	34
4.7.2	查找和查看基于 SSH 通用类的目标资源	36
4.7.3	管理基于 SSH 通用类的目标资源	36
4.8	管理 RDP 目标资源	36
4.8.1	创建 RDP 目标资源	36
4.8.2	查找和查看 RDP 目标资源	37
4.8.3	管理 RDP 目标资源	37
4.9	管理 JDBC 目标资源	38
4.9.1	创建 JDBC 目标资源	38
4.9.2	查找和查看 JDBC 目标资源	39
4.9.3	管理 JDBC 目标资源	39
4.10	管理 AS400 目标资源	40
4.10.1	创建 AS400 目标资源	40
4.10.2	查找和查看 AS400 目标资源	41
4.10.3	管理 AS400 目标资源	41
4.11	4.11 管理基于 Telnet 的 Cisco 目标资源	41
4.11.1	创建基于 Telnet 的 Cisco 目标资源	41
4.11.2	查找和查看基于 Telnet 的 Cisco 目标资源	43
4.11.3	管理基于 Telnet 的 Cisco 目标资源	43
4.12	管理基于 SSH 的 Cisco 目标资源	43
4.12.1	创建基于 SSH 的 Cisco 目标资源	43
4.12.2	查找和查看基于 SSH 的 Cisco 目标资源	45
4.12.3	管理基于 SSH 的 Cisco 目标资源	45
4.13	管理基于 Telnet 的 Huawei 防火墙目标资源	45
4.13.1	创建基于 Telnet 的 Huawei 防火墙目标资源	45
4.13.2	查找和查看基于 Telnet 的 Huawei 防火墙目标资源	47
4.13.3	管理基于 Telnet 的 Huawei 防火墙目标资源	47
4.14	管理基于 SSH 的 Huawei 防火墙目标资源	47
4.14.1	创建基于 SSH 的 Huawei 防火墙目标资源	47
4.14.2	查找和查看基于 SSH 的 Huawei 防火墙目标资源	49
4.14.3	管理基于 SSH 的 Huawei 防火墙目标资源	49
4.15	管理基于 Telnet 的 Huawei 切换目标资源	49
4.15.1	创建基于 Telnet 的 Huawei 切换目标资源	49
4.15.2	查找和查看基于 Telnet 的 Huawei 切换目标资源	51
4.15.3	管理基于 Telnet 的 Huawei 切换目标资源	51
4.16	管理基于 SSH 的 Topsec 防火墙目标资源	51
4.16.1	创建基于 SSH 的 Topsec 防火墙目标资源	51

4.16.2	查找和查看基于 SSH 的 Topsec 防火墙目标资源	53
4.16.3	管理基于 SSH 的 Topsec 防火墙目标资源	53
4.17	为 SSO 整合启用 PSM 目标资源	53
5	保险箱管理	54
5.1	简介	54
5.2	创建 PSM 保险箱	54
5.3	查找和查看 PSM 保险箱	57
5.4	管理 PSM 保险箱	59
6	凭证标签管理	60
6.1	简介	60
6.2	创建 PSM 凭证标签	60
6.3	查找和查看 PSM 凭证标签	62
6.4	管理 PSM 凭证标签	62
7	凭证管理	63
7.1	简介	63
7.2	管理凭证	64
7.2.1	创建凭证	64
7.2.2	查找和查看凭证	70
7.2.3	管理凭证	70
7.2.4	管理工作流程角色	71
7.3	管理有重设密码特权的凭证	74
7.3.1	创建有重设密码特权的凭证	74
7.3.2	查找和查看有重设密码特权的凭证	76
7.3.3	管理有重设密码特权的凭证	76
7.4	管理超级用户账号	76
7.4.1	创建超级用户账号	76
7.4.2	查找和查看超级用户账号	78
7.4.3	管理超级用户账号	78
7.5	管理凭证功能账号	78
7.5.1	创建凭证功能账号	78
7.5.2	查找和查看凭证功能账号	80
7.5.3	管理凭证功能账号	80
7.6	管理凭证网关账号	80
7.6.1	创建凭证网关账号	80
7.6.2	查找和查看凭证网关账号	81
7.6.3	管理凭证网关账号	81

8	目标资源存储管理.....	82
8.1	简介	82
8.2	创建目标资源存储	82
8.3	查找和查看目标资源存储.....	83
8.4	管理 PSM 目标资源存储	83
9	PSM 报告管理.....	84
9.1	简介	84
9.2	制作一般事件报告	84
9.3	制作凭证-用户报告	86
9.4	制作用户-凭证报告	87
9.5	制作 PSM 诊断报告.....	87

1 介绍

此章节描述本用户指南的结构。

1.1 简介

此用户指南提供安讯奔运维审计平台系统（简称“PSM”）管理用户界面的使用参考。它主要描述，使用管理控制台执行 PSM 相关管理和配置任务。

此文件的目标读者，是打算管理 PSM 配置和凭证（尤其是通过管理用户界面）的安全管理员。

备注：

除了 PSM 用户指南，您还可以参考 [PSM 管理控制台通用管理指南](#)，以了解关于其他一般管理任务的详细说明。

管理 PSM 系统：也就是管理 PSM 角色（管理员/用户，例如请求者和批准者）、配置和不同的 PSM 物件（如下章节所述）之后，管理员可以继续执行 PSM 配置管理操作，请参考相关的凭证管理指南以了解详细说明。

“ACMATRIX_ROOT”该词汇，在本指南中，是指在 Windows 和 Unix 平台中，AccessMatrix 的根或安装目录。

1.2 本用户指南的结构

本用户指南的结构和说明如下所述：

章节	描述
1	此用户指南的介绍。
2	描述不同的 PSM 角色、管理和配置。
3	描述 PSM 配置的管理。
4	描述 PSM 目标资源的管理。
5	描述 PSM 保险箱的管理。
6	描述 PSM 凭证标签的管理。
7	描述 PSM 凭证的管理。
8	描述 PSM 目标资源存储的管理。
9	描述不同的 PSM 报告。

2 PSM 角色、管理和配置

此章节描述不同的 PSM 角色、管理和配置。

2.1 PSM 角色

在执行 PSM 管理和配置任务之前，管理员应充分了解不同的 PSM 角色。主要有 2 类 PSM 角色，即“PSM 管理角色”和“PSM 凭证管理角色”（又名 PSM 工作流程角色），后者是内建角色，且不可修改。

2.1.1 PSM 管理角色

PSM 管理角色是一系列管理权力，每个权力包含所分配的许可（以对特定 PSM 相关特定物件做出特定操作）。成功设置 PSM 系统后，会有两类预先定义的 PSM 管理角色，如下所述。一般来说，您可以参考 [PSM 管理控制台通用管理指南](#)，以了解关于管理管理角色的更多信息。

■ PSMAAdminRole（PSM 管理角色）

角色描述：

- 通常是分配给 PSM 安全管理员。
- 负责审查系统中的用户和群组信息。
- 负责管理凭证、目标资源和保险箱。
- 负责分配和取消分配凭证请求者和批准者。

此角色有以下权限：

- 查看用户和群组；
- PSM 凭证管理，除了重设凭证密码外；
- PSM 目标资源和保险箱管理；
- 系统配置查看；
- 系统策略查看和编辑；和
- 加密密钥查看。

■ PSMPasswordOwner（PSM 凭证密码所有者）

角色描述：

- 通常是分配给 PSM 安全管理员。
- 负责管理凭证信息，例如凭证的安全策略，例批准级别、是否允许并发检出凭证等等。
- 负责在要求的时候，设定凭证的新密码。

此角色有以下权限：

- PSM 凭证管理，除了删除凭证外；和
- 系统策略查看。

2.1.2 PSM 凭证管理角色

有 2 类的 PSM 凭证管理角色，如下所述。

■ 请求者（凭证请求者）

角色描述：

- 通常分配给 PSM 支持员工，他们需要提出请求以检索凭证，来支持或其他因操作需要或紧急情况的目的。
- 请求者，可以批准任何仅在非工作时间所提出的凭证请求。

此角色有以下权限：

- 通过检出凭证请求使用。

■ 批准者（凭证申请批准者）

角色描述：

- 通常是分配给有权力批准的员工，他们在通常可操作的情况下，有权批准由上述请求者所提出的凭证请求。
- 批准者仅可以在其级别批准或拒绝凭证请求。若批准者拥有批准的较高级别，他/她不可以越开批准过程。
- 批准者仅可以在通常可操作情况（即不是在下班时间，和没有标识为下班时间请求）下，批准、拒绝或删除凭证请求。

此角色有以下权限：

- 批准、拒绝和删除除非工作时间外、任何时间提出的凭证请求。

重要备注：

凭证可以设为“**No Approval**”（无批准，又名 0 级别批准），即不需要批准。在这种情况下，当请求者提交请求以检出和查看这类凭证，系统将会自动并立即批准这种请求。

2.2 PSM 管理和配置

在成功设置 PSM 系统后，管理员可以先了解 PSM 配置，以便于入门。除非为了要满足特别用户需求，管理员都无须对 PSM 配置做出任何修改。这些配置决定 PSM 会如何做出行为，例如后台任务、非工作时间等等。

在正确配置上述 PSM 配置后，管理员可以执行 PSM 管理任务。这些管理任务包括，管理目标资源、保险箱和凭证，和分配/取消分配某个配置的 PSM 角色给/从要求的用户，等等。

2.3 PSM 管理界面

类似执行 AccessMatrix 一般管理任务，PSM 管理和配置，也是通过 AccessMatrix 管理控制台来完成的。那么，您可以参考 [PSM 管理控制台通用管理指南](#)，来了解从管理控制台入门的详细说明，和管理控制台的基本功能的详细说明。

为了执行 PSM 管理和配置任务，管理员必须确保 PSM 系统已经购买了 PSM 许可的功能。

在购买了 PSM 许可的功能后，管理员才可以管理配置 PSM 系统，如下方章节所述。

3 PSM 配置管理

此章节描述管理 PSM 配置。

3.1 简介

PSM 配置管理，是要执行的数项初始管理任务，尤其是对于新设立的 PSM 系统来说。PSM 配置，允许管理者配置 PSM 系统的以下方面：后台任务、非工作时间和 ESSO 模板。这些设置，是对整个 PSM 系统全局适用的。

PSM 提供**非工作时间**这个功能，是为了当用户有着急或紧急请求要检出凭证，而当时又是非工作时间，那么就可以让请求进行相应的自我批准了。通常，是所授权的的安全管理员不在，或者是非办公时间，无法批准请求，才会发生这种情况。

为了有效执行 PSM 管理，管理员应先充分了解 PSM 配置。如无需要，管理员请勿修改设置。当发生在下方部分内容的情况时候，才允许管理查看和编辑 PSM 配置。

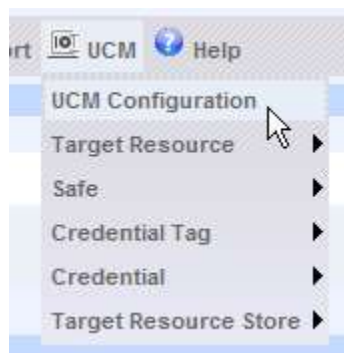
备注：

另外，管理员可参考 [PSM 管理控制台通用管理指南：附录 A](#)，来了解关于要执行要求的
管理任务，所需要的管理角色和管理权限的相关信息。

3.2 查看 PSM 配置

若要查看 PSM 配置，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#)所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如下所示：



图表 3-1: PSM 配置子菜单选项

下方屏幕将会出现：

View Configuration			
*Configuration Id:	UCMConfiguration	*Configuration Name:	UCMConfiguration
Description:	UCM Configuration	Version :	1
Implementation:	UCMConfiguration		
Attributes Off Business Hours ESSO Template Files			
Attribute Name	Attribute Value	Remark	
Password			
Password display timeout	30 (default)	To determine timeout of password display in seconds. 0 means no timeout	
Background Task			
Server instance	AccessMatrix	Server instance where the background tasks will run	
Credential Updater			
Force next task execution at	2012-05-18 01:00:01 (default)		
Scheduled period (hours)	24 (default)		
Credential Verifier			
Force next task execution at	2012-05-18 00:00:01 (default)		
Scheduled period (hours)	24 (default)		
Checkin Overdue Task			
Force next task execution at	2012-05-18 03:00:01 (default)		
Scheduled period (minutes)	15 (default)		
UCM CSV Import Task			
Force next task execution at	2012-05-18 03:00:01 (default)		
Scheduled period (minutes)	15 (default)		
Self Service Approval During Off Biz Hours			
Enable self service approval during off biz hours	false (default)	When this is set to true, requesters will be allowed to approve their own checkout requests during off biz hours as defined in the Off Biz Hours tab	
Credential Attribute Configuration			
Allowed Charset For Credential Id	[w-@\]* (default)		

图表 3-2: 查看 PSM 配置 – 属性

屏幕的上方部分包含一般属性，例如配置 ID 名称、描述、版本和实施。

屏幕的下方部分包含数个标签。第一个标签是属性，它包含以下相关属性：密码、后台任务、非工作时间自助服务批准，和凭证属性配置。

- 按一下“**Off Business Hours**”（非工作时间）标签，它包含非工作时间的时段以及假期的列表，如下所示：

Attributes			Off Business Hours	ESSO Template Files
Off Business Hours Time Slot				
Day of Week	Time Slot 1	Time Slot 2		
SUN	00:00 To 23:59	-		
MON	20:00 To 23:59	00:00 To 08:00		
TUE	20:00 To 23:59	00:00 To 08:00		
WED	20:00 To 23:59	00:00 To 08:00		
THU	20:00 To 23:59	00:00 To 08:00		
FRI	20:00 To 23:59	00:00 To 08:00		
SAT	00:00 To 23:59	-		
Holiday	00:00 To 23:59	-		
Holiday				
Holiday Date (dd-mm-yyyy)	Description			
25-12-2012	Christmas Day			
01-01-2013	New Year			

图表 3-3: 查看 PSM 配置 – 非工作时间

- 按一下“**ESSO Template Files**”（ESSO 模板文件）标签，它包含系统中创建的 ESSO 模板列表，如下所示：

Attributes			Off Business Hours	ESSO Template Files
Id	Description			
PUTTY	Putty	Download		
RDP-AD	RDP to AD	Download		

图表 3-4: 查看 PSM 配置 – ESSO 模板文件

PSM 配置属性的配置方法，将会在下方部分为您阐述。

3.3 编辑 PSM 配置

若要编辑 PSM 配置，请执行以下步骤：

- 执行 [3.2](#) 部分所述步骤来查看 PSM 配置。
- 按一下如图表 3-2 所示屏幕的“Edit”（编辑）按钮，屏幕将会变为编辑模式，如下所示：

Edit Configuration		
*Configuration Id:	UCMConfiguration	*Configuration Name: UCMConfiguration
Description:	UCM Configuration	Version : 3
Implementation:	UCMConfiguration	
Attributes Off Business Hours ESSO Template Files		
Attribute Name	Attribute Value	Remark
Password		
Password display timeout	<input type="text"/>	To determine timeout of password display in seconds. 0 means no timeout Default: 30 Value should be from 0 to 60
Background Task		
*Server instance	<input type="text" value="AccessMatrix"/>	Server instance where the background tasks will run
Credential Updater ?		
Force next task execution at	<input type="checkbox"/> <input type="text"/> HH <input type="text"/> MM <input type="text"/> SS	Default: 2012-05-18 01:00:01
Scheduled period (hours)	<input type="text"/>	Default: 24 Value should not be less than 1
Credential Verifier ?		
Force next task execution at	<input type="checkbox"/> <input type="text"/> HH <input type="text"/> MM <input type="text"/> SS	Default: 2012-05-18 00:00:01
Scheduled period (hours)	<input type="text"/>	Default: 24 Value should not be less than 1
Checkin Overdue Task ?		
Force next task execution at	<input type="checkbox"/> <input type="text"/> HH <input type="text"/> MM <input type="text"/> SS	Default: 2012-05-18 03:00:01
Scheduled period (minutes)	<input type="text"/>	Default: 15 Value should not be less than 1
UCM CSV Import Task ?		
Force next task execution at	<input type="checkbox"/> <input type="text"/> HH <input type="text"/> MM <input type="text"/> SS	Default: 2012-05-18 03:00:01
Scheduled period (minutes)	<input type="text"/>	Default: 15 Value should not be less than 1
Self Service Approval During Off Biz Hours		
Enable self service approval during off biz hours	<input type="text" value="(default)"/>	When this is set to true, requesters will be allowed to approve their own checkout requests during off biz hours as defined in the Off Biz Hours tab Default: false
Credential Attribute Configuration		
Allowed Charset For Credential Id	<input type="text"/>	Default: [\w-@\.]*

图表 3-5: 编辑 PSM 配置

若需要，请对属性做出相应更改。

■ 密码

“密码显示超时”属性决定的是，在 PSM 管理器中，对每个凭证请求，凭证密码以纯

文本形式显示的逾时时间段（单位为秒）。预设值是 30 秒。若值为 0，则表示没有设置逾时时间。

■ 后台任务

“服务器实例”属性，用于决定要后台任务要执行哪个 AM 服务器实例。

■ 凭证更新器

“凭证更新器”属性，定义后台更新器任务的行为，例如，若要更新凭证，更新器应该要执行什么动作。依照特定的用户情况和条件，更新器任务将会根据可用的凭证进行检出，或等候重设，如下方使用情况所述：

- i. 当凭证已经检入，但是检入后的密码更新却失败了，那么此任务将会定期更新密码。
- ii. 当根据密码过期策略（在保险箱级别所指定），凭证密码已经过期。

条件如下表格所述：

• 凭证状态	设为自动密码更新?	凭证密码已过期?	• 动作
可用于检出	• True 真	• True 真	• 更新凭证密码
		• False 假	• 不会采取动作
	• False 假	• True 真	• 记录密码过期事件
		• False 假	• 不会采取动作
等候密码重设	• True 真	True 真 / False 假	更新凭证密码，更改状态为可用以便于检出
	• False 假	• True 真	为升级记录密码过期事件
		• False 假	为升级记录密码手动重设事件

图表 3-6: 凭证更新器任务行为

■ 凭证验证器

“凭证验证器”属性定义，后台验证器任务的行为，它将会定期验证凭证登录信息，以侦测凭证是否还能正常发挥作用，或者是否有连接到目标资源的问题。将会取得上一次登录验证状态，并且相应记录到相关事件。

■ 检入过期任务

“检入过期任务”属性定义，后台过期任务的行为，即为了强制检入凭证，过期任务要执行的动作。根据特定的条件，过期任务将会对已检出状态的凭证，和在检出请求期间，已经超过所指定的检出时间的凭证，依照以下表格条件，做出动作：

强制检入凭证?	请求是上次检出条目?	请求是否从 PSM 管理器内发出?	• 动作
• True 真	• True 真	• True 真	提交检入动作到工作流程系统； 更新请求状态为已完成； 更新凭证状态为可用于检出；

			凭证密码可依照策略而进行更新。
		<ul style="list-style-type: none"> False 假 	更新凭证状态为可用于检出； 凭证密码可依照策略而进行更新。
	<ul style="list-style-type: none"> False 假 	<ul style="list-style-type: none"> True 真 	提交检入请求； 更新请求状态为已完成； 更新凭证状态为已检出。
		<ul style="list-style-type: none"> False 假 	更新凭证状态为已检出。
<ul style="list-style-type: none"> False 假 	<ul style="list-style-type: none"> True 真 	<ul style="list-style-type: none"> True 真 	提交检入逾时动作给工作流程系统； 更新请求状态为检入逾时； 更新凭证状态为检入逾时。
		<ul style="list-style-type: none"> False 假 	更新凭证状态为检出逾时（若允许多个检出，则在此状态不允许检出）。
	<ul style="list-style-type: none"> False 假 	<ul style="list-style-type: none"> True 真 	提交检入逾时动作给工作流程系统； 更新请求状态为检入逾时； 更新凭证状态为已检出。
		<ul style="list-style-type: none"> False 假 	更新凭证状态为已检出。

图表 3-7: 检入过期任务行为

■ CSV 输入任务

“PSM CSV 输入任务”属性决定，后台输入任务的行为，该任务会输入 CSV 格式文件的凭证。CSV 格式凭证文件的样本，请参考附录 A: CSV 格式的凭证文件内容样本。

重要备注：

管理员必须意识到，CSV 输入任务是一项不安全的操作，因为凭证密码将会以纯文本形式进行输入。

若要令输入任务恰当输入凭证，管理员必须执行下方步骤：

- i. 在“<ACMATRIX_ROOT>\PSM”文件夹下，创建另外一个文件夹，架构如下：
 - <ACMATRIX_ROOT>\PSM\csvimport\credentials\
 - <ACMATRIX_ROOT>\PSM\csvimport\credentials\processed\
- ii. 在上文的“credentials”文件夹中，只要有访问操作系统的人，都可以将上述 CSV 格式的凭证文件放到那里，以用于输入。CSV 文件格式，应依照下方格式：
 - CSV 文件的文件名称前缀必须是“credentials”，例如：credentials_demo.csv。
 - CSV 文件的第一行，是标题/标头，将不会被读取/输入。
 - 第二行及以后行，包含下方凭证数据：


```
cred type, cred id, description, workflowState, requiredApprovalLevels,
forceCheckInFlag, autoPwdUpdateFlag, targetResourceId, targetResourceStoreId
```

(most likely empty), passwordSafeld, userId, cred password in clear, "user group id 1@userStore1 for requester role, user group id 2@userStore2, user group id 3@userStore3", "user group id 1@userStore1 for approver role, user group id 2@userStore2, user group id 3@userStore3", "cred tag 1, cred tag2, cred tag3"

- 布林值应为“true”或“false”，规则流程状态应依照字符串枚举不变值，凭证请求器角色，将会被赋予到指定的群组 ID 列表（若没有指定的用户存储，将会使用预设存储），双引号里的最后栏位是凭证标签，将会关联它。

- iii. 完成整个输入过程后，将会制作一个摘要文件。此摘要文件与处理后的 CSV 格式的凭证文件，将会放在上文所述的“processed”文件夹中。

此摘要文件的内容，将会描述处理凭证成功或失败的数量，以及列出所有没有成功输入的凭证。

- iv. 输入过程的最后，将会制作一个事件，它记录以下内容：成功或失败处理的凭证数量，处理失败的凭证 ID 列表（带错误原因，若有）。

■ 在非工作时间的自助服务批准

“在非工作时间启用自助服务批准”属性定义，在非工作时间，是否允许请求者自己批准其检出的请求。若设定值为“true”，则表示允许自助服务批准。依照预设，此值是设为“false”。

■ 凭证属性配置

“允许凭证 ID 字符集”属性定义，是否允许凭证 ID 包含有字符。

备注：

在上述每个后台任务执行后，都会制作事件。您可以通过邮件通知来发出此事件，前提是请要配置好相关事件通知策略。

类似的，按一下要求的标签，可编辑相关属性，如下所示：

- 非工作时间

Edit Configuration			
*Configuration Id:	UCMConfiguration	*Configuration Name:	UCMConfiguration
Description:	UCM Configuration	Version:	3
Implementation:	UCMConfiguration		
<div style="display: flex; border-bottom: 1px solid black;"> Attributes Off Business Hours ESSO Template Files </div>			
Off Business Hours Time Slot			
Day of Week	Time Slot 1	Time Slot 2	
SUN	0 : 0 To 23 : 59	: To : :	
MON	20 : 0 To 23 : 59	0 : 0 To 8 : 0	
TUE	20 : 0 To 23 : 59	0 : 0 To 8 : 0	
WED	20 : 0 To 23 : 59	0 : 0 To 8 : 0	
THU	20 : 0 To 23 : 59	0 : 0 To 8 : 0	
FRI	20 : 0 To 23 : 59	0 : 0 To 8 : 0	
SAT	0 : 0 To 23 : 59	: To : :	
Holiday	0 : 0 To 23 : 59	: To : :	
Holiday			
Holiday Date (dd-mm-yyyy)	Description	Action	
25-12-2012	Christmas Day	<input type="button" value="Remove"/>	
01-01-2013	New Year	<input type="button" value="Remove"/>	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

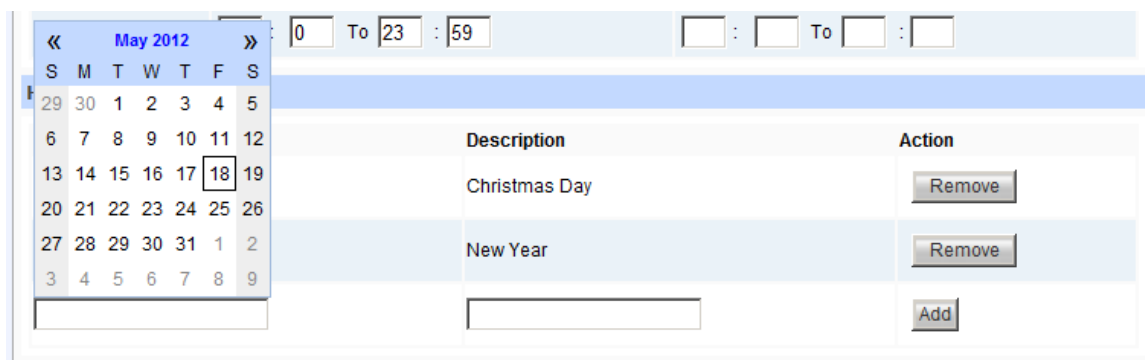
图表 3-8: 编辑 PSM 配置 – 非工作时间

为一周中,要求的某天(包括假期),指定非工作时间的时间段,24 小时格式,即 HH:MM, HH 表示小时,而 MM 表示分钟,例如: 20:00 至 23:59。允许管理员,对指定的某天,设定最多 2 个时间段。

■ 备注:

在非工作时间时间段,为“假期”指定的时间,将会应用到所有指定的假期,如下所述。

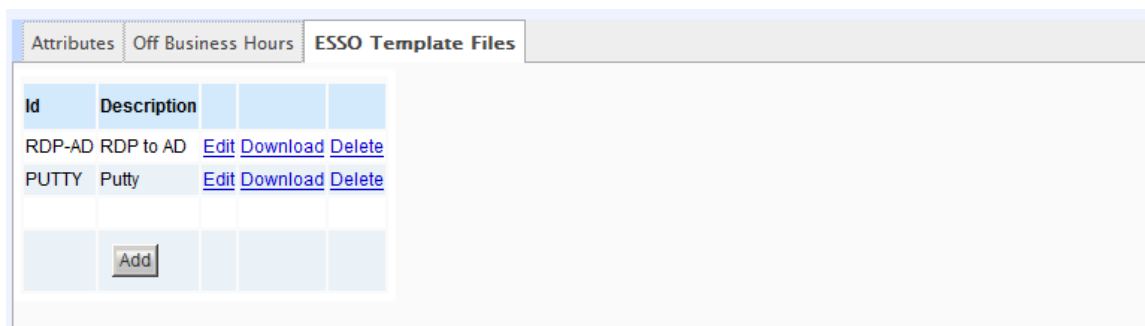
若要增加新的假期条目,请按一下“Holiday Date”(假期日期)输入栏位,将会出现日历,如下所示:



图表 3-9: 增加历史 – 选择某个日期

为假期选择要求的日期，和指定描述，然后按一下“Add”（增加）来增加到假期条目。您可以按一下“Remove”（移除）来删除要求的假期条目。

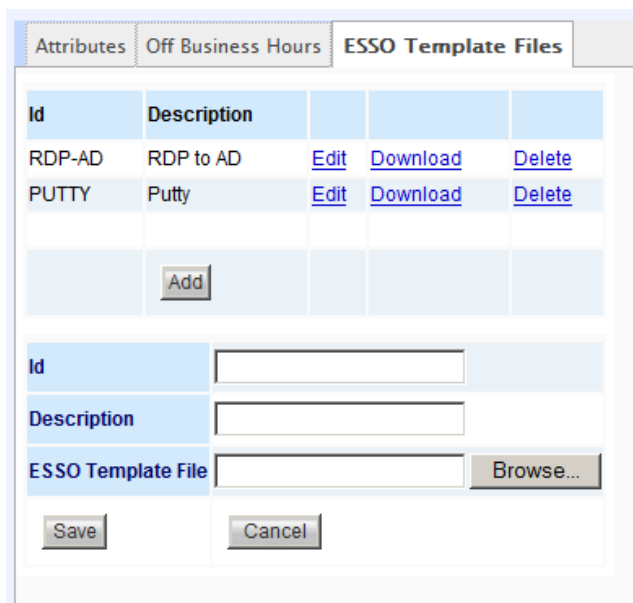
- **ESSO 模板文件**



图表 3-10: 编辑 PSM 配置 – ESSO 模板文件

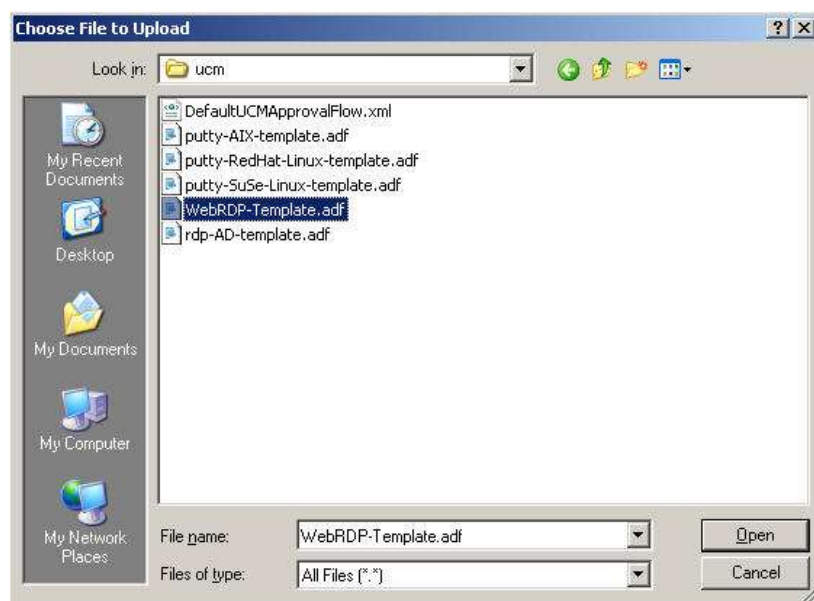
- ❖ **增加新的 ESSO 模板**

若要增加新的 ESSO 模板，请按一下“Add”（增加），下方屏幕将会出现：



图表 3-11: 增加 ADF 模板

按一下“Browse”（浏览）来前往要求的 ESSO 模板，以增加它，如下所示：



图表 3-12: 选择要求的 ESSO 模板

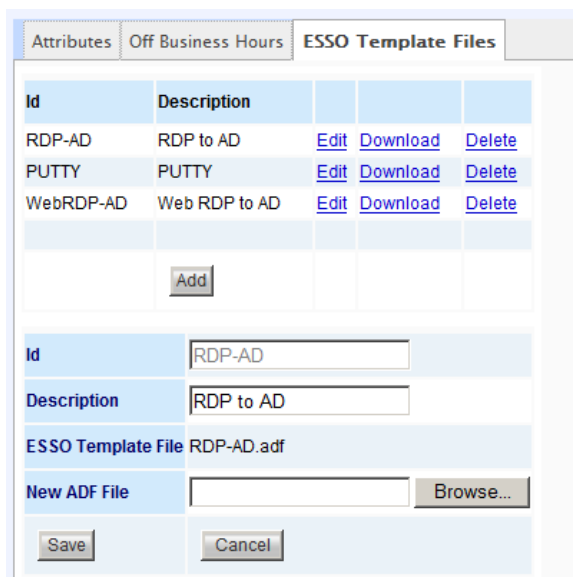
按一下“Open”（打开）来选择要增加的要求的 ESSO 模板，然后按一下“Save”（保存），那么 ESSO 模板将会增加到列表，如下所示：

Attributes		Off Business Hours		ESSO Template Files	
Id	Description				
RDP-AD	RDP to AD	Edit	Download	Delete	
PUTTY	PUTTY	Edit	Download	Delete	
WebRDP-AD	Web RDP to AD	Edit	Download	Delete	
<input type="button" value="Add"/>					

图表 3-13: 要求的 ESSO 模板已增加

❖ 编辑现有的 ESSO 模板

您可以通过按一下“Edit”（编辑）来修改现有模板，如下所示：

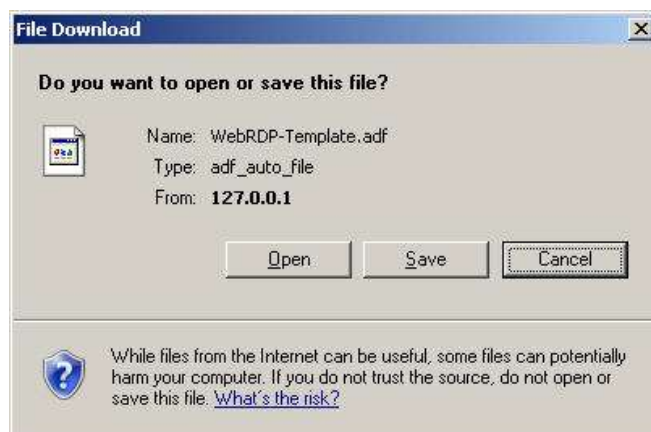


图表 3-14: 编辑要求的 ESSO 模板

您可以更新 ESSO 模板，方法是上传一个新的 ESSO 模板，步骤是按一下“Browse”（浏览）按钮，然后重复上文所提的步骤。

❖ 下载现有的 ESSO 模板

您可以下载现有的 ESSO 模板，方法是按一下“Download”（下载），然后会提示您要保存模板到本地目录，如下所示：



图表 3-15: 下载现有的 ESSO 模板

按一下“Save”（保存）来保存模板到本地文件夹。

❖ 删除现有 ESSO 模板

您可以删除现有模板，方法是按一下“Delete”（删除），那么将会立即删除要求的 ESSO 模板，而不会有任何删除确认出现。

3. 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4 目标资源管理

此章节描述，PSM 目标资源的管理。

4.1 简介

在正确配置了 PSM 配置（如之前章节所述）后，管理员可以继续管理 PSM 目标资源的不同类型。目标资源包含特定信息，这些信息是凭证用来连接到目标资源。目标资源，也可以配置为与 USO 整合，以提供单点登录（SSO）功能，将会在稍后部分为您提供详细说明。

目前，PSM 目标资源可以下方实施方式来实现：

■ Windows 服务器

这指的是运行 Windows 操作系统的服务器。

■ UNIX 服务器

这指的是运行 UNIX 操作系统的服务器，且支持基于 Telnet 或 SSH 的连接。

■ 通用类服务器

这指的是一般的服务器，且支持基于 Telnet 或 SSH 的连接。

■ RDP 服务器

这指的是支持 RDP 连接的服务器，例如 Microsoft Terminal Server。

■ JDBC 相容数据库服务器

这指的是 JDBC 相容的数据库服务器。

目前，支持：Microsoft SQL Server、Oracle、PostgreSQL 和 Sybase。

■ AS/400Server

这指的是 IBM AS/400 电脑系统。

■ 网络设备

这指的是网络设备，例如路由器、防火墙和交换机。

成功设置 PSM 系统后，会有数个预先定义的目标资源，管理员可以利用它们：应用相关更改到目标资源。

在管理目标资源之前，管理员必须先确保，相关 TCP 端口已经启用以允许 PSM 服务器和目标资源之间的通信。请继续了解下方部分内容，来管理相关 TCP 端口、PSM 目标资源的不同类型，和了解为 SSO 整合而启用 PSM 目标资源。

备注：

管理员可参考 [PSM 管理控制台通用管理指南：附录 A](#)，来了解关于要执行要求的管理任务，所需要的管理角色和管理权限的相关信息。

管理了要求的目标资源后，管理员可继续管理要求的凭证保险箱，将会在下方章节为您提供详细说明。

4.2 为 PSM 目标资源启用 TCP 端口

请确保，相关 TCP 端口已经启用以允许 PSM 服务器和目标资源之间的通信，如下表格所述：

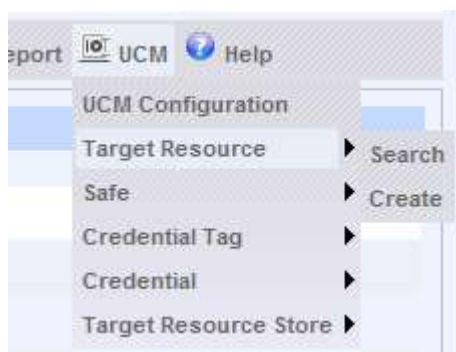
目标资源类型	要启用的 TCP 端口
基于 Windows 的服务器	<ol style="list-style-type: none"> 要开启端口 445 (SMB) 通信协定。 要启动目标服务器的工作站服务。 对于 Windows 6 系列, 请使用本地管理员账号, 启用“Reset Password”(重设密码)功能, 目标服务器必须停用 UAC。若使用域管理员账号完成重设密码, UAC 则无须停用。 <p>备注:</p> <p>PSM 使用普通的通信协议来实现文件共享, 您可以使用命令提示符的“net use”命令来测试。</p> <p>PSM 目标资源可以使用域名称或 IP 地址来连接到目标资源。若使用域或机器名称, 管理员必须确定 PSM 服务器可以相应解析名称。</p>
基于 UNIX 服务器	<ol style="list-style-type: none"> 应运行 SSH 和/或 Telnet 服务/进程。 依照目标服务器所配置的端口号码, SSH 连接的预设端口号码是 22, 而 Telnet 连接的是 23。
JDBC 相容的数据库服务器	<p>依照目标数据库服务器配置的端口号码, 预设的端口号码如下:</p> <ul style="list-style-type: none"> - MS SQL Server: 1433 - Oracle: 1521 - PostgreSQL: 5432 - Sybase: 5000

4.3 管理 Windows 目标资源

4.3.1 创建 Windows 目标资源

若要创建新的 Windows 目标资源条目, 请执行以下步骤:

- 通过管理控制台登录到系统, 如 [PSM 管理控制台通用管理指南](#) 所述。
- 在主菜单, 找到并点击 *PSM->Target Resource (目标资源)->Create (创建)*, 如下所示:



图表 4-1: 目标资源子菜单选项

- 选择“Windows Target Resource”(Windows 目标资源)作为实施, 然后按一下“Next”(下一步), 如下所示:

图表 4-2: 选择 Windows 目标资源实施

下方屏幕将会出现:

图表 4-3: 创建 Windows 目标资源

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段。

屏幕的下方部分包含**属性**标签，它包含系统定义属性：存储服务器连接信息，和目标资源测试连接信息。

备注：

* 表示强制属性。

ESSO 模板文件栏位是专门用于 PSM-SSO 整合的。将会在另外一本用户指南中为您提供详细说明。

更新密码模式，若适用，允许管理员指定，是否相关的凭证可用于，为存在于目标资源内的用户账号，更改密码或重设密码

有重设密码特权的凭证栏位，仅适用于重设密码操作。管理员要为要求的用户账号，指定相关有重设密码特权的凭证。将会在稍后章节，为您描述有重设密码特权的凭证。

请输入相应信息。

- 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.3.2 查找和查看 Windows 目标资源

若要查找和查看要求的 Windows 目标资源条目，请执行下方步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *PSM->Target Resource (目标资源) -> Create (创建)*，如 [图表 4-1](#) 所示
3. 输入搜索条件，然后按一下“Search”（搜索）来执行搜索，如下所示：

图表 4-4: 目标资源 – 搜索条件

备注:

搜索可以是通配符相符(*)或完全匹配,且区分大小写。例如,若管理员输入“DEMO*”到 ID 栏位,会找到“DEMO123”条目,而不会找到“123DEMO”条目。

同时,搜索条件也可以是基于“AND”(和、并且)条件。例如,管理员输入搜索条件到 ID 和名称栏位,则会找到同时符合 ID 和名称的条目。

4. 搜索目标资源结果页面,将会显示符合搜索条件的目标资源,如下所示:

Search Target Resource Result		
Total Records: 1 Page 1/1		
Target Resource Id	Target Resource Name	Description
DEMO-WINDOWS-TR	Demo Windows Target Resource	Demonstration Windows Target Resource

图表 4-5: 目标资源 – 搜索结果

管理员可以按一下要求的目标资源 ID,来查看具体资料,屏幕会处于查看模式,即不可编辑,如下所示:

View Target Resource			
*Target Resource Id:	DEMO-WINDOWS-TR	*Target Resource Name:	Demo Windows Target Resource
Description:	Demonstration Windows Target Resource	Version :	1
Implementation:	WindowsTargetResource	ESSO Template Files	
Segment			
Attributes			
Attribute Name	Attribute Value	Remark	
Server Name	192.168.1.30		
Domain name			
Update Password Mode	Change (default)		
Privileged Credential for Reset Password			
<input type="button" value="Test Connection"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Back"/>			

图表 4-6: 查看目标资源


5. 管理员可测试配置，以检查是否正确配置目标资源，方法是按一下“Test Connection”（测试连接）按钮，如图表 4-6 所示，然后下方窗口将会出现：

Test Connection	
Test connection user:	<input type="text"/>
Test connection password:	<input type="password"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

图表 4-7: 测试连接

。指定有效的用户信息来连接到目标资源，然后按一下“OK”（确认）。

若测试连接成功，将会出现下方提示信息窗口：

Information	
	Test Connection Successful!
<input type="button" value="OK"/>	

图表 4-8: 测试连接成功

按一下“OK”（确认）来关闭信息窗口。

管理员可以继续下方部分，来了解如何管理目标资源条目。

4.3.3 管理 Windows 目标资源

在创建了要求的 Windows 目标资源条目后，管理员可以管理条目：编辑或删除要求的条目。

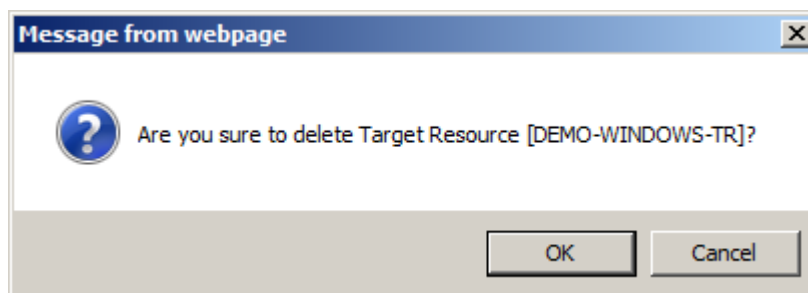
若要编辑目标资源条目，请执行以下步骤：

1. 执行在 [4.3.2](#) 部分所述的步骤，来查看要求的目标资源。

2. 按一下如**图表 4-6** 所示的“Edit”（编辑），屏幕将会变为编辑模式。
3. 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

若要删除目标资源条目，请执行以下步骤：

1. 执行在 **4.3.2** 部分所述的步骤，来查看要求的目标资源。
2. 按一下如**图表 4-6** 所示的“Delete”（删除），将会提示管理员删除确认屏幕，如下所示：



图表 4-9: 删除目标资源 – 确认

3. 按一下“OK”（确认）来删除，或者“Cancel”（取消）来取消操作。
4. 成功删除后，将会传回下方信息：



图表 4-10: 成功删除

4.4 管理基于 Telnet 的 UNIX 目标资源

4.4.1 创建基于 Telnet 的 UNIX 目标资源

若要创建新的基于 Telnet 的 UNIX 目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 **PSM 管理控制台通用管理指南** 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration（PSM 配置），如**图表 4-1** 所示。
3. 选择“Telnet Unix Target Resource”（Telnet Unix 目标资源）作为实施，然后按一下“Next”（下一步），如下所示：



图表 4-11: 选择 Telnet UNIX 目标资源实施

下方屏幕将会出现：

Create Target Resource

*Target Resource Id: *Target Resource Name:

Description: Version: -1

Implementation: TelnetUnixTargetResource ESSO Template Files

Segment

Attributes Connection Shell prompt

Attribute Name	Attribute Value	Remark
Update Password Mode	(default) ▾	Default: Change
Privileged Credential for Reset Password	▾	

图表 4-12: 创建 Telnet UNIX 目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

下方是其他标签的说明：

■ 连接

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt

Attribute Name	Attribute Value	Remark
*Server Type	- ▾	
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 23
Timeout (in seconds)	<input type="text"/>	Default: 5

图表 4-13: 创建 Telnet UNIX 目标资源 – 连接

备注：

所支持的服务器类型是：Linux、Solaris、HP-UX 和 AIX。

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Shell prompt	<input type="text"/>	Default: \$
Switch role command	<input type="text"/>	Default: su \$roleName
Enter role password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser login		
Switch user command	<input type="text"/>	Default: su \$userId
Enter Superuser password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser Shell prompt	<input type="text"/>	Default: #
Change Password		
Change password command (for current user)	<input type="text"/>	Default: passwd
Change password command	<input type="text"/>	Default: passwd \$userId
Enter current password prompt	<input type="text"/>	Default: .*exist.*
Enter new password prompt	<input type="text"/>	Default: .*[N n]ew.*
Confirm new password prompt	<input type="text"/>	Default: .*[R r]e-enter.*
Change password successful message	<input type="text"/>	Default: .*success.*
Reset Password		
Reset password command	<input type="text"/>	Default: passwd \$userId
Enter password prompt (reset)	<input type="text"/>	Default: .*[P p]assword.*
Enter new password prompt (reset)	<input type="text"/>	Default: .*[N n]ew.*
Confirm new password prompt (reset)	<input type="text"/>	Default: .*[R r]e-enter.*
Reset password successful message	<input type="text"/>	Default: .*success.*

图表 4-14: 创建 Telnet UNIX 目标资源 – Shell 提示

请输入相应信息。

- 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.4.2 查找和查看基于 Telnet 的 UNIX 目标资源

若要查找和查看基于 Telnet 的 UNIX 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

备注：

- i. 当查看基于 Telnet 的 UNIX 目标资源的时候，为管理员提供一个功能：发现与目标资源相关的凭证。若要如此，请按一下“Discover Credentials”（发现凭证）按钮，如下所示：

The screenshot shows the 'View Target Resource' window for a target resource named 'DEMO-TELNET-UNIX-TR'. The interface includes a table with the following details:

*Target Resource Id:	DEMO-TELNET-UNIX-TR	*Target Resource Name:	Demo Telnet-Based UNIX Target Resource
Description:	Demonstration Telnet-Based UNIX Target Resource	Version :	3
Implementation:	TelnetUnixTargetResource	ESSO Template Files	
Segment			

Below the table, there are tabs for 'Attributes', 'Connection', and 'Shell prompt'. The 'Attributes' tab is active, showing a table of attributes:

Attribute Name	Attribute Value	Remark
Update Password Mode	Change (default)	
Privileged Credential for Reset Password		

At the bottom of the window, there are five buttons: 'Discover Credentials', 'Test Connection', 'Edit', 'Delete', and 'Back'.

图表 4-15: 查看 Telnet UNIX 目标资源

下方屏幕将会出现：

The screenshot shows the 'Discover Credentials' dialog box. It contains the following elements:

- Two unchecked checkboxes:
 - Option to Connect Using Existing UCM Credential
 - Option to Connect Via Normal Account
- Two text input fields:
 - Root Account Id: []
 - Root Account Password: []
- A 'Discover Credentials' button.
- A 'Close' button.

图表 4-16: 查看 Telnet UNIX 目标资源 – 发现凭证

管理员可以选择，使用现有凭证来连接到目标资源，如下所示：

图表 4-17: 使用现有凭证发现凭证

对于上述情况，请从配置下拉列表中选择要求的凭证，然后按一下“Discover Credentials”（发现凭证）来发现凭证。

或者，管理员选择通过普通账号来连接目标资源，如下所示：

图表 4-18: 通过普通账号发现凭证

在上述情况，请指定根账号登录信息和要求的普通账号登录信息，然后按一下“Discover Credentials”（发现凭证）来发现凭证。

成功发现后，将会显示凭证列表，如下所示：

Total Records: 29 Page 1/3

User Id	Exist In UCM	Roles	Credential Id
acmatrix	<input type="checkbox"/>	Normaluser	
adm	<input type="checkbox"/>	Normaluser	
mycred01	<input type="checkbox"/>	Normaluser	
mycred02	<input type="checkbox"/>	Normaluser	

Close

图表 4-19: 所发现的凭证列表

- ii. 为管理员提供了一个测试配置的功能，以检验是否正确配置目标资源。请参考 4.3.2 部分内容来了解更多。

4.4.3 管理基于 Telnet 的 UNIX 目标资源

创建了要求的基于 Telnet 的 UNIX 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.5 管理基于 SSH 的 UNIX 目标资源

4.5.1 创建基于 SSH 的 UNIX 目标资源

若要创建新的基于 SSH 的 UNIX 目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration (PSM 配置)，如图表 4-1 所示。
3. 选择“Unix Target Resource”(Unix 目标资源)作为实施，然后按一下“Next”(下一步)，如下所示：

图表 4-20: 选择 SSH UNIX 目标资源实施

下方屏幕将会出现：

Attribute Name	Attribute Value	Remark
Update Password Mode	(default)	Default: Change
Privileged Credential for Reset Password		

图表 4-21: 创建 SSH UNIX 目标资源实施 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是属性标签，它包含目标资源的系统定义的属

性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

下方是其他标签的说明：

■ 连接

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Server Type	-	
*Host		
Port		Default: 22
Timeout (in seconds)		Default: 5

图表 4-22: 创建 SSH UNIX 目标资源实施 – 连接

备注：

所支持的服务器类型是：Linux、Solaris、HP-UX 和 AIX。

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Shell prompt	<input type="text"/>	Default: \$
Switch role command	<input type="text"/>	Default: su \$roleName
Enter role password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser login		
Switch user command	<input type="text"/>	Default: su \$userId
Enter Superuser password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser Shell prompt	<input type="text"/>	Default: #
Change Password		
Change password command (for current user)	<input type="text"/>	Default: passwd
Change password command	<input type="text"/>	Default: passwd \$userId
Enter current password prompt	<input type="text"/>	Default: .*exist.*
Enter new password prompt	<input type="text"/>	Default: .*[N n]ew.*
Confirm new password prompt	<input type="text"/>	Default: .*[R r]e-enter.*
Change password successful message	<input type="text"/>	Default: .*success.*
Reset Password		
Reset password command	<input type="text"/>	Default: passwd \$userId
Enter password prompt (reset)	<input type="text"/>	Default: .*[P p]assword.*
Enter new password prompt (reset)	<input type="text"/>	Default: .*[N n]ew.*
Confirm new password prompt (reset)	<input type="text"/>	Default: .*[R r]e-enter.*
Reset password successful message	<input type="text"/>	Default: .*success.*

图表 4-23: 创建 SSH UNIX 目标资源实施 – Shell 提示

请输入相应信息。

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.5.2 查找和查看基于 SSH 的 UNIX 目标资源

若要查找和查看基于 SSH 的 UNIX 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

备注：

- 当查看基于 SSH 的 UNIX 目标资源的时候，为管理员提供一个功能：发现与目标资源相关的凭证。请参考 4.4.2 部分内容来了解详细说明。
- 还为管理员提供测试配置的功能，以检查是否已正确配置目标资源。请参考 4.3.2 部分内容来了解详细说明。

还为管理员提供测试配置的功能，以检查是否已正确配置目标资源。请参考 4.3.2 部分内容来了解详细说明。

4.5.3 管理基于 SSH 的 UNIX 目标资源

创建了要求的基于 SSH 的 UNIX 目标资源后，管理员可以管理条目：编辑或删除要求的条目，

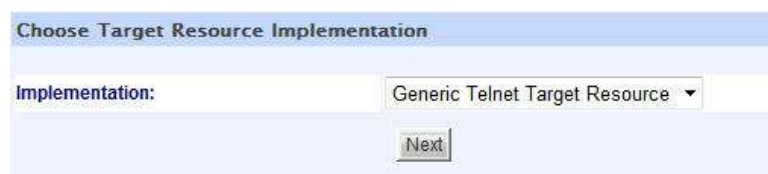
而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

4.6 管理基于 Telnet 通用类的目标资源

4.6.1 创建基于 Telnet 通用类的目标资源

若要创建新的基于 Telnet 通用类的目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration (PSM 配置)，如 [图表 4-1](#) 所示。
3. 选择“Generic Telnet Target Resource”（通用类 Telnet 目标资源）作为实施，然后按一下“Next”（下一步），如下所示：



The screenshot shows a web-based configuration interface. At the top, there is a blue header bar with the text "Choose Target Resource Implementation". Below this, there is a form with a label "Implementation:" followed by a dropdown menu. The dropdown menu is currently set to "Generic Telnet Target Resource". Below the dropdown menu, there is a button labeled "Next".

图表 4-24: 选择通用类 Telnet 目标资源实施

下方屏幕将会出现：

Create Target Resource

*Target Resource Id: *Target Resource Name:

Description: Version: -1

Implementation: GenericTelnetTargetResource ESSO Template Files

Segment

Attributes

Attribute Name	Attribute Value	Remark
Attributes		
Update Password Mode	(default) ▾	Default: Change
Privileged Credential for Reset Password	▾	
By filling these attributes, you can click the test script button for connection testing.		
*Host	<input type="text"/>	
*Port	<input type="text"/>	
Timeout (in seconds)	<input type="text"/>	Default: 10
Shell prompt		
Command Terminator	<input type="text"/>	
*Shell prompt	<input type="text"/>	
Superuser Shell prompt	<input type="text"/>	Default: #
Enter login username prompt	<input type="text"/>	Default: .*[L l]ogin.*
Enter login password prompt	<input type="text"/>	Default: .*[P p]assword.*
Switch role command	<input type="text"/>	
Switch Role Password Prompt	<input type="text"/>	Default: .*[P p]assword.*

图表 4-25: 创建基于 Telnet 通用类目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

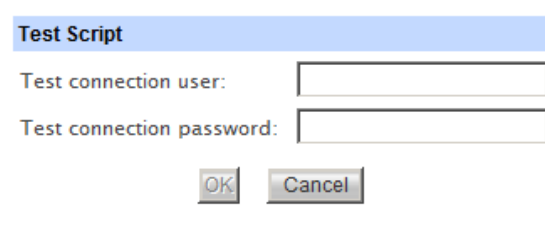
备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

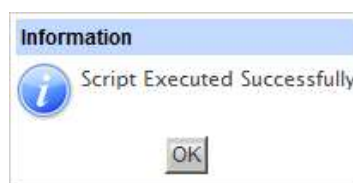
请输入相应信息。

您可以测试配置，方法是按一下“Test Script”（测试脚本）按钮，来确保配置正确，您需要为主机、端口和 Shell 提示栏位指定正确的值。将会提示您输入有效的测试用户的登录名称和密码，如下所示：



图表 4-26: 测试基于 Telnet 通用类目标资源

若测试成功，您会看到下方提示：



图表 4-27: 测试基于 Telnet 通用类目标资源成功

下方是其他标签的说明：

- **更改密码**

此标签包含为目标资源更改密码脚本，如下所示：

Attribute Name	Attribute Value	Remark
Change Password Script	<pre> /*this is a sample code, please remove the comment mark in this line and import com.isprint.am.dto.exception.UCMEException; import com.jscape.inet.telnet.TelnetException; try { logger.info("Send passwd command"); session.sendWait("passwd", ".*exist.*", true, timeout); } catch (TelnetException e) { logger.error("Send passwd command failed"); throw new UCMEException("Send passwd command failed"); } try { logger.info("Send old password"); session.sendWait(oldPassword, ".*[N]ew.*", true, timeout); } catch (TelnetException e) { logger.error("Send old password failed"); throw new UCMEException("Send old password failed"); } try { logger.info("Send new password"); session.sendWait(newPassword, ".*[R r]e-enter.*", true, timeout); } catch (TelnetException e) { logger.error("Send new password failed"); throw new UCMEException("Send new password failed"); } try { logger.info("Send confirm new password"); </pre>	<p>Macro variable :</p> <ul style="list-style-type: none"> - timeout : used as waiting time limit of certain operation. - session : session of connection, used for sendWait process in change and reset password scenario. - logger : used for logging purpose. - userId : username of credential being processed. - oldPassword : the current password of credential before change password or reset password process. - newPassword : the new password generated from server. Used to put it under sendWait in change and reset password process. <p>Additional variable :</p> <ul style="list-style-type: none"> - credential : credential object being processed. - targetResource : PasswordTargetResource object associated to the credential. <p>Method :</p> <ul style="list-style-type: none"> - session.sendWait (sentPrompt, expectedPrompt, isRegex, timeout) : used to send prompt in change or reset password scenario. - session.sendNoWait (sentPrompt) : used to send prompt without expecting any reply. <p>Parameter :</p> <ul style="list-style-type: none"> - sentPrompt (String) : the prompt being sent. - expectedPrompt (String) : the prompt expected after sending sentPrompt. - isRegex (boolean) : is using regex or not. - timeout : waiting time limit for getting the expected prompt.

图表 4-28: 创建基于 Telnet 通用类目标资源 – 更改密码

■ 重设密码

此标签包含为目标资源重设密码脚本，如下所示：

Attribute Name	Attribute Value	Remark
Reset Password Script	<pre> /*this is a sample code, please remove the comment mark in this line and import com.isprint.am.dto.exception.UCMEException; import com.jscape.inet.telnet.TelnetException; try { logger.info("Send passwd command"); session.sendWait("passwd "+userId, ".*[N n]ew.*", true, timeout); } catch (TelnetException e) { logger.error("Send passwd command failed"); throw new UCMEException("Send passwd command failed"); } try { logger.info("Send new password"); session.sendWait(newPassword, ".*[R r]e-enter.*", true, timeout); } catch (TelnetException e) { logger.error("Send new password failed"); throw new UCMEException("Send new password failed"); } try { logger.info("Send confirm new password"); session.sendWait(newPassword, ".*success.*", true, timeout); } catch (TelnetException e) { logger.error("Confirm new password failed"); throw new UCMEException("Confirm new password failed"); } logger.info("Reset password succeed"); */ </pre>	<p>Macro variable :</p> <ul style="list-style-type: none"> - timeout : used as waiting time limit of certain operation. - session : session of connection, used for sendWait process in change and reset password scenario. - logger : used for logging purpose. - userId : username of credential being processed. - oldPassword : the current password of credential before change password or reset password process. - newPassword : the new password generated from server. Used to put it under sendWait in change and reset password process. <p>Additional variable :</p> <ul style="list-style-type: none"> - credential : credential object being processed. - targetResource : PasswordTargetResource object associated to the credential. <p>Method :</p> <ul style="list-style-type: none"> - session.sendWait (sentPrompt, expectedPrompt, isRegex, timeout) : used to send prompt in change or reset password scenario. - session.sendNoWait (sentPrompt) : used to send prompt without expecting any reply. <p>Parameter :</p> <ul style="list-style-type: none"> - sentPrompt (String) : the prompt being sent. - expectedPrompt (String) : the prompt expected after sending sentPrompt. - isRegex (boolean) : is using regex or not. - timeout : waiting time limit for getting the expected prompt.

图表 4-29: 创建通用类 SSH 目标资源 – 重设密码

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.6.2 查找和查看基于 Telnet 通用类的目标资源

若要查找和查看要求的基于 Telnet 的通用类目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

4.6.3 管理基于 Telnet 通用类的目标资源

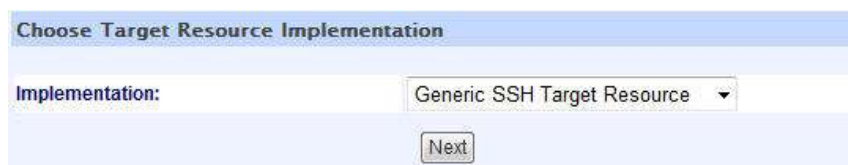
创建了要求的基于 Telnet 通用类的目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.7 管理基于 SSH 通用类的目标资源

4.7.1 创建基于 SSH 通用类的目标资源

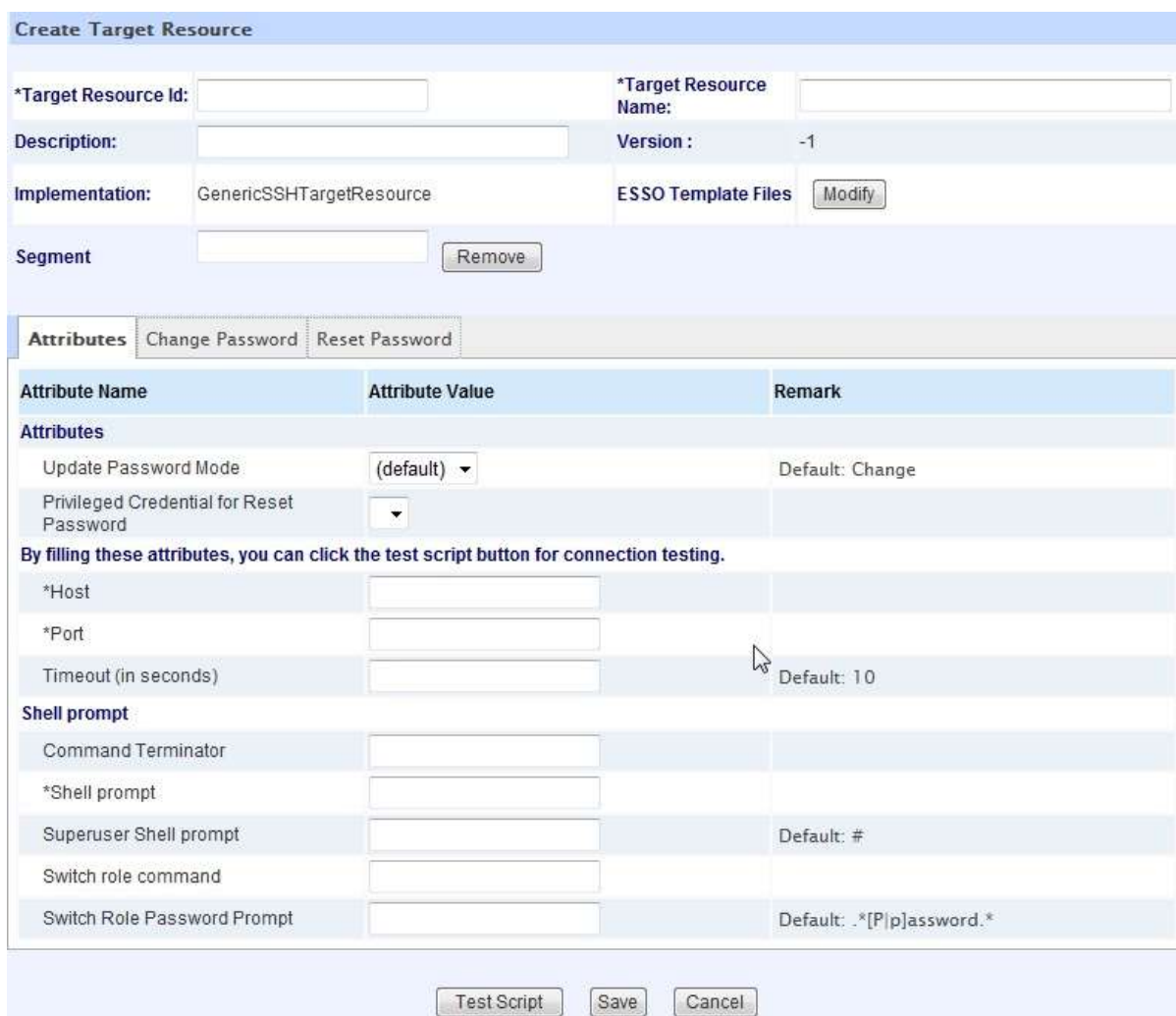
若要创建新的基于 SSH 通用类的目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration (PSM 配置)，如图表 4-1 所示。
3. 选择“Generic SSH Target Resource”(通用类 SSH 目标资源)作为实施，然后按一下“Next”(下一步)，如下所示：



图表 4-30: 选择通用类 SSH 目标资源实施

下方屏幕将会出现：



Attribute Name	Attribute Value	Remark
Attributes		
Update Password Mode	(default) ▾	Default: Change
Privileged Credential for Reset Password	▾	
By filling these attributes, you can click the test script button for connection testing.		
*Host	<input type="text"/>	
*Port	<input type="text"/>	
Timeout (in seconds)	<input type="text"/>	Default: 10
Shell prompt		
Command Terminator	<input type="text"/>	
*Shell prompt	<input type="text"/>	
Superuser Shell prompt	<input type="text"/>	Default: #
Switch role command	<input type="text"/>	
Switch Role Password Prompt	<input type="text"/>	Default: .*[P]p)assword.*

图表 4-31: 创建基于 SSH 通用类目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

您可以测试配置，以确保已正确配置它，如 4.6.1 部分所述。

下方是其他标签的说明：

■ 更改密码

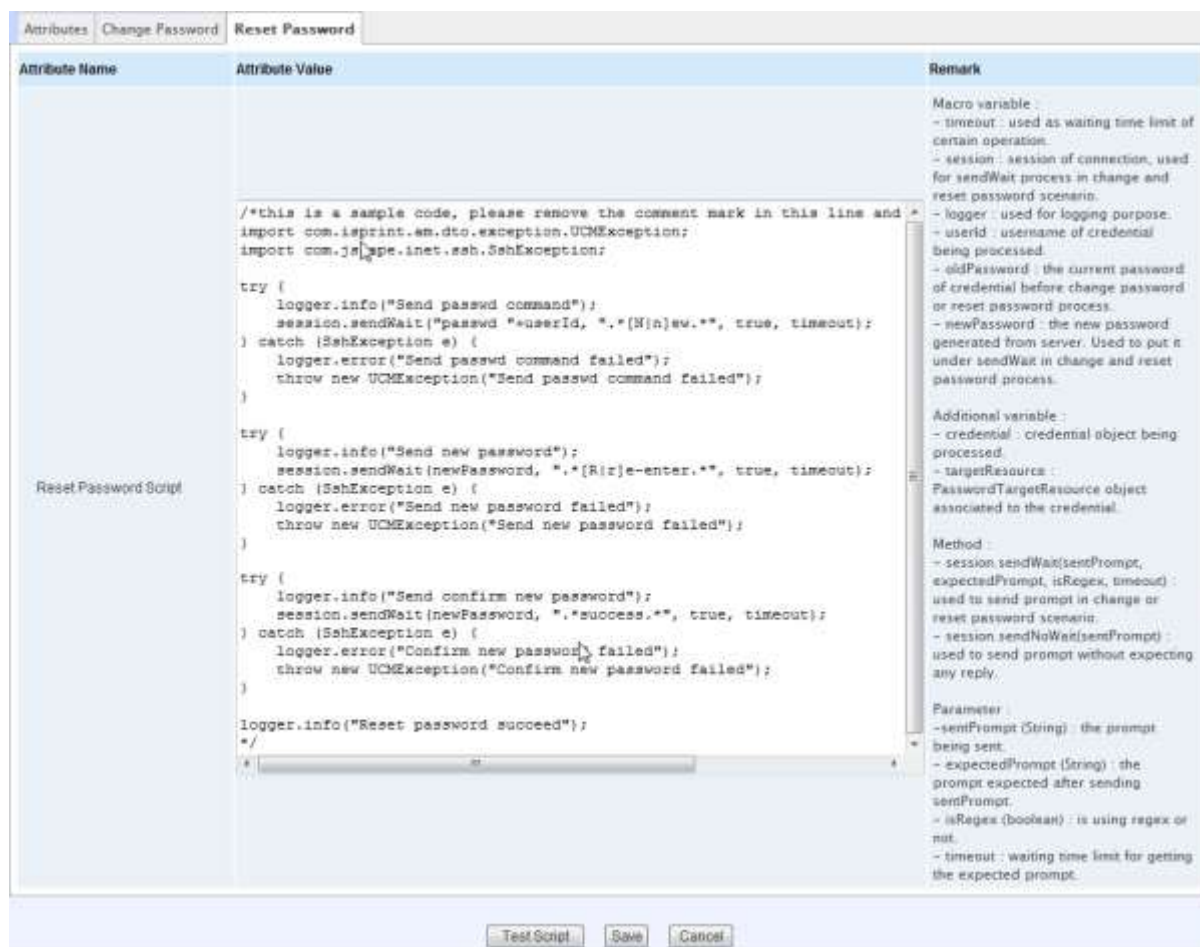
此标签包含为目标资源更改密码脚本，如下所示：

Attribute Name	Attribute Value	Remark
Change Password Script	<pre> /*this is a sample code, please remove the comment mark in this line and import com.isprint.am.dto.exception.UCMException; import com.jscape.inet.ssh.SshException; try { logger.info("Send passwd command"); session.sendWait("passwd", ".*exit.*", true, timeout); } catch (SshException e) { logger.error("Send passwd command failed"); throw new UCMException("Send passwd command failed"); } try { logger.info("Send old password"); session.sendWait(oldPassword, ".*[N n]ew.*", true, timeout); } catch (SshException e) { logger.error("Send old password failed"); throw new UCMException("Send old password failed"); } try { logger.info("Send new password"); session.sendWait(newPassword, ".*[R r]e-enter.*", true, timeout); } catch (SshException e) { logger.error("Send new password failed"); throw new UCMException("Send new password failed"); } try { logger.info("Send confirm new password"); </pre>	<p>Macro variable</p> <ul style="list-style-type: none"> - timeout : used as waiting time limit of certain operation. - session : session of connection, used for sendWait process in change and reset password scenario. - logger : used for logging purpose. - userid : username of credential being processed. - oldPassword : the current password of credential before change password or reset password process. - newPassword : the new password generated from server. Used to put it under sendWait in change and reset password process. <p>Additional variable</p> <ul style="list-style-type: none"> - credential : credential object being processed. - targetResource : PasswordTargetResource object associated to the credential. <p>Method</p> <ul style="list-style-type: none"> - session.sendWait(sendPrompt, expectedPrompts, isRegex, timeout) : used to send prompt in change or reset password scenario. - session.sendNoWait(sendPrompt) : used to send prompt without expecting any reply. <p>Parameter</p> <ul style="list-style-type: none"> - sendPrompt (String) : the prompt being sent. - expectedPrompts (String) : the prompt expected after sending sendPrompt. - isRegex (boolean) : is using regex or not. - timeout : waiting time limit for getting the expected prompt.

图表 4-32: 创建基于 SSH 通用类目标资源 – 更改密码

■ 重设密码

此标签包含为目标资源重设密码脚本，如下所示：



图表 4-33: 创建基于 SSH 通用类目标资源 – 重设密码

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.7.2 查找和查看基于 SSH 通用类的目标资源

若要查找和查看基于 SSH 通用类的目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

4.7.3 管理基于 SSH 通用类的目标资源

创建了要求的基于 SSH 通用类的目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

4.8 管理 RDP 目标资源

4.8.1 创建 RDP 目标资源

若要创建新的 RDP 目标资源条目，请执行以下步骤：

- 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
- 在主菜单，找到并点击 PSM -> PSM Configuration（PSM 配置），如图表 4-1 所示。

3. 选择“RDP Target Resource”（RDP 目标资源）作为实施，然后按一下“Next”（下一步），如下所示：

图表 4-34: 选择 RDP 目标资源实施

下方屏幕将会出现：

Attribute Name	Attribute Value	Remark
*Server Name	<input type="text"/>	
Domain name	<input type="text"/>	
Update Password Mode	(default) ▾	Default: Change
Privileged Credential for Reset Password	▾	

图表 4-35: 创建 RDP 目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.8.2 查找和查看 RDP 目标资源

若要查找和查看要求的 RDP 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

4.8.3 管理 RDP 目标资源

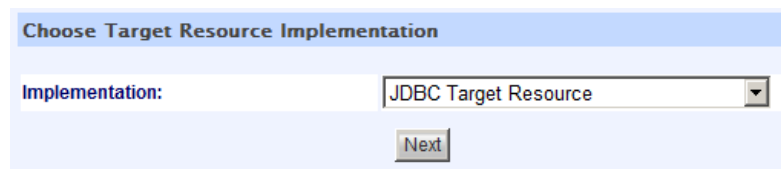
创建了要求的 RDP 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.9 管理 JDBC 目标资源

4.9.1 创建 JDBC 目标资源

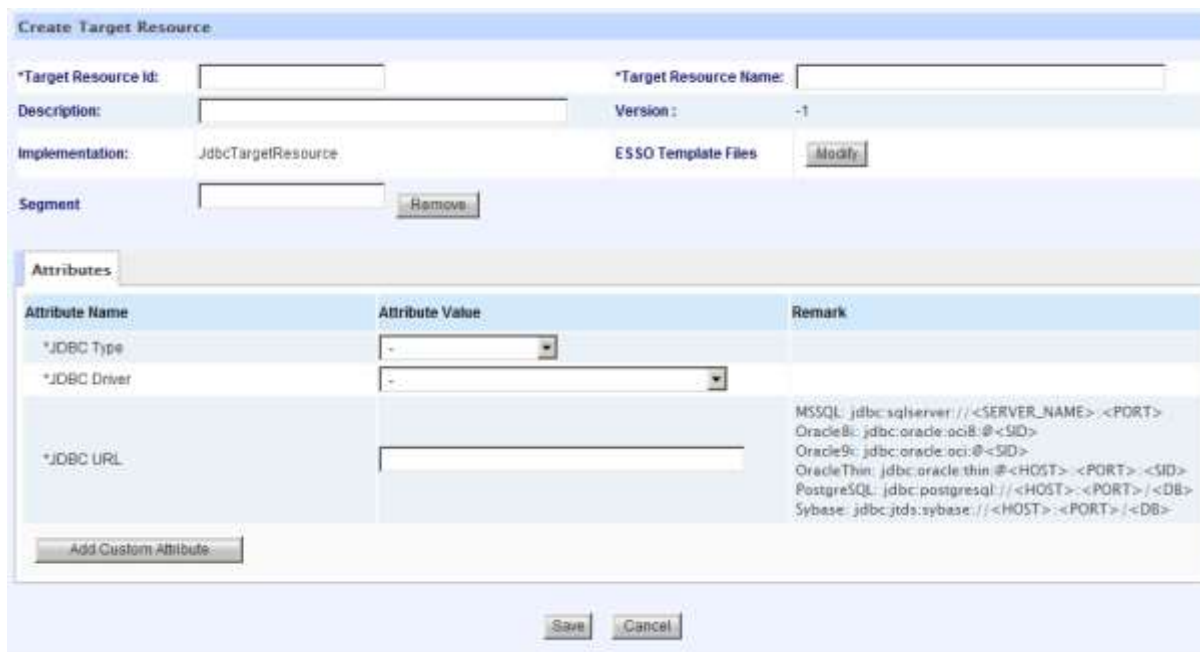
若要创建新的 JDBC 目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration (PSM 配置)，如 [图表 4-1](#) 所示。
3. 选择“JDBC Target Resource”(JDBC 目标资源) 作为实施，然后按一下“Next”(下一步)，如下所示：



图表 4-36: 选择 JDBC 目标资源实施

下方屏幕将会出现：



Attribute Name	Attribute Value	Remark
*JDBC Type	-	
*JDBC Driver	-	
*JDBC URL		MSSQL: jdbc:sqlserver://<SERVER_NAME>:<PORT> Oracle8: jdbc:oracle:oci8:@<SID> Oracle9: jdbc:oracle:oci:@<SID> OracleThin: jdbc:oracle:thin:@<HOST>:<PORT>:<SID> PostgreSQL: jdbc:postgresql://<HOST>:<PORT>/<DB> Sybase: jdbc:jtds:sybase://<HOST>:<PORT>/<DB>

图表 4-37: 创建 JDBC 目标资源

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含**属性**标签，它包含系统定义和自定义（用户定义）的属性。系统定义的属性存储连接到要求的 JDBC 数据库服务器的连接信息。管理员可以增加、编辑或删除任何自定义属性。

备注：

- * 表示强制属性。

您可以参考 [4.3.1](#) 部分内容，来了解关于 ESSO 模板文件栏位的更多说明。

请输入相应信息。

若要增加新的自定义属性，请按一下“Add Custom Attribute”（增加自定义属性），然后会出现弹出式窗口，如下所示：

图表 4-38: 增加新的属性

指定属性名称、数据类型和值，然后按一下“Apply”（应用）来保存属性。

备注：

若想要以加密形式来在安全注册表里存储属性值，请勾选“Encryption”（加密）选项。保存条目后，无法撤销此动作。

增加属性后，管理员可以编辑它的值，或者删除它：按一下其相关的“Delete”（删除）按钮，如下所示：

图表 4-39: 新的属性已增加

将会出现确认删除窗口以提示管理员，如下所示：

图表 4-40: 自定义属性删除确认

按一下“OK”（确认）来确认删除，或者“Cancel”（取消）来取消删除。

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.9.2 查找和查看 JDBC 目标资源

若要查找和查看要求的 JDBC 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

4.9.3 管理 JDBC 目标资源

创建了要求的 JDBC 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.10 管理 AS400 目标资源

4.10.1 创建 AS400 目标资源

若要创建新的 AS400 目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration (PSM 配置)，如 [图表 4-1](#) 所示。
3. 选择“AS400 Target Resource” (AS400 目标资源) 作为实施，然后按一下“Next” (下一步)，如下所示：

图表 4-41: 选择 AS400 目标资源实施

下方屏幕将会出现：

Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 23
Timeout (in seconds)	<input type="text"/>	Default: 15
Debug	(default) ▾	Default: true

图表 4-42: 创建 AS400 目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

- * 表示强制属性。

您可以参考 [4.3.1](#) 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.10.2 查找和查看 AS400 目标资源

若要查找和查看要求的 AS400 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源(如 4.3.2 部分所示)，请参考该部分内容。

4.10.3 管理 AS400 目标资源

. 创建了要求的 AS400 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.11 4.11 管理基于 Telnet 的 Cisco 目标资源

4.11.1 创建基于 Telnet 的 Cisco 目标资源

若要创建新的基于 Telnet 的 Cisco 目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如图表 4-1 所示。
3. 选择“Telnet Cisco Target Resource”（Telnet Cisco 目标资源）作为实施，然后按一下“Next”（下一步），如下所示：

图表 4-43: 选择 Telnet Cisco 目标资源实施

下方屏幕将会出现：

Attribute Name	Attribute Value	Remark
Update Password Mode	(default)	Default: Change
Privileged Credential for Reset Password		

图表 4-44: 创建基于 Telnet 的 Cisco 目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ 连接

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 23
Timeout (in seconds)	<input type="text"/>	Default: 10

图表 4-45: 创建基于 Telnet 的 Cisco 目标资源 – 连接

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[U u]ername.*
Enter login password prompt	<input type="text"/>	Default: .*[P p]assword.*
Shell prompt	<input type="text"/>	Default: >
Enable		
Start enable mode command	<input type="text"/>	Default: enable
Enable password prompt	<input type="text"/>	Default: .*[P p]assword.*
Enable shell prompt	<input type="text"/>	Default: #
End enabled mode command	<input type="text"/>	Default: exit
Update password		
Change password command (for current user)	<input type="text"/>	Default: username \$userId password \$newPassword
Change enable password command	<input type="text"/>	Default: enable secret \$newPassword
Configuration Mode		
Start configuration mode command	<input type="text"/>	Default: configure terminal
Configuration mode shell prompt	<input type="text"/>	Default: (config)
End configuration mode command	<input type="text"/>	Default: end
Save configuration command	<input type="text"/>	Default: write memory

图表 4-46: 创建基于 Telnet 的 Cisco 目标资源 – Shell 提示

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.11.2 查找和查看基于 Telnet 的 Cisco 目标资源

若要查找和查看要求的基于 Telnet 的 Cisco 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

4.11.3 管理基于 Telnet 的 Cisco 目标资源

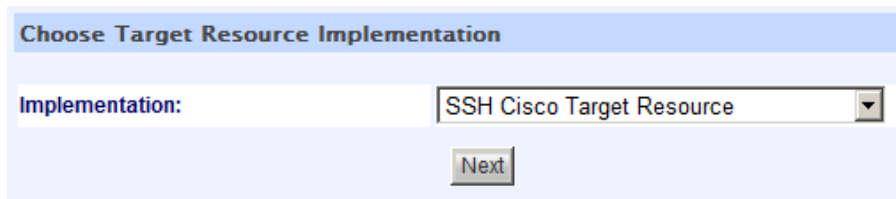
创建了要求的基于 Telnet 的 Cisco 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.12 管理基于 SSH 的 Cisco 目标资源

4.12.1 创建基于 SSH 的 Cisco 目标资源

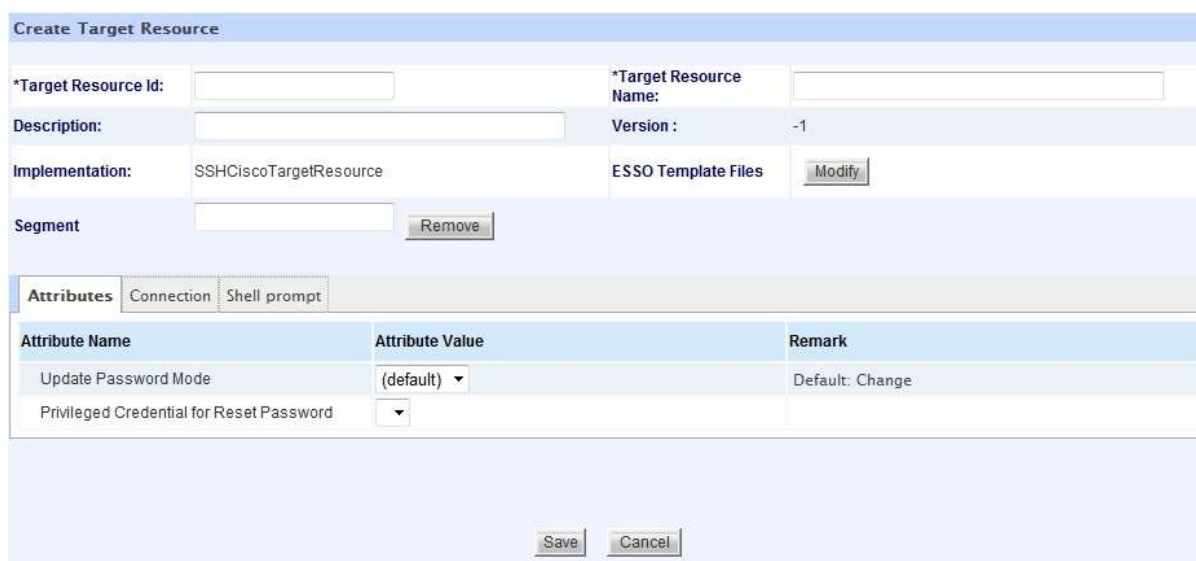
若要条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM -> PSM Configuration（PSM 配置），如 [图表 4-1](#) 所示。
3. 选择“SSH Cisco Target Resource”（SSH Cisco 目标资源）作为实施，然后按一下“Next”（下一步），如下所示：



图表 4-47: 选择基于 SSH 的 Cisco 目标资源实施

下方屏幕将会出现：



Attribute Name	Attribute Value	Remark
Update Password Mode	(default) ▾	Default: Change
Privileged Credential for Reset Password	▾	

图表 4-48: 创建基于 SSH 的 Cisco 目标资源 - 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ 连接

T 此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 22
Timeout (in seconds)	<input type="text"/>	Default: 10

图表 4-49: 创建基于 SSH 的 Cisco 目标资 – 连接

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[Uu]username.*
Enter login password prompt	<input type="text"/>	Default: .*[Pp]password.*
Shell prompt	<input type="text"/>	Default: >
Enable		
Start enable mode command	<input type="text"/>	Default: enable
Enable password prompt	<input type="text"/>	Default: .*[Pp]password.*
Enable shell prompt	<input type="text"/>	Default: #
End enabled mode command	<input type="text"/>	Default: exit
Update password		
Change password command (for current user)	<input type="text"/>	Default: username \$userId password \$newPassword
Change enable password command	<input type="text"/>	Default: enable secret \$newPassword
Configuration Mode		
Start configuration mode command	<input type="text"/>	Default: configure terminal
Configuration mode shell prompt	<input type="text"/>	Default: (config)
End configuration mode command	<input type="text"/>	Default: end
Save configuration command	<input type="text"/>	Default: write memory

图表 4-50: 创建基于 SSH 的 Cisco 目标资 – Shell 提示

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.12.2 查找和查看基于 SSH 的 Cisco 目标资源

若要查找和查看要求的基于 SSH 的 Cisco 目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2 部分](#)所示），请参考该部分内容。

4.12.3 管理基于 SSH 的 Cisco 目标资源

创建了要求的基于 SSH 的 Cisco 目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3 部分](#)所示），请参考该部分内容。

4.13 管理基于 Telnet 的 Huawei 防火墙目标资源

4.13.1 创建基于 Telnet 的 Huawei 防火墙目标资源

若要创建新的基于 Telnet 的 Huawei 防火墙条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#)所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如 [图表 4-1](#) 所示。
3. 选择“Telnet Huawei Firewall Target Resource”（Telnet Huawei 防火墙目标资源）作为实施，然后按一下“Next”（下一步），如下所示：

图表 4-51: 选择 Telnet Huawei 防火墙目标资源实施

下方屏幕将会出现：

Attribute Name	Attribute Value	Remark
Update Password Mode	Reset (default)	Default: Reset
Privileged Credential for Reset Password		

图表 4-52: 创建基于 Telnet 的 Huawei 防火墙目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是属性标签，它包含目标资源的系统定义的属

性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ **连接**

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 23
Timeout (in seconds)	<input type="text"/>	Default: 5

图表 4-53: 创建基于 Telnet 的 Huawei 防火墙目标资源 – 连接

■ **Shell 提示**

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[Ll]ogin.*
Enter login password prompt	<input type="text"/>	Default: .*[Pp]assword.*
Shell prompt	<input type="text"/>	Default: >
Enter Superuser password prompt	<input type="text"/>	Default: .*[Pp]assword.*
Superuser Shell prompt	<input type="text"/>	Default:]
Succeed Login As Superuser message	<input type="text"/>	Default: .*[Pp]rivilege note.*
Update password		
System command	<input type="text"/>	Default: system
Succeed execute system message	<input type="text"/>	Default: .*[C c]trl.*
Reset password command	<input type="text"/>	Default: local-user \$userId password cipher \$newPassword
Save command	<input type="text"/>	Default: save
Exit command	<input type="text"/>	Default: quit

图表 4-54: 创建基于 Telnet 的 Huawei 防火墙目标资源 – Shell 提示

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.13.2 查找和查看基于 Telnet 的 Huawei 防火墙目标资源

若要查找和查看要求的基于 Telnet 的 Huawei 防火墙目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容

4.13.3 管理基于 Telnet 的 Huawei 防火墙目标资源

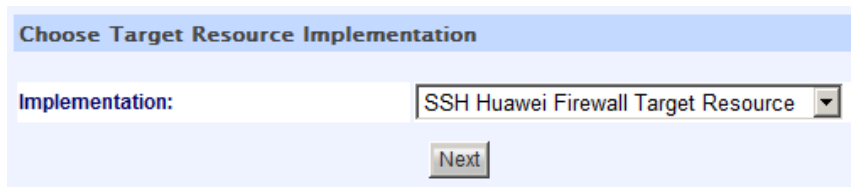
创建了要求的基于 Telnet 的 Huawei 防火墙目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

4.14 管理基于 SSH 的 Huawei 防火墙目标资源

4.14.1 创建基于 SSH 的 Huawei 防火墙目标资源

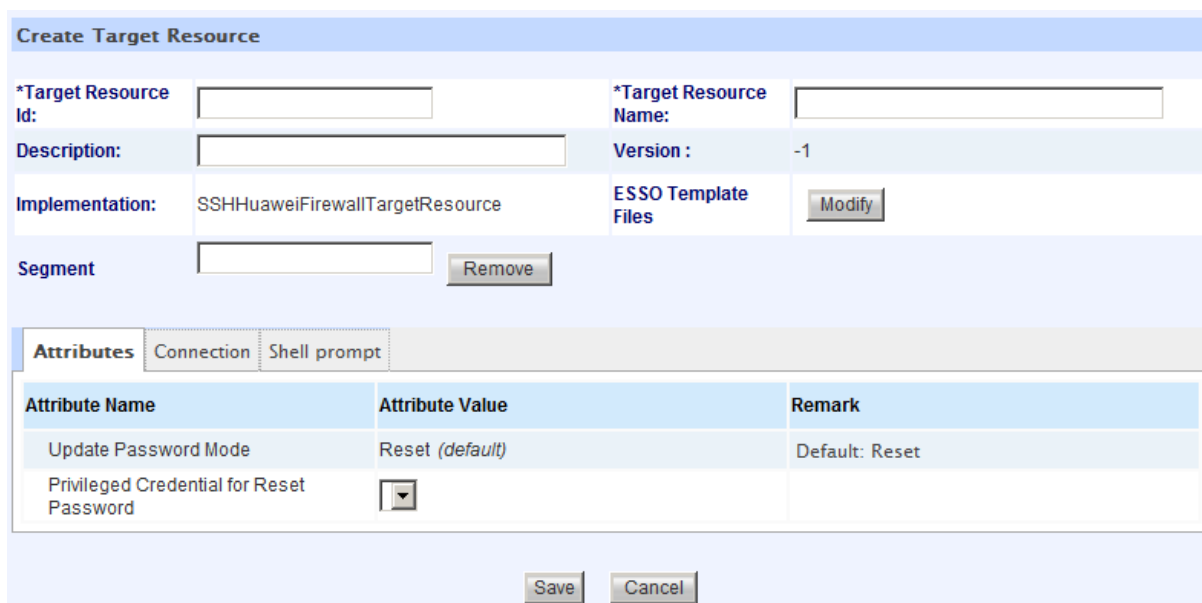
若要创建新的基于 SSH 的 Huawei 防火墙条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如 [图表 4-1](#) 所示。
3. 选择“SSH Huawei Firewall Target Resource”（SSH Huawei 防火墙目标资源）作为实施，然后按一下“Next”（下一步），如下所示：



图表 4-55: 选择基于 SSH 的 Huawei 防火墙目标资源实施

下方屏幕将会出现：



Attribute Name	Attribute Value	Remark
Update Password Mode	Reset (default)	Default: Reset
Privileged Credential for Reset Password	<input type="text"/>	

图表 4-56: 创建基于 SSH 的 Huawei 防火墙目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板

文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ 连接

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 22
Timeout (in seconds)	<input type="text"/>	Default: 5

图表 4-57: 创建基于 SSH 的 Huawei 防火墙目标资源 – 连接

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[Ll]ogin.*
Enter login password prompt	<input type="text"/>	Default: .*[Pp]assword.*
Shell prompt	<input type="text"/>	Default: >
Enter Superuser password prompt	<input type="text"/>	Default: .*[Pp]assword.*
Superuser Shell prompt	<input type="text"/>	Default:]
Succeed Login As Superuser message	<input type="text"/>	Default: .*[Pp]rivilege note.*
Update password		
System command	<input type="text"/>	Default: system
Succeed execute system message	<input type="text"/>	Default: .*[C c]trl.*
Reset password command	<input type="text"/>	Default: local-user \$userId password cipher \$newPassword
Save command	<input type="text"/>	Default: save
Exit command	<input type="text"/>	Default: quit

图表 4-58: 创建基于 SSH 的 Huawei 防火墙目标资源 – Shell 提示

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.14.2 查找和查看基于 SSH 的 Huawei 防火墙目标资源

若要查找和查看要求的基于 SSH 的 Huawei 防火墙目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

4.14.3 管理基于 SSH 的 Huawei 防火墙目标资源

创建了要求的基于 SSH 的 Huawei 防火墙目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

4.15 管理基于 Telnet 的 Huawei 切换目标资源

4.15.1 创建基于 Telnet 的 Huawei 切换目标资源

若要创建新的基于 Telnet 的 Huawei 切换条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如 [图表 4-1](#) 所示。
3. 选择“Telnet Huawei Switch Target Resource”（Telnet Huawei 切换目标资源）作为实施，然后按一下“Next”（下一步），如下所示：

The screenshot shows a dialog box titled "Choose Target Resource Implementation". It has a light blue header. Below the header, there is a label "Implementation:" followed by a dropdown menu that currently displays "Telnet Huawei Switch Target Resource". Below the dropdown menu is a "Next" button.

图表 4-59: 选择基于 Telnet 的 Huawei 切换目标资源实施

下方屏幕将会出现：

The screenshot shows the "Create Target Resource" form. It has a light blue header. The form contains several input fields and buttons:

- *Target Resource Id: [input field]
- *Target Resource Name: [input field]
- Description: [input field]
- Version: -1
- Implementation: TelnetHuaweiSwitchTargetResource
- ESSO Template Files: [input field] with a "Modify" button
- Segment: [input field] with a "Remove" button
- Attributes tab is selected, showing a table with columns: Attribute Name, Attribute Value, and Remark.

Attribute Name	Attribute Value	Remark
Update Password Mode	Reset (default)	Default: Reset
Privileged Credential for Reset Password	[dropdown menu]	

At the bottom of the form are "Save" and "Cancel" buttons.

图表 4-60: 创建基于 Telnet 的 Huawei 切换目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是属性标签，它包含目标资源的系统定义的属

性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ 连接

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 23
Timeout (in seconds)	<input type="text"/>	Default: 5

图表 4-61: 创建基于 Telnet 的 Huawei 切换目标资源 – 连接

■ Shell 提示

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[L l]ogin.*
Enter login password prompt	<input type="text"/>	Default: .*[P p]assword.*
Shell prompt	<input type="text"/>	Default: >
Enter Superuser password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser Shell prompt	<input type="text"/>	Default:]
Succeed Login As Superuser message	<input type="text"/>	Default: .*[P p]rivilege note.*
Update password		
System command	<input type="text"/>	Default: system
Succeed execute system message	<input type="text"/>	Default: .*[C c]trl.*
Pre-reset password command	<input type="text"/>	Default: local-user \$userid
Reset password command	<input type="text"/>	Default: password cipher \$newPassword
Save command	<input type="text"/>	Default: save
Write configuration prompt	<input type="text"/>	Default: .*[S s]ure.*
Write configuration command	<input type="text"/>	Default: y
Leave existing filename unchanged prompt	<input type="text"/>	Default: .*[U u]nchanged.*
Overwrite prompt	<input type="text"/>	Default: .*[O o]verwrite.*
Overwrite command	<input type="text"/>	Default: y
Succeed overwrite message	<input type="text"/>	Default: .*[V v]alidating.*
Exit command	<input type="text"/>	Default: quit

图表 4-62: 创建基于 Telnet 的 Huawei 切换目标资源 – Shell 提示

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.15.2 查找和查看基于 Telnet 的 Huawei 切换目标资源

若要查找和查看要求的基于 Telnet 的 Huawei 切换目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

4.15.3 管理基于 Telnet 的 Huawei 切换目标资源

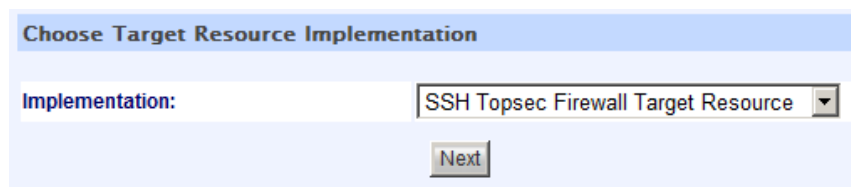
创建了要求的基于 Telnet 的 Huawei 切换目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

4.16 管理基于 SSH 的 Topsec 防火墙目标资源

4.16.1 创建基于 SSH 的 Topsec 防火墙目标资源

若要创建新的基于 SSH 的 Topsec 防火墙目标资源条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 PSM ->PSM Configuration（PSM 配置），如 [图表 4-1](#) 所示。
3. 选择“SSH Topsec Firewall Target Resource”（SSH Topsec 防火墙目标资源）作为实施，然后按一下“Next”（下一步），如下所示：



The screenshot shows a dialog box titled "Choose Target Resource Implementation". It contains a label "Implementation:" followed by a dropdown menu. The dropdown menu is currently set to "SSH Topsec Firewall Target Resource". Below the dropdown menu is a button labeled "Next".

图表 4-63: 选择基于 SSH 的 Topsec 防火墙目标资源实施

下方屏幕将会出现：

Create Target Resource

*Target Resource Id: *Target Resource Name:

Description: Version: -1

Implementation: SSHTopsecTargetResource ESSO Template Files

Segment

Attributes | Connection | Shell prompt

Attribute Name	Attribute Value	Remark
Update Password Mode	Reset (default)	Default: Reset
Privileged Credential for Reset Password	<input type="text"/>	

图表 4-64: 创建基于 SSH 的 Topsec 防火墙目标资源 – 属性

屏幕的上方部分包含一般属性，例如目标资源 ID、名称、描述、版本、实施、ESSO 模板文件和段栏位。

屏幕的下方部分包含数个标签。第一个标签是**属性**标签，它包含目标资源的系统定义的属性。

备注：

* 表示强制属性。

您可以参考 4.3.1 部分内容，来了解关于系统定义属性的更多说明。

请输入相应信息。

下方是其他标签的说明：

■ **连接**

此标签包含为目标资源存储的服务器连接信息的属性，如下所示：

Attributes | **Connection** | Shell prompt

Attribute Name	Attribute Value	Remark
*Host	<input type="text"/>	
Port	<input type="text"/>	Default: 22
Timeout (in seconds)	<input type="text"/>	Default: 5

图表 4-65: 创建基于 SSH 的 Topsec 防火墙目标资源 – 连接

■ **Shell 提示**

此标签包含映射属性值到实际 shell 提示的属性，和 shell 命令，如下所示：

Attributes Connection Shell prompt		
Attribute Name	Attribute Value	Remark
Login		
Enter login username prompt	<input type="text"/>	Default: .*[L l]ogin.*
Enter login password prompt	<input type="text"/>	Default: .*[P p]assword.*
Shell prompt	<input type="text"/>	Default: #
Enter Superuser password prompt	<input type="text"/>	Default: .*[P p]assword.*
Superuser Shell prompt	<input type="text"/>	Default: #
Update password		
System admininfo modify command	<input type="text"/>	Default: system admininfo modify
Reset password, enter username prompt	<input type="text"/>	Default: .*[i]nput manager's name.*
Modify name prompt	<input type="text"/>	Default: .*[M m]odify the name.*
Modify name command	<input type="text"/>	Default: n
Modify password command	<input type="text"/>	Default: y
Modify password prompt	<input type="text"/>	Default: .*[M m]odify the password.*
Enter password prompt (reset)	<input type="text"/>	Default: .*[P p]assword.*
Confirm new password prompt (reset)	<input type="text"/>	Default: .*[R r]e_enter.*
Modify privilege prompt	<input type="text"/>	Default: .*[M m]odify the privilege.*
Modify privilege command	<input type="text"/>	Default: n
Modify VSID prompt	<input type="text"/>	Default: .*[M m]odify the vsid.*
Modify VSID command	<input type="text"/>	Default: n
Modify comment prompt	<input type="text"/>	Default: .*[M m]odify the comment.*
Modify comment command	<input type="text"/>	Default: n
Reset password successful message	<input type="text"/>	Default: .*[S s]uccess.*

图 4-66: 创建基于 SSH 的 Topsec 防火墙目标资源 – Shell 提示

4. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

4.16.2 查找和查看基于 SSH 的 Topsec 防火墙目标资源

若要查找和查看要求的基于 SSH 的 Topsec 防火墙目标资源，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

4.16.3 管理基于 SSH 的 Topsec 防火墙目标资源

创建了要求的基于 SSH 的 Topsec 防火墙目标资源后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

4.17 为 SSO 整合启用 PSM 目标资源

PSM 目标资源可配置后，与 USO 整合以是使用相关凭证来提供单点登录（SSO）功能。然而，我们将不会在此为您详细描述这类 PSM 目标资源，而会在另外独立的用户指南中为您描述。

5 保险箱管理

此章节描述 PSM 保险箱的管理。

5.1 简介

在依照了之前章节来管理了要求的 PSM 目标资源后，管理员可以继续管理 PSM 保险箱。PSM 保险箱是一种容器，它包含特定信息，例如凭证密码策略和凭证备份文件密码，每个凭证可以加入到特定的保险箱以继承凭证密码策略。每个保险箱都有一个密码加密密钥，来保护所有它所包含的所有凭证。一个凭证仅能属于一个保险箱。

在成功设置 PSM 系统后，会有数个已经定义好的保险箱，管理员可以对其做出相应修改，然后投入使用。

备注：

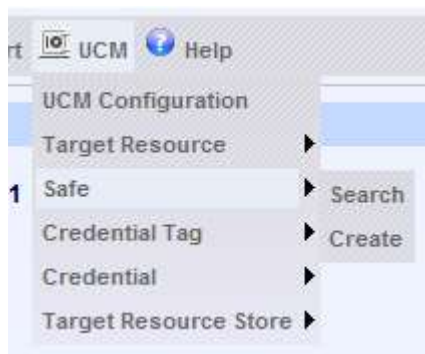
管理员可参考 [PSM 管理控制台通用管理指南：附录 A](#)，来了解关于要执行下方的管理任务，所需要的管理角色和管理权限的相关信息。

在管理了要求的保险箱后，管理员可以继续管理要求的凭证标签，将会在下方的章节为您具体描述相关内容。

5.2 创建 PSM 保险箱

若要创建新的 PSM 保险箱条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *PSM->Safe (保险箱) -> Create (创建)*，如下所示：



图表 5-1: 保险箱子菜单选项

下方屏幕将会出现：

Create Safe

*Safe Id:

*Safe Name:

Description:

Version: -1

Attributes

Attribute Name	Attribute Value	Remark
Password Policies		
Password Mask ?	<input type="text"/>	New password will be generated based on the specified password format and will be updated to the target resource upon checkin or manual reset Default: NN9NNNNNNN
Number of times clear password is displayed after checkout	<input type="text"/>	Default: 3 Value should be from 1 to 10
Password Expiry Days	<input type="text"/>	If the credential's password remains unchanged within the specified Password Expiry Days then password will be updated by the UCM Credential Updater background task. (0 means no expiry) Default: 60 Value should be from 0 to 365
Max. Checkout Duration(Hrs)	<input type="text"/>	Specifies the maximum checkout duration in hours for a credential before it is forced-checkin or changed to checkin overdue state by the Checkin Overdue Task Default: 24 Value should be from 1 to 2400
Disable Password Update On CheckIn	<input type="text" value="(default)"/>	Default: false
Key Management		
*Password Safe Key	<input type="text" value="-"/>	
Backup Management		
*Credential Backup File Password	<input type="text"/> <input type="button" value="Set Password"/>	Minimum password length is 8 characters
Last Backup File Generation Status	Required (default)	Applicable after PDF backup file password is changed Default: Required
Location of credential backup PDF file	<input type="text"/>	Specifies location of credential backup PDF file. Recommended to use a shared drive. Default: / \${ACMATRIX_HOME}/UCM/BackupFiles/ \${SAFE_ID}

Add Custom Attribute

图表 5-2: 创建保险箱

屏幕的上方部分包含一般属性，例如保险箱 ID、名称、描述和版本。

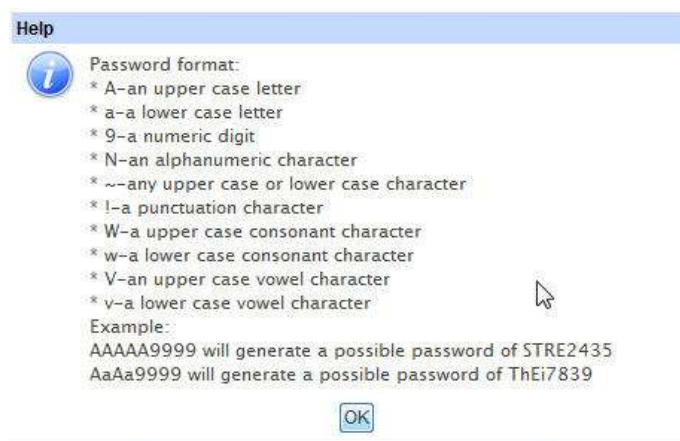
屏幕的下方部分包含**属性**标签，它包含系统定义和自定义（用户定义）的属性。系统定义的属性存储特定的信息，例如凭证策略信息等等。管理员可以增加、编辑或删除任何自定义属性。

备注：

* 表示强制属性。

❖ 密码遮罩

“密码遮罩”（ Password Mask）属性是用来决定，登录之后要制作的新密码格式，或者手动密码重设。预设是 NN9NNNNNNN。密码格式如下所示：



图表 5-3: 密码格式

❖ 密码显示的次数

“检出后显示纯文本密码的次数”（ Number of times clear password is displayed after checkout）属性是用来决定，每个凭证请求在 PSM 管理器中，凭证密码可以以纯文本形式显示的次数。预设值是 3。

❖ 密码过期天数

“密码过期天数”（ Password Expiry Days）属性是用来决定，若在指定期间内，且密码没有被更改，那么密码在多少天后将会过期。预设值是 60 天。若设为 0 则表示不会有过期。密码将会由 PSM 凭证更新器后台任务更新。

❖ 最长检出时间

“最长检出时间（小时）”（Max. Checkout Duration(Hrs)）属性是用于指定凭证的最长检出时间（单位是小时）。

❖ 在检入停用密码更新

“在检入停用密码更新”（Disable Password Update On CheckIn）属性，若设为 True，不管自动密码更新的值是什么，将不允许在检入后更新密码。预设值是 False。

❖ 密码保险箱密钥

“密码保险箱密钥”（ Password Safe Key）属性决定使用的加密密钥。

❖ 凭证备份文件密码

“凭证备份文件密码”（ Credential Backup File Password）属性决定凭证备份文件的密码。最少的密码长度是 8 个字符。

加密的凭证文件，将会以下方事件来创建或更新：

- Change of Credential Backup File Password（凭证备份文件密码的更改）
- Successful System Auto-Update of Credential Password（凭证密码的成功系统自动更新）
- Successful Creation of the Credential（凭证的成功创建）
- Manual Update of Credential Password（凭证密码的手动更新）

您可以参考附录 B：凭证备份文件内容样本，来查看配置备份文件的内容样本。

❖ 最新备份文件制作状态

“最新备份文件制作状态”（Last Backup File Generation Status）决定，PDF 备份文件制作的状态。预设值是要求（制作）。

❖ 凭证备份 PDF 文件的位置


“凭证备份 PDF 文件的位置”（Location of credential backup PDF file）属性指定凭证备份 PDF 文件的位置。建议使用共享的驱动。

3. 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

5.3 查找和查看 PSM 保险箱

若要查找和查看要求 PSM 保险箱，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

在查看要求的 PSM 保险箱信息的时候（如下方图表 5-4 所示），若适用，管理员可以按一下保险箱相关的密码保险箱密钥的超链接，来查看密码保险箱密钥，如下方图表 5-5 所示。

View Safe			
*Safe Id:	DEMO-SAFE	*Safe Name:	Demo Safe
Description:	Demonstration Safe	Version :	1
Attributes			
Attribute Name	Attribute Value	Remark	
Password Policies			
Password Mask 	NN9NNNNNNN (default)	New password will be generated based on the specified password format and will be updated to the target resource upon checkin or manual reset	
Number of times clear password is displayed after checkout	3 (default)		
Password Expiry Days	60 (default)	If the credential's password remains unchanged within the specified Password Expiry Days then password will be updated by the UCM Credential Updater background task. (0 means no expiry)	
Max. Checkout Duration(Hrs)	24 (default)	Specifies the maximum checkout duration in hours for a credential before it is forced-checkin or changed to checkin overdue state by the Checkin Overdue Task	
Disable Password Update On Checkin	false (default)		
Key Management			
Password Safe Key	PEK1		
Backup Management			
Credential Backup File Password	*****	Minimum password length is 8 characters	
Last Backup File Generation Status	Required (default)	Applicable after PDF backup file password is changed	
Location of credential backup PDF file	/ (default) \${ACMATRIX_HOME}/UCM/BackupFiles/ \${SAFE_ID}	Specifies location of credential backup PDF file. Recommended to use a shared drive.	
Custom Attributes			
Custom Attribute	Custom Value		

图表 5-4: 查看 PSM 保险箱

Password Safe Key (PEK1)

View Encryption Key

*Encryption Key Id: PEK1 *Encryption Key Name: PEK1

Description: PIN Encryption Key 1 Version: 1

Test KeyInfo

View KCV

Attributes Storage and Key Wrapping

Attribute Name	Attribute Value	Remark
Basic Key Attributes		
Purpose	PIN Encryption	
KeyProviderId	SystemKeyProvider	Default: SystemKeyProvider
JCE Provider		
JCE Provider	Default JCE Provider	Java Cryptography Extension Provider
Key Parameters		
Algorithm	AES	Default: AES
Key size	128	The version of JCE policy files that are bundled in the JDK 5.0 environment allow "strong" but limited, including key size limitations. For example, by default maximum key size for AES algorithm is 128 (SUN and IBM JRE). Default: 128
Mode	CFB	Default: CBC
Padding	PKCS5Padding	Default: PKCS5Padding
Initialization vector scheme	SHA1_IV	Default: SHA1_IV

View in main panel Close

图表 5-5: 查看 PSM 保险箱 – 密码保险箱密钥 (加解密钥)

管理员可以按一下“View in main panel”（在主面板查看），来在其主面板查看详细资料，或者“Close”（关闭）按钮来关闭对话框。

5.4 管理 PSM 保险箱

创建了要求 PSM 保险箱后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3 部分](#)所示），请参考该部分内容。

PSM 保险箱创建之后，就不能删除。

6 凭证标签管理

此章节描述 PSM 凭证标签的管理。

6.1 简介

在如之前章节所述，管理了要求的 PSM 保险箱后，管理员可以继续管理 PSM 凭证标签。

凭证标签可以，以“**Credential Tag -TypeValue**”（凭证标签-类型值）这种形式来，作为凭证的可辨识的方式：

- “凭证标签”指的是类别；
- “类型值”指的是，上述类别中的不同类型的一个或多个值。

这样的目标是，让管理员可以通过缩小他们的搜索条件范围，来快速找到要求的凭证。一个凭证可以属于多个凭证标签。

在成功设置 PSM 系统后，会有数个已经定义好的凭证标签，管理员可以对其做出相应修改，然后投入使用。

备注：

管理员可参考 [PSM 管理控制台通用管理指南：附录 A](#)，来了解关于要执行下方管理任务，所需要的管理角色和管理权限的相关信息。

管理了要求的凭证标签后，管理员可以继续管理要求的凭证，将会在下方的章节为您具体描述相关内容。

6.2 创建 PSM 凭证标签

若要创建新的 PSM 凭证标签条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *PSM->Credential Tag (凭证标签) -> Create (创建)*，如下所示：



图表 6-1: 凭证标签子菜单选项

下方屏幕将会出现：

图表 6-2: 创建凭证标签

屏幕的上方部分包含一般属性，例如凭证 ID、名称、描述和版本。

屏幕的下方部分包含**属性**标签，它包含系统定义的属性。

例如，若要分类凭证，方法是依照其平台（**by its platform**），例如 **Windows**、**Solaris** 等等，管理员可以创建一个凭证标签，它的“Category-TypeValue”设为“**ByPlatform-Windows**”、“**ByPlatform-Solaris**”等等。在这个例子中，“**Credential Id**”将被视为“类别”，应设为“**ByPlatform**”，而“**TypeValue**”应设为“**Windows**”、“**Solaris**”等等，如下所示：

图表 6-3: 创建凭证标签 – ByPlatform (依照平台)

备注：

* 表示强制属性。

请输入相应信息。

- 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

6.3 查找和查看 PSM 凭证标签

若要查找和查看要求的 PSM 凭证标签，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

6.4 管理 PSM 凭证标签

创建了要求的 PSM 凭证标签，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

备注：

凭证标签创建之后，仅允许管理员进行编辑，但是不允许其删除凭证标签。

7 凭证管理

此章节描述 PSM 凭证管理。

7.1 简介

PSM 凭证（又名用户凭证）存储机密信息，例如有特权的 ID 和密码，它们用于一般工作时间和非工作时间操作，以取用企业信息资源，例如数据库、关键服务器、网络设备等等。

PSM 提供下列凭证类型：

■ 凭证

这指的是以一般方式取用目标资源而使用到的凭证（又名普通凭证）。依照创建这种凭证时候所选的使用选项，用户可以交互检出这种凭证类型。

依照凭证的指定的使用情况选项，这类型的凭证也可以变成有特权的凭证；也就是，选项是以超级用户账号检出凭证（也就是，凭证带有共享的根账号），或启用以有超级用户账号特权。

■ 有重设密码特权的凭证

这是指被赋予为用户账号重设密码特权的凭证，用户账号可以是：基于 Windows 的用户账号，AD 域用户账号，基于 UNIX 的用户账号，或任何其他支持的目标资源用户账号。依照创建这种凭证时候所选的使用选项，用户可以交互检出这种凭证类型。

一般，这类型的有特权凭证是用于，当目标资源用户账号密码的密码更新模式，仅可以通过密码重设来完成。

请注意：

- 对于基于 Windows 的目标资源用户账号，有特权的凭证应拥有“管理者”权限；
- 对于基于 UNIX 的目标资源用户账号，有特权的凭证应拥有“root”权限；
- 对于基于 Cisco 的目标资源用户账号，有特权的凭证应拥有“15”权限

■ 超级用户账号

这指的是符合以下描述的凭证：包含账号信息，有“超级用户”或“root”权限，且可以执行根功能。依照创建这种凭证时候所选的使用选项，用户可以交互检出这种凭证类型。

请注意，目标资源的特定类型的超级用户账号，例如基于 Cisco 的目标资源，无法通过 PSM 管理器来交互检出，而仅能通过 XML-RPC API 呼叫完成。

同时，若超级用户账号受到直接登录到目标资源的限制，则凭证功能账号（包含功能 ID）可用于代表超级用户账号，在登录之前的动作中发挥作用。

■ 凭证功能账号

这指的是凭证包含有中信息，在超级用户账号在受到直接登录到目标资源的限制的时候，可将该信息用于桥或代理。此类有特权的凭证，用户无法交互检出。

■ 凭证网关账号

这是一种特别类型的目标资源相关的特别的凭证，这种目标资源是 RDP 目标资源（RDP，是 Remote Desktop Protocol 的缩写，远程桌面协议）。凭证是在访问 RDP 目标资源（也就是受限制的 Window 终端服务器）的时候作为网关账号使用的。仅会由系统自动分配仅一个凭证网关账号给请求者。此类型的凭证，用户无法交互检出。

成功设置 PSM 系统后，会有预先定义的凭证，管理员可对其做出相关修改后，投入使用。

PSM 凭证密码自动更新

PSM 提供密码更改功能给管理员，以便自动为某些类型的目标资源更新凭证信息，这些目标资源例如有基于 JDBC 的服务器、基于 UNIX 的服务器和活动目录服务器。这个功能包含有后台任务，您可以安排它由 AccessMatrix 服务器来运行。

PSM 凭证和预先要求

在创建任何 PSM 凭证之前，管理员必须先确定，已经事先创建了相关的 PSM 目标资源和保险箱。

例如，基于数据库服务器的目标资源，在数据库管理员为要求的数据库服务器创建了新的登录信息后，他/她会将这新创建的登录信息交给程序所有者。程序所有者会将下方信息提供给相关 PSM 安全管理员，以存放登录信息（作为初始凭证）到 AccessMatrix 安全注册表：

- Target ResourceName
- Target ResourceCredential User Id
- Target Resource Credential Password

7.2 管理凭证

7.2.1 创建凭证

若要创建新的凭证，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *PSM->Credential (凭证) -> Create (创建)*，如下所示：



图表 7-1: 凭证子菜单选项

3. 选择“Credential”作为类型，然后选择要求的保险箱和目标资源，如下所示：

Choose Credential Object Class	
Type:	Credential
Safe:	DEMO-SAFE
Target Resource:	DEMO-WINDOWS-TARGI
Next	

图表 7-2: 选择凭证物件类 – 凭证

备注：

选择要求的目标资源，按一下“...”按钮，然后查找要求的目标资源，如下所示：

Id	Name	Target Resource Type	Description
DEMO-WINDOWS-TARGET-RESOURCE	Demo Windows Target Resource	Windows Target Resource	Demonstration Windows Target Resources

图表 7-3: 查找要求的目标资源

选择要求的目标资源，然后按一下“OK”（确认）。

4. 根据提供的信息，填写下方相应栏位，如下所示：

图表 7-4: 创建凭证 – 基础

屏幕的上方部分包含一般属性，如下表所示：

属性	描述
Id	凭证 ID 您可以参考章节 3，凭证属性配置的部分的内容，来了解允许的字符设置。
描述	凭证的描述
类型	所选的凭证类型
状态	凭证的状态只能是激活或停用其中之一。 若停用，凭证就无法使用。

使用	配置的使用情况，即交互式或非交互式其中之一。 交互式表示，凭证可以被交互检出。而非交互式则表示，凭证不能通过 PSM 管理器界面来交互检出。 一旦创建凭证后，将无法更改任何值。
凭证状态	凭证的当前状态，例如可用于检出、等候重设等等。

表格 7-1: 凭证常见属性

备注:

* 表示强制属性。

屏幕的下方部分包含数个标签，如下所示:

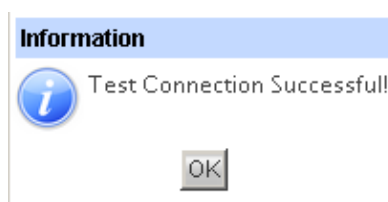
■ 基础 (Basic)

这是第一个标签，它包含凭证的登录信息，具体如下所示:

属性	描述
保险箱	所选的保险箱 ID。
目标资源	所选的目标资源 ID。
用户 ID	用来连接目标资源的用户 ID。
密码	与上述用户 ID 相关的密码
验证密码	重新输入上方指定的密码以验证。

表格 7-2: 基础属性

管理员可以验证登录信息，方法是按一下“Verify Login”（验证登录）按钮，如图表 7-4 所示。若验证成功，下方信息窗口将会出现:



图表 7-5: 验证登录 (测试连接) 成功

按一下“OK”（确认）来关闭信息窗口。

下方是其他标签的说明:

■ 安全策略

此标签包含凭证的安全策略设置，如下所示:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Required Approval Levels					
0					
Force Check-in					
<input checked="" type="radio"/> True <input type="radio"/> False					
Allow Concurrent Checkout					
<input checked="" type="radio"/> True <input type="radio"/> False					
Auto Password Update					
<input checked="" type="radio"/> True <input type="radio"/> False					

图表 7-6: 创建凭证 – 安全策略

下方表格为您提供对属性的详细描述:

属性	描述
要求的批准级别	<p>批准由请求者提出的凭证请求所要求的批准级别。</p> <p>最大的批准级别是 3 个级别。</p> <p>例如, 若值为 2, 则表示凭证需要得到 2 个级别的批准后, 才能使用。</p> <p>PSM 已经改善了, 凭证可设为 0 批准级别, 也就是无须批准。这样的话, 当用户提交请求以查看这类型凭证, 将会自动批准请求。</p> <p>备注:</p> <p>若在“Usage”(使用)栏位选择了“Non-Interactive”(非交互式), 此栏位将会不适用, 且会自动隐藏。</p>
强制检入	<p>此选项告诉系统, 是否在检出时间过期后, 自动强制凭证检入。</p> <p>备注:</p> <p>若在“Usage”(使用)栏位选择了“Non-Interactive”(非交互式), 此栏位将会不适用, 且会自动隐藏。</p>
允许并发检出	<p>此选项告诉系统是否允许凭证的多个检出。</p> <p>备注:</p> <p>若在“Usage”(使用)栏位选择了“Non-Interactive”(非交互式), 此栏位将会不适用, 且会自动隐藏。</p>
自动密码更新	<p>此选项告诉系统, 是否为凭证启用自动更新密码。</p>

表格 7-3: 安全策略属性

■ 最后操作状态

此标签包含凭证的最后操作状态的结果或信息, 如下所示:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Last Verify Login Result			-		
Last Verify Login Message			-		
Last Password Update Time			-		
Last Password Update Result			-		
Last Password Update Message			-		

图表 7-7: 创建凭证 – 上次操作状态

下方表格为您提供对属性的详细描述:

属性	描述
最后验证登录结果	系统执行的最后验证登录尝试的状态, 也就是成功或失败之一。
最后验证登录信息	系统执行的最后验证登录尝试的传回的信息。
最后密码更新时间	最后密码更新尝试的日期 / 时间。
最后密码更新结果	系统执行的最后密码更新尝试的状态, 也就是成功或失败之一。
最后密码更新信息	系统执行的最后密码更新尝试的传回的信息。

表格 7-4: 上次操作状态属性

■ 凭证标签

此标签包含凭证标签分配信息, 如下所示:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Credential Tag Id		Type Value			
ByEnvironment		SIT		Add	

图表 7-8: 创建凭证 – 凭证标签

下方表格为您提供对属性的详细描述:

属性	描述
凭证标签 ID	所选的凭证标签 ID
类型值	所选的凭证标签的类型值

表格 7-5: 凭证标签属性

■ 使用案例 Use Case

此标签包含目标资源连接的凭证使用案例选项列表, 如下所示:

若是 Windows / JDBC / AS400 / RDP 目标资源:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Restrict usage of this credential to this RDP target resource		Target Resource Store <input type="text"/> <input type="text"/>			

图表 7-9: 创建凭证 – 使用案例 : Windows/JDBC/AS400/RDP 目标资源

若是 UNIX 目标资源:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Option to checkout with this superuser credential		<input type="text"/>			
Restrict usage of this credential to this RDP target resource		Target Resource Store <input type="text"/> <input type="text"/>			

图表 7-10: 创建凭证 – 使用案例 : UNIX 目标资源

若是 Cisco 目标资源:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info
Option to checkout with this superuser credential		<input type="text"/>			
Superuser (Enable) account to change password		<input type="text"/>			
Restrict usage of this credential to this RDP target resource		Target Resource Store <input type="text"/> <input type="text"/>			

图表 7-11: 创建凭证 – 使用案例 : Cisco 目标资源

下方表格为您提供对属性的详细描述:

属性	描述
用此超级用户凭证检出的选项	指定所选目标资源的超级用户 ID 以共享根账号权限。 备注: 这是在 UNIX/Cisco 目标资源使用的。会在 PSM 管理器创建请求的时候, 显示 “Use superuser credential” (使用超级用户凭证) 复选框。
超级用户 (启用) 账号以更改密码	指定超级用户 ID, 就是启用账号 (用于更改 Cisco 凭证的密码)。
限制此凭证使用于此 RDP 目标资源	为凭证指定 RDP 目标资源 ID (内部/外部目标资源)。这表示将会使用某个凭证网关账号, 来作为连接凭证到目标服务器的网关。

表格 7-6: 使用案例属性

■ 使用信息

此标签包含关于凭证最后检出、最后批准和最后检入的详细信息, 如下所示:

Basic	Security Policy	Last Operation Status	Credential Tag	Use Case	Usage Info	
					Date/Time	User Id
					Last Checked Out	-
					Last Approved	-
					Last Checked In	-

图表 7-12: 创建凭证 – 使用信息

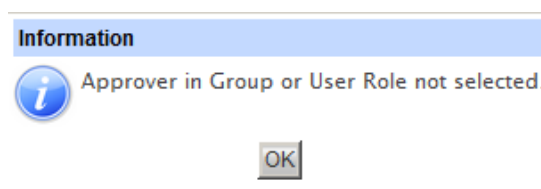
下方表格为您提供对使用信息属性的详细描述:

属性	描述
最后检出	这包含凭证的最后检出日期/时间, 和执行最后检出的请求者的用户 ID。
最后批准	这包含凭证的最后批准的日期/时间, 和最后批准检出请求的批准者的用户 ID。
最后检入	此包含凭证的最后检入日期/时间, 和执行最后检入的请求者的用户 ID。

表格 7-7: 使用信息属性

5. 按一下“Save”（保存）来保存更改, 或者“Cancel”（取消）来取消操作。

在保存操作成功后, 若凭证的“Usage”（使用）属性设为“Interactive Only”（仅交互式）, 和“Required Approval Levels”（要求的批准级别）设为非 0 值, 将会提示管理员, 为凭证指定要求的请求者和批准者（也就是工作流程角色）, 如下所示:



图表 7-13: 创建凭证 – 工作流程角色

按一下“OK”（确认）来关闭信息窗口。

关于为凭证管理工作流程角色的详细说明, 请参考下方的 7.2.4 部分内容。

7.2.2 查找和查看凭证

若要查找和查看要求凭证, 步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示）, 请参考该部分内容。

7.2.3 管理凭证

创建了要求的凭证, 管理员可以管理条目: 编辑或删除要求的条目, 而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示）, 请参考该部分内容。

备注:

在编辑凭证的时候，凭证的更改将会更新到 PSM 系统。若密码策略已经启用了自动更新功能，PSM 将会根据定义的密码策略，制作新的随机密码，并更新它到 AccessMatrix 和实际目标资源。

7.2.4 管理工作流程角色

为了管理工作流程角色，也就是凭证的请求者和批准者，请查找和查看要求的凭证，步骤如 7.2.2 部分所述，然后按一下“Manage Workflow Roles”（管理工作流程角色）按钮，如下所示：

The screenshot shows the 'View Credential' interface. It displays a table with the following data:

*Id	DEMO-CREDENTIAL	Description	Demo Credential
Type	Credential	Status	Activated
Usage	Interactive only	Credential State	Available for check-out

Below the table are several tabs: Basic, Security Policy, Last Operation Status, Credential Tag, Use Case, and Usage Info. The 'Basic' tab is selected, showing a table with the following data:

Safe	DEMO-SAFE
Target Resource	DEMO-WINDOWS-TARGET-RESOURCE
User Id	userid
Password	*****

At the bottom of the interface are four buttons: Edit, Manage Workflow Roles, Delete, and Back.

图表 7-14: 查看凭证 – 管理工作流程角色

下方屏幕将会出现：

The screenshot shows the 'Manage Workflow Roles' interface. It has two tabs: Requester and Approver. The 'Requester' tab is selected, showing a table with the following data:

User	Group
User Id	Action

Below the table are two buttons: Search and Add. At the bottom of the interface are two buttons: Save and Cancel.

图表 7-15: 查看凭证 – 管理工作流程角色（请求者和批准者）

通过用户级别分配请求者

在“Requester”（请求者）标签下，若要通过用户级别分配要求的请求者，按一下“User”（用户）子标签，然后按一下“Search”（搜索）来查找和选择要求的用户请求者，如下所示：

图表 7-16: 查看凭证 – 查找和选择用户

按一下“OK”（确认），然后按一下“Add”（增加）来增加所选的用户到列表，如下所示：

图表 7-17: 查看凭证 – 为请求者（用户级别）管理工作流程角色

若要移除所选的用户，请按一下“Remove”（移除）按钮，将不会提示删除确认，立即将用户从列表中移除。

通过群组级别分配请求者

在“Requester”（请求者）标签下，若要通过群组级别分配要求的请求者，按一下“Group”（群组）子标签，然后按一下“Search”（搜索）来查找和选择要求的群组请求者，如下所示：

图表 7-18: 查看凭证 – 查找和选择群组

按一下“OK”（确认），然后按一下“Add”（增加）来增加所选的群组到列表，如下所示：

Manage Workflow Roles	
Requester Approver	
User Group	
Group Id	Action
DEMO-GROUP	Remove
Search	Add
Save Cancel	

图表 7-19: 查看凭证 – 为请求者（群组级别）管理工作流程角色管理

若要移除所选的群组，请按一下“Remove”（移除）按钮，将不会提示删除确认，立即将群组从列表中移除。

通过用户级别分配批准者

在“Approver”（批准者）标签下，若要通过用户级别分配要求的批准者，按一下“User”（用户）子标签，然后按一下“Search”（搜索）来查找和选择要求的用户批准者，如图表 7-16 所示。

按一下“OK”（确认），然后为用户指定要求的批准级别，按一下“Add”（增加）来增加所选的用户到列表，如下所示：

Manage Workflow Roles		
Requester Approver		
User Group		
User Id	Approval Level	Action
DEMO-APPROVER-USER	1	Remove
Search	1	Add
Save Cancel		

图表 7-20: 查看凭证 – 为批准者（用户级别）管理工作流程角色管理

若要移除所选的用户，请按一下“Remove”（移除）按钮，将不会提示删除确认，立即将用户从列表中移除。

通过群组级别分配批准者

在“Approver”（批准者）标签下，若要通过群组级别分配要求的批准者，按一下“Group”（群组）子标签，然后按一下“Search”（搜索）来查找和选择要求的群组批准者，如图表 7-18 所示：

按一下“OK”（确认），然后为群组指定要求的批准级别，按一下“Add”（增加）来增加所选的群组到列表，如下所示：

Manage Workflow Roles		
Requester		Approver
User	Group	
Group Id	Approval Level	Action
DEMO-APPROVER-GROUP	1	Remove
Search	1	Add
Save		Cancel

图表 7-21: 查看凭证 – 为批准者（群组级别）管理工作流程角色管理

若要移除所选的群组，请按一下“Remove”（移除）按钮，将不会提示删除确认，立即将群组从列表中移除。

完成指定要求的请求者和批准者后，请按一下“Save”（保存）来保存更改。

7.3 管理有重设密码特权的凭证

7.3.1 创建有重设密码特权的凭证

若要创建新的有重设密码特权的凭证条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *PSM->Credential (凭证) -> Create (创建)*，如 [图表 7-1](#) 所示。
3. 选择“Privileged Credential For Reset Password”（有重设密码特权的凭证）作为类型，然后选择要求的保险箱和目标资源，接着按一下“Next”（下一步），如下所示：

Choose Credential Object Class	
Type:	Privileged Credential for Reset Password
Safe:	DEMO-SAFE
Target Resource:	DEMO-SSH-UNIX-TARGE
Next	

图表 7-22: 选择凭证物件类 – 有重设密码特权的凭证

备注：

您可以参考 7.2.1 部分，来了解如何选择要求的目标资源。

4. 请根据所提供的信息来填写所有对应的栏位，如下所示：

图表 7-23: 创建有重设密码特权的凭证 – 基础

屏幕的上方部分包含一般属性，例如凭证 ID、描述、类型、状态、使用和凭证状态栏位。

屏幕的下方部分包含数个标签。第一个标签是基础标签，它包含凭证的登录信息。您可以参考表格 7-1 和表格 7-2 来了解这些属性的详细说明。

备注：

* 表示强制属性。

管理员可以验证登录信息，方法是按一下“Verify Login”（验证登录）按钮，如图表 7-23 所示。若验证成功，信息窗口（如图表 7-5 所示）将会出现。

下方是其他标签的说明：

■ 安全策略

图表 7-24: 创建有重设密码特权的凭证以 – 安全策略

您可以参考表格 7-3 来了解属性的详细描述。

■ 最后操作状态

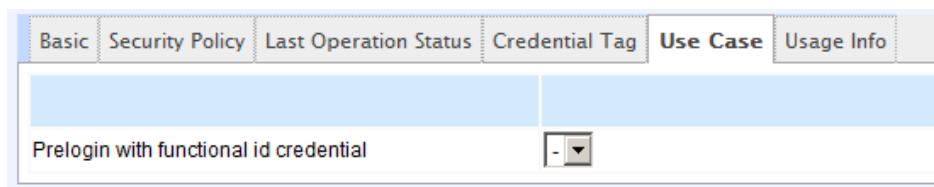
您可以参考图表 7-7 和表格 7-4 来了解属性的详细描述。

■ 凭证标签

您可以参考图表 7-8 和表格 7-5 来了解属性的详细描述。

■ 使用案例

此标签包含，目标资源连接的凭证的使用案例选项列表，如下所示：



图表 7-25: 创建凭证 – 使用案例

下方表格为您提供对使用信息属性的详细描述:

属性	描述
用功能 ID 凭证先登录	指定功能 ID 凭证，以用于登录到目标资源，尤其是若目标资源是 UNIX/Cisco 目标资源。 功能 ID 凭证，将会在 7.5 部分为您展开详细描述。

表格 7-8: 使用案例属性

■ 使用信息

您可以参考图表 7-12 和表格 7-7 来了解属性的详细描述。

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

7.3.2 查找和查看有重设密码特权的凭证

若要查找和查看要求的有重设密码特权的凭证条目，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2 部分](#)所示），请参考该部分内容。

7.3.3 管理有重设密码特权的凭证

创建了要求的有重设密码特权的凭证条目后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3 部分](#)所示），请参考该部分内容。

7.4 管理超级用户账号

7.4.1 创建超级用户账号

若要创建新的超级用户条目，请执行以下步骤：

- 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#)所述。
- 在主菜单，找到并点击 *PSM->Credential (凭证) -> Create (创建)*，如 [图表 7-1](#) 所示。
- 选择“Superuser Account”（超级用户账号）作为类型，选择要求的保险箱和目标资源，然后按一下“Next”（下一步），如下所示：

图表 7-26: 选择超级用户账号类型

备注:

您可以参考 7.2.1 部分，来了解如何选择要求的目标资源。

4. 请根据所提供的信息来填写所有对应的栏目，如下所示：

图表 7-27: 创建超级用户账号 – 基础

屏幕的上方部分包含一般属性，例如凭证 ID、描述、类型、状态、使用和凭证状态栏目。

屏幕的下方部分包含数个标签。第一个标签是基础标签，它包含凭证的登录信息。您可以参考表格 7-1 和表格 7-2 来了解这些属性的详细说明。

备注:

* 表示强制属性。

管理员可以验证登录信息，方法是按一下“Verify Login”（验证登录）按钮，如图表 7-27 所示。若验证成功，信息窗口（如图表 7-5 所示）将会出现。

下方是其他标签的说明：

■ **安全策略**

您可以参考表格 7-3 来了解属性的详细描述。

■ **最后操作状态**

您可以参考图表 7-7 和表格 7-4 来了解属性的详细描述。

■ 凭证标签

您可以参考图表 7-8 和表格 7-5 来了解属性的详细描述。

■ 使用案例

您可以参考图表 7-25 和表格 7-8 来了解属性的详细描述。

■ 使用信息

您可以参考图表 7-12 和表格 7-7 来了解属性的详细描述。

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

7.4.2 查找和查看超级用户账号

若要查找和查看要求的超级用户账号条目，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

7.4.3 管理超级用户账号

创建了要求的超级用户账号条目，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

7.5 管理凭证功能账号

7.5.1 创建凭证功能账号

若要创建新的凭证功能账号条目，请执行以下步骤：

- 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
- 在主菜单，找到并点击 *PSM->Credential (凭证) -> Create (创建)*，如图表 7-1 所示。
- 选择“Credential Functional Account”（凭证功能账号）作为类型，然后选择要求的保险箱和目标资源，接着按一下“Next”（下一步），如下所示：

Choose Credential Object Class	
Type:	Credential Functional Account
Safe:	DEMO-SAFE
Target Resource:	DEMO-SSH-UNIX-TARGE
Next	

图表 7-28: 选择凭证功能账号 – 类型

备注：

您可以参考 7.2.1 部分，来了解如何选择要求的目标资源。

- 请根据所提供的信息来填写所有对应的栏位，如下所示：

图表 7-29: 创建凭证功能账号 – 基础

屏幕的上方部分包含一般属性，例如凭证 ID、描述、类型、状态、使用和凭证状态栏位。

屏幕的下方部分包含数个标签。第一个标签是基础标签，它包含凭证的登录信息。您可以参考表格 7-1 和表格 7-2 来了解这些属性的详细说明。

备注：

* 表示强制属性。

此凭证类型仅适用于非交互式使用情况。

管理员可以验证登录信息，方法是按一下“Verify Login”（验证登录）按钮，如图表 7-29 所示。若验证成功，信息窗口（如图表 7-5 所示）将会出现。

下方是其他标签的说明：

■ **安全策略**

您可以参考表格 7-3 来了解属性的详细描述。

■ **最后操作状态**

您可以参考图表 7-7 和表格 7-4 来了解属性的详细描述。

■ **凭证标签**

您可以参考图表 7-8 和表格 7-5 来了解属性的详细描述。

■ **使用案例**

此标签包含，功能账号的使用案例选项，且仅适用于 Cisco 目标资源连接，如下所示：

图表 7-30: 创建凭证功能账号 – 使用案例

您可以参考表格 7-6 来了解属性的详细描述。

■ 使用信息

您可以参考图表 7-12 和表格 7-5 来了解属性的详细描述。

- 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

7.5.2 查找和查看凭证功能账号

若要查找和查看要求的凭证功能账号条目，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

7.5.3 管理凭证功能账号

创建了要求的凭证功能账号条目后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

7.6 管理凭证网关账号

7.6.1 创建凭证网关账号

若要创建新的凭证网关账号条目，请执行以下步骤：

- 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
- 在主菜单，找到并点击 *PSM->Credential (凭证) -> Create (创建)*，如图表 7-1 所示。
- 选择“Credential Gateway Account”（凭证网关账号）作为类型，然后选择要求的保险箱和目标资源，接着按一下“Next”（下一步），如下所示：

图表 7-31: 选择凭证网关账号

备注：

您可以参考 7.2.1 部分，来了解如何选择要求的目标资源。

如之前所述，仅 RDP 目标资源是适用于搜索此凭证类型。

- 请根据所提供的信息来填写所有对应的栏位，如下所示：

图表 7-32: 创建凭证网关账号 – 基础

屏幕的上方部分包含一般属性，例如凭证 ID、描述、类型、状态、使用和凭证状态栏位。

屏幕的下方部分包含数个标签。第一个标签是基础标签，它包含凭证的登录信息。您可以参考表格 7-1 和表格 7-2 来了解基础属性的详细说明。

备注：

* 表示强制属性。

此凭证类型仅适用于非交互式使用情况。

管理员可以验证登录信息，方法是按一下“Verify Login”（验证登录）按钮，如图表 7-23 所示。若验证成功，信息窗口（如图表 7-5 所示）将会出现。

下方是其他标签的说明：

■ **安全策略**

您可以参考表格 7-3 来了解属性的详细描述。

■ **最后操作状态**

您可以参考图表 7-7 和表格 7-4 来了解属性的详细描述。

■ **使用信息**

您可以参考图表 7-12 和表格 7-5 来了解属性的详细描述。

5. 按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

7.6.2 查找和查看凭证网关账号

若要查找和查看要求的凭证网关账号条目，步骤是类似搜索和查看要求的 Windows 目标资源（如 4.3.2 部分所示），请参考该部分内容。

7.6.3 管理凭证网关账号

创建了要求的凭证网关账号条目后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 4.3.3 部分所示），请参考该部分内容。

8 目标资源存储管理

此章节描述 PSM 目标资源存储的管理。

8.1 简介

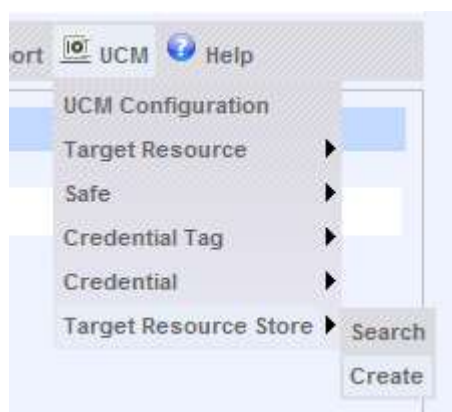
目标资源存储包含用户定义的目标资源列表。目标资源存储可以是内部的，即在 AccessMatrix 预设数据库内创建的，也可以是外部的，即指向外部数据库。

外部目标资源存储是通过预先定义的 SQL 视图（vw_target_resource，且假定它符合基于 JDBC 的用户存储的标准）来支持的。那么，在创建要求的目标资源存储之前，请事先创建好相关的基于 JDBC 的用户存储（它指向要求的数据库）。

8.2 创建目标资源存储

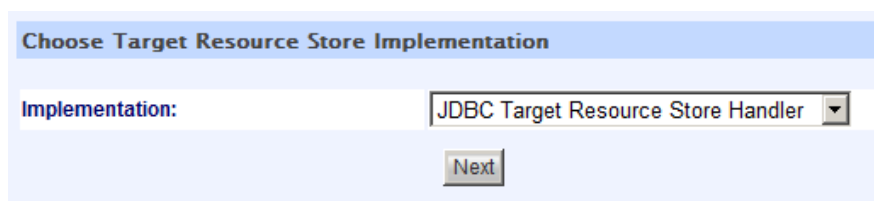
若要创建新的 PSM 目标资源存储条目，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#)所述。
2. 在主菜单，找到并点击 *PSM->Target Resource Store (目标资源存储) -> Create (创建)*，如下所示：



图表 8-1: 目标资源存储子菜单选项

下方屏幕将会出现：



图表 8-2: 选择目标资源存储实施

3. 选择要求的目标资源存储作为实施，然后按一下“Next”（下一步）按钮来继续。

备注：

目前，仅有一种实施类型可用，即“JDBC Target Resource Store Handler”（JDBC 目标资源存储处理器）

下方屏幕将会出现：

Create Target Resource Store

*Target Resource Store Id: <input style="width: 90%;" type="text"/>	*Target Resource Store Name: <input style="width: 90%;" type="text"/>
Description: <input style="width: 90%;" type="text"/>	Version : -1
Implementation: JdbcTargetResourceStoreHandler	

Attributes

Attribute Name	Attribute Value	Remark
*JDBC User Store	<input style="width: 90%;" type="text"/>	
Segment UUID Column	<input style="width: 90%;" type="text"/>	

Add Custom Attribute

图表 8-3: 创建目标资源存储

屏幕的上方部分包含一般属性，例如目标资源存储 ID、名称、描述和版本。

屏幕的下方部分包含**属性**标签，它包含系统定义的属性。

备注：

* 表示强制属性。

“JDBC 用户存储”属性可以设为要求的系统定义的基于 JDBC 的用户存储，即目标的基于 JDBC 的数据库的名称。

“Segment UUID Column”（段 UUID 列）属性，指的是“vw_target_resource”视图的“segment_id”列。此属性应映射到数据库中要求的目标资源存储表格的段 ID 列名称。

当且仅当指定了相应的“Segment UUID Column”属性值后，系统将为目标资源存储启用段支持。换句话说，可在段层面板中查看目标资源存储。

4. 完成编辑之后，您可以按一下“Save”（保存）来保存更改，或者“Cancel”（取消）来取消操作。

8.3 查找和查看目标资源存储

若要查找和查看要求的 PSM 目标资源存储，步骤是类似搜索和查看要求的 Windows 目标资源（如 [4.3.2](#) 部分所示），请参考该部分内容。

8.4 管理 PSM 目标资源存储

创建了要求的 PSM 目标资源存储后，管理员可以管理条目：编辑或删除要求的条目，而这些步骤是类似编辑和删除要求的 Windows 目标资源（如 [4.3.3](#) 部分所示），请参考该部分内容。

9 PSM 报告管理

此章节描述 PSM 制作的不同事件报告。

9.1 简介

PSM 记录所有 PSM 管理员和被授权用户所执行的的全部凭证管理和活动。您可以查看记录的或者审计的信息，方法是通过 PSM 制作的各种报告，这尤其适用于审计。若要查看报告（报告的格式可能是 HTML、PDF 或 CSV 格式），管理员或者被授权的用户必须拥有“Auditor”（审计员）管理角色。

PSM 提供四种基本类别的报告，即：

i. 一般事件

此报告提供所有 PSM 相关事件的摘要和信息。用户可以根据搜索条件（例如事件开始/结束日期和时间，事件类型等等）来查找事件信息。

ii. 凭证-用户

此报告提供关于以下的摘要和信息：分配到配置的用户或群组，分配到每个凭证的工作流程角色。

iii. 用户-凭证

此报告提供关于指定用户的摘要和凭证信息。

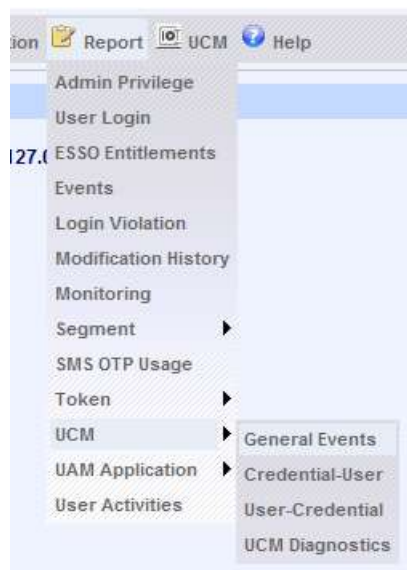
iv. PSM 诊断

此报告提供所有失败的登录验证和失败的更改密码尝试的摘要。通过此报告，管理员将会知道哪些凭证有问题，以及了解失败事件信息以便解决问题。

9.2 制作一般事件报告

若要制作一般事件报告，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 **Report (报告)** -> **PSM** -> **General Events (一般事件)**，如下所示：



图表 9-1: PSM 报告子菜单选项

下方屏幕将会出现:

The screenshot shows a web form titled "General Events Report". It contains the following fields and controls:

- Event Start Date:** A date and time selector showing 2012-06-25 00:00:00.
- Event End Date:** A date and time selector showing 2012-06-25 00:15:10.
- Credential Id:** An empty text input field.
- Event type:** A dropdown menu currently set to "All".
- Event Result:** A dropdown menu currently set to "All".
- Query Limit:** A text input field containing the number "1000".
- Generate:** A button to submit the report.
- Output Format:** A dropdown menu currently set to "HTML".

图表 9-2: 一般事件报告

3. 指定事件的开始日期和结束日期。
4. 若您想制作特定凭证 ID 的报告，请指定凭证 ID。
若您想要制作所有凭证的报告，请留空。
5. 您可以根据要求的事件类型和事件结果来过滤事件。

下图为您显示可用的事件类型列表:

- All
- Acknowledge
- ApproveRequest
- ChangePassword
- CheckInCredential
- CheckInCredentialRequest
- CheckinOverdue
- CheckinOverdueRequest
- CheckinOverdueTaskCompleted
- CheckinOverdueTaskStarted
- CheckOutCredential
- CheckOutCredentialRequest
- CreateRequest
- CredBackupPasswordChange
- CredPasswordExpired
- CredUpdaterCompleted
- CredUpdaterStarted
- CredVerifierCompleted
- CredVerifierStarted
- CsvImportTaskCompleted
- CsvImportTaskStarted
- DisplayPasswordCredential
- ImportCredentials
- ManualResetPassword
- PendingManualResetPassword
- RejectRequest
- SelfServiceApproveRequest
- VerifyPassword
- WithdrawRequest

图表 9-3: 一般事件 – 事件类型

您可以根据事件结果来过滤事件，可选结果为：Successful（成功的）、Failed（失败的）和 All（全部的，表示不过滤）。

- 依照预设，将会检索仅前 1000 个记录作为报告结果。
若要更改此值，请在“Query Limit”（查询限制）栏位指定您想要报告检索的记录数量。
- 指定要求的报告输出格式，然后按一下“Generate”（制作）按钮来制作报告。

备注：

若需 HTML 格式的一般事件报告范例，请查看，附录 C: 一般事件报告样本。

9.3 制作凭证-用户报告

若要制作制作凭证-用户报告，请执行以下步骤：

- 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
- 在主菜单，找到并点击 *Report (报告) -> PSM -> Credential-User (凭证-用户)*，如 [图表 9-1](#) 所示。
- 下方屏幕将会出现：

图表 9-4: 凭证-用户报告

- 若您想要制作特定的要求的凭证类型的报告，请指定“Credential Type”（凭证类型）。
- 若您想要制作特定的要求的凭证 ID 的报告，请指定“Credential Id”（凭证 ID）。
若您想要为所有凭证制作报告，请留空。
- 若您想要制作特定的要求的目标资源的报告，请指定“Target Resource”（目标资源）。
支持多个目标资源值（请用逗号隔开）。若您想要为所有目标资源制作报告，请留空。
- 指定“Credential Tag”（凭证标签）值。
支持多个凭证标签值（请在按住 Ctrl 键的时候，选择多个值）。若您想为所有的凭证标签制作报告，请选择“-”。
- 指定要求的报告输出格式，然后按一下“Generate”（制作）按钮来制作报告。

备注：

若需 PDF 格式的凭证-用户报告范例，请查看，附录 D: 凭证-用户报告样本。

9.4 制作用户-凭证报告

若要制作制作用户-凭证报告，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *Report (报告) -> PSM -> User-Credential (用户-凭证)* 如图表 9-1 所示。

下方屏幕将会出现：

The screenshot shows a web interface titled "User-Credential Report". It contains several form elements:

- User Store:** A dropdown menu with "DefaultStore" selected.
- User or Group:** A dropdown menu with "User" selected.
- User Id:** A text input field, currently empty, with a "Search" button to its right.
- Role:** A dropdown menu with "All" selected.
- Generate:** A button at the bottom left.
- HTML:** A dropdown menu at the bottom right, currently set to "HTML".

图表 9-5: 用户-凭证报告

3. 指定要求的“User Store”（用户存储）ID。
4. 指定“User”（用户）或“Group”（群组）级别之一。
若您想要为在所选的用户存储下的用户制作报告，请选择“User”（用户），否则请选择“User”（用户）。
5. 指定要求的用户 ID。
支持多个用户 ID 值（请用逗号隔开）。若您想要为所有的用户 ID 制作报告，请留空。
6. 指定用户角色来过滤，可选的角色有：All（全部）、Requester（请求者）或 Approver（批准者）。
All（全部）表示不过滤搜索结果。
7. 指定要求的报告输出格式，然后按一下“Generate”（制作）按钮来制作报告。

备注：

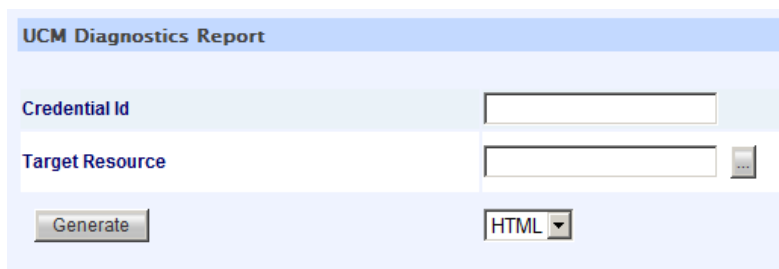
若需 PDF 格式的用户-凭证报告范例，请查看，附录 E: 用户-凭证报告样本。

9.5 制作 PSM 诊断报告

若要制作 PSM 诊断报告，请执行以下步骤：

1. 通过管理控制台登录到系统，如 [PSM 管理控制台通用管理指南](#) 所述。
2. 在主菜单，找到并点击 *Report (报告) -> PSM -> PSM Diagnostics (PSM 诊断)* 如图表 9-1 所示。

下方屏幕将会出现：



UCM Diagnostics Report

Credential Id

Target Resource ...

Generate HTML ▾

图表 9-6: PSM 诊断报告

3. 若您想要制作特定的要求的凭证 ID 的报告，请指定“Credential Id”（凭证 ID）。
支持多个凭证 ID 值（请用逗号隔开）。若您想要为所有的凭证制作诊断报告，请留空。
4. 若您想为特定的要求的目标资源制作报告，请指定“Target Resource”（目标资源）。
支持多个目标资源值（请用逗号隔开）。若您想要为所有的目标资源制作报告，请留空。
5. 指定要求的报告输出格式，然后按一下“Generate”（制作）按钮来制作报告。

备注：

若需 PDF 和 CSV 格式的 PSM 诊断报告范例，请查看，附录 F: PSM 诊断报告样本。