自助密码重置 1.1.x

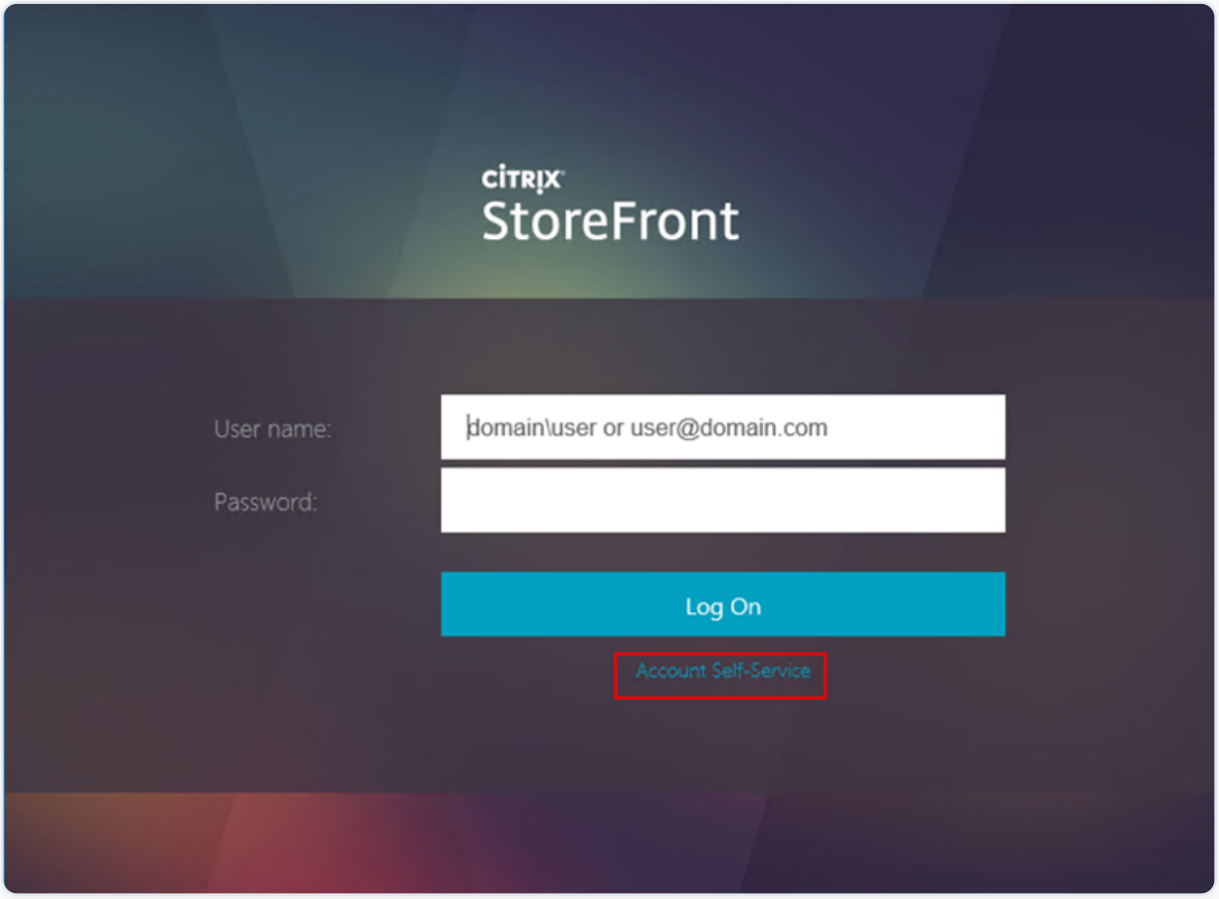
注意：

自助密码重置已弃用，在 Citrix Virtual Apps and Desktops™ 2006 及更高版本中不可用。

自助密码重置使用户能够更好地控制其用户帐户。配置自助密码重置后，如果最终用户在登录其系统时遇到问题，他们可以通过正确回答几个安全问题来解锁其帐户或将其密码重置为新密码。

提示：

在 StoreFront™ 的登录页面上可以看到**帐户自助服务**链接，供用户进行密码解锁和重置。



> 重置用户密码是一个固有的安全敏感过程。我们建议您参考安全配置文章，以确保您的部署配置正确。

新增功能

1.1.20 版新增功能

您可以配置允许连接到自助密码重置服务的 IP 地址。如果您不输入任何 IP 地址，则所有 IP 地址都将被列入白名单，即允许连接。

1.1.10 版新增功能

此版本解决了有助于提高整体性能和稳定性的一些问题。

1.1 版新增功能

此版本包含以下主要增强功能：

- 支持黑名单配置 - IT 管理员可以将用户和组添加到黑名单。黑名单中的用户和组无法使用任何自助密码重置功能。
- 支持简体中文 - 除了英语、法语、日语和西班牙语之外，现在还可以使用简体中文来定义安全问题。

自助密码重置包含三个组件：

- 自助密码重置配置控制台
- 自助密码重置服务
- StoreFront™ 中的安全问题注册

自助密码重置配置控制台

- **服务配置。** 配置自助密码重置服务，包括中央存储地址、数据代理帐户和自助密码重置帐户。
    - 中央存储地址：用于存储自助密码重置数据的网络共享位置。
    - 数据代理帐户：与中央存储通信。该帐户需要对中央存储的读写访问权限。
    - 自助密码重置帐户：用于解锁帐户和重置密码。
- **用户配置。** 配置哪些用户/组/OU 可以使用自助密码重置功能，并指定许可证服务器地址和默认服务地址。

  - 命名用户配置：定义自助密码服务的目标用户组，其中可以包括来自 Active Directory 的用户/组/OU。
  - 许可证服务器地址：您只能将自助密码重置与 Citrix Virtual Apps 或 Citrix Virtual Desktops Platinum 版本结合使用。最低许可证服务器版本必须为 11.13.1 或更高版本。
  - 选择或取消选择**解锁**和**重置**功能。
  - 默认服务地址：指定自助密码重置服务的 URL。

- **身份验证。** 配置用于注册以及解锁或重置密码的问卷。
  - 向问题存储中添加问题或组，问卷将从该存储生成。
  - 从问题存储中选择将用于注册的问题列表。
  - 导出/导入安全问题或组。

自助密码重置服务

自助密码重置服务在 Web 服务器上运行，允许用户重置其 Windows 密码并解锁其 Windows 帐户。最终用户的请求通过 StoreFront 发送到此服务。

StoreFront 中的安全问题注册

使用 StoreFront 允许用户注册其安全问题答案。注册后，他们可以重置域密码并解锁域帐户。有关详细信息，请参阅 配置身份验证服务 中的“自助密码重置安全问题”部分。

已修复的问题

版本 1.1.20

此版本没有修复任何问题。

版本 1.1.10

此版本已解决以下问题。

- 在 **自助密码重置** 服务器上禁用 TLS 1.0 后，将服务器 URL 添加到向导时可能会出现此错误消息：

  “无法访问您的服务器地址。” \[#LC7741\]

- 在域控制器上启用密码重置功能并应用任何自定义密码筛选器时，密码重置功能可能无法正常工作。将出现此错误消息：

  “提供的密码无效。” \[#LC7570\]

已知问题

版本 1.1.20

此版本中存在以下已知问题。

- 在用户配置向导中尝试添加用户组可能会失败，并显示一条消息，指出该用户组在黑名单中。此消息不正确。尝试失败是因为您已添加此组。

  \[#665520\]

- 在完成移除过程并关闭向导之前，您无法添加刚从配置向导中移除的用户和用户组。否则，将出现一条不正确的错误消息，指出用户或组在黑名单中。作为一种解决方法，请完成移除过程并关闭向导，然后重新打开向导以重新添加用户或组。

  \[#665352\]

- 如果在版本 1.0 控制台打开时将自助式密码重置升级到版本 1.1，则没有相应内容，并且版本 1.0 打开的控制台无法使用。

  \[#664390\]

- 在仅安装了 .Net Framework 4.5 的 Windows Server 2012 上尝试升级或卸载，以及在仅安装了 .Net Framework 4.6 的 Windows Server 2016 上尝试升级或卸载可能会失败。这些尝试失败的原因是，在 Windows Server 2012 和 Windows Server 2016 上进行就地升级或卸载依赖于 .Net Framework 3.5。作为一种解决方法，请在升级和卸载之前安装 .Net Framework 3.5。

  \[DNA-22761\]

版本 1.1.10

此版本中存在以下已知问题。

- 在用户配置向导中尝试添加用户组可能会失败，并显示一条消息，指出该用户组在黑名单中。此消息不正确。尝试失败是因为您已添加此组。

  \[#665520\]

- 在完成移除过程并关闭向导之前，您无法添加刚从配置向导中移除的用户和用户组。否则，将出现一条不正确的错误消息，指出用户或组在黑名单中。作为一种解决方法，请完成移除过程并关闭向导，然后重新打开向导以重新添加用户或组。

- 如果您在版本 1.0 控制台打开时将自助密码重置升级到版本 1.1，则没有相应的，并且版本 1.0 打开的控制台无法使用。

- 在仅安装了 .Net Framework 4.5 的 Windows Server 2012 上尝试升级或卸载，以及在仅安装了 .Net Framework 4.6 的 Windows Server 2016 上尝试升级或卸载可能会失败。这些尝试失败是因为在 Windows Server 2012 和 Windows Server 2016 上进行就地升级或卸载依赖于 .Net Framework 3.5。作为一种变通方法，请在升级和卸载之前安装 .Net Framework 3.5。

版本 1.1

此版本中存在以下已知问题。

- 在用户配置向导中尝试添加用户组可能会失败，并显示一条消息，指出该用户组在黑名单中。此消息不正确。尝试失败是因为您已添加此组。

- 在完成移除过程并关闭向导之前，您无法添加刚从配置向导中移除的用户和用户组。否则，会出现一条不正确的错误消息，指出用户或组在黑名单中。作为一种变通方法，请完成移除过程并关闭向导，然后重新打开向导以重新添加用户或组。

- 如果您在版本 1.0 控制台打开时将自助密码重置升级到版本 1.1，则没有相应的，并且版本 1.0 打开的控制台无法使用。

- 在仅安装了 .Net Framework 4.5 的 Windows Server 2012 上尝试升级或卸载，以及在仅安装了 .Net Framework 4.6 的 Windows Server 2016 上尝试升级或卸载可能会失败。这些尝试失败是因为在 Windows Server 2012 和 Windows Server 2016 上进行就地升级或卸载依赖于 .Net Framework 3.5。作为一种变通方法，请在升级和卸载之前安装 .Net Framework 3.5。

版本 1.0

此版本中存在以下已知问题。

- 打开自助密码重置控制台后，您可能无法将其固定到任务栏。

  \[#646300\]

  解决方法：通过**开始**菜单快捷方式将控制台固定到任务栏。

- 由于 Windows 2016 中的一个已知问题，您无法在 Windows 2016 中搜索自助密码重置控制台。

  \[#648939\]

  > 解决方法：使用**开始**菜单查找自助密码重置。

- 如果默认域策略中的密码策略中的最小密码使用期限为默认值（一天），并且您的用户尝试重置密码但重置失败（例如，他们不符合复杂性要求），并且他们关闭了密码重置向导，则他们无法在 24 小时内再次重置密码。

  \[#653221\]

- 当使用适用于 Mac 的 Citrix Workspace™ 应用程序时，用户首次登录 StoreFront 时会出现注册任务按钮。注销 StoreFront 后再次登录，任务按钮不会出现。

  \[#657263\]

解决方法： 1\. 单击 StoreFront 商店右上角的“用户名”。 2\. 单击下拉菜单中的“**刷新应用程序**”按钮。 3\. 关闭适用于 Mac 的 Citrix Workspace 应用程序，然后重新打开，任务按钮就会出现。

- 将安全问题从单点登录身份验证迁移到自助密码重置时，即使单击“**刷新**”后，问题也可能不会显示在自助密码重置控制台中。

  \[#657277\]

  > 解决方法：关闭控制台，然后重新打开。

- 问卷中包含特殊字符 **&** 的安全问题在 StoreFront 注册期间不显示。

  \[#654913\]

  > 解决方法：安全问题中不要包含 `**&**`。

- 在仅安装了 .Net Framework 4.5 的 Windows Server 2012 上尝试升级或卸载，以及在仅安装了 .Net Framework 4.6 的 Windows Server 2016 上尝试升级或卸载可能会失败。这些尝试失败的原因是，在 Windows Server 2012 和 Windows Server 2016 上进行就地升级或卸载依赖于 .Net Framework 3.5。解决方法是，在升级和卸载之前安装 .Net Framework 3.5。

  \[DNA-22761\]

系统要求

> **重要**
>
> Citrix® 不支持在域控制器上安装任何自助密码重置组件。请将自助密码重置组件部署在专用服务器上。

本文介绍了自助密码重置环境的硬件和软件要求。本文假设每台计算机都满足所安装操作系统的最低硬件要求。

软件

您的自助密码重置环境中的计算机可能需要以下支持系统软件。

- **Windows 2016 和 Windows 2012 R2** - 自助密码重置服务器所需。
- **Microsoft Windows Installer 2.0 或更高版本** - 所有组件均需要。
- **Microsoft .NET Framework** - 自助密码重置服务器所需。
  - 4.6.x（Windows 操作系统 2016）
  - 4.5.2（Windows 操作系统 2012 R2）
- **Internet Information Services (IIS)** - 自助密码重置服务器所需。
  - IIS 10.0 (适用于 Windows 2016)
  - IIS 8.5 (适用于 Windows 2012 R2)
- **VC++ 2008 SP1 运行时** - 自助密码重置服务器所需。

  首次安装时，您必须从 `<https://www.microsoft.com/zh-cn/download/details.aspx?id=26368>` 下载 vcredist_x86.exe，并将其安装在自助密码重置服务器上。

自助密码重置服务器

- 自助密码重置组件 - 中央存储

- 支持的环境 - SMB 文件共享
- 硬件要求 - 每用户 30 KB 磁盘空间

ASP.NET 3.5/4.X 要求

适用于 Windows Server 计算机上 .NET Framework 版本的 ASP.NET 组件。

安全和帐户要求

在安装自助密码重置服务之前，请确保有适当的帐户和组件来支持该服务。此外，由于该服务使用安全 HTTP (HTTPS)，因此它需要服务器身份验证证书才能与 StoreFront 进行传输层安全性 (TLS) 通信。

服务器身份验证要求：

在安装服务之前，请从证书颁发机构 (CA) 或内部公钥基础结构 (PKI)（如果可用）获取用于 TLS 通信的服务器身份验证证书。

服务模块所需的帐户：

注意： 确保这两个帐户都不会过期。

自助密码重置服务需要以下帐户类型才能在您的环境中运行时读取和写入数据：

- 数据代理帐户
- 自助服务帐户

当不同模块需要相同类型的帐户时，您可以将同一帐户用于多个模块。或者，您可以为每个模块指定不同的自定义帐户。

- **数据代理帐户**

需要对中央存储的读写访问权限。有关详细信息，请参阅 安装和配置 中的“**创建中央存储**”部分。

- **自助账户**

需要足够的权限以解锁和重置用户配置中相关用户的密码。有关详细信息，请参阅安全配置。

StoreFront

- StoreFront 3.7 到 1912

Citrix Workspace™ 应用程序

支持：

- 适用于 Web 的 Citrix Workspace 应用程序
- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序（需要 StoreFront 3.8）

不支持：

- 适用于 Chrome 的 Citrix Workspace 应用程序
- 移动设备（即使使用 Citrix Workspace app Web 版也不支持）

通过 Citrix Gateway 外部使用

不支持

安装和配置

安装清单

在开始安装之前，请完成此清单：

✓	步骤
	选择环境中将安装软件的计算机，并为安装做好准备。请参阅系统要求。
	安装 TLS 证书以及服务所需的帐户。请参阅系统要求中的**安全和帐户要求**。
	安装或将许可证服务器升级到最低版本 11.13.1.2。从 `<https://www.citrix.com/downloads/licensing.html>` 下载许可证服务器。有关详细信息，请参阅许可证服务器文档。

安装和配置顺序

Citrix® 建议您按以下顺序安装 Self-Service Password Reset：

1. 创建中央存储。请参阅创建中央存储。
2. 安装 Self-Service Password Reset。要安装服务并运行服务配置向导，您的登录帐户必须是域用户，并且属于服务器上的本地管理员组。有关详细信息，请参阅安装和配置 Self-Service Password Reset。
3. 使用控制台配置 Self-Service Password Reset。请参阅安装和配置 Self-Service Password Reset。
4. 在 StoreFront 上配置 Self-Service Password Reset。请参阅配置 StoreFront。
5. 确保您的 Self-Service Password Reset 配置已安全配置。请参阅安全配置。

创建中央存储

出于安全原因，我们建议您直接在运行 Self-Password Reset 服务的计算机上创建中央存储。对于需要多个 Self-Password Reset 服务器的部署，如果 Self-Service Password Reset 服务器和托管共享的服务器都支持 SMB 加密，则可以将中央存储托管在远程网络共享上。

此功能仅在 Windows Server 2012 R2 或 Windows Server 2016 上可用。

创建数据代理帐户

创建一个普通域用户作为数据代理帐户。请勿将域管理员/本地管理员组中的用户设置为数据代理帐户。

为 Windows Server 2012 R2 或 Windows Server 2016 创建中央存储

当同时将 Windows Server 2012 R2 或 Windows Server 2016 用于自助密码重置服务器和中央存储时，如果按照本节所述进行配置，则可以使用远程网络共享。确保选中“**加密数据访问**”并应用 (/zh-cn/self-service-password-reset/current-release/secure.html) 中提供的指导。

1. 要启动“**新建共享**”向导，请打开服务器管理器。在“**文件和存储服务**”详细信息页面中，在左侧窗格中选择“**共享**”，然后单击“**任务 \> 新建共享**”。

   新建共享的图像 (/en-us/self-service-password-reset/current-release/media/new-share.png)
2. 在左侧窗格中选择“**选择配置文件**”，选择“**SMB 共享 - 快速**”，然后单击“**下一步**”。

   选择配置文件的图像 (/en-us/self-service-password-reset/current-release/media/select-profile.png)
3. 在左侧窗格中选择“**共享位置**”。从列表中，选择要在其上创建新共享的服务器以及要在其上创建新共享文件夹的卷，然后单击“**下一步**”。

   共享位置的图像 (/en-us/self-service-password-reset/current-release/media/share-location.png)
4. 在左侧窗格中选择“**共享名称**”，键入新共享的名称，例如 **CITRIXSYNC$**，然后单击“**下一步**”。

   共享名称的图像 (/en-us/self-service-password-reset/current-release/media/share-name.png)
5. 在左侧窗格中选择“**其他设置**”，选择“**加密数据**”，取消选择“**允许共享缓存**”，然后单击“**下一步**”。

   其他设置的图像 (/en-us/self-service-password-reset/current-release/media/other-settings.png)
6. 要自定义**共享**权限，请在左窗格中选择**权限**，然后选择**自定义权限 \> 共享**。

   自定义权限的图像(/en-us/self-service-password-reset/current-release/media/customize-permissions.png)
7. 要自定义 NTFS 权限，请单击**禁用继承**，然后选择**将继承的权限转换为此对象上的显式权限**。

禁用继承的图像(/en-us/self-service-password-reset/current-release/media/inheritance.png)

8. 单击**权限**选项卡，删除除 **CREATOR OWNER**、**Local Administrators** 和 **SYSTEM** 之外的所有用户，然后添加具有完全控制权限的数据代理帐户。

   删除用户的图像(/en-us/self-service-password-reset/current-release/media/remove-users.png)

9. 选择 **CREATOR OWNER**，然后单击**编辑**以取消选中以下权限：

   - 完全控制
   - 删除子文件夹和文件
   - 更改权限
   - 取得所有权

   高级权限的图像(/en-us/self-service-password-reset/current-release/media/permissions-citrixsync.png)

10. 选择**共享**选项卡，删除**所有人**，然后添加具有完全控制权限的数据代理帐户、本地管理员和域管理员。

    共享权限的图像(/en-us/self-service-password-reset/current-release/media/share-permissions.png)

11. 在新共享向导的左窗格中选择**确认**，查看当前选定的共享设置，然后单击**创建**以开始创建新文件夹，然后单击**关闭**。

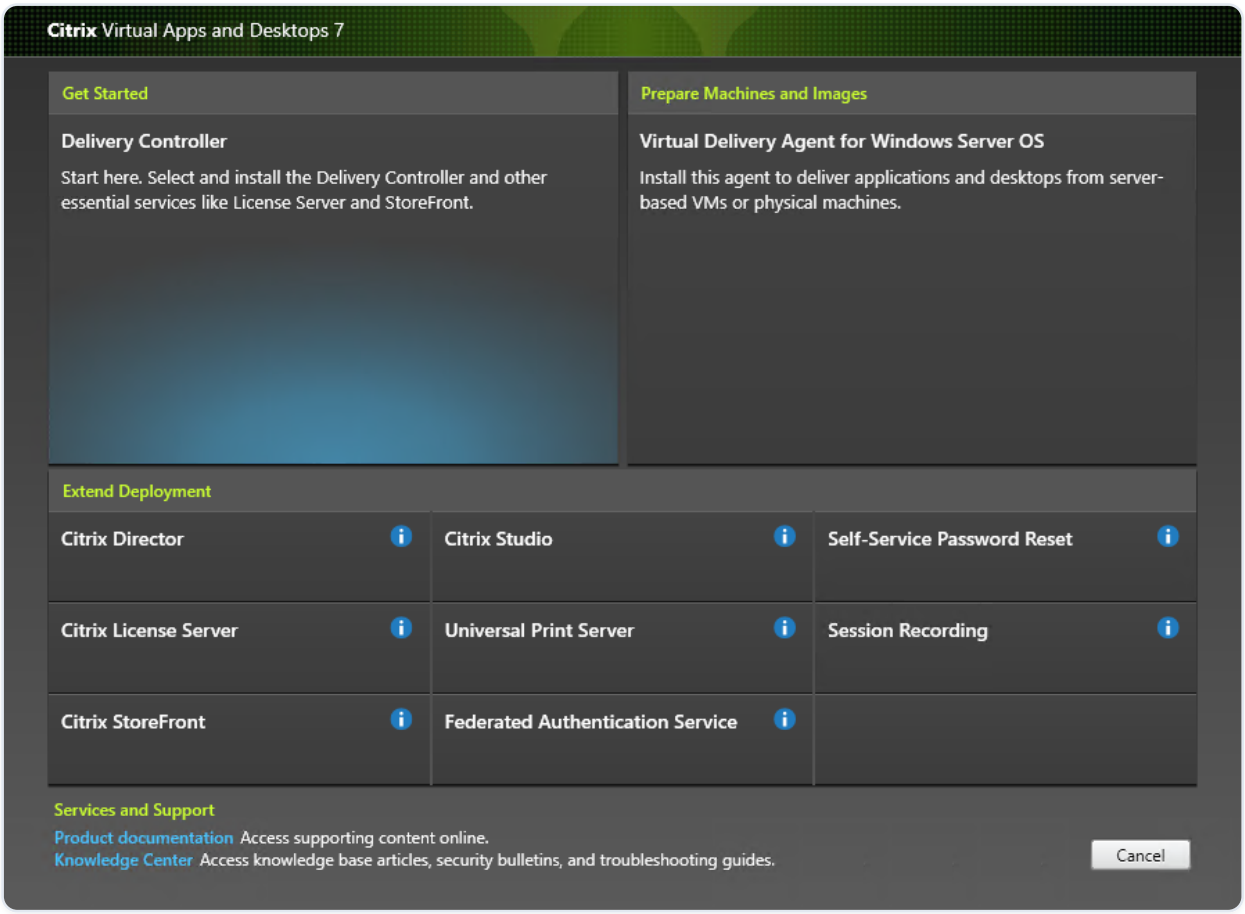
12. 在 **CITRIXSYNC$** 共享文件夹下创建两个子文件夹：**CentralStoreRoot** 和 **People**。

重要提示：确保数据代理帐户对这两个子文件夹具有**完全控制**权限。

您必须为自助密码重置中心存储配置 EncryptData、RejectUnencryptedAccess 和 RequireSecuritySignature。有关更多配置信息，请参阅以下 Microsoft 文章：`<https://docs.microsoft.com/zh-cn/powershell/module/smbshare/set-smbserverconfiguration>` `<https://docs.microsoft.com/zh-cn/powershell/module/smbshare/set-smbshare>`

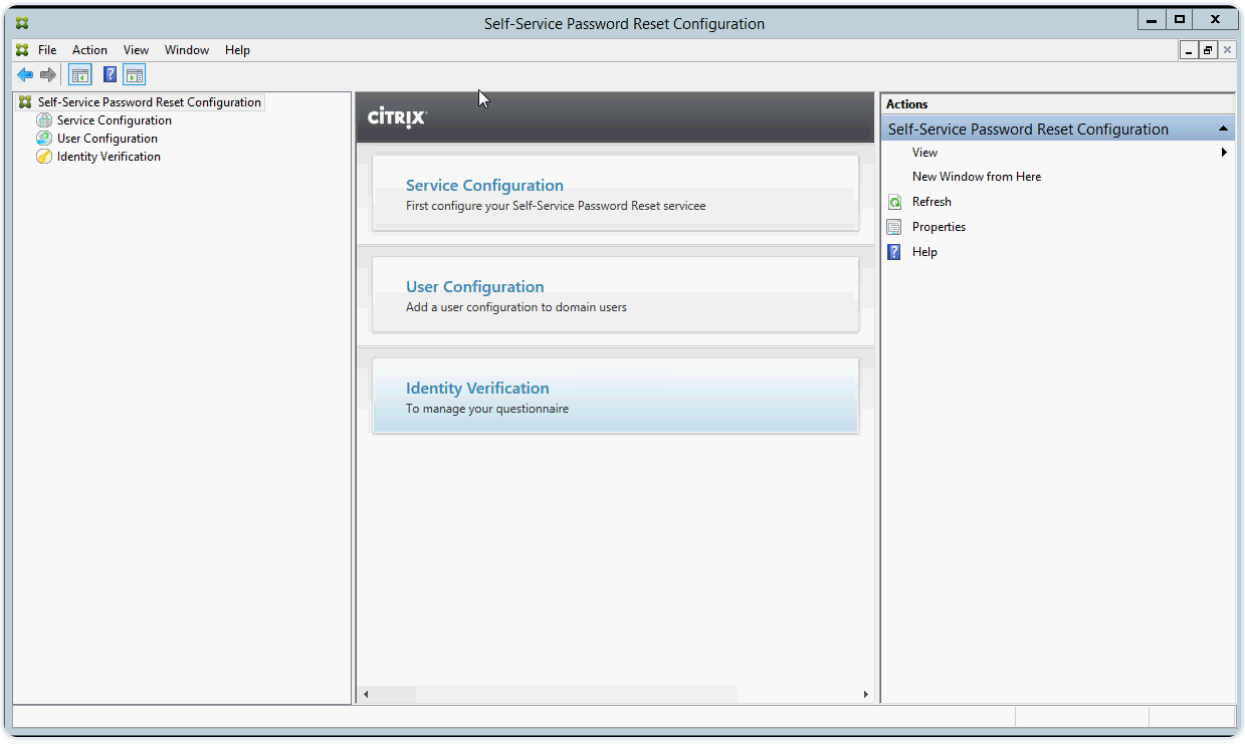
安装和配置自助密码重置

1. 使用 Citrix Virtual Apps and Desktops™ 安装程序安装自助密码重置。



2. 安装自助密码重置后，单击**开始 \> 所有程序 \> Citrix \> Citrix Self-Service Password Reset Configuration** 以配置 Citrix 自助密码重置服务。

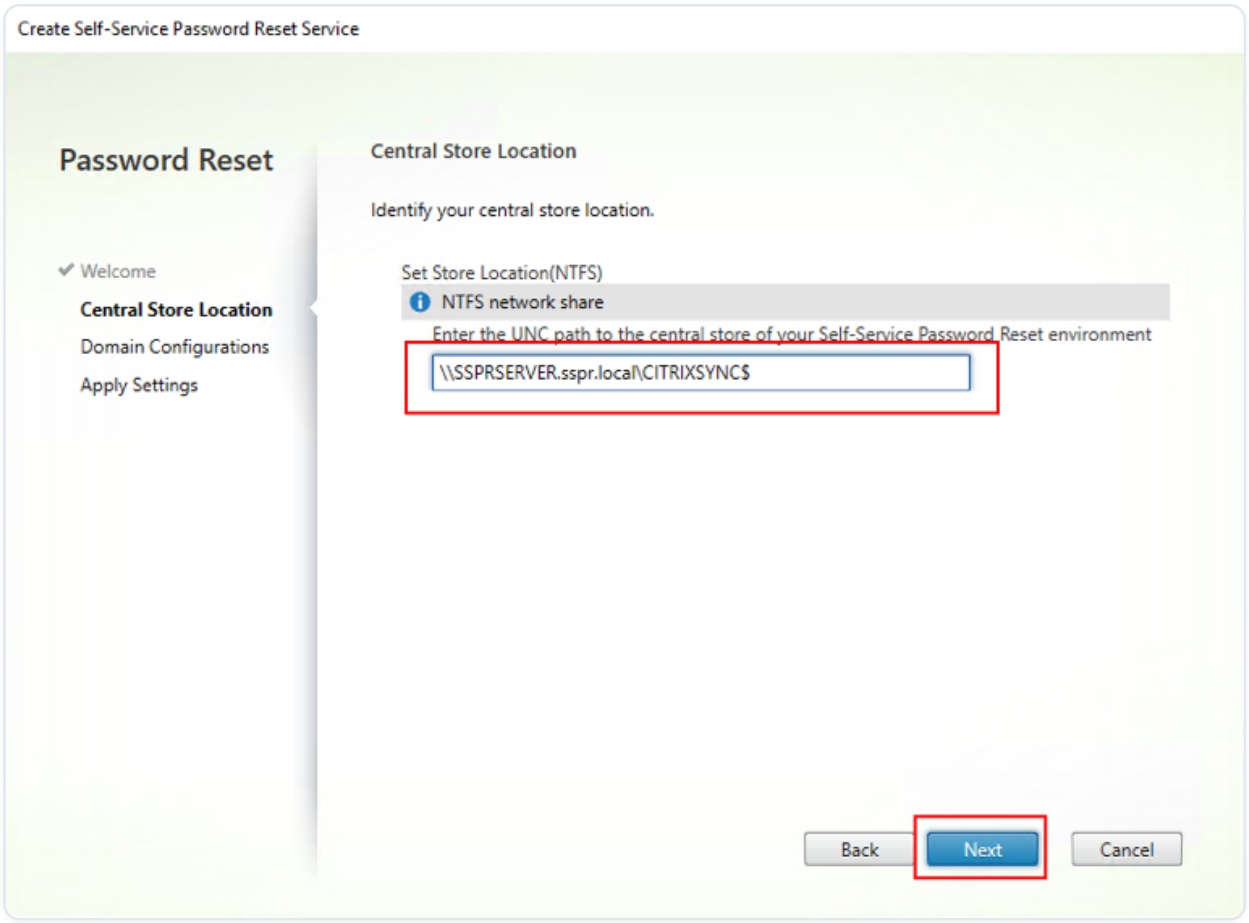
3. 控制台打开后，请按照以下三个基本步骤配置服务。



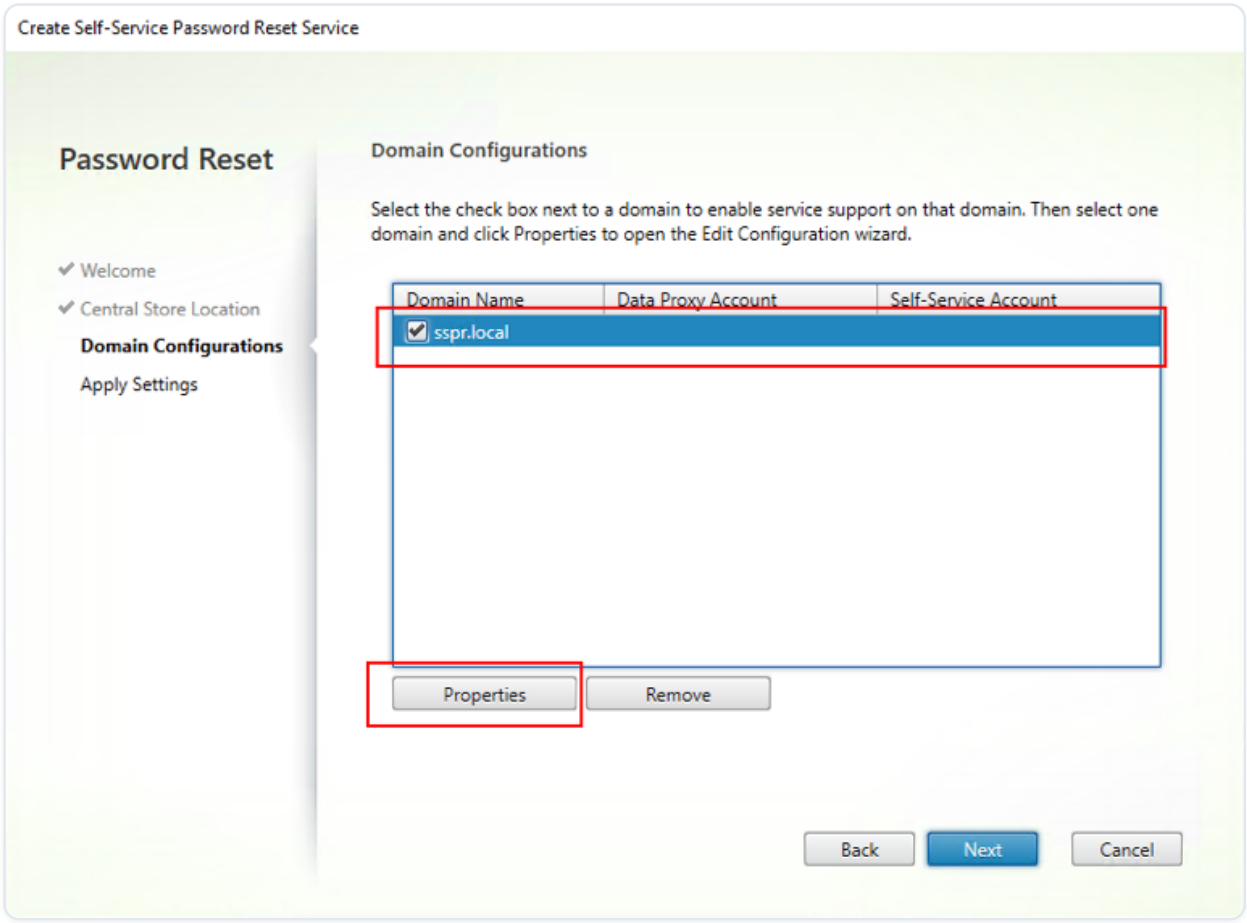
服务配置

在配置服务之前，请确保已创建中心存储、数据代理帐户和自助服务帐户。

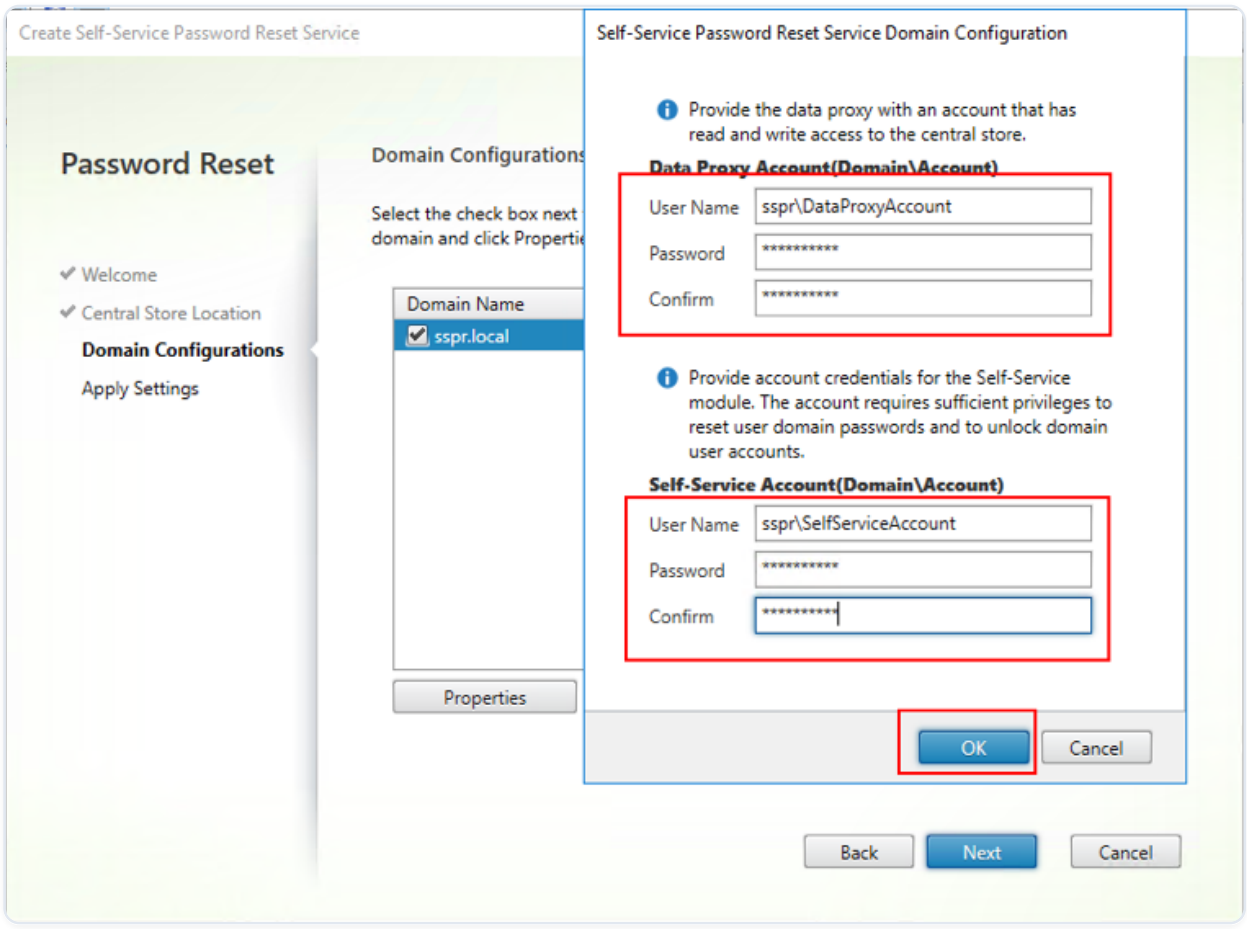
1. 在中间窗格中选择**服务配置**，然后单击右侧窗格中的**新建服务配置**。
2. 在**中心存储位置**屏幕上，指定中心存储位置，然后单击**下一步**。



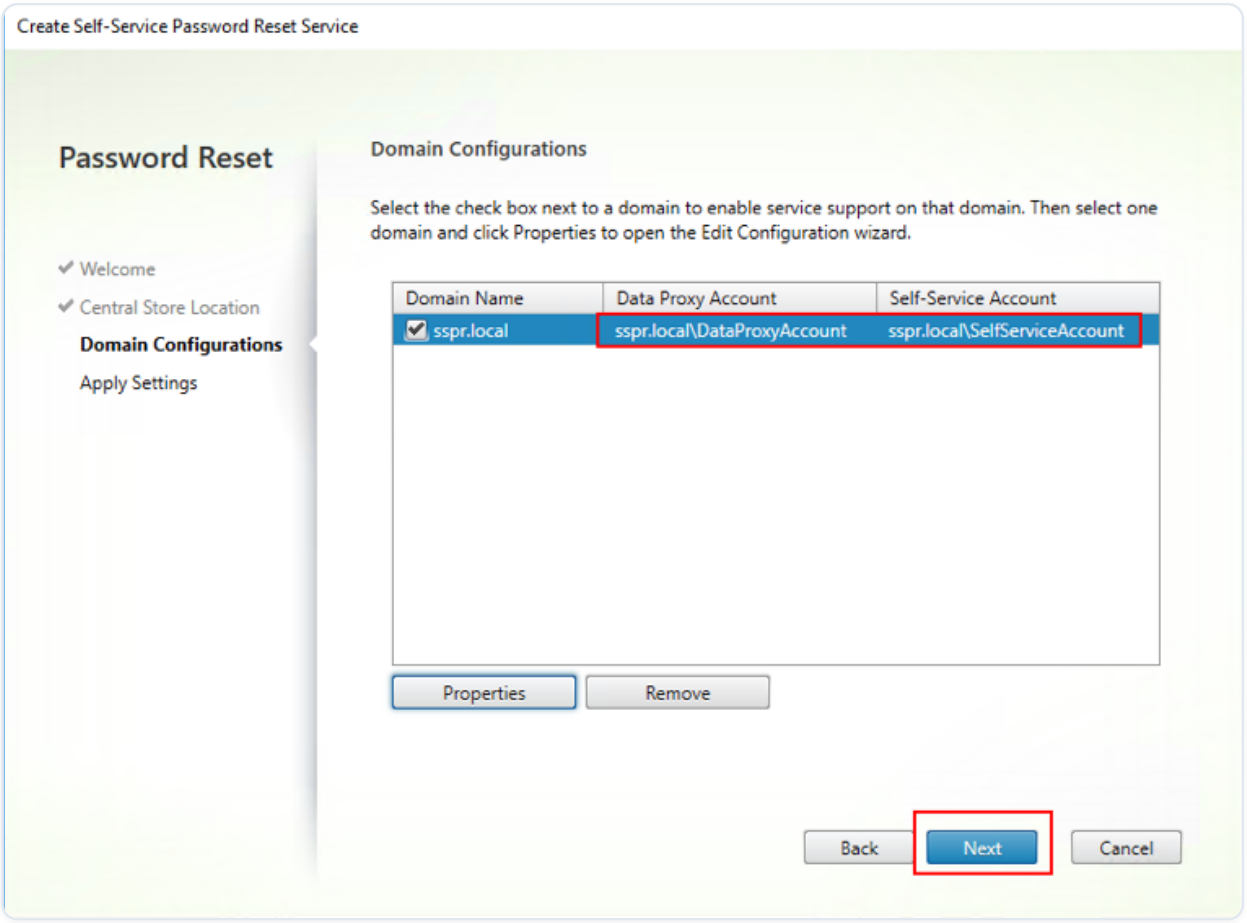
3. 在**域配置**屏幕上，选择要启用自助密码重置服务的域，然后单击**属性**。



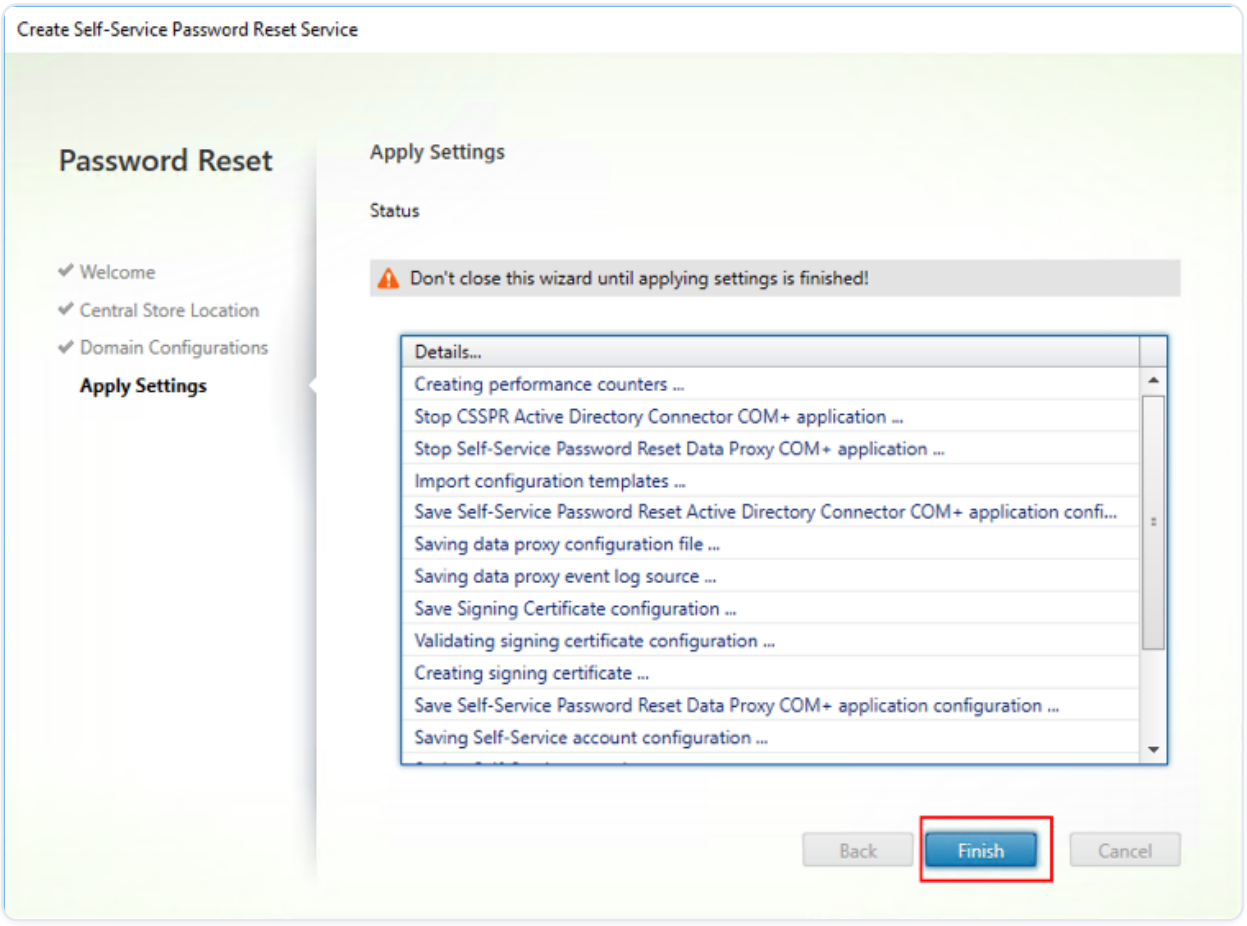
4. 指定 **数据代理账户** 用户名和密码以及 **自助服务账户** 用户名和密码，然后单击 **确定**。



5. 单击 **下一步** 以应用所有设置。

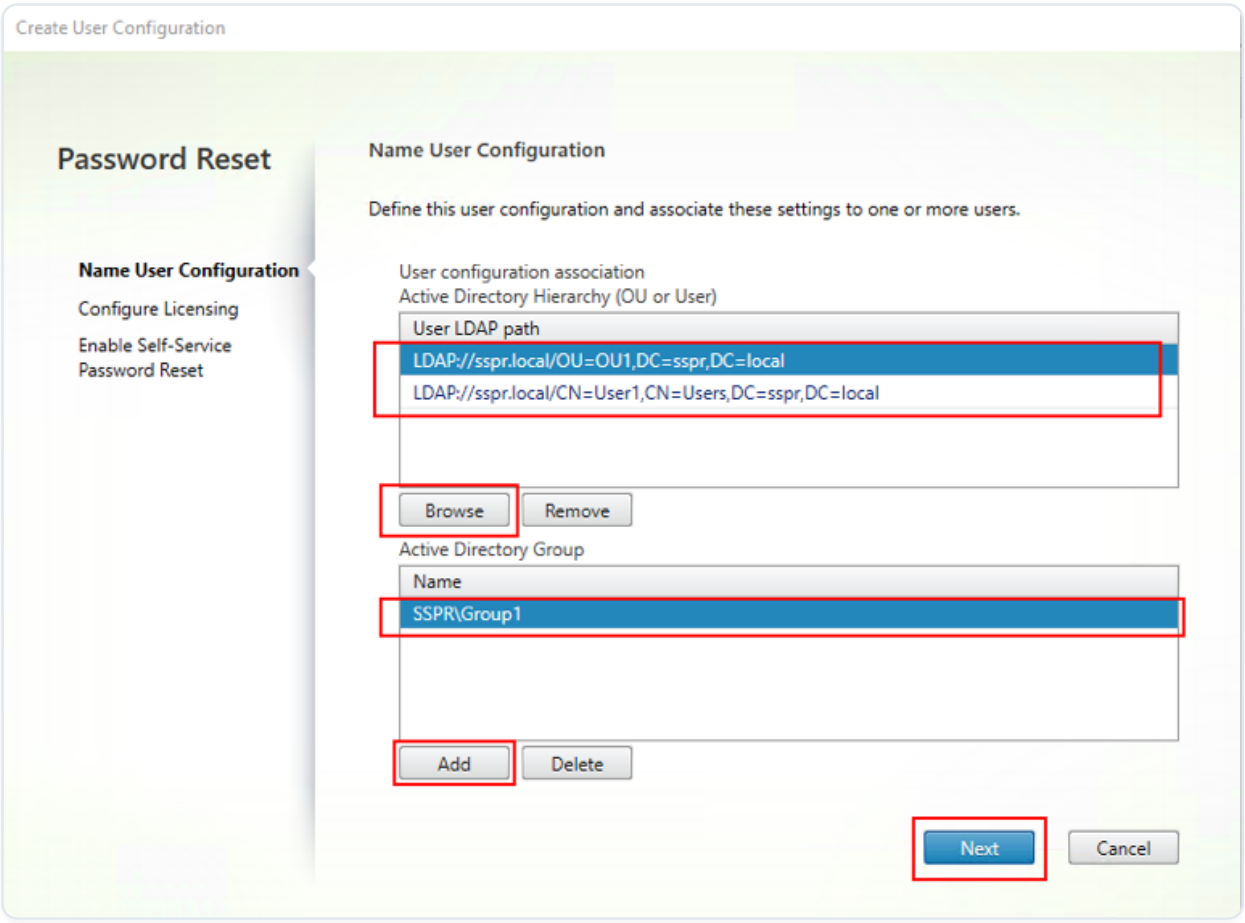


6. 单击 **完成** 以完成配置。

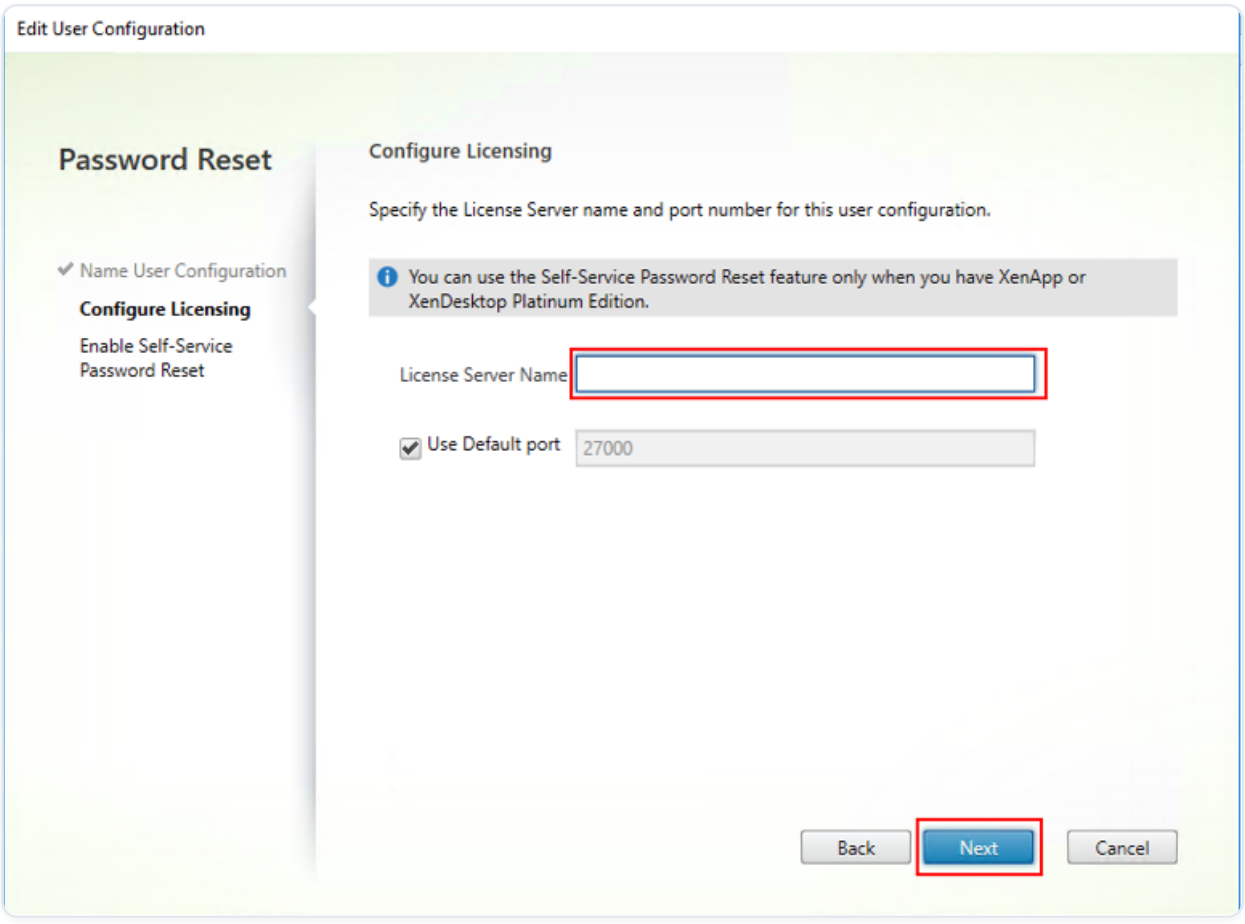


用户配置

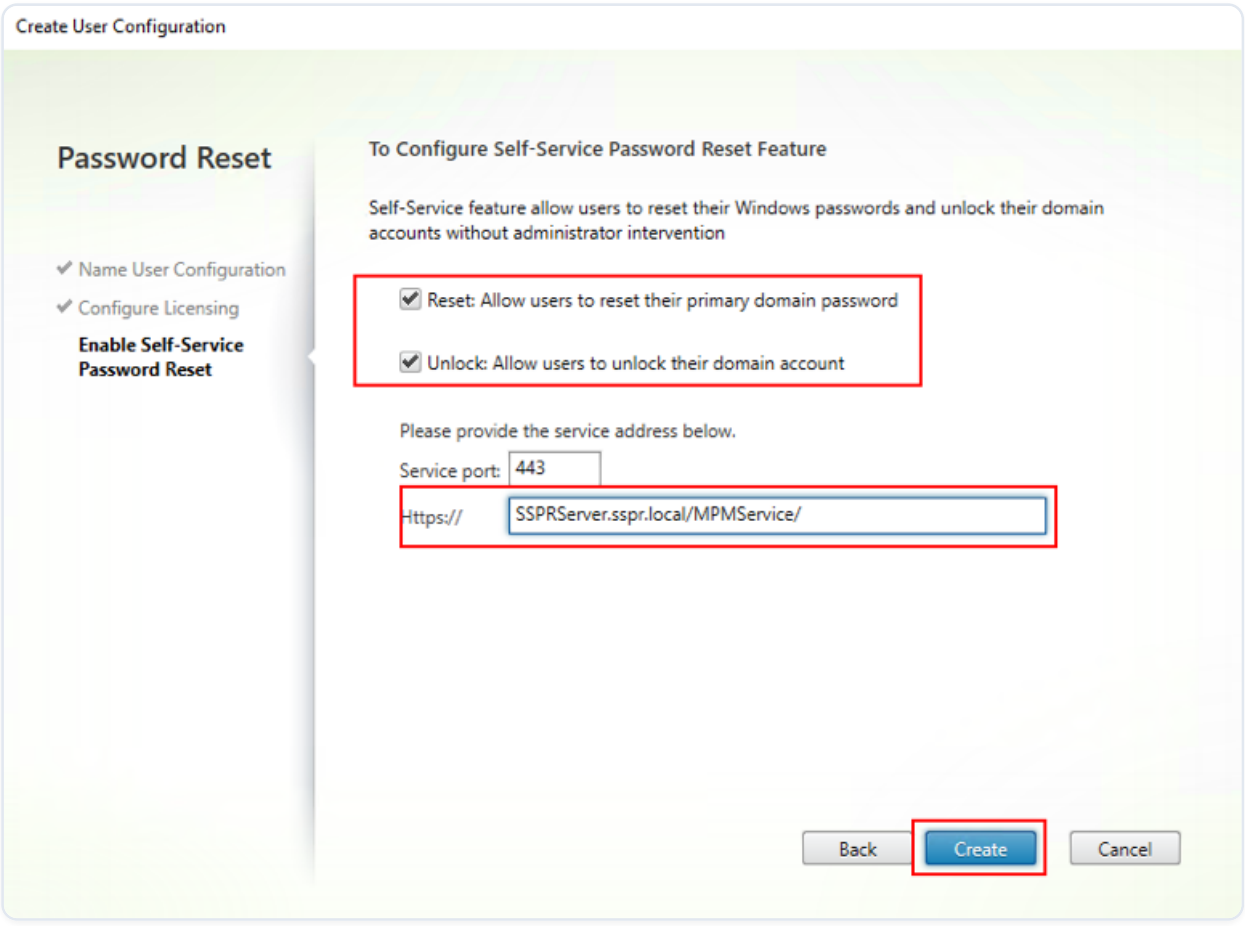
1. 在左侧窗格中，选择 **用户配置**，然后在右侧窗格中单击 **新建用户配置**。
2. 在 **命名用户配置** 屏幕上，定义自助服务密码服务目标用户组，从 Active Directory 添加用户/组/OU，然后单击 **下一步**。



3. 在 **配置许可** 屏幕上，指定许可证服务器，然后单击 **下一步**。



4. 在 **启用自助服务密码重置** 屏幕上，使用复选框指定用户是否可以在没有管理员干预的情况下重置其 Windows 密码并解锁其域帐户，指定服务端口和地址，然后单击 **创建**。



有关管理用户配置的更多信息，请参阅 管理用户配置。

身份验证

1. 在左窗格中，选择“**身份验证**”节点，然后在右窗格中单击“**管理问题**”。
2. 在“**基于问题的身份验证**”屏幕上，选择默认语言，使用复选框启用或禁用安全问题答案的掩码，然后单击“**下一步**”。
3. 在“**安全问题**”屏幕上，单击“**添加问题**”，在文本框中键入问题，单击“**确定**”，然后单击“**下一步**”。
4. 在“**问卷**”屏幕上，单击“**添加**”，然后选择一个问题。您可以使用“**上移**”和“**下移**”按钮重新组织问题和组。完成此页面后，单击“**创建**”和“**确定**”。

有关管理身份验证问题的详细信息，请参阅管理身份验证问题。

管理用户配置

用户配置使您能够控制用户登录 Storefront 时界面的行为和外观。创建新配置是在将自助密码重置分发给环境中的用户之前所采取的最后一步。您可以随时编辑现有用户配置。

用户配置是设置的唯一集合，您可以将其应用于与 Active Directory 层次结构（组织单位 \[OU\] 或单个用户）或 Active Directory 组关联的用户。

用户配置包括以下内容：

- 与 Active Directory 域层次结构（OU 或单个用户）或 Active Directory 组关联的用户

重要提示：不支持 Active Directory 混合模式下的通讯组和域本地组。

- 许可证服务器
- 自助服务功能（帐户解锁和密码重置）

在创建用户配置之前，请确保已创建或定义以下内容：

- 中央存储
- 服务配置

创建用户配置：

1. 单击 **开始** \> **所有程序** \> **Citrix** \> **Citrix 自助密码重置配置**。
2. 在左侧窗格中，选择“**用户配置**”节点。
3. 从“**操作**”菜单中，单击“**添加新用户配置**”。

添加用户、OU 或组：

用户配置向导的“**命名用户配置**”页面允许您将用户配置与用户关联。

用户配置关联：

您有两种选择：根据 Active Directory 层次结构（OU 或单个用户）或 Active Directory 组关联用户。如有必要，您可以通过单击“**操作**”菜单中的“**编辑用户配置**”来稍后将用户配置与不同的层次结构或组关联。

仅在使用 Active Directory 身份验证的 Active Directory 域中支持将用户配置与组关联。

在“**命名用户配置**”页面（来自“添加新用户配置”或“编辑用户配置”向导）上选择 OU、用户或组。

注意： 我们建议您不要将任何特权帐户（例如，本地管理员或域管理员）包含在自助密码重置帐户可以重置密码的用户组中。请使用新的专用组。

配置许可：

用户配置向导的“**配置许可**”页面允许您配置自助密码重置服务使用的许可证服务器。

注意： 仅当您拥有 Citrix Virtual Apps 或 Citrix Virtual Desktops™ Platinum Edition 时，才能使用解锁和重置功能。

在**配置许可**页面（从“添加新用户配置”或“编辑用户配置”向导）上输入许可证服务器名称和端口号。

要启用解锁或重置功能：

自助密码重置允许用户重置其 Windows 密码并解锁其域帐户，而无需管理员干预。在**启用自助密码重置**页面上，您可以选择要启用的功能。

在**启用自助密码重置**页面（从“添加新用户配置”或“编辑用户配置”向导）上，选择您希望用户使用的功能：**解锁**或**重置**。

要配置黑名单：

IT 管理员可以将用户和组添加到黑名单。黑名单中的用户和组无法使用任何自助密码重置功能，包括注册、帐户解锁和密码重置。此外，黑名单中的用户登录后无法在 Citrix Workspace™ 应用程序上看到**任务**按钮。

要配置黑名单：

1. 单击**开始 \> 所有程序 \> Citrix \> Citrix 自助密码重置配置**。
2. 在左侧窗格中，选择**用户配置**，然后在右侧窗格中单击**黑名单配置**。
3. 使用**添加**和**删除**按钮将用户或组添加到黑名单或从黑名单中删除。

管理身份验证问题

Citrix 自助密码重置配置控制台的身份验证功能为您提供了一个集中位置，用于管理与身份验证、自助密码重置和帐户解锁相关的所有安全问题。您可以将自己的安全问题自定义到默认问题列表中，并创建问题组。

- 如果在用户注册答案后编辑现有默认问题，请考虑编辑后问题的含义。编辑问题不会强制用户重新注册。但是，如果更改问题的含义，则最初回答该问题的用户可能无法提供正确答案。
- 在用户注册后添加、删除和替换安全问题意味着，所有以前使用旧问题集注册的用户都无法进行身份验证和重置密码，直到他们重新注册。用户在 Citrix Workspace 应用程序中打开“任务”时必须回答新的问题集。
- 单个安全问题可以属于多个安全问题组。创建安全问题组时，您创建的所有问题都可用于任何安全问题组。

使用以下步骤访问以下过程中引用的设置：

1. 单击 **开始 \> 所有程序 \> Citrix \> Citrix 自助密码重置配置**。

2. 在左侧窗格中，选择 **身份验证** 节点。
3. 从 **操作** 菜单中，单击 **管理问题**。

要设置默认语言：

在大多数情况下，用户会看到以与其当前用户配置文件关联的语言显示的安全问题。如果该语言不可用，自助密码重置将以您指定的默认语言显示问题。

1. 单击 **开始 \> 所有程序 \> Citrix \> Citrix 自助密码重置配置**。
2. 在左侧窗格中，选择 **身份验证** 节点。
3. 从 **操作** 菜单中，单击 **管理问题**。
4. 在 **基于问题的身份验证** 页面上的 **默认语言** 下拉列表中，选择默认语言。

要启用安全答案掩码：

安全答案掩码在用户注册安全问题答案或在身份验证期间提供答案时，为用户提供了额外的安全级别。启用此功能后，用户的答案将被隐藏。在答案注册过程中，这些用户需要输入两次答案，以避免打字和拼写错误。用户在身份验证期间只需输入一次答案，因为如果出现错误，系统会提示他们重试。

在 **基于问题的身份验证** 页面上，选择 **掩盖安全问题的答案**。

要创建新的安全问题：

您可以创建许多不同的问题，并为每个问题指定一种语言。您还可以为单个问题提供多种翻译。Citrix Workspace 应用程序中的注册会以与用户配置文件语言设置相对应的语言向用户显示问卷。如果该语言不可用，自助密码重置将以默认语言显示问题。

注意：当您为安全问题指定语言时，该问题会显示给其操作系统设置配置为该指定语言的用户。如果所选的操作系统设置与任何可用问题不匹配，则会向用户显示您选择的默认语言。

1. 在“**安全问题**”页面上的“**语言**”下拉列表中，选择一种语言，然后单击“**添加问题**”。此时将显示“安全问题”对话框。
2. 在“**安全问题**”对话框中创建新问题。

重要提示：使用“**编辑**”按钮可包含现有问题的翻译文本。如果您选择“**添加问题**”，则会创建一个与原始问题不关联的新问题。

要添加或编辑现有问题的文本：

在用户注册后添加、删除和替换安全问题意味着所有以前使用旧问题集注册的用户都无法进行身份验证和重置密码，直到他们重新注册。用户在 Citrix Workspace 应用程序中打开任务时必须回答新的问题集。编辑问题不会强制用户重新注册。

重要提示：如果您正在编辑现有问题，请注意不要更改问题的含义。这可能会导致在重新身份验证期间用户答案不匹配。也就是说，用户可能会提供一个与存储答案不匹配的不同答案。

1. 在“**安全问题**”页面上的“**语言**”下拉框中选择一种语言。
2. 选择问题，然后单击“**编辑**”。
3. 在“**安全问题**”对话框中编辑问题。

要创建安全问题组：

您可以创建一些安全问题，供用户回答以确认其身份。您添加到问卷中的每个问题都必须由用户回答。但是，您也可以将这些问题分组到一个安全问题组中。

例如，将问题分组可以使您向问卷中添加一组六个问题，并允许用户从该问题组中选择，例如回答六个问题中的三个。这为用户在选择问题和提供用于身份验证的答案方面提供了灵活性。

1. 在“**安全问题**”页面上单击“**添加组**”。
2. 在“**安全问题组**”对话框中，命名组，选择问题，并设置用户必须回答的问题数量。

编辑安全问题组：

选择要编辑的安全组，然后在“**安全问题**”页面上单击“**编辑**”。此时将显示“安全问题组”对话框，其中包含可作为组一部分的安全问题列表。组中当前的问题由复选标记指示。在此处，您可以编辑组的名称、向组中添加问题，以及选择用户必须回答的此组中的问题数量。

添加或删除现有问卷：

从问卷中添加或删除安全问题和问题组。向上和向下移动问题，以调整向用户呈现的顺序。如果问卷已更改，请通知用户在登录 Storefront 后执行重新注册任务。

1. 在“**问卷**”页面上单击“**添加**”以向问卷添加问题或组。
2. 单击“**删除**”以从问卷中删除问题。
3. 单击“**上移**”或“**下移**”以管理向用户呈现的问题。

导入或导出安全问题：

您可以导入或导出安全问题和组的数据。

1. 单击“**开始**” \> “**所有程序**” \> “**Citrix**” \> “**Citrix 自助密码重置配置**”。

2. 在左窗格中，选择“**身份验证**”节点。
3. 在“**操作**”菜单中，单击以下选项之一：

   导入安全问题 指定文件位置以导入安全问题和组的数据。

   导出安全问题 指定文件位置以导出安全问题和组的数据。

安全配置

本文包含确保自助密码重置组件安全部署和配置所需的步骤。

- 创建域用户帐户以重置用户密码并解锁用户帐户权限
- 配置防火墙设置

创建自助服务帐户

如果您正在使用自助密码重置的密码重置或帐户解锁功能，请在服务配置期间指定一个自助服务帐户，该帐户将由自助服务模块用于执行密码重置和帐户解锁。确保该帐户具有足够的权限，但我们不建议在生产部署中使用“域管理员”组中的帐户。建议的帐户权限为：

- 域成员
- 相关域用户的密码重置和帐户解锁权限

在“**Active Directory 用户和计算机**”中，创建具有重置用户密码和解锁用户帐户权限的组或用户帐户。

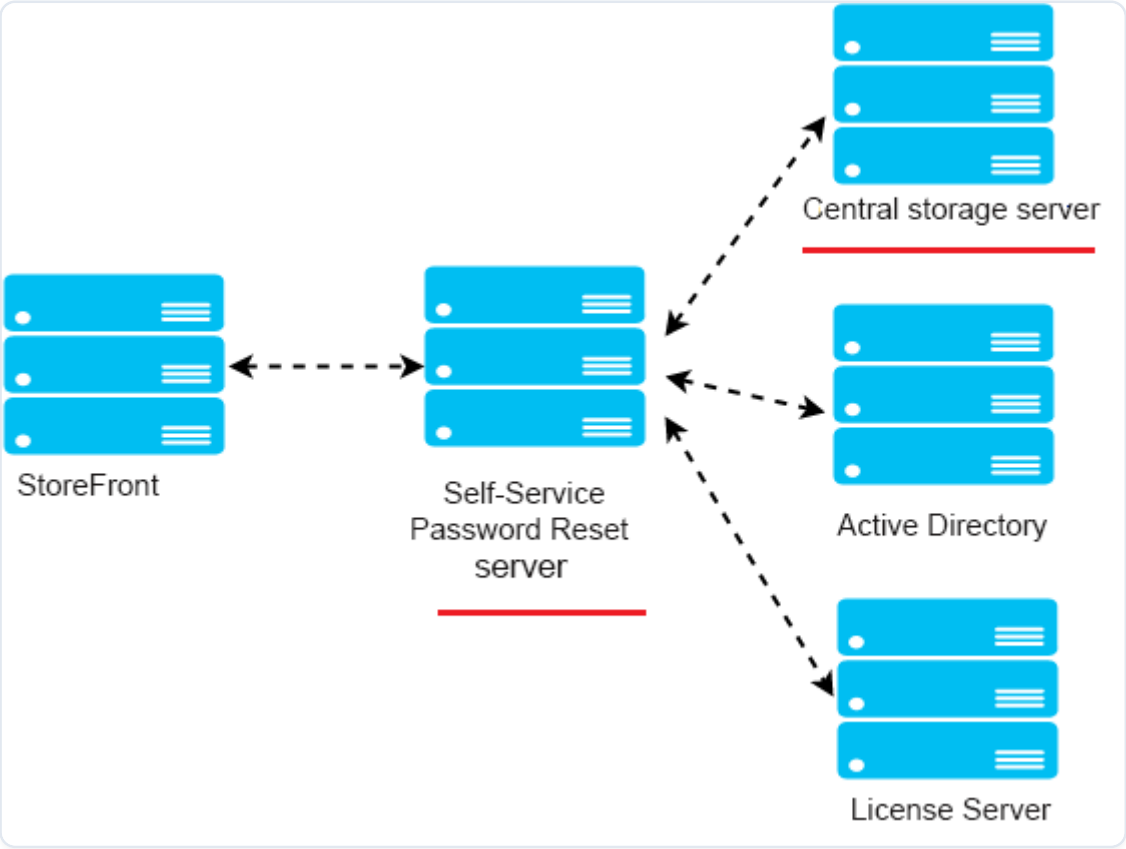
1. 在“**Active Directory 用户和计算机**”中，右键单击域，然后从菜单中单击“**委派控制**”。
2. 将显示“**委派控制**”向导。在“**欢迎**”对话框中，单击“**下一步**”。
3. 在“**用户和组**”对话框中，单击“**添加**”。在列表中选择要授予解锁帐户权限的组，然后单击“**确定**”。在“**用户和组**”对话框中，单击“**下一步**”。
4. 在“**要委派的任务**”对话框中，单击“**创建要委派的自定义任务**”，然后单击“**下一步**”。
5. 在“**Active Directory 对象类型**”对话框中，单击“仅文件夹中的以下对象 \> 用户对象”，然后单击“**下一步**”。
6. 在“**权限**”对话框中，选中“**常规**”和“**属性特定**”复选框。在“**权限**”列表中，选中“**读取 lockoutTime**”、“**写入 lockoutTime**”、“**重置密码、更改密码、读取 userAccountControl、写入 userAccountControl、读取 pwdLastSet 和写入 pwdLastSet**”复选框，然后单击“**下一步**”。
7. 在 **完成控制委派** 向导对话框中，单击 **完成**。

配置防火墙设置

由于 Self-Service Password Reset 服务器和中央存储服务器组件管理用户密码，我们强烈建议您将这些组件部署在受信任的网络上，并且它们只能由特定的受信任组件访问。本节介绍确保为这些服务器正确配置 Windows 防火墙的步骤。我们还建议您配置现有的网络基础设施，以确保这些服务器与不受信任的网络流量隔离。

完成部署中的这些配置后，Self-Service Password Reset 中央存储服务器只能通过使用服务器消息块 (SMB) 从 Self-Service Password Reset 服务器访问。Self-Service Password Reset 服务器只能通过 HTTPS 连接从 StoreFront™ 服务器访问。

Windows 2012 R2 的远程文件共享部署



环境

- 将 Self-Service Password Reset 组件部署在专用服务器上。不要将它们部署在与现有 StoreFront 或 Delivery Controller™ 组件相同的服务器上。否则，下面显示的防火墙配置可能会阻止 StoreFront 或控制器流量。
- StoreFront 和 Self-Service Password Reset 服务器之间没有非透明 HTTP/HTTPS 代理。

如果 StoreFront 和 Self-Service Password Reset 服务器之间存在任何非透明代理，请在防火墙规则中配置 Self-Service Password Reset 服务器，使其只能从代理服务器访问。

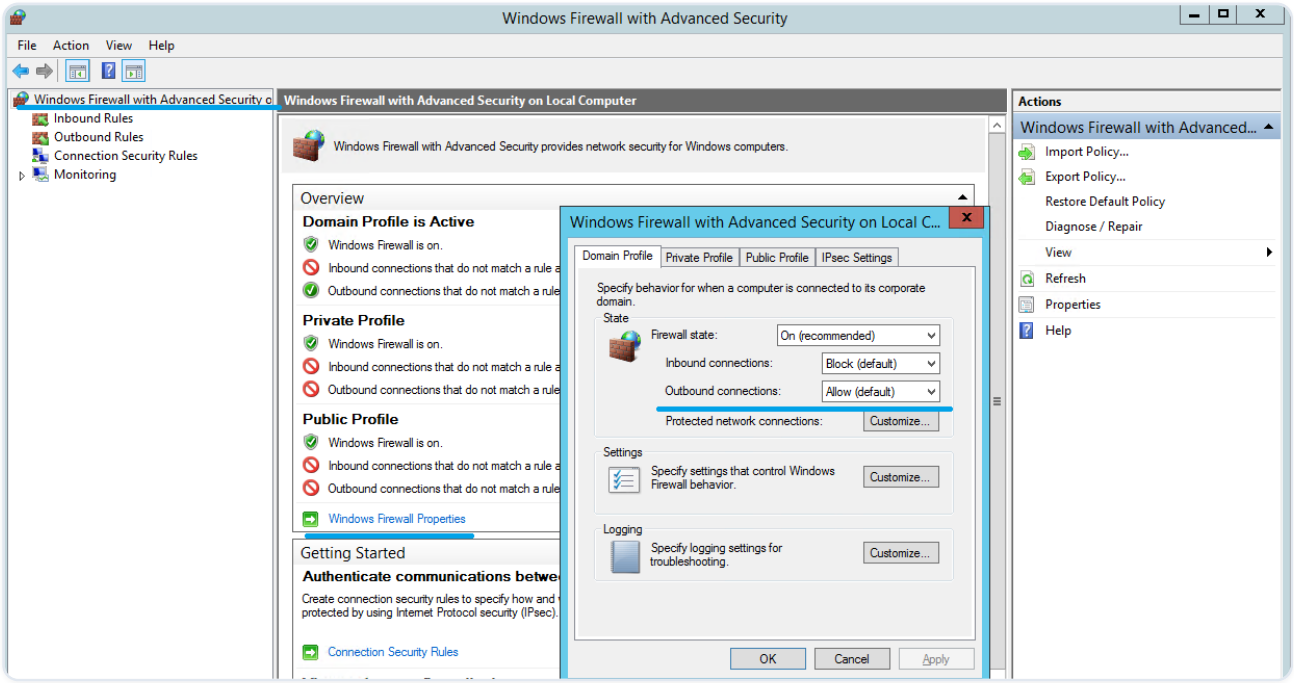
- 这些过程中的配置基于 Windows 默认防火墙规则。

为 Self-Service Password Reset 中央存储配置防火墙

完成配置后，Self-Service Password Reset 中央存储提供的 SMB 服务只能从入站的 Self-Service Password Reset 服务器访问。Self-Service Password Reset 中央存储服务器只能出站访问公司网络上的服务。

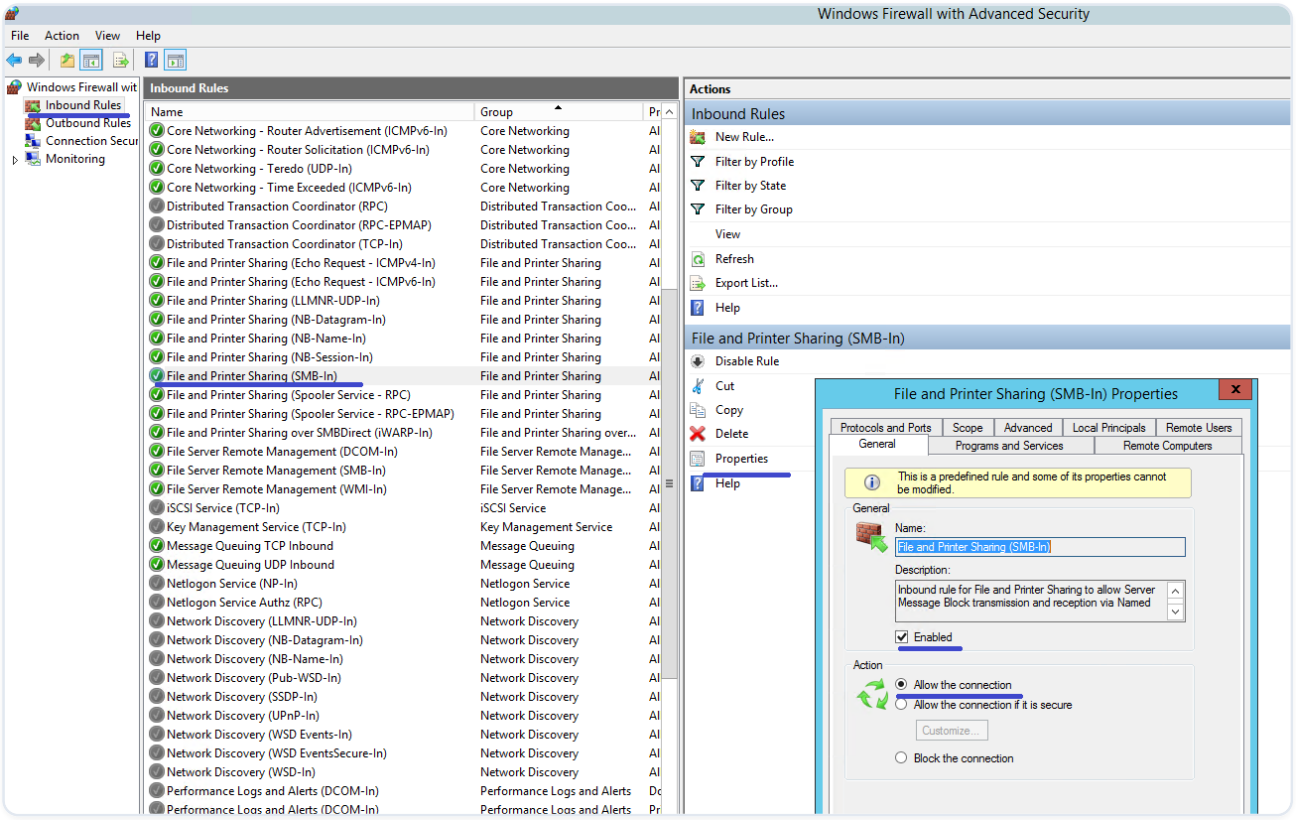
1\. 打开服务器管理器，然后从顶部导航栏上的 **工具** 菜单中选择 **带高级安全性的 Windows 防火墙**。

2\. 在 **带高级安全性的 Windows 防火墙** 中，在中间窗格中选择 **Windows 防火墙属性**。有三个防火墙配置文件 - 域、专用和公用。选择 **域配置文件** 选项卡。确保 **防火墙状态** 设置为 **开**，**入站连接** 设置为 **阻止**，**出站连接** 设置为 **允许**。



3\. 选择 **专用配置文件** 和 **公用配置文件** 选项卡。确保 **防火墙状态** 设置为 **开**，并且 **入站连接** 和 **出站连接** 都设置为 **阻止**。应用并保存更改。

4\. 从 **入站规则** 中，选择 **文件和打印机共享 (SMB-In)**，并确保此规则已 **启用** 且 **操作** 设置为 **允许连接**。



5\. 在**文件和打印机共享 (SMB-In) 属性**中，切换到**范围**选项卡。选择**这些 IP 地址**并将所有 Self-Service Password Reset 服务器 IP 地址添加到列表中。例如，Self-Service Password Reset 服务器 A (192.168.1.10) 和 Self-Service Password Reset 服务器 B (192.168.1.11)。

6\. 在**文件和打印机共享 (SMB-In) 属性**中，切换到**高级**选项卡，选择**域**、**专用**和**公共**配置文件，然后保存此规则的更改。

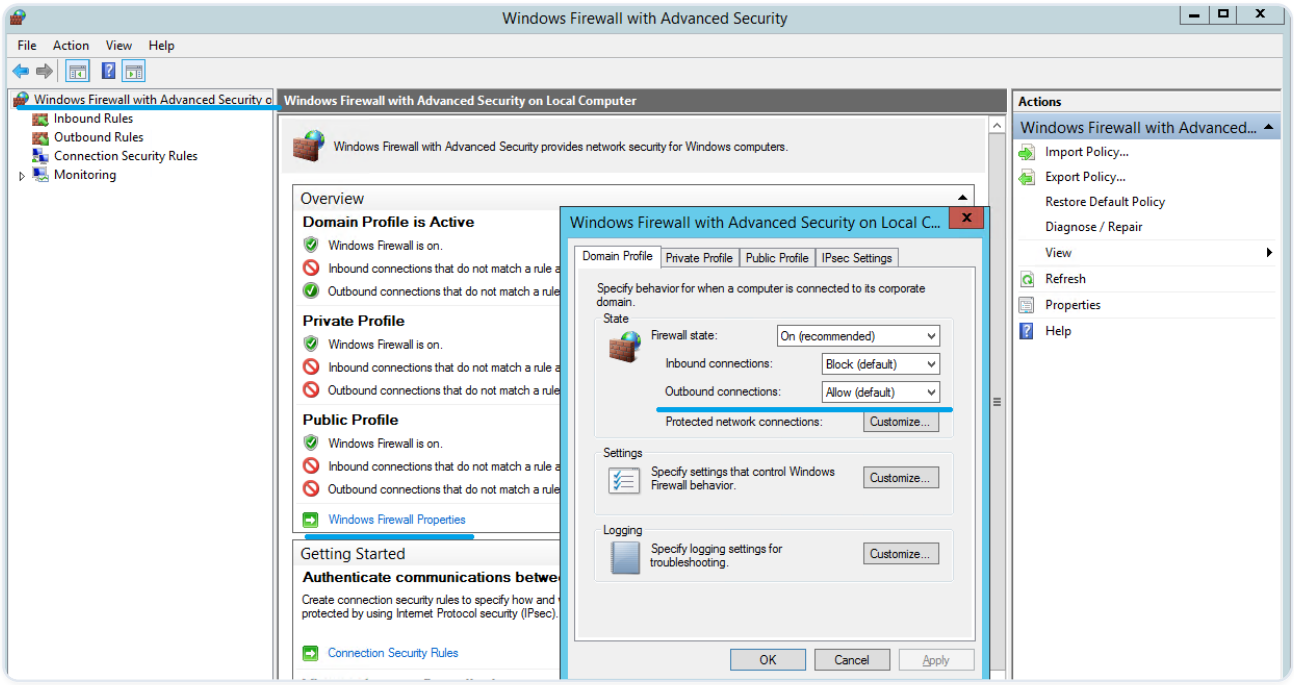
7\. 对**文件服务器远程管理 (SMB-In)** 和**文件和打印机共享 (NB-Session-In)** 的**入站**规则重复此过程。

配置自助密码重置服务器的防火墙

完成配置后，自助密码重置服务器提供的 Web 服务只能由 StoreFront 服务器使用 HTTPS 访问。自助密码重置服务器可以访问公司网络上的服务。

1\. 打开服务器管理器，然后从顶部导航栏上的**工具**菜单中选择**带高级安全性的 Windows 防火墙**。

2\. 在**带高级安全性的 Windows 防火墙**中，在中间窗格中选择**Windows 防火墙属性**。有三个防火墙配置文件 - 域、专用和公共。选择**域配置文件**选项卡。确保**防火墙状态**设置为**开**，**入站连接**设置为**阻止**，**出站连接**设置为**允许**。

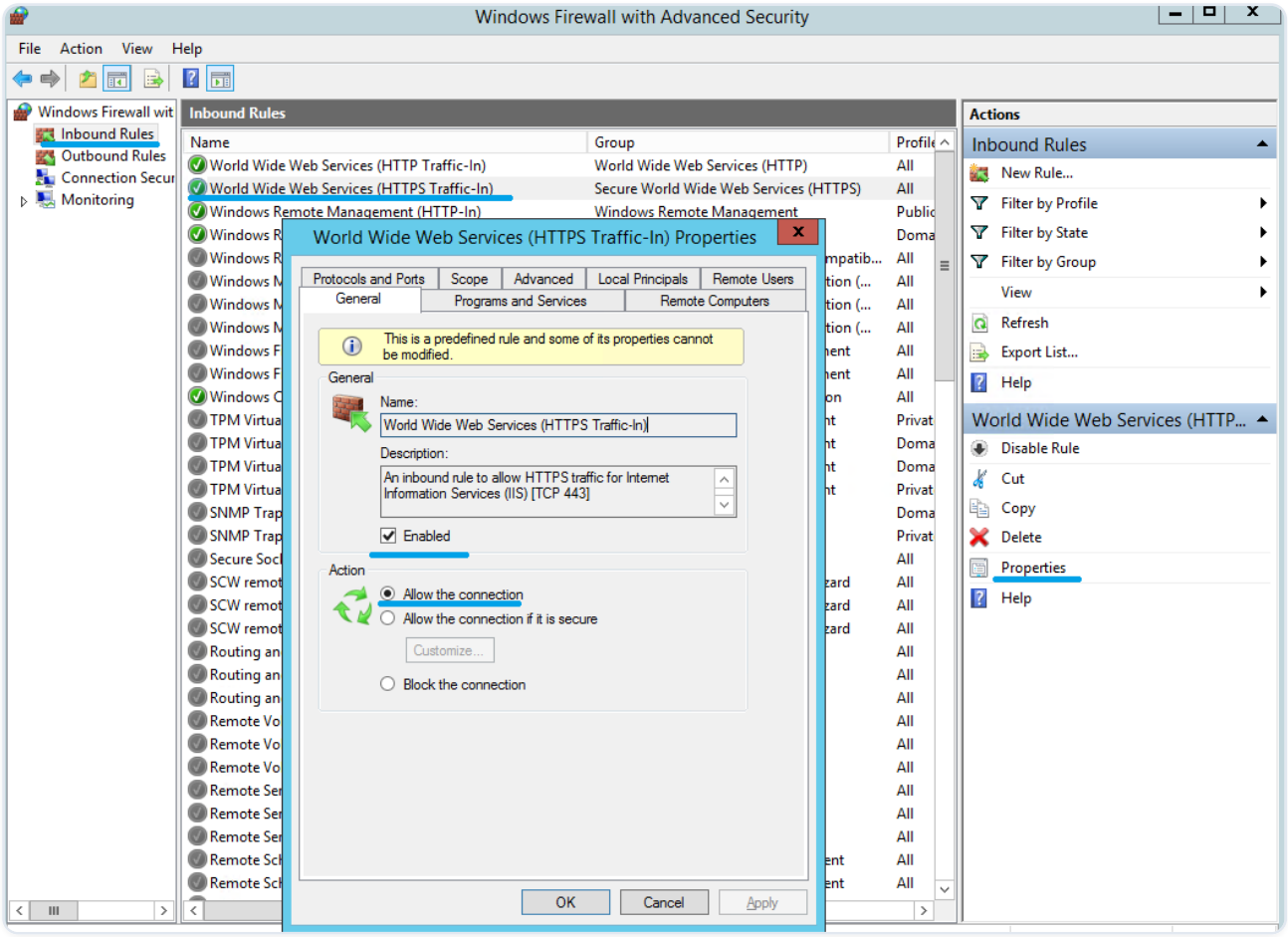


3\. 选择**专用配置文件**和**公共配置文件**选项卡，并确保**防火墙状态**设置为**开**。并且**入站连接**和**出站连接**都设置为**阻止**。应用并保存更改。

4\. 从**入站规则**中，选择**万维网服务 (HTTP 流量-入)**。并确保此规则已**启用**，并且**操作**设置为**阻止连接**。

5\. 在**万维网服务 (HTTP 流量-入) 属性**中，切换到**高级**选项卡。选择**域、专用**和**公共**配置文件，然后保存此规则的更改。

6\. 从**入站规则**中，选择**万维网服务 (HTTPS 流量-入)**。确保此规则已**启用**，并且**操作**设置为**允许连接**。



7\. 在**万维网服务 (HTTPS 流量-入) 属性**中，切换到**范围**选项卡。选择**这些 IP 地址**，并将所有 StoreFront 服务器 IP 地址添加到列表中。例如，StoreFront A (192.168.1.50) 和 StoreFront B (192.158.1.51)。

8\. 在**万维网服务 (HTTPS 流量-入) 属性**中，切换到**高级**选项卡。选择**域**、专用和**公共**配置文件，然后保存此规则的更改。

从单点登录中央存储迁移数据

单点登录中央存储是单点登录用于存储和管理用户和管理数据的集中式存储库。用户数据包括用户凭据、安全问题答案以及其他以用户为中心的数据。管理数据包括密码策略、应用程序定义、安全问题以及其他更广泛的数据。

您无法将所有数据从单点登录中央存储迁移到自助密码重置中央存储。下表说明了可以和不可以迁移的数据。

无法迁移	可以迁移
密码策略 - 不支持	包含注册数据的用户文件夹
应用程序模板 - 不支持	客户使用的问卷
应用程序定义 - 不支持	
用户配置 - 在自助密码重置控制台上创建	
应用程序组 - 不支持	
单点登录服务数据 - 在自助密码重置控制台上创建	

重要

- 自助密码重置不支持将 Active Directory 作为中央存储，仅支持网络共享。
- 自助密码重置仅支持来自单点登录 4.8 或 5.0 的数据。

从单点登录中央存储迁移数据

在迁移数据之前，请熟悉自助密码重置的安装和配置。有关详细信息，请参阅安装和配置。

1. 创建新的中央存储。
2. 安装自助密码重置服务和控制台。

3. 在控制台中，指定新的中央存储位置。
4. 创建新的用户配置，并包含已在单点登录上启用自助密码重置的用户。
5. 将单点登录注册数据和安全问题复制到新的中央存储。

注意： 确保数据代理帐户对所有复制的文件具有完全控制权限。

您只需要两个文件夹/文件。

示例

复制所有用户的注册数据：

\\\\SSO-SERVER\\citrixsync$\\People

到

\\\\SSPR-SVC\\citrixsync$\\People

使用此命令： **Robocopy \\\\SSO-SERVER\\citrixsync$\\People\\ \\\\SSPR-SVC\\citrixsync$\\People /e /xd QBA /Log+:copylog.txt /tee**

复制客户使用的安全问题：

\\\\SSOSERVERcitrixsync$\\CentralStoreRoot\\AdminConsole\\QuestionBasedAuthentication2\\ QuestionBasedAuthentication2

> 到

\\\\SSPRSVCcitrixsync$\\CentralStoreRoot\\AdminConsole\\QuestionBasedAuthentication2\\

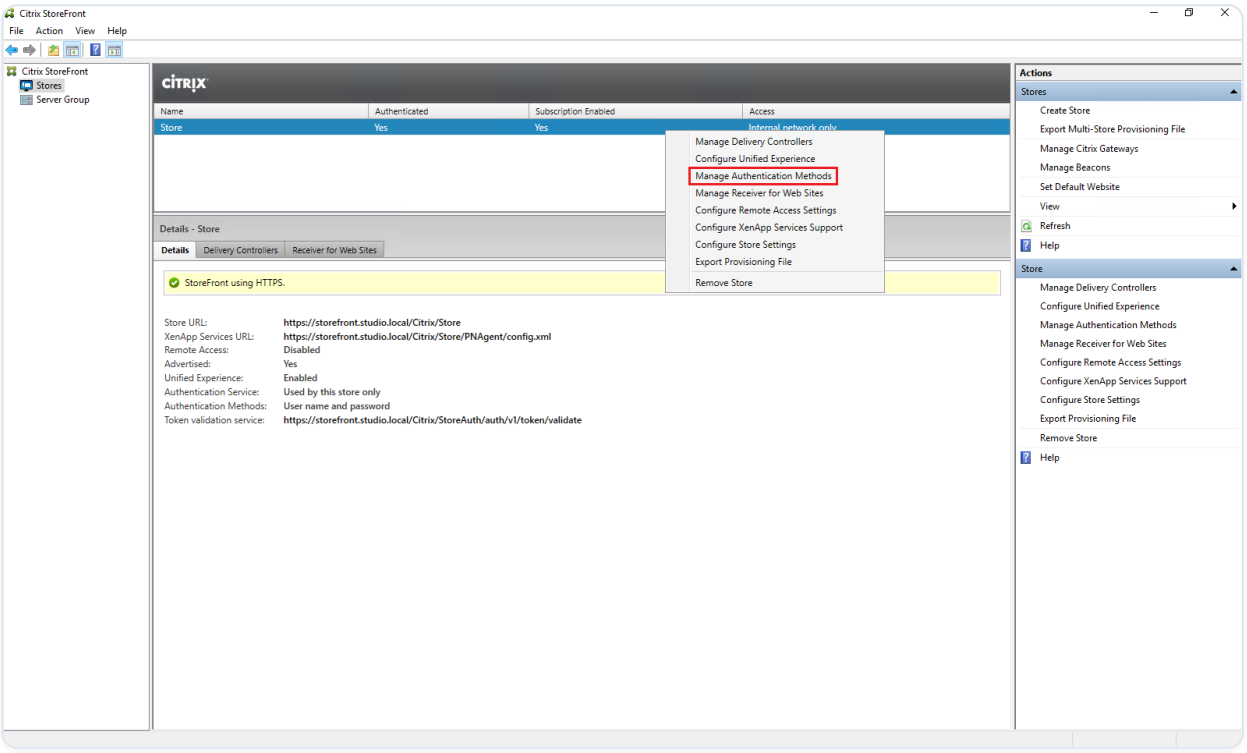
使用此命令： **Robocopy \\\\SSO-SERVER\\citrixsync$\\CentralStoreRoot\\AdminConsole\\QuestionBasedAuthentication2\\ \\\\SSPR-SVC\\citrixsync$\\CentralStoreRoot\\AdminConsole\\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee**

现在，所有用户都可以使用其单点登录注册问题和答案来解锁和重置。

配置 StoreFront™ 以允许用户记录安全问题的答案

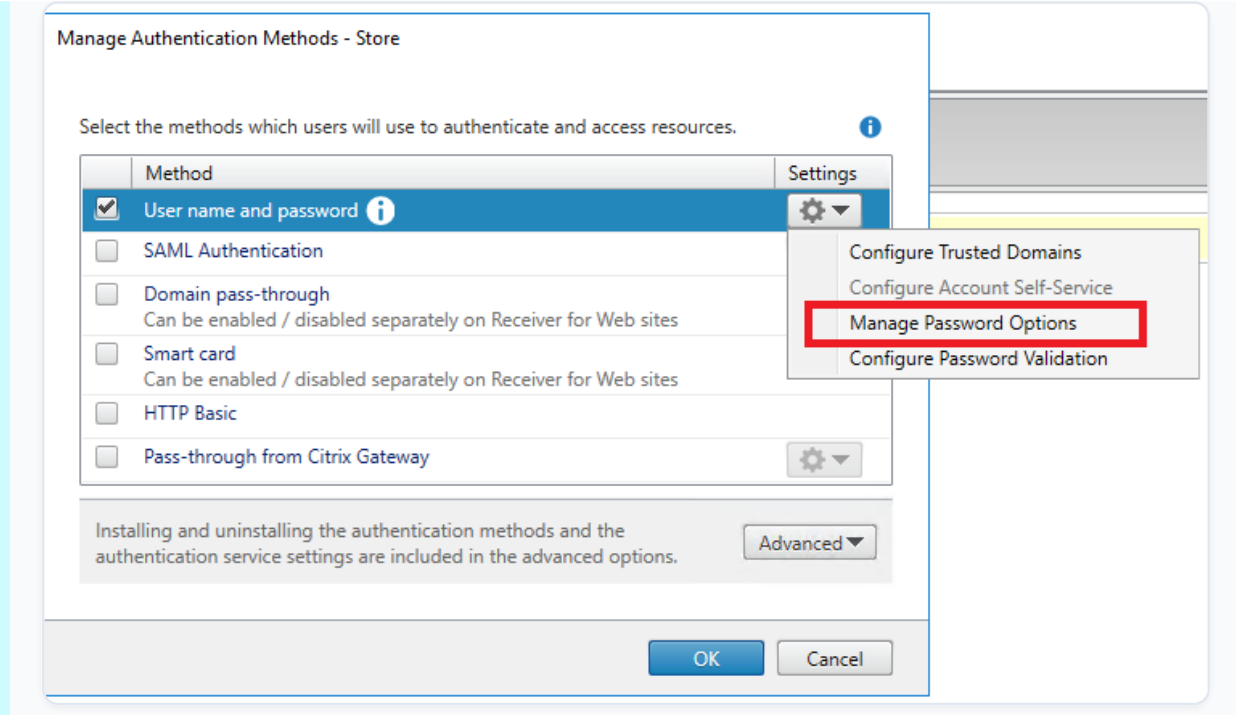
配置 StoreFront 以允许用户注册其安全问题的答案。注册后，他们可以重置域密码并解锁域帐户。有关详细信息，请参阅 StoreFront 文档。

1. 将 StoreFront 互联网信息服务 (IIS) 配置为 HTTPS。
2. 在 StoreFront 中创建部署。
3. 在 StoreFront 管理控制台的右侧窗格中，右键单击应用商店，然后选择 **管理身份验证方法**。

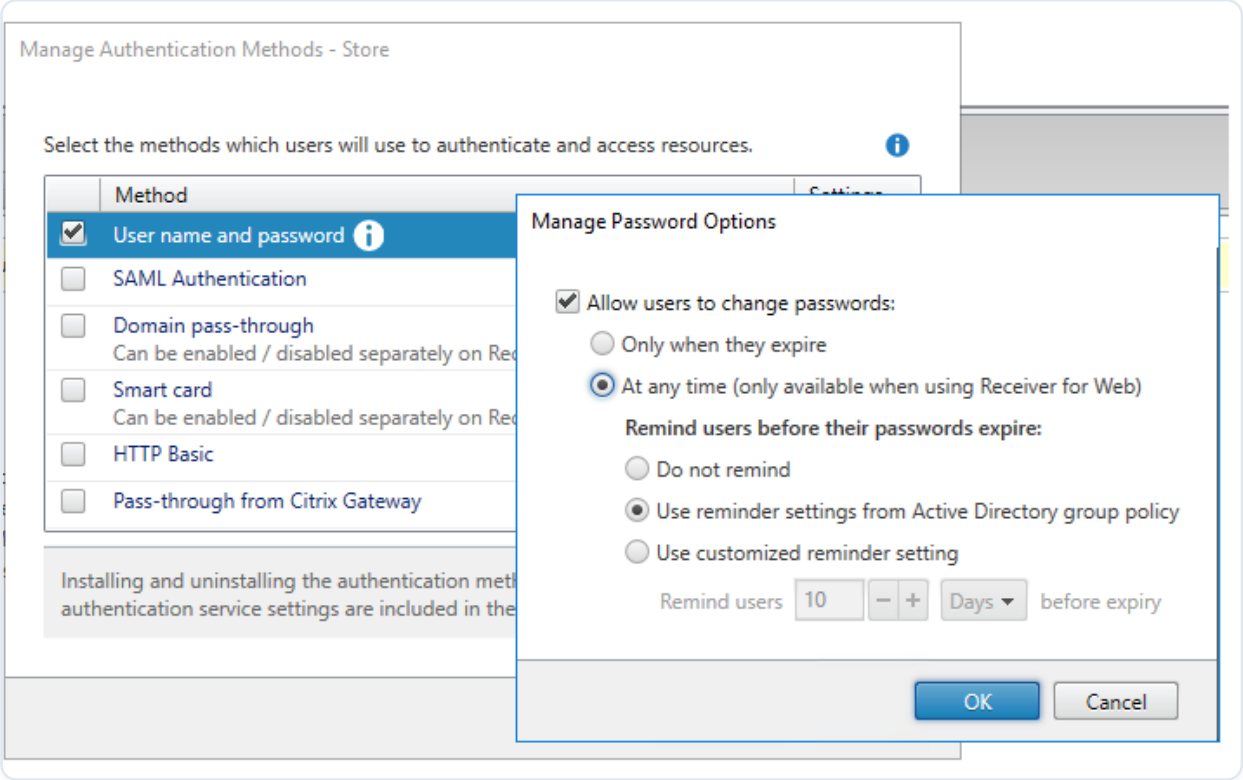


4. 在 **用户名和密码** 的设置下选择 **管理密码选项**。

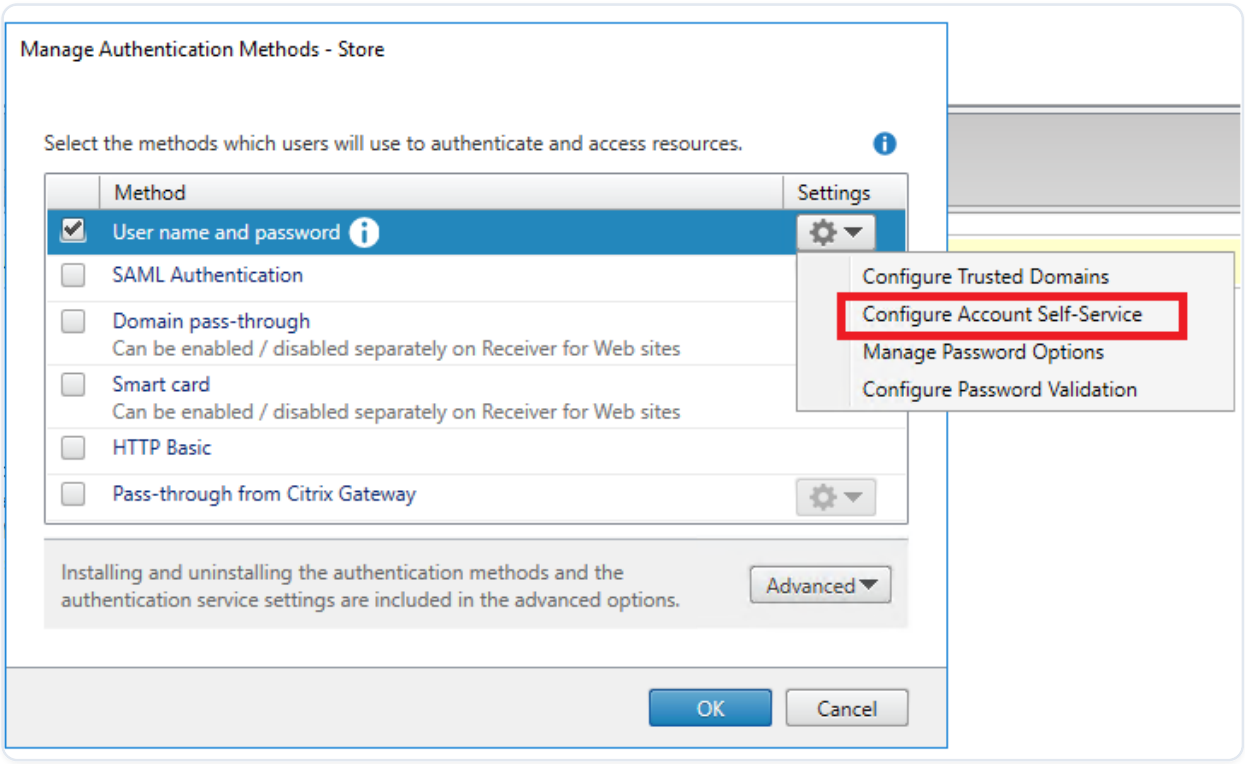
> **注意：**
>
> 自助密码重置 (SSPR) 仅支持 StoreFront 的 **用户名和密码** 身份验证方法。它不支持其他方法，例如域直通。



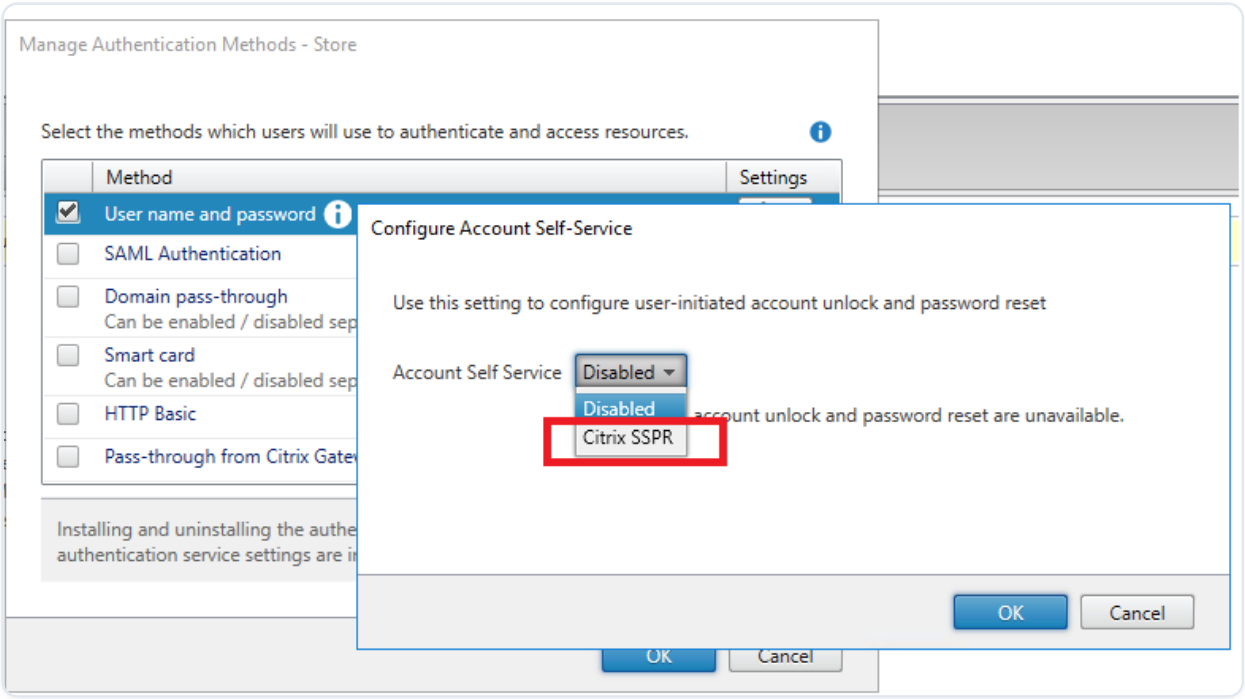
5. 选择您希望用户何时更改密码，然后单击 **确定**。



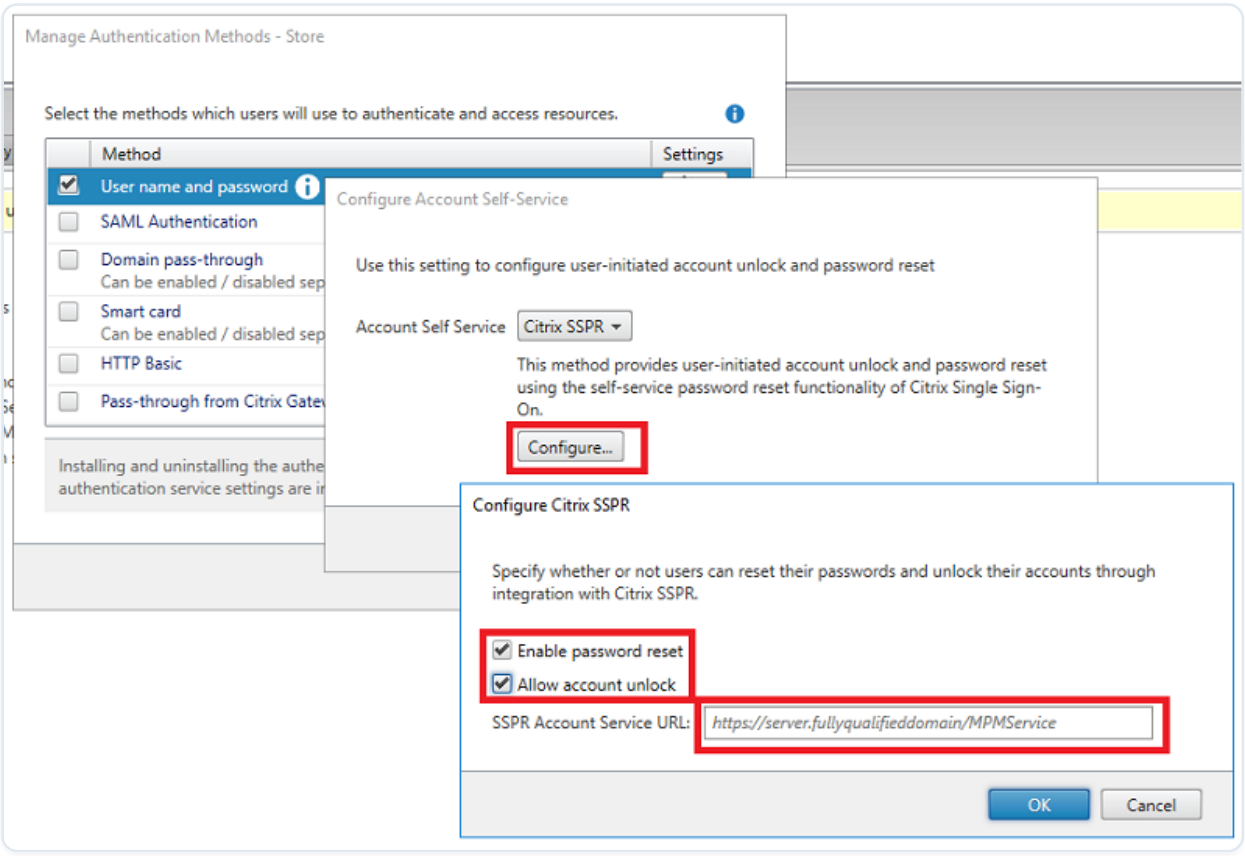
6. 在 **用户名和密码** 的设置下选择 **配置帐户自助服务**。



7. 选择 **Citrix SSPR** 以启用 **帐户自助服务**。



8. 点击“**配置**”，选择“**启用密码重置**”和“**允许帐户解锁**”，然后配置“**SSPR 帐户服务 URL**”(https://<SSPR 服务器的 FQDN>/MPMService)。

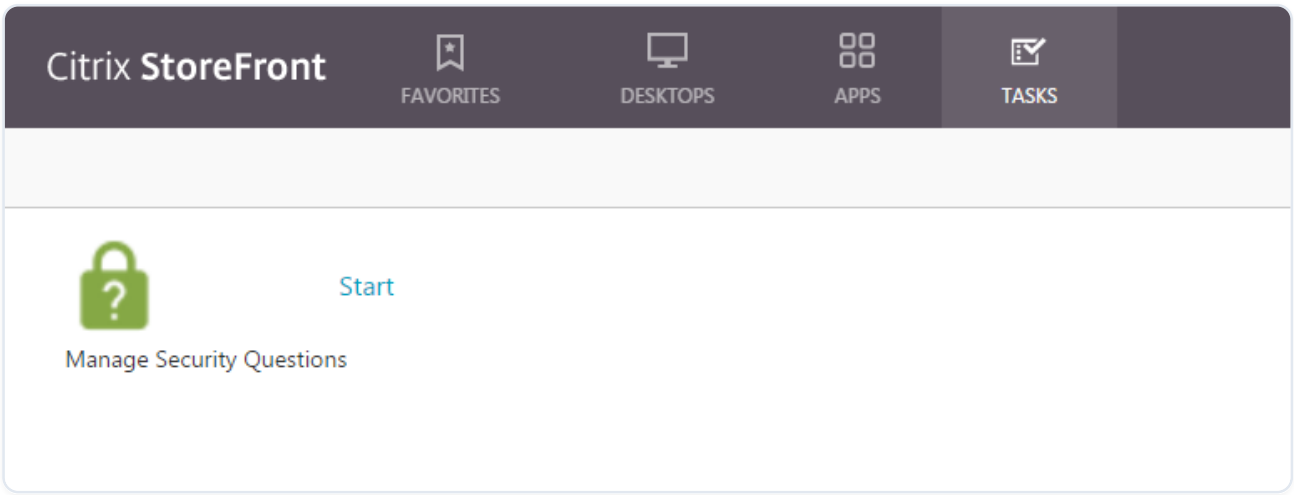


9. 点击“**确定**”以应用所有设置。

注意：

配置站点以使用统一体验。

用户下次登录 Citrix Workspace™ 应用程序或 Citrix Workspace Web 版应用程序时，即可进行安全注册。用户可以点击 “**开始**”来指定安全问题的答案，以便将来重置密码或解锁帐户。



自助服务密码重置文档历史记录

下表介绍了对自助服务密码重置 1.1.x 文档所做的重要变更。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
29 Aug 2018	发布自助服务密码重置 1.1.x	自助服务密码重置 1.1.x 中的新增功能