# 自适应身份验证服务

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

# Contents

发布说明 6
2026 年 10 月 6
新增功能 6
2026 年 9 月 6
新增功能 6
2026 年 8 月 7
新增功能 7
2026 年 6 月 7
新增功能 7
2026 年 3 月 7
新增功能 7
2025 年 11 月 8
新增功能 8
2025 年 6 月 8
新增功能 8
已修复问题 8
2024 年 10 月 8
新增功能 9
2024 年 1 月 9
新增功能 9
2023 年 9 月 9
新增功能 9
2023 年 7 月 10
新增功能 10
2023 年 4 月 10
新增功能 10

© 1997–2026 Citrix Systems, Inc. All rights reserved.

已修复问题 10
已知问题 11
配置自适应身份验证服务 12
如何配置自适应身份验证服务 12
访问自适应身份验证用户界面 12
先决条件 13
配置自适应身份验证实例 13
预配 14
控制台访问 14
上传证书 15
允许的 IP 地址 17
管理连接 18
实例管理 20
配置策略 22
示例 LDAP 和 LDAPS 负载平衡配置 23
先决条件 24
负载平衡 LDAP 服务器 24
LDAPS 服务器负载平衡 25
创建自定义监视器 26
RADIUS 负载均衡配置示例 26
先决条件 26
负载均衡 RADIUS 服务器 27
示例身份验证配置 28
带条件身份验证的多因素身份验证 28
与多因素身份验证的第三方集成 28
设备姿态扫描 (EPA) 28
其他场景 28
支持自定义商店 URL 29

© 1997–2026 Citrix Systems, Inc. All rights reserved.

支持使用自适应身份验证的智能访问 30
先决条件 30
了解智能访问的事件流 30
在自适应身份验证实例上配置智能访问策略 31
在 DaaS Studio 中定义标签 35
常见错误疑难解答 40
高可用性设置的配置更改 41
启用自适应身份验证 42
将您的身份验证方法迁移到自适应身份验证 43
自适应身份验证实例的升级和维护 47
安排您的自适应身份验证实例升级 47
配置备份和恢复 48
解除预配您的自适应身份验证实例 49
安全管理访问 50
启用对网关的安全访问 51
更新自适应身份验证 FQDN 51
编辑 FQDN 51
更新自适应身份验证证书 52
排查自适应身份验证问题 55
启用自适应身份验证日志的记录 55
预配问题 56
实例可访问性问题 56
AD 或 RADIUS 连接问题 57
身份验证问题 59
EPA 相关问题 60
智能访问标签问题 60
自适应身份验证实例的通用日志收集 61
共享安全职责 62

© 1997–2026 Citrix Systems, Inc. All rights reserved. 

客户需要采取的行动 62
客户和 Citrix 都需要采取的行动 62
规模调整和性能指南 63
用户身份验证速率 63
使用 Citrix Cloud™ Connectors 时的流量延迟和用户身份验证速率 63
使用 Azure VNet 对等互连时的流量延迟和用户认证速率 63
常见问题 65
升级自适应身份验证或 NetScaler 后，用户无法登录。我该怎么办? 65
为什么自适应身份验证 NetScaler 实例在 ADM/NetScaler Console 中显示为“Down”或“In Grace Period”? 65
为什么用户在自适应身份验证升级后会收到“依赖方请求的用户声明未找到”? 66
自适应身份验证无法通过 LDAP 端口 389 或 636 工作。我应该检查什么? 67
我正在尝试预配自适应身份验证设备，但入门流程要求我填写一个我无法访问的表单。我该怎么办? 67
提交表单后，启用自适应身份验证需要多长时间? 67
数据治理 68
数据驻留 68
自适应身份验证服务 68
自适应身份验证实例 68
数据收集 69
数据传输 70
数据控制 70
数据保留 70
数据导出 70
定义 70

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 发布说明

自适应身份验证发布说明是 NetScaler 发布说明的子集。自适应身份验证客户必须使用 NetScaler 发布说明 来了解自适应身份验证服务中的增强功能、已修复问题和已知问题。

## 2026 年 10 月

以下部分提供了有关 2026 年 10 月版本发布的更多信息。

### 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–73.46 及更高版本，以解决 CTX697191 中描述的安全漏洞。

  有关此版本自适应身份验证服务中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 发布说明。

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–73.41 及更高版本，以解决 CTX697174 中描述的安全漏洞。

  有关此版本自适应身份验证服务中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 发布说明。

## 2026 年 9 月

以下部分提供了有关 2026 年 9 月版本发布的更多信息。

### 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–73.37 及更高版本，以解决 CTX697096 中描述的安全漏洞。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关自适应身份验证服务此版本中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 版本说明。

# 2026 年 8 月

以下各节提供了有关 2026 年 8 月版本更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–73.33 及更高版本，以解决 CTX696939 中描述的安全漏洞。

  有关自适应身份验证服务此版本中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 版本说明。

# 2026 年 6 月

以下各节提供了有关 2026 年 6 月版本更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–72.61 及更高版本，以解决 CTX696604 中描述的安全漏洞。

  有关自适应身份验证服务此版本中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 版本说明。

# 2026 年 3 月

以下部分提供了有关 2026 年 3 月版本发布的更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例将自动升级到版本 14.1–66.59 及更高版本，以解决 CTX696300 中描述的安全漏洞。

- **用于自适应身份验证实例的 LAS 许可证**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自适应身份验证实例现在已自动重新许可为基于 LAS 的许可。此更改将消耗授权高级配额中分配的 NetScaler VPX 计数中的 2 个 VPX 以及 100 Mbps 的带宽。

有关此版本自适应身份验证服务中的增强功能、已修复问题以及已知问题的更多信息，请参阅 NetScaler 版本说明。

# 2025 年 11 月

以下部分提供了有关 2025 年 11 月版本发布的更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例将自动升级到版本 14.1–56.73 及更高版本，以解决 CTX695486 中描述的安全漏洞。

  有关此版本自适应身份验证服务中的增强功能、已修复问题以及已知问题的更多信息，请参阅 NetScaler 发行说明。

# 2025 年 6 月

以下部分提供了有关 2025 年 6 月版本发布的更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–47.46 及更高版本，以解决 CTX693420 和 CTX694788 中描述的安全漏洞。

  有关自适应身份验证服务此版本中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 发行说明。

## 已修复问题

- 当可用内存因内存泄漏而逐渐耗尽时，NetScaler® 可能会变得无响应且无法访问。

# 2024 年 10 月

以下各节提供了有关 2024 年 10 月版本的更多信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–34.101 及更高版本，以解决 CTX691608 中描述的安全漏洞。

  有关自适应身份验证服务此版本中的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 发行说明。

- **支持 RADIUS 负载平衡**

  Citrix 自适应身份验证实例现在支持 RADIUS 负载平衡。有关更多详细信息，请参阅 RADIUS 负载平衡配置示例。

- **支持将日志隧道传输到本地 syslog 服务器**

  在自适应身份验证部署中，客户现在可以将日志发送到其数据中心内的 syslog 服务器。配置 syslog 服务器时，请使用私有类 IP 地址 (RFC1918)。无需额外配置。

# 2024 年 1 月

以下部分提供了有关 2024 年 1 月版本更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例已自动升级到版本 14.1–12.35 及更高版本，以解决 CTX584986 中描述的安全漏洞。

  有关此版本自适应身份验证服务的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler 版本说明。

# 2023 年 9 月

以下部分提供了有关 2023 年 9 月版本更多信息。

## 新增功能

- **安全更新**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

自适应身份验证实例已自动升级到版本 14.1–8.50 及更高版本，以解决 CTX579459 中描述的安全漏洞。

有关此版本自适应身份验证服务的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler release notes。

# 2023 年 7 月

以下部分提供了有关 2023 年 7 月版本发布的更多信息。

## 新增功能

- **安全更新**

  自适应身份验证实例会自动升级到版本 13.1–49.101 及更高版本，以解决 CTX561482 中描述的安全漏洞。

  有关此版本自适应身份验证服务的增强功能、已修复问题和已知问题的更多信息，请参阅 NetScaler release notes。

# 2023 年 4 月

以下部分提供了有关 2023 年 4 月版本发布的更多信息。

## 新增功能

- **支持 LDAP 和 LDAPS 负载平衡**

  Citrix 自适应身份验证实例使用负载平衡虚拟服务器提供 LDAP 和 LDAPS 支持。有关更多详细信息，请参阅 Sample LDAP and LDAPS load balancing configuration。

- **将后端 AD 或 RADIUS 服务器子网映射到资源位置**

  管理员可以选择必须通过哪些连接器访问后端 AD 和 RADIUS 服务器。有关更多详细信息，请参阅 Provision Adaptive Authentication。

## 已修复问题

- 为自适应身份验证配置的智能访问策略和 OAuth 身份验证策略在 NetScaler GUI 中缺失。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 已知问题

- 对于自适应身份验证实例，当您使用 LDAP 配置文件（NetScaler 管理 GUI）中的**测试连接**选项检查连接性时，LDAP 服务器被错误地显示为可达，即使它实际上不可达。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 配置自适应身份验证服务

配置自适应身份验证服务涉及以下步骤。

1. 预置自适应身份验证
2. 配置自适应身份验证策略
3. 启用自适应身份验证

## 如何配置自适应身份验证服务

以下部分提供了有关配置自适应身份验证服务的更多信息。

### 访问自适应身份验证用户界面

您可以通过以下任一方法访问自适应身份验证用户界面。

- 手动键入 URL `<https://adaptive-authentication.cloud.com>`。
- 使用您的凭据登录并选择一个客户。

  成功通过身份验证后，您将被重定向到自适应身份验证用户界面。

或者

- 导航到 **Citrix Cloud™ > 身份和访问管理**。
- 在“身份验证”选项卡中，在“**自适应身份验证**”中，单击省略号菜单并选择“**管理**”。

自适应身份验证用户界面出现。

下图说明了配置自适应身份验证所涉及的步骤。

正在预置主页(/en-us/adaptive-authentication/media/adaptive-authentication-provisioning-main-page1.png)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意：**

- 请勿为任何自适应身份验证实例运行清除配置。
- 请勿修改任何带有前缀 `AA` 的配置（例如，AAuthAutoConfig），包括证书。这会扰乱自适应身份验证管理，并影响用户访问。
- 自适应身份验证实例不需要 SNIP 配置。
- 如果在客户设置中配置了代理，自适应身份验证实例将无法建立隧道。因此，建议您禁用自适应身份验证的代理配置。
- 如果您正在使用第三方身份验证服务（例如 SAML），则如果未找到所有声明，身份验证可能会失败。因此，建议客户在多因素身份验证配置中添加一个额外因素（例如 NOAUTH）以传递所有声明。

# 先决条件

- 请求自适应身份验证预配的访问权限。有关详细信息，请参阅云原生条件身份验证与基于 Netscaler 的自适应身份验证之间的比较。
- 为您的自适应身份验证实例保留一个 FQDN。例如，`aauth.xyz.com`，假设 `xyz.com` 是您的公司域。此 FQDN 在本文档中称为自适应身份验证服务 FQDN，并在预配实例时使用。将 FQDN 映射到 IdP 虚拟服务器的公共 IP 地址。此 IP 地址在预配后于“**上传证书**”步骤中获取。
- 为 aauth.xyz.com 获取证书。证书必须包含 SAN 属性。否则，证书将不被接受。
- 自适应身份验证 UI 不支持上传证书捆绑包。要链接中间证书，请参阅配置中间证书。
- 配置网络时间协议 (NTP) 服务器以避免时间偏差。有关详细信息，请参阅如何将系统时钟与网络上的服务器同步。

# 配置自适应身份验证实例

**重要提示：**

对自适应身份验证服务感兴趣的客户需要点击以下屏幕截图中所示的链接并填写表格。Citrix 自适应身份验证团队随后将启用自适应身份验证实例的配置。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 预配

1. 在**自适应认证** UI 上，点击**配置**。
2. 选择 **Citrix Cloud Connector™** 作为 Adaptive Authentication 的首选连接。

   连接类型(/en-us/adaptive-authentication/media/adaptive-authentication-step11.png)

   对于此连接类型，您必须在本地网络中设置连接器。Citrix 建议您在环境中部署至少两个 Citrix Cloud Connector，以设置与 Azure 上托管的 Citrix Gateway 的连接。您必须允许 Citrix Cloud Connector 访问您为 Adaptive Authentication 实例保留的域/URL。例如，允许 `<https://aauth.xyz.com/*>`。预配 Citrix Cloud Connector 可能需要长达 30 分钟才能完成设置。

   > **注意：**
   >
   > 对于连接器连接类型，请确保在预配后，您的 Adaptive Authentication FQDN 可从连接器虚拟机访问。

   有关 Citrix Cloud Connector 的详细信息，请参阅 Citrix Cloud Connector。
3. 单击 **Next** 转到 Console access 部分。

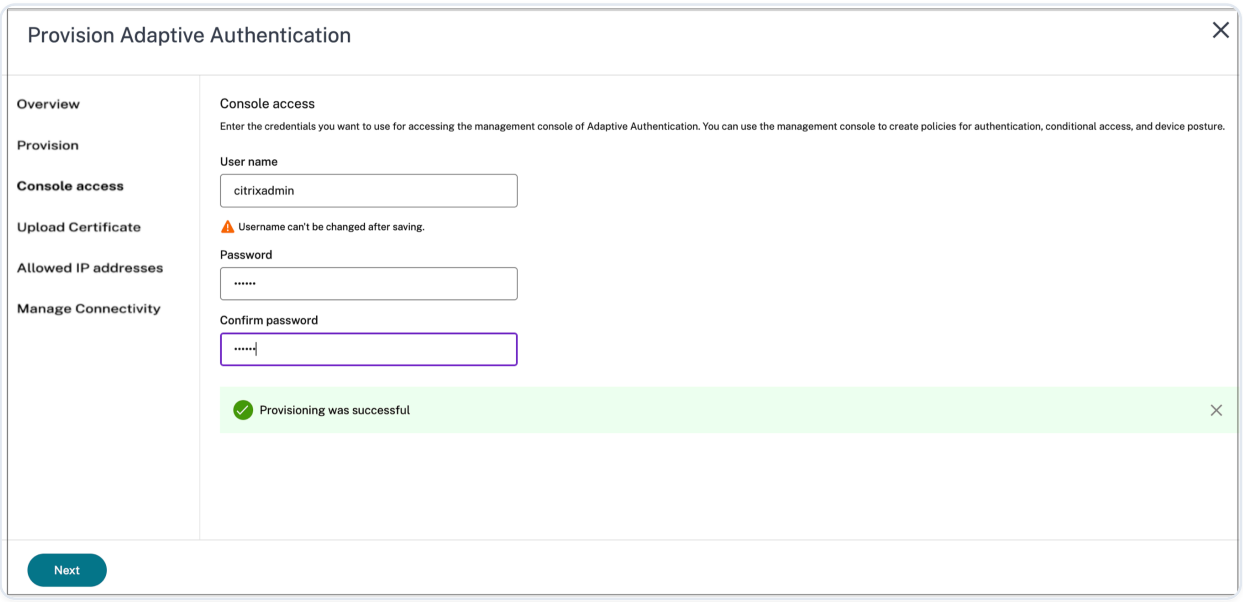
## 控制台访问

设置凭据以访问您已启用自适应身份验证的实例。您需要管理控制台访问权限才能创建身份验证、条件访问等策略。

1. 在**控制台访问**屏幕中，输入用户名和密码。

   > **注意：**
   >
   > 从**控制台访问**屏幕创建的用户被授予拥有 shell 访问权限的“超级用户”权限。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. 点击**下一步**以进入上传证书部分。

## 上传证书

**注意：**

建议通过自适应身份验证门户的用户界面执行上传证书配置，而不是直接在 NetScaler® 上（使用 GUI 或 CLI）。在 NetScaler 上所做的更改不会自动与自适应身份验证门户同步，并且可能会丢失。

1. 添加自适应身份验证服务 FQDN 并上传证书-密钥对。 您必须输入您选择的自适应身份验证服务 FQDN，用于可公开访问的身份验证服务器。此 FQDN 必须可公开解析。

   a. 在“**上传证书**”屏幕中，输入您为自适应身份验证预留的 FQDN。

   b. 选择证书类型。

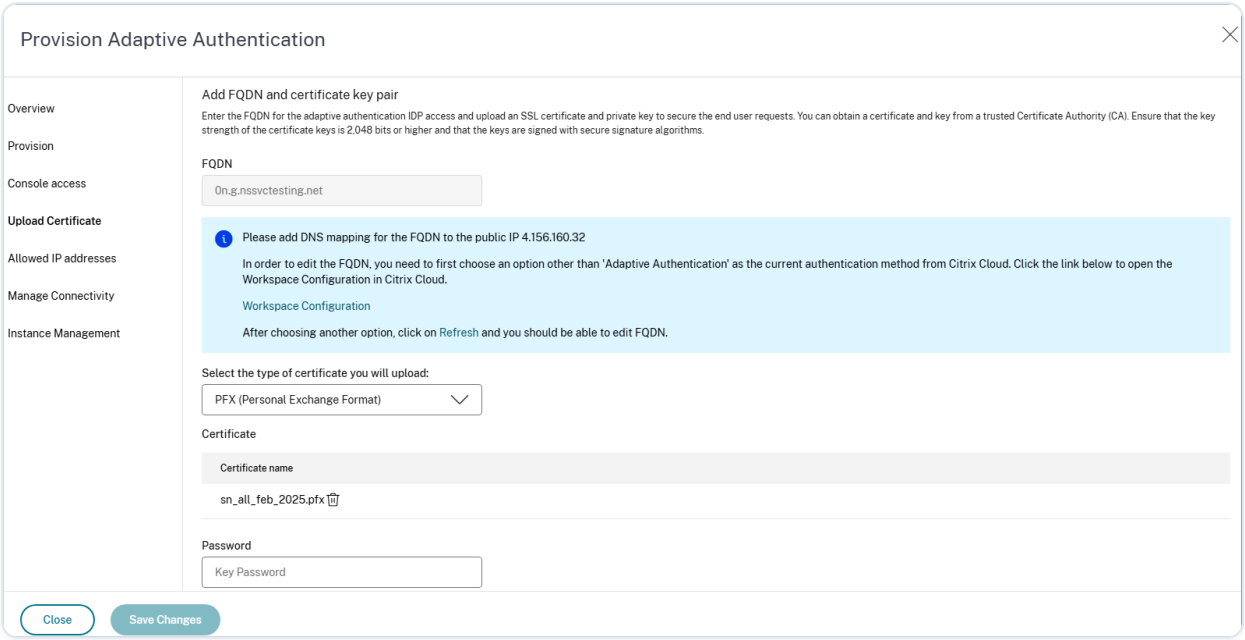
      - 自适应身份验证服务支持 PFX、PEM、DER 类型的证书用于实例预配。
      - 证书捆绑包仅支持 PEM 类型的证书。对于其他捆绑包类型，Citrix® 建议安装根证书和中间证书，并将其链接到服务器证书。

   c. 上传证书和密钥。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意：**

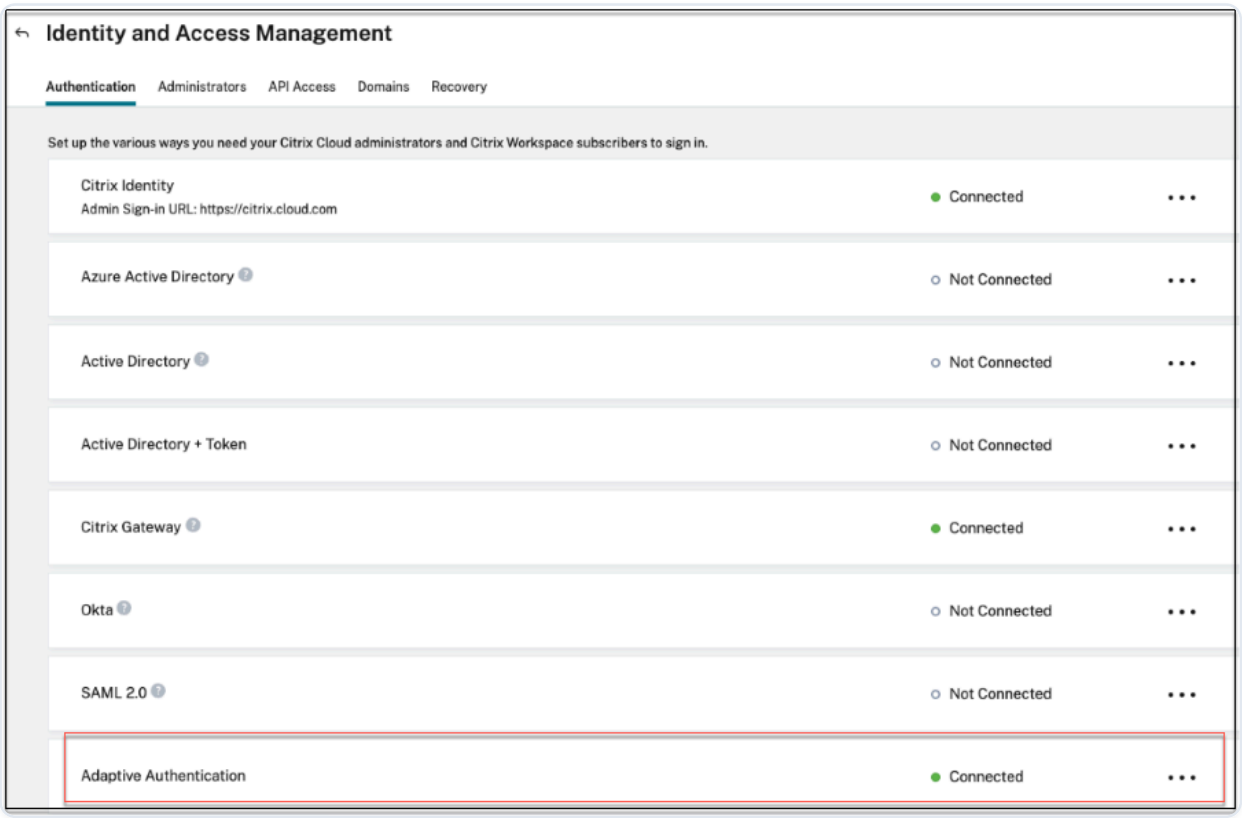
- 在自适应身份验证实例上安装您的中间证书，并将其与服务器证书链接。
  a. 登录到自适应身份验证实例。
  b. 导航到 **Traffic Management > SSL**。 有关详细信息，请参阅配置中间证书。
- 仅接受公共证书。不接受由私有或未知 CA 签名的证书。
- 证书配置或证书更新必须仅使用自适应身份验证 UI 完成。请勿直接在实例上更改，因为这可能导致不一致。




2. 上传证书和密钥。

证书上传成功后，自适应身份验证服务会自动连接到 Citrix Cloud™ 作为 IDP。可以从**身份和访问管理** UI 验证自适应身份验证服务的状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




3. 单击**下一步**转到允许的 IP 地址 部分。

## 允许的 IP 地址

自适应身份验证服务允许您输入最多 15 个公共 IP 子网和单个 IP 地址，以访问自适应身份验证 NetScaler® 管理控制台。

输入 IP 地址/子网时请注意以下几点：

- 确保公共 IP 子网的 CIDR 介于 /20 到 /32.B 之间。
- 确保条目之间没有重叠。

示例：

- 不接受 192.0.2.0/24 和 192.0.2.8，因为 192.0.2.8 位于 192.0.2.0/24 范围内。
- 重叠子网：不接受 192.0.2.0/24 和 192.0.0.0/20，因为子网重叠。
- 输入网络子网值时，请将网络 IP 地址作为 IP 地址值输入。

  示例：

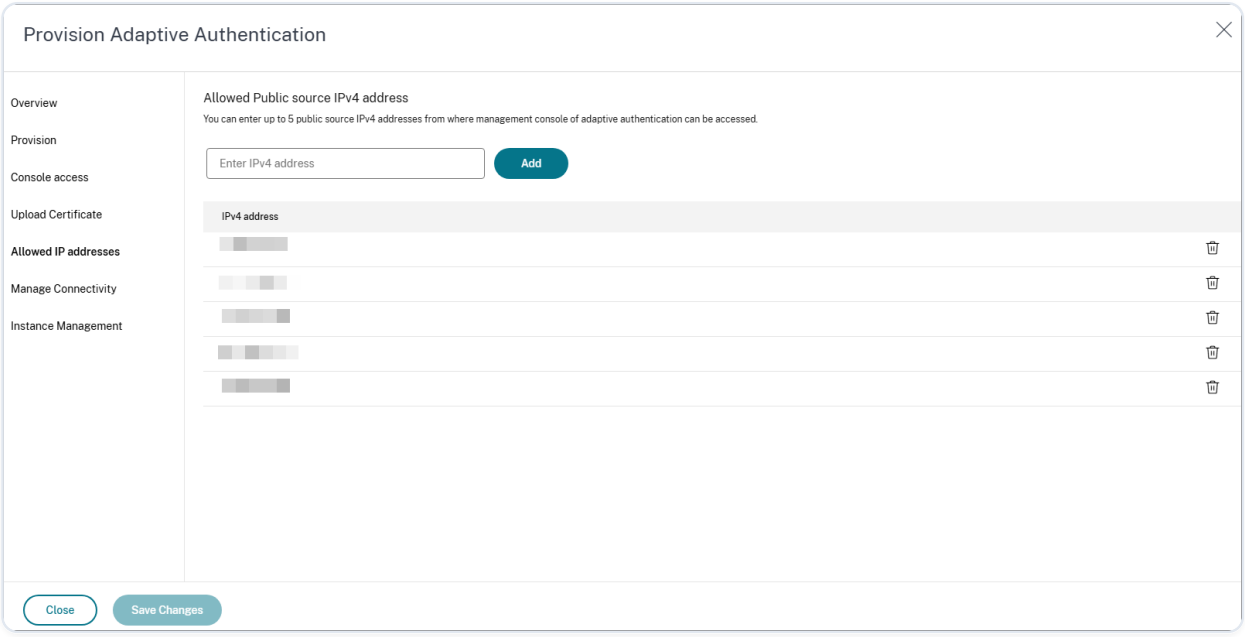
  - 192.0.2.2/24 不正确，请改用 191.0.2.0/24
  - 192.0.2.0/20 不正确，请改用 192.0.0.0/20

1. 设置一个 IP 地址，通过该地址可以访问自适应身份验证管理控制台。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. 在“**允许的 IP 地址**”屏幕中，对于每个实例，输入一个公共 IP 地址作为管理 IP 地址。要限制对管理 IP 地址的访问，您可以添加多个允许访问管理控制台的 IP 地址。

b. 要添加多个 IP 地址，您必须单击“**添加**”，输入 IP 地址，然后单击“**完成**”。每个 IP 地址都必须执行此操作。如果您不单击“**完成**”按钮，则 IP 地址不会添加到数据库中，而只会添加到用户界面中。



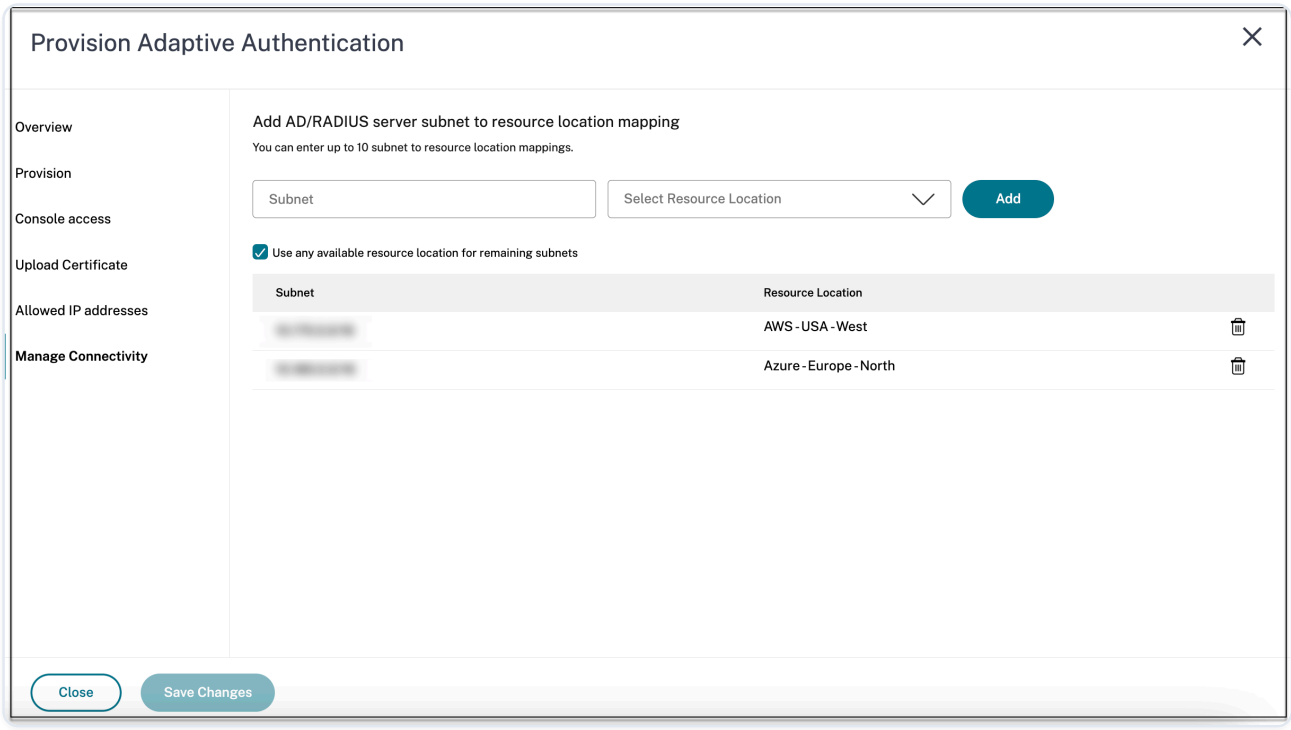

2. 点击 **下一步** 前往 管理连接 部分。

## 管理连接

您可以指定一组资源位置（连接器），通过这些位置可以访问 AD 或 RADIUS 服务器。管理员可以选择后端 AD 和 RADIUS 服务器必须通过哪些资源位置进行访问。

要启用此功能，客户可以在其后端 AD/RADIUS 服务器子网之间建立映射，以便如果身份验证流量属于特定子网，则该流量将定向到特定的资源位置。但是，如果资源位置未映射到子网，则管理员可以指定对这些子网使用通配符资源位置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**注意：**

建议通过自适应身份验证门户的用户界面而不是直接在 NetScaler® 上（使用 GUI 或 CLI）执行连接管理配置。在 NetScaler 上所做的更改不会自动与自适应身份验证门户同步，并且可能会丢失。

1. 在自适应身份验证 UI 上，单击**管理连接**。
2. 输入子网详细信息并选择相应的资源位置。

   **注意：**

   如果清除**对剩余子网使用任何可用的资源位置**复选框，则只有定向到已配置子网的流量才会被隧道传输。

3. 单击**添加**，然后单击**保存更改**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意：**

- 只允许 RFC1918 IP 地址子网。
- 每个客户的子网-资源位置映射数量限制为 10 个。
- 多个子网可以映射到一个资源位置。
- 要更新子网条目，请删除现有条目，然后进行更新。
- 如果您重命名或删除了资源位置，请务必从自适应身份验证用户界面中的“**管理连接**”屏幕中删除该条目。
- 通过使用以下 CLI 命令对资源位置映射所做的任何更改都将被从用户界面（**自适应身份验证预配 > 管理连接**）推送的更改覆盖。
  - set cloudtunnel parameter -subnetResourceLocationMappings
  - set policy expression aauth_allow_rfc1918_subnets <>
  - set policy expression aauth_listen_policy_exp <>

4. 单击“**下一步**”以转到实例管理部分。

## 实例管理

自适应身份验证团队负责管理自适应身份验证实例的所有升级和维护。因此，建议您不要将自适应身份验证实例升级或降级到随机 RTM 版本。Citrix® 默认管理自适应身份验证实例。

对于实例升级，VAR 目录中至少需要 7 GB 空间。因此，自适应身份验证服务团队会在应用升级之前清理实例上的磁盘空间。建议您不要在以下目录中保留任何敏感、专有或个人信息：

- /var/core
- /var/crash
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

© 1997–2026 Citrix Systems, Inc. All rights reserved.

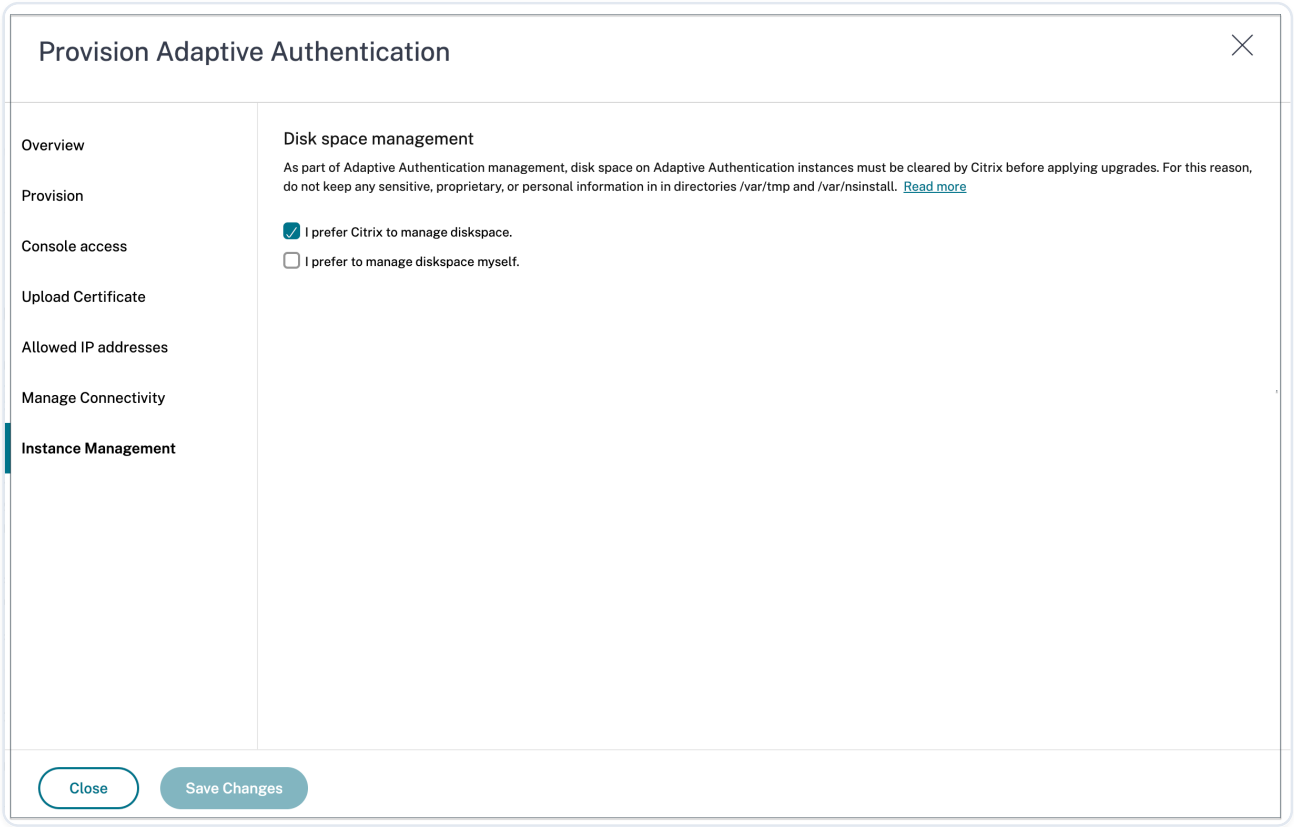
**注意：**

- 在升级期间，首先清除 /var/nsinstall 目录，然后清除 /var/tmp 目录。如果仍未满足最低空间要求，则其他目录（/var/core、/var/crash、/var/nstracem 和 /var/nslog）也会被清除。
- 客户负责管理和维护 NetScaler® 磁盘空间和磁盘清理。

**自行管理磁盘空间的选项：**

尽管 Citrix 默认管理自适应身份验证实例，但您可以选择自行清理实例上的磁盘空间。您可以通过执行以下操作来选择退出默认方法：

1. 在自适应身份验证导航窗格中，单击“**实例管理**”。
2. 选择**我更喜欢自己管理磁盘空间**，然后在确认消息对话框中点击**确认**。
3. 点击**保存更改**。



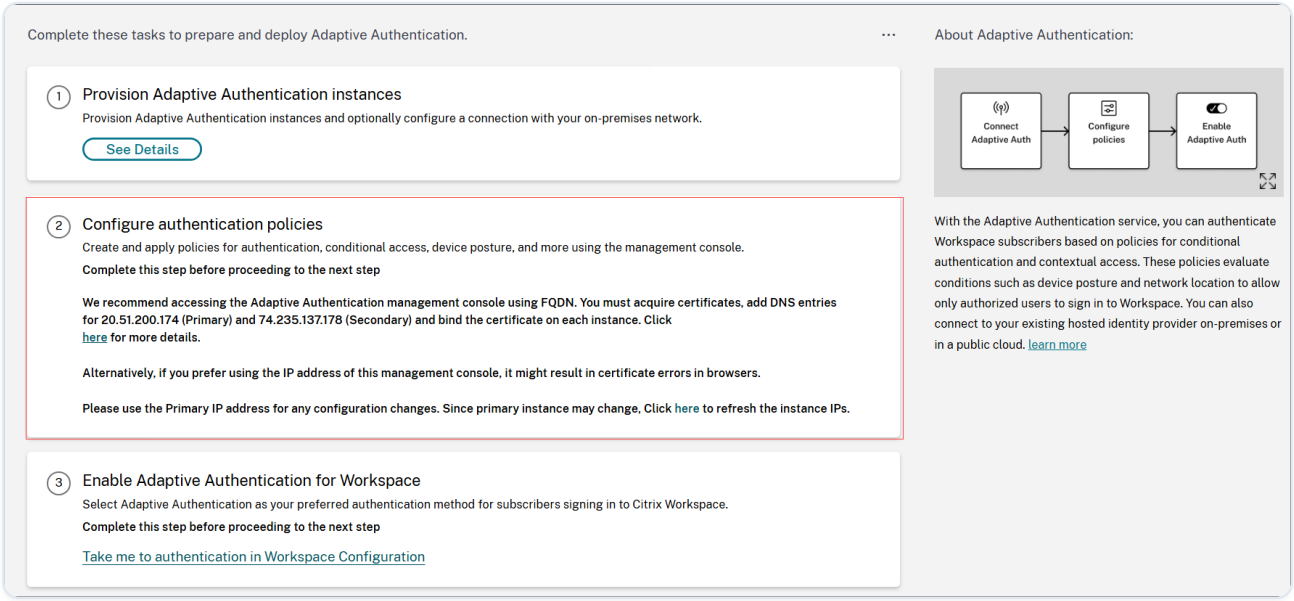

**注意：**

您还可以根据客户流量安排升级。Citrix Cloud™ 团队会相应地升级您的实例。 有关安排升级的信息，请参阅安排自适应身份验证实例的升级。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 配置策略

自适应身份验证 NetScaler® 实例的所有策略（例如，OAuth、智能访问和 syslog）都在自适应身份验证实例上配置。




**注意：**

- LDAP 或 RADIUS 操作的默认超时设置为 3 秒。我们建议将超时增加到 15 秒。
- 对于 RADIUS 服务器部署，请将所有连接器私有 IP 地址添加为 RADIUS 服务器中的 RADIUS 客户端。

**如何连接到您的自适应身份验证实例：**

预配后，您可以直接访问自适应身份验证管理 IP 地址。您可以使用 FQDN 或主 IP 地址访问自适应身份验证管理控制台。

**重要提示：**

要使用 FQDN 访问自适应身份验证管理控制台，请参阅为 ADC 管理员 UI 访问配置 SSL。

**访问自适应身份验证管理控制台：**

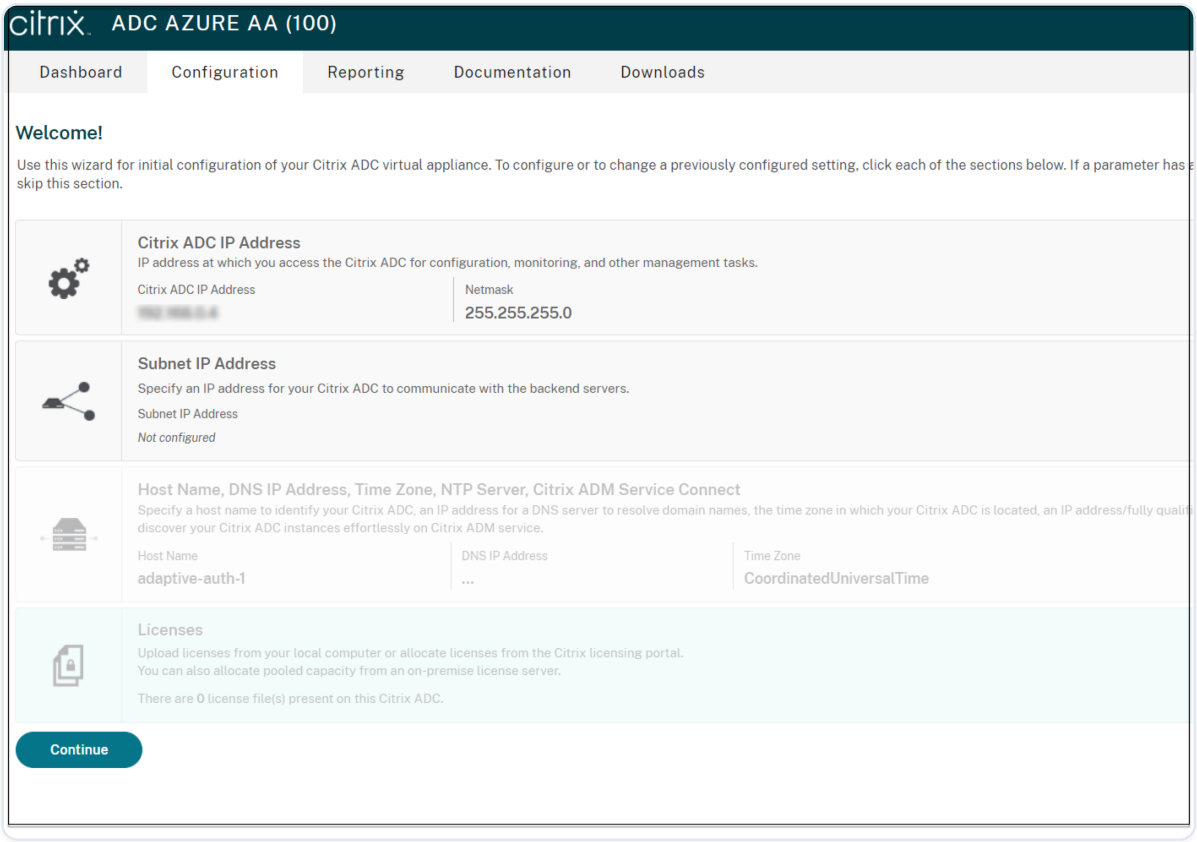
- 要使用主地址访问自适应身份验证，请执行以下操作：

  a. 从 GUI 的“**配置身份验证策略**”部分复制主 IP 地址，并在浏览器中访问该 IP 地址。

  b. 使用您在预配时输入的凭据登录。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 单击“**继续**”。




d. 导航到 **配置 > 安全 > AAA - 应用程序流量 > 虚拟服务器**。

e. 添加身份验证策略。有关各种用例，请参阅 LDAP 和 LDAPS 负载平衡配置示例 和 身份验证配置示例。

## 示例 LDAP 和 LDAPS 负载平衡配置

Citrix 自适应身份验证实例使用负载平衡虚拟服务器提供 LDAP/LDAPS 支持。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意：**

- 如果您不使用 LDAP/LDAPS 的负载平衡，请避免为 LDAP 服务器创建服务或服务器，因为这可能会破坏自适应身份验证隧道。
- 如果您正在使用 LDAP 的负载平衡，请创建一个服务组并将其绑定到负载平衡服务，而不是独立服务。
- 当使用负载平衡虚拟服务器进行身份验证时，请确保在 LDAP 操作中添加负载平衡虚拟服务器 IP 地址，而不是实际的 LDAP 服务器 IP 地址。
- 默认情况下，TCP 监视器绑定到您创建的服务。在自适应身份验证 NetScaler® 实例上，如果使用 TCP 监视器，则服务默认标记为 UP。
- 对于监视，建议您使用自定义监视器。

### 先决条件

负载平衡虚拟服务器的私有 IP 地址（RFC1918 地址）。它可以是一个虚拟 IP 地址，因为此地址用于内部配置。

### 负载平衡 LDAP 服务器

对于负载平衡 LDAP 服务器，请创建一个服务组并将其绑定到负载平衡虚拟服务器。不要为负载平衡 LDAP 服务器创建服务。

#### 使用 NetScaler CLI 配置 LDAP：

您可以使用以下 CLI 命令作为配置 LDAP 的参考。

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>) <port>`
3. `add lb vserver <name> <serviceType> <ip> <port>` - 端口必须是 389。此端口用于内部通信，并且与本地服务器的连接通过 SSL 进行，具体取决于为服务组配置的端口。
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> {-serverIP} <ip_addr> | {-serverName <string>}} <lb vserver ip>`
6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

**使用 NetScaler GUI 配置 LDAP：**

1. 导航到 **流量管理 > 负载平衡**，然后单击 **虚拟服务器**。
2. 创建类型为 TCP 且端口为 389 的虚拟服务器。

   不要创建类型为 SSL/SSL_TCP 的负载平衡虚拟服务器。
3. 导航到 **流量管理 > 负载平衡**，然后单击 **服务组**。
4. 创建类型为 TCP 且端口为 389 的服务组。
5. 将服务组绑定到您在步骤 1 中创建的虚拟服务器。

有关详细步骤，请参阅 设置基本负载平衡。

### LDAPS 服务器负载平衡

为了对 LDAPS 服务器进行负载均衡，您必须创建一个 TCP 类型的负载均衡虚拟服务器，以避免在自适应身份验证实例中进行内部 SSL 加密或解密。在这种情况下，负载均衡虚拟服务器会处理 TLS 加密/解密。不要创建 SSL 类型的负载均衡虚拟服务器。

**使用 NetScaler CLI 配置 LDAPS：**

您可以使用以下 CLI 命令作为配置 LDAPS 的参考。

1. `add lb vserver <name> <serviceType> <ip> <port>` - 端口必须是 636。
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> {-serverIP} <ip_addr> | {-serverName <string>}} <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

**使用 NetScaler GUI 配置 LDAPS：**

1. 导航到 **流量管理 > 负载均衡**，然后单击 **虚拟服务器**。
2. 创建 TCP 类型且端口为 636 的虚拟服务器。

   不要创建 SSL/SSL_TCP 类型的负载均衡虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 导航到 **流量管理 > 负载均衡**，然后单击 **服务**。
4. 创建 SSL_TCP 类型且端口为 636 的服务。
5. 将服务绑定到您在步骤 1 中创建的虚拟服务器。

有关这些过程的详细信息，请参阅 设置基本负载平衡。

### 创建自定义监视器

**使用 NetScaler GUI 创建自定义监视器：**

1. 导航到 **流量管理 > 负载平衡 > 监视器**。
2. 创建 LDAP 类型的监视器。确保将监视器探测间隔设置为 15 秒，将响应超时设置为 10 秒。
3. 将此监视器绑定到您的服务。

有关更多详细信息，请参阅 自定义监视器。

## RADIUS 负载均衡配置示例

Citrix 自适应身份验证实例通过负载均衡虚拟服务器提供 RADIUS 支持。

**注意：**

- 如果您不使用 RADIUS 的负载均衡，请避免为 RADIUS 服务器创建服务或服务器，因为这可能会破坏自适应身份验证隧道。
- 如果您正在使用 RADIUS 的负载均衡，请创建一个服务组并将您的 RADIUS 服务器绑定到该服务组。
- 当使用负载均衡虚拟服务器进行身份验证时，请确保在 RADIUS 操作中添加负载均衡虚拟服务器的 IP 地址，而不是实际的 RADIUS 服务器 IP 地址。
- 默认情况下，ping 监视器绑定到您创建的服务。在自适应身份验证 NetScaler® 实例上，服务将无法使用 ping 监视器启动。您需要创建 RADIUS 监视器并将其绑定到您已创建的服务组。
- 对于监视，建议您使用自定义监视器。
- 不支持 Ping 监视器，您必须创建 RADIUS 监视器。

### 先决条件

负载均衡虚拟服务器的私有 IP 地址（RFC1918 地址）。它可以是一个虚拟 IP 地址，因为此地址用于内部配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

### 负载均衡 RADIUS 服务器

对于负载均衡 RADIUS 服务器，请创建一个服务组并将其绑定到负载均衡虚拟服务器。不要为负载均衡 RADIUS 服务器创建服务。

#### 使用 NetScaler CLI 配置 RADIUS

您可以使用以下 CLI 命令作为配置 RADIUS 的参考。

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>) <port>`
3. `add lb vserver <name> <serviceType> <ip> <port>`
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication radiusAction <name> {-serverIP} <ip_addr> | {-serverName <string>}} <lb vserver ip>`
6. `add authentication policy <radius_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <radius_policy_name> -priority <radius_policy_priority> -gotoPriorityExpression NEXT`

#### 使用 NetScaler GUI 配置 RADIUS

1. 导航到 **流量管理 > 负载平衡**，然后单击 **虚拟服务器**。
2. 创建类型为 **RADIUS** 的虚拟服务器。
3. 导航到 **流量管理 > 负载平衡**，然后单击 **服务组**。
4. 创建类型为 **RADIUS** 的服务组。
5. 将服务组绑定到您在步骤 1 中创建的虚拟服务器。

有关详细步骤，请参阅 设置基本负载平衡。

#### 使用 NetScaler GUI 创建自定义监视器

1. 导航到 **流量管理 > 负载均衡 > 监视器**。
2. 创建一个 RADIUS 类型的监视器。确保将监视器探测间隔设置为 15 秒，响应超时设置为 10 秒。
3. 将此监视器绑定到您的服务组。

有关更多详细信息，请参阅 自定义监视器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 示例身份验证配置

客户可以配置他们选择的身份验证策略，并将其绑定到身份验证虚拟服务器。身份验证虚拟服务器不需要身份验证配置文件绑定。只能配置身份验证策略。以下是一些用例。

**重要提示：**

身份验证配置只能在主节点上完成。

### 带条件身份验证的多因素身份验证

- 使用双因素方案（仅一次用户输入）通过 LDAP 和 RADIUS 进行双因素身份验证
- 根据组织中用户的部门（员工、合作伙伴、供应商）使用下拉菜单选择部门的身份验证登录方法
- 根据用户域使用下拉菜单的身份验证登录方法
- 将电子邮件 ID（或用户名）输入配置为第一因素，并根据第一因素的电子邮件 ID 进行组提取的条件访问，并为每个组提供不同的登录类型
- 对拥有用户证书的用户使用证书身份验证，对非证书用户使用本机 OTP 注册的多因素身份验证
- 根据用户主机名输入的不同身份验证类型与条件身份验证
- 使用本机 OTP 身份验证的双因素身份验证

### 与多因素身份验证的第三方集成

- 将 Azure AD 配置为 SAML IdP（将下一因素配置为 LDAP 策略 - NO_AUTH 以完成 OAuth 信任）
- 以 SAML 作为第一因素的条件身份验证，然后根据 SAML 属性自定义登录到证书或 LDAP
- 第一因素为 webauth 登录，然后是 LDAP

### 设备姿态扫描 (EPA)

- 设备姿态检查（版本检查），然后是合规用户（RADIUS）和不合规用户（LDAP）的自定义登录
- LDAP 身份验证，然后是强制设备姿态扫描
- AD 身份验证前后的设备姿态检查 - 将预 EPA 和后 EPA 作为因素
- 设备证书作为 EPA 因素

### 其他场景

- 在身份验证中添加 EULA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 自定义 nFactor 策略标签、登录架构

## 支持自定义商店 URL

自定义商店 URL 允许您使用您选择的域来访问您的云商店。用户可以使用云商店 URL、自定义商店 URL 或两者来访问。

要配置自定义 URL，您必须执行以下操作：

1. 配置您的自定义域。有关详细信息，请参阅 配置您的自定义域。
2. 配置一个新的 OAuthIDP 配置文件，其客户端 ID、密钥和受众与您当前或默认配置文件 (AAuthAutoConfig_oauthIdpProf) 相同，但重定向 URL 不同。有关详细信息，请参阅 配置 OAuth 策略和配置文件。

   **示例：**

   当前配置文件：

   ```
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://accounts-internal.cloud.com/core/login-cip" -audience zzzz -sendPassword ON
   ```

   ```
   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -rule true -action AAuthAutoConfig_oauthIdpProf
   ```

   ```
   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol -priority 100 -gotoPriorityExpression NEXT
   ```

   新配置文件：

   ```
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1 -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://custom_domain/core/login-cip" -audience zzzz -sendPassword ON
   ```

   ```
   add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1 -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1
   ```

   ```
   bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Custom1 -priority 101 -gotoPriorityExpression NEXT
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要提示：**

- OAuth 策略和配置文件在预配阶段由自适应身份验证服务创建。因此，Citrix Cloud 管理员无法访问未加密的客户端密钥。您可以从 ns.conf 文件中获取加密密钥。要创建 OAuth 配置文件，您必须使用加密密钥并仅使用 CLI 命令创建配置文件。
- 您无法使用 NetScaler® 用户界面创建 OAuth 配置文件。

## 支持使用自适应身份验证的智能访问

Citrix Cloud™ 客户可以使用自适应身份验证作为 IdP 到云存储，为 Citrix DaaS 资源（虚拟应用和桌面）或安全私有访问服务提供智能访问（自适应访问）。

智能访问功能允许自适应身份验证服务将所有关于用户的策略信息呈现给 Citrix DaaS。自适应身份验证服务可以提供设备姿态 (EPA)、网络位置（公司网络内部或外部、地理位置）、用户属性（如用户组）、一天中的时间或这些参数的组合作为策略信息的一部分。Citrix DaaS 管理员随后可以使用此策略信息来配置对虚拟应用和桌面的上下文访问。虚拟应用和桌面可以根据之前的参数（访问策略）进行枚举或不枚举。某些用户操作，例如剪贴板访问、打印机重定向、客户端驱动器或 USB 映射，也可以进行控制。

示例用例：

- 管理员可以配置仅限从特定网络位置（如公司网络）显示或访问的应用程序组。
- 管理员可以配置仅限从公司托管设备显示或访问的应用程序组。例如，EPA 扫描可以检查设备是公司托管设备还是 BYOD 设备。根据 EPA 扫描结果，可以为用户枚举相关的应用程序。

### 先决条件

- 将自适应身份验证配置为云存储的身份验证方法。有关详细信息，请参阅 自适应身份验证服务。
- 与 Citrix DaaS 配合使用的自适应身份验证服务已启动并正在运行。
- 自适应访问功能已启用。有关详细信息，请参阅 启用自适应访问。

### 了解智能访问的事件流

1. 用户登录到其云存储。
2. 用户被重定向到配置为 IdP 的自适应身份验证服务。
3. 系统提示用户进行预身份验证 (EPA) 或身份验证。
4. 用户已成功通过身份验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 智能访问策略根据配置进行评估，并将标签与用户会话关联。
6. 自适应身份验证服务将标签推送到 Citrix Graph 服务。用户将被重定向到商店登录页面。
7. StoreFront Cloud 为此用户会话获取策略信息，匹配过滤器，并评估必须枚举的应用程序或桌面。
8. 管理员在 Citrix DaaS 上配置访问策略，以限制用户的 ICA® 访问。

### 在自适应身份验证实例上配置智能访问策略

在自适应身份验证实例上配置智能访问策略是一个两步过程：

1. 在自适应身份验证实例上使用智能访问标签定义智能访问策略。例如，请参阅 *步骤 1*。
2. 在您的 DaaS/Secure Private Access 上定义相同的标签以进行资源访问。例如，请参阅 *步骤 2*。

**用例 1：配置智能访问策略以允许从 Chrome 浏览器登录的用户访问，并阻止其剪贴板访问**

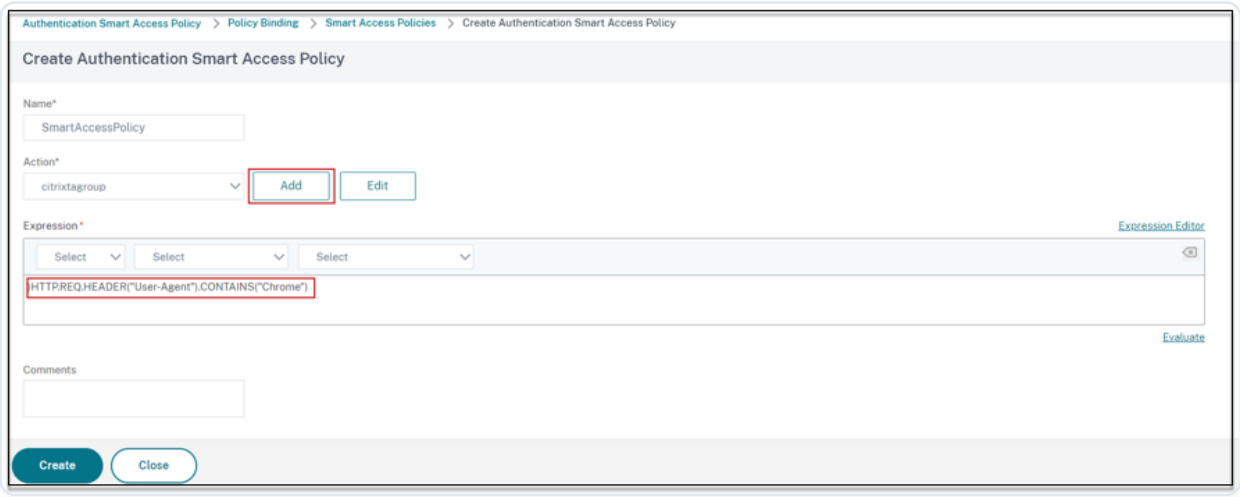
**步骤 1：在自适应身份验证实例上配置带有智能标签的智能访问策略：**

1. 登录到自适应身份验证实例。
2. 导航到自适应身份验证虚拟服务器（**安全 > AAA - 应用程序流量 > 虚拟服务器**）。
3. 选择身份验证虚拟服务器，然后单击**编辑**。
4. 单击**智能访问策略**。
5. 根据您的要求定义策略表达式。
    a. 单击“**添加绑定**”。
    b. 在“**选择策略**”中，单击“**添加**”。
    c. 输入智能访问策略的名称。
    d. 定义表达式。

    例如，对于允许从 Chrome 浏览器登录的用户访问，请输入表达式 `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")`

    同样，您可以根据时间、用户登录、身份验证和授权组以及其他选项创建表达式。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

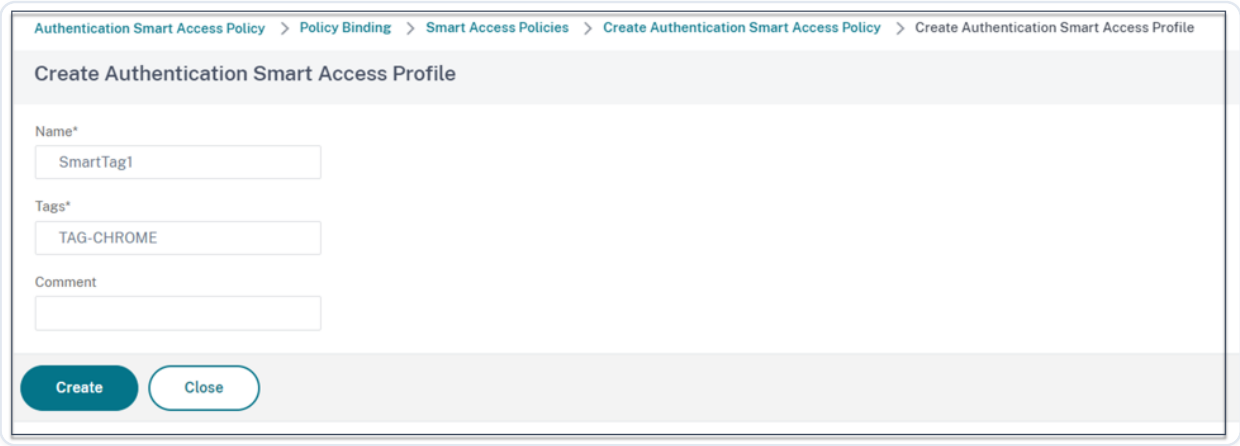



6. 现在，创建智能标签并将这些标签绑定到智能访问策略。

   a. 在“**操作**”中，单击“**添加**”。

   b. 在“**名称**”中，键入智能访问配置文件的名称。

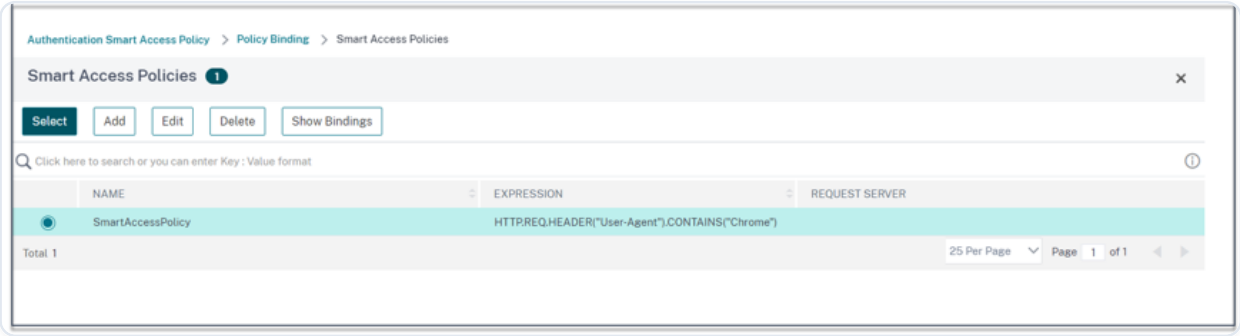
   c. 在“**标签**”中，定义智能访问标签。例如，TAG-CHROME。




   a. 单击“**创建**”。

   b. 选择智能访问策略，然后单击“**添加绑定**”。

   c. 将此智能访问标签绑定到之前创建的智能访问策略。




© 1997–2026 Citrix Systems, Inc. All rights reserved.

**注意：**

您还可以通过 **Security >AAA - Application Traffic > Policies > Authentication > Advanced Policies > Smart Access > Policies** 创建智能访问策略，然后将其绑定到身份验证虚拟服务器。

**步骤 2：在 DaaS Studio 中定义智能访问标签：**

1. 添加带有智能标签“TAG-CHROME”的策略。有关详细信息，请参阅在 Citrix Studio 中定义标签。

**用例 2：根据 EPA 结果配置智能访问策略，用于身份验证后**

**步骤 1：在 Adaptive Authentication 实例上配置带有智能标签的智能访问策略：**

对于基于端点分析等条件的智能访问，请配置 nFactor 流程，定义 EPA 操作，然后添加默认组。

要将 EPA 配置为 nFactor 流程中的一个因素，请参阅将 EPA 配置为一个因素。

**逻辑流程：**

1. 用户在 Web 浏览器或 Citrix Workspace 应用程序中打开其商店 URL。
2. 用户被重定向到 Adaptive Authentication 进行身份验证/EPA。
3. 对最终用户进行端点分析，并通过将用户添加到定义的默认组来存储结果。
4. 系统会提示用户进行下一个身份验证流程。
5. 评估智能访问策略，并为用户分配智能访问标签。

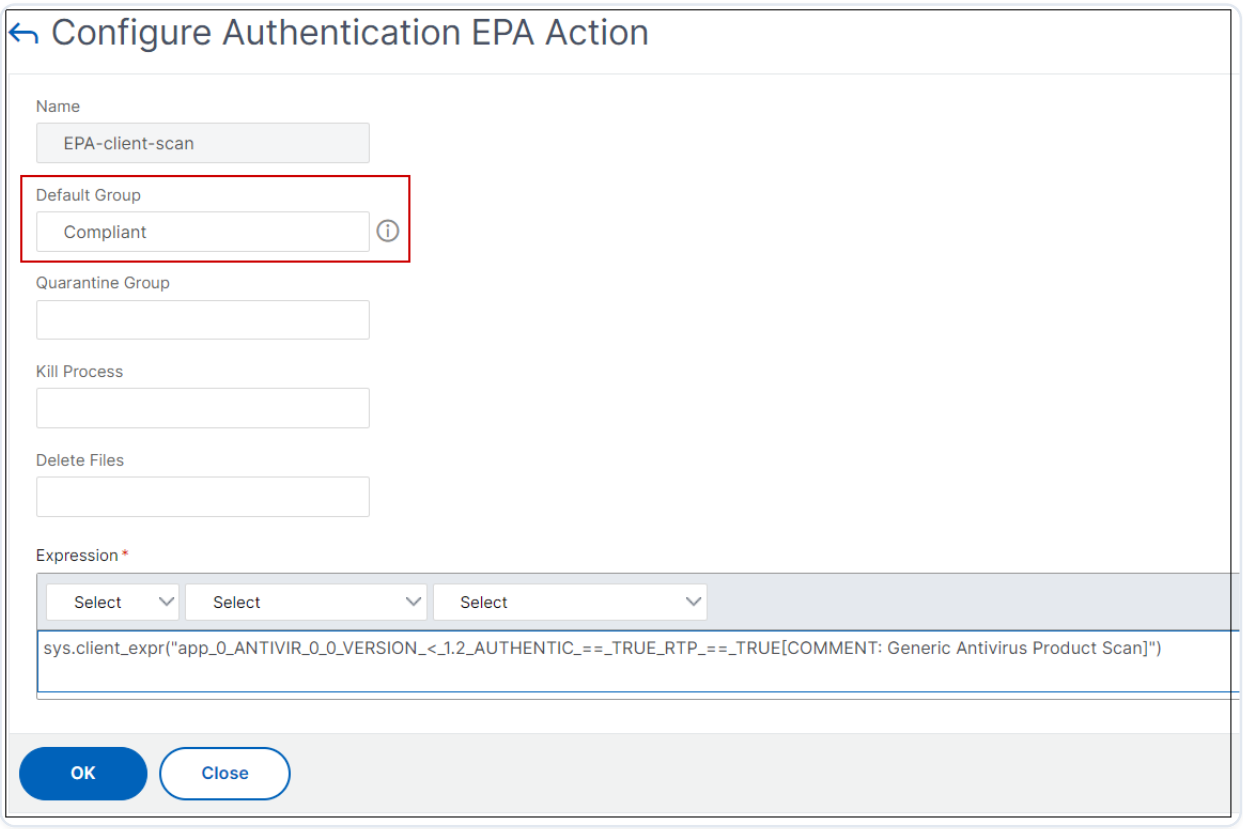
**配置：**

从安装了防病毒软件的计算机访问的用户必须标记为合规并提供完全访问权限。但是，未安装防病毒软件的用户计算机必须标记为不合规并提供有限访问权限。

1. 为 EPA 创建 nFactor 策略。有关详细信息，请参阅将 EPA 配置为因素。

   在 nFactor 流程中，确保第一个是用户身份验证因素。
2. 选择 EPA 表达式以检查防病毒软件是否存在。
3. 在 EPA 操作中定义默认组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




如果 EPA 成功运行，用户将被添加到此默认组。

4. 现在，创建智能访问策略

   a. 登录到 Adaptive Authentication 实例。

   b. 导航到自适应身份验证虚拟服务器 (**Security > AAA - Application Traffic > Virtual Servers**)。

   c. 选择 Adaptive Authentication 虚拟服务器，然后单击**编辑**。

   d. 单击**智能访问策略**。

   e. 使用以下表达式创建两个智能访问策略。

      - AAA.USER.IS_MEMBER_OF (“Compliant”) - 用于用户 EPA 通过条件
      - !AAA.USER.IS_MEMBER_OF (“Compliant”) – 用于用户 EPA 失败条件

   f. 为这两个策略定义智能访问标签。

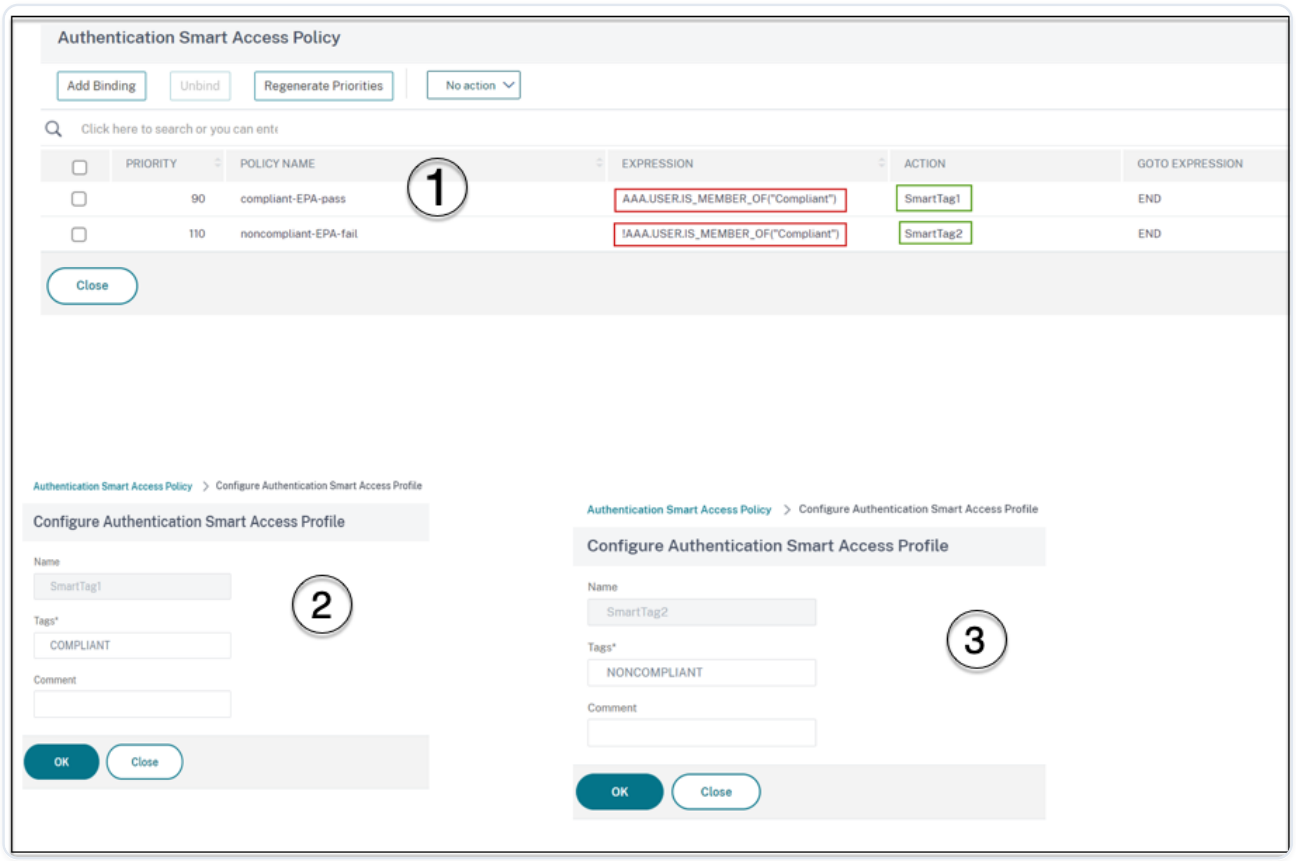
      示例：

      - 将名称 `SmartTag1` 标记为 COMPLIANT，用于 `AAA.USER.IS_MEMBER_OF (“Compliant”)`
      - 将名称 `SmartTag2` 标记为 NONCOMPLIANT，用于 `!AAA.USER.IS_MEMBER_OF (“Compliant”)`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

以 EPA 作为智能访问条件的自适应身份验证实例配置现已完成。

您可以根据您的要求配置标签和表达式。




**步骤 2：在 DaaS Studio 中配置智能访问标签：**

在相应的交付组中添加带有智能标签“COMPLIANT”和“NONCOMPLIANT”的策略。有关详细信息，请参阅在 Citrix Studio 中定义标签。

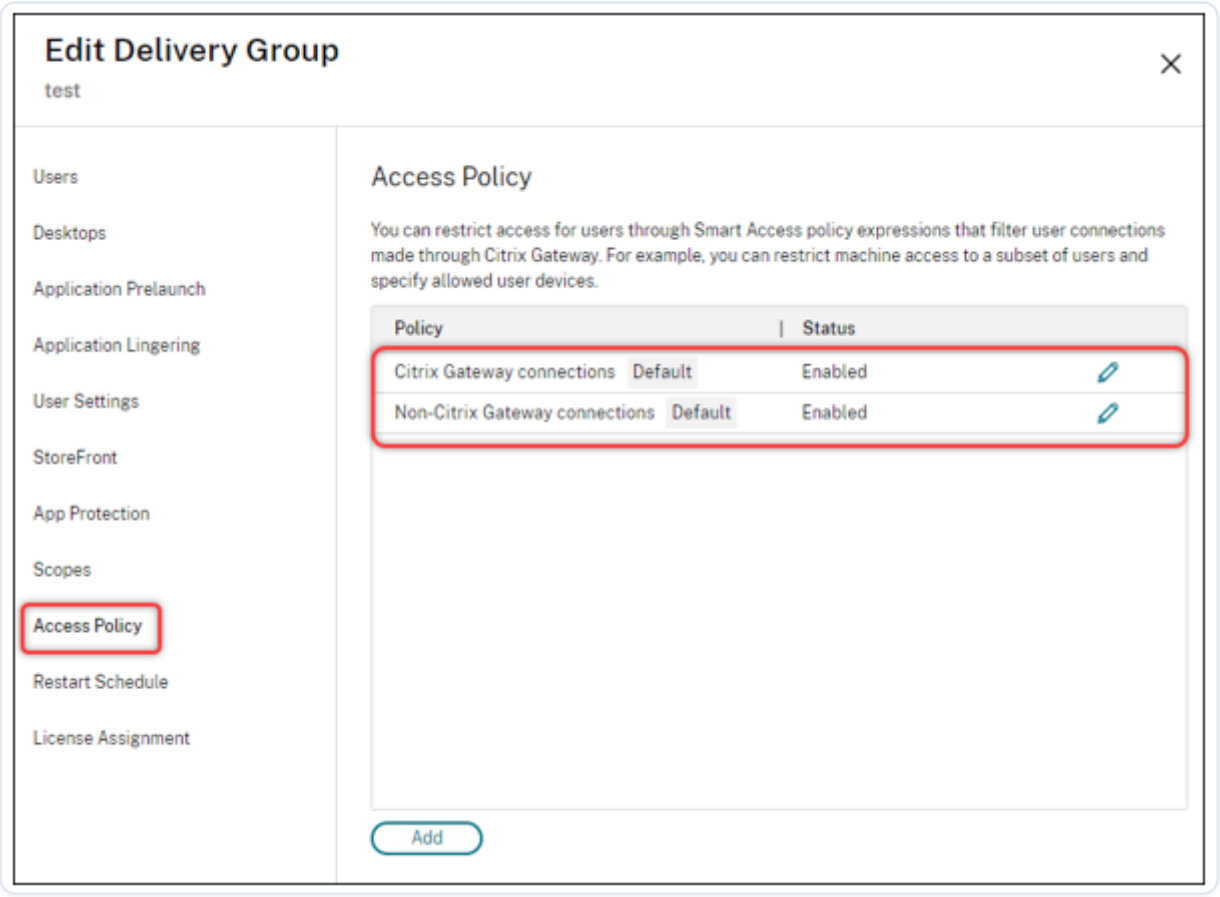
### 在 DaaS Studio 中定义标签

在交付组中定义标签以限制用户的应用程序枚举。

示例：分支机构用户必须查看来自包含所有应用程序的 **自适应访问交付组** 的应用程序。 而居家办公用户必须查看来自 **WFH 交付组** 的应用程序。

1. 登录到 Citrix Cloud。
2. 选择 **我的服务 > DaaS**。
3. 点击**管理**。
4. 根据您的要求创建交付组。有关详细信息，请参阅创建交付组。
5. 选择您已创建的交付组，然后点击**编辑交付组**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



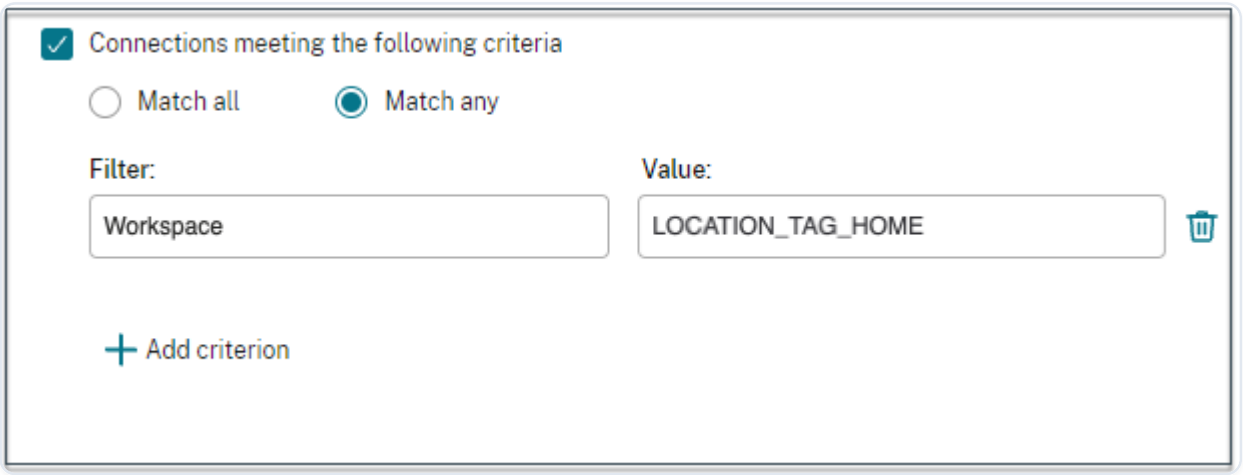

6. 点击**访问策略**。
7. 对于在 Citrix Workspace 平台中使用自适应访问的客户，请执行以下步骤，将交付组的访问权限限制为仅限内部网络：

   a. 右键点击交付组，然后选择**编辑**。

   b. 在左侧窗格中选择访问策略。

   c. 点击编辑图标以修改默认的 Citrix Gateway 连接策略。

   d. 在“编辑策略”页面上，选择**符合以下条件的连接**，选择**匹配任意**，然后添加条件。




对于居家办公用户，请在相应的交付控制器中输入以下值。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**场**：工作区

**筛选器**：LOCATION_TAG_HOME

对于分支机构用户，请在相应的交付控制器中输入以下值。

**筛选器**：工作区

**值**：LOCATION_TAG_BRANCHOFFICE

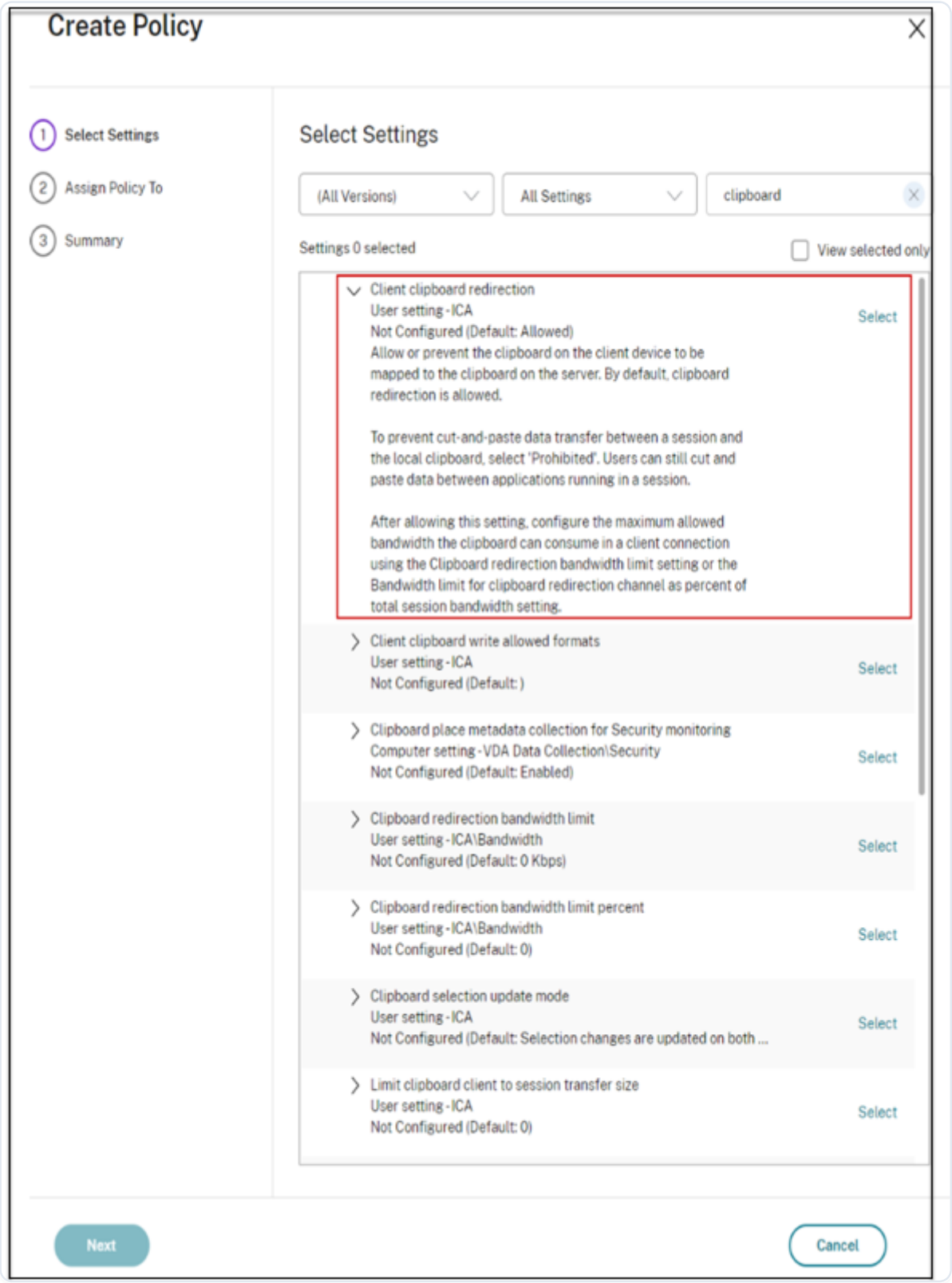
您现在可以使用这些标签来限制对应用程序的访问。

**限制对所提供应用程序的访问类型**

示例：居家办公用户不得拥有剪贴板权限。

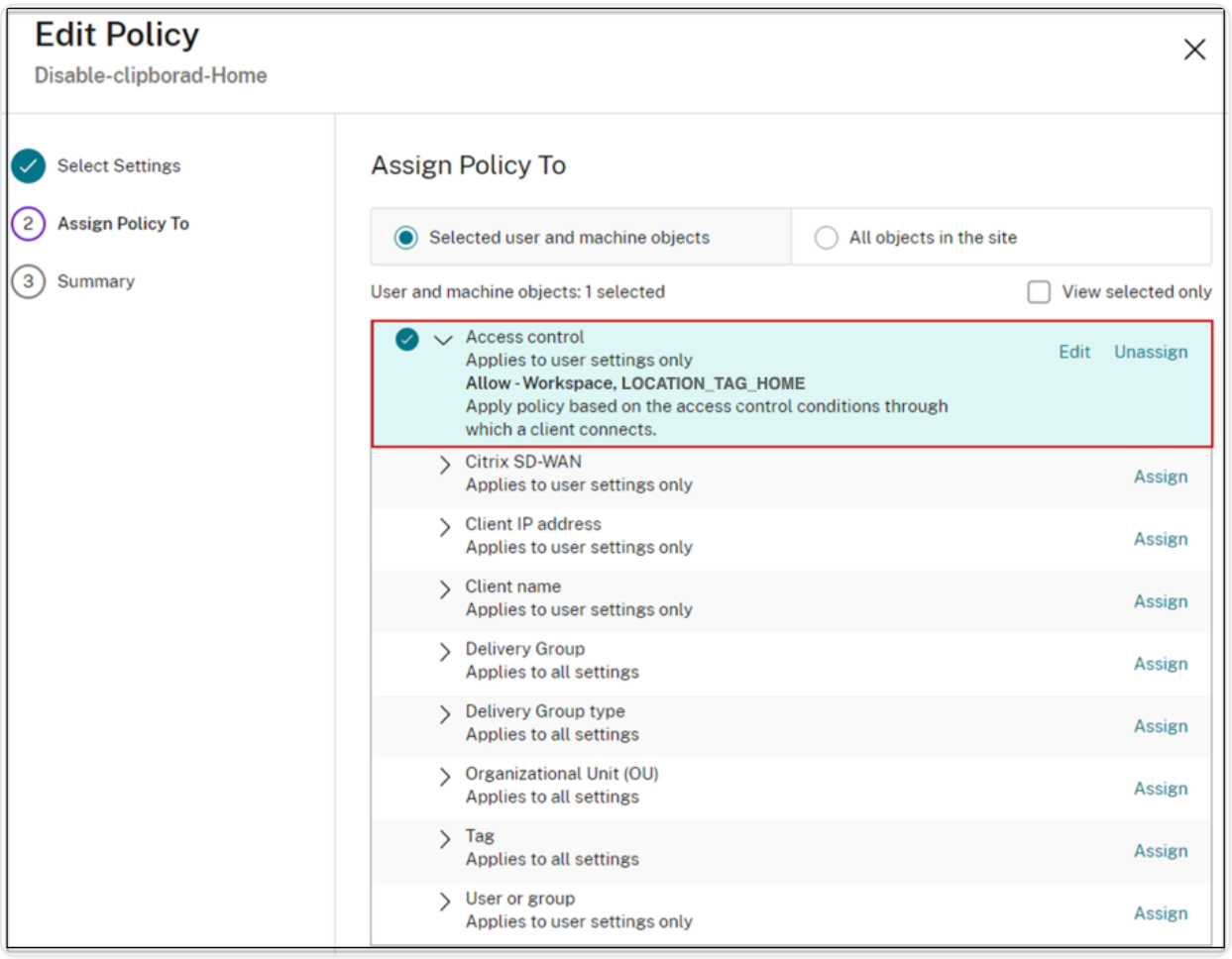
1. 在 DaaS Studio 中，导航到“**策略**”，然后单击“**创建策略**”。
2. 在“**创建策略**”页面中，选择要允许或禁止访问的设置。
3. 单击“**选择**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



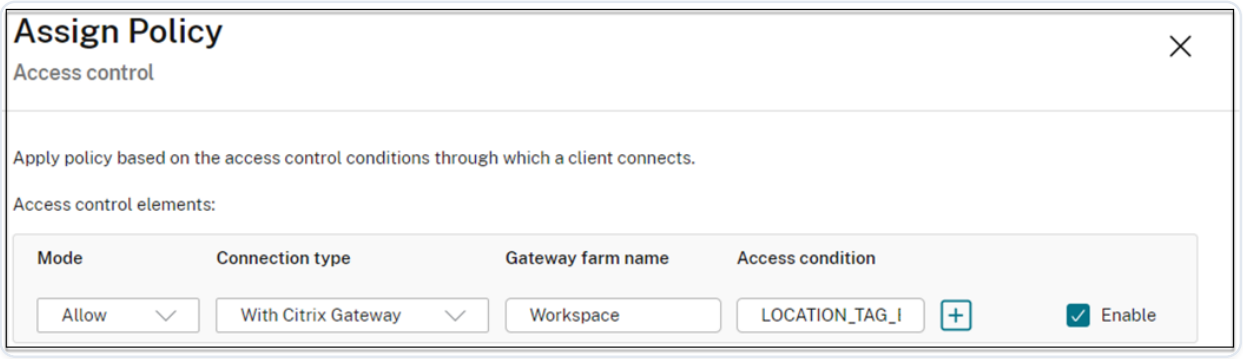

4. 在“**编辑设置**”页面中，单击“**允许**”或“**禁止**”，然后单击“**保存**”。
5. 单击“**下一步**”。
6. 在“**将策略分配到**”页面中，选择“**访问控制**”，然后单击“**下一步**”。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



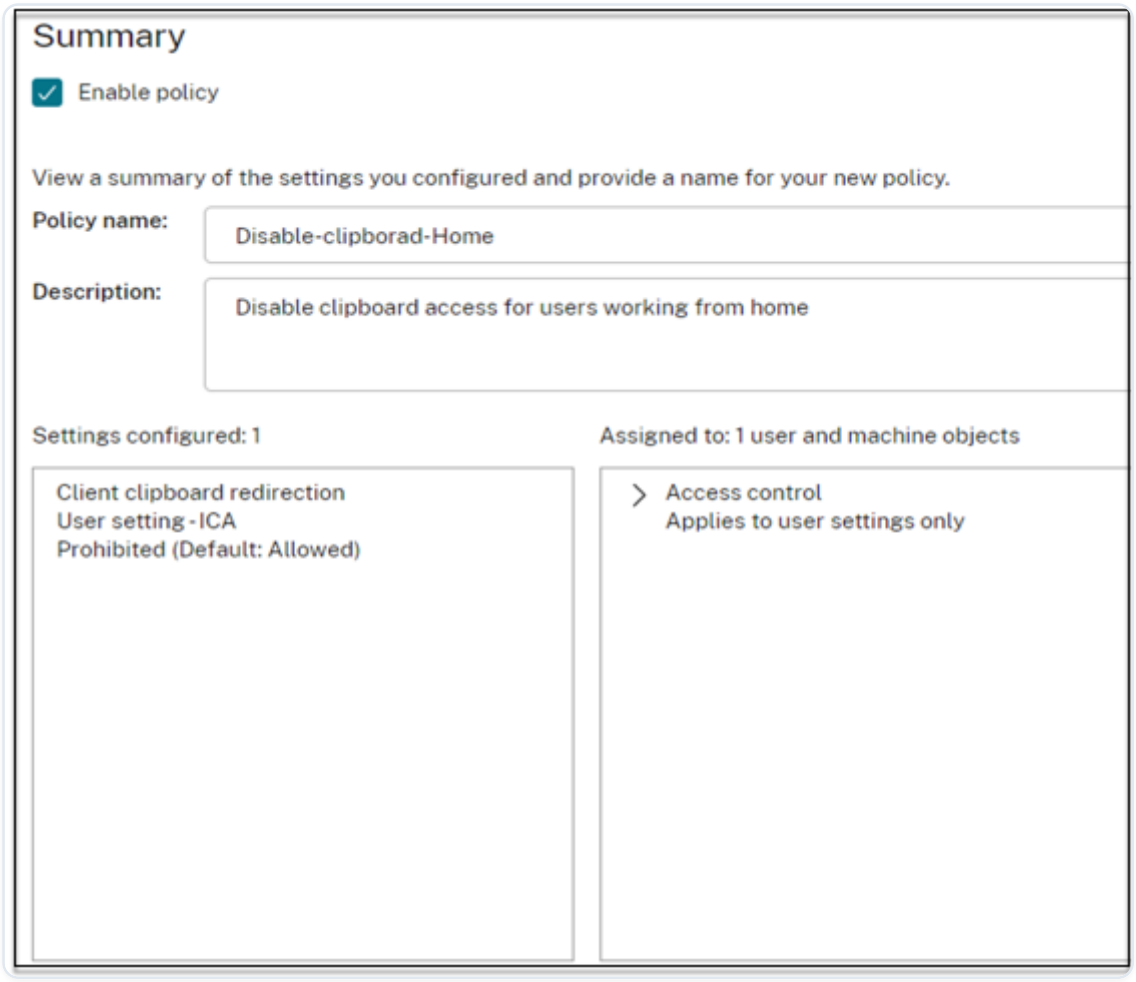

7. 使用以下详细信息定义策略：

   - **模式**：- 允许
   - **连接类型**：- 使用 Citrix Gateway
   - **场名称**：- 工作区
   - **访问条件**：LOCATION_TAG_HOME（全部大写）




8. 单击**下一步**，然后输入策略名称。
9. 单击**完成**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




您现在已准备好测试您的访问。

### 常见错误疑难解答

- **问题**：您看到消息“Cannot Complete your Request”。

  **解决方案**

  a. 确保已启用自适应访问。有关详细信息，请参阅启用自适应访问。

  b. 如果未启用该功能，请联系 Citrix 支持。

- **问题**：未发布任何应用程序或桌面。

  如果智能标签未从自适应身份验证推送到工作区，或者 DaaS 或安全专用访问未收到智能标签，则可能会出现此问题。

  **解决方案：**

  - 检查智能访问策略是否生效。有关详细信息，请参阅 <CTX138840。
  - 检查 Citrix Adaptive Authentication 实例是否能够连接到 `cas.citrix.com`。
  - 检查 Adaptive Authentication 实例以获取智能标签的详细信息。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 确保在 `set audit syslogParams` 命令中，logLevel 参数在所有实例上都设置为 `ALL`。
- 使用 putty 登录到 Adaptive Authentication 主实例。

  键入 shell

  `cd /var/log`

  `cat ns.log | more or cat ns.log | grep -I “smartaccess”`

- 如果这些操作无法解决问题，请联系 Citrix 支持。

### 高可用性设置的配置更改

有时，高可用性设置中的以下目录中可能会出现文件同步延迟。因此，在 Citrix ADM 注册期间创建的密钥无法及时读取。

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

为解决文件同步问题，请执行以下步骤以在辅助节点上重新运行 `set cloud` 命令。

```
> shell cat /var/mastools/conf/agent.conf

<?xml version="1.0" encoding="UTF-8" standalone="no"?>

<mps_agent>

<uuid>temp_str</uuid>

<url>fuji.agent.adm.cloud.com</url>

<customerid>customer_id</customerid>

<instanceid>instance_id</instanceid>

<servicename>MAS</servicename>

<download_service_url>download.citrixnetworkapistaging.net</
download_service_url>

<abdp_url>fuji.agent.adm.cloud.com</abdp_url>
```

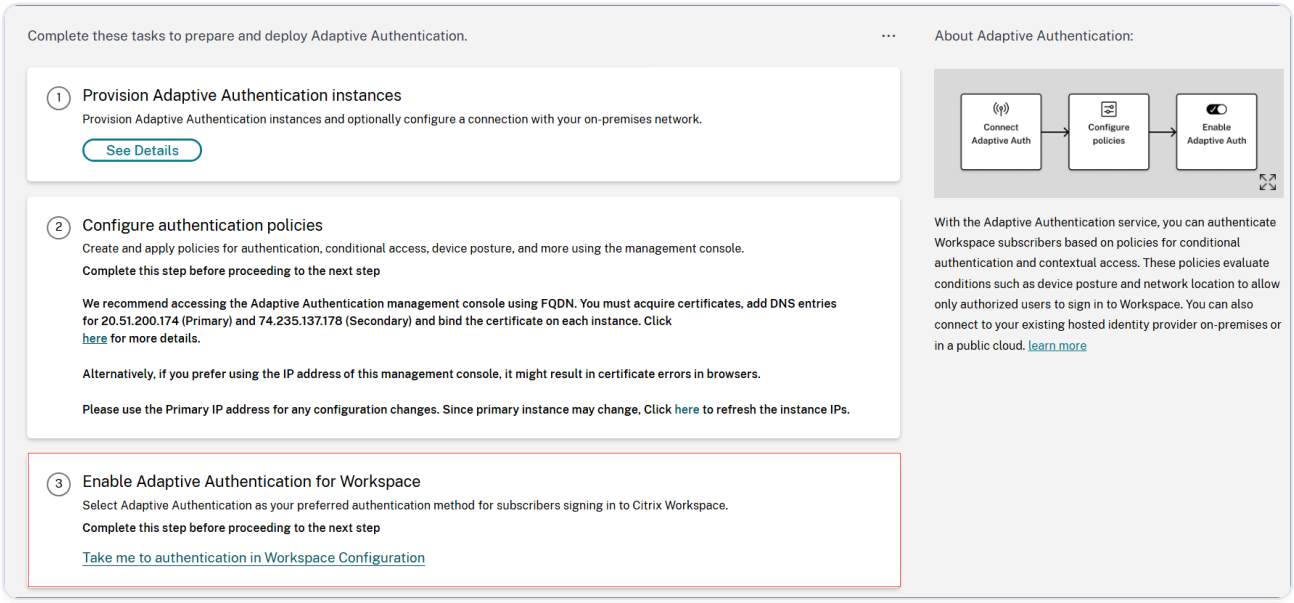
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>

</mps_agent> Done

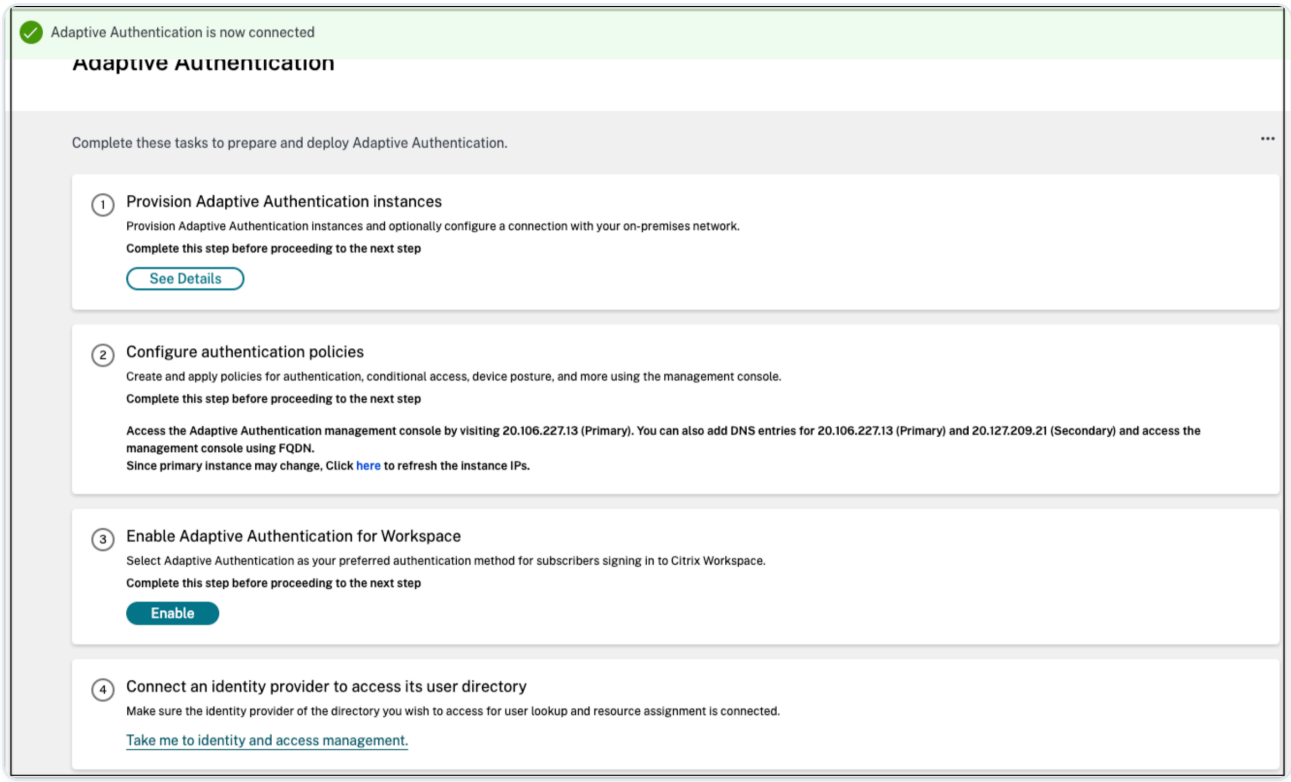
> set cloud param -CustomerID customer_id -InstanceID instance_id
-Deployment Production
```

# 启用自适应身份验证




预配完成后，您可以通过单击“**启用**”在“**为 Workspace 启用自适应身份验证**”部分中为云商店启用身份验证。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**注意：**

至此，自适应身份验证配置已完成。当最终用户访问其商店时，他们将被重定向到自适应身份验证 FQDN。

## 将您的身份验证方法迁移到自适应身份验证

已经使用自适应身份验证且身份验证方法为 **Citrix Gateway** 的客户必须迁移 **自适应身份验证**，然后从自适应身份验证实例中删除 OAuth 配置。

1. 切换到 Citrix Gateway 以外的其他身份验证方法。
2. 在 **Citrix Cloud™ > 身份和访问管理** 中，单击与 Citrix Gateway 对应的省略号按钮，然后单击 **断开连接**。

   断开网关连接(/en-us/adaptive-authentication/media/adaptive-authentication-different-authentication-method.png)
3. 选择 **我了解这对订阅者体验的影响**，然后单击 **确认**。

   单击 **确认** 后，在重新启用自适应身份验证之前，将不会使用自适应身份验证进行身份验证。
4. 在自适应身份验证实例管理控制台中，删除 OAuth 相关配置。

   通过使用 CLI：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
unbind authentication vs <authvsName> -policy <oauthIdpPolName>

rm authentication oauthIdpPolicy <oauthIdpPolName>

rm authentication oauthIdpProfile <oauthIdpProfName>
```

通过使用 GUI：

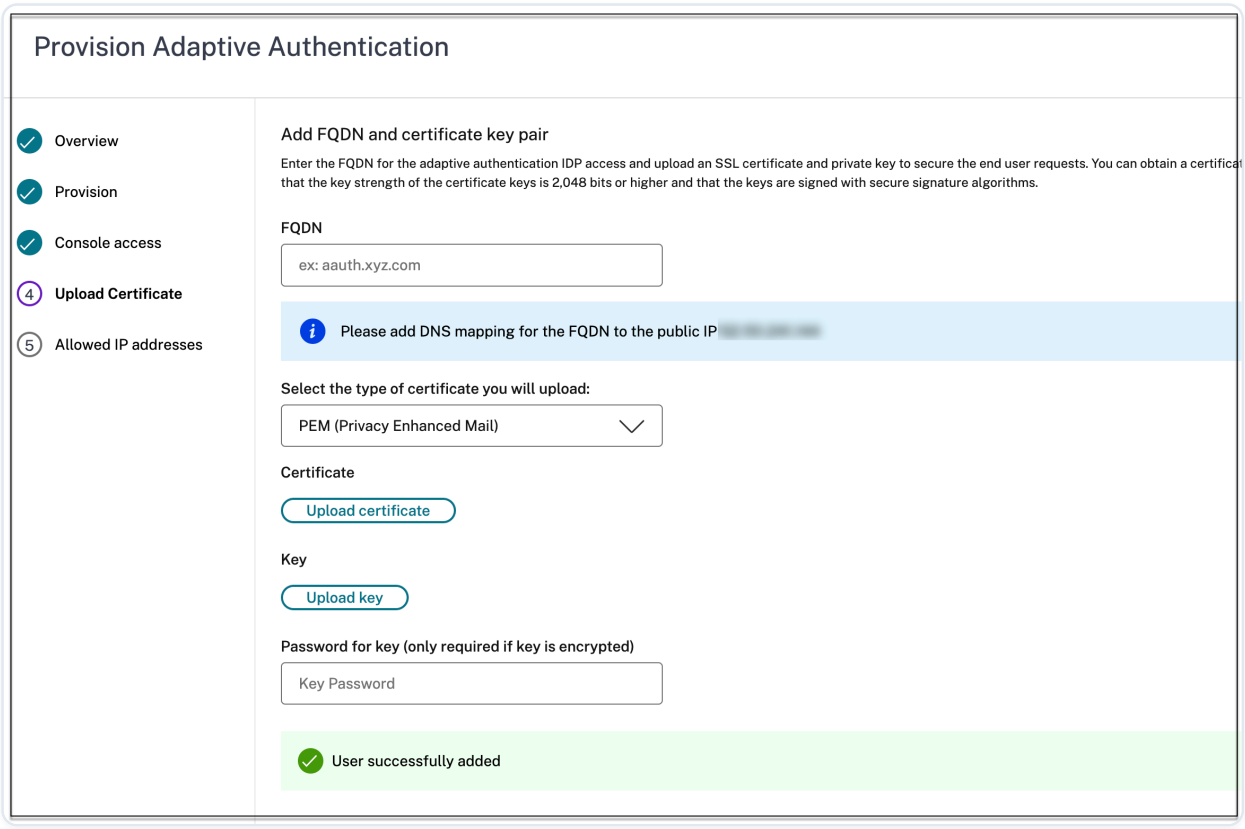
a. 导航到 **安全 > AAA - 应用程序流量 > 虚拟服务器**。
b. 解除绑定 OAuth 策略。
c. 导航到 **安全 > AAA - 应用程序流量 > 策略 > 身份验证 > 高级策略 > OAuth IDP**。
d. 删除 OAuth 策略和配置文件。

5. 导航到 **Citrix Cloud > 身份和访问管理**。 在“身份验证”选项卡中，在“自适应身份验证”下，单击省略号菜单并选择 **管理**。

   或访问 `<https://adaptive-authentication.cloud.com>`
6. 点击 **查看详细信息**。
7. 在 **上传证书**屏幕中，执行以下操作：

   - 添加自适应身份验证 FQDN。
   - 删除证书和密钥文件并重新上传。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




**重要提示：**

如果您直接编辑 FQDN 或证书-密钥对而未迁移到 **自适应身份验证**，则与身份和访问管理的连接将失败并显示以下错误。您必须迁移到自适应身份验证方法才能修复这些错误。

- ADC 命令失败并出现错误。策略已绑定到指定优先级。
- ADC 命令失败并出现错误。无法解除绑定未绑定的策略。

8. 点击 **保存更改**。

   此时，身份和访问管理将 **自适应身份验证** 显示为 **已连接**，并且自适应身份验证实例已自动配置 OAuth 配置文件。

   您可以从 GUI 验证此项。

   a. 访问您的自适应身份验证实例并使用您的凭据登录。
   b. 导航到 **Security > AAA - Application Traffic > Virtual Servers**。您应该会看到 OAuth IdP 配置文件已创建。
   c. 导航到 **Citrix Cloud > 身份和访问管理**。自适应身份验证处于“**已连接**”状态。

9. 在自适应身份验证主页中，通过单击“**启用**”（步骤 3）再次启用自适应身份验证方法。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

启用身份验证(/en-us/adaptive-authentication/media/adaptive-authentication-enable.png)

此步骤将身份验证方法设置为自适应身份验证，用于您的云存储。

10. 单击“**启用**”后，单击步骤 3 中的 StoreFront Cloud 链接。您应该会看到身份验证方法已更改为自适应身份验证。

**注意：**

新用户必须遵循相同的步骤，不包括删除 OAuth 相关配置的步骤。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 自适应身份验证实例的升级和维护

自适应身份验证实例的所有升级和维护均由 Citrix Cloud 团队管理。建议您不要将自适应身份验证实例升级或降级到随机 RTM 版本。您可以根据客户流量安排升级。有关详细信息，请参阅安排自适应身份验证实例的升级。Citrix Cloud 团队随后会相应地升级您的实例。

**重要提示：**

- Citrix Cloud™ 团队会定期检查与实例的通信。如果出现断开连接，自适应身份验证支持团队可能会联系您以重新获得实例的管理权限。如果实例管理问题未解决，自适应身份验证团队将无法管理升级。这可能导致您运行易受攻击的版本。
- 建议您启用电子邮件通知，以接收有关授权到期和磁盘空间使用情况详细信息的电子邮件。有关详细信息，请参阅通知。
- 由于自适应身份验证实例升级由 Citrix 管理，因此客户必须确保 VAR 目录中有足够的空间（至少 7 GB）用于升级。有关如何释放 VAR 目录空间的详细信息，请参阅如何释放 VAR 目录上的空间。
- 请勿将高可用性状态从 ENABLED 更改为 STAY PRIMARY 或 STAY SECONDARY。自适应身份验证的高可用性状态必须为 ENABLED。
- 请勿更改自适应身份验证实例上用户 (authadmin) 的密码。如果密码更改，自适应身份验证团队将无法管理升级。

## 安排您的自适应身份验证实例升级

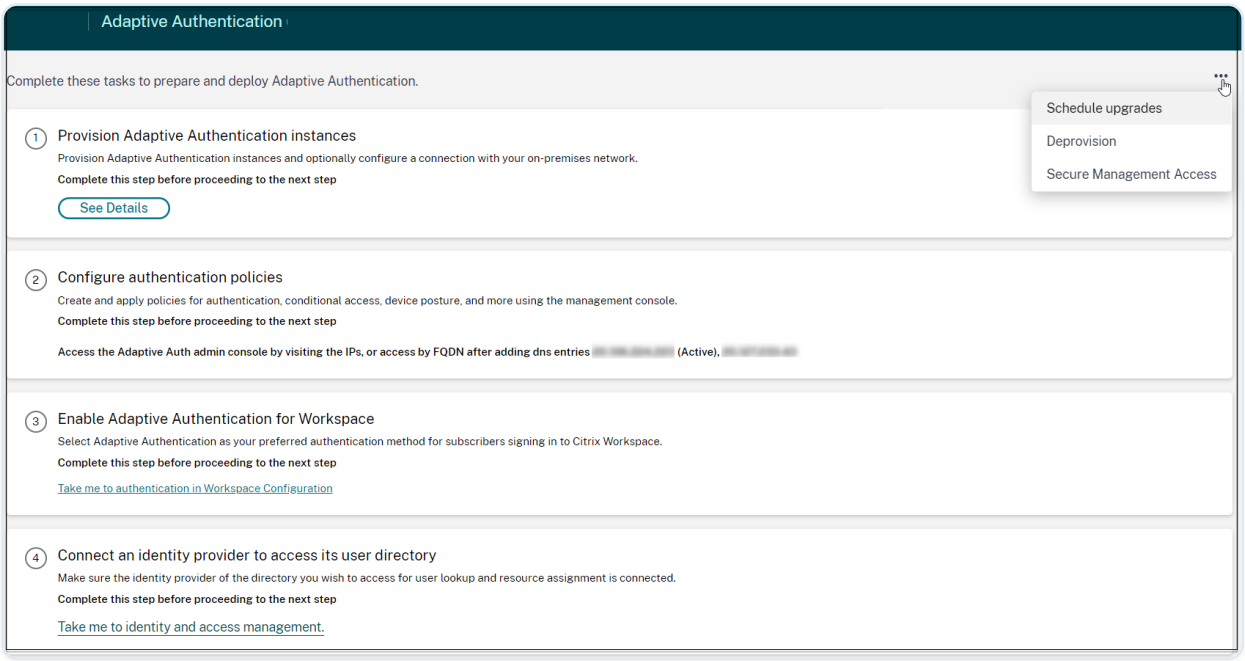
对于当前站点或部署，您可以选择用于升级的维护窗口。

**重要：**

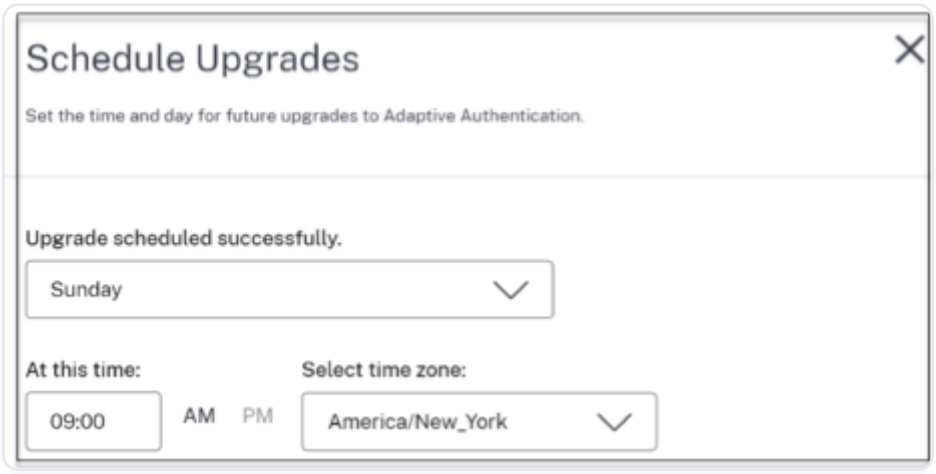
请勿将自适应身份验证实例升级到随机的 RTM 版本。所有自适应身份验证实例升级均由 Citrix 管理。

1. 在 **自适应身份验证** UI 上，在 **预配自适应身份验证实例** 部分中，单击省略号按钮。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. 单击 **安排升级**。
3. 选择进行升级的日期和时间。




# 配置备份和恢复

NetScaler Console 服务执行适用于自适应身份验证实例的备份管理。有关详细信息，请参阅 备份和恢复 NetScaler 实例。

**注意：**

如果您没有看到已载入的服务，请载入 NetScaler Console 服务。有关详细信息，请参阅 入门。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 解除预配您的自适应身份验证实例

客户可以在以下情况下并根据 Citrix® 支持的建议解除预配自适应身份验证实例。

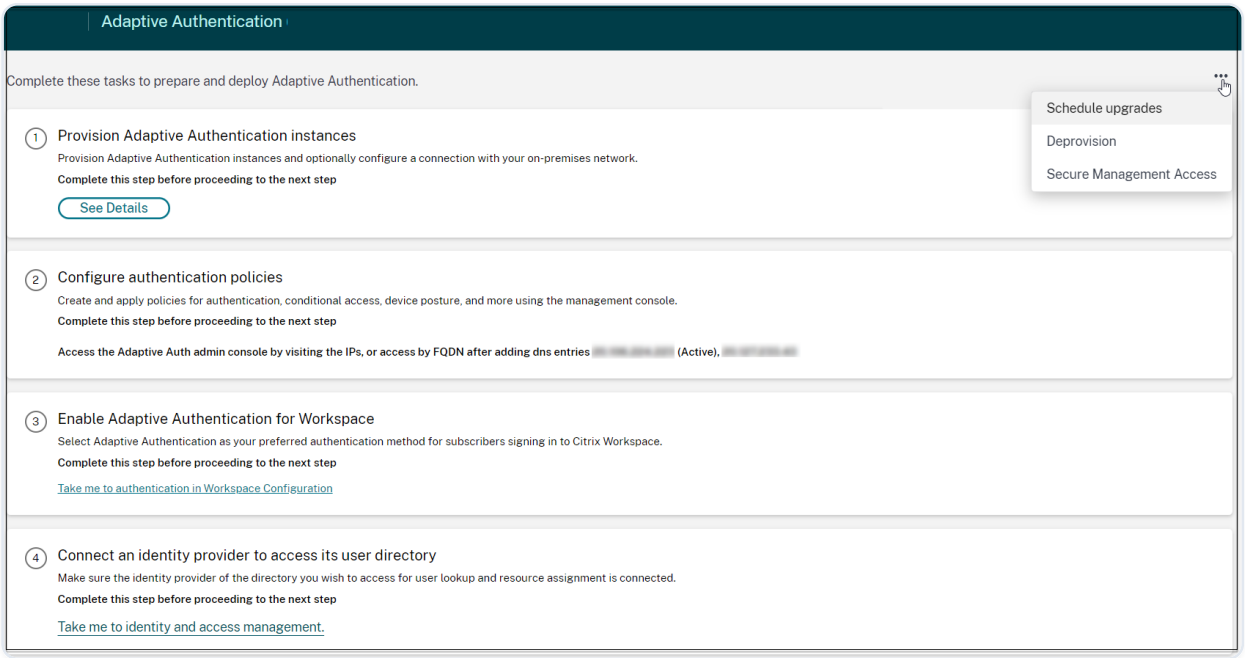
- 自适应身份验证实例无法访问（尤其是在计划升级后），尽管这种情况可能不会发生。
- 如果客户必须从 VNet 对等模式切换到连接器模式，反之亦然。
- 如果客户在预配 VNet 对等模式时选择了错误的子网（该子网与其数据中心或 Azure VNet 中的其他子网冲突）。

**注意：**

解除预配还会删除实例的配置备份。因此，在解除预配您的自适应身份验证实例之前，您必须下载并保存备份文件。

执行以下操作以解除预配自适应身份验证实例：

1. 在 **自适应身份验证** UI 中，在 **预配自适应身份验证实例** 部分中，单击省略号按钮。



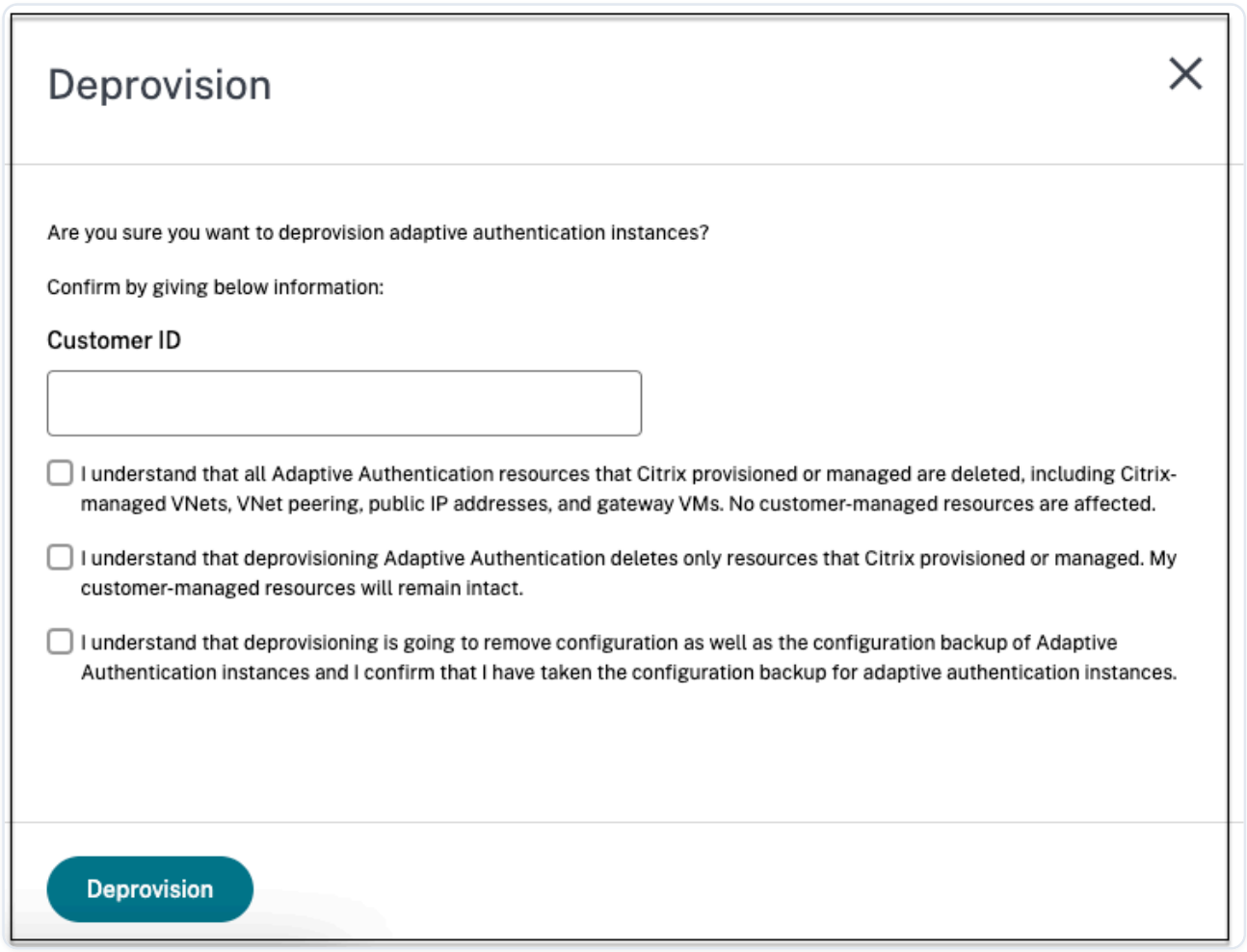

2. 单击 **解除预配**。

**注意：**

在解除预配之前，您必须断开 **Citrix Gateway** 与 StoreFront Cloud 的连接。

3. 输入客户 ID 以解除预配自适应身份验证实例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




# 安全管理访问

**重要提示：**

- 确保您已完成自适应身份验证实例的预配。有关详细信息，请参阅预配自适应身份验证。
- 如果您在 Windows 上使用 PuTTY 连接到自适应身份验证实例，则必须将下载的私钥转换为 PEM 格式。
- 建议使用以下命令通过 MAC 终端或 Windows（版本 10）的 PowerShell/命令提示符连接到自适应身份验证实例。

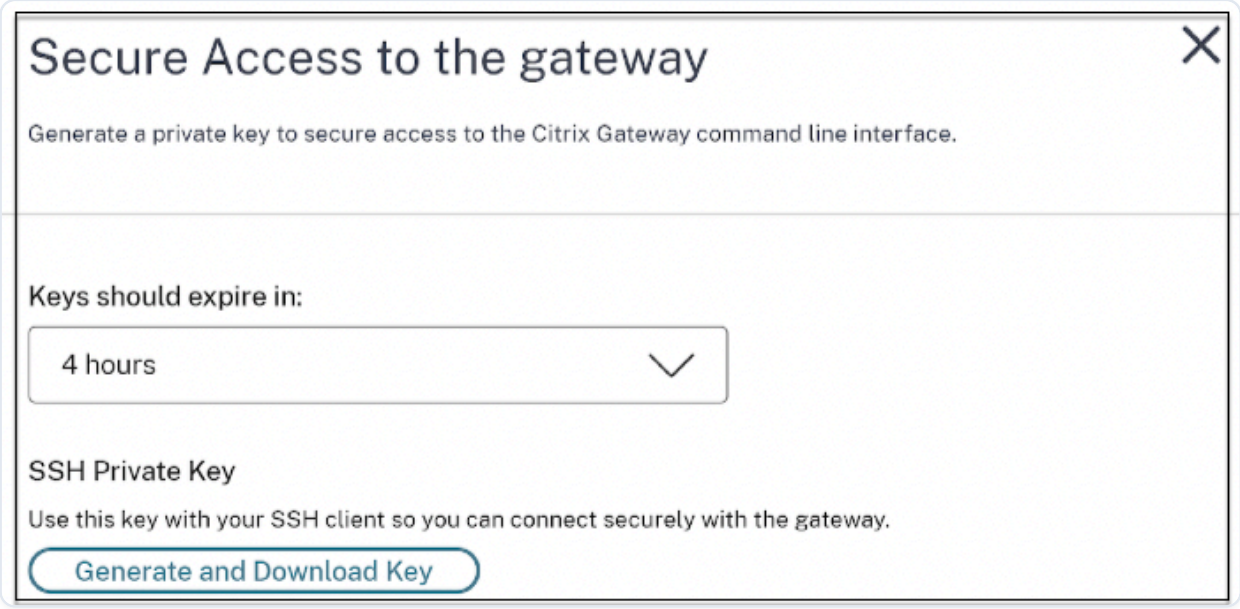
```
ssh -i &lt;path-to-private-key> authadmin@&lt;ip address of ADC>
```

- 如果您希望 AD 用户访问自适应身份验证 GUI，则必须将他们添加为 LDAP 组的新管理员。有关详细信息，请参阅 CTX123782。
- 对于所有其他配置，Citrix® 建议您使用自适应身份验证 GUI，而不是 CLI 命令。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

## 启用对网关的安全访问

1. 在**自适应身份验证** UI 上，单击省略号按钮。
2. 单击**安全管理访问**。




3. 在**密钥应在以下时间过期**中，为新的 SSH 密钥选择一个过期持续时间。
4. 单击**生成并下载密钥**。 复制或下载 SSH 私钥以备后用，因为页面关闭后将不再显示。此密钥可用于使用用户名 `authadmin` 登录自适应身份验证实例。

   如果之前的密钥对过期，您可以单击**生成并下载密钥**以创建新的密钥对。但是，只能有一个密钥对处于活动状态。
5. 单击**完成**。

# 更新自适应身份验证 FQDN

您可以更新或编辑在预配自适应身份验证服务时所做的配置。单击“**预配自适应身份验证实例**”选项卡上的“**查看详细信息**”，然后单击“**编辑**”以更新设置。

更新自适应身份验证实例(/en-us/adaptive-authentication/media/update-aa-instances.png)

## 编辑 FQDN

如果在 StoreFront Cloud 中选择 **自适应身份验证** 作为身份验证方法，则无法编辑 FQDN。您必须切换到其他身份验证方法才能编辑 FQDN。但是，如有必要，您可以编辑证书。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

**重要：**

- 在修改 FQDN 之前，请确保新的 FQDN 已映射到 IdP 虚拟服务器的公共 IP 地址。
- 使用 OAuth 策略连接到 **Citrix Gateway** 的现有用户必须将其身份验证方法迁移到 **自适应身份验证**。有关详细信息，请参阅将身份验证方法迁移到自适应身份验证。

要编辑 FQDN，请执行以下操作：

1. 从 **自适应身份验证** 切换到其他身份验证方法。

   切换身份验证方法(/en-us/adaptive-authentication/media/adaptive-authentication-adaptive-authentication-connected.png)

2. 选择“**我了解这对订阅者体验的影响**”，然后单击“**确认**”。

   当您单击“**确认**”时，最终用户的工作区登录将受到影响，并且在再次启用自适应身份验证之前，不会使用自适应身份验证进行身份验证。因此，建议您在维护窗口期间修改 FQDN。

3. 在“**上传证书**”屏幕中，修改 FQDN。

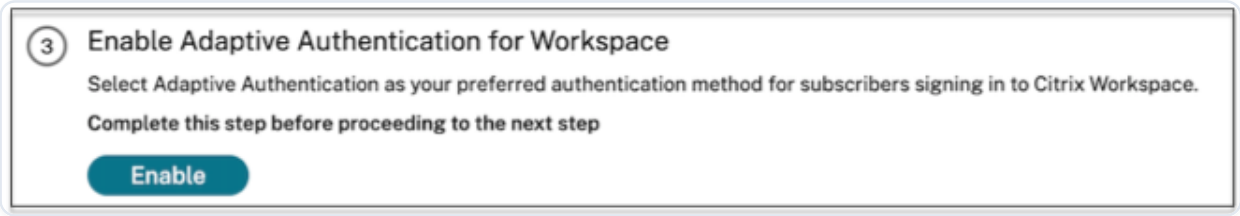
   编辑 FQDN(/en-us/adaptive-authentication/media/adaptive-authentication-edit-fqdn.png)

4. 点击“**保存更改**”。

   **重要提示：**

   如果您编辑了 FQDN，则还必须重新上传证书。

5. 在自适应身份验证主页中，点击“**启用**”（步骤 3），再次启用自适应身份验证方法。

6. 点击“**刷新**”。

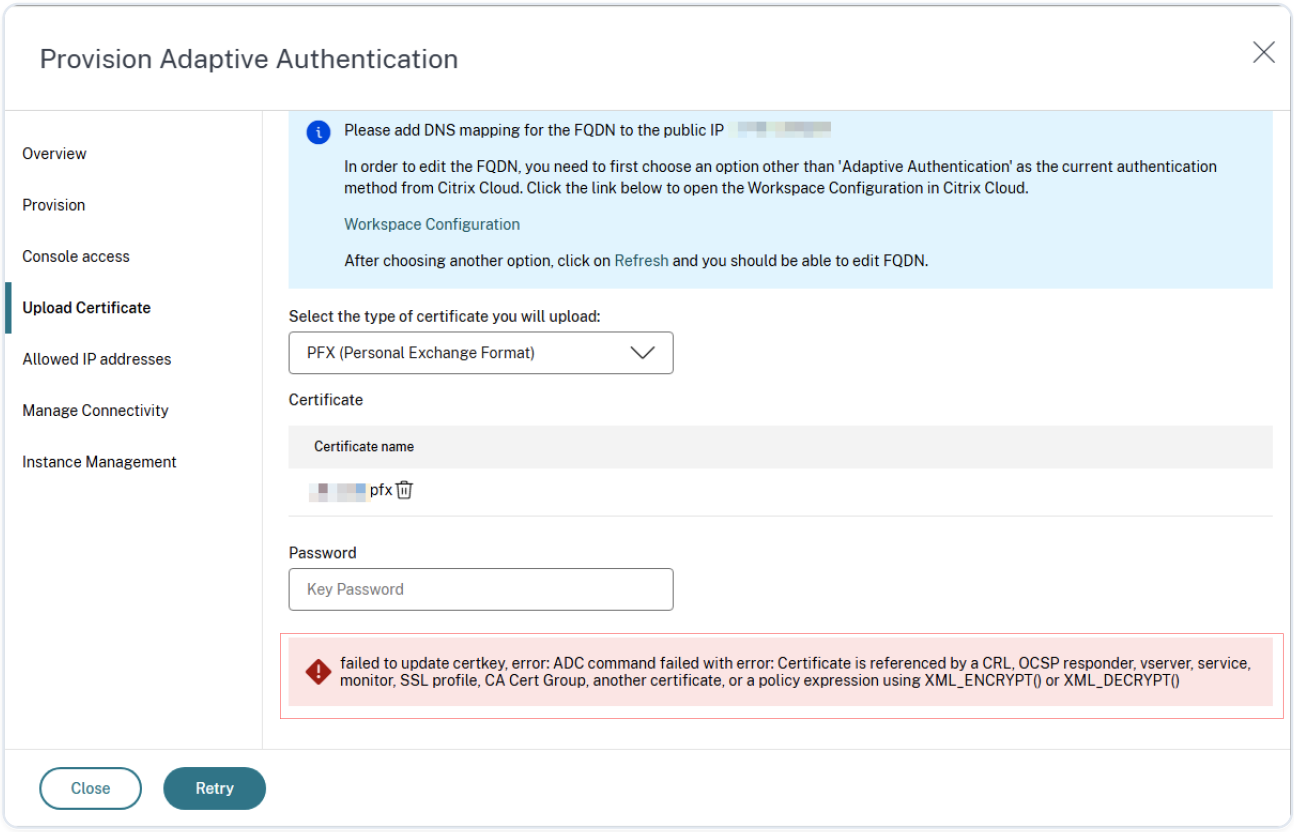
# 更新自适应身份验证证书

我们建议您从自适应身份验证服务门户中的“**上传证书**”选项卡上传新的或更新的证书。从该门户上传的证书将以默认名称“tenant-id.pfx”保存在 `/nsconfig/ssl/` 文件夹中。系统会自动创建一个 SSL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

证书密钥，指向此证书，名称为“-certkey”。默认绑定点（auth_vs 和 VPN global）也会自动更新为新的证书密钥。

您不得将此证书密钥用于任何其他目的，例如安全断言标记语言 (SAML) 或负载平衡 (LB)。如果证书密钥在默认绑定点（auth_vs 和 VPN global）之外使用，则在从自适应身份验证服务门户上传证书时，您可能会遇到“failed to update certkey”错误。




要解决此错误，您必须手动从其他绑定点移除证书密钥并重新上传证书。

以下是当证书密钥与 LB 虚拟服务器一起使用时解决此错误的示例步骤：

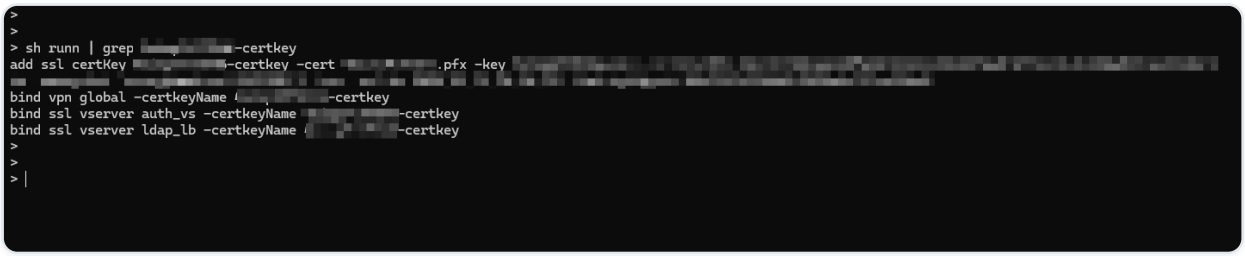
1. 识别所有正在使用证书密钥“-certkey”的绑定点（如果尚未知晓）。

   - 使用安全外壳 (SSH) 登录到 NetScaler® 的主节点并运行以下命令：

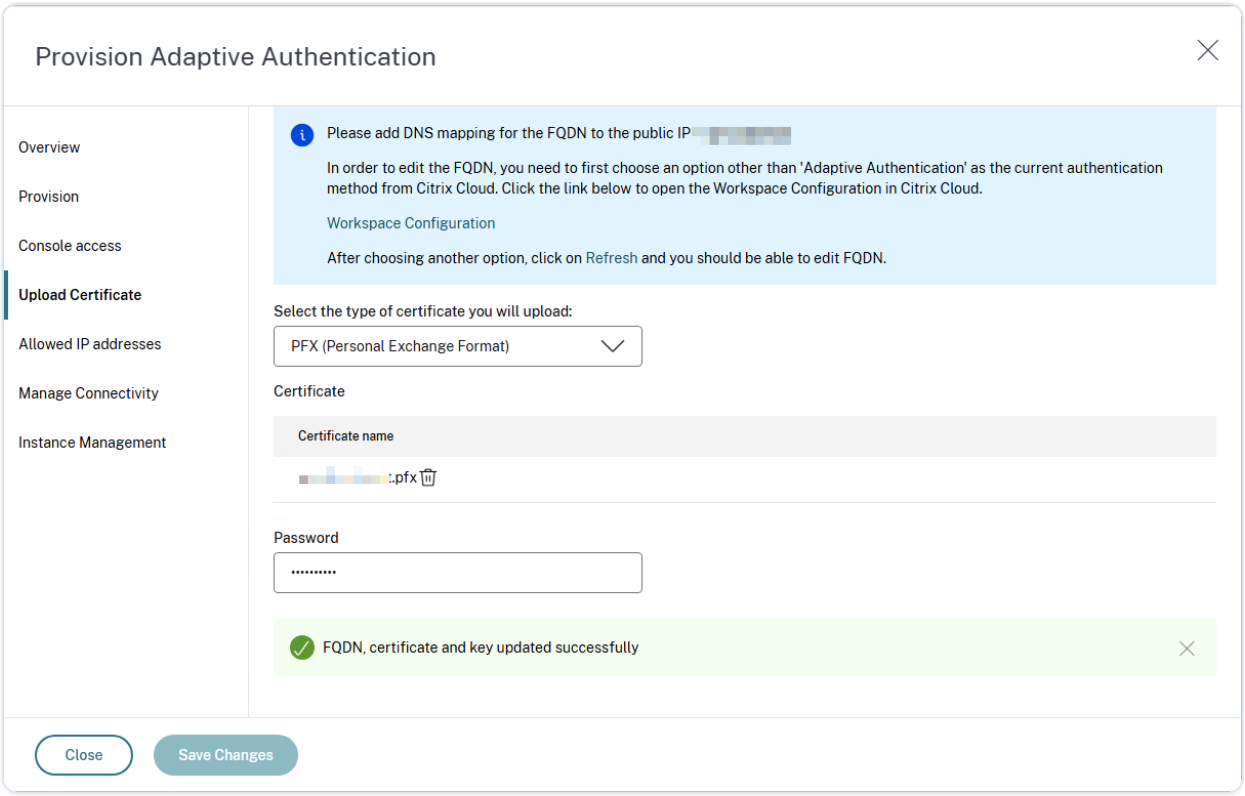
   ```
   sh runn | grep [tenant-id]-certkey
   ```

   在下图中，除了默认绑定点（auth_vs 和 VPN global）之外，证书密钥还绑定到 LB 虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.




2. 从 LB 虚拟服务器解除绑定证书密钥。有关详细信息，请参阅 使用 CLI 从虚拟服务器解除绑定 SSL 证书密钥对。
3. 从自适应身份验证服务门户重新上传证书。有关详细信息，请参阅 上传证书。




4. 将新的证书密钥（名称仍为“-certkey”）重新绑定到 LB 虚拟服务器。有关详细信息，请参阅 将证书密钥对绑定到 SSL 虚拟服务器。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 排查自适应身份验证问题

这些问题根据配置中的不同阶段进行分类：

- 预配
- 实例可访问性问题
- AD/RADIUS 连接和身份验证问题
- 身份验证问题
- EPA/设备姿态相关问题
- 智能标签相关问题
- 日志收集

您也可以使用自适应身份验证 CLI 排查这些问题。要连接到 CLI，请执行以下操作：

- 在您的计算机上下载 SSH 客户端，例如 putty/securecrt。
- 使用管理 IP（主）地址访问自适应身份验证实例。
- 使用您的凭据登录。

有关详细信息，请参阅访问 NetScaler 设备。

## 启用自适应身份验证日志的记录

确保启用日志级别以捕获自适应身份验证日志。

**注意：**

确保在正常操作期间禁用调试日志级别，并仅在需要时启用。如果调试日志级别始终启用，可能会导致管理 CPU 占用过高。这可能导致在高流量负载期间系统崩溃。有关详细信息，请参阅 CTX222945。

**使用 CLI 启用日志：**

1. 登录到自适应身份验证实例 CLI。
2. 使用 PuTTY 输入管理凭据。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 运行命令 `set audit syslogParams logLevel ALL`

**使用 GUI 启用日志：**

1. 使用浏览器登录到自适应身份验证实例。
2. 导航到 **配置 > 系统 > 审计**。
3. 在“Auditing”页面中，在 **Settings** 下，单击 **Change Auditing syslog Settings**。
4. 在 **Log Levels** 中，选择 **ALL**。

# 预配问题

- **无法访问自适应身份验证 UI**

  检查是否为您的客户 ID/租户启用了授权。

- **在预配页面停留超过 45 分钟**

  收集错误屏幕截图（如果有），然后联系 Citrix 支持寻求帮助。

- **VNet 对等互连已关闭**

  - 检查 Azure 门户中是否有与此对等互连对应的警报，并采取建议的操作。
  - 删除对等互连，然后从自适应身份验证 UI 再次添加。

- **取消预配未完成**

  联系 Citrix 支持寻求帮助。

# 实例可访问性问题

- **实例的管理 IP 地址无法访问**

  - 检查用于访问的客户端公共 IP 地址是否在允许的源 IP 地址之列。
  - 验证是否有任何代理正在更改客户端源 IP 地址。

- **无法登录实例**

  确保管理员访问权限使用您在预配期间输入的凭据正常工作。

- **最终用户没有完整权限**

  确保在添加用户时，您已绑定了合适的命令策略以进行访问。有关详细信息，请参阅用户、用户组和命令策略。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# AD 或 RADIUS 连接问题

**Azure VNet 对等连接类型问题：**

- 检查自适应身份验证实例是否可访问客户管理的 Azure VNet。
- 检查从客户管理的 Azure VNet 到 AD 的连接/可达性是否正常工作。
- 确保已添加适当的路由，以将流量从本地导向 Azure VNet。

**基于 Windows 的连接器：**

- 所有日志都位于目录 /var/log/ns.log 中，并且每个日志都以 为前缀。
- 日志中的 ConnectionID 可用于关联不同的事务。
- 确保连接器虚拟机的私有 IP 地址已作为 RADIUS 服务器中的 RADIUS 客户端之一添加，因为该 IP 地址是连接器的源 IP 地址。

  对于每个身份验证请求，隧道在自适应身份验证实例 (NS - AAAD 进程) 和身份验证服务器之间建立。一旦隧道成功建立，就会进行身份验证。

  确保连接器虚拟机可以解析自适应身份验证 FQDN。
- 连接器已安装，但本地连接失败。

  验证 NSAUTH-TUNNEL 是否正在建立。

  `cat ns.log | grep -I “tunnel”`

  如果身份验证请求的以下示例日志未打印在 ns.log 文件中，则可能在建立隧道时出现问题或连接器端出现问题。

  ```
  LDAP:

  [NS_AAUTH_TUNNEL] Entering bitpump for

  Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
  Connection2 => Src : 10.106.103.70:2271, Dst : 10.106.103.80:443"

  RADIUS:

  [NS_AAUTH_UDP_TUNNEL] MUX channel established"
  ```

  检查日志详细信息并采取适当措施。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 日志详细信息 | 纠正措施 |
| --- | --- |
| 日志文件中不包含前缀为 `[NS_AAUTH_TUNNEL]` 的日志 | 运行 `show cloudtunnel vserver` 命令。此命令必须列出状态为“UP”的（TCP 和 UDP）云隧道虚拟服务器。 |
| `[NS_AAUTH_TUNNEL] Waiting for outbound from connector` 对于此日志，如果未收到以下响应：`[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"` | 检查连接器计算机是否能够访问自适应身份验证 FQDN **或**检查连接器端防火墙是否有到自适应身份验证 FQDN 的出站连接 |
| `[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` 和 `[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"` | 联系 Citrix 支持。 |

**连接器无响应：**

- 确保从连接器虚拟机可以访问自适应身份验证 FQDN。
- 确保您已将中间证书绑定并链接到自适应身份验证实例上的服务器证书。

**LDAP/RADIUS 设置不正确：**

如果您的 AD/RADIUS 服务器 IP 地址是公共 IP 地址，则必须在 NetScaler 中添加子网或 IP 地址表达式。请勿编辑现有范围。

- 要使用 CLI 添加子网或 IP 地址：

```
set policy expression aauth_allow_rfc1918_subnets
"(CLIENT.IP.DST.BETWEEN(10.0.0.0,10.255.255.255) ||
CLIENT.IP.DST.BETWEEN(172.16.0.0,172.31.255.255) ||
CLIENT.IP.DST.BETWEEN(192.168.0.0, 192.168.255.255) ||
CLIENT.IP.DST.BETWEEN(13.14.0.0, 13.14.255.255)||
CLIENT.IP.DST.EQ(1.2.5.4))"
```

- 通过 GUI 添加子网或 IP 地址：

  a. 导航到 **Appexpert > 表达式**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 添加表达式 **aauth_allow_rfc1918_subnets**。

如果隧道已建立但身份验证仍然失败，请使用以下步骤排查问题。

**LDAP：**

- 验证 Bind DN 详细信息。
- 使用测试连接确认错误。
- 使用 `aaad` debug 验证错误。
- 使用 CLI 登录到 Adaptive Authentication 实例。

```
shell

cd /tmp

cat aaad.debug
```

**常见 LDAP 错误：**

- 服务器超时 – 连接器对 LDAP 查询无响应。
- 其他 LDAP 错误，请参阅 CTX138663。

**RADIUS 协议：**

- 必须在 RADIUS 服务器配置中将连接器 IP 地址添加为 RADIUS 客户端源 IP 地址。

# 身份验证问题

- **OAuth 的断言后错误**
  - 确保所有声明都由 AD 提供。要成功，您需要 7 个声明。
  - 验证 /var/log/ns.log 中的日志，以查找 OAuth 失败的错误。

```
cat /var/log/ns.log
```

  - 验证 OAuth 配置文件参数。

- **Azure AD 身份验证卡在断言后**

  将 AD 身份验证添加为下一个因素，并将身份验证设置为关闭。这是为了获取成功身份验证所需的所有声明。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# EPA 相关问题

- **插件已存在，但用户收到下载插件的提示。**

  可能的原因：版本不匹配或文件损坏

  - 运行开发人员工具并验证插件列表文件是否包含与 NetScaler® 和您的客户端计算机相同的版本。
  - 确保 NetScaler 上的客户端版本与客户端计算机上的版本相同。

    更新 NetScaler 上的客户端。

    在自适应身份验证实例上，导航到 **Citrix Gateway > Global Settings > Update client libraries**。

    Citrix Downloads 上的 EPA 插件库页面为您提供了详细信息。
  - 有时，即使版本已更新，请求也可能缓存在 NetScaler 上。

    `show cache object` 显示缓存的插件详细信息。您可以使用以下命令将其删除；

    `flush cache object -locator 0x00000023345600000007`

  有关 EPA 日志收集的详细信息，请参阅 CTX209148。
- **用户选择选项后，是否有办法恢复 EPA 设置（始终、是、否）？**

  目前，EPA 设置的恢复是手动完成的。

  - 在客户端计算机上，导航到 C:\Users\<user_name>\AppData\Local\Citrix\AGEE。
  - 打开 `config.js` 文件并将 trustAlways 设置为 null - `"trustAlways":null`

# 智能访问标签问题

- **配置智能访问后，应用程序不可用**

  确保标签在自适应身份验证实例和 Citrix VDA 交付组上都已定义。

  检查标签是否以全大写形式添加到交付组中。

  如果此方法无效，您可以收集 ns.log 并联系 Citrix 支持。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 自适应身份验证实例的通用日志收集

- 技术支持包：有关详细信息，请参阅 如何从 SDX 和 VPX 设备收集技术支持包以进行洞察分析。
- 跟踪文件。有关详细信息，请参阅 如何在 NetScaler 上记录数据包跟踪。

联系 Citrix 支持寻求指导。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 共享安全职责

以下部分提供了有关共享安全职责的更多信息。

## 客户需要采取的行动

以下是客户作为安全最佳实践一部分需要采取的一些行动。

- 访问自适应身份验证 UI 的凭据：客户负责创建和维护用于访问自适应身份验证 UI 的凭据。如果客户正在与 Citrix 支持部门合作解决问题，则客户可能需要与支持人员共享这些凭据。
- 多因素身份验证：作为最佳实践，客户必须配置多因素身份验证策略，以防止未经授权访问资源。
- 身份验证凭据：客户必须根据通用安全和密码标准配置其身份验证凭据。
- 远程 CLI 访问安全：Citrix 为客户提供远程 CLI 访问。但是，客户负责在运行时维护实例的安全性。
- SSL 私钥：由于 NetScaler® 由客户控制，Citrix 无法访问文件系统。客户必须确保保护其在 NetScaler 实例上托管的证书和密钥。
- 数据备份：备份配置、证书、密钥、门户自定义以及任何其他文件系统修改。
- NetScaler 实例的磁盘映像：维护和管理 NetScaler 磁盘空间和磁盘清理。有关详细信息，请参阅 实例管理。
- 有关负载均衡 LDAPS 配置示例，请参阅 LDAP 和 LDAPS 负载均衡配置示例。

## 客户和 Citrix 都需要采取的行动

- 灾难恢复：在受支持的 Azure 区域中，NetScaler 高可用性实例部署在独立的可用区中，以防止数据丢失。如果发生 Azure 数据丢失，Citrix 将尽可能多地恢复 Citrix 管理的 Azure 订阅中的资源。

  如果整个 Azure 区域丢失，客户负责在新区域中重建其客户管理的虚拟网络并创建新的 VNet 对等互连。

- 通过公共管理 IP 地址保护访问：

  通过分配的公共 IP 地址保护对管理接口的访问，并允许出站连接到 Internet。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 规模调整和性能指南

自适应身份验证允许客户使用部署在其数据中心中的 Cloud Connector 或 Azure VNet 对等互连（如果已从客户管理的 VNet 建立数据中心可达性）访问其本地身份验证服务器。本主题包含有关 Citrix Cloud Connector™ 和 Azure VNet 对等互连部署的性能数据，以及 Citrix Cloud Connector 计算机的推荐规模和大小配置。

## 用户身份验证速率

具有 2 个 vCPU 和 7 GB RAM 的连接器虚拟机每秒可验证 14 个用户。

默认情况下，如果连接器服务发生故障或崩溃，它会配置为自动重启两次。在随后的故障或崩溃中，服务将停止。此外，目前，如果身份验证速率超过每秒 4 次身份验证，连接器服务将失败。通过将连接器服务配置为在发生任何次数的故障后重新启动（**Citrix Netscaler Cloud Gateway > 恢复 > 重新启动服务**），可以实现此速率。如果未配置此设置，速率将降至每秒 4 次身份验证。

## 使用 Citrix Cloud™ Connectors 时的流量延迟和用户身份验证速率

下表显示了使用 Citrix Cloud Connectors 时的流量延迟和用户身份验证速率：

| 身份验证类型 | 身份验证延迟 (P95)（毫秒） | 每秒身份验证或用户登录速率 |
|---|---|---|
| LDAP | 5.99 | 14 |
| RADIUS | 3.17 | 14 |
| LDAP+RADIUS | 4.59 | 14 |
| LDAPS | 26.75 | 14 |
| LDAPS+RADIUS | 15.61 | 14 |

## 使用 Azure VNet 对等互连时的流量延迟和用户认证速率

下表显示了使用 Azure VNet 对等互连时的流量延迟和用户认证速率：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

| 认证类型 | 请求延迟 (P95) (MS) | 每秒认证或用户登录速率 |
| --- | --- | --- |
| LDAP | 6.95 | 17.54 |
| LDAPS | 7.19 | 16.98 |

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 常见问题

以下部分提供了有关一些最常见问题的更多信息。

## 升级自适应身份验证或 NetScaler 后，用户无法登录。我该怎么办?

**自我评估检查：**

- 如果自适应身份验证 IdP FQDN 无法访问：
  - 检查身份验证虚拟服务器 (auth_vs) 是否处于 UP 状态。
  - 如果它未处于 UP 状态，请验证证书是否正确绑定。

  未保存的配置或配置错误可能导致证书解除绑定或丢失，从而使身份验证虚拟服务器处于 DOWN 状态。
- 使用以下命令从主自适应身份验证 NetScaler CLI 检查云隧道虚拟服务器是否处于 UP 状态：`show cloudtunnel vserver`。

  由于间歇性 Azure IMDS 连接问题，云隧道虚拟服务器配置在重启后可能会丢失。

  **解决方法：** 执行另一次重启。
- 如果使用 LDAP，请确保 `ldapAction` 配置了 7-10 秒的超时时间 (`authTimeout`)。

> **注意：**
>
> 无论是否执行了升级，都可能发生此与 LDAP 相关的登录问题。

## 为什么自适应身份验证 NetScaler 实例在 ADM/NetScaler Console 中显示为“Down”或“In Grace Period”?

自适应认证 NetScaler 实例条目显示在 **控制台服务 > 基础设施 > 实例 > NetScaler** 中。

- 控制台中显示的 UP（绿色）或 DOWN（红色）状态表示控制台服务与自适应身份验证 NetScaler 实例之间的连接性，而不是自适应身份验证节点的实际状态。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DOWN 连接状态不影响用户登录或功能，但可能会产生以下影响：
  - Citrix 无法将升级推送到 NetScaler 实例。
  - 如果连接状态保持 DOWN 超过 30 天，自适应身份验证 NetScaler LAS 许可证租约刷新可能会失败，并且实例带宽可能会限制为 10 Mbps。NetScaler 管理员 UI 中会出现警告横幅。

**恢复连接：**

如果 ADM/NetScaler 控制台中显示连接状态为 DOWN，则必须恢复它。请执行以下步骤或联系 Citrix 支持：

1. 通过 SSH 连接到连接状态显示为 DOWN 的 NetScaler 实例。
2. 运行 shell。
3. 验证 mastools 进程是否正在运行：

   ```
   ps -ax | grep mastools
   ```

   输出必须显示 mastools 和 mastools_upgrade 进程都在运行。
4. 如果需要，请重新启动 mastools：

   ```
   cd /var/mastools/scripts
   ```

   ```
   ./mastoolsd restart
   ```

# 为什么用户在自适应身份验证升级后会收到“依赖方请求的用户声明未找到”?

- 如果问题发生在自适应身份验证 IdP 登录页面出现之前，请联系 Citrix 支持。
- 如果问题发生在自适应身份验证 IdP 登录页面出现之后以及输入凭据之后：
  - 确保用户在 AD 中拥有以下所有 7 个必需的声明。
    - 电子邮件地址
    - 显示名称
    - 通用名称
    - sAMAccountName
    - 用户主体名称
    - 对象标识符 (OID)
    - 安全标识符 (SID)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 如果您正在使用 SAML 或 RADIUS，请在末尾添加一个 NOAUTH LDAP 因子以提取所有 7 个必需的声明。

## 自适应身份验证无法通过 LDAP 端口 389 或 636 工作。我应该检查什么?

确保仅从主节点执行连接测试（GUI：**测试网络连接**）。

1. 通过检查 `ns.log` 中的 **Entering bitpump** 日志条目，验证到本地 AD 的隧道是否成功。
2. 如果隧道成功，运行 `cat /tmp/aaad.debug` 查看身份验证错误。
3. 如果问题仍然存在，请联系 Citrix 支持。

## 我正在尝试预配自适应身份验证设备，但入门流程要求我填写一个我无法访问的表单。我该怎么办?

用于请求自适应身份验证预配的表单可能会向某些客户显示“访问被拒绝”错误。

**解决方法：**

请直接联系 Citrix 支持提交预配请求。

## 提交表单后，启用自适应身份验证需要多长时间?

至少三个工作日。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 数据治理

本主题提供有关 Citrix 自适应身份验证服务和自适应身份验证实例收集、存储和保留日志的信息。未在 定义 中定义的任何首字母大写术语均具有 Citrix 最终用户服务协议 中指定的含义。

- 自适应身份验证服务：管理员可以登录以部署和管理自适应身份验证实例的 Citrix Cloud™ 服务。
- 自适应身份验证实例：由自适应身份验证服务部署的 NetScaler® 虚拟机，允许管理员管理用户身份验证。

## 数据驻留

### 自适应身份验证服务

Citrix 自适应身份验证服务客户内容数据驻留在 Azure 云服务东部区域。为实现可用性和冗余，它们被复制到以下 Azure 区域：

- 美国西部
- 北欧

以下是服务配置和运行时日志的不同目的地。

- Splunk 服务，用于系统监控和调试日志，仅限美国和欧盟（European Union）地区。
- NetScaler Application Delivery Management 服务，用于聚合的用户访问日志。有关详细信息，请参阅 NetScaler ADM 数据治理。
- Citrix Cloud 系统日志服务，用于管理员审计日志。有关详细信息，请参阅 Citrix Cloud 服务客户内容和日志处理以及地理位置注意事项。

### 自适应身份验证实例

NetScaler Application Delivery Management 服务，用于备份所有配置、实例特定工件。有关详细信息，请参阅 NetScaler ADM 数据治理。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

# 数据收集

Citrix 自适应身份验证服务允许客户管理员通过自适应身份验证 UI 和配套的连接器设备通过控制台配置服务。收集以下客户内容：

- 自适应身份验证服务
  - IdP（身份提供商）端点的 FQDN（完全限定域名）和 IP 地址。
  - IP 地址/范围、端口和协议
  - 用于访问 IdP 身份验证虚拟服务器的证书
  - 管理端点的公共 IP 地址
  - 对于 Azure VNet 对等互连，具有网络参与者角色的服务主体。有关详细信息，请参阅 使用 Azure VNet 对等互连设置与本地身份验证服务器的连接。
- 应用程序授权的用户标识符
- Citrix Cloud Connector 相关详细信息。有关详细信息，请参阅 Citrix Cloud Connector。
  - IP 地址或 FQDN
  - 用户、设备和资源位置标识符
  - 内部代理配置

对于服务组件收集的运行时日志，关键信息包括：

- 客户端 IP 地址和端口
- 目标 FQDN/地址和端口
- 客户端用户代理
- 应用程序 URL 路径
- 应用程序访问时间和持续时间
- 请求字节数
- 响应字节数
- HTTP 事务 ID
- 部署模式（连接器或 Azure VNet 对等互连）
- Azure 资源
  - 资源组名称
  - VNet（IP 地址、CIDR）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 子网（IP 地址、CIDR）
- 虚拟机名称

## 数据传输

Citrix 自适应身份验证服务将日志发送到受传输层安全保护的目标 (Splunk)。

## 数据控制

Citrix 自适应身份验证服务目前不提供客户关闭日志发送或阻止客户内容在全球复制的选项。

## 数据保留

根据 Citrix Cloud 数据保留策略，客户配置数据将在订阅过期 90 天（约 3 个月）后从服务中清除。

日志目标维护其服务特定的数据保留策略。

- 有关存储在 Citrix Application Delivery Management 中的事件。请参阅 Citrix ADM 数据治理。
- Splunk 日志会在 90 天（约 3 个月）后存档并最终删除。
- 自适应身份验证实例在订阅过期 30 天（约四个半星期）后解除分配。

## 数据导出

针对不同类型的日志，有不同的数据导出选项。

- 管理员审计日志可从 Citrix Cloud 系统日志控制台访问。
- Splunk 日志不供客户使用。这些事件也可以从 Splunk 导出为 CSV 文件。

## 定义

- 客户内容是指上传到客户帐户进行存储的任何数据，或 Citrix 为执行服务而获得访问权限的客户环境中的数据。
- 日志是指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性和支持的记录。
- 服务是指前面概述的 Citrix Cloud 服务，旨在促进客户用例。

© 1997–2026 Citrix Systems, Inc. All rights reserved.