Web Interface 5.4

2015-05-07 20:21:46 UTC

目录

Web Interface 5.4

更新日期： 2014-11-25

Web Interface 可为用户提供对 XenApp 应用程序和内容以及 XenDesktop 虚拟桌面的访问权限。 用户可以通过标准 Web 浏览器或 Citrix 联机插件访问其资源。

本部分中包含的内容

库的本部分介绍了有关安装、配置和管理 Web Interface 的最新信息，其中包括以下信息：

Web Interface 5.4 自述文件	有关最新更新和已知问题的信息。
Web Interface 5.4 中已修复的问题	自上一版 Web Interface 后已修复问题的详细信息。
Web Interface 功能	Web Interface 简介。
本版本中的新增功能	新增功能概述。
Web Interface 组件	Web Interface 部署说明。
Web Interface 的系统要求	软件、配置、Web 服务器、用户和设备要求。
安装 Web Interface	安装 Web Interface 并配置 Web 服务器。
Web Interface 入门	创建并配置 Web Interface 站点。
管理服务器和场	配置并管理服务器设置以及与服务器场的通信。
为 Web Interface 配置身份验证	配置 Web Interface、服务器场与 Citrix 插件之间的身份验证。
管理客户端	通过 Web Interface 部署并使用 Citrix 插件。
管理安全访问	配置并管理对站点的访问。
编辑客户端代理设置	配置通过代理服务器连接且运行 XenApp 或 XenDesktop 的 Citrix 客户端和服务器。
为用户自定义外观	自定义 Web Interface 显示给用户的方式。
管理会话首选项	指定用户可以调整的设置。
配置工作区控制	允许用户快速与资源断开连接、重新连接以及从资源注销。
配置 Web Interface 安全性	确保 Web Interface 环境中数据的安全。
使用配置文件配置站点	使用配置文件管理 Web Interface 站点。
配置对 Web Interface 的 AD FS 支持	创建和配置 Microsoft Active Directory 联合身份验证服务 (AD FS) 集成 Web Interface 站点。

Web Interface 5.4 自述文件

自述文件版本：1.0

目录

相关文档

有关可能影响 Web Interface 用户的客户端相关问题，请参见当前为用户部署的 Citrix 客户端的自述文件。

有关此版本中已解决问题的列表，请参阅知识中心文章 http://support.citrix.com/article/CTX124164。

要访问许可文档，请转到许可使用本产品。

获取支持

Citrix 主要通过 Citrix 解决方案顾问提供技术支持。 可以与供应商联系获得一线支持，或使用 Citrix 在线技术支持服务查找最近的 Citrix 解决方案顾问。

Citrix 在 Citrix 技术支持 Web 站点上提供了在线技术支持服务。 “支持”页面包含指向下载、Citrix 知识中心、Citrix 咨询服务以及其他有用支持页面的链接。

此版本中的已知问题

下面列出了此版本中的已知问题。 请在安装此产品前仔细阅读。

- 在运行 WinCE 6.0 WFR3 和 Internet Explorer 6 的设备上不能正常显示图标
- 已发布桌面添加到 Internet Explorer 的收藏夹时可能出现用户错误
- 尝试使用已弃用的客户端连接时显示错误消息
- Citrix 联机插件无法在运行 Windows Embedded 操作系统的设备上升级
- 在运行 Windows Server 2008 的 XenApp 服务器上配置进行委派时，使用 Kerberos 失败

- 从一些运行 Windows Embedded CE 6.0 的设备上访问 Web Interface 时，虚拟桌面启动失败
- 工作区控制和客户端升级对于 Firefox 3.6 用户不可用
- 在一些运行 Windows Mobile 6.1 的设备上，工作区控制不可用
- 在一些运行 Windows Embedded CE 6.0 R2 的设备上工作区控制间歇性不可用
- 无法与 XenApp 6.0 一起使用来自 Access Gateway 的通过智能卡传递身份验证

在运行 WinCE 6.0 WFR3 和 Internet Explorer 6 的设备上不能正常显示图标

在运行 Internet Explorer 6 和 WinCE 6.0 WFR3 的设备上查看图标时，.png 格式的图标不能正常显示（热修补 3 内部版本 664）。 要解决此问题，请使用 Internet Explorer 5 或更早版本。 或者，要在 Internet Explorer 6 中显示 .png 文件，请根据 Microsoft 文章 http://support.microsoft.com/kb/294714 中介绍的解决方法进行操作。

[#41839]

用户可能无法将已发布的桌面和应用程序添加到 Internet Explorer 收藏夹中

将已发布的桌面和应用程序添加到 Internet Explorer 的“收藏夹”时，用户可能会遇到问题。在某些情况下，最终显示的收藏夹链接的标题不正确，并且单击时无法链接到相应的页面。要将应用程序添加到“收藏夹”，请在该应用程序图标上单击鼠标右键。 要添加桌面，请在桌面标题文本上单击鼠标右键。

[#244446]

尝试使用已弃用的客户端连接时显示错误消息

此版本的 Web Interface 不支持使用 7.0 以下版本的客户端。 当尝试使用较低版本的客户端连接远程应用程序时，用户可能会遇到错误“50: 无法连接到服务器”。用户可以通过将客户端升级到最新版本来避免此错误。 如果此方法不可行，可以通过以下方法编辑模板 .ica 文件来阻止该错误发生：

1. 使用文本编辑器（例如记事本）打开以下文件：default.ica、bandwidth_high.ica、bandwidth_low.ica、bandwidth_medium.ica 以及 bandwidth_medium_high.ica。 这些文件通常位于 IIS 中的 C:\inetpub\wwwroot\Citrix\SiteName\conf 目录，以及 Java 应用程序服务器中 Web Interface 站点的 /WEB-INF 目录。
2. 在每个文件中找到并删除以下行：

   ```
   DoNotUseDefaultCSL=On
   BrowserProtocol=HTTPonTCP
   LocHttpBrowserAddress=!
   ```

[#163695]

Citrix 联机插件无法在运行 Windows Embedded 操作系统的设备上升级

Web Interface 可能会提供在运行 Windows Embedded 操作系统的设备上安装或升级 Citrix 联机插件；但安装会失败。 您可以通过在嵌入式设备上手动安装最新版本的 Citrix 联机插件来避免此问题。 如果此方法不可行，可以为站点修改设置来阻止这些安装标题出现：

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。

3. 在 Action（操作）窗格中，单击 Client Deployment（客户端部署）。 对于只提供联机应用程序的站点，请选中 Native client（本机客户端）复选框，并单击 Properties（属性）。

4. 单击 Client Detection（客户端检测）。

5. 清除 Offer upgrades for clients（为客户端提供升级）复选框，然后选择 Only if resources cannot be accessed（仅当资源无法访问时）或 Never（从不）。

[#164709]

在运行 Windows Server 2008 的 XenApp 服务器上配置进行委派时，使用 Kerberos 失败

由于 Windows Server 2008 的一个问题，在信任 XenApp 服务器进行委派时，将 Active Directory 配置为仅使用 Kerberos 进行身份验证会导致身份验证失败。 此问题发生在运行 Windows Server 2008 with Service Pack 2、Windows Server 2008 x64 Editions with Service Pack 2 和 Windows Server 2008 R2 的 XenApp 服务器上。 要在运行 Windows Server 2008 的 XenApp 服务器上启用 AD FS 集成和来自 Access Gateway 的通过智能卡传递身份验证，请选择文档中指示的使用任何身份验证协议设置，而不是仅使用 Kerberos 设置。 [#169269]

从一些运行 Windows Embedded CE 6.0 的设备上访问 Web Interface 时，虚拟桌面启动失败

在某些情况下，运行 Windows Embedded CE 6.0 和 Internet Explorer 6.x 的 WYSE V30LE 瘦客户端用户可能会发现，当他们登录到 XenApp Web 站点并单击文本链接以启动虚拟桌面时，桌面无法启动。 用户可以通过单击文本链接旁边显示的图标来启动该桌面以避免此问题。 [#218317]

工作区控制和客户端升级对于 Firefox 3.6 用户不可用

由于 Mozilla Firefox 3.6 的一个更改，对于使用此浏览器访问 Web Interface 的用户，工作区控制会自动禁用。 此外，客户端检测和部署进程无法检测使用 Firefox 3.6 的用户安装的 Citrix 客户端的版本号，并且因此无法提供给这些用户升级其客户端的机会。 [#230068]

在一些运行 Windows Mobile 6.1 的设备上，工作区控制不可用

在某些情况下，运行 Windows Mobile 6.1 Professional 和 Internet Explorer Mobile 的 HP iPAQ 910c 手持式设备的用户可能会发现，当他们登录到 XenApp Web 站点时，工作区控制无法正常运行。 [#230580]

在一些运行 Windows Embedded CE 6.0 R2 的设备上工作区控制间歇性不可用

在某些情况下，运行 Windows Embedded CE 6.0 R2 和 Internet Explorer 6.x 的 HP t5540 瘦客户端用户可能会发现，当他们登录到 XenApp Web 站点时，在单击重新连接按钮时工作区控制有时无法正常运行。 [#230654]

无法与 XenApp 6.0 一起使用来自 Access Gateway 的通过智能卡传递身份验证

由于 XenApp 6.0 的一个问题，登录到 Access Gateway 集成站点的智能卡用户在启用了来自 Access Gateway 的通过智能卡传递身份验证功能时，无法访问资源。 用户单击链接访问通过 XenApp 6.0 交付的资源时会遇到错误“建立请求的连接时发生错误”。可以通过配置站点提示智能卡用户在每次访问资源时输入其 PIN 来避免此问题。 [#230942]

http://www.citrix.com.cn/

Web Interface 管理

Web Interface 可为用户提供对 XenApp 应用程序和内容以及 XenDesktop 虚拟桌面的访问权限。 用户可以通过标准 Web 浏览器或 Citrix 联机插件访问其资源。

Web Interface 利用在 Web 服务器上执行的 Java 和 .NET 技术为 XenApp Web 站点动态创建服务器场的 HTML 描述。 服务器场中发布的所有可用资源（应用程序、内容和桌面）均向用户提供。 您可以创建用于访问资源的独立 Web 站点，也可以创建能够集成到企业门户中的 Web 站点。 此外，Web Interface 还允许您配置通过 Citrix 联机插件访问资源的用户设置。

可以使用 Citrix Web Interface Management 控制台在 Microsoft Internet Information Services (IIS) 中创建和配置 Web Interface 站点。 该控制台仅与 Microsoft Internet Information Services 的 Web Interface 一起安装： 有关使用此工具的详细信息，请参阅使用 Citrix Web Interface Management 控制台配置站点。

您也可以编辑站点配置文件 (WebInterface.conf) 来管理 Web Interface 站点。 有关详细信息，请参阅使用配置文件配置站点。

此外，还可以自定义和扩展 XenApp Web 站点。 Web Interface SDK 文档说明了如何使用这些方法配置站点。

Web Interface 功能

通过以下两种 Web Interface 站点类型，可以根据用户需要为用户提供访问其资源的不同方法。

XenApp Web 站点。 可以为用户提供他们可使用 Web 浏览器登录到的 Web 站点。 进行身份验证后，用户可以使用 Citrix 客户端访问联机资源和脱机应用程序。

XenApp Services 站点。 可以将 Citrix 联机插件与 Web Interface 结合使用来将资源与用户的桌面集成。 用户通过单击其桌面上的图标或开始菜单，或者通过在其计算机桌面的通知区域中单击，可访问应用程序、虚拟桌面和联机内容。 您可以确定您的用户可以访问和修改的配置选项（如果有），例如音频、显示和登录设置。

管理功能

更新日期： 2014-11-24

多个服务器场支持。 您可以配置多个服务器场，并且为用户显示所有场中的可用资源。 您可以使用 Citrix Web Interface Management 控制台中的服务器场任务来分别配置每个服务器场。 有关详细信息，请参阅使用配置文件配置站点。

灾难恢复。 您可以指定 XenApp 和 XenDesktop 服务器场，以供用户在无法访问其任何生产场（可能是因为电源故障或网络中断）时紧急使用。 这使您可以进行置备，以应对无法访问所有生产服务器的情况，使行业应用程序或桌面不会突然变得不可用。

共享站点配置。 使用 Microsoft Internet Information Services 的 Web Interface，您可以指定一个通过网络共享其配置文件的“主”站点。 然后，可以将其他站点配置为使用主站点的配置，而不是使用本地文件。

与常用 Web 技术集成。 Web Interface 的 API 可以从 Microsoft 的 ASP.NET 和 Sun Microsystems 的 JavaServer Pages 进行访问。 用于 Java 应用程序服务器的 Web Interface 与平台无关，因此，可以在未将 Microsoft Internet Information Services (IIS) 用作 Web 服务器的 Windows 操作系统上安装它。

资源访问功能

XenApp VM 托管应用程序。 XenApp 具有从虚拟机提供联机应用程序的功能。 通过此功能，您可以发布与远程桌面服务不兼容或尚未针对远程桌面服务进行验证的应用程序，或者发布不支持在 Windows Server 操作系统上安装的应用程序。

用户漫游。 您可以将用户组与特定服务器场相关联，以提供一致的用户体验，而不管用户的当前位置或要登录的服务器。 例如，这使因公在国外旅行的用户可以登录本地 Web Interface 服务器，并自动接收本国/地区场的母语资源。

支持 UNIX 场。 通过支持 XenApp for UNIX 场，Web Interface 可以为用户设备显示和提供在 UNIX 平台上运行的应用程序。

Active Directory 和用户主体名称支持。 所有 Web Interface 组件都与 Microsoft Active Directory 兼容。 访问 XenApp Web 站点的用户可以登录属于 Active Directory 部署的服务器场，并无缝访问应用程序和内容。 登录屏幕与 Active Directory 使用用户主体名称 (UPN) 兼容。

匿名用户。 借助 Web Interface，用户可以通过使用匿名帐户登录 XenApp Web 站点来访问 XenApp 应用程序。

安全功能

安全套接字层/传输层安全性支持。 Web Interface 支持安全套接字层 (SSL) 协议，以便保障 Web Interface 服务器和服务器场之间的通信安全。 在 Web 服务器和支持 SSL 的 Web 浏览器上实现 SSL，可以确保数据在网络中传送的安全性。 Web Interface 使用 Microsoft .NET Framework 实现 SSL 和加密。

Access Gateway 支持。 Citrix Access Gateway 是一种通用的 SSL 虚拟专用网络 (VPN) 设备，该设备与 Web Interface 共同为任何信息资源（数据和语音）提供单一的安全访问点。 Access Gateway 组合了 Internet 协议安全 (IPSec) 和 SSL VPN 的最佳功能，同时避免了成本高且繁琐的实现和管理，它可以通过任何防火墙并支持所有资源和协议。

Secure Gateway 支持。 Secure Gateway 和 Web Interface 共同通过 Internet 为公司内部网络的服务器提供单一、安全的加密访问点。 Secure Gateway 可以简化证书管理，因为只有在 Secure Gateway 服务器上才需要服务器证书，而不是在场中的每个服务器上都需要服务器证书。

智能卡支持。 Web Interface 支持使用智能卡来验证用户身份，以便对应用程序、内容和桌面提供安全访问。 使用智能卡可以简化用户的身份验证过程，同时增强登录的安全性。

票据记录。 此功能可提供增强的身份验证安全性。 Web Interface 将获取对访问资源的用户进行身份验证的票据。 票据具有可配置的到期期限，并且对单一登录有效。 在使用或到期之后，票据将会失效，无法再用于访问资源。 通过使用票据，便无需在 .ica 文件中显式包含 Web Interface 用于连接资源的凭据。

Secure Ticket Authority 冗余。 您可以为通过 Access Gateway 访问其资源的用户配置多个冗余 Secure Ticket Authority (STA)。 这使您可以减少 STA 在用户会话期间变得不可用的几率，防止重新连接会话。 启用冗余后，Web Interface 会尝试从两个不同的 STA 获取两份票据并交付给网关。 如果在用户会话期间无法访问其中一个 STA，将使用另一个 STA 保持会话不中断。

更改密码。 使用显式提供的域凭据登录到 Web Interface 或 Citrix 联机插件的用户，可在 Windows 密码到期时更改其密码。 无论用户的计算机是否位于他们尝试对其验证身份的域中，用户都可以更改密码。

帐户自助服务。 通过与 Citrix Password Manager 提供的帐户自助服务功能集成，用户可以通过回答一系列安全问题，重置其网络密码和解除帐户锁定。

客户端部署功能

基于 Web 的客户端安装。 当用户访问 XenApp Web 站点时，Web Interface 会检测设备和 Web 浏览器类型，并提示用户安装相应的 Citrix 客户端（如果可用）。 增加最新操作系统和 Web 浏览器的安全限制后，会使用户很难下载和部署 Citrix 客户端，因此 Web Interface 提供了一个客户端检测和部署过程，以便引导用户完成客户端部署过程，包括在适当情况下重新配置用户的 Web 浏览器。 这样，即使是在限制最严格的环境中，也可确保用户在访问其资源时获得最佳体验。

Citrix 联机插件支持。 通过 Citrix 联机插件，用户可以直接从其桌面访问资源，而无需使用 Web 浏览器。 Citrix 联机插件的用户界面也可以“锁定”，以防止用户错误配置。

Citrix 脱机插件支持。 通过 Citrix 脱机插件，用户可以将 XenApp 应用程序通过流技术推送到其桌面，并在本地打开它们。 您可以将该插件与 Citrix 联机插件安装在一起，以提供全套 Citrix 客户端应用程序虚拟化功能，也可以将该插件单独安装在用户桌面上，以便用户使用 XenApp Web 站点通过 Web 浏览器访问应用程序。

本版本中的新增功能

更新日期： 2014-12-02

Web Interface 在此版本中提供以下新增功能和增强功能：

更新了最终用户界面。 更新了最终用户的布局和颜色方案，有助于改善导航性能和可读性。

VM 托管应用程序的会话共享。 Web Interface 现在支持虚拟机 (VM) 托管应用程序共享会话。 此功能仅适用于无缝应用程序和非匿名用户。

用户的多桌面访问。 在早期版本的 Web Interface 中，用户仅能访问每个桌面组中某个桌面的单个实例。 现在，用户可以访问桌面组中桌面的多个实例。 有关将桌面分配给用户的详细信息，请参阅 XenDesktop 5 文档。

改善了针对 Access Gateway 的智能卡支持。 现在，针对 Web Interface 的智能卡身份验证与许多环境都兼容。 Web Interface 现在可以接受来自 Access Gateway 的用户主体名称 (UPN) 以及用户名和域。 此外，更新后的 Web Interface 还符合 FIPS 标准。 这项新功能仅能用于智能卡选项的传递身份验证，您必须以域管理员身份登录。 有关针对 Access Gateway 配置智能卡支持的详细信息，请参阅存档的 Access Gateway 文档。

设置其他默认值的功能。 管理员可以针对所有与带宽相关的设置配置默认值，这些设置例如音频质量、颜色深度、带宽配置文件、打印机映射和窗口大小。

ICA 文件签名。 Web Interface 可以对生成的 ICA 文件进行数字签名，以使兼容的 Citrix 客户端和插件能够确认该文件源自受信任的源。

Web Interface 组件

Web Interface 部署涉及与三个网络组件之间的交互：

- 一个或多个服务器场
- 一台 Web 服务器
- 一个具有 Web 浏览器和 Citrix 客户端的用户设备

服务器场

作为单个实体来管理并一起运行以便为用户提供资源服务的一组服务器统称为服务器场。 服务器场由许多服务器组成，所有这些服务器都运行 XenApp 或 XenDesktop，但不能混合运行这二者。

服务器场最重要的功能之一是资源发布。 利用这一过程，管理员可使服务器场提供的特定资源（应用程序、内容和桌面）能够供用户使用。 管理员为一组用户发布资源时，该资源将作为一个对象提供，Citrix 客户端可以连接到该对象并启动会话。

使用 Web Interface，用户可以登录服务器场并接收为其单个用户名发布的自定义资源列表。此资源列表称为资源集。 Web Interface 服务器充当用于连接到一个或多个服务器场的访问点。Web Interface 服务器将在服务器场中查询资源集信息，然后将结果的格式设置为用户可在 Web 浏览器中查看的 HTML 页。

要从服务器场获取信息，Web Interface 服务器将与服务器场中的一台或多台服务器上运行的 Citrix XML Service 进行通信。 Citrix XML Service 是 XenApp 和 XenDesktop 的一个组件，它使用 TCP/IP 和 HTTP 向 Citrix 客户端和 Web Interface 服务器提供资源信息。 此服务充当服务器场和 Web Interface 服务器之间的联系点。 Citrix XML Services 是随 XenApp 和 XenDesktop 一起安装的。

Web 服务器

Web 服务器托管 Web Interface。 Web Interface 提供以下服务：

- 通过一个或多个服务器场对用户进行身份验证
- 检索有关可用资源的信息，包括用户可以访问的资源列表

用户设备

用户设备是能够运行 Citrix 客户端和 Web 浏览器的任何计算设备。 用户设备包括桌面 PC、便携式计算机、网络计算机、终端以及手持计算机等其他设备。

在用户设备中，浏览器和 Citrix 客户端分别作为查看器和引擎配合工作。 通过浏览器，用户可以查看资源集（在 Web Interface 服务器上由服务器端脚本创建），而客户端则充当允许用

户访问资源的引擎。

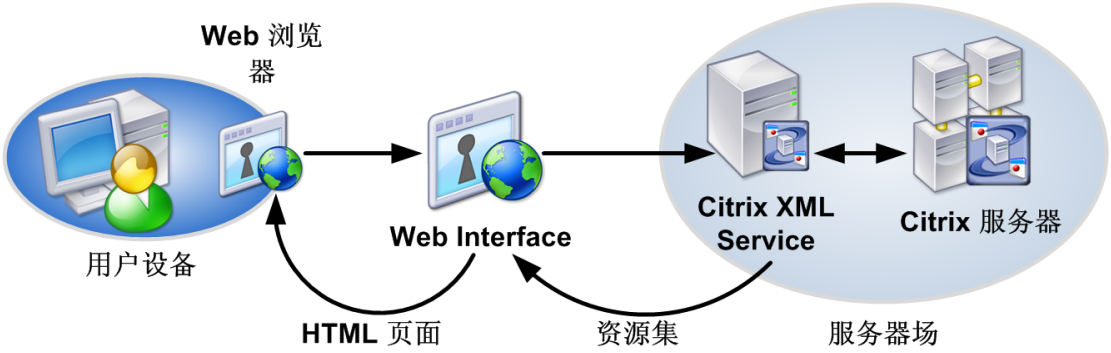
Web Interface 提供基于 Web 的客户端部署，该方法可从 Web 站点部署 Citrix 客户端。 当用户访问使用 Web Interface 创建的站点时，基于 Web 的客户端检测和部署过程将检测设备，并且系统会提示用户部署相应的 Citrix 客户端。 对于某些环境，客户端检测和部署过程还可以检测是否存在已安装的客户端，并且仅在必要时提示用户。 有关详细信息，请参阅配置客户端部署和安装标题。

Web Interface 支持多种浏览器和 Citrix 客户端组合。 有关支持的浏览器和客户端组合的完整列表，请参阅用户设备要求。

Web Interface 的工作方式

下面将介绍服务器场、运行 Web Interface 的服务器以及用户设备之间的典型交互。

下图显示了典型的 Web Interface 交互的示例。 用户设备上的 Web 浏览器向 Web 服务器发送信息，而该服务器与服务器场进行通信，以便为用户提供对资源的访问权限。



- 用户通过 Web 浏览器针对 Web Interface 进行身份验证。
- Web 服务器读取用户的凭据，然后将信息转发给服务器场中的服务器上的 Citrix XML Service。 指定服务器将充当 Web 服务器和场中其他服务器之间的代理。
- 指定服务器上的 Citrix XML Service 从服务器检索用户可以访问的资源列表。 这些资源组成了用户的资源集。 Citrix XML Service 从 Independent Management Architecture (IMA) 系统检索该资源集。
- 在 XenApp for UNIX 场中，指定服务器上的 Citrix XML Service 使用从 ICA 浏览器收集的信息来确定用户可以访问哪些应用程序。
- 然后，Citrix XML Service 将用户的资源集信息返回至该服务器上运行的 Web Interface。
- 用户单击 HTML 页上代表资源的图标。
- 联系 Citrix XML Service，在场中找到最空闲的服务器。 Citrix XML Service 确定最空闲的服务器，并将该服务器的地址返回至 Web Interface。
- Web Interface 与 Citrix 客户端进行通信（某些情况下使用 Web 浏览器作为中介）。
- Citrix 客户端根据 Web Interface 所提供的连接信息启动与场中服务器的会话。

Web Interface 的系统要求

更新日期： 2014-11-24

要运行 Web Interface，您的服务器必须运行支持的 Citrix 产品。

Web Interface 支持以下产品版本：

- Citrix XenApp 7.6 和 XenDesktop 7.6
- Citrix XenApp 7.5 和 XenDesktop 7.5
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7
- Citrix XenDesktop 5.6 Service Pack 1
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenDesktop 5.0 Service Pack 1
- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0 Feature Pack 2 for Microsoft Windows Server 2003 x64
- Citrix XenApp 5.0 Feature Pack 2 for Microsoft Windows Server 2003
- Citrix XenApp 5.0 Feature Pack 1 for Microsoft Windows Server 2008 x64
- Citrix XenApp 5.0 Feature Pack 1 for Microsoft Windows Server 2008
- Citrix XenApp 5.0 Feature Pack 1 for Microsoft Windows Server 2003 x64
- Citrix XenApp 5.0 Feature Pack 1 for Microsoft Windows Server 2003
- Citrix XenApp 5.0 for Microsoft Windows Server 2008 x64
- Citrix XenApp 5.0 for Microsoft Windows Server 2008
- Citrix XenApp 5.0 for Microsoft Windows Server 2003 x64
- Citrix XenApp 5.0 for Microsoft Windows Server 2003

- 适用于 UNIX 操作系统的 Citrix XenApp 4.0 Feature Pack 1
- Citrix Presentation Server 4.5 Feature Pack 1 for Windows Server 2003 x64
- Citrix Presentation Server 4.5 Feature Pack 1 for Windows Server 2003
- Citrix Presentation Server 4.5 for Windows Server 2003 x64
- Citrix Presentation Server 4.5 for Windows Server 2003

重要：为了与适用于 UNIX 的 XenApp 4.0 Feature Pack 1 兼容，需要执行另外的手动站点配置步骤。 有关详细信息，请参阅配置对适用于 UNIX 的 XenApp 4.0 Feature Pack 1 的支持。

Web Interface 可在其支持的所有平台上与这些产品一起运行。 有关支持的平台的列表，请参阅 Citrix 服务器的文档。 Citrix 建议您为服务器上的操作系统安装最新的 Service Pack。

常规配置要求

服务器必须是服务器场的成员。 服务器场中的服务器必须发布有资源（应用程序、内容和/或桌面）。 有关服务器场成员身份和在服务器场中发布资源的详细信息，请参阅 Citrix 服务器文档。

XenApp for UNIX 服务器也必须发布有应用程序。 此外，还必须对这些应用程序进行配置，以便与 Web Interface 配合使用。 有关安装适用于 UNIX 的 Citrix XML Service 和配置应用程序以便与 Web Interface 配合使用的详细信息，请参阅 XenApp for UNIX 文档。

最低软件要求

如果使用的不是最新版本，一些新功能将不可用。 例如，无缝场迁移只有在升级到 XenApp 6.0 时才可用。

下表总结了针对主要 Web Interface 功能的最低软件要求。

注: 要确认在特定版本的 Citrix 产品中是否支持 Web Interface 5.4，请参阅该产品的系统要求。

Web Interface 功能	软件要求
XenApp 场迁移	Citrix XenApp 6.0
用户漫游	Citrix XenDesktop 4.0 Citrix XenApp 6.0
XenApp VM 托管应用程序	Citrix XenApp 5.0 Feature Pack 2
灾难恢复	Citrix XenDesktop 4.0 Citrix XenApp 5.0 Feature Pack 2
Secure Ticket Authority 冗余	Citrix XenDesktop 4.0 Citrix XenApp 5.0 Feature Pack 2 Citrix Access Gateway 4.6 Standard Edition
对 Windows 7 和 Internet Explorer 8.0 的支持	Citrix XenDesktop 4.0 Citrix XenApp 5.0 Feature Pack 2 Citrix 联机插件 11.2 Citrix 脱机插件 5.2
虚拟桌面重新启动	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
特殊文件夹重定向	Citrix XenApp 5.0 适用于 Windows 的 Citrix XenApp Plugin 托管应用程序 11.0
字体平滑	Citrix XenApp 5.0 适用于 Windows 的 Citrix XenApp Plugin 托管应用程序 11.0
对 XenDesktop 的支持	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition 10.250

对 Windows Vista 和 Internet Explorer 7.0 的支持	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 Windows 的 Citrix Presentation Server Clients 10.1
对脱机应用程序的支持	Citrix Presentation Server 4.5 Citrix Streaming Client 1.0 Citrix Program Neighborhood Agent 10.0
AD FS 支持	Citrix Presentation Server 4.5
访问控制策略支持	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 带有高级访问控制的 Citrix Access Gateway 4.2 适用于 32 位 Windows 版本 9.0 的 Citrix MetaFrame Presentation Server Clients
帐户自助服务	Citrix Password Manager 4.0
用户更改密码	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Program Neighborhood Agent 10.1
会话可靠性	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 32 位 Windows 版本 9.0 的 Citrix MetaFrame Presentation Server Clients
工作区控制	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 32 位 Windows 版本 8.0 的 Citrix MetaFrame Presentation Server Client
智能卡支持	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 适用于 32 位 Windows 7.0 的 Citrix ICA Client

Secure Gateway 支持	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 UNIX 操作系统的 Citrix XenApp 4.0 Feature Pack 1 适用于 32 位 Windows 7.0 的 Citrix ICA Client
NDS 身份验证	Citrix Presentation Server 4.5 适用于 32 位 Windows 7.0 的 Citrix ICA Client
DNS 寻址	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 UNIX 操作系统的 Citrix XenApp 4.0 Feature Pack 1 适用于 32 位 Windows 7.0 的 Citrix ICA Client
增强内容发布	Citrix Presentation Server 4.5 适用于 32 位 Windows 7.0 的 Citrix ICA Client
负载平衡	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 UNIX 操作系统的 Citrix XenApp 4.0 Feature Pack 1
服务器端防火墙支持	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 适用于 UNIX 操作系统的 Citrix XenApp 4.0 Feature Pack 1
客户端防火墙支持	适用于 32 位 Windows 7.0 的 Citrix ICA Client
传递身份验证	Citrix Presentation Server 4.5 适用于 32 位 Windows 的 Full Program Neighborhood Client Citrix Program Neighborhood Agent 7.0
远程桌面连接 (RDP)	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

Web 服务器要求

更新日期： 2014-09-24

Citrix 客户端必须存在于对这些客户端进行基于 Web 的部署的服务器上。 有关支持的客户端版本的详细信息，请参阅用户设备要求。 有关将客户端复制到 Web Interface 服务器的详细信息，请参阅将客户端安装文件复制到 Web Interface。

在 Windows 平台上

可以在下列 Windows 平台上安装 Web Interface：

操作系统	Web 服务器	Runtime/JDK	Servlet 引擎

Windows Server 2008 R2 x64 带有 Service Pack 1 的 Windows Server 2008 R2	Internet Information Services 7.5	.NET Framework 3.5 Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	不适用
带有 Service Pack 2 的 Windows Server 2008 x64 版本 带有 Service Pack 2 的 Windows Server 2008 x86	Internet Information Services 7.0		
带有 Service Pack 2 的 Windows Server 2003 R2 x86 带有 Service Pack 2 的 Windows Server 2003 Standard Edition x86 带有 Service Pack 2 的 Windows Server 2003 Enterprise Edition x86 带有 Service Pack 2 的 Windows Server 2003 R2 Standard Edition x86 带有 Service Pack 2 的 Windows Server 2003 R2 Standard Edition x64	Internet Information Services 6.0		
带有 Service Pack 2 的 Windows Server 2003 Standard Edition x86	Apache 2.2.x	Apache 1.6.x	Apache Tomcat 6.0.x

如果要使用 Microsoft Internet Information Services (IIS)，则必须配置服务器以添加相应的服务器角色并安装 IIS 和 ASP.NET（IIS 的一个子组件）。 如果安装 .NET Framework 时未安装 IIS，则必须安装 IIS 并重新安装 .NET Framework，或者安装 IIS 并运行 C:\Windows\Microsoft.NET\Framework\Version 目录中的 aspnet_regiis.exe -i 命令。 .NET Framework 和 J# 可重新分发文件包含在 XenApp 和 XenDesktop 安装介质的 \Support 文件夹中。

用户要求

更新日期： 2014-05-23

用户可以使用以下支持的 Web 浏览器和操作系统组合来访问 Web Interface 站点：

浏览器	操作系统
Internet Explorer 11	Windows 8.1（32 位） Windows 8.1（64 位） Windows 8（32 位） Windows 8（64 位） Windows 2012（64 位） Windows 2012 R2（64 位） 带 Service Pack 1 (SP1) 的 Windows 7（32 位） 带 Service Pack 1 (SP1) 的 Windows 7（64 位） 带 Service Pack 1 (SP1) 的 Windows Server 2008 R2（64 位）
Internet Explorer 10	带 Service Pack 1 (SP1) 的 Windows 7（32 位） 带 Service Pack 1 (SP1) 的 Windows 7（64 位） 带 Service Pack 1 (SP1) 的 Windows Server 2008 R2（64 位）
Internet Explorer 9.x （32 位模式）	带有 Service Pack 2 或更高版本的 Windows Vista（32 位版本） 带有 Service Pack 2 或更高版本的 Windows Vista（64 位版本） Windows 7 RTM 或更高版本（32 位版本） Windows 7 RTM 或更高版本（64 位版本） 带有 Service Pack 2 或更高版本的 Windows Server 2008（32 位版本） 带有 Service Pack 2 或更高版本的 Windows Server 2008（64 位版本） Windows Server 2008 R2（64 位）

Internet Explorer 8.x （32 位模式）	Windows 7（64 位版本） Windows 7（32 位版本） Windows XP Professional Service Pack 3 带有 Service Pack 2 的 Windows XP Professional（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） 带有 Service Pack 2 的 Windows Vista（64 位版本） Windows Server 2008 R2 Windows Server 2008 Service Pack 2 Windows Server 2003 Service Pack 2
Internet Explorer 7.x （32 位模式）	带有 Service Pack 2 的 Windows Vista（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） Windows Server 2008 Service Pack 2 Windows Server 2003 Service Pack 2
Safari 5.x	Mac OS X Snow Leopard 10.6
Safari 4.x	Mac OS X Leopard 10.5
Mozilla Firefox 4.x （32 位模式）	Windows 7（64 位版本） Windows 7（32 位版本） Windows XP Professional Service Pack 3 带有 Service Pack 2 的 Windows XP Professional（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） 带有 Service Pack 2 的 Windows Vista（64 位版本） Windows Server 2003 Service Pack 2

Mozilla Firefox 3.x	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 带有 Service Pack 3 的 Windows XP Professional（32 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） Windows 7（32 位版本） Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003 Service Pack 2
Mozilla 1.7	Solaris 10

注：仅此页面列出的软件版本支持 Web Interface 5.4。 尽管更新版本的软件可能有效，但这些软件尚未经过测试，并且不受支持。

访问脱机应用程序的要求

用户可以使用以下支持的 Web 浏览器和操作系统组合来访问脱机应用程序：

浏览器	操作系统
Internet Explorer 8.x （32 位模式）	Windows 7（64 位版本） Windows 7（32 位版本） 带有 Service Pack 2 的 Windows Vista（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） 带有 Service Pack 2 的 Windows XP Professional（64 位版本） Windows XP Professional Service Pack 3 Windows Server 2008 R2 带有 Service Pack 2 的 Windows Server 2008 x64 版本 Windows Server 2008 Service Pack 2 带有 Service Pack 2 的 Windows Server 2003 x64 版本 Windows Server 2003 Service Pack 2
Internet Explorer 7.x （32 位模式）	带有 Service Pack 2 的 Windows Vista（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） 带有 Service Pack 2 的 Windows XP Professional（64 位版本） Windows XP Professional Service Pack 3 带有 Service Pack 2 的 Windows Server 2008 x64 版本 Windows Server 2008 Service Pack 2 带有 Service Pack 2 的 Windows Server 2003 x64 版本 Windows Server 2003 Service Pack 2

Mozilla Firefox 3.x	Windows 7（64 位版本） Windows 7（32 位版本） 带有 Service Pack 2 的 Windows Vista（64 位版本） 带有 Service Pack 2 的 Windows Vista（32 位版本） 带有 Service Pack 2 的 Windows XP Professional（64 位版本） Windows XP Professional Service Pack 3 Windows Server 2003 Service Pack 2

其他用户设备的要求

用户可以访问瘦客户端上的 Web Interface、个人数字助理 (PDA) 以及具有以下配置的手持式设备：

设备	操作系统	浏览器
iPhone	不适用	Safari 5.x
iPad	不适用	Safari 5.x
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSE V90	Windows XP Embedded Service Pack 2	Internet Explorer 6.x
HP T5730	Windows Embedded Standard 2009	Internet Explorer 7.x
HP T5540	Windows Embedded CE 6.0 R2	Internet Explorer 6.x
HP RK270 WYSE V30	Windows Embedded CE 6.0	Internet Explorer 6.x
HP GY231	Debian Linux 4.0	Debian Iceweasel 2.0
Symbian E61/E70	Symbian	Symbian 浏览器

用户设备要求

要使用 Web Interface，用户设备至少必须安装受支持的 Citrix 客户端或 Web 浏览器（带 Java Runtime Environment）。 XenApp 和 XenDesktop 安装介质随附的所有客户端都与 Web Interface 兼容， 也可从 Citrix Web 站点免费下载这些客户端。

Citrix 建议您为用户部署最新客户端，以确保他们可以利用最新功能。 每个客户端的功能各不相同，有关支持的客户端功能的详细信息，请参阅相关客户端的文档。

安装 Web Interface

使用 XenApp 或 XenDesktop 安装介质来安装 Web Interface。

可以在下列平台上安装 Web Interface：

- 受支持的 Windows 操作系统，其上运行有：
  - Microsoft Internet Information Services (IIS)
  - Apache Tomcat
- 受支持的 UNIX 操作系统，其上运行有：
  - Apache Tomcat
  - IBM WebSphere
  - Sun GlassFish Enterprise Server

有关 Web 服务器安装要求的详细信息，请参阅 Web 服务器要求。

可以通过命令行脚本执行无提示安装和站点管理。 有关如何将命令行与 Web Interface 结合使用的详细信息，请参阅知识中心。

有关如何安装 Web Interface 的详细信息，请参阅在 Microsoft Internet Information Services 上安装 Web Interface和在 Java 应用程序服务器上安装 Web Interface。

安全注意事项

如果计划在基于 Windows 的服务器上安装 Web Interface，Citrix 建议您按照 Microsoft 标准指南来配置 Windows 服务器。 对于 UNIX 实现，请按照制造商针对特定操作系统的建议进行操作。

查看 Citrix XML Service 端口分配

在 Web Interface 站点创建 (IIS) 或 .war 文件生成 (Java) 期间，系统会提示您指定 Citrix XML Service 将使用的端口。 Citrix XML Service 是服务器场和 Web Interface 服务器之间的通信链路。

在 Windows 平台中，可对 Citrix XML Service 进行配置，以共享 Internet Information Services 的 TCP/IP 端口。 在此情况下，要确定 Citrix XML Service 端口，必须找到 Internet Information Services 的 WWW 服务使用的端口。 默认情况下，WWW 服务使用端口 80。 如果 Citrix XML Service 需要使用专用端口，Citrix 建议使用端口 8080。

如需 Windows 平台中使用的端口列表，请在命令提示符下键入 netstat -a。 在 XenApp for UNIX 服务器上，在命令提示符下键入 ctxnfusesrv -l 以查看端口信息。

注: 如有必要，可以更改 Citrix XML Service 在服务器上使用的端口。 有关详细信息，请参阅您的 Citrix 服务器文档。

在 Microsoft Internet Information Services 上安装 Web Interface

安装 Web Interface 之前，必须对服务器进行配置以添加 Web 服务器角色和安装 IIS 与 ASP.NET。

要在 Windows Server 2008 上使用 IIS 7.x，请安装 Web 服务器 (IIS) 角色，然后启用以下角色服务：

- Web 服务器 > 应用程序开发 > ASP.NET
- 管理工具 > IIS 6 管理兼容性 > IIS 6 元数据库兼容性

如果计划启用传递身份验证、通过智能卡传递身份验证和/或智能卡身份验证，则还需要安装以下角色服务：

- 对于传递身份验证和通过智能卡传递身份验证，请启用 Web 服务器 > 安全性 > Windows 身份验证
- 对于智能卡身份验证，请启用 Web 服务器 > 安全性 > 客户端证书映射身份验证

要在 Windows Server 2003 上使用 IIS 6.0，请添加应用程序服务器（IIS、ASP.net）角色并启用 ASP.NET。

在 IIS 上，为每个站点分配一个应用程序池。 应用程序池配置包含一个可以确定最大工作进程数的设置。 如果更改其默认值，则可能无法运行 Web Interface。

配置服务器角色后，请确保已安装 .NET Framework 3.5 Service Pack 1 和 Visual J#.NET 2.0 Second Edition。

如果要从早期版本的 Web Interface（不超过版本 4.5）升级，安装程序将会提示您在升级之前备份现有的站点。

重要：不再支持集中配置的站点和 Conferencing Manager Guest Attendee 站点。 如果从早期版本的 Web Interface 升级，安装程序将删除 Web 服务器上任何现有的 Conferencing Manager Guest Attendee 站点。 任何现有的集中配置站点将会升级，并转换为使用本地配置。

1. 以管理员身份登录。

   如果要从 XenApp 或 XenDesktop 安装介质安装 Web Interface，请将光盘插入 Web 服务器的光驱中。

   如果从 Citrix Web 站点下载了 Web Interface，请将文件 WebInterface.exe 复制到 Web 服务器。

2. 导航到文件 WebInterface.exe 并双击该文件。

3. 从列表中选择语言。 操作系统的语言会自动被检测，并显示为默认选择。 单击确定。

4. 在欢迎页面上，单击下一步。

5. 在许可协议页上，选择我接受许可协议，然后单击下一步。

6. 在安装位置页上，浏览至 Web Interface 的安装位置（默认路径为 C:\Program Files (x86)\Citrix\Web Interface\）。 单击 Next（下一步）。

7. 在 Clients 位置页上，选择将 clients 复制到此计算机。 单击浏览以搜索 Citrix 客户端安装文件的安装介质或您的网络。

   安装程序会将安装介质或网络共享上的 \Citrix Receiver and Plug-ins 文件夹的内容复制到 Web Interface \Clients 文件夹，路径通常为 C:\Program Files (x86)\Citrix\Web Interface\Version\Clients。 通过安装过程创建的所有 Web 站点都假定 Web 服务器在该目录结构中包含客户端文件。

   在 Web Interface 安装期间，如果您不希望将 clients 复制到 Web 服务器，请选择跳过此步骤。 您可以稍后将 clients 复制到服务器。

8. 单击下一步继续，然后再次单击下一步以确认安装准备工作就绪。

9. 安装完成后，单击完成。

10. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management，以访问 Citrix Web Interface Management 控制台，并开始创建和配置您的站点。

与 Windows Server 2003 x64 版本中的其他组件的兼容性

在 64 位版本的 Windows Server 2003 上，安装适用于 Microsoft Internet Information Services 的 Web Interface 会在 IIS 6.0 中启用 32 位 Web 扩展支持，并会禁用 64 位扩展支持。 如果在 64 位版本的 Windows Server 2003 上安装适用于 Microsoft Internet Information Services 的 Web Interface，请确保先安装 Web Interface，然后再安装任何其他 Citrix 软件，包括 XenApp、XenDesktop 和 License Management Console。 此特定安装顺序使各个产品可以在 IIS 6.0 中适应 32 位支持。 如果按错误顺序安装这些产品，访问 Web 服务器时，可能会产生错误消息，例如“Service unavailable”（服务不可用）。

在 Windows Server 2003 x64 版本中安装时，适用于 Microsoft Internet Information Services 的 Web Interface 可能与需要 64 位 ISAPI 过滤器的产品（例如，Windows 组件“HTTP 代理上的 RPC”）不兼容。 在安装 Web Interface 之前，必须先卸载“HTTP 代理上的 RPC”。

卸载“HTTP 代理上的 RPC”

1. 在 Windows 开始菜单中，单击控制面板 > 添加或删除程序。
2. 选择添加/删除 Windows 组件。
3. 选择网络服务，然后单击详细信息。
4. 选中 HTTP 代理上的 RPC 复选框，然后单击确定。
5. 单击下一步卸载“HTTP 代理上的 RPC”并重新启动服务器。

在 Java 应用程序服务器上安装 Web Interface

注: 如果要在 IBM WebSphere 上安装 Web Interface，则会出现一条应用程序安全警告消息，其中指出 was.policy 文件的内容存在问题。 如果您在 Security（安全性）> Global Security（全局安全性）下选择了 Enforce Java 2 Security（强制 Java 2 安全性），则该策略文件是 WebSphere 创建的。 请确保依照 WebSphere Java 2 Security 策略编辑 was.policy 文件，否则，Web Interface 可能无法正常进行。 该策略文件位于 WEBSPHERE_HOME/AppServer/installedApps/NodeName/WARFileName.ear/META-INF。

适用于 Java 应用程序服务器的 Web Interface 需要一个 servlet 引擎才能运行。 Apache Web 服务器需要另外一个 servlet 引擎才可为 Web Interface 提供支持，例如 Tomcat（请注意，Tomcat 可用作独立的 Web 服务器或 servlet 引擎）。

在 Tomcat 上安装 Web Interface

1. 将 WebInterface.jar 文件从安装介质上的 Web Interface 目录复制到临时位置。
2. 从命令提示符处，导航到安装文件的下载目录，然后键入 java -jar WebInterface.jar 运行安装程序。
3. 按 ENTER 键阅读许可协议。
4. 键入 Y 接受许可协议。
5. 从提供的列表中选择站点类型。
6. 通过回答屏幕上出现的问题指定站点的初始配置。
7. 此时将显示所选选项的摘要。 如果站点详细信息是正确的，请键入 Y 创建 .war 文件。此时将创建 .war 文件并从安装介质复制 Citrix 客户端（如果需要）。
8. 按照屏幕上的说明完成 .war 文件的安装。

配置 Sun GlassFish Enterprise Server 的安全策略

在创建 XenApp Web 站点并配置为允许在 Sun GlassFish Enterprise Server 上使用帐户自助服务之前，必须手动配置服务器的安全策略。

1. 在服务器上部署站点的 .war 文件。
2. 停止 Web 服务器。
3. 编辑所部署的域配置目录下的 server.policy 文件。 例如，如果 Sun GlassFish Enterprise Server 安装在 SunGlassFishEnterpriseServerRoot/AppServer 下，并且站

点部署在“domain1”中，则该文件位于 SunGlassFishEnterpriseServerRoot/AppServer/domains/domain1/config。

4. 在添加任何一般 grant 块之前，先添加以下配置：

```
 grant codeBase
"file:${com.sun.aas.instanceRoot}/applications/
j2ee-modules/WARFileName/-"{
permission java.lang.RuntimePermission
"getClassLoader";
permission java.lang.RuntimePermission
"createClassLoader";
permission java.util.PropertyPermission
"java.protocol.handler.pkgs", "read, write";
 };
```

其中 WARFileName 是您站点的 .war 文件的文件名的前面部分，例如“XenApp”。

5. 编辑位于 SunGlassFishEnterpriseServerRoot/ApplicationServer/lib 中的 launcher.xml 文件，以将 javax.wsdl 添加到系统属性 key="com.sun.enterprise.overrideablejavaxpackages" 元素的值列表中。

6. 启动 Web 服务器。

使用语言包

语言包包含将您的站点本地化为特定语言［中文（繁体和简体）、英语、法语、德语、日语、韩语、俄语和西班牙语］所需的全部内容，其中包括：

- 站点的资源文件
- 用户帮助
- 本地化图标和图像

在 IIS 上，可通过复制树或解包 \languages 文件夹（通常为 C:\Program Files (x86)\Citrix\Web Interface\Version\languages）中的文件，将语言包添加到 Web Interface 安装中。 要自定义特定站点的语言，可将语言包复制到该站点的位置并进行修改。 然后，该站点将使用修改后的语言包，而其他站点继续使用默认语言包。

注: 要在 IIS 上以正确的语言显示 Windows 错误消息，必须为 Microsoft .NET Framework 安装相应的语言包。

在 Java 应用程序服务器上，可通过将额外的语言包移动到站点中的相应目录并提取文件来安装这些语言包。

英语语言包用作回退语言，必须始终存在于服务器上。 语言包特定于随其一起提供的 Web Interface 版本，而不能配合更低或更高版本使用。 有关使用语言包的详细信息，请参阅 Web Interface SDK。

删除语言包

某些设备（如运行 Windows CE 的那些设备）无法显示特定语言（例如，日语）。 在这种情况下，用户界面中的语言选择列表将显示不可用语言的块字符。 为避免此问题，可以删除所有站点的语言，或仅删除特定站点的语言。

对于 IIS 上的站点，请删除 \languages 文件夹（通常为 C:\Program Files (x86)\Citrix\Web Interface\Version\languages）中的 LanguageCode.lang（例如 ja.lang）。 此操作将从服务器的所有站点中删除该语言。 如果要为特定站点启用此语言，请将 .lang 文件移至该站点的 \languages 文件夹。

对于 Java 应用程序服务器上的站点，请在创建 .war 文件后，使用相应的工具打开 .war 文件，删除该 .lang 文件，然后重新打包。 此操作将从通过该 .war 文件部署的站点中删除该语言。

升级现有安装

通过从 XenApp 或 XenDesktop 安装介质或者从 Web 下载文件安装 Web Interface，可将版本 4.5 或更高版本的 Web Interface 升级到最新版本。

不能降级到早期版本的 Web Interface。

重要：不再支持集中配置的站点和 Conferencing Manager Guest Attendee 站点。 如果从早期版本的 Web Interface 升级，安装程序将删除 Web 服务器上任何现有的 Conferencing Manager Guest Attendee 站点。 任何现有的集中配置站点将会升级，并转换为使用本地配置。

\Clients 文件夹的目录结构（用于对用户进行基于 Web 的客户端部署）在 Web Interface 5.1 和早期版本中有所不同。 如果使用 XenApp 或 XenDesktop 安装介质升级 Web Interface 安装，请在升级安装时从安装介质中复制目录结构。 如果使用 Web 下载升级，则必须为 Web Interface 安装手动重新创建所需的目录结构。 然后，可以从 Citrix Web 站点下载所需的客户端。 有关 \Clients 目录结构的详细信息，请参阅将客户端安装文件复制到 Web Interface。

默认情况下，Web Interface 假定客户端安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。 如果从 Citrix Web 站点下载客户端或计划部署早期版本的客户端，请检查 XenApp Web 站点的配置文件中是否为 ClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32 和 ClientStreamingWin32 参数指定了相应的客户端安装文件名。 有关 Web Interface 配置文件参数的详细信息，请参阅 WebInterface.conf 参数。

安装后要执行的操作

安装 Web Interface 之后，需要使 Web Interface 对用户可用。 为此，可以使用 Citrix Web Interface Management 控制台创建并配置站点，也可以直接编辑 WebInterface.conf 配置文件。

此外，可能还需要配置 Web Interface 以与安装的其他组件交互，或者可能要自定义或扩展 Web Interface 的功能。

- 有关如何使用控制台或 WebInterface.conf 文件配置 Web Interface 的信息，请分别参阅使用 Citrix Web Interface Management 控制台配置站点或使用配置文件配置站点
- 有关如何使用 Citrix Web Interface Management 控制台配置用于 Access Gateway 或 Secure Gateway 的 Web Interface 的信息，请参阅配置网关设置
- 有关配置 Web Interface 以使用 AD FS 的信息，请参阅配置对 Web Interface 的 AD FS 支持
- 有关安全注意事项的信息，请参阅配置 Web Interface 安全性
- 有关扩展和自定义 Web Interface 功能的信息，请参阅 Web Interface SDK

Web Interface 安装疑难解答

在使用 IIS 的 Windows 平台上，可以使用修复选项对 Web Interface 安装进行故障排除。 如果修复选项不能解决问题，或者此选项不可用（例如，在 Java 应用程序服务器安装中），请尝试卸载 Web Interface，然后再重新安装。 有关详细信息，请参阅卸载 Web Interface。 您必须在重新安装 Web Interface 后重新创建您的所有站点。

使用“修复”选项

如果安装 Web Interface 时遇到问题，请尝试使用修复选项来解决该问题。 修复选项会重新安装常用文件，而不会修复或替换现有站点。

重要：如果 Web interface 安装包括自定义代码并且您选择修复选项，该自定义代码会被删除。 Citrix 建议您在使用此选项之前，先备份您自定义的任何文件。

1. 双击 WebInterface.exe 文件。
2. 选择修复并单击下一步。
3. 按照屏幕上的说明进行操作。

卸载 Web Interface

卸载 Web Interface 时，将删除所有 Web Interface 文件，包括 \Clients 文件夹。 因此，如果要保留任何 Web Interface 文件，请在卸载 Web Interface 之前将其复制到其他位置。

有时，Web Interface 卸载程序可能会失败。 可能的原因包括：

- 卸载程序的注册表访问权限不足
- 安装 Web Interface 后从系统中删除了 IIS

在 Microsoft Internet Information Services 上卸载 Web Interface

1. 在 Windows 开始菜单中，依次单击控制面板 > 程序和功能。
2. 选择 Citrix Web Interface，然后单击卸载。
3. 按照屏幕上的说明进行操作。

在 Java 应用程序服务器上卸载 Web Interface

如果 Web 服务器提供了用于帮助您卸载 Web 应用程序的工具，请按照制造商建议的过程来卸载 Web Interface。 或者，可以手动卸载 Web Interface。

1. 从命令提示符处，导航到最初将 .war 文件复制到的目录。
2. 停止 Web 服务器并删除 .war 文件。

   可能还需要删除 .war 文件所展开到的目录。 通常，该目录与 .war 文件处于相同目录中并且名称相同。 例如，“mysite.war”的内容将展开到一个名为 /mysite 的目录中。

   注: 卸载 Web Interface 时，某些文件可能仍保留在服务器上。 有关保留的文件的详细信息，请参阅 Citrix XenApp 自述文件。

Web Interface 入门

更新日期： 2014-11-24

确定要使用的配置方法

可以使用 Citrix Web Interface Management 控制台或配置文件来配置和自定义 Web Interface。

使用 Citrix Web Interface Management 控制台

Citrix Web Interface Management 控制台是 Microsoft 管理控制台 (MMC) 3.0 管理单元，可用于创建和配置在 Microsoft Internet Information Services (IIS) 中托管的 XenApp Web 和 XenApp Services 站点。 Web Interface 站点类型显示在左窗格中。 中间的结果窗格显示在左窗格中选择的站点类型容器中的可用站点。

通过 Citrix Web Interface Management 控制台，可以快速轻松地执行日常管理任务。 操作窗格列出了当前可用的任务。 与左窗格中选择的项目相关的任务显示在顶部，适用于结果窗格中所选项目的操作显示在下面。

使用控制台时，配置将在您使用控制台提交更改后生效。 因此，如果某些 Web Interface 设置的值与当前配置不相关，并在 WebInterface.conf 中将相应设置重置为其默认值，则可能会禁用这些 Web Interface 设置。 Citrix 建议您为您的站点创建 WebInterface.conf 和 config.xml 文件的定期备份。

在安装适用于 Microsoft Internet Information Services 的 Web Interface 时，会自动安装 Citrix Web Interface Management 控制台。 通过依次单击开始 > 所有程序 > Citrix > Management Consoles > Citrix Web Interface Management 来运行此控制台。

注：必须确保安装 Web Interface 的服务器上安装有 MMC 3.0，这是安装 Citrix Web Interface Management 控制台的必备条件。 默认情况下，可在支持托管 Web Interface 的所有 Windows 平台上使用 MMC 3.0。

使用配置文件

可以编辑以下配置文件来配置 Web Interface 站点：

- Web Interface 配置文件。 使用 Web Interface 配置文件 WebInterface.conf 可以更改许多 Web Interface 属性；可在 Microsoft Internet Information Services (IIS) 和 Java 应用程序服务器中获取该文件。 您可以使用此文件执行日常管理任务以及自定义更多设置。 编辑 WebInterface.conf 中的值并保存更新文件以应用更改。 有关使用 WebInterface.conf 配置 Web Interface 的详细信息，请参阅使用配置文件配置站点。

- Citrix 联机插件配置文件。 可以在 Web Interface 服务器上使用 config.xml 文件配置 Citrix 联机插件。

在 Java 应用程序服务器上创建站点

在 Java 应用程序服务器上，运行 Web Interface 安装程序可以创建新站点。 该安装程序会为站点创建自定义 .war 文件，您随后可安装该文件（通常是将 .war 文件放在 Servlet 引擎的相应位置）。 您可以通过编辑解压缩的 .war 文件的内容来修改站点，以及通过删除 .war 文件来删除站点。

使用 Citrix Web Interface Management 控制台配置站点

Citrix Web Interface Management 控制台是 Microsoft 管理控制台 (MMC) 3.0 管理单元，可用于创建和配置在 Microsoft Internet Information Services (IIS) 中托管的 XenApp Web 和 XenApp Services 站点。 Web Interface 站点类型显示在左窗格中。 中间的结果窗格显示在左窗格中选择的站点类型容器中的可用站点。

通过 Citrix Web Interface Management 控制台，可以快速轻松地执行日常管理任务。 操作窗格列出了当前可用的任务。 与左窗格中选择的项目相关的任务显示在顶部，适用于结果窗格中所选项目的操作显示在下面。

使用控制台时，配置将在您使用控制台提交更改后生效。 因此，如果某些 Web Interface 设置的值与当前配置不相关，并在 WebInterface.conf 中将相应设置重置为其默认值，则可能会禁用这些 Web Interface 设置。 Citrix 建议您为您的站点创建 WebInterface.conf 和 config.xml 文件的定期备份。

在安装适用于 Microsoft Internet Information Services 的 Web Interface 时，会自动安装 Citrix Web Interface Management 控制台。 通过依次单击开始 > 所有程序 > Citrix > Management Consoles > Citrix Web Interface Management 来运行此控制台。

注: 必须确保安装 Web Interface 的服务器上安装有 MMC 3.0，这是安装 Citrix Web Interface Management 控制台的必备条件。 默认情况下，可在支持托管 Web Interface 的所有 Windows 平台上使用 MMC 3.0。

使用配置文件配置站点

可以编辑以下配置文件来配置 Web Interface 站点：

- Web Interface 配置文件。 使用 Web Interface 配置文件 WebInterface.conf 可以更改许多 Web Interface 属性；可在 Microsoft Internet Information Services (IIS) 和 Java 应用程序服务器中获取该文件。 您可以使用此文件执行日常管理任务以及自定义更多设置。 编辑 WebInterface.conf 中的值并保存更新文件以应用更改。 有关使用 WebInterface.conf 配置 Web Interface 的详细信息，请参阅使用配置文件配置站点。

- Citrix 联机插件配置文件。 可以在 Web Interface 服务器上使用 config.xml 文件配置 Citrix 联机插件。

共享配置

对于 IIS 上托管的站点，可以指定 Web Interface 站点从一个“主”站点来获取其配置，该主站点应已配置为通过网络共享其配置文件。 设置相应的文件权限后，可以通过在本地站点的 bootstrap.conf 文件中指定主站点配置文件 (WebInterface.conf) 的绝对路径，来允许其他站点共享主站点的配置。 对于使用共享配置的 XenApp Services 站点，Web Interface 也会尝试从为 WebInterface.conf 指定的同一目录中读取 Citrix 联机插件配置文件 (config.xml)。

在将站点修改为从共享文件获取其配置后，将无法直接管理该站点的配置。 必须改用控制台，或在托管主站点的 Web 服务器上直接编辑配置文件，来更改主站点的配置。 对主站点的配置进行的任何更改都会影响共享主站点的配置文件的所有其他站点。 共享配置不适用于 Java 应用程序服务器上托管的站点。

共享站点配置

1. 设置相应的文件共享权限，以允许通过网络访问主站点的 \conf 文件夹（通常为 C:\inetpub\wwwroot\Citrix\SiteName\conf）以及站点配置文件 (WebInterface.conf)（通常位于 \conf 文件夹中）。 对于 XenApp Services 主站点，需要为 Citrix 联机插件配置文件 (config.xml)（通常也位于站点的 \conf 文件夹中）设置相同的权限。

2. 使用文本编辑器，为将从共享配置文件获取其配置的站点打开 bootstrap.conf 文件（通常位于 \conf 文件夹中）。

3. 更改 ConfigurationLocation 参数的设置以指定主站点的配置文件的绝对网络路径，例如：

   ConfigurationLocation=\\ServerName\ShareName\WebInterface.conf

在 Microsoft Internet Information Services 上创建站点

使用 Citrix Web Interface Management 控制台中的创建站点任务，可以创建以下站点之一：

- XenApp Web 站点。 针对使用 Web 浏览器访问资源的用户。
- XenApp Services 站点。 针对使用 Citrix 联机插件访问资源的用户。

通过此任务可以指定托管站点的 IIS 位置、要应用更改的 URL 以及站点的身份验证设置。 可在以后使用站点维护任务更新这些设置。 只有运行 Web Interface 的服务器上的本地管理员才能创建站点。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 Citrix Web Interface 容器。
3. 在操作窗格中，单击创建站点。
4. 选择要创建的站点类型。
5. 为站点指定 URL 和名称。
6. 按照屏幕上的说明创建站点。

Microsoft Internet Information Services 托管

使用 Citrix Web Interface Management 控制台中站点维护下的管理 IIS 托管任务，可以更改 IIS 中的 Web Interface 站点的位置。

指定身份验证点

更新日期： 2014-12-02

在使用 Citrix Web Interface Management 控制台创建 XenApp Web 站点时，必须指定身份验证点，它是部署中进行用户身份验证的点。

在 Web Interface 上进行身份验证

您可以通过使用一系列内置身份验证方法的 Web Interface 来启用用户身份验证，这些身份验证方法包括显式身份验证、传递身份验证和智能卡身份验证。 有关 Web Interface 身份验证方法的详细信息，请参阅为 Web Interface 配置身份验证。

在 Active Directory 联合身份验证服务帐户合作伙伴处进行身份验证

您可以启用 Active Directory 联合身份验证服务 (AD FS) 部署的帐户合作伙伴，以访问 XenApp 应用程序。 这样，就可以为帐户合作伙伴上的用户提供访问应用程序的权限。

如果您打算创建 AD FS 集成站点，需要注意以下内容：

- XenDesktop 不支持 AD FS 身份验证。
- 对于用于 Java 应用程序服务器的 Web Interface，不提供 AD FS 支持。
- Java 客户端和嵌入的远程桌面连接 (RDP) 软件不支持访问 AD FS 集成站点。
- AD FS 集成站点仅支持使用 AD FS 进行身份验证。 不支持其他身份验证方法。
- 创建 AD FS 集成站点后，不能将该站点配置为使用内置身份验证或 Access Gateway 身份验证，而不使用 AD FS 身份验证。

有关详细信息，请参阅配置对 Web Interface 的 AD FS 支持。

在 Access Gateway 进行身份验证

可通过 Access Gateway 为显式和智能卡身份验证启用用户凭据的身份验证和传递。 可通过使用策略来控制用户对资源的访问。

如果用户使用显式凭据登录 Access Gateway，则默认情况下会启用传递身份验证。 用户登录 Access Gateway 并且无需针对 Web Interface 重新进行身份验证即可访问其资源。 为增强安全性，可禁用传递身份验证，以便在显示资源集之前提示用户输入密码。

如果用户使用智能卡登录 Access Gateway，则不需要重新进行身份验证即可访问 Web Interface。 但在默认情况下，会在用户访问资源时提示其输入 PIN。 您可以对站点进行配置，使用户无需提供 PIN 便可访问其 XenApp 资源。 XenDesktop 不支持此功能。

可以随时使用 Citrix Web Interface Management 控制台中的身份验证方法任务更新这些设置。

在使用 Kerberos 的第三方进行身份验证

可以使用第三方联合/单点登录产品验证用户身份并将用户身份映射到 Active Directory 用户帐户。 然后，可以使用 Kerberos 单点登录到 Web Interface。 有关 Kerberos 的详细信息，请参阅配置 Kerberos 登录。

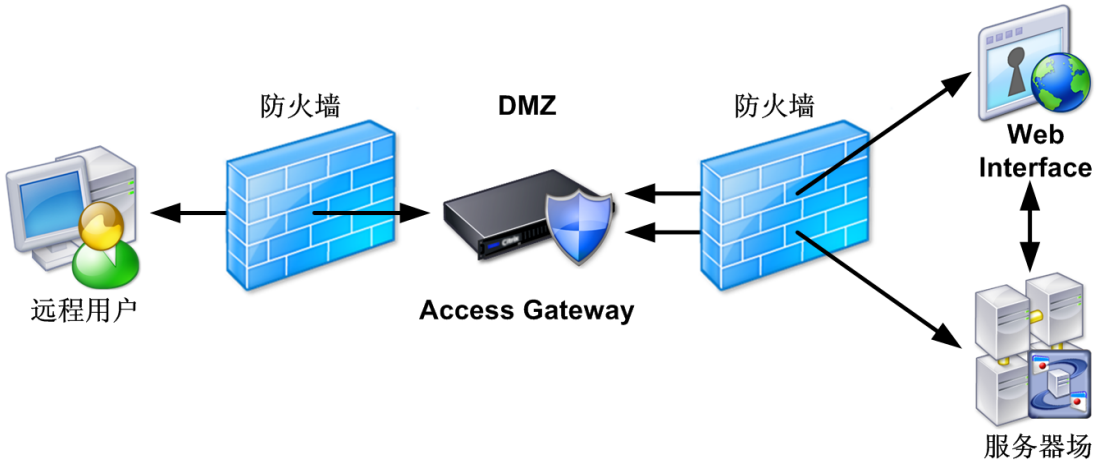
在 Web 服务器上进行身份验证

可以在使用 Kerberos 的 Web 服务器上启用用户身份验证。 有关 Kerberos 的详细信息，请参阅配置 Kerberos 登录。

将 Access Gateway 与 Web Interface 一起部署

在将 Access Gateway 与 Web Interface 一起部署时，Citrix 建议将 XenApp/XenDesktop 以及 Web Interface 都安装在内部网络中的服务器上，将 Access Gateway 设备安装在隔离区 (DMZ) 内。

下图显示了将 Access Gateway 与 Web Interface 一起部署时的推荐配置。



DMZ 是位于安全的内部网络与 Internet（或任何外部网络）之间的子网。 在 DMZ 中部署 Access Gateway 时，用户将使用 Citrix 安全访问插件或 Citrix 客户端访问 Access Gateway。 根据所配置的访问策略，用户登录时，Access Gateway 将验证用户的身份，然后将用户定向到各自的资源。

使用户可以使用资源

通过 Access Gateway，用户可以登录领域（对于 Access Gateway Standard Edition）、登录点（对于 Access Gateway Advanced Edition 和 Access Gateway 5.0）或虚拟服务器（对于 Access Gateway Enterprise Edition）以访问各自的资源。 您可以通过配置领域、登录点或虚拟服务器以提供对 XenApp Web 站点的访问权限，从而使用户可以使用资源。

Access Gateway 提供了多种用于集成 Web Interface 创建的 XenApp Web 站点的方法，包括：

- 将 XenApp Web 站点配置为领域、登录点或虚拟服务器的默认主页。 用户登录后，即可看到 XenApp Web 站点。
- 将 XenApp Web 站点内嵌在 Access Interface 中。 选择 Access Interface 作为默认主页时，XenAPP Web 站点将与文件共享、访问中心和 Web 应用程序一起显示。 Access Interface 仅可用于 Access Gateway Advanced Edition 和 Enterprise Edition。

将 XenApp Web 站点与 Access Gateway 相集成

更新日期： 2014-10-30

要将站点与 Access Gateway 相集成，请创建一个 XenApp Web 站点，并在 Access Gateway 中为该站点配置 Web 资源。

创建与 Access Gateway 集成的站点

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 Citrix Web Interface 容器。
3. 在操作窗格中，单击创建站点。
4. 选择 XenApp Web 并单击下一步。
5. 在指定 IIS 位置页上，指定站点的 IIS 位置、路径和名称。 单击 Next（下一步）。
6. 在指定身份验证点页上，选择在 Access Gateway，然后单击下一步。
7. 在指定 Access Gateway 设置页上的身份验证服务 URL 框中，键入 Access Gateway 身份验证服务的 URL。
8. 指定用户登录 Access Gateway 的方式，然后单击下一步：
   - 如果您的用户使用用户名和密码登录 Access Gateway，请选择显式。 要通过禁用从 Access Gateway 向 Web Interface 传递用户凭据来提高安全性，请选中在显示应用程序和桌面之前提示用户输入密码复选框。
   - 如果用户使用智能卡登录 Access Gateway，请选中智能卡。 为智能卡选项启用传递身份验证前，确保以域管理员身份登录。

   重要：与 Access Gateway 集成的 XenApp Web 站点可以支持显式身份验证或智能卡身份验证，但不同时支持两者。 如果有的用户使用显式身份验证来登录 Access Gateway，有的用户使用智能卡身份验证来登录 Access Gateway，则必须针对每种身份验证方法创建并配置不同站点。 然后，对 Access Gateway 进行配置，以将用户定向到适用于其身份验证方法的相应站点。
9. 如果要针对显式身份验证配置站点，请继续步骤 10。 如果要配置智能卡身份验证，请在指定智能卡设置页上，指定是否要求用户在可访问资源之前提供 PIN。
   - 如果您需要用户每次访问资源时都输入 PIN，请选择提示用户输入 PIN。 要启用此功能，还需要执行其他配置步骤。 有关详细信息，请参阅允许智能卡用户在提供 PIN 的情况下通过 Access Gateway 访问资源。

     注：对于使用与登录 Access Gateway 时所用智能卡相同的智能卡登录桌面的 Windows XP 用户，您可以允许这些用户在访问资源时不必提供 PIN。 有关详细信息，请参阅允许智能卡用户在提供 PIN 的情况下通过 Access Gateway 访问资源。
   - 如果要允许所有用户在访问 XenApp 资源时都不必提供 PIN，请选择启用智能卡传递。 XenDesktop 不支持此功能，仅当 Web 服务器与您的用户在同一域中时才能使用此功能。 您可能需要重新启动 Web 服务器，以启用从 Access Gateway 中通过智能卡传递服务。 要启用此功能，还需要执行其他配置步骤。 有关详细信息，请参阅允许智能卡用户在不提供 PIN 的情况下通过 Access Gateway 访问资源。

     注：默认情况下，会为所有域用户启用从 Access Gateway 中通过智能卡传递。 要限制允许的用户列表，请编辑 PTSAccess.txt 文件的用户权限，该文件通常位于 C:\Program Files (x86)\Citrix\DeliveryServices\ProtocolTransitionService\ 目录中。

10. 确认新站点的设置并单击下一步以创建站点。

通过 Access Gateway 提供对站点的访问

这些步骤概述了如何通过 Access Gateway 提供对站点的访问。 有关详细信息，请参阅适用于您的 Access Gateway 版本的文档，存档在此处。

1. 配置 XenApp 或 XenDesktop，使其与 Access Gateway 通信。
2. 配置 Access Gateway，以提供对 XenApp Web 站点的访问。

   重要：请以 domain 而不是 domain.com 的格式指定域。 Web Interface 的从 Access Gateway 中通过智能卡传递服务无法识别 domain.com 格式的域，所以如果以这种方式指定域，用户将无法登录。

3. 请确保为 Access Gateway 和 Web Interface 都正确配置了工作区控制（仅适用于 Access Gateway Advanced Edition）和会话超时设置。

允许智能卡用户在不提供 PIN 的情况下通过 Access Gateway 访问资源

如有要允许所有用户不必提供 PIN 即可访问其 XenApp 资源，必须为托管 XenApp Web 站点的 IIS 站点启用安全套接字层 (SSL)。 有关详细信息，请参阅适用于 IIS 7.x 和 IIS 6.0 的 Microsoft 文档。

在启用 SSL 后，请确保 Web 服务器与您的用户在同一个域中，并配置 Active Directory 以允许受限委派。

确保该域位于正确的功能级别

重要：要提升域级别，域中的所有域控制器都必须正在运行 Windows Server 2008 或 Windows Server 2003。 如果您拥有或者计划添加运行 Windows Server 2003 的域控制器，请不要将域功能级别提升至 Windows Server 2008。 在提升域功能级别后，将无法回滚至较低的级别。

1. 以域管理员的身份登录域控制器，并打开 MMC Active Directory 域和信任管理单元。
2. 在左窗格中，选择域名，然后在操作窗格中单击属性。
3. 如果域未处于可能达到的最高功能级别，请选择域名并在操作窗格中单击 Raise Domain Functional Level（提升域功能级别）。
4. 要提升域功能级别，请单击相应级别，然后单击 Raise（提升）。

信任运行 Web Interface 和 Citrix XML Service 的服务器进行委派

1. 以域管理员的身份登录域控制器，并打开 MMC Active Directory 用户和计算机管理单元。
2. 在视图菜单上，单击 Advanced Features（高级功能）。
3. 在左窗格中，单击计算机节点并选择 Web 服务器。
4. 在操作窗格中，单击属性。
5. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和 Use any authentication protocol（使用任意身份验证协议），然后单击添加。
6. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
7. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix XML Service 的服务器的名称，然后单击确定。
8. 从列表中选择 http 服务类型，然后单击确定。
9. 在 Delegation（委派）选项卡上，确认运行 Citrix XML 服务的服务器的 http 服务类型显示在 Services to which this account can present delegated credentials（此帐户可以提出委派凭据的服务）列表中，然后单击确定。
10. 对场中运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的每台服务器，重复步骤 3-9。
11. 在左窗格中，单击计算机节点，然后选择运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的服务器。
12. 在操作窗格中，单击属性。
13. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和仅使用 Kerberos，然后单击添加。
14. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
15. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix XML Service 的服务器的名称，然后单击确定。
16. 从列表中选择 HOST（主机）服务类型，然后单击确定。
17. 在委派选项卡上，确认运行 Citrix XML Service 的服务器的 HOST（主机）类型显示在此帐户可以提出委派凭据的服务列表中，然后单击确定。
18. 对场中运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的每台服务器，重复步骤 11-17。
19. 出于安全原因，必须将场中的所有服务器配置为进行受限委派。 要为用户提供对这些服务器中的资源的访问权限，必须将相关服务（如用于 Web 服务器的 http 服务）添加到 Services to which this account can present delegated credentials（此帐户可以提

出委派凭据的服务）列表中。

有关更多详细信息，请参阅 Citrix 知识中心中的 Service Principal Names and Delegation in Presentation Server（《Presentation Server 中的服务主体名称和委派》）白皮书 (CTX110784)。

确定可从服务器场访问哪些资源

1. 以域管理员的身份登录域控制器，并打开 MMC Active Directory 用户和计算机管理单元。
2. 在左窗格中，单击计算机节点并从场中选择服务器。
3. 在操作窗格中，单击属性。
4. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和仅使用 Kerberos，然后单击添加。
5. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
6. 在 Select Users or Computers（选择用户或计算机）对话框的 Enter the object names to select（输入要选择的对象名称）框中，键入服务器的名称，然后单击确定。
7. 从列表中选择 cifs 和 ldap 服务类型，然后单击确定。

   注：如果 ldap 服务显示两个选项，请选择一个与域控制器的 FQDN 匹配的选项。
8. 在 Delegation（委派）选项卡上，确认域控制器的 cifs 和 ldap 服务类型显示在 Services to which this account can present delegated credentials（此帐户可以提出委派凭据的服务）列表中，然后单击确定。
9. 对场中的每台服务器重复此过程。

在域级别配置访问资源的时间限制

警告：注册表编辑器使用不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。

默认情况下，用户有权访问网络上的资源 15 分钟。 您可以通过在运行 Citrix XML Service 的服务器上修改以下注册表项，来增加该时间限制：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\S4UTicketLifetime

该值指定在会话开始后用户有权访问资源的分钟数。

域安全策略会控制可以对 S4ULifetime 设置的最大值。 如果为 S4UTicketLifetime 指定的值大于在域级别指定的值，则域级别的设置将优先。

1. 以域管理员的身份登录域控制器，并打开 MMC 域安全策略管理单元。
2. 在左窗格中，选择 Account Policies（帐户策略）> Kerberos Policy（Kerberos 策略）。

3. 在结果窗格中，选择 Maximum lifetime for service ticket（服务票据的最长寿命）。
4. 在操作窗格中，单击属性。
5. 在 Ticket expires in（票据到期时间）框中输入所需的时间限制（以分钟为单位）。

如果不想配置访问资源的时间限制，请在确定可以访问服务器场中的哪些资源时，选择 Use any authentication protocol（使用任意身份验证协议）。 如果选择此选项，将会忽略为 S4UTicketLifetime 指定的任何值。 有关详细信息，请访问 Microsoft Web 站点：http://support.microsoft.com/。

允许智能卡用户在提供 PIN 的情况下通过 Access Gateway 访问资源

更新日期： 2014-07-04

如果希望智能卡用户每次通过 Access Gateway 访问资源时都输入 PIN，则必须在 Citrix XML Service 中启用对用户的安全标识符 (SID) 的枚举。

警告：注册表编辑器使用不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。

1. 如果用户帐户存在于与包含服务器场的域不同的域中，请确保这些域共享双向信任关系。
2. 确认 Citrix XML Service 可以解析 IP 地址并联系用户帐户域的域控制器。 如果 Citrix XML Service 无法与域控制器通信，对 Citrix XML Service 的请求可能会超时。
3. 向运行 Citrix XML Service 所用的 Windows 帐户授予对每个域的 Active Directory 中的 TGGAU 属性的读取访问权限。 有关 TGGAU 属性的详细信息，请参阅 Microsoft 知识库文章 331951。 默认情况下，将 Citrix XML Service 配置为以网络服务帐户运行。 可通过将此帐户添加到以下内置 Active Directory 组中来授予所需权限：
   - Pre-Windows 2000 Compatibility Access
   - Windows Authorization Access
4. 在运行 Citrix XML Service 的服务器上，导航到系统注册表中的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\XMLService\。
5. 在 XMLService 节点下，添加名为 EnableSIDEnumeration 的 DWORD 值并将该值设置为 1。

   注：对于 XenDesktop 5 及更高版本，注册表项为 [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer] "EnableXmlServiceSidEnumeration"=REG_DWORD:1
6. 在 Web 服务器中重新启动 IIS。 如果要使新权限立即生效而不等到 Kerberos 票证缓存期到期，请重新启动运行 Citrix XML Service 的服务器。
7. 如果 Windows XP 用户在登录桌面时使用的智能卡与登录 Access Gateway 时使用的智能卡相同，则配置通过智能卡传递身份验证便可允许这些用户在不提供 PIN 的情况下访问其资源：
   a. 使用管理员帐户在用户设备上安装 Citrix 联机插件或 Citrix Desktop Viewer。
   b. 将客户端模板添加到组策略对象编辑器。 有关详细信息，请参阅步骤 1：为实现智能卡身份验证安装插件。
   c. 使用组策略为所有 Citrix 客户端启用传递身份验证。 有关详细信息，请参阅步骤 1：为实现智能卡身份验证安装插件。

协调 Web Interface 和 Access Gateway 设置

某些 XenApp 和 XenDesktop 设置可以在 Web Interface 和 Access Gateway 中进行配置。 但是，由于与 Access Gateway 集成的 XenApp Web 站点可由多个领域（用于 Access Gateway Standard Edition）、登录点（用于 Access Gateway Advanced Edition）或虚拟服务器（用于 Access Gateway Enterprise Edition）引用，因此有可能一个领域、登录点或虚拟服务器将 XenApp Web 站点嵌入其 Access Interface，而另一个领域、登录点或虚拟服务器将该站点显示为其默认主页。 这会导致与某些资源设置冲突。

为确保您的设置按预期运行，请按照下面的说明操作：

- Session time-out（会话超时）。 确保所有领域、登录点或虚拟服务器使用与 XenApp Web 站点相同的设置。
- 工作区控制。 对于 Access Gateway Advanced Edition，为将 XenApp Web 站点作为其主页的登录点禁用所有工作区控制设置。 这样可确保使用在 Web Interface 中配置的设置。 所有其他登录点可根据需要配置工作区控制。

指定站点的初始配置设置

使用控制台创建站点后，可通过选中“创建站点”向导最后一页上的立即配置此站点复选框来指定初始配置设置。 使用“指定初始配置”向导可配置与一个或多个服务器场的通信，以及指定可供用户使用的资源类型。

指定服务器场

配置新站点时，必须输入将为站点用户提供资源的服务器场的详细信息。

可以随时使用 Citrix Web Interface Management 控制台中的服务器场任务更新这些设置。有关配置与服务器场的通信的详细信息，请参阅管理服务器和场。

重要：为了与适用于 UNIX 的 XenApp 4.0 Feature Pack 1 兼容，需要执行另外的手动站点配置步骤。 有关详细信息，请参阅配置对适用于 UNIX 的 XenApp 4.0 Feature Pack 1 的支持。

指定身份验证方法

在配置使用身份验证点在 Web Interface 创建的新 XenApp Web 站点时，可以指定用户在登录到 Web Interface 时如何进行身份验证。

可以随时使用 Citrix Web Interface Management 控制台中的身份验证方法任务更新这些设置。有关配置身份验证的详细信息，请参阅为 Web Interface 配置身份验证。

指定域限制

在配置使用身份验证点在 Web Interface 创建的新 XenApp Web 站点时，可以仅限特定域中的用户能够访问该站点。

可以随时使用 Citrix Web Interface Management 控制台中的身份验证方法任务更新这些设置。有关配置域限制的详细信息，请参阅配置域限制设置。

指定登录屏幕的外观

配置新的 XenApp Web 站点时，可以指定用户的登录屏幕的样式。 既可以选择其中只显示相应登录字段的简约布局，也可以选择包含导航栏的布局。

可以随时使用 Citrix Web Interface Management 控制台中的 Web 站点外观任务更新此设置。有关自定义用户界面的外观的详细信息，请参阅为用户自定义外观。

指定可供用户使用的资源类型

在配置新站点时，必须指定您要使其可用的资源类型。 Web Interface 通过 Web 浏览器或 Citrix 联机插件为用户提供对资源（应用程序、内容和桌面）的访问权限。 通过与脱机应用程序功能集成，用户可以将应用程序通过流技术推送到其桌面，并在本地打开它们。

可按如下所示为用户授予对资源的访问权限：

- 联机。 用户可以访问远程服务器上托管的应用程序、内容和桌面。 用户需要网络连接才能处理其资源。
- 脱机。 用户可以将应用程序通过流技术推送到其桌面并在本地将其打开。 对于 XenApp Service 站点，在传递应用程序后，用户即可随时运行这些应用程序，而无需连接到网络。 对于 XenApp Web 站点，用户需要网络连接才能登录到站点并启动其应用程序。 在运行应用程序后，无需对连接进行维护。
- 双模式。 用户可以在同一个站点上访问脱机应用程序和联机应用程序、内容和桌面等所有内容。 如果脱机应用程序不可用，将在可能时提供联机版本。

可以随时使用 Citrix Web Interface Management 控制台中的资源类型任务更新此设置。 有关 Citrix 客户端类型的详细信息，请参阅管理客户端。

升级现有站点

如果要从早期版本（版本 4.5 及更低版本）的 Web Interface 升级您的安装，则对升级现有站点（Conferencing Manager Guest Attendee 站点除外）提供了支持。

重要：不再支持 Conferencing Manager Guest Attendee 站点。 如果从早期版本的 Web Interface 升级，安装程序将删除 Web 服务器上任何现有的 Conferencing Manager Guest Attendee 站点。

按如下方式处理现有访问平台/XenApp Web 和 Program Neighborhood Agent Services/XenApp Services 站点：

- 本地配置的站点。 安装期间，Web Interface 安装程序会自动将所有本地配置的站点升级到最新版本。
- 集中配置的站点和分组站点。 安装期间，Web Interface 安装程序会自动将任何现有的集中配置的站点或分组站点转换为使用本地配置。 转换后的站点随后将升级到最新版本。

默认情况下，Web Interface 假定客户端安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。 如果从 Citrix Web 站点下载客户端或计划部署早期版本的客户端，请检查 XenApp Web 站点的配置文件中是否为 ClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32 和 ClientStreamingWin32 参数指定了相应的客户端安装文件名。 有关 Web Interface 配置文件参数的详细信息，请参阅 WebInterface.conf 参数。

使用站点任务

要配置站点，请在 Citrix Web Interface Management 控制台的左窗格中选择站点类型，然后在结果窗格中单击该站点并在操作窗格或操作菜单中选择可用任务。 或者，可以在结果窗格中右键单击站点名称并从上下文菜单中选择任务。

有些任务仅适用于某些站点类型和配置。 下面的表中提供了适用于每种站点类型的任务的详细信息。

任务	XenApp Web 站点		XenApp Services 站点		AD FS 集成站点
	联机/双模式	仅脱机	联机/双模式	仅脱机	
身份验证方法	*	*			
身份验证方法	*	*	*	*	*
客户端代理	*		*		*
客户端部署	*	*			*
资源刷新			*	*	
资源类型	*	*	*	*	*
安全访问	*		*		*
服务器场	*	*	*	*	*
服务器设置			*	*	
会话选项			*		
会话首选项	*	*			*
快捷方式			*	*	
站点维护	*	*	*	*	*
Web 站点外观	*	*			*
工作区控制	*				*

修复和卸载站点

使用 Citrix Web Interface Management 控制台中站点维护下的修复站点和卸载站点任务，可以分别修复和删除站点。 卸载站点将从系统中完全删除它，并且您将无法再对该站点执行任务。

重要：如果为站点创建了脚本和图像并运行修复站点任务，则会删除这些自定义文件。 使用管理 IIS 托管任务时，也会删除自定义文件。 Citrix 建议您在使用其中一项任务之前，先备份所创建的任何文件。

使用户可以使用 Web Interface

安装并配置 Web Interface 后，请向用户通知登录屏幕的 URL。 如果用户要将此页面加入到其 Web 浏览器书签中，Citrix 建议将该书签设置为 http://ServerName/SitePath，而不指定具体页面（例如 login.aspx）。

在 Java 应用程序服务器上，站点路径（主机名称和端口后面的 URL 部分）由 servlet 引擎确定。 在 servlet 引擎内安装 .war 文件时，您可以修改此路径。 此路径通常默认为 /WARFileName，其中 WARFileName 是站点 .war 文件名的第一部分。

直接访问站点

如果用户直接或通过使用 Citrix 安全访问插件的 Access Gateway Enterprise Edition 访问 XenApp Web 站点，则可以启用对资源 URL 的支持。 这样，用户便可以创建使用 Web Interface 访问的资源的持久链接。

注：对于通过 Access Gateway Standard Edition 或 Advanced Edition 访问站点的用户，或通过 Access Gateway Enterprise Edition 使用无客户端访问的用户，资源 URL 不受支持。

用户可以将持久链接添加到其快捷方式列表或桌面。 要使用 Citrix Web Interface Management 控制台启用对资源 URL 的支持，请单击左窗格中的 XenApp Web 站点，在结果窗格中选择站点，在操作窗格中单击会话首选项，单击持久 URL，然后选中使用户可以通过浏览器书签访问资源复选框。

重要：启用此功能会禁用跨站点请求伪造保护。

将登录屏幕设置为 Microsoft Internet Information Services 的默认屏幕

您可以将 Web Interface 登录屏幕设置为 Web 服务器用户的默认屏幕，使 URL 为 http://ServerName/。 为此，请在创建站点时或此后任何时间，在 Citrix Web Interface Management 控制台的站点维护下的管理 IIS 托管任务中，选中设置为 IIS 站点的默认页面复选框。

管理服务器和场

更新日期： 2014-11-24

本部分介绍如何将 Web Interface 配置为与服务器场进行通信。 此外，还介绍了如何配置和管理服务器设置，以及在运行 Citrix XML 服务的服务器之间启用负载平衡。

密码更改注意事项

如果您的服务器场之间存在差异，则存在可能阻止用户更改其密码的其他问题。 例如：

- 域策略可能阻止用户更改密码
- 当单个站点将 XenApp for UNIX 场与 XenApp for Windows 和/或 XenDesktop 场聚合在一起时，只能更改 Windows 密码

Citrix 建议您在这些情况下禁用用户密码更改。

聚合多个场时，请确保站点配置文件中所列的第一个场要么在运行 Presentation Server 4.5 或更高版本，要么在运行 XenDesktop。

如有必要，可以在混合服务器场部署中启用密码更改。 Web Interface 将按照服务器场的定义顺序访问服务器场，直至某个服务器场报告密码已成功更改，此时才会停止该过程。 这样，您就可以指定要向其发出密码更改请求的服务器场。 如果密码更改请求失败，将会向序列中的下一个服务器场发出密码更改请求。 在服务器场之间使用合适的密码复制机制，可以确保用户密码保持一致。

添加服务器场

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器场。
4. 单击添加。
5. 在场名称框中输入服务器场的名称。
6. 在服务器设置区域中，单击添加以指定服务器名称。 要更改服务器名称，请从列表中选择名称，然后单击编辑。 要删除服务器名称，请选择名称，然后单击删除。
7. 如果指定了多个服务器名称，请从列表中选择名称，然后单击上移或下移将这些名称按相应的故障转移顺序放置。

重要：为了与适用于 UNIX 的 XenApp 4.0 Feature Pack 1 兼容，需要执行另外的手动站点配置步骤。 有关详细信息，请参阅配置对适用于 UNIX 的 XenApp 4.0 Feature Pack 1 的支持。

配置容错

Web Interface 可以在运行 Citrix XML Service 的服务器之间提供容错功能。 使用 Citrix Web Interface Management 控制台中的服务器场任务可以配置容错功能。 如果与服务器通信时出错，则在在以下时间内绕过任何有故障的服务器框中指定的时间过去之前，Web Interface 不会尝试与有故障的服务器联系，但仍会继续与服务器列表上的其他服务器进行通信。

默认情况下，绕过有故障的服务器的时间是 1 小时。 如果列表上的所有服务器均未能响应，则 Web Interface 将每 10 秒重新尝试与服务器联系。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器场。
4. 单击添加（如果要添加场），或者从列表中选择一个名称并单击编辑以配置现有场。
5. 在服务器列表上，按优先级顺序对服务器进行排列。 从列表中选择名称，然后单击上移或下移将这些名称按相应顺序排列。
6. 在在以下时间内绕过任何有故障的服务器框中，更改绕过有故障的服务器的时间长度。

在服务器之间启用负载平衡

更新日期： 2014-11-25

您可以在运行 Citrix XML Service 的服务器之间启用负载平衡。 通过启用负载平衡，可以在这些服务器之间均匀分配连接，以便不会出现任何服务器过载。 默认情况下禁用负载平衡。

如果与一台服务器通信时出现错误，将在列表中的其余服务器之间对所有更多通信进行负载平衡。 系统会在特定时间段（默认为一小时）内绕过有故障的服务器，但您可以使用 Citrix Web Interface Management 控制台中的服务器场任务更改此设置。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器场。
4. 单击添加（如果要添加场），或者从列表中选择一个名称并单击编辑以配置现有场。
5. 在服务器列表中，添加要用于负载平衡的服务器。
6. 选中使用服务器列表实现负载平衡复选框。
7. 在在以下时间内绕过任何有故障的服务器框中，更改绕过有故障的服务器的时间长度。

配置一个场中所有服务器的设置

您可以使用 Citrix Web Interface Management 控制台中的服务器场任务，指定 Citrix XML Service 如何在 Web Interface 和运行 XenApp 或者 XenDesktop 的服务器之间传输数据。 Citrix XML Service 是 XenApp 和 XenDesktop 的组件，充当服务器场和 Web Interface 服务器之间的联系点。 默认情况下，端口号是在创建站点期间输入的值。 此端口号必须与 Citrix XML Service 使用的端口号一致。

此外，还可以为服务器生成的票据指定到期时间。 票据记录避免了将用户凭据通过 .ica 文件从 Web 服务器发送到用户设备，为显式登录提供了增强的身份验证安全性。

默认情况下，每个 Web Interface 票据的有效时间都是 200 秒。 例如，由于到期的票据无法针对服务器场对用户进行身份验证，如果您希望调整该时间以适应网络性能，则可以更改票据寿命。 如果更改正在运行 Citrix XML Service 的服务器的 IP 地址或其他地址，票据记录只有在重新启动服务器之后才能起作用。 在更改服务器的 IP 地址或者其他地址之后，请确保重新启动服务器。

指定所有服务器的设置

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器场。
4. 单击添加（如果要添加场），或者从列表中选择一个名称并单击编辑以配置现有场。
5. 在通信设置区域中，在 XML Service 端口框中输入端口号。 此端口号必须与 Citrix XML Service 使用的端口号一致。
6. 从传输类型列表中，选择下列选项之一：
   - HTTP。 通过标准 HTTP 连接发送数据。 如果对此链接的安全性进行了其他设置，请使用此选项。
   - HTTPS。 通过使用安全套接字层 (SSL) 或传输层安全性 (TLS) 的安全 HTTP 连接发送数据。 必须确保 Citrix XML Service 设置为与 Internet Information Services (IIS) 共享其端口，并确保 IIS 配置为支持 HTTPS。
   - SSL Relay。 通过使用 SSL Relay（在运行 XenApp 或 XenDesktop 的服务器上运行）执行主机身份验证和数据加密的安全连接发送数据。
7. 如果您使用的是 SSL Relay，请在 SSL Relay 端口框中指定 SSL Relay 的 TCP 端口（默认端口为 443）。 Web Interface 在对运行 SSL Relay 的服务器进行身份验证时使用根证书。 确保运行 SSL Relay 的所有服务器都配置为监听同一端口。

   注：如果您使用的是 SSL Relay 或 HTTPS，请确保所指定的服务器名称与运行 XenApp 或 XenDesktop 的服务器的证书上的名称完全一致（包括大小写）。
8. 要配置票据记录，请单击票据记录设置。
9. 在 ICA 票据寿命框中为用于联机资源的 Citrix 客户端输入票据寿命。
10. 在流票据寿命框中输入 Citrix 脱机插件的票据寿命。

指定高级服务器设置

更新日期： 2014-12-02

使用高级场设置对话框，可以启用套接字池和内容重定向，指定 Citrix XML Services 超时持续时间，以及指定在认定失败之前尝试联系 Citrix XML Services 的次数。

启用套接字池

启用套接字池后，Web Interface 会保留一个套接字池，而不是在每次需要时创建一个套接字，并在连接关闭时将其返回至操作系统。 启用套接字池可以提高性能，特别是对于 SSL 连接。

套接字池仅适用于使用身份验证点在 Web Interface 或在 Access Gateway 创建的站点，并在默认情况下启用。 如果 Web Interface 配置为使用一个或多个运行 XenApp for UNIX 的服务器，则不应使用套接字池。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器场。
4. 单击高级。
5. 在套接字池区域中，选中启用套接字池复选框。

启用内容重定向

您可以使用 Citrix Web Interface Management 控制台中的服务器场任务，为各个 XenApp Services 站点启用和禁用从插件到服务器的内容重定向。 此设置将覆盖为 XenApp 配置的任何内容重定向设置。

在启用从插件到服务器的内容重定向时，运行 Citrix 联机插件的用户使用服务器提供的应用程序打开联机内容和本地文件。 例如，使用本地运行的电子邮件程序接收电子邮件附件的 Citrix 联机插件用户可在联机应用程序中打开该附件。 禁用内容重定向时，用户使用本地安装的应用程序打开联机内容和本地文件。

默认情况下，为 XenApp Services 站点启用从插件到服务器的内容重定向。

通过将应用程序与文件类型相关联，可以配置从插件到服务器的内容重定向。 有关文件类型关联的详细信息，请参阅将已发布应用程序与文件类型相关联。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。

3. 在操作窗格中，单击服务器场。

4. 单击高级。

5. 在内容重定向区域中，选中启用内容重定向复选框。

配置 Citrix XML Service 通信

默认情况下，与 Citrix XML Service 的联系将在一分钟后超时，在两次尝试与该服务进行通信均不成功之后，该服务将被视为失败。 可以使用 Citrix Web Interface Management 控制台中的服务器场任务更改这些默认设置。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。

3. 在操作窗格中，单击服务器场。

4. 单击高级。

5. 要配置 Citrix XML Service 超时持续时间，请在套接字超时框中输入相应的值。

6. 要指定在将 Citrix XML Service 视为失败并绕过它之前尝试与该服务联系的次数，请在尝试联系 XML Service 的次数框中输入一个值。

管理服务器设置

使用 Citrix Web Interface Management 控制台中的服务器设置任务，可以配置 Citrix 联机插件如何与站点通信，以及在出现站点故障时是否将用户重定向到备用站点。

配置服务器通信设置

使用服务器通信设置可以：

- 启用 SSL/TLS 以进行通信。 默认情况下，未在插件和 Web Interface 服务器之间启用智能卡登录和通过 SSL/TLS 保障安全的通信。 您可以从此对话框中启用 SSL/TLS 通信，强制 URL 自动应用 HTTPS 协议。 此外，还必须在运行 XenApp 或者 XenDesktop 的服务器上启用 SSL。
- 允许用户自定义服务器 URL。 服务器 URL 会将 Citrix 联机插件定向到正确的配置文件。 默认路径是根据安装过程中输入的服务器地址确定的。 您可以允许用户更改 URL，该操作将在 Citrix 联机插件选项对话框的服务器选项页面上启用服务器 URL 框。
- 配置自动刷新。 您可以定义插件应刷新其配置设置的频率。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器设置。
4. 要在 Citrix 联机插件和站点之间使用安全通信，请选择使用 SSL/TLS 实现插件与站点之间的通信。
5. 要允许用户更改 URL，从而将 Citrix 联机插件定向到配置文件，请选择允许用户自定义服务器 URL。
6. 要配置 Citrix 联机插件刷新其配置设置的频率，请选择按以下周期安排自动刷新，然后在刷新周期中输入小时数、天数、周数或年数。

指定 Citrix 联机插件备份 URL

如果主 Web Interface 服务器不可用，可以为 Citrix 联机插件指定要联系的备份服务器。 使用 Citrix Web Interface Management 控制台中的服务器设置任务可以指定备份服务器的 URL。 在出现服务器故障时，用户将自动连接到最初在备份站点路径列表中指定的备份服务器。 如果此服务器出现故障，Citrix 联机插件会尝试联系列表中的下一台服务器。

重要：所有备份 URL 必须指向与主站点同类型的 Web 服务器上托管的站点。 例如，如果主站点是针对 Microsoft Internet Information Services 的 Web Interface 站点，则任何备份站点也必须是针对 Microsoft Internet Information Services 的 Web Interface 站点。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器设置。
4. 单击备份。
5. 单击添加。
6. 在备份 URL 框中输入用户连接到的站点的 URL。 可以为每个站点最多定义五个备份 URL。
7. 单击确定。
8. 如果指定了多个备份服务器 URL，请从列表中选择 URL，然后单击上移或下移将这些 URL 按相应的故障转移顺序放置。

配置站点重定向

使用重定向设置可以定义何时将用户重定向到其他站点。 例如，您要为 HR 部门创建一个新站点，并希望将旧站点中的所有用户重定向到不包含这些用户的新站点，同时无需手动输入 URL。您可以使用 Citrix Web Interface Management 控制台中的服务器设置任务指定新站点的详细信息。 这样，用户将会立即或者在下一次启动 Citrix 联机插件时重定向到该新站点。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击服务器设置。
4. 单击重定向。
5. 选择下列选项之一：
   - 如果您不希望配置站点重定向，请选择不重定向
   - 如果您希望立即将用户重定向到备用站点，请选择刷新 Citrix 联机插件配置时重定向
   - 如果您希望在下次启动插件时将用户重定向到备用站点，请选择 Citrix 联机插件下次启动时重定向
6. 在重定向 URL 框中输入备用站点的 URL。

为 Web Interface 配置身份验证

更新日期： 2014-11-25

身份验证方法

当用户访问资源（应用程序、内容和桌面）时，将进行身份验证。 如果身份验证成功，则会显示用户资源集。

可以针对 Web Interface 配置以下身份验证方法：

- 显式（XenApp Web 站点）或提示（XenApp Services 站点）。 用户需要提供用户名和密码才能登录。 可以使用用户主体名称 (UPN)、基于 Microsoft 域的身份验证和 Novell 目录服务 (NDS)。 对于 XenApp Web 站点，还可以使用 RSA SecurID 和 SafeWord 身份验证。

  注：Novell 身份验证无法用于适用于 Java 应用程序服务器的 Web Interface，且不受 XenApp 6.0、XenApp 5.0 for Windows Server 2008 或 XenDesktop 支持。 但是，XenApp 6.0 与 Novell Domain Services for Windows 兼容。

- 传递。 用户可以使用在登录到其物理 Windows 桌面时提供的凭据进行身份验证。 用户不需要重新输入其凭据，其资源集可自动显示。 此外，还可以使用集成了 Kerberos 的 Windows 身份验证连接到服务器场。 如果指定了 Kerberos 身份验证选项，但 Kerberos 失败，传递身份验证也将失败，用户将无法进行登录。 有关 Kerberos 的信息，请参阅配置 Kerberos 登录。

- 通过智能卡传递。 用户可以通过向连接到用户设备的智能卡读卡器中插入智能卡来进行身份验证。 如果用户安装了 Citrix 联机插件，则当用户登录到用户设备时，系统会提示用户输入其智能卡 PIN。 登录后，用户可以访问其资源，而不会再出现其他登录提示。 系统不会提示连接到 XenApp Web 站点的用户输入 PIN。 如果要配置 XenApp Services 站点，可以使用集成了 Kerberos 的 Windows 身份验证连接到 Web Interface，并使用智能卡针对服务器场进行身份验证。 如果指定了 Kerberos 身份验证选项，但 Kerberos 失败，传递身份验证也将失败，用户将无法进行登录。

  注：由于 Windows Vista 引入了安全增强功能，因此即使启用通过智能卡传递身份验证，运行 Windows Vista 或 Windows 7 的智能卡用户也仍需在访问应用程序时提供其 PIN。

- 智能卡。 用户可以使用智能卡进行身份验证。 系统将提示用户输入智能卡 PIN。

  注：传递身份验证、通过智能卡传递身份验证和智能卡身份验证无法用于适用于 Java 应用程序服务器的 Web Interface。

- 匿名。 匿名用户可以在不提供用户名和密码的情况下进行登录，并访问针对匿名用户发布的资源。

  重要：匿名用户尽管未由 Web Interface 进行身份验证，但仍可获取 Secure Gateway 票据。 由于 Secure Gateway 依赖于仅向已通过身份验证的用户颁发票据的 Web Interface，因此这将削弱使用 Secure Gateway 的安全优势之一。

注：XenDesktop 不支持匿名用户。

身份验证建议

如果打算启用传递身份验证、通过智能卡传递身份验证或智能卡身份验证，需要注意以下内容：

- 如果用户使用智能卡登录到其计算机，并且您希望启用传递身份验证，请选择使用 Kerberos 身份验证的选项
- 如果用户使用显式凭据登录到其计算机，请不要对访问 Web Interface 的用户启用智能卡身份验证或通过智能卡传递身份验证

  注：如果用户使用显式凭据登录 Windows，并在随后访问配置为通过智能卡传递身份验证的站点，在他们访问资源时，系统将向其显示欢迎使用 Windows 对话框。 要取消此对话框，用户必须按右 Alt (Alt GR) + Delete。 Citrix 建议为使用智能卡登录的用户和使用显式凭据登录的用户创建独立的站点。

如果更改了针对 Web Interface 进行身份验证的方法，则会向当前登录的所有用户显示错误消息。 如果其中的任何用户正在通过 Web 浏览器访问 Web Interface，则必须关闭并重新启动其浏览器，然后再尝试重新登录。

配置身份验证

使用 Citrix Web Interface Management 控制台中的身份验证方法任务，可以配置用户针对 XenApp、XenDesktop 和 Citrix 联机插件进行身份验证的方式。

配置域限制设置

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并确保匿名身份验证不是为用户启用的唯一身份验证方法。
4. 单击属性并选择域限制。
5. 指定是否仅限选定域中的用户访问。 选择以下选项：
   - 如果不希望基于域限制访问，请选择允许任何域
   - 如果希望仅限选定域中的用户访问，请选择限制到以下域
6. 单击添加。
7. 在登录域框中，输入要添加到域限制列表中的任何域名。

   注：要仅限来自特定域的用户访问，必须在域和 UPN 限制列表中输入相同的域名。 有关详细信息，请参阅使用基于域的身份验证。

配置自动登录设置

使用 Citrix Web Interface Management 控制台中的身份验证方法任务，可以为使用传递身份验证、通过智能卡传递身份验证和智能卡身份验证访问其资源的用户配置自动登录设置。

如果匿名身份验证是为用户启用的唯一身份验证方法，则这些用户会自动登录，而不管设置是由管理员还是用户配置。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法，并选中传递、通过智能卡传递和智能卡复选框中的一个或多个。
4. 单击属性并选择自动登录。

5. 指定是否希望允许用户自动登录，以及是否将在帐户设置屏幕上向用户显示启用和禁用自动登录的选项。

使用基于域的身份验证

如果要使用显式或提示身份验证，请使用 Citrix Web Interface Management 控制台中的身份验证方法任务，来配置用户是否使用 Windows 或 Novell 目录服务 (NDS) 进行身份验证。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并根据需要选中显式、提示和/或传递复选框。
4. 单击属性并选择身份验证类型。
5. 选择 Windows 或 NIS (UNIX)。
6. 指定用户登录的凭据格式。 选择下列选项之一：
   - 要允许用户以用户主体名称 (UPN) 或域用户名格式输入其登录详细信息，请选择域用户名和 UPN
   - 要指定用户只能以域用户名格式输入其登录详细信息，请选择 Domain user name only（仅限域用户名）
   - 要指定用户只能以 UPN 格式输入其登录详细信息，请选择 UPN only（仅限 UPN）
7. 单击设置。
8. 在域显示区域中，配置以下设置：
   - 指定是否在登录屏幕上显示域框。
   - 指定是否使用域列表预填写域框以供用户选择，或用户是否必须在域框手动输入值

     注：如果用户在登录时收到“Domain must be specified”（必须指定域）错误消息，这可能是因为域框为空。 要解决此问题，请选择隐藏域框。 如果场中仅包含 XenApp for UNIX 服务器，请在 Domain list（域列表）框中选择预填写，并添加 UNIX 作为域名。
   - 指定要在登录屏幕的域框中显示的域
9. 在 UPN 限制区域中，配置以下设置：
   - 指定是否接受所有 UPN 后缀。 默认情况下，允许所有 UPN 后缀。
   - 指定要接受的 UPN 后缀。

     注：要仅限来自特定域的用户访问，必须在域和 UPN 限制列表中输入相同的域名。有关详细信息，请参阅配置身份验证。

使用 Novell 目录服务身份验证

如果要使用显式或提示身份验证，请使用 Citrix Web Interface Management 控制台中的身份验证方法任务，来配置用户是否使用 Windows 或 Novell 目录服务 (NDS) 进行身份验证。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并根据需要选中显式、提示和/或传递复选框。
4. 单击属性并选择身份验证类型。
5. 选择 NDS。
6. 在默认树名称框中输入一个名称。
7. 单击设置并相应配置上下文限制或无上下文身份验证。

   注：默认情况下，eDirectory 不提供对 cn 属性的匿名连接访问，而无上下文身份验证需要该形式的访问。 有关如何重新配置 eDirectory 的信息，请访问 http://developer.novell.com/wiki/index.php/Developer_Home。
8. 对于 XenApp Services 站点，如果希望安装了 Novell 客户端的 Citrix 联机插件用户使用其 Windows 凭据进行传递身份验证，请选择 Use Windows credentials（使用 Windows 凭据）。

启用显式身份验证

如果启用显式身份验证，用户必须具有用户帐户并提供相应的凭据才能登录。

您可以使用控制台更改显式身份验证设置。 例如，可以配置是否允许用户在会话中更改其密码。

显式身份验证仅适用于 XenApp Web 站点。

启用显式身份验证

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中显式复选框。
4. 单击属性为显式身份验证配置更多设置。

配置显式身份验证的密码设置

使用 Citrix Web Interface Management 控制台中的身份验证方法任务，可以为用户配置密码更改和密码过期提醒选项。 某些密码设置会受到为站点配置的其他身份验证设置的影响。

- 如果在双因素身份验证页面上选择了 RSA SecurID 和 使用 Windows 密码集成选项，将禁用在任何时间选项。

- 选择使用 Active Directory 组策略中的提醒设置选项可能意味着将根据您当前的 Windows 策略来配置提醒设置。 如果当前的 Windows 策略未设置提醒周期，则在密码过期之前，用户将收不到更改其当前密码的提醒。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。

3. 在操作窗格中，单击身份验证方法并选中显式复选框。

4. 单击属性，然后选择密码设置。

5. 如果希望用户能够在一次 Web Interface 会话中更改其密码，请选中允许用户更改密码复选框。

6. 要指定用户何时可以更改其密码，请选择以下选项之一：

   - 要在密码过期时允许用户进行更改，请选择仅在过期时。 选择此选项后，如果用户由于密码过期而无法登录到 Web Interface，则会将其重定向到更改密码对话框。 更改密码后，系统将使用新密码自动为用户登录。

   - 要允许用户在 Web Interface 中随时更改其密码，请选择在任何时间。 选择此选项后，用户的应用程序和帐户设置屏幕上将显示更改密码按钮。 当用户单击该按钮时，将出现一个对话框，用户可在其中输入新密码。

7. 要配置一条用于在密码过期之前通知用户的提醒消息，请选择以下选项之一：

   - 如果不希望在密码过期之前通知用户，请选择不提醒。

   - 要使用您当前的 Windows 策略提醒设置，请选择使用 Active Directory 组策略中的提醒设置。

   - 要提醒用户其密码将在指定的天数后过期，请选择使用自定义提醒设置。 在 Remind users before expiry（在密码过期之前提醒用户）框中，指定天数、周数或年数。

启用双因素身份验证

如果需要，可使用 Citrix Web Interface Management 控制台中的身份验证方法任务为用户启用双因素身份验证。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中显式复选框。
4. 单击属性并选择双因素身份验证。
5. 从双因素设置列表中选择要使用的双因素身份验证的类型，然后适当地配置任何其他设置。

有关配置 Aladdin SafeWord、RSA SecurID 和 RADIUS 身份验证的详细信息，请参阅配置双因素身份验证。

配置帐户自助服务

通过与 Password Manager 提供的帐户自助服务功能集成，用户可以通过回答一系列安全问题，重置其网络密码和解除帐户锁定。

为站点启用帐户自助服务，会将敏感的安全功能暴露给任何可以访问该站点的用户。 如果您的站点可从 Internet 访问，则对哪些用户可以访问这些功能没有任何限制。 如果您的组织的安全策略将用户帐户管理功能限制为仅供内部使用，则必须确保不能从内部网络之外访问该站点。

重要：当设置 Password Manager 时，应指定哪些用户能够重置密码和解锁其帐户。 如果对 Web Interface 启用这些功能，根据配置的 Password Manager 设置，仍可以拒绝用户执行这些任务的权限。

帐户自助服务仅供使用 HTTPS 连接访问 Web Interface 的用户使用。 如果用户使用 HTTP 连接访问 Web Interface，则不能使用帐户自助服务。 帐户自助服务无法供 Access Gateway 集成站点使用。

帐户自助服务不支持 UPN 登录，例如 username@domain.com。

在为站点配置帐户自助服务之前，必须确保：

- 该站点配置为使用基于 Windows 的显式身份验证。
- 该站点配置为仅使用一项 Password Manager Service。 如果 Web Interface 配置为使用同一域或受信任域中的多个场，Password Manager 必须配置为接受来自所有这些域中的凭据。
- 该站点配置为允许用户在希望启用密码重置功能时随时更改其密码。

配置帐户自助服务

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中显式复选框。
4. 单击属性并选择帐户自助服务。
5. 指定是否希望用户能够重置其密码或解锁其帐户。
6. 在密码管理器服务 URL 框中输入 Password Manager 的 URL。

启用提示身份验证

更新日期： 2014-11-24

如果启用提示身份验证，用户必须具有用户帐户并提供相应的凭据才能登录。

提示身份验证仅适用于 XenApp Services 站点。

启用提示身份验证

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中提示复选框。
4. 单击属性为提示身份验证配置更多设置。

配置提示身份验证的密码设置

使用 Citrix Web Interface Management 控制台中的身份验证方法任务，可以指定用户是否可以保存其密码和为用户配置密码更改选项。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中提示复选框。
4. 单击属性，然后选择密码设置。
5. 要允许用户保存其密码，请选择允许用户保存密码选项。
6. 如果希望用户能够在密码过期时更改其密码，请选中允许用户通过联系相关人员更改过期的密码复选框。
7. 通过选择以下选项之一，指定路由更改密码请求所通过的路径：
   - 如果希望 Citrix 联机插件用户通过直接连接到域控制器更改其密码，请选择域控制器(直接)。 此选项最为安全，因为密码更改请求将绕过 Web Interface 和 XenApp/XenDesktop，而直接从 Citrix 联机插件路由到域控制器。
   - 如果希望 Citrix 联机插件用户通过直接连接到域控制器更改其密码，但要在首选连接方法失败时通过 Web Interface 和 XenApp/XenDesktop 启用连接，请选择域控制器(

直接)，回退到服务器场。

- 如果希望 Citrix 联机插件用户通过 Web Interface 和 XenApp/XenDesktop 连接到域控制器来更改其密码，请选择服务器场。 此选项可确保当用户更改其密码时，能够使用新密码更新 Web Interface 以及 XenApp 和/或 XenDesktop。 但是，由于通过更多的网络连接来路由新密码，因此可能会导致安全性降低。

启用 Pass-Through 身份验证

更新日期： 2013-02-21

使用控制台，您可以为通过用户名、密码和域凭据登录其物理桌面的用户启用传递身份验证。 通过此功能，用户可以使用在登录其物理 Windows 桌面时提供的凭据进行身份验证。 用户不需要重新输入凭据，其资源集可自动显示。

传递要求

要使用传递身份验证功能，则必须在 IIS 上运行 Web Interface，并且用户必须运行支持的 Internet Explorer 版本。 对于 XenApp Web 站点，用户必须使用 Internet Explorer 将该站点添加到 Windows“可信站点”或“本地 Intranet 区域”。

如果您使用的是 Internet Explorer 版本 7 或更高版本，请执行以下操作：

1. 将此站点添加到 Windows“可信站点”，单击“Internet 选项”并浏览到“安全”选项卡。
2. 突出显示“可信站点”区域，单击“自定义级别”。
3. 导航到“安全设置”窗口底部的“用户身份验证”，单击“登录”，并将其设置为“使用当前用户名和密码自动登录”。

对于在 Windows Server 2008 上运行的 IIS 7.x，请确保为 Web 服务器 (IIS) 角色启用了 Web 服务器 > 安全 > Windows 身份验证角色服务。

重要：如果您的服务器运行的版本低于 Citrix MetaFrame XP Feature Release 2，则用户可在使用传递时查看所有应用程序和内容。

如果用户使用的 Windows 客户端的版本低于 6.30 并启用了 ICA 加密 (SecureICA)，则无法使用传递身份验证。 要将传递与 ICA 加密一起使用，用户必须安装最新的 Citrix 客户端。 对于用于 Java 应用程序服务器的 Web Interface，传递身份验证不可用。

重要：当用户访问资源时，会将一个文件发送至 Citrix 客户端（某些情况下使用 Web 浏览器作为中介）。 该文件可以包含一个设置，用于指示客户端将用户的工作站凭据发送到服务器。 默认情况下，客户端不会采用此设置；不过，如果在 Citrix 联机插件上启用了传递功能，则将会存在风险，攻击者可能会向用户发送文件，导致用户的凭据被错误路由到未经授权的服务器或假冒服务器。 因此，请仅在安全、受信任的环境中使用传递身份验证。

步骤 1：安装传递身份验证插件

更新日期： 2014-12-02

必须使用管理员帐户在用户设备上安装 Citrix 联机插件或 Citrix Desktop Viewer。 传递身份验证仅在 XenApp 和 XenDesktop 安装介质上包括的那些插件中可用。 出于安全原因，Citrix 联机插件 - Web 不包含此功能。 这意味着，您不能使用基于 Web 的客户端安装将包含此功能的 Citrix 插件部署到用户。

在安装后，必须使用组策略为所有 Citrix 客户端启用传递身份验证。 有关详细信息，请参阅 http://support.citrix.com/article/CTX122676 和存档的 Online Plug-in for Windows 文档。

步骤 2：为插件启用传递身份验证

为客户端启用传递身份验证包括两个步骤。 首先，将客户端模板添加到组策略对象编辑器。添加后，即可使用此模板来为所有客户端启用传递身份验证。

为传递身份验证向组策略对象编辑器添加客户端模板

1. 打开 MMC 组策略对象编辑器管理单元。
2. 选择要编辑的组策略对象。
3. 选择管理模板节点，然后在操作菜单中单击添加/删除模板。
4. 单击添加并浏览到客户端模板文件 icaclient.adm。 此文件安装在客户端的 \Configuration 文件夹中，通常为 C:\Program Files (x86)\Citrix\ClientName\Configuration。
5. 单击打开添加该模板，然后单击关闭。

为所有客户端启用传递身份验证

1. 打开 MMC 组策略对象编辑器管理单元。
2. 选择要编辑的组策略对象。
3. 在左窗格中，展开管理模板节点。
4. 依次选择 Classic Administrative Templates (ADM)（经典管理模板(ADM)）> Citrix Components（Citrix 组件）。 展开所安装的客户端的节点，然后选择 User authentication（用户身份验证）。
5. 在结果窗格中，选择 Local user name and password（本地用户名和密码）。
6. 在 Action（操作）菜单中，单击 Edit（编辑）。
7. 单击 Enabled（已启用）并确认已选中 Enable pass-through authentication（启用传递身份验证）复选框。
8. 确保在组策略对象编辑器中对用户和计算机均完成了上述所有步骤。
9. 注销然后再次登录以使得对策略的更改生效。

步骤 3：使用控制台启用传递

使用 Citrix Web Interface Management 控制台可以启用传递身份验证。 启用此功能时，用户无需重新输入其凭据，用户的资源集会自动显示。

此外，还可以为 XenApp Web 和 XenApp Services 站点启用带有传递身份验证的 Kerberos。对于 XenApp Services 站点，还可以为通过智能卡传递身份验证指定 Kerberos。

启用传递身份验证

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并选中传递复选框。
4. 单击属性并选择 Kerberos 身份验证。
5. 如果要启用 Kerberos 身份验证，请选中使用 Kerberos 身份验证连接到服务器复选框（适合 XenApp Web 站点），或选中仅使用 Kerberos 复选框（适合 XenApp 服务站点）。

启用智能卡身份验证

更新日期： 2014-12-02

要使用智能卡身份验证，必须在 IIS 上运行 Web Interface，并且用户必须运行支持的 Internet Explorer 或 Firefox 版本。 对于通过智能卡传递身份验证，用户必须运行支持的 Internet Explorer版本；通过智能卡传递身份验证不支持 Firefox。

如果计划为 XenApp Web 站点启用通过智能卡传递身份验证，用户必须使用 Internet Explorer 将该站点添加到 Windows“可信站点”或“本地 Intranet 区域”。

对于在 Windows Server 2008 上运行的 IIS 7.x，请确保为 Web 服务器 (IIS) 角色启用了 Web 服务器 > 安全性 > 客户端证书映射身份验证角色服务。 如果计划启用通过智能卡传递身份验证，还请确保启用了 Web 服务器 > 安全性 > Windows 身份验证角色服务。

适用于 Java 应用程序服务器的 Web Interface 不支持智能卡身份验证。

必须在 Web 服务器上启用安全套接字层 (SSL)，因为 SSL 用于保障 Web 浏览器和服务器之间的通信安全。 有关详细信息，请参阅您的 Web 服务器文档。

要启用智能卡身份验证（具有或不具有其他身份验证方法），必须配置登录屏幕以便只能使用 HTTPS 连接访问它。 如果使用简单 HTTP 或 HTTPS 配置不正确，用户会收到错误消息并且无法登录。 要避免此问题，请向所有用户提供完整的 HTTPS URL；例如 https://www.MyCompany.com:443/Citrix/XenApp。

有关智能卡身份验证的用户设备要求和服务器要求的详细信息，请参阅将智能卡与 XenApp 一起使用。

步骤 1：为实现智能卡身份验证安装插件

要使用智能卡身份验证，用户需要安装 Citrix 联机插件或 Citrix Desktop Viewer。 或者，用户也可以使用基于 Web 的客户端安装从适当配置的 XenApp Web 站点下载并安装 Citrix 联机插件 - web。 但是，要使用通过智能卡传递身份验证，必须使用管理员帐户在用户设备上安装 Citrix 联机插件或 Citrix Desktop Viewer。 传递身份验证仅在 XenApp 和 XenDesktop 安装介质上包括的那些插件中可用。 出于安全原因，Citrix 联机插件 - Web 不包含此功能。

如果计划启用通过智能卡传递身份验证，必须在安装插件后使用组策略先为所有 Citrix 客户端启用传递身份验证。 为客户端启用传递身份验证包括两个步骤。 首先，将客户端模板添加到组策略对象编辑器。 添加后，即可使用此模板来为所有客户端启用传递身份验证。

为传递身份验证向组策略对象编辑器添加客户端模板

1. 打开 MMC 组策略对象编辑器管理单元。
2. 选择要编辑的组策略对象。
3. 选择管理模板节点，然后在操作菜单中单击添加/删除模板。
4. 单击添加并浏览到客户端模板文件 icaclient.adm。 此文件安装在客户端的 \Configuration 文件夹中，通常为 C:\Program Files (x86)\Citrix\ClientName\Configuration。
5. 单击打开添加该模板，然后单击关闭。

为所有客户端启用通过智能卡传递身份验证

1. 打开 MMC 组策略对象编辑器管理单元。
2. 选择要编辑的组策略对象。
3. 在左窗格中，展开管理模板节点。
4. 依次选择 Classic Administrative Templates (ADM)（经典管理模板(ADM)）> Citrix Components（Citrix 组件）。 展开所安装的客户端的节点，然后选择 User authentication（用户身份验证）。
5. 在结果窗格中，选择 Smart card authentication（智能卡身份验证）。
6. 在 Action（操作）菜单中，单击 Edit（编辑）。
7. 单击 Enabled（已启用）并选中 Allow smart card authentication（允许智能卡身份验证）和 Use pass-through authentication for PIN（对 PIN 使用传递身份验证）复选框。

步骤 2：启用 Windows 目录服务映射器

要启用智能卡身份验证，必须确保 Web Interface 服务器上启用了 Windows 目录服务映射器。

Web Interface 身份验证使用 Windows 域帐户，即用户名和密码凭据。 但是，智能卡中包含证书。 目录服务映射器使用 Windows Active Directory 将证书映射到 Windows 域帐户。

在 Microsoft Internet Information Services 7.x 上启用 Windows 目录服务映射器

1. 在 Web Interface 服务器上，确保没有为 Web 服务器(IIS) 角色安装 Web 服务器 > 安全性 > IIS 客户端证书映射身份验证角色服务。
2. 打开 MMC Internet Information Services (IIS) 管理器管理单元。
3. 在左窗格中选择 Web 服务器，然后在 Features View（功能视图）中双击身份验证。
4. 在身份验证页上，启用 Active Directory 客户端证书身份验证方法。

在 Microsoft Internet Information Services 6.0 上启用 Windows 目录服务映射器

1. 在 Web Interface 服务器上，打开 MMC Internet Information Services (IIS) 管理器管理单元。
2. 选择位于 Web Interface 服务器下的 Web 站点节点，并在操作窗格中单击属性。
3. 从目录安全性选项卡中，选择安全通信区域中的启用 Windows 目录服务映射器。

步骤 3：在 Web Interface 上启用智能卡身份验证

必须将 Web Interface 配置为启用智能卡身份验证（以便用户可以访问 Web Interface 并获取其资源集）和服务器身份验证（以便用户可以在会话中使用 Web Interface 访问资源）。

为 XenApp Web 站点启用智能卡身份验证

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并根据需要选中智能卡或通过智能卡传递复选框。
4. 单击属性为智能卡身份验证配置更多设置。

为 XenApp Services 站点启用智能卡身份验证

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击身份验证方法并根据需要选中智能卡或通过智能卡传递复选框。
4. 单击属性并选择漫游。
5. 要配置拔出智能卡时的 Web Interface 行为，请选择启用漫游，并选择下列选项之一：
   - 要在拔出智能卡时断开用户的会话连接，请选择拔出智能卡时断开会话连接
   - 要在拔出智能卡时注销用户会话，请选择拔出智能卡时注销会话
6. 如果已启用通过智能卡传递身份验证并且要在插件与 XenApp Services 站点之间使用 Kerberos 身份验证，请单击 Kerberos 身份验证并选中使用 Kerberos 对 XenApp 服务站点进行身份验证复选框。

示例：为用户启用智能卡身份验证

您需要为用户启用通过智能卡传递身份验证。 用户的计算机正在运行 Windows XP。 应将智能卡读卡器连接到该计算机，并在服务器场上对智能卡支持进行配置。 当前，可将 Web Interface 配置为仅显式/提示身份验证（用户名和密码）。

启用通过智能卡传递身份验证

1. 使用相应的安装介质在用户计算机上安装 Citrix 联机插件或 Citrix Desktop Viewer。 安装该插件是使用管理员帐户来执行的。 对于 XenApp Web 站点，请使用 Internet Explorer 将该站点添加到用户计算机上的 Windows“可信站点”或“本地 Intranet 区域”。

2. 使用组策略为所有 Citrix 客户端启用传递身份验证。 有关详细信息，请参阅步骤 1：为实现智能卡身份验证安装插件。 此外，还必须确保在场中启用传递身份验证。 有关详细信息，请参阅您的 Citrix 服务器文档。

3. 确保 Windows 目录服务映射器已启用。 有关详细信息，请参阅步骤 2：启用 Windows 目录服务映射器。

4. 使用 Citrix Web Interface Management 控制台中的身份验证方法任务启用通过智能卡传递身份验证。 有关详细信息，请参阅步骤 3：在 Web Interface 上启用智能卡身份验证。 用户使用智能卡登录自己的物理 Windows 桌面。 用户在访问资源时，会自动登录。 如果启用智能卡身份验证时未进行传递，则用户在访问资源时必须重新输入 PIN。

配置双因素身份验证

您可以为 XenApp Web 站点配置以下双因素身份验证方法：

- Aladdin SafeWord for Citrix。 这种身份验证方法使用由 SafeWord 令牌生成的字母数字代码或者使用 PIN 数字来创建通行码。 用户在访问服务器上的应用程序之前，在登录屏幕上输入其域凭据和 SafeWord 通行码。

- RSA SecurID。 这种身份验证方法使用由 RSA SecurID 令牌（令牌代码）生成的数字和 PIN 数字来创建通行码。 用户在访问服务器上的资源之前，在登录屏幕上输入其用户名、域、密码和 RSA SecurID 通行码。 在 RSA ACE/Server 上创建用户时，用户登录名必须与其域用户名相同。

  注：当使用 RSA SecurID 身份验证时，系统会生成一个新 PIN 并将其显示给用户。 该 PIN 将显示 10 秒钟，或者直到用户单击确定或者取消为止，以确保该 PIN 不被其他人看到。 PDA 不支持此项功能。

- RADIUS 服务器。 这种身份验证方法使用远程身份验证拨入用户服务 (RADIUS) 身份验证协议（而不是专有代理软件）。 SafeWord 和 SecurID 都可以安装并配置为充当 RADIUS 服务器。 对于适用于 Java 应用程序服务器的 Web Interface，RADIUS 身份验证是唯一可用的双因素身份验证选项。

在 Microsoft Internet Information Services 上启用 SafeWord 身份验证

本节介绍如何启用 RSA SecurID 6.0 支持。

SafeWord 的要求

将 SafeWord 身份验证与 Microsoft Internet Information Services 的 Web Interface 结合使用：

- 从 Aladdin 知识系统获取最新版本的 SafeWord Agent。 如果要求支持 UPN 身份验证，请确保将最新的自动更新应用于 Web Interface 的 SafeWord Agent，以及应用于 SafeWord 服务器。
- 确保在安装 Web Interface 的 SafeWord Agent 之前，先安装了 Web Interface。
- 确保将 Web Interface 的 SafeWord Agent 安装到 Web Interface 服务器上。

有关配置 SafeWord 产品的详细信息，请访问 http://www.aladdin.com/safeword/default.aspx。

使用控制台启用 RSA SecurID 身份验证

您必须将 Web Interface 配置为启用 RSA SecurID 身份验证，以便用户访问和显示其资源集。 为此，请使用 Citrix Web Interface Management 控制台中的身份验证方法任务。

在 Microsoft Internet Information Services 上启用 RSA SecurID 身份验证

更新日期： 2014-11-24

本部分介绍如何启用 RSA SecurID 7.0 支持。

SecurID 要求

将 SecurID 身份验证与 Microsoft Internet Information Services 的 Web Interface 结合使用：

- 必须在 Web 服务器上安装 RSA ACE/Agent for Windows 7.0 或更高版本。
- 必须在安装 RSA ACE/Agent 之后安装 Web Interface。
- 必须在 Microsoft Internet Information Services 6.0 中托管 Web Interface。

将 Web Interface 服务器添加为代理主机

您必须在 RSA ACE/Server 数据库中为 Web 服务器创建代理主机，以便 RSA ACE/Server 识别和接受来自 Web 服务器的身份验证请求。 在创建代理主机时，请将 Web Interface 配置为 NetOS 代理。 RSA ACE/Server 使用此设置来确定如何与 Web Interface 进行通信。

复制 sdconf.rec 文件

在 RSA ACE/Server 上查找（或者如有必要，可以创建）sdconf.rec 文件并将其复制到 Web Interface 服务器上的 \System32 文件夹，通常位于 C:\Windows\System32。 此文件可为 Web Interface 提供连接到 RSA ACE/Server 所需的信息。

使用控制台启用 RSA SecurID 身份验证

您必须将 Web Interface 配置为启用 RSA SecurID 身份验证，以便用户访问和显示其资源集。 为此，请使用 Citrix Web Interface Management 控制台中的身份验证方法任务。

RSA SecurID 多域支持

如果您的用户帐户共享相同的用户名，但位于不同的 Windows 域中，则必须在 RSA ACE/Server 数据库中，使用域\用户名（与仅使用用户名相对应）的默认登录形式标识这些帐户，并且使用 Citrix Web Interface Management 控制台中的身份验证方法任务配置 Web Interface，以便将域和用户名发送到 RSA ACE/Server。

启用 RSA SecurID Windows 密码集成

Web Interface 支持 RSA SecurID 的 Windows 密码集成功能。 启用此功能后，Web Interface 用户就可以利用其 SecurID 通行码登录和访问资源。 用户第一次登录 Web Interface 或需要更改其密码时，只需提供 Windows 密码。

要将 SecurID Windows 密码集成与 Microsoft Internet Information Services 的 Web Interface 结合使用，必须注意以下事项：

- 必须在 Web 服务器上安装 RSA ACE/Agent Local Authentication Client for Windows（管理员必须使用本地服务器管理员凭据登录 Web Interface）
- 必须在安装 RSA ACE/Agent 之后安装 Web Interface
- RSA Authentication Agent Offline Local Service 必须在 Web 服务器上运行
- 必须将 RSA ACE/Server 数据库中 Web 服务器的代理主机配置为启用 Windows 密码集成功能
- 必须将数据库系统参数配置为在系统级别上启用 Windows 密码集成功能

在 Web 服务器上重置节点密钥注册表项

节点密钥用于确保 Web Interfac 和 RSA ACE/Serverr 之间的通信安全。

在下列情况下，节点密钥在这两种服务器之间可能会不同步：

- 重新安装 Web Interface 时
- 重新安装 RSA ACE/Server 时
- 删除 Web 服务器的代理主机记录，然后重新添加该记录时
- 在 Web 服务器上删除 NodeSecret 注册表项时
- 当未选中 RSA ACE/Server 的编辑代理主机对话框中的已创建节点密钥复选框时

如果 Web Interface 服务器和 RSA ACE/Server 上的节点密钥不匹配，SecurID 将会失败。您必须重置 Web Interface 服务器和 RSA ACE/Server 上的节点密钥。

警告：注册表编辑器使用不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。

1. 在系统注册表中，导航至：
   - 32 位服务器上的 HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT
   - 64 位服务器上的 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SDTI\ACECLIENT
2. 删除 NodeSecret 项。

注：重新安装 Web Interface 不会删除 NodeSecret 项。 如果代理主机条目在 RSA ACE/Server 上保持不变，则可以重新使用节点密钥。

启用 RADIUS 身份验证

更新日期： 2014-11-24

本节介绍如何安装和配置作为 RADIUS 服务器出现的 Aladdin SafeWord 与 RSA SecurID。 RADIUS 身份验证是唯一的双因素身份验证选项，适用于 Java 应用程序服务器的 Web Interface。

通过 SafeWord 启用 RADIUS

安装 SafeWord 服务器软件时，请选择安装 IAS RADIUS Agent。

按照屏幕上有关通过 Windows Internet Authentication Service (IAS) 管理单元将 RADIUS 客户端安装到 Microsoft 管理控制台的说明操作。 对于根据 SafeWord 服务器验证用户身份的每个 Web Interface 服务器，需要配置新的 RADIUS 客户端。

必须为所创建的每个 RADIUS 客户端提供以下信息：

- 与 RADIUS 客户端关联的 Web Interface 服务器的完全限定域名或 IP 地址。
- 对关联的 Web Interface 服务器可用的机密。
- 必须将客户端类型设置为 RADIUS standard（RADIUS 标准）。
- 为了增强安全性，必须选择 Request must contain the Message Authenticator attribute（请求必须包含消息身份验证程序属性）选项。

通过 RSA SecurID 启用 RADIUS

可以使用 SecurID Configuration Management Tool 在 RSA Authentication Manager 中启用 RADIUS。 有关此工具的详细信息，请参阅 RSA Authentication Manager 文档。

将 Web Interface 和 RADIUS 服务器添加为身份验证代理

假定验证用户身份的 RSA Authentication Manager 还充当 RADIUS 服务器，则必须在 RSA Authentication Manager 数据库中为本地 RADIUS 服务器创建身份验证代理记录。 在创建身份验证代理记录时，请将名称和 IP 地址设置为本地服务器的名称和 IP 地址，并将此服务器配置为 NetOS 身份验证代理。 必须将本地服务器分配为执行服务器。

此外，还必须在 RSA Authentication Manager 数据库中为每个 Web Interface 服务器创建身份验证代理记录，以便 RSA Authentication Manager 通过 RADIUS 服务器识别和接受来自 Web Interface 的身份验证请求。 创建身份验证代理记录时，请将 Web Interface 配置为通信服务器，并将加密密钥设置为与 Web Interface 共享的密钥值。

使用 RADIUS 质询模式

默认情况下，SecurID RADIUS 服务器处于 RADIUS 质询模式。 在此模式下：

- Web Interface 将显示一个通用质询屏幕，其中包含消息、HTML 密码框以及确定和取消按钮。
- Web Interface 未本地化质询消息。 消息采用 SecurID RADIUS 服务器上设置的质询消息的语言。

如果用户不提交响应（例如，如果他们单击取消），则他们将定向回登录屏幕。

Citrix 建议，仅当 Web Interface 之外的软件组件或产品也使用 RADIUS 服务器进行身份验证时，才使用此模式。

使用自定义质询消息

可以为 SecurID RADIUS 服务器配置自定义质询消息。 使用 Web Interface 可识别的自定义消息时，RADIUS 服务器可显示与适用于 Microsoft Internet 信息服务的 Web Interface 所显示相同的用户界面页面，并且这些页面已本地化。

此功能要求对 RADIUS 服务器配置进行更改，并且只有 RADIUS 服务器专用于对 Web Interface 用户进行身份验证时才能实现。

可以通过启动 RSA RADIUS 配置实用工具来更改质询消息。 有关使用此工具的详细信息，请参阅 SecurID 软件文档。 要对访问 IIS 和 Java 应用程序服务器上的站点的用户显示相同的消息，必须更新以下质询：

以下项的消息	数据包	更新的值
用户是否需要系统 PIN	质询	CHANGE_PIN_EITHER
用户是否准备获取系统 PIN	质询	SYSTEM_PIN_READY
用户对系统 PIN 是否满意	质询	CHANGE_PIN_SYSTEM_[%s]
固定长度的新数字 PIN	质询	CHANGE_PIN_USER
固定长度的新字母数字 PIN	质询	CHANGE_PIN_USER
可变长度的新数字 PIN	质询	CHANGE_PIN_USER
可变长度的新字母数字 PIN	质询	CHANGE_PIN_USER
新 PIN 已接受	质询	SUCCESS
输入“是”或“否”	质询	FAILURE
需要下一个令牌代码	质询	NEXT_TOKENCODE

为 RADIUS 创建共享机密

RADIUS 协议需要使用共享机密，共享机密是仅对 RADIUS 客户端（即 Web Interface）和用于验证该客户端身份的 RADIUS 服务器可用的数据。 Web Interface 将共享机密存储在本地文件系统的文本文件中。 此文件的位置由 web.config 文件（用于 IIS 中托管的站点）或 web.xml 文件（用于 Java 应用程序服务器中托管的站点）中的 RADIUS_SECRET_PATH 配置值给定。 提供的位置与 IIS 中托管的站点的 \conf 文件夹和 Java 应用程序服务器中托管的站点的 /WEB_INF 目录相对。

要创建共享机密，请创建一个名为 radius_secret.txt 的包含任何字符串的文本文件。 将此文件移到相关配置文件中指定的位置，并确保它是锁定的，只能由相应的用户或进程访问。

指定 RADIUS 的网络访问服务器标识符

RADIUS 协议要求对 RADIUS 服务器的访问请求包括 IP 地址或 RADIUS 客户端（即 Web Interface）的其他标识符。 要启用 RADIUS 身份验证，必须提供 Web 服务器的 IP 地址或为 RADIUS 网络访问服务器 (NAS) 标识符属性指定一个值。 NAS 标识符属性的值可为包含三个或三个以上字符的任意字符串。 尽管每个 RADIUS 客户端的这一属性不必是唯一的，但为每个客户端设置唯一的标识符有助于诊断 RADIUS 通信问题。

要提供 RADIUS 客户端的 IP 地址，请在 web.config 文件（用于在 IIS 中托管的站点）或 web.xml 文件（用于在 Java 应用程序服务器中托管的站点）中输入 Web 服务器的 IP 地址作为 RADIUS_IP_ADDRESS 配置参数的值。 要设置 RADIUS NAS 标识符，请在 web.config 或 web.xml 中指定 RADIUS_NAS_IDENTIFIER 的值。

使用控制台启用 RADIUS 双因素身份验证

您必须对 Web Interface 启用双因素身份验证，以便用户访问和显示其资源集。 为此，请使用 Citrix Web Interface Management 控制台中的身份验证方法任务。 除了启用双因素身份验证之外，还可以指定一个或多个 RADIUS 服务器地址和端口（可选）、服务器的负载平衡或故障转移行为以及响应超时。

重要：启用 RADIUS 身份验证时，还必须提供 RADIUS 客户端的 IP 地址，或为站点的 web.config 文件 (IIS) 或 web.xml 文件（Java 应用程序服务器）中的 RADIUS 网络访问服务器标识符属性指定一个值。

管理客户端

更新日期： 2014-11-24

本部分介绍了有关通过 Web Interface 部署和使用 Citrix 客户端的信息。 此外，还介绍了如何设置安全访问。

用于联机资源的客户端

下列 Citrix 客户端可用于访问联机资源：

- 本机客户端。 管理员会将相应的本机客户端安装在用户的设备上。 此外，没有本机客户端的用户也可以使用客户端检测和部署过程，下载并部署 Citrix 联机插件 - Web。 支持无缝窗口；资源显示在可以调整大小的桌面窗口中。 如果用户通过 PDA 设备访问资源，您必须启用本机客户端。

- Java 客户端。 用户在访问资源时运行 Java 客户端。 此客户端通常用于以下情况：用户没有安装本机客户端，并且无法下载和部署 Citrix 联机插件 - Web；或者用户的设备配置或 XenApp Web 站点禁止其下载和部署该插件。 Java 客户端支持无缝窗口；资源显示在可以调整大小的桌面窗口中。

- 嵌入的远程桌面连接 (RDP) 软件。 如果此选项可用，则用户可以使用已作为其 Windows 操作系统的一部分安装的远程桌面连接 (RDP) 软件。 客户端检测和部署过程不会向没有安装远程桌面连接 (RDP) 软件的用户提供该软件。 不支持无缝窗口；资源内嵌在浏览器窗口中显示。

  注: 在运行 Windows CE 或 Windows Mobile 的设备上，不支持 Java 客户端和嵌入的远程桌面连接 (RDP) 软件。 Java 客户端和嵌入的远程桌面连接 (RDP) 软件不支持与 AD FS 集成站点一起使用。

配置 Citrix 联机插件

通过 Citrix 联机插件，用户可以直接从物理 Windows 桌面访问应用程序、内容和虚拟桌面，而无需使用 Web 浏览器。 您可以远程将指向资源的链接位置配置在开始菜单、Windows 桌面或 Windows 通知区域中。 Citrix 联机插件的用户界面也可以“锁定”，以防止用户错误配置。您可以使用 Citrix Web Interface Management 控制台或者 config.xml 文件配置 Citrix 联机插件。

使用 Citrix Web Interface Management 控制台进行配置

可以为 Citrix 联机插件配置默认显示选项、身份验证方法和服务器连接选项。 Citrix Web Interface Management 控制台允许您更改默认设置以防止用户更改特定选项。

使用配置文件

您还可以使用 config.xml 和 WebInterface.conf 文件配置 Citrix 联机插件。这些文件通常位于 Web Interface 服务器上的 C:\inetpub\wwwroot\Citrix\PNAgent\conf 目录中。

管理插件配置文件

使用控制台配置的 Citrix 联机插件选项存储在 Web Interface 服务器的配置文件中。 该配置文件可控制作为选项显示在用户的 Citrix 联机插件选项对话框中的参数范围。 用户可从可用选项中选择以设置其 ICA 会话的首选项，包括登录模式、屏幕大小、音频质量和资源链接位置。

对于新站点，可使用默认设置安装一个标准的配置文件 config.xml；该配置文件可以在大多数网络环境中使用，而不需要修改。 config.xml 文件存储在站点的 \conf 文件夹中。

将客户端安装文件复制到 Web Interface

更新日期： 2014-11-24

要使用基于 Web 的客户端安装，客户端安装文件必须在 Web Interface 服务器上可用。

在 Web Interface 安装期间，安装程序会提示您访问 XenApp 或 XenDesktop 安装介质。 在 IIS 上，安装程序将安装介质中 \Citrix Receiver and Plug-ins 文件夹的内容复制到根目录下名为 \Clients 的文件夹；例如，C:\Program Files (x86)\Citrix\Web Interface\Version\Clients。 在 Java 应用程序服务器上，安装程序从安装介质复制 Citrix 客户端并将它们打包在 .war 文件中。

如果您在安装 Web Interface 期间未将客户端安装文件复制到 Web 服务器，请务必先将这些文件复制到 Web 服务器，然后再使用基于 Web 的客户端安装；例如，将 Citrix Receiver and Plug-ins/Windows 文件夹中的文件复制到 Web 服务器。 如果 XenApp 或 XenDesktop 安装介质不可用，则必须手动重新创建必需的目录结构，然后从 Citrix Web 站点下载所需的客户端。

默认情况下，Web Interface 假定客户端安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。 如果从 Citrix Web 站点下载客户端或计划部署早期版本的客户端，请检查 XenApp Web 站点的配置文件中是否指定了相应的客户端安装文件名。

将客户端文件复制到 Microsoft Internet Information Services 上的 Web Interface

1. 找到 Web Interface 安装中的 \Clients 文件夹；例如，C:\Program Files (x86)\Citrix\Web Interface\Version\Clients。

2. 将安装介质插入 Web 服务器的光驱，或浏览网络找到安装介质的共享映像。

3. 导航到安装介质上的 \Citrix Receiver and Plug-ins 文件夹。 将安装介质上的该文件夹的内容复制到 Web Interface 服务器上的 \Clients 文件夹。 确保仅复制该文件夹的内容，而不复制 \Citrix Receiver and Plug-ins 文件夹本身。

   如果 XenApp 或 XenDesktop 安装介质不可用，则必须手动重新创建下面的目录结构，然后从 Citrix Web 站点下载所需的客户端。

   C:\Program Files (x86)\Citrix\Web Interface\Version\Clients

   - \de
     - \Unix

       将具有德语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此文件夹中。
   - \en
     - \Unix

       将具有英语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此文件夹中。
   - \es
     - \Unix

       将具有西班牙语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此文件夹中。
   - \fr
     - \Unix

       将具有法语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此文件夹中。
   - \ja
     - \Unix

       将具有日语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此文件夹中。
   - \Java

     将 Java 客户端文件放在此文件夹中。

   - \Linux

     将 Citrix Receiver for Linux 安装文件（linuxx86-版本.tar.gz）放在此文件夹中。

- \Mac
  - \Web Online Plug-in

    将适用于 Macintosh 的 Citrix 联机 Web 插件安装文件 {Citrix online plug-in (web).dmg} 放在此文件夹中。
- \Windows
  - \Offline Plug-in

    将 Citrix 脱机插件安装文件 (CitrixOfflinePlugin.exe) 放在此文件夹中。
  - \Online Plug-in

    将 Citrix 联机插件 - Web 安装文件 (CitrixOnlinePluginWeb.exe) 放在此文件夹中。

默认情况下，Web Interface 假定客户端安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。 如果从 Citrix Web 站点下载客户端或计划部署早期版本的客户端，请检查 XenApp Web 站点的配置文件中是否为 ClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32 和 ClientStreamingWin32 参数指定了相应的客户端安装文件名。

将客户端安装文件复制到上面的目录结构后，为基于 Web 的客户端安装配置的任何 XenApp Web 站点会自动为需要客户端的用户提供客户端。

将客户端文件复制到 Java 应用程序服务器上的 Web Interface

1. 在站点展开的 .war 文件中，找到 /Clients 目录。

2. 将安装介质插入 Web 服务器的光驱，或浏览网络找到安装介质的共享映像。

3. 将目录更改为安装介质上的 /Citrix Receiver and Plug-ins 目录。 将安装介质上的该目录内容复制到 Web Interface 服务器上的 /Clients 目录。 确保仅复制该目录的内容，而不复制 /Citrix Receiver and Plug-ins 目录本身。

   如果 XenApp 或 XenDesktop 安装介质不可用，则必须手动重新创建下面的目录结构，然后从 Citrix Web 站点下载所需的客户端。

   XenAppWebSiteRoot/Clients

   - /de
     - /Unix

       将具有德语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此目录中。
   - /en
     - /Unix

       将具有英语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此目录中。
   - /es
     - /Unix

       将具有西班牙语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此目录中。
   - /fr
     - /Unix

       将具有法语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此目录中。
   - /ja
     - /Unix

       将具有日语语言支持的 UNIX 客户端安装文件（solaris.tar.Z、sol86.tar.Z）放在此目录中。
   - /Java

     将 Java 客户端文件放在此目录中。

   - /Linux

     将 Citrix Receiver for Linux 安装文件（linuxx86-版本.tar.gz）放在此目录中。

- /Mac
  - /Web Online Plug-in

    将适用于 Macintosh 的 Citrix 联机 Web 插件安装文件 {Citrix online plug-in (web).dmg} 放在此目录中。
- /Windows
  - /Offline Plug-in

    将 Citrix 脱机插件安装文件 (CitrixOfflinePlugin.exe) 放在此目录中。
  - /Online Plug-in

    将 Citrix 联机插件 - Web 安装文件 (CitrixOnlinePluginWeb.exe) 放在此目录中。

默认情况下，Web Interface 假定客户端安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。 如果从 Citrix Web 站点下载客户端或计划部署早期版本的客户端，请检查 XenApp Web 站点的配置文件中是否为 ClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32 和 ClientStreamingWin32 参数指定了相应的客户端安装文件名。

4. 将客户端安装文件复制到上面的目录结构后，请重新启动 Web 服务器。

   如果已为基于 Web 的客户端安装配置 XenApp Web 站点，则会为需要客户端的用户提供客户端。

配置客户端部署和安装标题

更新日期： 2014-11-24

Web Interface 提供了客户端检测和部署过程，用于检测可以将哪些 Citrix 客户端部署在用户环境中，然后引导这些客户端完成部署过程，包括需要时重新配置其 Web 浏览器。

可以允许用户最多通过三种方式访问客户端检测和部署过程：

- 可以将客户端检测和部署过程配置为在用户访问 XenApp Web 站点时自动运行。 客户端检测和部署过程将自动启动，从而帮助用户确定和部署相应的 Citrix 客户端以访问其资源。对于某些环境，客户端检测和部署过程还可以检测是否存在已安装的客户端，并且仅在必要时提示用户。

- 可以允许用户指定访问联机资源的首选客户端。 这会将运行客户端检测按钮添加到设置屏幕，从而使用户能够手动启动客户端检测和部署过程。

- 可以为用户提供安装标题，即在消息屏幕上向用户显示的链接。 用户单击链接即可启动客户端检测和部署过程。

当用户访问 XenApp Web 站点时，基于 Web 的客户端检测和部署过程会尝试确定用户计算机上是否安装了首选的 Citrix 客户端。 用户登录到配置了自动客户端检测和部署的 XenApp Web 站点前，检测和部署过程将自动启动，引导用户完成确定和部署适用的 Citrix 客户端以访问其资源的过程，其中包括重新配置其 Web 浏览器（如果适用）。

用户也可以使用消息屏幕上显示的链接来访问客户端检测和部署过程。 用户单击链接即可启动客户端检测和部署过程。 这些链接称为安装标题。

可以为没有合适客户端的用户提供安装标题，也可以将安装标题用于使用户能够访问客户端检测和部署过程，以将其 Citrix 客户端升级到更新版本或可提供更强功能的备用客户端类型。

可以使用 Citrix Web Interface Management 控制台中的客户端部署任务来指定用户在何种情况下可以访问客户端检测和部署过程。

配置客户端部署和安装标题

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。

3. 在 Action（操作）窗格中，单击 Client Deployment（客户端部署）。 对于只提供联机应用程序的站点，请选中 Native client（本机客户端）复选框，并单击 Properties（属性）。

4. 单击 Client Detection（客户端检测）。

5. 在用户（不具有合适的 Citrix 客户端）访问 XenApp Web 站点时，如果希望自动启动客户端检测和部署过程，请选中登录时执行客户端检测复选框。

6. 要在客户端检测和部署过程检测到可以从 XenApp Web 站点下载更新版本时，提示用户升级其客户端，请选中为客户端提供升级复选框。

7. 通过选择以下选项之一，指定何时向用户显示安装标题：

   - 要在无法检测到相应的客户端或提供了更合适的客户端时通知用户，请选择每当需要客户端时。 此为默认设置。

   - 要仅在无法检测到相应客户端时通知用户，请选择仅当资源无法访问时。

   - 如果希望在任何情况下都不显示安装标题，请选择从不。

配置 ICA 文件签名

更新日期： 2014-12-02

Web Interface 可以使用所选证书对生成的 ICA 文件进行数字签名，以使兼容的 Citrix 客户端和插件能够确认该文件源自贵组织。

要使用 ICA 文件签名功能，需要以下组件：

- Web Interface 5.4 或更高版本
- Merchandising Server 1.2 或更高版本（用于非受管客户端安全策略部署）
- 组策略对象（用于受管客户端安全策略部署）
- 用于 Windows Server 2003 或更高版本的管理模板文件格式

Citrix 建议（按优先级顺序）：

- 从公共证书颁发机构（例如 Verisign）购买代码签名证书或 SSL 签名证书。
- 如果企业已经有私有证书颁发机构，应使用私有证书颁发机构创建代码签名证书或 SSL 签名证书。
- 使用现有的 SSL 证书，例如 Web Interface 或 Dazzle 服务器证书。
- 创建新的根证书颁发机构并使用组策略对象将其分发给客户端。

证书必须满足以下要求：

- 证书必须包含专有密钥。
- 证书不能是过期的。
- 必须满足以下条件之一：
  - 证书不含密钥用法字段或增强型密钥用法字段。
  - 密钥用法字段允许对数字签名使用密钥。
  - 增强型密钥用法字段设置为“代码签名”或“服务器身份验证”。

Web Interface 使用 SHA-1 或 SHA-256 哈希算法对 ICA 文件进行签名。 SHA-256 哈希算法更新也更安全，但只有运行 Windows 2008 或更高版本的服务器以及运行 Windows Vista 或更高版本的客户端支持这种算法。 SHA-1 哈希算法可以用在所有支持的服务器和客户端操作系统上。

ICA 文件签名不能与 Java 客户端、RDP 客户端、Citrix Streaming 客户端配合使用，也不能用于从网络共享下载的已发布文档。

要启用 ICA 文件签名，必须将站点配置为使用本机客户端并显示联机应用程序，并且必须在 Webinterface.conf 文件中将 EnableLegacyIcaClientSupport 设置为 Off。

有关对 Citrix 联机插件启用 ICA 文件签名功能的详细信息，请参阅 Citrix Merchandising Server 文档。

在 Web Interface Management 控制台中启用 ICA 文件签名

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在 Action（操作）窗格中，单击 Client Deployment（客户端部署）。
4. 单击 ICA File Signing（ICA 文件签名）。
5. 选择 Enable ICA File Signing（启用 ICA 文件签名），并从下拉菜单中选择证书。 如果列表中没有所需的证书，请单击导入，以将证书导入个人证书存储中。
6. 如果正在运行 Windows 2008 或更高版本，可以选择所用的哈希算法类型。 否则将使用 SHA-1。 在 Windows 2003 上配置 ICA 文件签名功能后，需要重新启动计算机。

配置流会话监视

您可以使用 Citrix Web Interface Management 控制台中的客户端部署任务配置 Web Interface，从而为 Citrix 管理员提供有关用户会话的信息。 Web Interface 通过会话 URL 的方式提供这些信息，这使得可以与 Citrix 脱机插件进行通信。 大多数情况下，系统会自动检测该 URL。 但是，也可能需要手动进行设置，例如，如果客户端代理正在使用中。

您可以使用交付服务控制台查看会话信息。 您可以查看多个场中的所有用户会话、特定应用程序、连接到特定服务器的会话或特定用户的会话和应用程序的信息。

配置流会话监视

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在 Action（操作）窗格中，单击 Client Deployment（客户端部署）。
4. 单击 Citrix 脱机插件。
5. 选择 Web Interface 与 Citrix 脱机插件的通信方式。 选择以下选项：
   - 要自动检测用于与插件通信的会话 URL，请选择自动检测会话 URL
   - 要手动设置会话 URL，请选择指定会话 URL，然后输入 URL 详细信息

部署远程桌面连接软件

远程桌面连接 (RDP) 功能在运行 Internet Explorer 的 32 位 Windows 系统上可用。 已安装 6.0（Windows XP Service Pack 3 随附）或更高版本的 Microsoft 远程桌面连接 (RDP) 软件的用户可以使用它来访问其资源。 如果用户无法使用任何其他客户端，客户端检测和部署过程将检查远程桌面连接 (RDP) 软件是否可用，并帮助用户启用终端服务 ActiveX 控件（如有必要）。 使用远程桌面连接 (RDP) 软件的选项仅可用于只提供联机应用程序的站点。

注: 如果 Internet Explorer 未将 XenApp Web 站点放在“本地 Intranet”或“受信任的站点”区域，它将显示错误消息。 Web Interface 客户端检测和部署过程为用户提供了有关如何将站点添加到相关 Windows 安全区域的说明。

部署 Java 客户端

如果您要通过低带宽网络部署 Citrix 客户端，或者不确定用户运行的是哪个平台，请考虑使用 Java 客户端。 Java 客户端是一个跨平台兼容的小程序，可由 Web Interface 服务器部署到任何与 Java 兼容的 Web 浏览器。

由于 Java 客户端在用户环境、设备、操作系统和 Web 浏览器方面提供最广泛的支持，因此它可用作无法使用本机客户端的方案的回退选项。 您可以配置客户端检测和部署过程，以便为没有本机客户端或者无法从 XenApp Web 站点下载和部署客户端的用户提供 Java 客户端。

必须确保 Java 客户端在 XenApp Web 站点的 \Clients 目录中可用，才能将其部署到用户。

配置回退到 Java 客户端

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。

3. 在 Action（操作）窗格中，单击 Client Deployment（客户端部署）。 对于只提供联机应用程序的站点，请选中 Native client（本机客户端）复选框，并单击 Properties（属性）。

   注：要提供回退功能，无需使 Java 客户端可供用户使用。

4. 单击回退行为。

5. 通过选择以下选项之一，指定在何种情况下为没有本机客户端的用户提供 Java 客户端：

   - 如果希望没有本机客户端的用户下载和部署相应的 Citrix 客户端，请选择部署本机客户端。 此为默认设置。

   - 如果希望为没有本机客户端的用户提供 Java 客户端，并仅在其无法使用 Java 客户端时提示下载和部署本机客户端，请选择部署本机客户端并允许用户在此客户端与 Java 客户端之间进行选择。

   - 除了为没有本机客户端的用户提供 Java 客户端之外，如果还希望提示其下载和部署相应的客户端，请选择自动回退到 Java 客户端。

自定义 Java 客户端部署

更新日期： 2014-11-25

您可以配置 Java 客户端部署中包含的组件。

Java 客户端的大小由所包含的软件包确定。 选择的软件包越少，其大小就越小（最小可为 540 KB）。 如果要对使用低带宽连接的用户限制 Java 客户端的大小，可以只部署一组最少的组件。 或者，可以允许用户选择所需的组件。 有关 Java 客户端及其组件的详细信息，请参阅 Java 客户端文档。

注：在 Java 客户端中可用的某些组件可能需要在用户的设备或服务器上进一步配置。

下表介绍了可用的选项：

软件包	说明
音频	使服务器上运行的资源能够通过用户计算机上安装的声音设备来播放声音。 要控制服务器上映射的客户端音频使用的带宽量，请配置 Citrix 用户策略。
剪贴板	使用户能够在联机资源与其设备上本地运行的应用程序之间复制文本和图形。
本地文本回显	加快用户设备上的输入文本的显示。
SSL/TLS	使用安全套接字层（SSL）和 TLS（传输层安全性）保护通信。SSL/TLS 提供服务器身份验证、数据流加密以及消息完整性检查。
加密	提供强加密功能，可以增强 Citrix 客户端连接的隐私性。
客户端驱动器映射	使用户能够从会话中访问其本地驱动器。 当用户连接到服务器时，系统将自动装载其客户端驱动器（例如软盘、网络驱动器和光驱）。 用户可以访问其本地存储的文件，在其会话中使用这些文件，以及将它们重新保存到本地驱动器或服务器上的驱动器。 要启用此设置，用户还必须在 Java 客户端设置对话框中配置客户端驱动器映射。 有关详细信息，请参阅 Java 客户端文档。
打印机映射	使用户能够从会话中打印到其本地打印机或网络打印机。
配置 UI	启用 Java 客户端设置对话框。 用户可使用此对话框来配置 Java 客户端。

将私有根证书用于 Java 客户端版本 9.x

如果使用从私有证书颁发机构获得的服务器证书配置了 Secure Gateway 或 SSL Relay 服务（例如，如果使用 Microsoft Certificate Services 颁发自己的证书），则必须将根证书导入每个用户的设备上的 Java 密钥库。 有关详细信息，请参阅 Java 客户端文档。

管理安全访问

默认情况下，所有新的 Web Interface 站点都被配置为直接访问，其中 Citrix 服务器的实际地址会提供给所有 Citrix 客户端。 但是，如果您在部署中使用的是 Access Gateway、Secure Gateway 或防火墙，则可以使用 Citrix Web Interface Management 控制台中的安全访问任务将 Web Interface 配置为包含相应的设置。 此外，还可以为不同的用户组配置不同的访问方法。 例如，可以将通过公司 LAN 登录的内部用户配置为直接访问，而将通过 Internet 登录的外部用户配置为通过 Access Gateway 访问 Web Interface。

本节介绍了如何使用安全访问任务指定访问设置、编辑地址转换以及配置网关设置。

配置直接访问路由

如果要向一组特定 Citrix 客户端提供 Citrix 服务器的实际地址，可以使用 Citrix Web Interface Management 控制台中的安全访问任务指定用户设备地址和掩码。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击安全访问。
4. 在指定访问方法页面上，单击添加以添加新的访问路由，或者从列表中选择一个条目并单击编辑以编辑现有路由。
5. 从访问方法列表中，选择直接。
6. 输入用于标识客户端网络的网络地址和子网掩码。
7. 使用上移和下移按钮按照用户设备地址表中的优先级顺序排列访问路由。

配置备用地址设置

如果要向一组特定 Citrix 客户端提供 Citrix 服务器的备用地址，可以使用 Citrix Web Interface Management 控制台中的安全访问任务指定用户设备地址和掩码。 该服务器必须配置有备用地址，并对防火墙配置网络地址转换。

注: 如果使用了备用地址，则无法访问 XenDesktop 虚拟桌面。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击安全访问。
4. 在指定访问方法页面上，单击添加以添加新的访问路由，或者从列表中选择一个条目并单击编辑以编辑现有路由。
5. 从访问方法列表中，选择替代。
6. 输入用于标识客户端网络的网络地址和子网掩码。
7. 使用上移和下移按钮按照用户设备地址表中的优先级顺序排列访问路由。

配置内部防火墙地址转换

如果要在部署中使用防火墙，则可以使用 Web Interface 定义从内部地址到外部地址和端口的映射。 例如，如果 Citrix 服务器未配置有备用地址，则可以配置 Web Interface 以向 Citrix 客户端提供备用地址。 为此，请使用 Citrix Web Interface Management 控制台中的安全访问任务。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击安全访问。
4. 在指定访问方法页面上，单击添加以添加新的访问路由，或者从列表中选择一个条目并单击编辑以编辑现有路由。
5. 从访问方法列表中，选择已转换。
6. 输入用于标识客户端网络的网络地址和子网掩码。 使用上移和下移按钮按照用户设备地址表中的优先级顺序排列访问路由，然后单击下一步。
7. 在指定地址转换页面上，单击添加以添加新的地址转换，或者从列表中选择一个条目并单击编辑以编辑现有地址转换。
8. 在访问类型区域中，选择以下选项之一：
   - 如果希望 Citrix 客户端使用转换的地址连接到 Citrix 服务器，请选择用户设备路由转换
   - 如果已在用户设备地址表中配置了网关转换路由，且希望客户端和网关服务器都使用转换的地址连接到 Citrix 服务器，请选择用户设备和网关路由转换
9. 输入 Citrix 服务器的内部和外部（已转换）端口和地址。 连接到服务器的客户端使用外部端口号和地址。 确保创建的映射与 Citrix 服务器所使用的寻址类型匹配。

配置网关设置

更新日期： 2014-11-25

如果要在部署中使用 Access Gateway 或 Secure Gateway，则必须配置 Web Interface 以便支持网关。 为此，请使用 Citrix Web Interface Management 控制台中的安全访问任务。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击安全访问。
4. 在指定访问方法页面上，单击添加以添加新的访问路由，或者从列表中选择一个条目并单击编辑以编辑现有路由。
5. 从访问方法列表中，选择以下选项之一：
   - 如果要向网关提供 Citrix 服务器的实际地址，请选择网关(直接)。
   - 如果要向网关提供 XenApp 服务器的备用地址，请选择网关(替代)。 XenApp 服务器必须配置有备用地址，并对防火墙配置网络地址转换。

     注：如果使用了备用地址，则无法访问 XenDesktop 虚拟桌面。
   - 如果您希望由 Web Interface 中设置的地址转换映射来确定向网关提供的地址，请选择网关(已转换)。
6. 输入用于标识客户端网络的网络地址和子网掩码。 使用上移和下移按钮按照用户设备地址表中的优先级顺序排列访问路由，然后单击下一步。
7. 如果没有使用网关地址转换，请继续执行步骤 10。 如果正在使用网关地址转换，请在指定地址转换页上单击添加以添加新的地址转换，或者从列表中选择一个条目，然后单击编辑以编辑现有地址转换。
8. 在访问类型区域中，选择以下选项之一：
   - 如果希望网关使用转换的地址连接到 Citrix 服务器，请选择网关路由转换。
   - 如果已在用户设备地址表中配置了客户端转换路由，且希望 Citrix 客户端和网关都使用转换的地址连接到 Citrix 服务器，请选择用户设备和网关路由转换。
9. 输入 Citrix 服务器的内部和外部（已转换）端口和地址，然后单击确定。 当网关连接到 Citrix 服务器时，它将使用外部端口号和地址。 确保创建的映射与服务器场所使用的寻址类型匹配。 单击 Next（下一步）。
10. 在指定网关设置页面上，指定客户端必须使用的网关的完全限定域名 (FQDN) 和端口号。此 FQDN 必须与网关中安装的证书上的 FQDN 匹配。
11. 在客户端尝试自动重新连接时，如果希望 Citrix 服务器使断开的会话保持打开状态，请选中启用会话可靠性复选框。

12. 如果已启用了会话可靠性，并希望使用来自两个 Secure Ticket Authority (STA) 的同步票据记录，请选中从两个 STA (如果可用)请求票据复选框。 启用此选项时，Web Interface 会从两个不同的 STA 获取票据，以便在整个会话期间，当某个 STA 变得不可用时不会由此而中断用户会话。 如果由于任何原因 Web Interface 无法与两个 STA 联系，则它将回退到使用单个 STA。 单击 Next（下一步）。

    注: 要使用此功能必须部署 Access Gateway。 Secure Gateway 当前不支持多个冗余 STA。

13. 在指定 Secure Ticket Authority 设置页面上，单击添加以指定 Web Interface 可以使用的 STA 的 URL，或从列表中选择一个条目，然后单击编辑以编辑现有 STA 详细信息。 STA 随 Citrix XML Service 一起提供，例如在 http[s]://servername.domain.com/scripts/ctxsta.dll 中。 可以为容错指定多个 STA，但 Citrix 建议不要使用外部负载平衡器来实现此目的。 可以使用上移和下移按钮将 STA 按优先级顺序排列。

14. 选择是否使用用于实现负载平衡选项在 STA 之间启用负载平衡。 通过启用负载平衡，可以在服务器之间均匀分配连接，以便不会出现任何服务器过载。

15. 在在以下时间内绕过有故障的服务器框中，指定应绕过无法联系的 STA 的时间长度。 Web Interface 可以在 Secure Ticket Authority URL 列表上的服务器之间提供容错功能，以便当出现通信错误时，在指定的时间段内绕过有故障的服务器。

配置默认访问设置

用户设备地址表中的条目显示顺序即为规则应用顺序。 如果用户设备地址与任何显式定义的访问规则不匹配，则会应用默认规则。 创建站点时，将自动配置默认路由以便直接访问。 使用 Citrix Web Interface Management 控制台中的安全访问任务，可以指定适用于您的部署的默认访问方法。

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击安全访问。
4. 在指定访问方法页面上，从列表中选择标记为默认的条目，并单击编辑。
5. 从访问方法列表中，选择以下选项之一：
   - 如果要向 Citrix 客户端提供 Citrix 服务器的实际地址，请选择直接。
   - 如果要向客户端提供 Citrix 服务器的备用地址，请选择替代。 XenApp 服务器必须配置有备用地址，并对防火墙配置网络地址转换。

     注：如果使用了备用地址，则无法访问 XenDesktop 虚拟桌面。
   - 如果您希望由 Web Interface 中的地址转换映射来确定向客户端提供的地址，请选择已转换。
   - 如果要向网关提供 Citrix 服务器的实际地址，请选择网关(直接)。
   - 如果要向网关提供 XenApp 服务器的备用地址，请选择网关(替代)。 XenApp 服务器必须配置有备用地址，并对防火墙配置网络地址转换。

     注：如果使用了备用地址，则无法访问 XenDesktop 虚拟桌面。
   - 如果您希望由 Web Interface 中设置的地址转换映射来确定向网关提供的地址，请选择网关(已转换)。
6. 输入用于标识客户端网络的网络地址和子网掩码。 使用上移和下移按钮按照用户设备地址表中的优先级顺序排列访问路由。
7. 如果要在部署中使用地址转换或网关，请单击下一步并为默认配置指定其他相应设置。 有关详细信息，请参阅配置内部防火墙地址转换和配置网关设置。

编辑客户端代理设置

如果在 Web Interface 安装的客户端使用代理服务器，可以配置 Citrix 客户端是否必须通过代理服务器与运行 XenApp 或 XenDesktop 的服务器进行通信。 使用 Citrix Web Interface Management 控制台中的客户端代理任务可执行此操作。

位于 Web Interface 安装的客户端的代理服务器提供的安全好处包括：

- 信息隐藏，防火墙内部的系统名称不会通过 DNS（域名系统）在防火墙外部公开
- 通过一个连接为不同的 TCP 连接提供通道

使用 Citrix Web Interface Management 控制台，可以为 Citrix 客户端设置默认代理规则。但是，也可以对单个用户的设备配置此行为的例外。 要配置例外，可将代理服务器的外部 IP 地址与 Web Interface 代理设置进行关联。

此外，还可以指定代理行为由客户端控制。 例如，要在 XenApp 和 XenDesktop 中使用安全代理功能，请将 Web Interface 配置为使用客户端上指定的代理设置并为客户端配置安全代理。 有关使用 Citrix 客户端控制代理行为的详细信息，请参阅相关客户端的文档。

配置默认代理设置

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。
3. 在操作窗格中，单击客户端代理。
4. 单击添加创建新映射，或从列表中选择条目并单击编辑以编辑现有映射。
5. 在 IP 地址和子网掩码框中，分别输入代理的外部地址和用户设备子网掩码。
6. 从代理列表中，选择下列选项之一：
   - 如果希望 Citrix 客户端根据用户的浏览器配置自动检测 Web 代理，请选择用户的浏览器设置。
   - 如果希望客户端使用 Web 代理自动发现 (WPAD) 协议自动检测 Web 代理，请选择 Web 代理自动检测。
   - 如果要使用用户为客户端配置的设置，请选择客户端已定义。
   - 如果要使用 SOCKS 代理服务器，请选择 SOCKS。 如果选择此选项，则必须输入代理服务器的地址和端口号。 代理地址可以为 IP 地址或 DNS 名称。
   - 如果要使用安全代理服务器，请选择安全(HTTPS)。 如果选择此选项，则必须输入代理服务器的地址和端口号。 代理地址可以为 IP 地址或 DNS 名称。
   - 如果不希望使用代理，请选择无。
7. 如果输入了多个映射，请使用上移和下移按钮按优先级顺序将映射放在表中。

为用户自定义外观

可以自定义用户界面的外观，例如，在您希望站点具有特定的企业“外观和风格”时。

使用 Citrix Web Interface Management 控制台中的 Web 站点外观任务，可以自定义：

- 布局。 指定可供用户使用的控件并定义 Web 站点的显示方式。 可以执行以下操作：
  - 为 XenApp Web 站点选择自动、完整图形或低分辨率图形屏幕布局。 低分辨率图形用户界面是一种精简版，专门为在小型设备上或通过速度较慢的网络连接访问其资源的用户而设计。 通过自动选项，系统可以根据用户的计算机屏幕的大小为每个用户选择最合适的站点布局。
  - 配置用户的应用程序屏幕上的可用功能和控件（包括搜索和提示），并指定是否允许用户自定义其屏幕。
  - 在完整图形和低分辨率图形屏幕布局中，为用户的资源集设置默认视图样式。 此外，还可以指定可供用户选择的视图样式。
  - 指定应如何在用户的应用程序屏幕上对资源进行分组。 可以为应用程序、内容和桌面配置单独的选项卡，也可以在一个选项卡上将所有资源收集在一起。
- 外观。 通过在整个站点中显示不同的图像和颜色，使用户界面呈现自定义的外观和风格。 可以执行以下操作：
  - 指定用户的登录屏幕的样式。 既可以选择简约布局（只显示适当的登录字段），也可以选择包含导航栏（用户可以访问消息和登录前的首选项屏幕）的布局。
  - 对完整图形布局或低分辨率图形布局使用自定义站点标志图像，（可选）并为这些图像添加超链接。 此外，还可以更改站点标题区域的背景图像，或只使用一种特定颜色即可。
- 内容。 定义自定义消息和屏幕文本，并为用户在访问站点时可能使用的语言指定此文本的本地化版本。 您可以为用户的登录和应用程序屏幕指定页标题和消息，以及指定要在所有屏幕上显示的通用页脚文本。 另外，还可以配置用户必须接受才能登录的登录前免责声明。

管理资源快捷方式和刷新选项

更新日期： 2014-11-24

您可以使用 Citrix Web Interface Management 控制台中的快捷方式任务，指定 Citrix 联机插件如何显示资源快捷方式。

您可以创建以下类型的快捷方式：

- “开始”菜单。 您可以使用快捷方式任务中指定的设置，也可以使用在 XenApp 和 XenDesktop 上发布资源时定义的设置，或同时使用这两种设置。 您也可以定义是否在“开始”菜单中显示快捷方式以及如何在开始菜单中显示快捷方式，并且允许用户指定此设置。 另外，您还可以在所有程序菜单中创建快捷方式、创建其他子菜单和/或允许用户指定子菜单名称。

- Desktop。 您可以使用快捷方式任务中指定的设置，也可以使用在 XenApp 和 XenDesktop 上发布资源时定义的设置，或同时使用这两种设置。 您也可以定义如何在桌面上显示快捷方式以及是否在桌面上显示快捷方式，并且允许用户指定此设置。 另外，您还可以使用自定义文件夹名称和/或允许用户选择一个名称。

- 通知区域。 您可以在通知区域中显示资源和/或允许用户指定如何显示资源。

使用快捷方式任务，您还可以删除快捷方式。 您可以指定何时删除快捷方式（可以是在 Citrix 联机插件关闭时，也可以是用户从 XenApp 注销时）；对于运行 Windows CE 或 Linux 的用户，除了指定 Citrix 联机插件快捷方式外，还可以指定是否删除用户创建的快捷方式。 如果您选择同时删除 Citrix 联机插件快捷方式和用户创建的快捷方式，则还可以通过限制文件夹的搜索深度来提高性能。

指定资源刷新选项

使用 Citrix Web Interface Management 控制台中的资源刷新任务，可以指定刷新用户的资源列表的时间以及他们是否可以自定义这些设置。 可以在 Citrix 联机插件启动时或访问资源时启用刷新，并可以指定刷新列表的频率。

管理会话首选项

使用 Citrix Web Interface Management 控制台中的会话设置任务，可以指定用户能够调整的设置。 此外，还可以使用此任务指定非活动用户在多长时间后从 Web Interface 中注销，以及指定 Web Interface 是否应该覆盖联机资源客户端的用户设备名称。

对于 XenApp Web 站点，您可以为用户会话配置以下设置：

- 用户自定义设置。 启用或禁用 kiosk 模式，并指定是否在用户的应用程序屏幕中为用户显示设置按钮。
- Web 会话。 指定在注销用户之前，用户会话可以处于非活动状态的时间长度。
- 持久 URL。 指定用户是否可以使用浏览器书签访问站点。
- 连接性能。 指定预设默认设置或允许用户自定义其带宽控制、颜色深度、音频质量和打印机映射设置。
- 显示。 指定用户是否可以在联机会话中控制其窗口大小，并允许 Web Interface 使用 ClearType 字体平滑，前提是为用户的 Windows 操作系统、用户的 Citrix 客户端软件和服务器场配置了对应设置。
- 本地资源。 配置 Windows 组合键、PDA 同步和特殊文件夹重定向的设置。
- 用户设备名称。 指定 Web Interface 是否应覆盖联机资源的用户设备名称。

  重要：如果要对 8.x 和 9.x 版的 Clients for Windows 使用工作区控制，则必须启用覆盖用户设备名称设置。

对于提供联机资源的 XenApp Services 站点，可以使用 Citrix Web Interface Management 控制台中的会话选项任务配置以下用户会话设置：

- 显示。 选择可用于 ICA 会话的窗口大小，并以像素或屏幕百分比为单位定义自定义大小。 此外，还可以允许 Web Interface 使用 ClearType 字体平滑，条件是为用户的 Windows 操作系统、Citrix 联机插件和服务器场配置相应设置。
- 颜色和声音。 用户可选择在此部分中启用的选项。
- 本地资源。 启用用户可选择的 Windows 组合键目标。 Windows 组合键不会影响无缝连接。 可启用以下目标：
  - 本地桌面。 组合键仅适用于本地物理桌面；它们不会传递到 ICA 会话。
  - 远程桌面。 组合键适用于 ICA 会话中的虚拟桌面。
  - 仅限全屏桌面。 仅当 ICA 会话中的虚拟桌面处于全屏模式时，组合键才适用于该虚拟桌面。

  启用“特殊文件夹重定向”，以便用户在联机资源中打开、关闭或保存到 \Documents 或 \Desktop 文件夹时，其操作会重定向到其本地计算机上的文件夹。 有关详细信息，请参阅特殊文件夹重定向。

- 工作区控制。 配置重新连接和注销行为。 有关详细信息，请参阅配置工作区控制。

带宽控制

通过带宽控制，用户可以根据其连接带宽来选择会话设置。 这些选项将在用户登录前或登录后显示在设置屏幕上。 通过带宽控制，可以调整颜色深度、音频质量和打印机映射。 此外，还可以使用 Web Interface Management 控制台为用户指定默认或自定义设置。 使用管理会话设置任务，可以通过连接性能选项自定义带宽设置。 从连接速度下拉列表中选择自定义后，可以激活颜色质量、声音和启用打印机映射选项。

如果使用了 Java 客户端，带宽控制将确定音频和打印机映射软件包是否可用。 如果使用了远程桌面连接 (RDP) 软件，则音频质量将映射为打开或关闭，并且不会提供进一步的质量控制。 建议对无线 WAN 连接使用低带宽设置。

注：如果与带宽控制配合使用远程桌面连接 (RDP) 软件，Web Interface 会指定适用于选定带宽的参数。 但是，实际行为取决于使用的远程桌面连接 (RDP) 软件的版本、终端服务器和服务器配置。

默认情况下，用户可以调整会话的窗口大小。

如果阻止用户调整某设置，则该设置不会显示在用户界面中，将使用为服务器上的资源指定的设置。

ClearType 字体平滑

ClearType 是 Microsoft 开发的一种亚像素消除锯齿技术，可以改进文本在 LCD 屏幕上的呈现，同时减少可见赝像并使文本看起来比较平滑。 ClearType 字体平滑是 Windows XP 中引入的一项功能。 Windows 7 和 Windows Vista 中默认启用字体平滑，但 Windows XP 中没有启用该功能。

ICA 会话期间，Web Interface 和 Citrix 联机插件支持 ClearType 字体平滑。 当运行 Windows XP 或更高版本的用户连接到服务器时，插件会自动检测用户计算机上的字体平滑设置并将其发送到服务器。 该设置随后将用于整个会话期间。

必须在用户的操作系统、Citrix 联机插件、Web Interface 站点和服务器场上启用字体平滑。使用 Citrix Web Interface Management 控制台中的会话设置任务，可以为 XenApp Web 站点启用字体平滑；使用会话选项任务，可以为 XenApp Services 站点启用字体平滑。

字体平滑仅适用于联机资源。 此功能不可用于脱机应用程序。

特殊文件夹重定向

更新日期： 2014-11-24

利用“特殊文件夹重定向”功能，用户能够将服务器的 Windows 特殊文件夹映射到其本地计算机上的文件夹，以便他们可以更轻松地使用联机资源。 特殊文件夹这一术语具体是指标准 Windows 文件夹（例如 \Documents 和 \Desktop），无论使用何操作系统，这些文件夹始终以相同方式显示。

注: 在 Windows Vista 之前的版本中，特殊文件夹的名称前加有“My”这个单词，例如“Documents”文件夹在 Windows XP 中称为“My Documents”文件夹。

用户在未启用“特殊文件夹重定向”的会话中打开、关闭或保存文件时，显示在用户的联机资源内的导航对话框中的文档和桌面图标代表用户在服务器上的 \Documents 和 \Desktop 文件夹。 “特殊文件夹重定向”对打开或保存文件等操作进行重定向，以便用户打开或保存 \Documents 和 \Desktop 件夹中的文件时，可以访问到自己本地计算机上的这些文件夹。 当前，只有 \Documents 和 \Desktop 文件夹支持重定向。

“特殊文件夹重定向”仅适用于联机资源。 此功能不可用于脱机应用程序。

启用特殊文件夹重定向

默认情况下，XenApp Web 和 XenApp Services 站点均会禁用特殊文件夹重定向支持。 如果为站点启用特殊文件夹重定向，则必须确保服务器场中现有的任何策略规则都不会阻止用户访问或保存到其本地驱动器。

使用 Citrix Web Interface Management 控制台中的会话设置任务，可以为 XenApp Web 站点启用特殊文件夹重定向；使用会话选项任务，可以为 XenApp Services 站点启用特殊文件夹重定向。 此外，还可以允许用户选择是否在设置屏幕上启用此功能。

启用特殊文件夹重定向后，用户应始终在 Citrix 连接中心的客户端文件安全对话框中选择完全访问权限，授予资源对本地文件和文件夹的完全读写权限。 在其他设备上启动新会话之前，用户必须从所有活动会话中注销。 Citrix 建议您不要为从多个设备同时连接到同一会话的用户启用特殊文件夹重定向。

配置工作区控制

使用工作区控制可以允许用户快速断开与所有资源（应用程序、内容和桌面）的连接、重新连接到断开连接的资源以及从所有资源中注销。 这将使用户可以在设备之间移动，以及在登录状态下或随时手动访问其所有资源（仅限已断开连接的资源，或者已断开连接的资源和活动资源）。 例如，医院的临床医生可能需要在不同的工作站之间移动，并在每次登录时访问同一组资源。

工作区控制要求

以下功能、要求和建议适用于工作区控制功能：

- 要将工作区控制与 8.x 和 9.x 版的 Clients for Windows 一起使用，必须在 Citrix Web Interface Management 控制台的会话首选项任务中启用覆盖用户设备名称设置。
- 如果 Web Interface 检测到正在从一个 Citrix 会话访问它，将禁用工作区控制功能。
- 根据安全设置情况，Internet Explorer 可以阻止下载可能不是用户直接启动的文件，因此尝试使用本机客户端重新连接到资源的操作可能被阻止。 在不能重新连接的情况下，将显示一条警告消息，并且为用户提供重新配置其 Internet Explorer 安全设置的选项。
- 每个 Web 会话将在非活动周期（通常为 20 分钟）后超时。 当 HTTP 会话超时后，注销屏幕将会出现；但是，在该会话中访问或重新连接的任何资源都不会断开连接。 用户必须使用注销或断开连接按钮手动断开连接、注销或重新登录到 Web Interface。
- 只要 Citrix XML Service 设置为信任 Web Interface 凭据，则当匿名用户和已通过身份验证的用户断开连接时，已发布用于匿名使用的资源就会被终止。 因此，在用户断开连接后，他们不能重新连接到匿名资源。
- 要使用传递身份验证、智能卡身份验证或通过智能卡传递身份验证，必须在 Web Interface 服务器与 Citrix XML 服务之间建立信任关系。 有关详细信息，请参阅对 XenApp Web 站点使用工作区控制和集成身份验证方法。
- 如果未对 XenApp Services 站点启用凭据传递，将提示智能卡用户对正在重新连接的每个 Citrix 会话输入其 PIN。 这不是 XenApp Services 站点上传递身份验证或通过智能卡传递身份验证存在的问题，因为已使用这些选项启用凭据传递。

工作区控制限制

如果打算启用工作区控制，需要了解以下限制：

- 工作区控制不适用于配置为提供脱机应用程序的站点。 如果将站点配置为双模式交付，则工作区控制仅使用联机资源。
- 不能将工作区控制与版本 8 之前的 32 位 Windows 客户端或远程桌面连接 (RDP) 软件一起使用。 此外，此功能仅适用于运行 Presentation Server 4.5 或更高版本的服务器。
- 工作区控制只允许重新连接到已断开连接的 XenDesktop 虚拟桌面。 用户不能重新连接到已挂起的虚拟桌面。

对 XenApp Web 站点使用工作区控制和集成身份验证方法

以下部分仅适用于 XenApp Web 站点。 如果用户使用传递身份验证、智能卡身份验证或通过智能卡传递身份验证登录，则必须在 Web Interface 服务器和运行 Citrix XML Service 并且 Web Interface 将与之联系的任何服务器之间建立信任关系。 Citrix XML Service 在 Web Interface 与运行 XenApp 和 XenDesktop 的服务器之间传递有关资源的信息。 如果没有建立信任关系，则断开连接、重新连接和注销按钮对于使用智能卡身份验证或传递身份验证登录的用户来说将失效。

如果您的用户由服务器场进行身份验证（即，如果用户不使用智能卡身份验证或传递身份验证方法登录），则不需要建立信任关系。

设置信任关系

如果将服务器配置为信任发送到 Citrix XML Service 的请求，请考虑以下因素：

- 建立信任关系时，依赖 Web Interface 服务器对用户进行身份验证。 为了避免安全风险，请使用 IPSec、防火墙或任何可确保只有受信任的服务与 Citrix XML Service 进行通信的技术。 如果您建立信任关系但不使用 IPSec、防火墙或其他安全技术，则任何网络设备都可能断开或终止会话。 如果仅使用显式身份验证配置站点，则不需要信任关系。
- 仅在 Web Interface 直接联系的服务器上启用信任关系。 Citrix Web Interface Management 控制台中的服务器场任务中列出了这些服务器。
- 将用于保障环境安全的技术配置为仅限 Web Interface 服务器可访问 Citrix XML Service。 例如，如果 Citrix XML Service 与 Microsoft Internet Information Services (IIS) 共享端口，您可以使用 IIS 中的 IP 地址限制功能来限制对 Citrix XML Service 的访问。

1. 登录到场中的服务器，依次单击开始 > 所有程序 > Citrix > 管理控制台 > Citrix 交付服务控制台。
2. 在控制台的左窗格中，导航到 Citrix 资源 > XenApp，展开场的节点，然后单击策略。
3. 在控制台的详细信息窗格中，选择计算机选项卡并单击新建。
4. 输入新策略的名称和描述（可选），并单击下一步。
5. 在类别列表中，单击 XML Service，并在设置下选择信任 XML 请求，然后单击添加。
6. 选择已启用，然后单击确定。 单击 Next（下一步）。
7. 如果需要，请对策略应用过滤器以确定应用该策略的环境，然后单击下一步。
8. 确保选中启用此策略复选框，然后单击保存。

用户登录时启用自动重新连接

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。

3. 在操作窗格中，选择适合站点类型的任务：

   · 对于 XenApp Web 站点，请单击工作区控制

   · 对于 XenApp Services 站点，请单击会话选项并选择工作区控制
4. 选择用户登录时自动重新连接到会话选项。

5. 选择下列选项之一：

   · 要自动重新连接已断开的会话和活动会话，请选择重新连接到所有会话。

   · 要仅自动重新连接已断开的会话，请选择仅重新连接到已断开的会话。
6. 选中允许用户自定义复选框，以便用户自行配置此设置。 用户可以在 XenApp Web 站点的设置屏幕上或 Citrix 联机插件的选项对话框中更改此设置。

启用“重新连接”按钮

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。

2. 在 Citrix Web Interface Management 控制台的左窗格中，根据需要单击 XenApp Web 站点或 XenApp Services 站点，并在结果窗格中选择您的站点。

3. 在操作窗格中，选择适合站点类型的任务：

   - 对于 XenApp Web 站点，请单击工作区控制

   - 对于 XenApp Services 站点，请单击会话选项并选择工作区控制
4. 选择启用“重新连接”按钮选项。

5. 选择下列选项之一：

   - 要将重新连接按钮配置为使用户重新连接到已断开的会话和活动会话，请选择重新连接到所有会话

   - 要将重新连接按钮配置为使用户仅重新连接到已断开的会话
6. 选中允许用户自定义复选框，以便用户自行配置此设置。 用户可以在 XenApp Web 站点的设置屏幕上或者 XenApp Services 站点 Citrix 联机插件的选项对话框中更改此设置。

配置注销行为

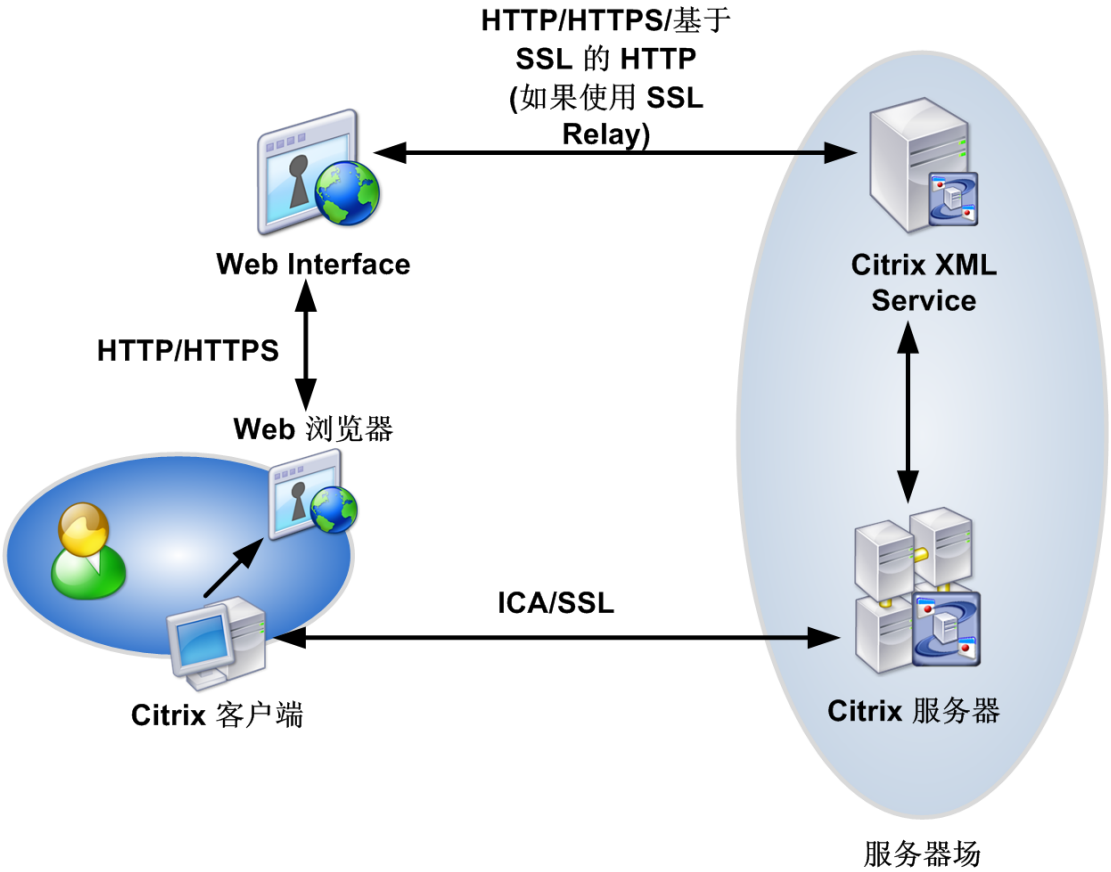
1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenApp Web Sites（XenApp Web 站点），并在结果窗格中选择您的站点。
3. 在操作窗格中，单击工作区控制。
4. 选中用户从站点注销时注销活动会话复选框，以使用户从 Web Interface 和所有活动会话注销。 如果未选择此选项，则在用户注销之后，用户会话仍将保持活动状态。
5. 选中允许用户自定义复选框，以允许用户在站点的设置屏幕上自行配置此设置。

配置 Web Interface 安全性

一套完整的安全计划必须在资源交付过程的各个环节为数据提供保护。 本节介绍以下每个通信链接的 Web Interface 安全问题和建议：

- 用户设备/Web Interface 通信。 讨论有关在 Web 浏览器和服务器之间传递 Web Interface 数据的问题，以及讨论用于保护传输数据和用户设备上写入的数据的建议策略。
- Web Interface/Citrix 服务器通信。 介绍如何保护在 Web Interface 服务器和服务器场之间传递的身份验证与资源信息。
- 用户会话/服务器通信。 阐述有关在 Citrix 客户端和服务器之间传递会话信息的问题。讨论可保护此类数据的 Web Interface 和 XenApp/XenDesktop 安全功能的实现。

下图显示了用户设备如何与运行 XenApp 或 XenDesktop 的服务器及 Web Interface 服务器交互。



常规安全注意事项

与任何基于 Windows 的服务器一样，Citrix 建议您按照配置服务器的 Microsoft 标准指南进行操作。

始终确保使用最新的修补程序更新所有组件。 有关如何检查最新的下载推荐的详细信息，请访问 Microsoft 网站：http://support.microsoft.com/。

SSL 和 TLS

更新日期： 2014-12-02

通过安全套接字层 (SSL) 协议，可以保障网络中的数据通信安全。 SSL 提供服务器身份验证、数据流加密以及消息完整性检查。

SSL 使用加密对消息进行编码，验证消息身份并确保消息内容的完整性。 这样可以防范各种风险，例如窃取、误传和数据操纵。 SSL 依靠证书颁发机构颁发的公钥证书来确保身份证明。 有关 SSL、加密和证书的详细信息，请参阅保护服务器场和安全的企业网络下面的主题。

传输层安全性

传输层安全性 (TLS) 是 SSL 协议的最新标准化版本。 互联网工程工作小组 (Internet Engineering Taskforce, IETF) 在接管 SSL 开放式标准的开发任务后，将 SSL 更名为 TLS。 与 SSL 一样，TLS 提供服务器身份验证、数据流加密以及消息完整性检查。

所有受支持的 XenApp for Windows 和 XenDesktop 版本中都包括对 TLS 版本 1.0 的支持。 由于 SSL 版本 3.0 与 TLS 版本 1.0 之间只有一些微小的技术差异，因此在安装过程中用于 SSL 的服务器证书也同样适用于 TLS。

有些组织（包括美国政府组织）要求使用 TLS 来保障数据通信的安全。 这些组织可能还要求使用验证的加密，例如联邦信息处理标准 (FIPS) 140。 FIPS 是一个加密标准。

注: 适用于 Java 应用程序服务器的 Web Interface 支持的最大 SSL/TLS 证书密钥大小是 2048 位。

SSL Relay

SSL Relay 是一个组件，它使用 SSL 来保障 Web Interface 服务器和服务器场之间的通信安全。 SSL Relay 为 TCP/IP 连接提供服务器身份验证、数据加密和消息完整性。 SSL Relay 由 Citrix XTE Service 提供。

SSL Relay 相当于 Web Interface 服务器和 Citrix XML Service 之间的通信的中介。 在使用 SSL Relay 时，Web 服务器首先会根据受信任证书颁发机构的列表，检查中继的服务器证书来验证 SSL Relay 的身份。

在进行此身份验证后，Web 服务器和 SSL Relay 将对会话的加密方法进行协商。 然后，Web 服务器将加密形式的所有信息请求发送到 SSL Relay。 SSL Relay 对请求进行解密，然后将其发送给 Citrix XML Service。 将信息返回到 Web 服务器时，Citrix XML Service 通过运行 SSL Relay 的服务器发送所有信息，从而对数据进行加密并将其转发给 Web 服务器进行解密。 消息完整性检查用于验证各个通信是否被篡改。

ICA 加密

使用 ICA 加密，可以对服务器和 Citrix 客户端之间发送的信息进行加密。 这使未经授权的用户难以解译加密传输。

ICA 加密可提供机密性，这有助于防范窃听威胁。 但是，也存在其他安全风险，因此使用加密只是综合安全策略的一个方面。 与 SSL/TLS 不同，ICA 加密不提供服务器身份验证。 因此，当信息通过网络时理论上可能会被截获，并被重新路由到假冒服务器。 此外，ICA 加密也不提供完整性检查。

ICA 加密不适用于 XenApp for UNIX 服务器。

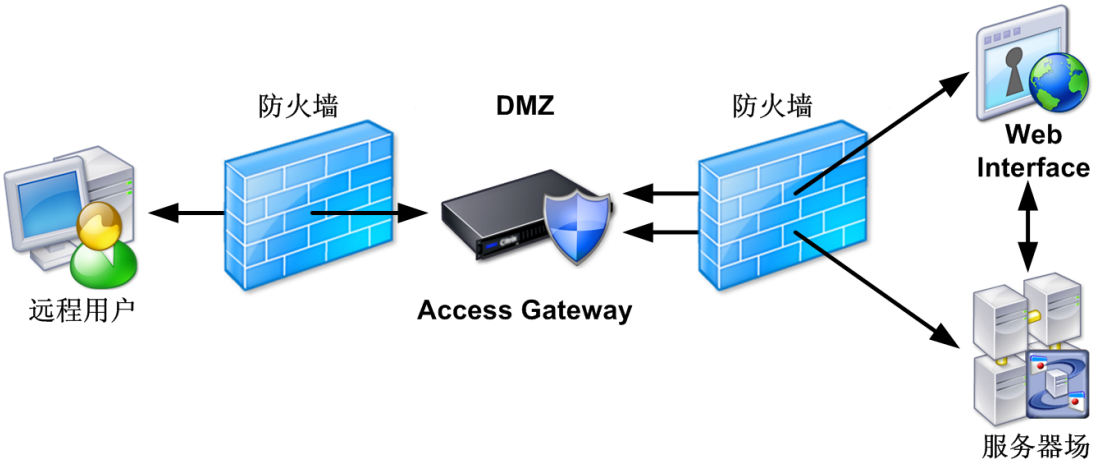
Access Gateway

您可以将 Access Gateway 与 Web Interface 和 Secure Ticket Authority (STA) 配合使用，为从运行 XenApp 或者 XenDesktop 的服务器传递的资源（应用程序、内容和桌面）提供身份验证、授权和重定向。

Access Gateway 是一种通用的安全套接字层 (SSL) 虚拟专用网络 (VPN) 设备，为任何信息资源（数据和语音）提供单一的安全访问点。 Access Gateway 用于对所有资源和协议进行加密和提供支持。

Access Gateway 可为远程用户提供对授权的应用程序、内容、桌面和网络资源的无缝安全访问，使这些用户就像在其组织的防火墙内工作一样，对网络驱动器上的文件、电子邮件、Intranet 站点和资源进行处理。

下图显示了 Access Gateway 如何保障启用了 SSL/TLS 的 Citrix 客户端和服务器之间的通信安全。



有关 Access Gateway 的详细信息，请参阅 Access Gateway 文档。 有关如何使用 Citrix Web Interface Management 控制台配置 Web Interface 以获得 Access Gateway 支持的详细信息，请参阅配置网关设置。

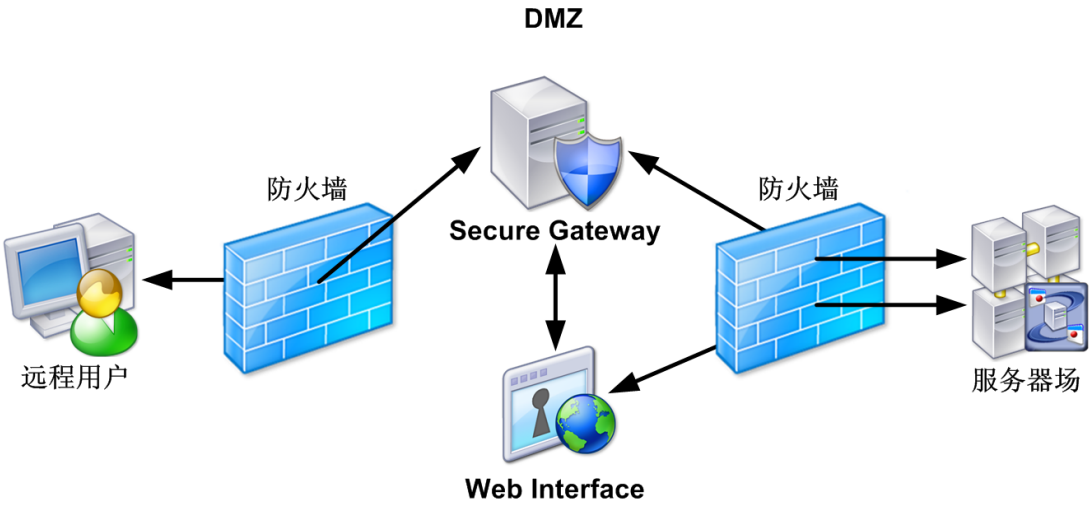
Secure Gateway

更新日期： 2014-11-25

您可以使用 Secure Gateway 和 Web Interface，通过 Internet 为公司内部网络的服务器提供单一、安全的加密访问点。

Secure Gateway 充当启用了 SSL/TLS 的 Citrix 客户端和服务器之间的安全 Internet 网关，并对 ICA 通信进行加密。 用户设备和 Secure Gateway 服务器之间的通信的 Internet 部分是使用 SSL/TLS 进行加密的。 这意味着用户可以远程访问信息，而不会影响安全性。 Secure Gateway 还可以简化证书管理，因为只有在 Secure Gateway 服务器上才需要证书，而不是在场中的每个服务器上都需要证书。

下图显示了 Secure Gateway 如何保障启用了 SSL/TLS 的 Citrix 客户端和服务器之间的通信安全。



有关如何使用 Citrix Web Interface Management 控制台配置 Web Interface 以获得 Secure Gateway 支持的详细信息，请参阅配置网关设置。

使用 SSL 保障 Citrix 联机插件的安全

要通过 Citrix Web Interface Management 控制台使用 SSL 保障 Citrix 联机插件和 Web Interface 服务器之间的通信安全，请单击左窗格中的 XenApp 服务站点，在结果窗格中选择站点，单击操作窗格中的服务器设置，然后选中使用 SSL/TLS 实现插件与站点之间的通信复选框。

确保在交付服务控制台中的应用程序属性对话框的客户端选项页上，为每个应用程序选中启用 SSL 和 TLS 协议复选框。

用户设备/Web Interface 通信

Citrix 客户端和 Web Interface 服务器之间的通信包括传递多种不同类型的数据。 在用户对其自身进行标识、浏览其资源并最终选择要访问的资源时，Web 浏览器和 Web 服务器会传递用户凭据、资源集和会话初始化文件。 具体而言，此网络通信包括：

- HTML 表单数据。 用户登录时，Web Interface 站点使用标准 HTML 表单将用户凭据从 Web 浏览器传输到 Web 服务器。 Web Interface 表单以明文形式传递用户名和凭据。

- HTML 页面和会话 Cookie。 用户在登录屏幕上输入其凭据之后，这些凭据将存储在 Web 服务器中并受会话 Cookie 保护。 从 Web 服务器发送到浏览器的 HTML 页面包含资源集。 这些页面列出了可供用户使用的资源。

- ICA 文件。 当用户选择资源时，Web 服务器会将该资源的 .ica 文件发送到 Citrix 客户端（在某些情况下使用 Web 浏览器作为中介）。 .ica 文件包含可用于登录到服务器的票据。 ICA 文件不包含传递身份验证或智能卡身份验证的票据。

  在某些情况下，启动客户端时，系统会在用户的硬盘上将 .ica 文件另存为纯文本文件。 但是，这不会妨碍客户端成功启动。

  通过 ICA 文件签名功能，用户可以确认其启动的应用程序或桌面来自受信任的 Web 服务器。 有关详细信息，请参阅配置 ICA 文件签名。

用户设备/Web Interface 通信的安全问题

攻击者可以在 Web Interface 数据通过 Web 服务器和浏览器之间的网络和写入到用户设备自身上时攻击这些数据。

- 攻击者可以截获在 Web 服务器和浏览器之间传输的登录数据、会话 Cookie 和 HTML 页面。
- 尽管 Web Interface 使用的会话 Cookie 存在时间是短暂的，且会在用户关闭 Web 浏览器后消失，但有权访问该用户的浏览器的攻击者可以检索该 Cookie，并可能使用凭据信息。
- 尽管 .ica 文件不包含任何用户凭据，但在默认情况下，它包含将在 200 秒后到期的一次性使用票据。 在授权的用户可以使用此票据并进行连接之前，攻击者可以使用截获的 .ica 文件连接到服务器。
- 如果使用 HTTPS 连接访问 Web 服务器的 Internet Explorer 用户选择了阻止对加密页面进行缓存的选项，则会在 Windows\Temporary Internet Files 文件夹中以纯文本文件形式保存 .ica 文件。 有权访问用户的 Internet Explorer 缓存的攻击者可以检索此 .ica 文件以获取网络信息。
- 如果在 Citrix 客户端上启用了传递身份验证，攻击者可以向该用户发送一个 .ica 文件，该文件将导致用户的凭据被错误路由到未经授权的服务器或假冒服务器。 如果客户端在用户登录其设备时捕获到这些用户的凭据，并将这些凭据转发到任何服务器（如果 .ica 文件中包含相应设置），则会发生上述情况。

保障用户设备/Web Interface 通信安全的建议

以下建议结合了行业标准安全性做法和 Citrix 提供的安全措施，以保护在用户设备和 Web 服务器之间传输的数据以及写入到用户设备的数据。

实施支持 SSL/TLS 的 Web 服务器和浏览器

为了确保 Web 服务器与 Web Interface 浏览器组件之间的通信安全，可以首先实施安全 Web 服务器和浏览器。 许多安全 Web 服务器依靠 SSL/TLS 技术确保 Web 通信的安全。

在典型的 Web 服务器与浏览器之间发生的事务中，浏览器首先会根据受信任的证书颁发机构的列表，检查该服务器的证书来对其进行身份验证。 验证之后，浏览器将对用户页面请求进行加密，然后解密 Web 服务器返回的文档。 在事务的每一端，TLS 或 SSL 消息完整性检查可确保数据不会在传输时被篡改。

在 Web Interface 部署中，SSL/TLS 身份验证与加密会创建一个安全连接，用户可以通过此连接传递登录屏幕上发布的凭据。 从 Web 服务器发送的数据（包括凭据、会话 Cookie、.ica 文件和 HTML 资源集页面）都是同样安全的。

要在网络上实施 SSL/TLS 技术，您必须拥有支持 SSL/TLS 的 Web 服务器和支持 SSL/TLS 的 Web 浏览器。 使用这些产品对 Web Interface 是透明的。 您无需为 Web Interface 配置 Web 服务器或浏览器。 有关将 Web 服务器配置为支持 SSL/TLS 的详细信息，请参阅您的 Web 服务器文档。

重要：许多支持 SSL/TLS 的 Web 服务器均使用 TCP/IP 端口 443 进行 HTTP 通信。 默认情况下，SSL Relay 也使用此端口。 如果您的 Web 服务器也在运行 SSL Relay，请确保将 Web 服务器或 SSL Relay 配置为使用不同的端口。

不启用传递身份验证

为防止可能将用户凭据错误路由到未经授权的服务器或假冒服务器，请不要在安全安装中启用传递身份验证。 仅在小型受信任环境中使用此功能。

Web Interface/Citrix 服务器通信

Web Interface 与运行 XenApp 或 XenDesktop 的服务器之间的通信涉及在 Web Interface 和服务器场中的 Citrix XML Service 之间传递用户凭据和资源集信息。

在典型会话中，Web Interface 将凭据传递给 Citrix XML 服务以进行用户身份验证，Citrix XML Service 返回资源集信息。 服务器和场使用 TCP/IP 连接和 Citrix XML 协议传递信息。

Web Interface/Citrix 服务器通信的安全问题

Web Interface XML 协议使用明文交换除密码之外的所有数据，密码使用混码进行传输。 通信容易受到以下攻击：

- 攻击者可截获 XML 通信并窃取资源集信息和票据。 能够破解混码的攻击者还可以获取用户凭据。
- 攻击者可以模拟服务器并截获身份验证请求。

保障 Web Interface/Citrix 服务器通信安全的建议

Citrix 建议实施下列安全措施之一来保障在 Web Interface 服务器和服务器场之间发送的 XML 通信的安全：

- 使用 SSL Relay 作为 Web Interface 服务器和服务器场之间的安全中介。 SSL Relay 执行主机身份验证和数据加密。
- 在不支持 SSL Relay 的部署中，在运行 XenApp 或 XenDesktop 的服务器上安装 Web Interface。
- 使用 HTTPS 协议通过使用 SSL 的安全 HTTP 连接发送 Web Interface 数据（如果在运行 XenApp 或 XenDesktop 的服务器上安装了 IIS）。

使用 SSL Relay

更新日期： 2014-12-02

SSL Relay 是 XenApp 和 XenDesktop 的默认组件。

在服务器端上，必须在运行 SSL Relay 的服务器上安装服务器证书并验证服务器的配置。 有关在服务器上安装服务器证书和配置 SSL Relay 的详细信息，请参阅配置服务器和客户端之间的 SSL/TLS 下面的主题。 此外，还可以参阅 SSL Relay 配置工具中的应用程序帮助。 有关 XenApp for UNIX 服务器的信息，请参阅 SSL Relay for UNIX 管理。

在配置 SSL Relay 时，请确保运行 SSL Relay 的服务器允许将 SSL 通信传递给要用作 Citrix XML Service 联系点的服务器。 默认情况下，SSL Relay 仅将通信转发给已安装它的服务器。 但是，可以配置 SSL Relay 将通信转发给其他服务器。 如果部署中的 SSL Relay 所在的服务器不同于要将 Web Interface 数据发送到的服务器，请确保 SSL Relay 的服务器列表包含要将 Web Interface 数据转发到的服务器。

可以使用 Citrix Web Interface Management 控制台或 WebInterface.conf 文件将 Web Interface 配置为使用 SSL Relay。 有关使用控制台将 Web Interface 配置为使用 SSL Relay 的详细信息，请参阅配置一个场中所有服务器的设置。

使用 WebInterface.conf 将 Web Interface 配置为使用 SSL Relay

1. 使用文本编辑器打开 WebInterface.conf 文件。
2. 将 Farm<n> 参数中的 SSLRelayPort 设置更改为服务器上的 SSL Relay 的端口号。
3. 将 Farm<n> 参数中的 Transport 设置的值更改为 SSL。

向 Web Interface 服务器添加新的根证书

要添加对证书颁发机构的支持，您必须向 Web Interface 服务器添加证书颁发机构的根证书。

将根证书复制到 Web 服务器。

- 在 IIS 上，使用 Microsoft 管理控制台 (MMC) 证书管理器管理单元复制证书。
- 在 Java 应用程序服务器上，使用 keytool 命令行工具将证书复制到特定平台的相应密钥库目录。 必须将证书添加到与为网页提供服务的 Java 虚拟机关联的密钥库。 密钥库通常位于以下位置之一：
  - {javax.net.ssl.trustStore}
  - {java.home}/lib/security/jssecacerts
  - {java.home}/lib/security/cacerts

在运行 XenApp 或 XenDesktop 的服务器上启用 Web Interface

对于不支持 SSL Relay 的那些部署，可以通过在提供 Web Interface 数据的服务器上运行 Web 服务器来消除网络攻击的可能性。 在此类 Web 服务器上托管 Web Interface 站点，可以将所有 Web Interface 请求路由至本地主机上的 Citrix XML Service，从而避免了通过网络传输 Web Interface 数据。 但是，必须将避免网络传输的好处与利用 Web 服务器的风险进行权衡。

作为第一步，可以将 Web 服务器和运行 XenApp 或 XenDesktop 的服务器放在防火墙之后，以便两者之间的通信不会向开放的 Internet 环境公开。 在此方案中，用户设备必须能够通过防火墙与 Web 服务器和运行 XenApp 或 XenDesktop 的服务器进行通信。 对于用户设备到 Web 服务器的通信，防火墙必须允许 HTTP 通信（如果正在使用安全 Web 服务器，则通常通过标准 HTTP 端口 80 或 443 进行通信）。 对于客户端到服务器的通信，防火墙必须允许在端口 1494 和 2598 上进行入站 ICA 通信。 有关将 ICA 与网络防火墙结合使用的详细信息，请参阅您的 Web 服务器文档。 有关将 Web Interface 与网络地址转换结合使用的详细信息，请参阅 Web Interface SDK。

注: 在运行 XenApp 的系统上，安装程序使您能够强制 Citrix XML Service 共享 Internet Information Services 的 TCP/IP 端口，而不是使用专用端口。 通过 XenDesktop，安装程序可自动启用端口共享。 启用端口共享后，在默认情况下，Citrix XML Service 和 Web 服务器会使用同一端口。

使用 HTTPS 协议

可以使用 HTTPS 协议保障在 Web 服务器和运行 XenApp 或 XenDesktop 的服务器之间传递的 Web Interface 数据安全。 HTTPS 使用 SSL/TLS 提供强数据加密。

Web 服务器在运行 XenApp 或 XenDesktop 的服务器上与 IIS 建立 HTTPS 连接。 这要求在运行 XenApp 或 XenDesktop 的服务器上共享 IIS 端口，并使该服务器上的 IIS 启用 SSL。 所指定的服务器名称（使用控制台，或在 WebInterface.conf 的 Farm<n> 参数中）必须是与 IIS SSL 服务器证书名称匹配的完全限定的 DNS 名称。

可通过 https://ServerName/scripts/wpnbr.dll 访问 Citrix XML Service。 有关如何使用 Citrix Web Interface Management 控制台将 Web Interface 配置为使用 HTTPS 协议的详细信息，请参阅管理安全访问。

使用 WebInterface.conf 文件将 Web Interface 配置为使用 HTTPS

1. 使用文本编辑器打开 WebInterface.conf 文件。
2. 将 Farm<n> 参数中的 Transport 设置的值更改为 HTTPS。

用户会话/服务器通信

用户设备和服务器之间的 Web Interface 通信包括传递多种不同类型的会话数据，这些数据包括初始化请求和会话信息。

- 初始化请求。 建立会话的第一个步骤称为初始化，该步骤要求 Citrix 客户端请求一个会话，并生成会话配置参数列表。 这些参数控制会话的各个方面，例如，要登录的用户、要绘制的窗口的大小，以及要在会话中执行的程序。

- 会话信息。 初始化会话之后，将通过大量虚拟通道在 Citrix 客户端和服务器之间传递信息；例如，鼠标输入（从客户端到服务器）和图形更新（从服务器到客户端）。

用户会话/服务器通信的安全问题

要捕获和破译客户端与服务器之间的网络通信，攻击者必须能够破解二进制客户端协议。 了解二进制客户端协议的攻击者可以：

- 截获从 Citrix 客户端发送的初始化请求信息，包括用户凭据

- 截获会话信息，包括用户输入的文本和鼠标单击操作以及从服务器发送的屏幕更新

保障用户会话/服务器通信安全的建议

更新日期： 2014-12-02

Citrix 建议通过对通信进行加密或部署 Access Gateway，来保障在用户设备和服务器之间发送的数据的安全。

使用 SSL/TLS 或 ICA 加密

Citrix 建议实现 SSL/TLS 或 ICA 加密来保障 Citrix 客户端和服务器之间的通信安全。 这两种方法都支持对客户端和服务器之间的数据流进行 128 位加密，但 SSL/TLS 还支持对服务器的身份进行验证。

所有受支持的 XenApp 和 XenDesktop 版本中都包括对 SSL 的支持。 所有受支持的 XenApp for Windows 和 XenDesktop 版本中都包括对 SSL/TLS 和 ICA 加密的支持。 有关支持每种方法的 Citrix 客户端的列表，请参阅客户端文档或 Citrix 下载站点。 有关 ICA 加密的详细信息，请参阅 XenApp 管理。

使用 Access Gateway

可以使用 Access Gateway 保障 Citrix 客户端和服务器之间通过 Internet 进行的通信的安全。 Access Gateway 是一种通用的 SSL VPN 设备，该设备可为所有资源提供单一的安全访问点。 有关 Access Gateway 的详细信息，请参阅存档的 Access Gateway 文档。 有关如何使用 Citrix Web Interface Management 控制台配置 Web Interface 以获得 Access Gateway 支持的详细信息，请参阅配置网关设置。

控制诊断日志记录

使用 Citrix Web Interface Management 控制台中站点维护下的诊断日志记录任务，可以提高错误日志记录的系统安全性。 您可以禁止重复记录重复事件，并配置重复事件的记录数量和记录频率。

此外，还可以使用此任务指定错误重定向的 URL。 如果指定自定义的错误回调 URL，则必须处理具有此 URL 的所有错误 ID 并为用户提供错误消息。 另外，即使用户已成功注销且未出现任何错误，此错误回调 URL 也会替换用户的注销屏幕。

使用配置文件配置站点

更新日期： 2014-11-24

站点配置文件

Web Interface 站点包括一个名为 WebInterface.conf 的文件，其中包含该站点的配置数据。您可以使用此文件执行日常管理任务以及自定义站点的设置。 例如，您可以指定用户可更改的设置，并且可以配置针对 Web Interface 的身份验证。

如果您在编辑配置文件时为设置输入无效的值，并且随后使用 Citrix Web Interface Management 控制台，则控制台会将无效值替换为保存文件时的默认值。

如果手动编辑站点配置文件时 Citrix Web Interface Management 控制台正在运行，则您使用控制台所做的任何后续更改都将会导致所编辑的所有配置文件内容被覆盖。 Citrix 建议您在编辑站点配置文件之前关闭 Citrix Web Interface Management 控制台。 如果无法这样做，请在使用控制台进行任何进一步更改之前，刷新控制台以提交您手动编辑的配置文件内容。

可从站点配置目录中获取 WebInterface.conf 文件：

- 在 Microsoft Internet Information Services (IIS) 上，该目录通常为 C:\inetpub\wwwroot\Citrix\SiteName\conf
- 在 Java 应用程序服务器（例如 Apache Tomcat）上，该目录可能为 . /usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF

您可以在 Web 服务器脚本中按页覆盖 WebInterface.conf 中的某些配置值。 有关 Web 服务器脚本的详细信息，请参阅 Web Interface SDK。

注: 您可能需要停止 Web 服务器并重新启动，以使对 WebInterface.conf 进行的更改在 Java 应用程序服务器上生效。 此外，确保使用 UTF-8 编码保存所做的更改。

配置与服务器的通信

在此示例中，您希望指定运行 Citrix XML Service 的其他服务器的名称。 Citrix XML Service 充当服务器场和 Web Interface 服务器之间的通信链路。

当前正在与名为“rock”的服务器进行通信，但是您希望添加一台名为“roll”的服务器，以防 rock 发生故障。 为此，您需要：

1. 使用文本编辑器打开 WebInterface.conf 文件并找到以下行：

   Farm1=rock,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

2. 编辑该行，使其包含其他服务器，如下所示：

   Farm1=rock,roll,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

配置 SSL Relay 通信

在此示例中，您希望使用安全套接字层 (SSL)，来保障 Web 服务器和运行 XenApp 或者 XenDesktop 的服务器之间的通信安全。 SSL Relay 安装在运行 XenApp 或者 XenDesktop 的服务器上，该服务器的完全限定的域名为“blues.mycompany.com”。SSL Relay 侦听 TCP 端口 443 上的连接。

当前正在与名为“rhythm”的服务器进行通信，但是您希望将 rhythm 替换为 blues.mycompany.com。 为此，您需要：

1. 使用文本编辑器打开 WebInterface.conf 文件并找到以下行：

   Farm1=rhythm,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443

2. 将传输更改为 SSL，如下所示：

   Farm1=blues.mycompany.com,Name:Farm1,XMLPort:80, Transport:SSL,SSLRelayPort:443

注: 指定的服务器名称必须与服务器证书上的名称一致。

配置 Secure Gateway 支持

在此示例中，您想要使用以下两个 Secure Ticket Authority 地址指定名为“csg1.mycompany.com”的 Secure Gateway 服务器（其上的 Citrix 客户端使用端口 443）：

- http://country.mycompany.com/scripts/ctxsta.dll
- http://western.mycompany.com/scripts/ctxsta.dll

在 WebInterface.conf 中添加以下行：

```
AlternateAddress=Mapped

CSG_STA_URL1=http://country.mycompany.com/scripts/ctxsta.dll

CSG_STA_URL2=http://western.mycompany.com/scripts/ctxsta.dll

CSG_Server=csg1.mycompany.com

CSG_ServerPort=443

ClientAddressMap=*,SG
```

最后一行为所有用户启用了 Secure Gateway。

配置灾难恢复场

在此示例中，所预留的两个服务器场将仅在用户访问生产场受阻时使用，例如出现电源故障或网络中断一类的问题。

场中运行 Citrix XML Service 的服务器名称为“jazz”和“fusion”。您希望指定这些场用于进行灾难恢复。 为此，请使用文本编辑器打开 WebInterface.conf 文件并添加下列行，以根据您的环境配置此参数的设置：

```
RecoveryFarm1=jazz,Name:RecoveryFarm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60
RecoveryFarm2=fusion,Name:RecoveryFarm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:
```

请注意，只有在第一个灾难恢复场无法访问时才可使用第二个场。 由于资源适用于生产场，因此不能在两个灾难恢复场中聚合。 Web Interface 会按顺序尝试与每个灾难恢复场进行联系，并枚举与其建立通信的第一个场中的资源。

WebInterface.conf 参数

更新日期： 2014-11-25

下表按字母顺序列出了 WebInterface.conf 可以包含的参数。默认值以粗体文本显示。 如果某个参数在 WebInterface.conf 中未指定，则将使用其默认值。

AccountSelfServiceUrl

- 说明：指定 Password Manager Service 的 URL。
- 值：使用 HTTPS 的 URL
- 站点类型：XenApp Web

AdditionalExplicitAuthentication

- 说明：指定除 SAM、ADS 或 NDS 外必须执行的显式双因素身份验证。
- 值：None | SecurID | SafeWord | RADIUS
- 站点类型：XenApp Web

AddressResolutionType

- 说明：指定 .ica 启动文件中要使用的地址类型。
- 值：dns-port | dns | ipv4-port | ipv4
- 站点类型：XenApp Web 和 XenApp Services

AGAuthenticationMethod

- 说明：为 Access Gateway 集成站点指定允许的身份验证方法。 如果用户使用用户名和密码登录 Access Gateway，则必须将此参数设置为“Explicit”（显式）。 如果用户使用智能卡登录 Access Gateway，则将此参数设置为 SmartCard 即表示用户每次访问资源时都需要输入 PIN。 SmartCardKerberos 选项允许使用智能卡登录 Access Gateway 的用户在不提供 PIN 的情况下访问资源。
- 值：Explicit | SmartCard | SmartCard Kerberos
- 站点类型：XenApp Web

AGEPromptPassword

- 说明：指定当用户从 Access Gateway 登录页登录时是否提示他们重新输入密码。
- 值：Off | On
- 站点类型：XenApp Web

AGEWebServiceURL

- 说明：指定 Access Gateway 身份验证服务的 URL。
- 值：有效的 URL
- 站点类型：XenApp Web

AllowBandwidthSelection

- 说明：指定用户是否可以指示其网络连接速度，以便优化 ICA 设置。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeAudio

- 说明：指定是否允许用户调整 ICA 会话的音频质量。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeAutoLogin

- 说明：指定是否允许用户启用和禁用自动登录。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizeClientPrinterMapping

- 说明：指定是否允许用户启用和禁用客户端打印机映射。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeJavaClientPackages

- 说明：指定是否允许用户选择要使用的 Java 客户端软件包。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeLayout

- 说明：指定是否允许用户选择是使用低分辨率图形用户界面还是完整图形用户界面。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeLogoff

- 说明：指定是否允许用户在从服务器注销时覆盖工作区控制功能的行为。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizePersistFolderLocation

- 说明：指定是否允许用户启用和禁用在重新登录时返回上次在“应用程序”屏幕上访问的文件夹的功能。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeReconnectAtLogin

- 说明：指定是否允许用户在登录时覆盖工作区控制功能的行为。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizeReconnectButton

- 说明：指定是否允许用户在单击“重新连接”按钮时覆盖工作区控制功能的行为。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizeSettings

- 说明：指定是否允许用户自定义其 Web Interface 会话。 当此参数设置为 Off 时，“首选项”按钮将不会显示在用户的“登录”屏幕和“应用程序”屏幕上。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizeShowHints

- 说明：指定是否允许用户在“应用程序”屏幕上显示和隐藏提示。
- 值：On | Off
- 站点类型：XenApp Web

AllowCustomizeShowSearch

- 说明：指定是否允许用户在“应用程序”屏幕上启用和禁用搜索。
- 值：Off | On

- 站点类型：XenApp Web

AllowCustomizeSpecialFolderRedirection

- 说明：指定是否允许用户启用和禁用特殊文件夹重定向功能。
- 值 Off | On
- 站点类型 XenApp Web

AllowCustomizeTransparentKeyPassthrough

- 说明：指定是否允许用户选择键组合传递行为。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeVirtualCOMPortEmulation

- 说明：指定是否允许用户启用和禁用 PDA 同步。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeWinColor

- 说明：指定是否允许用户更改 ICA 会话的颜色深度。
- 值：Off | On
- 站点类型：XenApp Web

AllowCustomizeWinSize

- 说明：指定是否允许用户更改 ICA 会话的窗口大小。
- 值：On | Off
- 站点类型：XenApp Web

AllowDisplayInFrames

- 说明：指定是否允许将 XenApp Web 站点显示在嵌入到第三方网页中的框架内。
- 值：On | Off
- 站点类型：XenApp Web

AllowFontSmoothing

- 说明：指定 ICA 会话是否允许字体平滑。
- 值：On | Off

- 站点类型：XenApp Web 和 XenApp Services

AllowUserAccountUnlock

- 说明：指定是否允许用户使用帐户自助服务解除其帐户锁定。
- 值：Off | On
- 站点类型：XenApp Web

AllowUserPasswordChange

- 说明：指定用户可以更改其密码的条件。
- 值：Never | Expired-Only | Always（仅限 XenApp Web 站点）
- 站点类型：XenApp Web 和 XenApp Services

AllowUserPasswordReset

- 说明：指定是否允许用户使用帐户自助服务重置其密码。
- 值：Off | On
- 站点类型：XenApp Web

AlternateAddress

- 说明：指定是否返回 .ica 文件中的备用服务器地址。
- 值：Off | Mapped | On
- 站点类型：XenApp Web 和 XenApp Services

ApplicanceEmbeddedSmartCardSSO

- 说明：指定智能卡身份验证是否使用嵌入的 ActiveX 控件实现单点登录。
- 值：Off | On
- 站点类型：Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- 说明：嵌入式智能卡身份验证 PIN 输入屏幕进入非活动状态后在返回登录屏幕前等待的时间（秒数）。
- 值：20
- 站点类型：Desktop Appliance Connector

ApplianceMultiDesktop

- 说明：指定在为用户分配多个桌面的情况下是否显示桌面列表。
- 值：Off | On

- 站点类型：Desktop Appliance Connector

ApplicationAccessMethods

- 说明：指定用户是否可以使用适用于联机资源的客户端、Citrix 脱机插件或这两者来访问应用程序。
- 值：Remote, Streaming
- 站点类型：XenApp Web 和 XenApp Services

AppSysMessage _<Language Code >

- 说明：指定显示在“应用程序”屏幕的主要内容区域底部的已本地化文本。LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

AppTab<n>

- 说明：指定要显示在“应用程序”屏幕上的选项卡。 可以使用多个实例定义多个选项卡。 或者，可以使用 AllResources 值定义一个包含用户可用的所有资源的选项卡。
- 值：Applications | Desktops | Content | AllResources
- 站点类型：XenApp Web

AppWelcome Message _<Language Code >

- 说明：指定显示在“应用程序”屏幕的主要内容区域顶部的已本地化文本。LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

AuthenticationPoint

- 说明：指定进行用户身份验证的位置。
- 值：WebInterface | ADFS | AccessGateway | 3rdParty | WebServer
- 站点类型：XenApp Web

AutoLaunchDesktop

- 说明：指定是否启用对桌面进行自动访问。 当此参数设置为 On 时，如果用户桌面是所有场中可供用户使用的唯一资源，Web Interface 将会自动启动用户桌面。
- 值：Off | On
- 站点类型：XenApp Web

AutoLoginDefault

- 说明：指定默认情况下是否对使用传递身份验证、通过智能卡传递身份验证和智能卡身份验证访问其资源的用户启用自动登录。
- 值：On | Off
- 站点类型：XenApp Web

BrandingColor

- 说明：指定页眉和页脚区域的颜色。
- 值：十六进制颜色编号或颜色名称
- 站点类型：XenApp Web

BrandingImage

- 说明：指定页眉和页脚区域的商标渐变图像的 URL。
- 值：有效的 URL
- 站点类型：XenApp Web

BypassFailedRadiusServerDuration

- 说明：指定多长时间后考虑重用出现故障的 RADIUS 服务器。
- 值：以分钟为单位的时间 (60)
- 站点类型：XenApp Web

BypassFailedSTADuration

- 说明：指定多长时间后考虑重用对网关设备运行 Secure Ticket Authority 的故障服务器。
- 值：以分钟为单位的时间 (60)
- 站点类型：XenApp Web

ClientAddressMap

- 说明：为服务器端防火墙配置指定客户端地址/地址类型对。 条目中的第一个字段为子网地址和掩码，而第二个字段接受以下值：Normal、Alternate、Translated、SG、SGAlternate 和 SGTranslated。 使用星号 (*) 代替客户端地址或子网表示所有其他未指定的 Citrix 客户端的默认值。
- 值：<Subnet Address>/ <SubnetMask> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …
- 站点类型：XenApp Web

ClientDefaultURL

- 说明：指定当相应的客户端不可下载时客户端检测和部署过程将用户重定向至的 URL。
- 值：http://www. citrix.com/ download。 有效的 URL。

- 站点类型：XenApp Web

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- 说明：为指定的平台配置客户端检测和部署过程。 如果尚未配置相应的参数，用户将被重定向至 ClientDefaultURL 参数所指定的网页。 默认情况下，将为 XenApp 6.0 安装介质上所提供的本机客户端配置这些参数。

  前两个字段指定客户端安装程序的位置和文件名。 如果找不到该文件，用户将被重定向至 ClientDefaultURL 参数所指定的网页。

  Mui 字段指定 Directory 和 Filename 字段所指定的客户端是否支持多种语言。 如果此字段设置为 No，客户端检测和部署过程将检查 <LanguageCode>\<FolderName> 文件夹以查找指定的文件。

  Version 字段提供由 Directory 和 Filename 字段所指定的客户端的版本号（用逗号分隔）。 如果未指定版本号，客户端检测和部署过程将尝试根据指定的文件确定版本。

  ShowEULA 字段指定用户是否需要接受 Citrix 许可协议，以便安装指定的客户端。

  ClassID 字段指定 Windows 客户端的类 ID，该字段是这些客户端的必需设置。

  Url 字段指定当用户单击“下载”按钮并且未使用 Directory 和 Filename 字段指定客户端文件时被重定向至的网页。 仅当客户端文件不可用时，才应使用此设置。

  Description 字段指定要在“下载”按钮上显示的自定义消息。 请注意，此文本未本地化。

- 值：Directory: <FolderName>, Filename: <FileName>, [Mui:Yes | No,] [Version: <Version Number>,] [ShowEULA: Yes | No,] [ClassID: <Value>,] [Url: <ValidURL>,] [Description: <Caption>]

- 站点类型：XenApp Web

ClientProxy

- 说明：为客户端防火墙指定客户端子网地址和掩码以及相关联的代理设置。 返回的 ICA 文件中的客户端地址由这些设置确定。 每个条目包括三个字段。 第一个字段为子网地址和掩码。 使用星号 (*) 表示所有其他未指定的 Citrix 客户端的默认值。 第二个字段为六种代理类型之一。 除非第二个字段（代理类型）为显式代理类型（SOCKS 或 Secure），否则将忽略每组条目（包括三个字段）中第三个字段（代理地址）的值，但此字段必须始终出现，其默认值为减号 (-)。

- 值：<Subnet Address>/ <SubnetMask> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <Proxy Address> | <ProxyAddress>: <ProxyPort>, …

- 站点类型：XenApp Web 和 XenApp Services

CompactHeaderImage

- 说明：指定用户界面的低分辨率图形版本中页眉图像的 URL。
- 值：有效的 URL
- 站点类型：XenApp Web

CompactViewStyles

- 说明：指定低分辨率图形用户界面的“应用程序”屏幕上可供用户使用的视图样式。
- 值：Icons, List
- 站点类型：XenApp Web

CredentialFormat

- 说明：指定显式 Windows 和 NIS 登录接受的凭据格式。
- 值：All | UPN | DomainUsername
- 站点类型：XenApp Web 和 XenApp Services

CSG_EnableSessionReliability

- 说明：指定是否对 Secure Gateway 或 Access Gateway 使用会话可靠性。
- 值：On | Off
- 站点类型：XenApp Web 和 XenApp Services

CSG_Server

- 说明：指定 Access Gateway 设备或 Secure Gateway 服务器的地址。
- 值：None。 FQDN 格式的服务器地址
- 站点类型：XenApp Web 和 XenApp Services

CSG_ServerPort

- 说明：指定 Access Gateway 设备或 Secure Gateway 服务器的端口。
- 值：None。 服务器端口
- 站点类型：XenApp Web 和 XenApp Services

CSG_STA_URL<n>

- 说明：指定对网关设备运行 Secure Ticket Authority 的服务器的 URL。
- 值：None。 STA 的 URL
- 站点类型：XenApp Web 和 XenApp Services

CSG_UseTwoTickets

- 说明：指定在通过 Access Gateway 访问资源时 Web Interface 是否从两个不同的 Secure Ticket Authority 请求票据。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

DefaultAudioQuality

- 说明：指定用于 ICA 连接的默认音频质量。
- 值：NoPreference | High | Medium | Low | Off
- 站点类型：XenApp Web

DefaultBandwidthProfile

- 说明：指定用于 ICA 连接的默认带宽配置文件（即与带宽相关的设置集，例如音频质量和颜色深度）。
- 值：Custom | High | Medium High | Medium | low
- 站点类型：XenApp Web

DefaultColorDepth

- 说明：指定用于 ICA 连接的默认颜色深度。
- 值：NoPreference | TrueColor | HighNoPreferenceColor
- 站点类型：XenApp Web

DefaultCompactViewStyle

- 说明：指定低分辨率图形用户界面的“应用程序”屏幕上的默认视图样式。
- 值：List | Icons
- 站点类型：XenApp Web

DefaultCustomTextLocale

- 说明：指定用于自定义文本的默认区域设置。 必须在定义的任何自定义文本参数 (*_<LanguageCode>) 中指定相同的区域设置。
- 值：None. en | de | es | fr | ja | any other supported language identifier
- 站点类型：XenApp Web

DefaultPrinterMapping

- 说明：指定是否对 ICA 连接默认启用打印机映射。
- 值：On | Off

- 站点类型：XenApp Web

DefaultViewStyle

- 说明：指定完整图形用户界面的“应用程序”屏幕上的默认视图样式。
- 值：Icons | Details | Groups | List | Tree
- 站点类型：XenApp Web

DefaultWindowSize

- 说明：指定用于 ICA 会话的默认窗口模式。 可以使用 X% 格式以总屏幕面积的百分比形式指定，或者使用 XxY 格式以固定大小自定义尺寸形式指定
- 值：FullScreen | Seamless | X% | XxY
- 站点类型：XenApp Web

DisplayBrandingImage

- 说明：指定是否对页眉和页脚区域显示商标渐变图像。
- 值：On | Off
- 站点类型：XenApp Web

DomainSelection

- 说明：指定“登录”屏幕上列出的用于显式身份验证的域名。
- 值：NetBIOS 域名的列表
- 站点类型：XenApp Web 和 XenApp Services

DuplicateLogInterval

- 说明：指定监视到 DuplicateLogLimit 个日志条目所用的时间段。
- 值：以秒为单位的时间 (60)
- 站点类型：XenApp Web 和 XenApp Services

DuplicateLogLimit

- 说明：指定在 DuplicateLogInterval 指定的时间段内允许的重复日志条目数。
- 值：大于 0 的整数 (10)
- 站点类型：XenApp Web 和 XenApp Services

EnableFileTypeAssociation

- 说明：指定是否对站点启用文件类型关联。 如果此参数设置为 Off，则站点不能使用内容重定向。

- 值：On | Off
- 站点类型：XenApp Web 和 XenApp Services

EnableKerberosToMPS

- 说明：指定是否启用 Kerberos 身份验证。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

EnableLegacyICAClientSupport

- 说明：指定是否支持无法读取 UTF-8 .ica 文件的旧版 Citrix 客户端。 如果此参数设置为 Off，服务器将生成 UTF-8 编码的 .ica 文件。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

EnableLogoffApplications

- 说明：指定当用户从服务器注销时工作区控制功能是否注销活动资源。
- 值：On | Off
- 站点类型：XenApp Web

EnablePassthroughURLs

- 说明：指定是否允许用户创建使用 Web Interface 访问的资源的持久链接。
- 值：Off | On
- 站点类型：XenApp Web

EnableRadiusServerLoadBalancing

- 说明：指定是否在配置的 RADIUS 服务器之间对会话进行负载平衡。 无论此参数的设置如何，服务器之间仍会出现故障转移。
- 值：Off | On
- 站点类型：XenApp Web

EnableSTALoadBalancing

- 说明：指定是否在为网关设备配置的 Secure Ticket Authority 服务器之间对请求进行负载平衡。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

EnableVirtualCOMPortEmulation

- 说明：指定是否通过联网的 USB 连接启用 PDA 同步。
- 值：Off | On
- 站点类型：XenApp Web

EnableWizardAutoMode

- 说明：指定客户端检测和部署过程是否以自动模式运行。
- 值：On | Off
- 站点类型：XenApp Web

EnableWorkspaceControl

- 说明：指定工作区控制功能是否对用户可用。
- 值：On | Off
- 站点类型：XenApp Web

ErrorCallbackURL

- 说明：指定发生错误时 Web Interface 重定向至的 URL。 该 URL 所引用的网页必须接受并处理以下四个查询字符串参数：

  CTX_MessageType

  CTX_MessageKey

  CTX_MessageArgs

  CTX_LogEventID

- 值：有效的 URL
- 站点类型：XenApp Web

Farm<n>

- 说明：指定有关场的所有信息。 最多可以配置 512 个场。
- 值：Citrix XML Service address [,Citrix XML Service address,] [,Name:<Name>] [,XMLPort: <Port>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <Port>] [,Bypass Duration: <TimeInMinutes (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <TimeInSeconds (200)>] [,RADETicket TimeToLive: <TimeInSeconds (200)>]
- 站点类型：XenApp Web 和 XenApp Services

Farm<n>Groups

- 说明：指定允许从服务器场枚举资源的 Active Directory 组。 包括此参数的设置将激活用户漫游功能。 对于使用 Farm<n> 参数定义的每个场，最多可以指定 512 个用户组。

- 值：None。 Domain\ UserGroup[,...]
- 站点类型：XenApp Web、XenApp Services 和 XenDesktop

FooterText _<Language Code>

- 说明：指定显示在所有页面的页脚区域中的已本地化页脚文本。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

HeaderFontColor

- 说明：指定页眉区域的字体颜色。
- 值：十六进制颜色编号或颜色名称
- 站点类型：XenApp Web

HeadingHomePage

- 说明：指定作为主页标题显示的图像的 URL。
- 值：有效的 URL
- 站点类型：XenApp Web

HeadingImage

- 说明：指定作为 Web Interface 标题显示的图像的 URL。
- 值：有效的 URL
- 站点类型：XenApp Web

HideDomainField

- 说明：指定“域”字段是否显示在“登录”屏幕上。
- 值：Off | On
- 站点类型：XenApp Web

IcaFileSigningCertificateThumbprint

- 说明：ICA 文件签名所用的证书的缩略图。
- 值：None。 可能包含或不包含空白的缩略图
- 站点类型：XenApp Web 和 Desktop Appliance Connector

IcaFileSigningEnabled

- 说明：启用和禁用 ICA 文件签名功能。

- 值：Off | On
- 站点类型：XenApp Web 和 Desktop Appliance Connector

IcaFileSigningHashAlgorithm

- 说明：ICA 文件签名所用的哈希算法。
- 值：SHA1 | SHA256
- 站点类型：XenApp Web 和 Desktop Appliance Connector

IgnoreClientProvidedClientAddress

- 说明：指定是否忽略 Citrix 客户端提供的地址。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

InternalServerAddressMap

- 说明：指定正常地址/转换地址对。 正常地址用于标识与网关通信的服务器，而转换地址返回到 Citrix 客户端。
- 值：NormalAddress = Translated Address, …
- 站点类型：XenApp Web 和 XenApp Services

JavaClientPackages

- 说明：指定对用户可用的默认 Java 客户端软件包集。
- 值：ClipBoard、ConfigUI、PrinterMapping、SecureICA、SSL、Audio、ClientDriveMapping、ZeroLatency
- 站点类型：XenApp Web

JavaFallbackMode

- 说明：指定当用户未安装本机客户端时是否回退到 Java 客户端。 仅当 LaunchClients 参数包括值 Ica-Local 时，此参数才适用。 通过 Manual 设置，用户可以选择是否尝试使用 Java 客户端。
- 值：None | Manual | Auto
- 站点类型：XenApp Web

KioskMode

- 说明：指定用户设置是应持久，还是仅持续到会话寿命结束为止。 启用 kiosk 模式时，用户设置不会从一个会话持续到另一个会话。
- 值：Off | On
- 站点类型：XenApp Web

LaunchClients

- 说明：指定允许用户选择的 Citrix 客户端。 对于双模式站点，将忽略此参数，此时参数设置始终为 Ica-Local。省略 Ica-Java 设置不会阻止为用户提供 Java 客户端。 为此，还需要将 JavaFallbackMode 参数设置为 None。
- 值：Ica-Local、Ica-Java、Rdp-Embedded
- 站点类型：XenApp Web

LoginDomains

- 说明：指定用于访问限制的域名。
- 值：NetBIOS 域名的列表
- 站点类型：XenApp Web 和 XenApp Services

LoginSys Message _<Language Code>

- 说明：指定显示在“登录”屏幕的主要内容区域底部的已本地化文本。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

LoginTitle _<Language Code>

- 说明：指定显示在“登录”屏幕的欢迎消息上方的已本地化文本。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

LoginType

- 说明：指定对用户显示的“登录”屏幕的类型。 “登录”屏幕可以是基于域的，也可以是基于 NDS 的。
- 值：Default | NDS
- 站点类型：XenApp Web 和 XenApp Services

LogoffFederationService

- 说明：指定在 AD FS 集成站点中单击“注销”按钮时是只将用户从 XenApp Web 站点注销，还是将用户从联合身份验证服务全局注销。
- 值：On | Off
- 站点类型：XenApp Web

MultiFarmAuthenticationMode

- 说明：此模式有三个选项，用于指定允许使用的身份验证方法。 “All”选项为默认设置，在此设置下，将对所有场进行身份验证以枚举任意应用程序。 “Any”选项允许为通过身份验证的用户枚举任意场中的应用程序，但如果用户错误地输入了凭据，则即使在其中任何场中的身份验证失败，也会向每个场提供不正确的凭据以进行身份验证。 这还可能会锁定帐户。 “Primary”选项允许用户在回退到“Any”模式之前针对主要场（为 Web Interface 配置的场列表中的第一个场）进行身份验证；此选项有助于防止锁定帐户。
- 值：All | Any | Primary
- 站点类型：XenApp Web

MultiLaunchTimeout

- 说明：指定在用户初次单击资源图标以启动资源后图标处于非活动状态的时间。
- 值：以秒为单位的时间 (2)
- 站点类型：XenApp Web

NDSContextLookupLoadbalancing

- 说明：指定是否在配置的 LDAP 服务器之间对 NDS 请求进行负载平衡。 无论此参数的设置如何，服务器之间仍会出现故障转移。
- 值：Off | On
- 站点类型：XenApp Web

NDSContextLookupServers

- 说明：指定要使用的 LDAP 服务器。 如果未指定端口，将根据协议推断端口：如果此参数设置为 ldap，将使用默认 LDAP 端口 (389)；如果此参数设置为 ldaps，将使用默认 LDAP over SSL 端口 (636)。 最多可以配置 512 个 LDAP 服务器。

  如果未定义此参数或此参数不存在，则会禁用无上下文登录功能。
- 值：None。ldap://[:] | ldaps://[:],
- 站点类型：XenApp Web

NDSTreeName

- 说明：指定使用 NDS 身份验证时要使用的 NDS 树。
- 值：None。 NDS 树名称
- 站点类型：XenApp Web 和 XenApp Services

OverlayAutologonCredsWithTicket

- 说明：指定登录票据是必须在登录票据条目中重复，还是必须仅放在一个单独的 .ica 启动文件票据条目中。 启用凭据覆盖后，登录票据将会重复。
- 值：On | Off
- 站点类型：XenApp Web

OverrideIcaClientname

- 说明：指定 Web Interface 生成的 ID 是否必须在 .ica 启动文件的 clientname 条目中传递。
- 值：Off | On
- 站点类型：XenApp Web

PasswordExpiryWarningPeriod

- 说明：指定密码到期前多少天提示用户更改其密码。
- 值：0 到 999 之间的整数 (14)
- 站点类型：XenApp Web

PersistFolderLocation

- 说明：指定当用户重新登录时是否返回上次在“应用程序”屏幕上访问的文件夹。
- 值：Off | On
- 站点类型：XenApp Web

PNAChangePasswordMethod

- 说明：指定 Citrix 联机插件如何处理来自用户的更改密码请求。 如果此参数设置为 Direct-Only，插件将通过直接与域控制器通信来更改密码。 Direct-With-Fallback 表示插件最初将尝试访问域控制器，但如果访问失败，它将使用 XenApp Services 站点。 Proxy 选项表示插件通过访问 XenApp Services 站点来更改密码。
- 值：Direct-Only | Direct-With- Fallback | Proxy
- 站点类型：XenApp Services

PooledSockets

- 说明：指定是否使用套接字池。
- 值：On | Off
- 站点类型：XenApp Web 和 XenApp Services

PreLoginMessageButton _<Language Code >

- 说明：指定登录前消息确认按钮的已本地化名称。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

PreLoginMessageText _<Language Code >

- 说明：指定显示在登录前消息页上的已本地化文本。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

PreLoginMessageTitle _<Language Code >

- 说明：指定登录前消息页的已本地化标题。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

RADERequestValidation

- 说明：指定是否对来自 Citrix 脱机插件的传入请求执行文本验证。
- 值：
- 站点类型：XenApp Web 和 XenApp Services

RADESessionURL

- 说明：指定 RADE 会话页的 URL。 如果此参数设置为 auto，将自动生成 URL。
- 值：Auto。 有效的 URL
- 站点类型：XenApp Web 和 XenApp Services

RadiusRequestTimeout

- 说明：指定等待来自会话的 RADIUS 服务器的响应时要使用的超时值。
- 值：以秒为单位的时间 (30)
- 站点类型：XenApp Web

RadiusServers

- 说明：指定要使用的 RADIUS 服务器以及这些服务器侦听的端口（可选）。 可以使用 IP 地址或名称指定服务器，并且每个元素的服务器和端口用冒号分隔。 如果未指定端口，将使用默认 RADIUS 端口 (1812)。 最多可以配置 512 个服务器。
- 值：Server [:Port] [,…]
- 站点类型：XenApp Web

ReconnectAtLogin

- 说明：指定当用户登录时工作区控制是否应重新连接到资源，如果应重新连接到资源，则指定是重新连接到所有资源，还是仅重新连接到已断开连接的资源。
- 值：Disconnected AndActive | Disconnected | None

- 站点类型：XenApp Web

ReconnectButton

- 说明：指定当用户单击“重新连接”按钮时工作区控制是否应重新连接到应用程序，如果应重新连接到应用程序，则指定是重新连接到所有应用程序，还是仅重新连接到已断开连接的应用程序。
- 值：Disconnected AndActive | Disconnected | None
- 站点类型：XenApp Web

RecoveryFarm<n>

- 说明：指定有关灾难恢复场的所有信息。 最多可以配置 512 个场。
- 值：Citrix XML Service address [,Citrix XML Service address,] [,Name:<Name>] [,XMLPort: <Port>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <Port>] [,Bypass Duration: <TimeInMinutes (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <TimeInSeconds (200)>] [,RADETicket TimeToLive: <TimeInSeconds (200)>]
- 站点类型：XenApp Web、XenApp Services 和 XenDesktop

RequestedHighColorIcons

- 说明：指定是否从 Citrix XML Service 请求高颜色深度的 32 位图标，如果是，则列出图标大小（以像素为单位）。 如果此参数设置为 None，则仅请求标准 4 位 32 x 32 图标。 默认设置根据站点类型及其配置会有所不同。
- 值：16, 32, 48 | None

  对于 XenApp Services 站点，默认设置是请求所有图标。 对于 XenApp Web 站点，默认情况下仅请求 16 x 16 和 32 x 32 大小。
- 站点类型：XenApp Web 和 XenApp Services

RequestICAClientSecureChannel

- 说明：指定 TLS 设置。
- 值：Detect-Any Ciphers、TLS- GovCiphers、SSL-AnyCiphers
- 站点类型：XenApp Web 和 XenApp Services

RequireLaunchReference

- 说明：指定是否强制使用启动引用。 启动引用是向 XenApp VM 托管应用程序传递身份验证所必需的。 如果需要与适用于 UNIX 的 XenApp 4.0 Feature Pack 1 兼容，则必须将此参数设置为 Off。
- 值：On | Off
- 站点类型：XenApp Web 和 XenApp Services

RestrictDomains

- 说明：指定是否使用 LoginDomains 参数来限制用户访问。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

SearchContextList

- 说明：指定用于 NDS 身份验证的上下文名称。
- 值：None。 用逗号分隔的上下文名称的列表
- 站点类型：XenApp Web 和 XenApp Services

ServerAddressMap

- 说明：为服务器端防火墙配置指定正常地址/转换地址对。 正常地址用于标识服务器，而转换地址返回到 Citrix 客户端。
- 值：NormalAddress, Translated Address, …
- 站点类型：XenApp Web 和 XenApp Services

ServerCommunicationAttempts

- 说明：指定在认为 Citrix XML Service 出现故障之前尝试向该服务发送请求的次数。
- 值：大于 0 的整数 (2)
- 站点类型：XenApp Web 和 XenApp Services

ShowClientInstallCaption

- 说明：指定安装标题的显示方式和显示时间。 如果将此参数设置为 Auto，将导致在用户没有安装 Citrix 客户端或更好的客户端可用时显示安装标题。 如果此参数设置为 Quiet，则仅当用户没有客户端时才显示安装标题。 “登录”屏幕的行为略有不同，因为标题仅对用于联机资源的客户端显示，以及仅在未检测到客户端时才显示。 因此，Auto 和 Quiet 设置对于“登录”屏幕没有任何差别。
- 值：Auto | Quiet | Off
- 站点类型：XenApp Web

ShowDesktopViewer

- 说明：指定当用户访问其桌面时，默认情况下是否启用 Citrix Desktop Viewer 窗口和工具栏。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

ShowHints

- 说明：指定“应用程序”屏幕上是否显示提示。

- 值：On | Off
- 站点类型：XenApp Web

ShowPasswordExpiryWarning

- 说明：指定为用户显示密码过期警告的条件。
- 值：Never | WindowsPolicy | Custom
- 站点类型：XenApp Web

ShowRefresh

- 说明：指定“应用程序”屏幕上的“刷新”按钮是否对用户可用。
- 值：Off | On
- 站点类型：XenApp Web

ShowSearch

- 说明：指定“应用程序”屏幕上的搜索控件是否对用户可用。
- 值：On | Off
- 站点类型：XenApp Web

SpecialFolderRedirection

- 说明：指定是否启用特殊文件夹重定向功能。 如果此参数设置为 On，将定向资源以使用用户本地计算机上的 \Documents 和 \Desktop 文件夹。 将此参数设置为 Off，表示应用程序中可用的 \Documents 和 \Desktop 文件夹会是服务器上的文件夹。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

SuppressDuplicateResources

- 说明：指定是否向用户隐藏在不同场中发布的名称和文件夹位置都相同的资源的存在情况。
- 值：Off | On
- 站点类型：XenApp Web 和 XenApp Services

Timeout

- 说明：指定与 Citrix XML Service 通信时要使用的超时值。
- 值：以秒为单位的时间 (60)
- 站点类型：XenApp Web 和 XenApp Services

TransparentKeyPassthrough

- 说明：指定 Windows 键组合传递的模式。
- 值：FullScreen Only | Local | Remote
- 站点类型：XenApp Web 和 XenApp Services

TwoFactorPasswordIntegration

- 说明：指定是否启用与 RSA SecurID 6.0 的密码集成。
- 值：Off | On
- 站点类型：XenApp Web

TwoFactorUseFullyQualifiedUserNames

- 说明：指定在双因素身份验证期间是否将完全限定的用户名传递给身份验证服务器。
- 值：Off | On
- 站点类型：XenApp Web

UpgradeClientsAtLogin

- 说明：当更新版本的相应本机客户端或 Citrix 脱机插件可用时，指定在用户登录时客户端检测和部署过程是否自动运行。 仅当 EnableWizardAutoMode 设置为 On 时，此参数才适用。
- 值：Off | On
- 站点类型：XenApp Web

UPNSuffixes

- 说明：指定限制进行显式身份验证的 UPN 身份验证后缀。
- 值：UPN 后缀列表
- 站点类型：XenApp Web 和 XenApp Services

UserInterfaceBranding

- 说明：指定站点是重点针对访问应用程序的用户还是访问桌面的用户。 如果将此参数设置为 Desktops，可更改站点功能以改善 XenDesktop 用户的体验。 Citrix 建议对包括 XenDesktop 的任何部署都使用此设置。
- 值：Applications | Desktops
- 站点类型：XenApp Web

UserInterfaceLayout

- 说明：指定是否使用精简用户界面。
- 值：Auto | Normal | Compact

- 站点类型：XenApp Web

UserInterfaceMode

- 说明：指定“登录”屏幕的外观。 如果此参数设置为 Simple，将只显示所选身份验证方法的登录字段。 如果将此参数设置为 Advanced，可显示导航栏，导航栏提供对登录前的“消息”和“首选项”屏幕的访问。
- 值：Simple | Advanced
- 站点类型：XenApp Web

ViewStyles

- 说明：指定完整图形用户界面的“应用程序”屏幕上可供用户使用的视图样式。
- 值：Details | Groups | Icons | List | Tree
- 站点类型：XenApp Web

WebSessionTimeout

- 说明：指定空闲 Web 浏览器会话的超时值。
- 值：以分钟为单位的时间 (20)
- 站点类型：XenApp Web

Welcome Message _<Language Code>

- 说明：指定显示在“登录”屏幕欢迎区域中的已本地化的欢迎消息文本。 LanguageCode 为 en、de、es、fr、ja 或其他任何支持的语言标识符。
- 值：None。 纯文本以及任意数目的 HTML 换行标记
 和超链接
- 站点类型：XenApp Web

WIAuthenticationMethods

- 说明：为没有与 Access Gateway 集成的站点指定允许的身份验证方法。 这是一个逗号分隔的列表，可以按任意顺序包含任何指定的值。
- 值：Explicit、Anonymous、Certificate SingleSignOn、Certificate、SingleSignOn 的任意组合
- 站点类型：XenApp Web、XenApp Services 和 Desktop Appliance Connector

config.xml 文件的内容

更新日期： 2014-12-02

config.xml 文件包含很多参数，这些参数分为多个不同的类别。 您可以编辑以下类别的参数：

- FolderDisplay。 指定资源图标的显示位置：开始菜单中，物理 Windows 桌面上或通知区域中。 另外，还有一个参数用来指定开始菜单中的特定文件夹。 这些参数与 Citrix 联机插件选项对话框的应用程序显示页中的控件对应。
- DesktopIntegration。 指定是否向开始菜单、桌面或通知区域添加快捷方式。
- ConfigurationFile。 为要在以后使用的插件的 config.xml 指定其他 URL。 这有助于将用户移动到其他 Web Interface 服务器。
- Request。 指定插件应从哪个位置请求资源数据以及刷新信息的频率。
- Failover。 指定主服务器不可用时要联系的备份服务器 URL 的列表。
- 登录。 指定要使用的登录方法。
- ChangePassword。 指定在哪些情况下允许 Citrix 联机插件用户更改其密码以及用于路由请求的路径。
- UserInterface。 指定是否隐藏或显示作为 Citrix 联机插件用户界面的一部分向用户显示的某些选项组。
- ReconnectOptions。 指定用户是否能够使用工作区控制功能。
- FileCleanup。 指定用户从 Citrix 联机插件注销时是否删除快捷方式。
- ICA_Options。 定义插件连接的显示和声音选项。 这与 Citrix 联机插件选项对话框的会话选项页中的设置对应。
- AppAccess。 指定可供用户使用的资源类型。

有关使用 config.xml 文件的详细信息，请参阅适用于 Windows 的联机插件。

Citrix 联机插件注意事项

特定的 WebInterface.conf 参数设置会影响 Citrix 联机插件请求的验证。 Citrix 建议将 WebInterface.conf 中的设置与 Citrix 联机插件的 config.xml 文件中的设置保持一致。

WebInterface.conf 文件中的设置

下表包含 WebInterface.conf 中的参数，这些参数必须与 config.xml 文件中的参数一致。 表中还对影响 Citrix 联机插件及其建议设置的参数进行了说明。

参数	建议设置
LoginType	如果设置为 NDS，则还必须在 config.xml 中启用 Novell 身份验证。
NDSTreeName	Config.xml 的 Logon 部分中的 DefaultTree 必须包含相同的设置。
PNAChangePasswordMethod	Config.xml 的 ChangePassword 部分中的方法必须包含相同的设置。
WIAuthenticationMethods	使用 WebInterface.conf 文件中配置的同一身份验证方法。 如果此方法不同于 config.xml 中的方法，则身份验证会失败。

使用 Citrix 联机插件时配置 Web Interface

1. 使用文本编辑器打开 WebInterface.conf 文件。
2. 查找下列参数：
   - LoginType
   - NDSTreeName
   - PNAChangePasswordMethod
   - WIAuthenticationMethods
3. 按 config.xml 文件的内容中所述修改这些参数的设置。
4. 重新启动 Web Interface 服务器以应用所做的更改。

有关 WebInterface.conf 文件设置的详细信息，请参阅 WebInterface.conf 参数。

Bootstrap.conf 文件中的设置

下表列出了 bootstrap.conf 文件中的设置。

参数	说明	值	站点类型
ConfigurationLocation	指定 Web Interface 站点应从中获取其配置的文件。 该文件可以是本地文件，也可以是通过网络共享的远程文件（对于 IIS 上托管的站点）。	WebInterface.conf 的绝对路径	XenApp Web XenApp Services
DefaultLocale	指定 Web 浏览器请求不受支持的语言时要使用的默认语言。	en | de | es | fr | ja | 其他任何支持的语言标识符	XenApp Web XenApp Services
SiteName	指定显示在 Citrix Web Interface Management 控制台中的站点的名称。 默认设置使用站点的 URL。	有效字符串	XenApp Web XenApp Services

配置对适用于 UNIX 的 XenApp 4.0 Feature Pack 1 的支持

在此示例中，您要配置一个站点，使其与适用于 UNIX 的 XenApp 4.0 Feature Pack 1 兼容。 新的 Web Interface 站点最初与此产品不兼容，需要执行另外的手动站点配置步骤。

1. 使用文本编辑器打开 WebInterface.conf 文件并找到以下行：

   OverrideIcaClientname=Off

   RequireLaunchReference=On

2. 按如下所示更改设置：

   OverrideIcaClientname=On

   RequireLaunchReference=Off

   注: 将 RequireLaunchReference 参数设置为 Off，可禁用对 XenApp VM 托管应用程序的传递身份验证。 此站点的用户在每次访问 VM 托管应用程序时，将都需要输入其凭据。

配置用户漫游

在此示例中，您希望将公司的美国办事处中的用户组与特定服务器场关联起来，以便这些用户在访问日本办事处时可以登录到本地 Web Interface 服务器，并从美国的场自动接收英语语言资源。

配置文件中已将现有的场（服务器“waltz”上正在运行 Citrix XML 服务）定义为 Farm1，该场可供登录到美国 Web Interface 服务器的所有用户使用。 用户组“SalesMgrs”和“SalesTeam”位于域“ussales.mycompany.com”中，“Accounts”用户组位于“finance.mycompany.com”域中。 您希望将这些组中的用户与场关联起来，在这些场中，运行 Citrix XML Service 的服务器的名称是“foxtrot”和“tango”。为此，您需要：

1. 使用文本编辑器打开美国 Web Interface 服务器上的 WebInterface.conf 文件，找到以下行：

```
Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalanc
```

> 重要：如果启用了用户漫游，则配置文件中定义的第一个场必须正在运行 XenApp 6.0 或更高版本或者 XenDesktop 4.0 或更高版本。 如果列出的第一个场运行的是早期版本，则不会对任何用户显示资源。

2. 通过添加以下行来定义新的场：

```
Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBala
Farm3=tango,Name:Farm3,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalanc
```

3. 通过添加以下行，为新的场分配用户组：

```
Farm2Groups=ussales.mycompany.com\SalesMgrs,ussales.mycompany.com\SalesTeam,finance.mycompany.
Farm3Groups=ussales.mycompany.com\SalesMgrs
```

[redacted] **Farm<*n*>** [redacted] **Farm<*n*>Groups** [redacted]

4. 通过添加以下行，确保用户可以继续访问现有场：

```
Farm1Groups=mycompany.com\DomainUsers
```

[redacted] Web Interface [redacted]

5. 使用文本编辑器在日本的 Web Interface 服务器上打开 WebInterface.conf 文件，并插入第 2 步和第 3 步中所示的行。 同时，确保为所有现有日语场分配用户组，以便本地用户可以继续访问这些场。

记录的消息和事件 ID

更新日期： 2014-11-25

Web Interface 会记录所有站点类型和平台的事件 ID。 在 Windows 操作系统中，可以使用事件查看器查看事件 ID，Citrix EdgeSight 或第三方监视和报告工具可以使用事件 ID。 在 Java 应用程序服务器中，事件 ID 包括在写入 Web 服务器日志文件的日志消息中。

下表显示了 Web Interface 事件 ID 和关联的日志消息， 还简要说明了一些问题及其解决方案建议。

事件 ID	消息	严重程度	说明
10001	出现配置解析错误：<错误说明>。	错误	站点配置文件出现问题。 检查 WebInterface.conf 以查看错误。
10002	出现配置加载错误。	错误	站点配置文件丢失或无法访问。 检查 WebInterface.conf 未被删除，并且已配置相应权限以允许读取此文件。
10003	无法检索 Citrix 联机插件配置。	错误	联机插件配置文件丢失或无法访问。 检查 config.xml 未被删除，并且已配置相应权限以允许读取此文件。
10004	已成功地重新加载配置数据。	信息	已验证并接受对站点配置文件 (WebInterface.conf) 或联机插件配置文件 (config.xml) 的最新更改。
10005	配置文件的以下项是重复的：<项名>。	警告	站点配置文件中有一个重复参数。请在 WebInterface.conf 中更正该错误。
10006	未知的身份验证点：<身份验证点>。	错误	在站点配置文件中为 AuthenticationPoint 参数指定了错误值。请在 WebInterface.conf 中更正该错误。
10007	启用用户漫游时不能使用匿名登录。	错误	XenDesktop 不支持匿名用户。要将用户漫游功能用于 XenDesktop，请禁用匿名身份验证。
10008	该配置无效：在此版本的 Web Interface 中，不支持 NDS 身份验证。	错误	重新配置此站点的身份验证方法，选择用户主体名称 (UPN) 或基于 Microsoft 域的身份验证。

10009	该配置无效：在此版本的 Web Interface 中，不支持智能卡和传递身份验证。	错误	如果使用 UNIX/JSP 版本的 Web Interface，并且使用设置了传递身份验证、智能卡身份验证或通过智能卡传递身份验证的 Web Interface 身份验证点，或者使用设置了智能卡身份验证或通过智能卡传递身份验证的 Access Gateway 身份验证点，则将显示此错误。
10010	双因素身份验证配置出现问题。	错误	检查是否已正确配置 Aladdin SafeWord for Citrix、RSA SecurID 或 RADIUS 服务器身份验证。
10011	当前没有可用的身份验证方法。	错误	检查是否已正确配置站点并且指定了一种或多种有效的身份验证方法。
10101	协议转换服务配置错误。 请确保 web.config 中定义了 tokenManager，并且它定义了一种或多种令牌服务。	错误	检查 XenApp Web 站点的 web.config 文件是否指定了具有关联证书引用的一个或多个令牌颁发机构，可通过这些证书引用来保证与 Access Gateway 中通过智能卡传递服务之间的信任关系。
10201	该配置无效：在此版本的 Web Interface 中，不支持 ICA 文件签名。	错误	必须运行 Web Interface 5.4 或更高版本，才能使用 ICA 文件签名。
10202	启用了旧版客户端支持时，无法使用 ICA 文件签名。	错误	要启用 ICA 文件签名，必须将站点配置为使用本机客户端，并且必须在 Webinterface.conf 文件中将 EnableLegacyIcaClientSupport 设置为 Off。
10203	对脱机应用程序不能使用 ICA 文件签名。	错误	检查站点是否配置为显示联机或双模式应用程序。
10204	必须允许用户选择本机客户端，以便使用 ICA 文件签名。	信息	要启用 ICA 文件签名，站点必须配置为使用本机客户端。
10205	尝试对 ICA 文件进行签名时出错：<错误消息>	错误	有关可能需要采取的任何措施的进一步详细信息，请参考错误消息中的信息。
10206	尝试对 ICA 文件进行签名时出错：<>。 请重新启动 Web 服务器，以确保启用 ICA 文件签名服务。	错误	重新启动 Web 服务器，并使用 Web Interface Management 控制台，以确保 ICA 文件签名已经启用。
11001	传递给客户端检测和下载过程的重定向 URL 无效。	错误	重定向 URL 指定用户在完成客户端检测和部署过程时定向到的 Web 页面。 此错误指示已在站点代码中修改了重定向 URL。

11002	客户端检测和部署过程不能部署任何已启用的客户端。 检查用户的浏览器、操作系统和访问方法是否与已启用的客户端兼容，这些客户端是否位于 XenApp Web 站点的 \Clients 文件夹中。	错误	用户无法从站点获取客户端。 检查是否已在 Web 服务器中提供并在站点中启用用于用户设备、操作系统、浏览器和访问方法的适当客户端。
11003	用户计算机中的操作系统不支持客户端检测和部署过程。	错误	由于客户端检测和部署过程无法识别用户设备中的操作系统，因此用户无法从站点获取客户端。
11004	由于缺少提供平台信息的用户-代理 HTTP 头，因此无法处理用户设备 <IP 地址> 上运行的浏览器所发出的请求。	错误	由于浏览器发出的请求不包含用于标识用户的浏览器和平台的用户-代理 HTTP 头，因此该用户无法访问站点。 请检查网络环境，确保未从用户请求中去除用户-代理头。
12001	Web Interface 阻止了 <number> 次使用此唯一事件 ID 记录消息的尝试。 报告率现已降低，Web Interface 将开始重新记录这些消息。	信息	使用 Citrix Web Interface Management 控制台中站点维护下的诊断日志记录任务，可以禁止重复记录重复事件，并配置记录的重复事件数量和记录频率。
12002	将阻止使用此唯一日志 ID 记录消息的进一步尝试，直至报告率降低为止。	信息	使用 Citrix Web Interface Management 控制台中站点维护下的诊断日志记录任务，可以禁止重复记录重复事件，并配置记录的重复事件数量和记录频率。
12003	无法加载事件 ID 文件。 在 <文件名> 中检查事件 ID 文件的路径是否正确。	警告	事件 ID 文件丢失或无法访问。 请检查 web.config（用于 IIS 中托管的站点）或 web.xml（用于 Java 应用程序服务器中托管的站点）中给定的路径是否正确。 此外，检查 WebInterfaceEventIds.txt 未被删除，并且已配置相应权限以允许读取此文件。
12004	消息项 <项名> 对应的事件 ID 无效。 检查事件 ID 文件中 <项名> 对应的项是否有效。 事件 ID 必须是介于 1 和 65535 之间的整数。	警告	在事件 ID 文件中找不到指定的事件 ID。 检查是否未从 WebInterfaceEventIds.txt 中删除此事件 ID。
13001	无法在 <服务器地址>:<端口> 建立与 Web 服务的 SSL 连接。 基础平台报告的消息为 <错误说明>。	错误	出现 SSL 错误，在错误消息末尾提供了该错误的特定详细信息。 检查 Web Interface 是否进行了正确配置，可通过 SSL 与 Access Gateway 或 Password Manager 集成。

13002	至少无法检索一个组的安全标识符。 检查 Citrix XML Service 是否可访问并支持用户漫游，配置文件中的组是否正确。	错误	为用户漫游功能配置的一个或多个用户组出现问题。 检查场中的所有服务器是否都在运行支持用户漫游功能的 XenApp 或 XenDesktop 版本。 此外，请检查指定的组名是否有效，是否可与 Citrix 服务器进行通信。
14001	RSA SecurID ACE/Agent 出现问题。 检查 ACE/Agent 是否已正确安装，aceclnt.dll 文件的路径是否已添加到 PATH 环境变量中。	错误	要将 SecurID 身份验证与 Microsoft Internet Information Services 的 Web Interface 结合使用，必须在安装 RSA Authentication Agent for Web for Internet Information Services 之后安装 Web Interface。
14002	RSA SecurID ACE/Agent 出现问题。 检查是否安装了 ACE/Agent 的正确版本。	错误	检查是否在 Web 服务器上安装了受支持的 RSA Authentication Agent for Web for Internet Information Services 版本。
14003	Aladdin SafeWord Agent 出现问题。 检查 Agent 是否已正确安装。	错误	检查是否已将 Web Interface 的 SafeWord Agent 安装到 Web 服务器上。 必须在安装 SafeWord Agent 之前安装 Web Interface。
14004	无法更新 RSA SecurID ACE/Agent 缓存的密码。 检查 RSA SecurID ACE/Agent 和 ACE/Server 版本是否兼容，ACE/Agent 和 ACE/Server 是否都配置为使用 Windows 密码集成。	错误	检查 RSA Authentication Manager 和 RSA Authentication Agent for Web for Internet Information Services 版本是否兼容。 此外，检查是否已配置 RSA Authentication Manager 数据库系统参数，以在系统级别启用 Windows 密码集成。
14005	无法获取 RSA SecurID ACE/Agent 缓存的密码。 检查 RSA SecurID ACE/Agent 和 ACE/Server 版本是否兼容，ACE/Agent 和 ACE/Server 是否都配置为使用 Windows 密码集成。	错误	检查 RSA Authentication Manager 和 RSA Authentication Agent for Web for Internet Information Services 版本是否兼容。 此外，检查是否已配置 RSA Authentication Manager 数据库系统参数，以在系统级别启用 Windows 密码集成。
14006	验证用户身份时，SafeWord 身份验证程序出现问题。	错误	SafeWord 服务器出现问题。 有关详细信息，请参阅 SafeWord 服务器上的日志文件。
14007	RSA SecurID ACE/Agent 出现问题。 请检查是否已针对 32 位或 64 位应用程序配置了适合于所安装 ACE/Agent 版本的 Web Interface 应用程序池。	错误	检查所运行 ACE/Agent 版本的应用程序要求。

15001	从 <文件路径> 读取客户端版本时出现问题。 系统将不会提示用户升级到此客户端的较新版本。	错误	检查是否已配置相应权限以允许读取指定客户端安装程序文件。
15002	读取语言包文件 <文件名> 时出现问题。 请检查该文件是否可访问，以及所用格式是否正确。	错误	检查指定的文件未被删除，并且已配置相应权限以允许读取此文件。
15003	无法访问目录 <目录名称>。 无法将此目录内的客户端提供给用户使用。 请确保网络服务帐户具有相应权限，可以访问该目录，然后重新启动 Web 服务器。	错误	检查指定的目录未被删除，并且已配置相应权限以允许访问此目录。
15004	读取语言包文件 <文件名> 时出现问题。 文件中缺少版本声明，因此无法使用语言包。	错误	语言包文件中没有版本号。 请在指定文件中更正该错误。
15005	读取语言包文件 <文件名> 时出现问题。 该语言包版本为 <版本号>，它与 Web Interface 的当前版本不兼容。	错误	Web Interface 和语言包文件的版本不匹配。 语言包特定于随其一起提供的 Web Interface 版本，而不能用于较低或较高版本。 根据需要升级或恢复指定文件。
15006	找不到用于默认区域设置 <安装区域设置> 的语言包。 找到语言包 <文件名>，会将它用作默认语言包。	警告	当 Web Interface 找不到用于在安装期间选择的区域设置的语言包时，Web Interface 将回退到第一个可用的兼容语言包。
16001	无法读取 RADIUS 机密文件 <文件路径>。	错误	RADIUS 机密文件丢失或无法访问。 请检查 web.config（用于 IIS 中托管的站点）或 web.xml（用于 Java 应用程序服务器中托管的站点）中给定的路径是否正确。 此外，检查 RADIUS 机密文件未被删除，并且已配置相应权限以允许读取此文件。
16002	RADIUS 机密文件 <文件路径> 为空。	错误	RADIUS 协议需要使用共享机密，共享机密是仅对 RADIUS 客户端 (Web Interface) 和用于验证该客户端身份的 RADIUS 服务器可用的数据。 RADIUS 机密文件可以包含任意字符串，但不得为空。
16003	验证用户身份时，RADIUS 身份验证程序出现问题。	错误	RADIUS 服务器出现问题。 有关详细信息，请参阅 RADIUS 服务器上的日志文件。

16004	站点的 Web 配置文件中必须存在 RADIUS_NAS_IDENTIFIER 和/或 RADIUS_IP_ADDRESS 值。 RADIUS_NAS_IDENTIFIER 值必须至少包含 3 个字符。 RADIUS_IP_ADDRESS 必须是有效的 IP 地址。	错误	RADIUS 协议要求对 RADIUS 服务器的访问请求包括 RADIUS 客户端 (Web Interface) 的 IP 地址或其他标识符。 请检查 web.config（用于 IIS 中托管的站点）或 web.xml（用于 Java 应用程序服务器中托管的站点）中是否包含有效的 RADIUS NAS 标识符或 IP 地址。
17001	在服务器 <服务器地址>:<异常> 上，上下文查找失败。 已将此服务器暂时从活动服务器列表中删除。	错误	指定的 NDS 服务器出现问题。 将绕过此服务器，直至问题得以解决。 有关详细信息，请参阅 NDS 服务器上的日志文件。
17002	所有 NDS 服务器均出现故障，所以无法进行上下文查找。 请尝试使用完全限定的用户名登录，即 username.mycompany.com。	错误	无法访问任何 NDS 服务器。 请尝试以 .username.mycompany.com 形式输入凭据。 有关详细信息，请参阅 NDS 服务器上的日志文件。
18001	尝试访问 <URL> 处的高级访问控制身份验证服务时，出现通信错误。 请检查该身份验证服务是否正在运行。 基础平台报告的消息为 <错误说明>。	错误	访问 Access Gateway 身份验证服务时出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Access Gateway 设备上的日志文件。
18002	尝试在 <URL> 处使用 Access Gateway 身份验证服务关闭会话时，发生通信错误。 请检查该身份验证服务是否正在运行。 基础平台报告的消息为 <错误说明>。	错误	访问 Access Gateway 身份验证服务时出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Access Gateway 设备上的日志文件。
18003	Access Gateway 身份验证服务对用户的身份验证失败。 该服务报告的消息为 <错误说明> [状态代码:<代码号>]。	错误	Access Gateway 身份验证服务出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Access Gateway 设备上的日志文件。
18004	Access Gateway 身份验证服务无法关闭会话。 该服务报告的消息为 <错误说明> [状态代码:<代码号>]。	错误	Access Gateway 身份验证服务出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Access Gateway 设备上的日志文件。
18005	站点配置中的 Access Gateway 身份验证服务 URL 无效：<URL>。	错误	在站点配置文件中为 AGEWebServiceURL 参数指定了无效 URL。 请在 WebInterface.conf 中更正该错误。
18006	用户 <用户名> 无法登录站点：<站点名称>。 请重新启动 Web 服务器，以确保来自 Access Gateway 服务的通过智能卡传递已启用。	错误	智能卡用户无法登录到 Access Gateway 集成站点。 请重新启动 Web 服务器，以确保 Access Gateway 中通过智能卡传递服务正在运行。

18007	此版本的 Access Gateway 不支持 Web Interface 更改密码功能。 要使用户能够更改自己的密码，您必须升级到支持此功能的 Access Gateway 版本。	错误	如果在您的站点启用了更改密码功能，但您使用的 Access Gateway 版本不支持此功能，则将发生此错误。 应禁用密码更改功能或将 Access Gateway 升级到支持此功能的版本。
19001	断开用户资源的连接时出错。 未启用工作区控制，用户是匿名的，或者检索用户的凭据或客户端名称时出错。	错误	工作区控制出现问题。 请检查是否为站点启用了工作区控制，以及用户是否已使用匿名身份验证之外的身份验证方法登录。
19002	重新连接用户资源时出错。 未启用工作区控制，用户是匿名的，或者检索用户的凭据或客户端名称时出错。	错误	工作区控制出现问题。 请检查是否为站点启用了工作区控制，以及用户是否已使用匿名身份验证之外的身份验证方法登录。
20001	尝试访问 <URL> 处的 Password Manager Service 时，出现通信错误。 请检查该服务是否正在运行。 基础平台报告的消息为 <错误说明>。	错误	访问 Password Manager Service 时出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Password Manager 服务器上的日志文件。
20002	站点配置中的 Password Manager Service URL 无效：<URL>。	错误	在站点配置文件中为 AccountSelfServiceUrl 参数指定了无效 URL。 请在 WebInterface.conf 中更正该错误。
21001	出现严重的服务器错误。	错误	在 Web 页面中运行的脚本之一出现了 Java 异常。 请尝试重新加载该页面。 或者，使用 Citrix Web Interface Management 控制台中站点维护下的修复站点任务重新安装站点的脚本。
21002	严重的服务器错误：<.NET 错误说明>。	错误	在 Web 页面中运行的脚本之一出现了 .NET 异常。 请尝试重新加载该页面。 或者，使用 Citrix Web Interface Management 控制台中站点维护下的修复站点任务重新安装站点的脚本。
21003	由于出现错误，无法在路径 <站点配置目录> 处创建文件监视器。	错误	请检查站点配置文件夹的路径是否正确，以及是否已配置相应权限以允许读取此目录。 或者，尝试重新启动 IIS，以用最新配置更改来更新站点。
21004	用户无法访问站点，因为 Web 服务器的完全限定域名包含下划线 (_)。 请重命名 Web 服务器和/或域，删除下划线。 如果不能进行重命名，请为 Web 服务器配置不含下划线的备用地址，或指示用户使用 Web 服务器的 IP 地址访问站点。	错误	如果站点名称中包含无法识别的字符（例如下划线），则无法访问站点。 请检查确认 Web 服务器名中不包含下划线，如果需要更改服务器名，请使用 Web Interface Management 控制台。

21005	类 ID 为 <ID 号> 的 Citrix 联机插件 ActiveX 控件无法启动。 请检查是否已在站点配置文件中指定正确的类 ID。	错误	检查 ActiveX 类 ID 与 Webinterface.conf 文件中的 ID 号是否匹配。
21006	类 ID 为 <ID 号> 的 Citrix 联机插件 ActiveX 控件无法启动。 请检查是否已在站点配置文件中指定正确的类 ID。	错误	检查 ActiveX 类 ID 与 Webinterface.conf 文件中的 ID 号是否匹配。
22001	在服务器上找不到 Java 客户端文件。 检查 XenApp Web 站点的 \Clients 文件夹中是否提供了这些文件。	错误	Java 客户端软件包丢失或无法访问。 检查这些文件未被删除，并且已配置相应权限以允许读取这些文件。
23001	尝试访问用户 <用户名> 的桌面时出现 ICA 错误。	错误	Citrix 联机插件无法访问用户的桌面。 请检查该桌面是否正在运行并且可以访问。
23002	用户 <用户名> 无法通过 Internet Explorer 访问桌面。 请检查用户的设备上是否已安装 Citrix Desktop Appliance Lock，Desktop Appliance Connector 是否已添加到 Internet Explorer 中相应的 Windows 安全区域。	错误	桌面设备用户无法访问“仅全屏模式”桌面。 检查用户设备中是否已正确安装并配置了 Citrix 联机插件。
23003	已授权用户 <用户名> 访问 <number> 个桌面。 对于通过 Desktop Appliance Connector 访问“仅全屏模式”桌面的用户，永远只应允许他们访问一个桌面。	警告	已为桌面设备用户提供多个桌面。该用户可以访问桌面。 但是，由于无法选择所需桌面，用户下次登录时可能无法连接至同一桌面。 配置 Desktop Appliance Connector 以便只允许用户访问一个桌面。
23004	指定的身份验证方法无效。 您必须指定“显式”或“证书”两者之一，但不能这两种方法都指定。	错误	在站点配置文件中同时为 WIAuthenticationMethods 参数指定了显式和证书值。 同一 Desktop Appliance Connector 不能既启用显式身份验证又启用智能卡身份验证。 请在 WebInterface.conf 中更正该错误。
23005	嵌入式智能卡 SSO 身份验证配置无效。 身份验证方法必须包括“证书”。	错误	对于 Desktop Appliance Connector，站点配置文件中的 WIAuthenticationMethods 参数必须指定证书值。 请在 WebInterface.conf 中更正该错误。
23006	指定的身份验证方法无效。 不支持身份验证方法的这种组合。	错误	在站点配置文件 WIAuthenticationMethods 参数中指定的 Desktop Appliance Connector 身份验证方法不能一起使用。 请在 WebInterface.conf 中更正该错误。

24001	未经身份验证的用户进行了登录尝试。 验证是否为系统的所有预期用户创建了影子帐户。 如果该问题持续存在，请尝试使用 Access Management Console 修复该站点。	错误	AD FS 集成站点出现问题。 无法验证用户的身份。 检查是否为资源合作伙伴域中的用户创建了影子帐户。 或者，使用 Citrix Web Interface Management 控制台中站点维护下的修复站点任务重新安装站点。
24002	未经身份验证的用户进行了登录尝试。 如果该问题持续存在，请尝试使用 Access Management Console 修复该站点。	错误	XenApp Web 或 XenApp Services 站点出现问题。 无法验证用户的身份。 请检查是否已在该域中为用户创建用户帐户。 或者，使用 Citrix Web Interface Management 控制台中站点维护下的修复站点任务重新安装站点。
30001	尝试从 Citrix 服务器读取信息时出错：〈场名〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30002	尝试将信息写入 Citrix 服务器时出错：〈场名〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30003	尝试通过端口 〈端口〉 连接到服务器 〈服务器地址〉 时出错。 请验证 Citrix XML Service 是否正在运行并且正在使用正确的端口。 如果 XML Service 配置为与 Microsoft Internet Information Services (IIS) 共享端口，请验证 IIS 是否正在运行。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查 XML Service 是否已配置为与 IIS 共享 TCP/IP 端口，如果是这样，请检查 IIS 是否正在运行。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30004	无法解析服务器名称 〈服务器地址〉。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30005	Citrix 服务器发送的 HTTP 语法不正确。 请验证当前的 Web Interface 版本是否与所使用的服务器兼容。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查服务器场是否正在运行 XenDesktop 或 Presentation Server 4.5 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30006	Citrix 服务器发送了不正确或意外的响应。 请验证当前的 Web Interface 版本是否与所使用的服务器兼容。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查服务器场是否正在运行 XenDesktop 或 Presentation Server 4.5 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30008	Citrix 服务器意外地关闭了连接。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30009	Citrix 服务器发送的 HTTP 头指出发生了错误：<详细信息>。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30010	Citrix 服务器此时无法处理请求。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30011	尝试完成请求时 Citrix 服务器上发生错误：<详细信息>。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30012	Citrix 服务器遇到版本不匹配错误。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30013	Citrix 服务器收到错误的请求。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30014	分析请求时 Citrix 服务器上发生错误。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30015	位于地址 <文件路径> 的 Citrix XML Service 无法处理请求。	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30016	找不到 Citrix XML Service 对象：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30017	不支持 Citrix XML Service 方法：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30018	无法接受 Citrix XML Service 响应：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30019	需要 Citrix XML Service 请求长度：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30020	Citrix XML Service 请求太短：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30021	Citrix XML Service 请求超出最大大小：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30022	Citrix XML Service 或 Citrix 服务器可能不可用或暂时过载：〈详细信息〉。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30023	无法处理 Citrix 服务器发送的 XML 文档。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30024	无法处理 Citrix 服务器发送的 XML 文档，因为其中包含无效的 XML。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。 〈错误说明〉	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30025	尝试从 Citrix 服务器读取信息时出错：<场名>。 此错误可能是尝试与 SSL Relay 的替代项通信而引起的。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 要对服务器场的连接使用 SSL/TLS 加密，必须使用 SSL Relay 在每台服务器上配置支持。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30026	尝试与 SSL Relay 进行连接时出错：<服务器地址>:<端口>。 请验证 SSL Relay 是否正在运行并且正在侦听有效的端口。 SSL Relay 所配置的要联系的服务器证书中包含的名称必须与尝试连接的服务器名称完全相同。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查 SSL Relay 是否正在运行并且正在侦听适当的端口（通常为端口 443），SSL Relay 服务器证书是否包含尝试与其连接的服务器的完全限定名称（大小写正确）。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30027	一个或多个 Citrix 服务器可能不支持票据记录。 要使用此功能，您必须升级运行 XML Service 的服务器，或禁用票据记录。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查场中的所有服务器是否都在运行 XenDesktop 或 MetaFrame XP 1.0 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30028	无法解析 SSL Relay <服务器地址> 的名称。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30029	无法建立 SSL 连接：<SSL 错误说明>。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30030	无法建立 SSL Relay 连接：<SSL 错误说明>。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30031	位于地址 <文件路径> 的 Citrix XML Service 不支持功能 <功能名称>。	错误	检查场中的所有服务器是否都在运行支持指定功能的 XenApp 或 XenDesktop 版本。 有关详细信息，请参阅最低软件要求。
30101	更改密码尝试失败。	错误	出于安全考虑，用户不能更改 Windows 密码。 有关详细信息，请参阅 Citrix 服务器和/或域控制器上的日志文件。

30102	Citrix 服务器报告位于地址 <文件路径> 的 XML Service 发生了未指定的错误。	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30103	Citrix 服务器报告找不到替代地址。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30104	连接到 Citrix 服务器以访问资源时出错。 请验证服务器是否正在运行并且网络正常。 此错误由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 请检查服务器场和网络是否存在问题。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30105	Citrix 服务器不信任该服务器。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	检查 Web Interface 服务器与 Citrix XML Service 之间是否存在信任关系。 有关详细信息，请参阅对 XenApp Web 站点使用工作区控制和集成身份验证方法。
30106	Citrix 服务器未获许可，无法支持请求的操作。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 请检查 Citrix 许可证服务器是否正在运行并且可以访问。 Citrix 建议您将许可证服务器升级到最新版本，以确保与最新产品兼容。 有关详细信息，请参阅 Citrix 服务器和/或许可证服务器上的日志文件。
30107	Citrix 服务器报告它们太忙，无法提供对选定资源的访问。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 请检查该服务器场是否过载。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30108	票据记录功能已在 Citrix 服务器上禁用。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查场中的所有服务器是否都在使用同一端口与 XML Service 通信。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30109	位于地址 <文件路径> 的 Citrix XML Service 报告了注册错误。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30110	位于地址 <文件路径> 的 Citrix XML Service 报告了 <错误类型> 类型的错误（错误 ID 为 <错误 ID>）。 服务器的事件日志中可能包含更多信息，视运行 XML Service 的服务器而定。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30111	Citrix 服务器不支持指定的地址类型。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30112	访问桌面组 <组名> 时未找到可供用户 <用户名> 使用的资源。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查是否已将用户分配给指定桌面组，组中是否存在未使用的桌面。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30113	处理用户 <用户名> 的桌面组 <组名> 初始化时，拒绝了 Citrix 服务器准备建立连接的请求。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30114	拒绝了 Citrix 服务器检索用户的安全标识符的访问。 请授予 XML Service 对 Active Directory 中 Token-Groups-Global-And-Universal 属性的读取权限，或禁用 XML Service 中的安全标识符枚举功能。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 如果 XML Service 配置为枚举用户的安全标识符，请检查是否已在 Active Directory 中授予适当权限。 有关详细信息，请参阅 CTX117489 和 Citrix 服务器上的日志文件。
30115	Citrix 服务器无法检索用户的安全标识符。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 CTX117489 和 Citrix 服务器上的日志文件。
30116	初始化桌面组 <组名> 时，无法为用户 <用户名> 连接到处于维护模式的桌面。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查用户的桌面是否尚未置于维护模式。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30117	Citrix 服务器不支持桌面重新启动操作。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查服务器场是否正在运行 XenDesktop 3.0 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30118	Citrix 服务器在等待针对用户 <用户名> 关闭桌面组 <组名> 中的计算机时超时。 此消息由位于地址 <文件路径> 的 XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30119	无法针对用户 <用户名> 关闭桌面组 <组名> 中处于维护模式的计算机。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查用户的桌面是否尚未置于维护模式。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30120	找不到用户 <用户名>。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。 <错误说明>	错误	Citrix XML Service 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30201	无效的 Secure Ticket Authority 地址：<URL>。 <错误说明>	错误	在站点配置文件中为 CSG_STA_URL<n> 参数指定了无效 URL。 请在 WebInterface.conf 中更正该错误。
30202	Secure Ticket Authority <URL> 不支持版本 4 请求。 所有 Secure Ticket Authority 通信现在都会回退至版本 1。 通过 Secure Gateway 的新连接不会使用会话可靠性。	错误	正在使用的 Secure Gateway 版本不支持 Secure Ticket Authority 冗余功能。 因此，已禁用此功能。
30203	Secure Ticket Authority <URL> 返回一个具有意外认证机构或类型的票据 - <错误类型>、<错误 ID>、<SSL 错误说明>、<详细信息>。 <错误说明>	错误	Secure Ticket Authority 出现问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30204	无法联系指定的 Secure Ticket Authority，已暂时从活动服务列表中删除此服务。	错误	Secure Ticket Authority 出现问题。 将绕过此服务，直至问题得以解决。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
30205	所有已配置的 Secure Ticket Authority 都无法响应此 XML 事务。	错误	无法联系任何 Secure Ticket Authority。 请尝试重新启动 Web 服务器。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

30301	HTTP 响应指示基础连接已关闭。	错误	检查服务器场是否正在运行 XenDesktop 或 Presentation Server 4.5 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。
30401	事务层已强制破坏套接字。	错误	检查场数据存储是否有损坏的应用程序。 有关详细信息，请参阅 CTX114769。
31001	无法联系指定的 Citrix XML Service，已暂时从活动服务列表中删除此服务。	错误	Citrix XML Service 出现问题。将绕过此服务器，直至问题得以解决。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31002	此 XML Service 事务失败，但尚未将 XML Service 从活动服务列表中删除。	错误	虽然可以访问 Citrix XML Service，但无法完成请求或指令。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31003	为场 〈场名〉 配置的所有 Citrix XML Service 都无法响应此 XML Service 事务。	错误	无法联系用于所指定场的任何 Citrix XML Service 主机。 请尝试重新启动 Web 服务器。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31004	无法将 XML 协议错误 〈错误 ID〉 转换为访问状态错误。	错误	检查用户是否拥有 Citrix 服务器的 Active Directory 登录权限。
31005	已忽略 〈number〉 个资源（共 〈number〉 个），因为这些资源无效。	错误	Citrix XML Service 无法枚举所有可用资源。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31006	由于用户 〈用户名〉 未获许可，因此拒绝其登录。	错误	由于没有可用的 Citrix 许可证或 Microsoft 远程桌面服务客户端访问许可证，用户无法登录。请检查 Citrix 许可证服务器是否正在运行并且可以访问。 Citrix 建议您将许可证服务器升级到最新版本，以确保与最新产品兼容。 有关详细信息，请参阅 Citrix 服务器和/或许可证服务器上的日志文件。
31007	Citrix 服务器未获许可，无法支持工作区控制。 此消息由位于地址 〈文件路径〉 的 XML Service 报告。	错误	检查 Citrix 许可证是否启用了包括工作区控制功能的产品版本。此外，请检查 Citrix 许可证服务器是否正在运行并且可以访问。 Citrix 建议您将许可证服务器升级到最新版本，以确保与最新产品兼容。 有关详细信息，请参阅 Citrix 服务器和/或许可证服务器上的日志文件。

31008	Citrix 服务器未获许可，无法启动资源 <资源名称>。 此消息由位于地址 <文件路径> 的 XML Service 报告。	错误	检查 Citrix 许可证是否启用了包括此类型资源的产品版本。 此外，请检查 Citrix 许可证服务器是否正在运行并且可以访问。 Citrix 建议您将许可证服务器升级到最新版本，以确保与最新产品兼容。 有关详细信息，请参阅 Citrix 服务器和/或许可证服务器上的日志文件。
31009	无法检索以下帐户的帐户数据：<帐户名列表> 检查该名称拼写是否正确。 此消息由位于地址 <文件路径> 的 Citrix XML Service 报告。	错误	Citrix XML Service 无法访问指定帐户。 检查这些帐户未被删除，并且已配置相应权限以允许 XML Service 读取这些帐户。 此外，请检查输入的帐户名是否正确。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31101	用户 <用户名> 具有服务器会话 <会话 ID>，但没有权限访问创建该会话的资源 <资源名称>。 因此，用户无法访问此会话。	错误	用户的访问权限已更改，但用户的会话仍处于活动状态。 请重置会话。 注意，此操作将导致用户数据丢失。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31201	已将场 <场名> 配置为使用票据记录，但未收到任何票据标记。 请检查该场是否支持票据记录。	错误	检查所指定场中的所有服务器是否都在运行 XenDesktop 或 MetaFrame XP 1.0 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
31202	用户尝试启动当前已禁用的资源 <资源名称>。	错误	检查托管指定资源的服务器上是否启用了该资源。
31203	已将场 <场名> 配置为使用启动引用，但 Citrix XML Service 中未收到启动引用。 检查该场是否支持启动引用或禁用启动引用请求。	错误	要使用启动引用，所指定场中的所有服务器都必须运行 XenDesktop 或 Presentation Server 4.5 或更高版本。 Citrix 建议场中的所有服务器都运行同一产品和版本。 如果场正在运行适用于 UNIX 的 XenApp 4.0 Feature Pack 1 或 Presentation Server 4.0 及更低版本，确保在 XenApp Web 站点配置文件 WebInterface.conf 中将 RequireLaunchReference 参数设置为 Off，将 OverrideIcaClientname 设置为 On。
31301	场 <场名> 的配置无效。	错误	指定的服务器场出现问题。 有关详细信息，请参阅 Citrix 服务器上的日志文件。

32001	配置不包括任何 Citrix 服务器的详细信息。	错误	在 XenApp Services 站点配置文件中没有为 Farm<n> 参数指定任何场。 请在 WebInterface.conf 中更正该错误。
32002	无法分析提供程序链配置。	错误	XenApp Services 站点出现问题。检查站点配置文件以查看错误。
32003	<错误原因> 发生以下系统错误：<错误说明>	错误	XenApp Services 站点出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查站点配置文件以查看错误。
33001	Citrix Streaming Service：无法联系指定的 Citrix XML Service，已暂时从活动服务列表中删除此服务。	错误	Citrix 脱机插件遇到 Citrix XML Service 问题。 将绕过此服务，直至问题得以解决。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
33002	Citrix Streaming Service：此 Citrix XML Service 事务失败，但尚未将 XML Service 从活动服务列表中删除。	错误	虽然 Citrix 脱机插件可以访问 Citrix XML Service，但无法完成请求或指令。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
33003	Citrix Streaming Service：为场 <场名> 配置的所有 Citrix XML Service 都无法响应此 XML Service 事务。	错误	Citrix 脱机插件无法联系用于所指定场的任何 Citrix XML Service 主机。 请尝试重新启动 Web 服务器。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
33004	Citrix Streaming Service：场 <场名> 的配置无效。	错误	Citrix 脱机插件遇到指定的服务器场出现问题。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
33005	Citrix Streaming Service：配置不包括任何 Citrix 服务器的详细信息。	错误	在站点配置文件中没有为 Farm<n> 参数指定任何场。 请在 WebInterface.conf 中更正该错误。
33006	无法加载配置文件 RadeValidationRules.conf。 检查是否可从站点配置文件夹中获取该文件。	错误	配置文件 RadeValidationRules.conf 丢失或无法访问。 检查该文件未被删除，并且已配置相应权限以允许读取此文件。
33007	由于配置文件 RadeValidationRules.conf 包含无效规则，因此无法使用该文件。 检查所有规则是否都使用有效的正则表达式语法。	错误	配置文件 RadeValidationRules.conf 出现问题。 应使用正则表达式语法给定此文件中的所有规则。 检查该文件以查看错误。或者，使用 Citrix Web Interface Management 控制台中站点维护下的修复站点任务重新安装站点。 将放弃您对文件进行的任何更改。

34001	配置不包括任何 Citrix 服务器的详细信息。	错误	在 Desktop Appliance Connector 或 XenApp Web 站点配置文件中没有为 Farm<n> 参数指定任何场。 请在 WebInterface.conf 中更正该错误。
34002	无法分析提供程序链配置。	错误	Desktop Appliance Connector 或 XenApp Web 站点出现问题。检查 WebInterface.conf 以查看错误。
34003	<错误原因> 发生以下系统错误：<错误说明>	错误	XenApp Services 站点出现问题，在错误消息末尾提供了该问题的特定详细信息。 检查 WebInterface.conf 以查看错误。
40001	枚举用户资源时出错。 从用户设备中收到无法识别的 XML 消息。	错误	在连接到 Citrix 服务器时，Citrix 联机插件遇到问题。 检查用户设备中是否已正确配置了 Citrix 联机插件。
40002	枚举用户资源时出错。 从用户设备中收到无法识别的 XML 消息。	错误	在连接到 Citrix 服务器时，Citrix 联机插件遇到问题。 检查用户设备中是否已正确配置了 Citrix 联机插件。
40003	重新连接用户资源时出错。 从用户设备中收到无法识别的 XML 消息。	错误	在重新连接到 Citrix 服务器时，Citrix 联机插件遇到问题。检查用户设备中是否已正确配置了 Citrix 联机插件。
40004	<IP 地址> 请求 Citrix 联机插件配置 <文件名>，该配置文件不存在。	错误	在用户设备中检查是否在 Citrix 联机插件的选项对话框中正确输入了配置文件 URL。
40005	启动用户资源时出错：<错误说明>	错误	Citrix 联机插件遇到问题，在错误消息末尾提供了该问题的特定详细信息。 有关详细信息，请参阅 Citrix 服务器上的日志文件。
40006	执行桌面控制操作时出错。 从用户设备中收到无法识别的 XML 消息。	错误	在重新启动用户桌面时，Citrix 联机插件遇到问题。 检查用户设备中是否已正确配置了 Citrix 联机插件。

禁用错误消息

在 IIS 上，您可以禁用 Web Interface 提供的错误消息并显示出现的底层错误。 为此，请编辑位于站点的根目录中的 web.config 文件。 将以下行：

<customErrors mode="On" defaultRedirect="~/html/serverError.html">

更改为：

<customErrors mode="Off" defaultRedirect="~/html/serverError.html">

此外，还可以显示您自定义的错误消息。 为此，请将该行更改为：

<customErrors mode="On" defaultRedirect="~/html/CustomErrorPage">

其中，CustomErrorPage 是自定义错误页的文件名。

配置对 Web Interface 的 AD FS 支持

更新日期： 2014-11-24

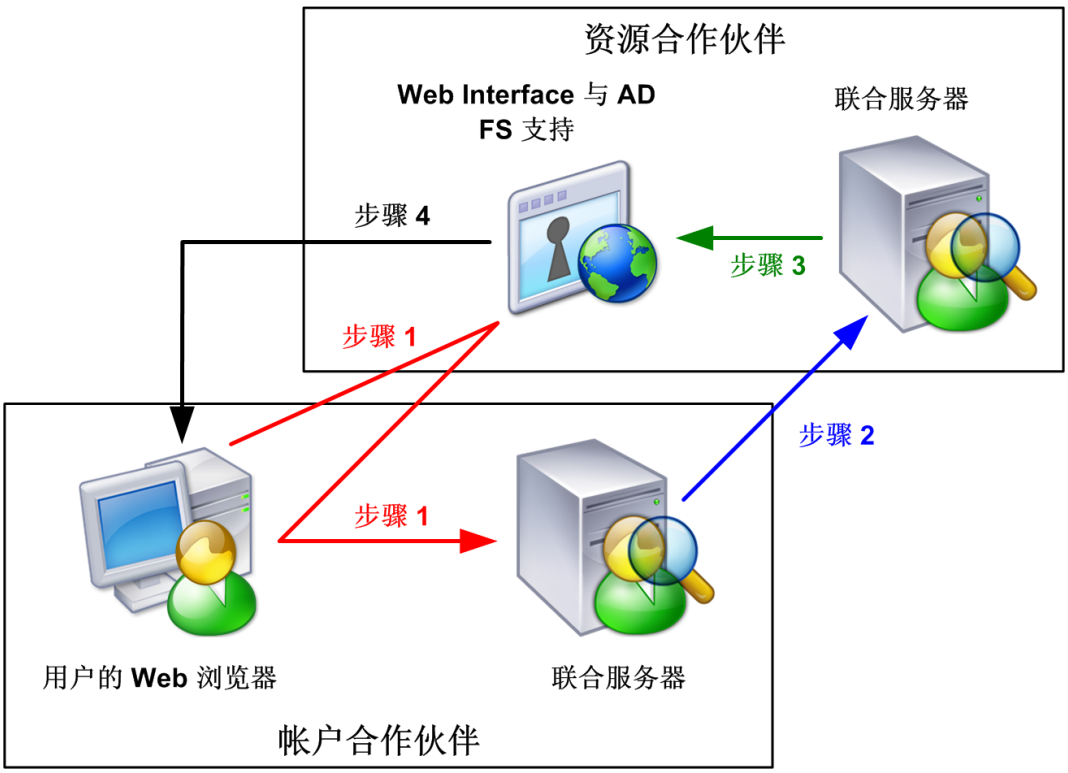
通过面向 Web Interface 的 Microsoft Active Directory 联合身份验证服务支持，AD FS 部署的资源合作伙伴可以使用 XenApp。 管理员可以创建 AD FS 站点，以便为用户提供对资源合作伙伴上的应用程序和内容的访问权限。

重要：AD FS 要求在 Web 浏览器、Web 服务器和联合服务器之间进行安全通信。 Web Interface 用户必须使用 HTTPS/SSL 才能访问该站点。

Active Directory 联合身份验证服务集成站点的工作方式

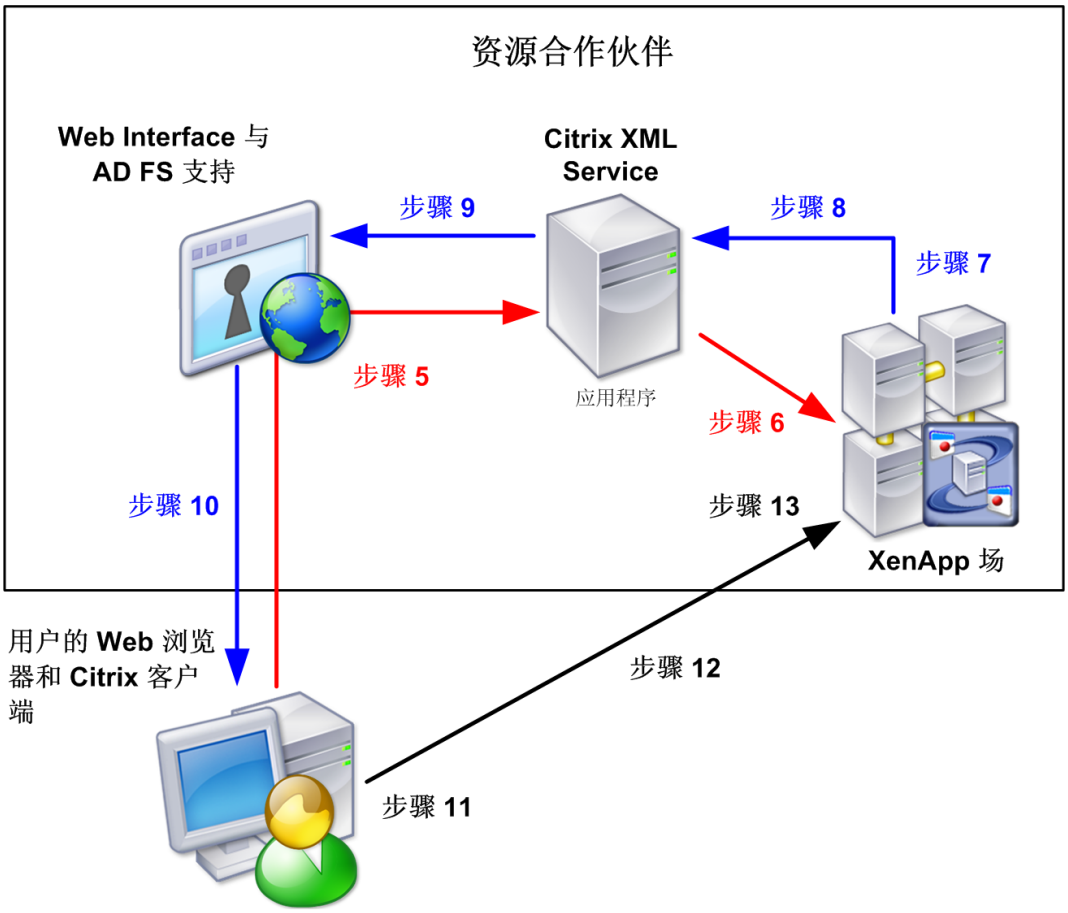
当帐户合作伙伴的用户访问资源合作伙伴的应用程序时，将执行以下步骤：

- 步骤 1： 打开资源合作伙伴的 Web Interface 主页的用户被重定向到帐户合作伙伴的身份验证页。
- 步骤 2： 帐户合作伙伴对该用户进行身份验证，并将安全令牌发回到资源合作伙伴。
- 步骤 3： 资源合作伙伴上的 AD FS 验证安全令牌，将其转换为 Windows 标识（代表影子帐户），然后将该用户重定向到 Web Interface 登录屏幕。
-



步骤 4： Web Interface 显示该用户的应用程序集。 下图显示了来自帐户合作伙伴域的用户进行登录以访问其应用程序集时所执行的步骤。

- 步骤 5： 用户通过单击页面上的超链接访问应用程序。 Web Interface 联系 Citrix XML Service 以请求访问。
- 步骤 6： Citrix XML Service 生成安全支持提供程序接口数据，并将其发送至 XenApp 服务器。
- 步骤 7： 该服务器使用安全支持提供程序接口数据对用户进行身份验证，并存储一个登录令牌以供将来验证身份。
- 步骤 8： 该服务器生成启动票据来唯一地代表所存储的登录令牌，并将此票据返回至 Citrix XML Service。
- 步骤 9： Citrix XML Service 将启动票据返回至 Web Interface。
- 步骤 10： Web Interface 创建一个包含启动票据的 .ica 文件，并将其发送至用户的 Web 浏览器。
- 步骤 11： 用户设备打开此 .ica 文件，并尝试与该服务器建立 ICA 连接。
- 步骤 12： Citrix 客户端将启动票据发送至 XenApp 服务器。
-



步
骤

13： 该服务器接收启动票据，并将其与先前生成的登录令牌相匹配，然后使用此登录令牌将用户登录到该服务器上的 ICA 会话。 ICA 会话使用影子帐户的标识运行。下图显示了来自帐户合作伙伴域的用户访问应用程序时所执行的步骤。

当用户注销时，他们将从 Web Interface 注销，或者从 Web Interface 和 AD FS 注销，具体取决于为站点配置的设置。 如果从 Web Interface 和 AD FS 注销，则用户也会从所有 AD FS 应用程序注销。

创建 Active Directory 联合身份验证服务站点之前

创建 AD FS 站点之前，必须执行以下步骤。 忽略其中的任何步骤都可能意味着您无法创建站点。

- 将帐户合作伙伴联合服务器和资源合作伙伴联合服务器上的时钟同步为彼此相差时间在五分钟之内。 否则，资源合作伙伴可能无法接受帐户合作伙伴生成的安全令牌，因为这些令牌似乎已过期。 要避免此问题，两个组织必须将其服务器与同一 Internet 时间服务器同步。 有关详细信息，请参阅设置域之间的关系。
- 确保资源合作伙伴联合服务器和 Web 服务器能够访问证书颁发机构的证书吊销列表 (CRL)。 如果这些服务器不能确保证书不被吊销，则 AD FS 可能会失败。 有关详细信息，请参阅设置域之间的关系。
- 确保部署中的所有服务器都可信任以便进行委派。 有关详细信息，请参阅为部署中的服务器配置委派。
- 在资源合作伙伴域中为可通过 AD FS 针对 Web Interface 进行身份验证的每一外部用户设置影子帐户。 有关详细信息，请参阅设置影子帐户。
- 安装 XenApp，确保 Citrix XML Service 设置为与 IIS 共享其端口，并确保 IIS 配置为支持 HTTPS。
- 在 Web Interface 服务器和场中运行 Citrix XML Service 并且 Web Interface 将与之联系的任何其他服务器之间建立信任关系。 有关详细信息，请参阅对 XenApp Web 站点使用工作区控制和集成身份验证方法。

重要：本节不介绍如何安装 AD FS。 在尝试创建 AD FS 站点之前，您必须具有有效的 AD FS 安装，并且外部帐户用户能够访问资源合作伙伴中启用了 AD FS 的应用程序。

Active Directory 联合身份验证服务的软件要求

必须在您的环境中安装并配置以下软件：

- 适用于联合服务器和 Web 服务器的 Windows Server 2008 或 Windows Server 2003 R2。对于 Web 服务器，仅支持 32 位版本的 Windows Server 2008 和 Windows Server 2003 R2。
- 资源合作伙伴和帐户合作伙伴上的 Active Directory 联合身份验证服务。 应同时安装声明感知代理和基于 Windows 令牌的 AD FS Web 代理。

设置域之间的关系

此处介绍的部署由两个域（在其自己的林中）组成，一个针对帐户合作伙伴，另一个针对资源合作伙伴。 请注意，所需的组件无需位于单独的计算机上。

设置域之间的关系

1. 确保您具有下列组件。 帐户合作伙伴需要：

   - 域控制器
   - 联合服务器
   - 用户设备

   资源合作伙伴需要：

   - 域控制器
   - 联合服务器
   - Web 服务器
   - XenApp 场的一台或多台服务器

   联合服务器必须托管于运行 Windows Server 2008 或 Windows Server 2003 R2 的计算机上并且必须安装 ActiveDirectory 联合身份验证服务服务器角色。

   Web 服务器必须托管于运行 32 位版本的 Windows Server 2008 或 Windows Server 2003 R2 的计算机上。 必须安装声明感知代理和基于 Windows 令牌的代理角色服务，以及 Web 服务器(IIS)服务器角色的所有角色服务。

2. 为 Web 服务器和两台联合服务器获取单独的服务器证书。

   - 所有证书都必须由称为证书颁发机构的受信任的实体签发。
   - 服务器证书标识特定的计算机，因此您必须知道每台服务器的完全限定域名 (FQDN)，例如“xenappserver1.mydomain.com”。
   - 将 Web 服务器证书安装到 Microsoft Internet Information Services (IIS) 中以便为 IIS 默认 Web 站点启用 SSL 通信。
   - 使用 Microsoft 管理控制台 (MMC) 证书管理单元安装联合服务器证书。 有关详细信息，请参阅位于 http://technet.microsoft.com/ 上的 Step-by-Step Guide to the Microsoft Management Console（《Microsoft 管理控制台分步指南》）。

3. 为确保资源合作伙伴的联合服务器信任帐户合作伙伴的联合服务器，请将帐户合作伙伴的联合证书安装到资源合作伙伴的联合服务器上的受信任的根证书颁发机构存储中。

4. 为确保 Web 服务器信任资源合作伙伴的联合服务器，请将资源合作伙伴的联合证书安装到 Web 服务器上的受信任的根证书颁发机构存储中。

   重要：资源联合服务器和 Web 服务器必须能够访问证书颁发机构的 CRL。 资源联合服务器必须能够访问帐户合作伙伴的证书颁发机构，Web 服务器必须能够访问资源合作伙伴的证书颁发机构。 如果这些服务器不能确保证书不被吊销，则 AD FS 可能会失败。

5. 在资源合作伙伴联合服务器上，打开 MMC Active Directory 联合身份验证服务管理单元。

6. 在左窗格中，选择 Federation Service（联合身份验证服务）> Trust Policy（信任策略）> Partner Organizations（合作伙伴组织）> Account Partners（帐户合作伙伴），然后选择帐户合作伙伴名称。

7. 在操作窗格中，单击属性。

8. 在 Resource Accounts（资源帐户）选项卡上，选择 Resource accounts exist for all users（所有用户存在资源帐户），并单击确定。

9. 使用同一 Internet 时间服务器，将帐户合作伙伴联合服务器和资源合作伙伴联合服务器上的时钟同步为彼此相差时间在五分钟之内。 否则，资源合作伙伴可能无法接受帐户合作伙伴生成的安全令牌，因为这些令牌似乎已过期。 资源合作伙伴和帐户合作伙伴可以位于不同的时区，但必须正确对它们进行同步。 例如，帐户合作伙伴位于纽约并设置为东部标准时间 (EST) 16:00。 位于加利福尼亚的资源合作伙伴必须设置为介于太平洋标准时间 (PST) 12:55 和 13:05 之间。 （EST 和 PST 时区之间有三个小时的时差。）

10. 在 Web 服务器上，打开 MMC Internet Information Services (IIS) 管理器管理单元。

11. 在左窗格中选择您的 Web 服务器，并在 Features View（功能视图）中双击 Federation Service URL（联合身份验证服务 URL）。

12. 在 Federation Service URL（联合身份验证服务 URL）页上，输入资源合作伙伴联合服务器的 URL，并在操作窗格中单击应用。

为部署中的服务器配置委派

更新日期： 2014-11-24

必须确保部署中的所有服务器都可信任以便进行委派。 为此，请在以域管理员身份登录到资源合作伙伴域的域控制器上后完成以下任务。

确保资源合作伙伴域位于正确的功能级别

重要：要提升域级别，域中的所有域控制器都必须正在运行 Windows Server 2008 或 Windows Server 2003。 如果您拥有或者计划添加运行 Windows Server 2003 的域控制器，请不要将域功能级别提升至 Windows Server 2008。 在提升域功能级别后，将无法回滚至较低的级别。

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 域和信任管理单元。
2. 在左窗格中，选择资源合作伙伴域名，然后在操作窗格中单击属性。
3. 如果域未处于可能达到的最高功能级别，请选择域名并在操作窗格中单击 Raise Domain Functional Level（提升域功能级别）。
4. 要提升域功能级别，请单击相应级别，然后单击 Raise（提升）。

信任 Web Interface 服务器进行委派

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 用户和计算机管理单元。
2. 在视图菜单上，单击 Advanced Features（高级功能）。
3. 在左窗格中，单击资源合作伙伴域名下的计算机节点，然后选择 Web Interface 服务器。
4. 在操作窗格中，单击属性。在操作窗格中，单击属性。
5. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和 Use any authentication protocol（使用任意身份验证协议），然后单击添加。
6. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
7. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix XML Service 的服务器的名称，然后单击确定。
8. 从列表中选择 http 服务类型，然后单击确定。
9. 在 Delegation（委派）选项卡上，确认 XenApp 服务器的 http 服务类型显示在 Services to which this account can present delegated credentials（此帐户可以提出委派凭据的服务）列表中，然后单击确定。
10. 对场中运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的每台服务器，重复上述过程。

信任运行 Citrix XML Service 的服务器进行委派

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 用户和计算机管理单元。
2. 在左窗格中，单击资源合作伙伴域名下的计算机节点，然后选择运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的服务器。
3. 在操作窗格中，单击属性。
4. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和仅使用 Kerberos，然后单击添加。
5. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
6. 在选择用户或计算机对话框中的输入要选择的对象名称框中，键入运行 Citrix XML Service 的服务器的名称，然后单击确定。
7. 从列表中选择 HOST（主机）服务类型，然后单击确定。
8. 在委派选项卡上，确认运行 Citrix XML Service 的服务器的 HOST（主机）类型显示在此帐户可以提出委派凭据的服务列表中，然后单击确定。
9. 对场中运行 Citrix XML Service 且 Web Interface 已配置为将与之联系的每台服务器，重复上述过程。

确定可从 XenApp 服务器访问哪些资源

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 用户和计算机管理单元。
2. 在左窗格中，单击资源合作伙伴域名下的计算机节点，然后选择 XenApp 服务器。
3. 在操作窗格中，单击属性。
4. 在 Delegation（委派）选项卡上，单击 Trust this computer for delegation to specified services only（仅信任此计算机来委派指定的服务）和仅使用 Kerberos，然后单击添加。
5. 在 Add Services（添加服务）对话框中，单击 Users or Computers（用户或计算机）。
6. 在 Select Users or Computers（选择用户或计算机）对话框的 Enter the object names to select（输入要选择的对象名称）框中，键入资源合作伙伴域控制器的名称，然后单击 OK（确定）。
7. 从列表中选择 cifs 和 ldap 服务类型，然后单击确定。

   注：如果 ldap 服务显示两个选项，请选择一个与域控制器的 FQDN 匹配的选项。
8. 在 Delegation（委派）选项卡上，确认资源合作伙伴域控制器的 cifs 和 ldap 服务类型显示在 Services to which this account can present delegated credentials（此帐户可以提出委派凭据的服务）列表中，然后单击确定。
9. 对场中的每台 XenApp 服务器重复此过程。

配置服务器以便进行受限委派

出于安全原因，必须将所有 XenApp 服务器配置为进行受限委派。 要向用户提供对这些服务器上的资源的访问权限，必须使用 MMC Active Directory 用户和计算机管理单元将相关服务添加到 Services to which this account can present delegated credential（此帐户可以提出委派凭据的服务）列表中。 例如，要允许用户针对主机“peter”上的 Web 服务器进行身份验证，请为服务器 peter 添加 http 服务；要允许用户针对主机“lois”上的 SQL 服务器进行身份验证，请为服务器 lois 添加 MSSQLSvc 服务。

有关更多详细信息，请参阅 Citrix 知识中心中的 Service Principal Names and Delegation in Presentation Server（《Presentation Server 中的服务主体名称和委派》）白皮书 (CTX110784)。

配置访问资源的时间限制

警告：注册表编辑器使用不当会导致严重问题，可能需要重新安装操作系统。 Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。 使用“注册表编辑器”需自担风险。

默认情况下，AD FS 用户有权访问网络上的资源 15 分钟。 您可以通过在运行 Citrix XML Service 的服务器上修改以下注册表项，来增加该时间限制：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\S4UTicketLifetime

该值指定在会话开始后用户有权访问资源的分钟数。

域安全策略会控制可以对 S4ULifetime 设置的最大值。 如果为 S4UTicketLifetime 指定的值大于在域级别指定的值，则域级别的设置将优先。

在域级别配置访问资源的时间限制

1. 在资源合作伙伴域控制器上，打开 MMC 域安全策略管理单元。
2. 在左窗格中，选择 Account Policies（帐户策略）> Kerberos Policy（Kerberos 策略）。
3. 在结果窗格中，选择 Maximum lifetime for service ticket（服务票据的最长寿命）。
4. 在操作窗格中，单击属性。
5. 在 Ticket expires in（票据到期时间）框中输入所需的时间限制（以分钟为单位）。

如果不想配置访问资源的时间限制，请在确定可以访问 XenApp 服务器中的哪些资源时，选择 Use any authentication protocol（使用任意身份验证协议）。 如果选择此选项，将会忽略为 S4UTicketLifetime 指定的任何值。 有关详细信息，请访问 Microsoft Web 站点：http://support.microsoft.com/。

设置影子帐户

要提供对应用程序的访问，XenApp 需要真实的 Windows 帐户。 因此，您必须在资源合作伙伴域中为每个外部用户（通过 AD FS 针对 Web Interface 进行身份验证的外部用户）手动创建一个影子帐户。

如果帐户合作伙伴域中有大量用户访问资源合作伙伴域中的应用程序和内容，可以使用第三方帐户设置产品在 Active Directory 中快速创建用户影子帐户。

要创建影子帐户，请在以域管理员身份登录到资源合作伙伴域的域控制器上后完成以下任务。

添加用户主体名称后缀

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 域和信任管理单元。
2. 在左窗格中，选择 Active Directory Domains and Trusts（Active Directory 域和信任）。
3. 在操作窗格中，单击属性。
4. 为每个外部帐户合作伙伴添加一个 UPN 后缀。 例如，如果帐户合作伙伴的 Active Directory 域为“adomain.com”，则可将 adomain.com 添加为 UPN 后缀。

定义影子帐户用户

1. 在资源合作伙伴域控制器上，打开 MMC Active Directory 用户和计算机管理单元。
2. 在左窗格中，选择资源合作伙伴域名。
3. 在操作窗格中，单击新建 > 用户。
4. 在对应的框中键入用户的名字、姓名缩写和姓氏。
5. 在 User logon name（用户登录名）框中，键入帐户名称。 确保此名称与帐户合作伙伴域控制器上的名称匹配。
6. 从列表中选择外部 UPN 后缀，然后单击下一步。
7. 在密码和确认密码框中，键入一个符合密码策略的密码。 此密码将从不使用，因为用户通过 AD FS 进行身份验证。
8. 清除 User must change password at next logon（用户下次登录时必须更改密码）复选框。
9. 选中 User cannot change password（用户不能更改密码）和 Password never expires（密码永不过期）复选框。
10. 单击下一步，然后单击完成。

创建 Active Directory 联合身份验证服务集成站点

从 Citrix Web Interface Management 控制台运行创建站点任务，并将 Web Interface 站点配置为使用 AD FS 进行身份验证。

注：不支持在 AD FS 环境中交付 XenDesktop 虚拟桌面。 此外，Java 客户端和嵌入的远程桌面连接 (RDP) 软件不支持访问 AD FS 集成站点。

创建 Active Directory 联合身份验证服务集成站点

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 Citrix Web Interface 容器。
3. 在操作窗格中，单击创建站点。
4. 选择 XenApp Web 并单击下一步。
5. 在指定 IIS 位置页上，指定站点的 IIS 位置、路径和名称。 单击 Next（下一步）。
6. 在指定身份验证点页上，选择在 Microsoft AD FS 帐户合作伙伴。 设置 Web Interface 的返回 URL 并单击下一步。
7. 确认新站点的设置并单击下一步以创建站点。

将站点配置为 Active Directory 联合身份验证服务应用程序

在创建站点之后，必须将其配置为 AD FS 应用程序，以便联合服务器可识别它。

将站点配置为 Active Directory 联合身份验证服务应用程序

1. 在资源合作伙伴联合服务器上，打开 MMC Active Directory 联合身份验证服务管理单元。
2. 在左窗格中，选择 Federation Service（联合身份验证服务）> Trust Policy（信任策略）> My Organization（我的单位）> Applications（应用程序）。
3. 在操作窗格中，单击新建 > 应用程序。
4. 单击下一步，选择 Claims-aware application（声明感知应用程序），然后再单击下一步。
5. 在 Application display name（应用程序显示名称）框中输入您站点的名称。
6. 在 Application URL（应用程序 URL）框中，输入您 Web Interface 站点的 URL，该 URL 应与创建该站点时 Web Interface 返回 URL 中显示的完全一样，然后单击下一步。

   注：确认是使用 HTTPS 和 Web 服务器的 FQDN。
7. 选中 User principal name (UPN)（用户主体名称(UPN)）复选框，然后单击下一步。
8. 确保选中 Enable this application（启用此应用程序）复选框，然后单击下一步。
9. 单击完成，将您的站点添加为 AD FS 应用程序。

测试部署

更新日期： 2014-12-02

将站点配置为 AD FS 应用程序后，应测试部署以确保帐户合作伙伴和资源合作伙伴之间的一切操作均可正常工作。

测试 Web Interface Active Directory 联合身份验证服务部署

1. 登录到帐户合作伙伴域中的某个用户设备。
2. 打开 Web 浏览器并键入之前创建的 AD FS 集成 Web Interface 站点的 FQDN URL。

   此时将出现您的应用程序集。

   注：如果还没有为集成身份验证配置 AD FS，系统可能会提示您输入凭据或插入智能卡。
3. 如果还没有安装 Citrix 联机插件，请立即进行安装。 有关详细信息，请参阅 Online Plug-in for Windows 文档。
4. 单击应用程序以访问它。

从 Active Directory 联合身份验证服务集成站点注销

使用 Citrix Web Interface Management 控制台中的身份验证方法任务，可以指定用户单击 Web 站点上的注销或断开连接按钮时是否注销：

- 仅限 Web Interface
- Web Interface 和 AD FS 联合身份验证服务

如果指定用户仅从 Web Interface 注销，用户将被定向到 Web Interface 的注销屏幕。 如果指定用户从 Web Interface 和 AD FS 联合身份验证服务注销，用户将被定向到联合身份验证服务注销页并从所有 AD FS 应用程序注销。

注：使用 AD FS 进行身份验证的用户无法解除 XenApp 会话锁定，因为他们不知道密码。 要解除会话锁定，用户必须从 Web Interface 注销，然后使用 AD FS 身份验证重新登录并重新启动应用程序。 当用户执行此操作后，将解除先前的会话锁定并关闭新窗口。

指定用户注销的服务

1. 在 Windows 开始菜单中，依次单击所有程序 > Citrix > 管理控制台 > Citrix Web Interface Management。
2. 在 Citrix Web Interface Management 控制台的左窗格中，单击 XenAppWeb 站点，并在结果窗格中选择您的 AD FS 集成站点。
3. 在操作窗格中，单击身份验证方法。
4. 要指定用户从 Web Interface 和 AD FS 联合身份验证服务注销，请选中执行全局注销复选框。 要指定用户仅从 Web Interface 注销，请清除执行全局注销复选框。