Webinterface 5.4

2015-05-07 20:29:12 UTC

Inhalt

Webinterface 5.4

Aktualisiert: 2014-11-25

Das Webinterface bietet Benutzern Zugriff auf XenApp-Anwendungen und -Inhalte und virtuelle XenDesktop-Desktops. Benutzer greifen über einen Standardwebbrowser oder das Citrix Online Plug-In auf Ressourcen zu.

In diesem Abschnitt

In diesem Bereich der Bibliothek finden Sie aktuelle Informationen über das Installieren, Konfigurieren und Verwalten des Webinterface, einschließlich dieser Themenbereiche.

Readme für das Webinterface 5.4	Informationen zu aktuellen Updates und bekannten Problemen.
Im Webinterface 5.4 behobene Probleme	Einzelheiten zu Problemen, die seit dem letzten Release des Webinterface behoben wurden.
Webinterface-Funktionen	Einführung in das Webinterface.
Neue Funktionen in diesem Release	Ein Überblick über die neuen Funktionen
Webinterface-Komponenten	Eine Beschreibung der Webinterface-Bereitstellung.
Systemanforderungen für das Webinterface	Anforderungen für Software, Konfiguration, Webserver, Benutzer und Geräte.
Installieren des Webinterface	Installieren des Webinterface und Konfigurieren des Webservers.
Erste Schritte mit dem Webinterface	Erstellen und Konfigurieren von Webinterface-Sites.
Verwalten von Servern und Farmen	Konfigurieren und Verwalten von Servereinstellungen und der Kommunikation mit Serverfarmen.
Konfigurieren der Authentifizierung für das Webinterface	Konfigurieren der Authentifizierung zwischen dem Webinterface, den Serverfarmen und den Citrix Plug-Ins.
Verwalten von Clients	Bereitstellen und Verwenden von Citrix Plug-Ins mit dem Webinterface.
Verwalten des sicheren Zugriffs	Konfigurieren und Verwalten des Zugriffs auf Sites.
Bearbeiten von clientseitigen Proxyeinstellungen	Konfigurieren von Citrix Clients und Servern, auf denen XenApp oder XenDesktop über Proxyserver ausgeführt wird.
Anpassen der Darstellung für Benutzer	Anpassen der Webinterface-Darstellung für Benutzer.

Verwalten der Sitzungseinstellungen	Angeben von Einstellungen, die Benutzer anpassen können.
Konfigurieren von Workspace Control	Ermöglichen, dass Benutzer die Verbindung zu Ressourcen schnell trennen, wiederherstellen und sich von Ressourcen schnell abmelden können.
Konfigurieren der Webinterface-Sicherheit	Sichern der Daten in einer Webinterface-Umgebung.
Konfigurieren von Sites mit der Konfigurationsdatei	Verwalten von Webinterface-Sites mit den Konfigurationsdateien.
Konfigurieren der ADFS-Unterstützung für das Webinterface	Erstellen und Konfigurieren von Webinterface-Sites mit Microsoft Active Directory-Verbunddienste-Integration.

Readme für das Webinterface 5.4

Readmeversion: 1.0

Inhalt

Verwandte Dokumentation

Informationen zu Clientproblemen, die sich auf Webinterface-Benutzer auswirken könnten, finden Sie in den Readmedateien der Citrix Clients, die zurzeit für Ihre Benutzer bereitgestellt sind.

Eine Liste der in diesem Release behobenen Probleme finden Sie im Knowledge Center-Artikel http://support.citrix.com/article/CTX124164.

Lizenzierungsdokumentation finden Sie unter Lizenzieren des Produkts.

Support

Citrix bietet technischen Support hauptsächlich durch Citrix Solutions Advisor an. Bei Supportfragen wenden Sie sich bitte zuerst an Ihren Händler oder finden Sie mit Citrix Online Technical Support einen Citrix Solutions Advisor in Ihrer Nähe.

Citrix bietet technischen Support auf der Citrix Supportwebsite an. Auf der Supportseite finden Sie Links zu Downloads, zum Citrix Knowledge Center, zu den Citrix Consulting Services und zu anderen Supportseiten.

Bekannte Probleme

Im Anschluss finden Sie eine Liste bekannter Probleme in diesem Release. **Lesen Sie sie bitte vor der Installation des Produkts sorgfältig durch**.

- Symbole werden auf Geräten, auf denen WinCE 6.0 WFR3 und Internet Explorer 6 ausgeführt wird, nicht richtig angezeigt
- Wenn veröffentlichte Desktops den Internet Explorer-Favoriten hinzugefügt werden, kann es zu Benutzerfehlern kommen
- Fehlermeldung beim Versuch, eine Verbindung mit veralteten Clients herzustellen

- Citrix Online Plug-In kann nicht auf Geräten aktualisiert werden, auf denen Windows Embedded-Betriebssysteme ausgeführt werden
- Kerberos-Verwendung schlägt fehl, wenn Delegierung auf XenApp-Servern mit Windows Server 2008 konfiguriert wird
- Virtueller Desktop startet nicht, wenn auf das Webinterface von manchen Geräten mit Windows Embedded CE 6.0 zugegriffen wird
- Upgrade für Workspace Control und Client ist nicht für Firefox 3.6-Benutzer verfügbar
- Workspace Control steht auf manchen Geräten mit Windows Mobile 6.1 nicht zur Verfügung
- Workspace Control ist auf manchen Geräten mit Windows Embedded CE 6.0 R2 nicht durchgängig verfügbar
- Passthrough mit Smartcard von Access Gateway kann nicht mit XenApp 6.0 verwendet werden

Symbole werden auf Geräten, auf denen WinCE 6.0 WFR3 und Internet Explorer 6 ausgeführt wird, nicht richtig angezeigt

Symbole im PNG-Format werden auf Geräten, auf denen Internet Explorer 6 mit WinCE 6.0 WFR3 (HotFix 3 Build 664) ausgeführt wird, nicht richtig angezeigt. Um dieses Problem zu lösen, verwenden Sie Internet Explorer Version 5 oder früher. Um PNG-Dateien in Internet Explorer 6 anzuzeigen, können Sie auch den Lösungsvorschlag im Microsoft-Artikel http://support.microsoft.com/kb/294714 verwenden.

[#41839]

Benutzer können u. U. veröffentlichte Desktops und Anwendungen nicht als Internet Explorer-Favoriten hinzufügen

Es können Probleme auftreten, wenn Benutzer versuchen, den Internet Explorer-Favoriten veröffentlichte Desktops und Anwendungen hinzuzufügen. In manchen Situationen hat der daraus entstandene Favoriten-Link einen falschen Titel und funktioniert nicht richtig. Um eine Anwendung den Favoriten hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Symbol der Anwendung. Um Desktops hinzuzufügen, klicken Sie mit der rechten Maustaste auf den Titel des Desktops.

[#244446]

Fehlermeldung beim Versuch, eine Verbindung mit veralteten Clients herzustellen

Dieses Release des Webinterface unterstützt nicht die Verwendung von Clients vor Version 7.0. Beim Versuch, eine Remoteanwendung mit einem früheren Client zu öffnen, wird u. U. eine Fehlermeldung angezeigt, dass keine Verbindung zum Server hergestellt werden kann. Benutzer können dieses Problem vermeiden, indem Sie ein Upgrade auf die aktuelle Version des Clients durchführen. Sollte dies nicht möglich sein, kann der Fehler verhindert werden, indem Sie die ICA-Vorlagendateien folgendermaßen bearbeiten:

1. Öffnen Sie die folgenden Dateien in einem Texteditor, z. B. Editor: default.ica, bandwidth_high.ica, bandwidth_low.ica, bandwidth_medium.ica und bandwidth_medium_high.ica. Diese Dateien befinden sich in IIS normalerweise im Verzeichnis C:\inetpub\wwwroot\Citrix*Sitename*\conf und auf Java-Anwendungsservern

im Verzeichnis /WEB-INF der Webinterface-Site.

2. Löschen Sie die folgenden Zeilen in jeder Datei:

   DoNotUseDefaultCSL=On
   BrowserProtocol=HTTPonTCP
   LocHttpBrowserAddress=!

[#163695]

Citrix Online Plug-In kann nicht auf Geräten aktualisiert werden, auf denen Windows Embedded-Betriebssysteme ausgeführt werden

Das Webinterface bietet u. U. an, das Citrix Online Plug-In auf Geräten, auf denen Windows Embedded-Betriebssysteme ausgeführt werden, zu installieren oder zu aktualisieren. Die Installation wird jedoch fehlschlagen. Sie können dieses Problem vermeiden, indem Sie die aktuelle Version des Citrix Online Plug-Ins manuell auf dem eingebetteten Gerät installieren. Sollte dies nicht möglich sein, können Sie die Einstellungen für die Site ändern, damit diese Installationsmeldungen nicht mehr angezeigt werden:

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Clientbereitstellung. Für Sites, die nur Onlineanwendungen anbieten, aktivieren Sie das Kontrollkästchen Nativer Client und klicken Sie auf Eigenschaften.

4. Klicken Sie auf Clienterkennung.

5. Deaktivieren Sie das Kontrollkästchen Upgrades für Clients anbieten und wählen Sie Nur wenn Zugriff auf Ressourcen nicht möglich ist oder Nie.

[#164709]

Kerberos-Verwendung schlägt fehl, wenn Delegierung auf XenApp-Servern mit Windows Server 2008 konfiguriert wird

Aufgrund eines Problems bei Windows Server 2008 schlägt die Authentifizierung fehl, wenn Active Directory für die Authentifizierung nur Kerberos verwendet, wenn XenApp Servern für Delegierungszwecke vertraut wird. Dieses Problem auf XenApp-Servern auf, auf denen die folgenden Betriebssysteme ausgeführt werden: Windows Server 2008 mit Service Pack 2, Windows Server 2008 x64-Editionen mit Service Pack 2 und Windows Server 2008 R2. Um ADFS-Integration und Passthrough mit Smartcard von Access Gateway auf XenApp-Servern zu ermöglichen, auf denen Windows Server 2008 ausgeführt wird, aktivieren Sie die Einstellung Beliebiges Authentifizierungsprotokoll verwenden anstatt der in der Dokumentation genannten Einstellung Nur Kerberos verwenden. [#169269]

Virtueller Desktop startet nicht, wenn auf das Webinterface von manchen Geräten mit Windows Embedded CE 6.0 zugegriffen wird

In manchen Fällen, wenn sich Benutzer von WYSE V30LE Thin Clients mit Windows Embedded CE 6.0 und Internet Explorer 6.*x* an XenApp Web-Sites anmelden und auf einen Textlink klicken, um einen virtuellen Desktop zu starten, schlägt der Start des Desktops

fehl. Benutzer können dieses Problem vermeiden, indem sie auf das Symbol neben dem Textlink klicken, um den Desktop zu starten. [#218317]

Upgrade für Workspace Control und Client ist nicht für Firefox 3.6-Benutzer verfügbar

Wegen einer Änderung in Mozilla Firefox 3.6 wird Workspace Control automatisch für Benutzer aktiviert, die mit diesem Browser auf das Webinterface zugreifen. Außerdem kann der Clienterkennungs- und -bereitstellungsprozess die Versionsnummern der von Firefox 3.6-Benutzern installierten Citrix Clients nicht ermitteln und daher den Benutzern keinen Upgrade der Clients anbieten. [#230068]

Workspace Control steht auf manchen Geräten mit Windows Mobile 6.1 nicht zur Verfügung

Benutzer von HP iPAQ 910c-Handheldgeräten mit Windows Mobile 6.1 Professional und Internet Explorer Mobile stellen u. U. fest, dass bei der Anmeldung an XenApp Web-Sites Workspace Control nicht richtig funktioniert. [#230580]

Workspace Control ist auf manchen Geräten mit Windows Embedded CE 6.0 R2 nicht durchgängig verfügbar

Benutzer von HP t5540-Thin Clients mit Windows Embedded CE 6.0 R2 und Internet Explorer 6.*x* stellen bei der Anmeldung an XenApp Web-Sites u. U. fest, dass Workspace Control manchmal nicht funktioniert, wenn Sie auf die Schaltfläche Wiederverbinden klicken. [#230654]

Passthrough mit Smartcard von Access Gateway kann nicht mit XenApp 6.0 verwendet werden

Wegen eines Problems mit XenApp 6.0 können Smartcard-Benutzer, die sich an in Access Gateway integrierten Sites anmelden, nicht auf Ressourcen zugreifen, wenn die Funktion für Passthrough mit Smartcard von Access Gateway aktiviert ist. Benutzer, die auf einen Link klicken, um auf eine mit XenApp 6.0 bereitgestellte Ressource zuzugreifen, erhalten die Fehlermeldung "Beim Herstellen der angeforderten Verbindung ist ein Fehler aufgetreten." Sie können dieses Problem vermeiden, indem Sie die Site so konfigurieren, dass Smartcard-Benutzer jedes Mal, wenn sie auf eine Ressource zugreifen, aufgefordert werden, ihre PIN-Nummer einzugeben. [#230942]

http://www.citrix.com/

Webinterface-Verwaltung

Das Webinterface bietet Benutzern Zugriff auf XenApp-Anwendungen und -Inhalte und virtuelle XenDesktop-Desktops. Benutzer greifen über einen Standardwebbrowser oder das Citrix Online Plug-In auf Ressourcen zu.

Das Webinterface setzt Java- und .NET-Technologie ein, die auf einem Webserver ausgeführt wird und dynamisch HTML-basierte Darstellungen von Serverfarmen für XenApp Web-Sites erstellt. Benutzer sehen alle in der Serverfarm bzw. den Serverfarmen veröffentlichten Ressourcen (Anwendungen, Inhalte und Desktops), die Sie bereitstellen. Sie können eigenständige Websites für den Zugriff auf Ressourcen erstellen sowie Websites, die Sie in Ihr Unternehmensportal integrieren können. Mit dem Webinterface können Sie außerdem Einstellungen für Benutzer konfigurieren, die mit dem Citrix Online Plug-In auf Ressourcen zugreifen.

Sie können mit der Citrix Webinterface Management Console in Microsoft Internetinformationsdienste (IIS) Webinterface-Sites erstellen und konfigurieren. Diese Konsole wird nur mit dem Webinterface für Microsoft Internetinformationsdienste installiert. Weitere Informationen zum Verwenden dieses Tools finden Sie unter Konfigurieren von Sites mit der Citrix Webinterface Management Console.

Sie können außerdem die Konfigurationsdatei der Site (WebInterface.conf) bearbeiten, um Webinterface-Sites zu verwalten. Weitere Informationen finden Sie unter Konfigurieren von Sites mit Konfigurationsdateien.

Darüber hinaus können Sie XenApp Web-Sites anpassen und erweitern. In der Dokumentation für das Webinterface-SDK wird das Konfigurieren von Sites mit diesen Verfahren erläutert.

Webinterface-Funktionen

Mit den zwei Webinterface-Sites stellen Sie den Benutzern verschiedene Methoden für den Zugriff auf Ressourcen bereit.

XenApp Web-Sites: Sie können Benutzern eine Website bereitstellen, an der sie sich mit einem Webbrowser anmelden. Nach der Authentifizierung können Benutzer mit einem Citrix Client auf Onlineressourcen und Offlineanwendungen zugreifen.

XenApp Services-Sites: Mit dem Citrix Online Plug-In und dem Webinterface können Sie Ressourcen in die Desktops der Benutzer integrieren. Benutzer greifen über Symbole auf dem Desktop, im Startmenü oder im Infobereich auf Anwendungen, virtuelle Desktops und Onlineinhalte zu. Sie können die Konfigurationseinstellungen festlegen, auf die Benutzer zugreifen können und die sie ändern können, wie zum Beispiel Audio-, Darstellungs- und Anmeldungseinstellungen.

Verwaltungsfunktionen

Aktualisiert: 2014-11-24

Unterstützung für mehrere Serverfarmen: Sie können mehrere Serverfarmen konfigurieren und Benutzern die in allen Farmen verfügbaren Ressourcen anzeigen. Mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console können Sie jede Serverfarm einzeln verwalten. Weitere Informationen finden Sie unter Konfigurieren von Sites mit der Konfigurationsdatei.

Wiederherstellung im Notfall: Sie können XenApp- und XenDesktop-Serverfarmen für Notfälle angeben, wenn Benutzer aufgrund eines Strom- oder Netzwerkausfalls nicht auf die üblichen Farmen zugreifen können. Hiermit können Sie sicherstellen, dass bei Ausfällen der Geschäftsserver unternehmensrelevante Anwendungen oder Desktops weiterhin verfügbar sind.

Gemeinsam verwendete Sitekonfiguration: Im Webinterface für Microsoft Internetinformationsdienste können Sie eine "Mastersite" angeben, deren Konfigurationsdatei über das Netzwerk gemeinsam genutzt werden kann. Andere Sites können dann so konfiguriert werden, dass sie die Konfiguration der Mastersite anstelle einer lokalen Datei verwenden.

Integration mit bekannten Webtechnologien: Sie können mit ASP.NET von Microsoft und JavaServer Pages von Sun Microsystems auf die Webinterface-API zugreifen. Das Webinterface für Java-Anwendungsserver ist plattformunabhängig und kann daher auch auf Windows-Betriebssystemen, auf denen nicht Microsoft Internetinformationsdienste (IIS) als Webserver verwendet wird, installiert werden.

Funktionen für den Ressourcenzugriff

XenApp VM Hosted Apps: Mit XenApp können Onlineanwendungen von virtuellen Maschinen bereitgestellt werden. Hiermit können Sie Anwendungen veröffentlichen, die mit Remotedesktopdienste nicht kompatibel sind bzw. noch nicht für die Verwendung mit Terminaldienste getestet worden sind, oder Anwendungen, deren Installation auf Windows Server-Betriebssystemen nicht unterstützt wird.

Benutzerroaming: Sie können Benutzergruppen mit bestimmten Serverfarmen verknüpfen, um Benutzern ein konsistentes Benutzererlebnis zu bieten unabhängig von ihrem aktuellen Standort oder dem Server, an dem sie sich anmelden. Hierdurch können sich Benutzer, die z. B. geschäftlich ins Ausland reisen, an einem lokalen Webinterface-Server anmelden und automatisch Ressourcen in ihrer Sprache von einer Farm in ihrem Heimatland erhalten.

Unterstützung für UNIX-Farmen: Durch die Unterstützung von XenApp für UNIX-Farmen kann das Webinterface Anwendungen, die auf UNIX-Plattformen ausgeführt werden, auf Benutzergeräten anzeigen und bereitstellen.

Unterstützung für Active Directory und Benutzerprinzipalnamen: Alle Webinterface-Komponenten sind mit Microsoft Active Directory kompatibel. Benutzer, die XenApp Web-Sites öffnen, können sich an Serverfarmen anmelden, die Teil einer Active Directory-Bereitstellung sind, und die Anwendungen und Inhalte problemlos verwenden. Die Anmeldeseiten sind mit der Verwendung von Benutzerprinzipalnamen (UPN) von Active Directory kompatibel.

Anonyme Benutzer: Das Webinterface ermöglicht Benutzern, die sich mit einem anonymen Konto an XenApp Web-Sites anmelden, den Zugriff auf XenApp-Anwendungen.

Sicherheitsfeatures

SSL (Secure Sockets Layer)/TLS (Transport Layer Security)-Unterstützung: Das Webinterface unterstützt SSL für das Sichern der Kommunikation zwischen dem Webinterface-Server und den Serverfarmen. Das Implementieren von SSL auf dem Webserver und die Verwendung von Webbrowsern, die SSL unterstützen, gewährleisten eine sichere Datenübertragung im Netzwerk. Das Webinterface verwendet das Microsoft .NET Framework zur Implementierung von SSL und Kryptografie.

Access Gateway-Unterstützung: Das Citrix Access Gateway ist ein universelles SSL-VPN-Gerät, das zusammen mit dem Webinterface zentralen, sicheren Zugriff auf alle Informationsressourcen ermöglicht, sowohl Daten als auch Sprache. Access Gateway vereint die besten Funktionen von IPSec (Internet Protocol Security) und SSL VPN, ohne die kostspielige und aufwändige Implementierung und Verwaltung. Es kann mit jeder Firewall eingesetzt werden und unterstützt alle Ressourcen und Protokolle.

Secure Gateway-Unterstützung: Secure Gateway stellt zusammen mit dem Webinterface einen gemeinsamen, sicheren und verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit. Secure Gateway vereinfacht die Zertifikatverwaltung, da nur der Secure Gateway-Server und nicht jeder Server in der Farm ein Serverzertifikat benötigt.

Smartcardunterstützung: Das Webinterface unterstützt die Verwendung von Smartcards für die Benutzerauthentifizierung, um sicheren Zugriff auf Anwendungen, Inhalte und Desktops zu ermöglichen. Smartcards erleichtern die Authentifizierung für Benutzer, während gleichzeitig die Sicherheit bei der Anmeldung erhöht wird.

Ticketing: Diese Funktion bietet erhöhte Sicherheit bei der Authentifizierung. Das Webinterface erhält Tickets, mit denen Benutzer bei Ressourcen authentifiziert werden. Tickets besitzen eine konfigurierbare Gültigkeitsdauer und gelten nur für eine einzige Anmeldung. Nach Benutzung oder Ablauf ist das Ticket ungültig und kann nicht mehr für den Zugriff auf Ressourcen verwendet werden. Durch die Verwendung von Ticketing müssen Anmeldeinformationen nicht explizit in den ICA-Dateien enthalten sein, mit denen das Webinterface Verbindungen zu Ressourcen herstellt.

Secure Ticket Authority-Redundanz: Sie können mehrere redundante Secure Ticket Authoritys (STAs) für Benutzer konfigurieren, die über Access Gateway auf ihre Ressourcen zugreifen. Hierdurch können Sie Vorsorge treffen für Situationen, in denen eine Secure Ticket Authority mitten in einer Benutzersitzung ausfällt und eine Wiederverbindung nicht möglich ist. Wenn Redundanz aktiviert ist, versucht das Webinterface zwei Tickets von verschiedenen Secure Ticket Authorities abzurufen und an das Gateway weiterzugeben. Wenn zu einer der Secure Ticket Authorities während einer Benutzersitzung keine Verbindung hergestellt werden kann, wird die Sitzung ohne Unterbrechung mit der zweiten Secure Ticket Authority fortgesetzt.

Kennwortänderungen: Benutzer, die sich mit expliziten Domänenanmeldeinformationen am Webinterface oder am Citrix Online Plug-In anmelden, haben die Möglichkeit, ihre Windows-Kennwörter zu ändern, wenn diese ablaufen. Benutzer können das Kennwort ändern, unabhängig davon, ob sich der Computer in der Domäne befindet, an der sie sich authentifizieren möchten.

Konto-Self-Service: Durch die Integration der Citrix Password Manager-Funktion Konto-Self-Service können Benutzer, die Password Manager verwenden, ihr Netzwerkkennwort zurücksetzen und die Sperrung ihres Kontos aufheben, indem sie eine Reihe von Sicherheitsfragen beantworten.

Clientbereitstellungsfunktionen

Webbasierte Clientinstallation: Wenn ein Benutzer eine XenApp Web-Site öffnet, erkennt das Webinterface das Gerät sowie den Webbrowsertyp und fordert den Benutzer zur Installation eines entsprechenden Citrix Clients auf, falls einer vorhanden ist. Erhöhte Sicherheitsvorkehrungen moderner Betriebssysteme und Webbrowser können Benutzern den Download und die Bereitstellung von Citrix Clients erschweren. Das Webinterface enthält daher einen Clienterkennungs- und -bereitstellungsprozess, der die Benutzer bei der Bereitstellung und, falls erforderlich, bei der Neukonfigurierung ihrer Webbrowser unterstützt. Hierdurch wird sichergestellt, dass Benutzer selbst in extrem stark gesicherten Umgebungen optimal auf Ressourcen zugreifen können.

Unterstützung für Citrix Online Plug-In: Mit dem Citrix Online Plug-In können Benutzer direkt von ihren Desktops ohne einen Webbrowser auf Ressourcen zugreifen. Die Benutzeroberfläche des Citrix Online Plug-Ins kann auch "gesichert" werden, um eine falsche Konfiguration durch die Benutzer zu verhindern.

Unterstützung für Citrix Offline Plug-In: Mit dem Citrix Offline Plug-In können Benutzer XenApp-Anwendungen auf ihren Desktop übertragen und lokal öffnen. Sie können das Plug-In zusammen mit dem Citrix Online Plug-In installieren, damit die clientseitige Anwendungsvirtualisierung von Citrix in vollem Umfang genutzt werden kann, oder Sie können es nur auf den Desktops der Benutzer installieren, damit Benutzer über einen Webbrowser und eine XenApp Web-Site auf Anwendungen zugreifen können.

Neue Funktionen in diesem Release

Aktualisiert: 2014-12-02

Das Webinterface enthält die folgenden neuen Funktionen und Verbesserungen in diesem Release:

Aktualisierte Oberfläche für Endbenutzer: Das Layout und Farbschema für Endbenutzer wurden aktualisiert, um die Navigation und Lesbarkeit zu verbessern.

Sitzungsfreigabe für auf virtuellen Maschinen gehostete Anwendungen: Das Webinterface unterstützt jetzt Sitzungsfreigabe für auf virtuellen Maschinen (VMs) gehostete Anwendungen. Diese Funktion ist nur für Seamless-Anwendungen und nicht-anonyme Bernutzer verfügbar.

Zugriff auf mehrere Desktops für Benutzer: In früheren Versionen des Webinterface konnten Benutzer nur auf eine Instanz eines Desktops pro Desktopgruppe zugreifen. Jetzt können Benutzer auf mehrere Instanzen von Desktops in Desktopgruppen zugreifen. Weitere Informationen zum Zuweisen von Desktops finden Sie in der Dokumentation für XenDesktop 5.

Verbesserte Smartcard-Unterstützung für Access Gateway: Smartcard-Authentifizierung am Webinterface ist jetzt mit den meisten Umgebungen kompatibel. Das Webinterface kann jetzt neben Benutzernamen und Domänen auch Benutzerprinzipalnamen (UPNs) vom Access Gateway akzeptieren. Zusätzlich wurde das Webinterface aktualisiert, um FIPS-Anforderungen zu erfüllen. Diese neue Funktion kann nur mit der Passthrough-Authentifizierung für Smartcard verwendet werden und Sie müssen als Domänenadministrator angemeldet sein. Weitere Informationen zur Konfiguration der Smartcard-Unterstützung für Access Gateway finden Sie in der archivierten Access Gateway-Dokumentation.

Festlegen zusätzlicher Standardwerte: Administratoren können Standardwerte für alle Einstellungen, die die Bandbreite betreffen, z. B. Audioqualität, Farbtiefe, Bandbreitenprofil, Druckerzuordnung und Fenstergröße, konfigurieren.

ICA-Dateisignierung: Das Webinterface signiert ICA-Dateien digital, damit kompatible Citrix Clients und Plug-Ins prüfen können, ob die Datei von einer vertrauenswürdigen Quelle stammt.

Webinterface-Komponenten

Eine Webinterface-Bereitstellung umfasst drei Netzwerkkomponenten:

- Eine oder mehrere Serverfarmen
- Einen Webserver
- Ein Benutzergerät mit einem Webbrowser und einem Citrix Client

Serverfarmen

Eine Gruppe von Servern, die als eine Einheit verwaltet werden und gemeinsam Ressourcen für Benutzer bereitstellen, wird als *Serverfarm* bezeichnet. Eine Serverfarm besteht aus einer Reihe von Servern, auf denen entweder XenApp oder XenDesktop, jedoch nicht eine Mischung aus beiden, ausgeführt wird.

Eine der Hauptfunktionen einer Serverfarm ist das Veröffentlichen von Ressourcen. Dies ist ein Prozess, mit dem Administratoren Benutzern bestimmte Ressourcen (Anwendungen, Inhalte und Desktops) verfügbar machen, die von der Serverfarm bereitgestellt werden. Wenn eine Ressource von einem Administrator für eine Gruppe von Benutzern veröffentlicht wird, steht diese Ressource in Form eines Objekts zur Verfügung, zu dem die Citrix Clients eine Verbindung herstellen und Sitzungen starten können.

Beim Webinterface wird den Benutzern nach der Anmeldung an der Serverfarm eine benutzerspezifische Liste aller Ressourcen angezeigt, die für den jeweiligen Benutzernamen veröffentlicht sind. Diese Liste wird Ressourcengruppe genannt. Der Webinterface-Server bildet einen Zugriffspunkt, über den eine Verbindung zu den Serverfarmen hergestellt wird. Der Webinterface-Server fragt die Serverfarmen nach Informationen zur Ressourcengruppe ab und gibt die Ergebnisse in Form von HTML-Seiten aus, die Benutzer in einem Webbrowser anzeigen können.

Um Informationen von Serverfarmen zu erhalten, kommuniziert der Webinterface-Server mit dem Citrix XML-Dienst, der auf mindestens einem Server ausgeführt wird. Der Citrix XML-Dienst ist eine Komponente von XenApp und XenDesktop, die Citrix Clients und Webinterface-Servern über TCP/IP und HTTP Informationen über Ressourcen zur Verfügung stellt. Dieser Dienst stellt den Kontaktpunkt zwischen der Serverfarm und dem Webinterface-Server dar. Der Citrix XML-Dienst wird mit XenApp und XenDesktop installiert.

Webserver

Der Webserver hostet das Webinterface. Folgende Dienste werden vom Webinterface zur Verfügung gestellt:

- Authentifizieren von Benutzern bei einer oder mehreren Serverfarmen
- Abrufen von Informationen über verfügbare Ressourcen, einschließlich einer Liste von Ressourcen, auf die Benutzer zugreifen können

Benutzergerät

Ein *Benutzergerät* ist ein beliebiges Computinggerät, auf dem ein Citrix Client und ein Webbrowser ausgeführt werden können. Hierzu zählen u. a. Desktop-PCs, Laptops, Netzwerkcomputer, Terminals und Handheld-Computer.

Auf dem Benutzergerät übernimmt der Webbrowser die Rolle des Viewers und der Citrix Client die Rolle der Engine. Der Webbrowser zeigt den Benutzern die Ressourcengruppen an, die mit serverseitigen Skripten auf dem Webinterface-Server erstellt wurden, und der Client dient als Engine für den Zugriff auf Ressourcen.

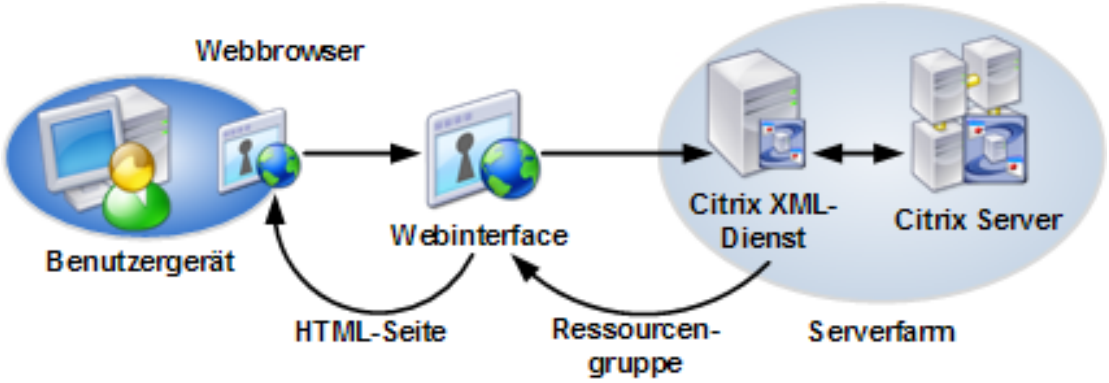
Das Webinterface bietet *webbasierte Clientbereitstellung*, eine Methode zur Bereitstellung von Citrix Clients von einer Website. Wenn ein Benutzer eine mit dem Webinterface erstellte Website öffnet, erkennt der webbasierte Clienterkennungs- und -bereitstellungsprozess das Gerät und der Benutzer wird zur Installation eines entsprechenden Citrix Clients aufgefordert. In einigen Umgebungen kann der webbasierte Clienterkennungs- und -bereitstellungsprozess auch erkennen, ob ein Client installiert ist. Dem Benutzer wird in diesem Fall nur dann eine Installationsaufforderung angezeigt, wenn dies erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Clientbereitstellung und Installationsmeldungen.

Das Webinterface unterstützt eine Vielzahl von Kombinationen aus Webbrowsern und Citrix Clients. Sie finden eine vollständige Liste der unterstützten Kombinationsmöglichkeiten unter Benutzergerätanforderungen.

Funktionsweise des Webinterface

Unten wird ein Zusammenspiel zwischen einer Serverfarm, einem Webinterface-Server und einem Benutzergerät beschrieben.

Diese Abbildung zeigt die Interaktion der einzelnen Komponenten mit dem Webinterface. Der Webbrowser auf dem Benutzergerät sendet Informationen an den Webserver, der mit der Serverfarm kommuniziert, damit Benutzer auf Ressourcen zugreifen können.



- Benutzer authentifizieren sich über einen Webbrowser beim Webinterface.
- Der Webserver liest die Anmeldeinformationen des Benutzers und gibt die Informationen an den Citrix XML-Dienst auf den Servern in den Serverfarmen weiter. Der angegebene Server dient als Vermittler zwischen dem Webserver und den anderen Servern in der Farm.
- Der Citrix XML-Dienst auf dem angegebenen Server ruft dann von den Servern die Liste der Ressourcen ab, auf die der Benutzer zugreifen kann. Diese Ressourcen stellen die Ressourcengruppe des Benutzers dar. Der Citrix XML-Dienst ruft die Ressourcengruppe vom IMA-System (Independent Management Architecture) ab.
- In einer Farm mit XenApp für UNIX ermittelt der Citrix XML-Dienst anhand der vom ICA-Browser gesammelten Informationen auf dem angegebenen Server die Anwendungen, auf die der Benutzer zugreifen kann.
- Der Citrix XML-Dienst übergibt dann die Ressourcengruppen-Informationen des Benutzers an das auf dem Server ausgeführte Webinterface.
- Der Benutzer klickt auf ein Symbol, das eine Ressource auf der HTML-Seite darstellt.
- Der Citrix XML-Dienst sucht den am geringsten ausgelasteten Server in der Farm. Der Citrix XML-Dienst ermittelt den am wenigsten ausgelasteten Server und gibt die Adresse dieses Servers an das Webinterface zurück.
- Das Webinterface kommuniziert mit dem Citrix Client (in einigen Fällen mit dem Webbrowser als Vermittler).
- Der Citrix Client initiiert eine Sitzung mit dem Server in der Farm basierend auf den Verbindungsinformationen vom Webinterface.

Systemanforderungen für das Webinterface

Aktualisiert: 2014-11-24

Für die Webinterface-Ausführung muss ein unterstütztes Citrix Produkt auf den Servern ausgeführt werden.

Das Webinterface unterstützt folgende Produktversionen:

- Citrix XenApp 7.6 und XenDesktop 7.6
- Citrix XenApp 7.5 und 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 für Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 für Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0, mit Feature Pack 2, für Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, mit Feature Pack 2, für Microsoft Windows Server 2003
- Citrix XenApp 5.0, mit Feature Pack 1, für Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0, mit Feature Pack 1, für Microsoft Windows Server 2008
- Citrix XenApp 5.0, mit Feature Pack 1, für Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, mit Feature Pack 1, für Microsoft Windows Server 2003
- Citrix XenApp 5.0 für Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0 für Microsoft Windows Server 2008

- Citrix XenApp 5.0 für Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0 für Microsoft Windows Server 2003
- Citrix XenApp 4.0, mit Feature Pack 1, für UNIX-Betriebssysteme
- Citrix Presentation Server 4.5, mit Feature Pack 1, für Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5, mit Feature Pack 1, für Windows Server 2003
- Citrix Presentation Server 4.5 für Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5 für Windows Server 2003

Wichtig: Um Kompatibilität mit XenApp 4.0, mit Feature Pack 1, für UNIX zu erreichen, ist ein zusätzlicher manueller Konfigurationsschritt erforderlich. Weitere Informationen finden Sie unter So konfigurieren Sie Unterstützung für XenApp 4.0, mit Feature Pack 1, für UNIX.

Das Webinterface kann mit diesen Produkten auf allen unterstützten Plattformen eingesetzt werden. Eine Liste der unterstützten Plattformen finden Sie in der Dokumentation für den Citrix Server. Citrix empfiehlt, dass Sie auf Ihren Servern immer die aktuellen Service Packs für die Betriebssysteme installieren.

Allgemeine Konfigurationsanforderungen

Server müssen Mitglied einer Serverfarm sein. Auf den Servern in der Farm müssen Ressourcen (Anwendungen, Inhalte und/oder Desktops) veröffentlicht sein. Weitere Informationen zur Mitgliedschaft in einer Serverfarm und zum Veröffentlichen von Ressourcen in einer Serverfarm finden Sie in der Dokumentation für Ihren Citrix Server.

Auch auf Servern mit XenApp für UNIX müssen Anwendungen veröffentlicht sein. Darüber hinaus müssen diese Anwendungen für die Verwendung mit dem Webinterface konfiguriert sein. Weitere Informationen zum Installieren des Citrix XML-Dienstes für UNIX und zum Konfigurieren von Anwendungen für die Verwendung mit dem Webinterface finden Sie in der XenApp für UNIX-Dokumentation.

Mindestanforderungen für die Software

Ohne das aktuelle Release stehen einige neue Funktionen nicht zur Verfügung. Nahtlose Farmmigration ist z. B. nur bei Upgrades auf XenApp 6.0 verfügbar.

In der folgenden Tabelle sind die Mindestsoftwareanforderungen für wichtige Webinterface-Funktionen zusammengefasst.

Hinweis: Weitere Informationen dazu, ob Web Interface 5.4 in bestimmten Releases von Citrix Produkten unterstützt wird, finden Sie in den Systemanforderungen des jeweiligen Produkts.

Webinterface-Funktion	Softwareanforderungen
XenApp-Farm-Migration	Citrix XenApp 6.0
Benutzerroaming	Citrix XenDesktop 4.0 Citrix XenApp 6.0
XenApp VM Hosted Apps	Citrix XenApp 5.0 mit Feature Pack 2
Wiederherstellung im Notfall	Citrix XenDesktop 4.0 Citrix XenApp 5.0 mit Feature Pack 2
Secure Ticket Authority-Redundanz	Citrix XenDesktop 4.0 Citrix XenApp 5.0 mit Feature Pack 2 Citrix Access Gateway 4.6, Standard Edition
Support für Windows 7 und Internet Explorer 8.0	Citrix XenDesktop 4.0 Citrix XenApp 5.0 mit Feature Pack 2 Citrix Online Plug-In 11.2 Citrix Offline Plug-In 5.2
Neustart virtueller Desktops	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
Umleitung spezieller Ordner	Citrix XenApp 5.0 Citrix XenApp Plug-In für gehostete Anwendungen 11.0 für Windows
Schriftartenglättung	Citrix XenApp 5.0 Citrix XenApp Plug-In für gehostete Anwendungen 11.0 für Windows

Unterstützung für XenDesktop	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition 10.250
Support für Windows Vista und Internet Explorer 7.0	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Presentation Server Clients 10.1 für Windows
Unterstützung für Offlineanwendungen	Citrix Presentation Server 4.5 Citrix Streaming Client 1.0 Citrix Program Neighborhood Agent 10.0
ADFS-Unterstützung	Citrix Presentation Server 4.5
Unterstützung für Zugriffssteuerungsrichtlinien	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Access Gateway 4.2 mit Advanced Access Control Citrix MetaFrame Presentation Server Clients für 32-Bit-Windows, Version 9.0
Konto-Self-Service	Citrix Password Manager 4.0
Benutzerseitige Kennwortänderung	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Program Neighborhood Agent 10.1
Sitzungszuverlässigkeit	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Clients für 32-Bit-Windows, Version 9.0
Workspace Control	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Client für 32-Bit-Windows, Version 8.0
Smartcardunterstützung	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 Citrix ICA-Client für 32-Bit-Windows 7.0

Unterstützung für Secure Gateway	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, mit Feature Pack 1, für UNIX-Betriebssysteme Citrix ICA-Client für 32-Bit-Windows 7.0
NDS-Authentifizierung	Citrix Presentation Server 4.5 Citrix ICA-Client für 32-Bit-Windows 7.0
DNS-Adressauflösung	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, mit Feature Pack 1, für UNIX-Betriebssysteme Citrix ICA-Client für 32-Bit-Windows 7.0
Erweitertes Veröffentlichen von Inhalten	Citrix Presentation Server 4.5 Citrix ICA-Client für 32-Bit-Windows 7.0
Load Balancing	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, mit Feature Pack 1, für UNIX-Betriebssysteme
Serverseitige Firewall-Unterstützung	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, mit Feature Pack 1, für UNIX-Betriebssysteme
Clientseitige Firewall-Unterstützung	Citrix ICA-Client für 32-Bit-Windows 7.0
Passthrough-Authentifizierung	Citrix Presentation Server 4.5 Vollständiger Program Neighborhood Client für 32-Bit-Windows Citrix Program Neighborhood Agent 7.0
Remotedesktopverbindung (RDP)	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

Webserveranforderungen

Aktualisiert: 2014-09-24

Für die webbasierte Clientbereitstellung müssen die Citrix Clients auf dem Server vorhanden sein. Weitere Informationen über unterstützte Clientversionen finden Sie unter Benutzergerätanforderungen. Weitere Informationen über das Kopieren der Clients auf den Webinterface-Server finden Sie unter Kopieren der Installationsdateien für Clients zum Webinterface.

Windows-Plattformen

Sie können das Webinterface auf den folgenden Windows-Plattformen installieren:

Betriebssystem	Webserver	Runtime/JDK	Servlet-Engine

Windows Server 2008 R2 x64 Windows Server 2008 R2 mit Service Pack 1	Internetinformationsdienste 7.5	.NET Framework 3.5 mit Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	nicht zutreffend
Windows Server 2008 x64-Editionen mit Service Pack 2 Windows Server 2008 x86 mit Service Pack 2	Internetinformationsdienste 7.0		
Windows Server 2003 R2 x86 mit Service Pack 2 Windows Server 2003 Standard Edition x86 mit Service Pack 2 Windows Server 2003 Enterprise Edition x86 mit Service Pack 2 Windows Server 2003 R2 Standard Edition x86 mit Service Pack 2 Windows Server 2003 R2 Standard Edition x64 mit Service Pack 2	Internet-Informationsdienste 6.0		
Windows Server 2003 Standard Edition x86 mit Service Pack 2	Apache 2.2.*x*	Java 1.6.*x*	Apache Tomcat 6.0.*x*

Wenn Sie Microsoft Internetinformationsdienste (IIS) verwenden möchten, müssen Sie Ihrem Server die entsprechende Serverrolle hinzufügen und IIS und ASP.NET (eine Unterkomponente von IIS) installieren. Wenn IIS bei der Installation von .NET Framework nicht installiert ist, müssen Sie IIS installieren und das Framework erneut installieren. Sie können auch IIS installieren und im Verzeichnis C:\Windows\Microsoft.NET\Framework*Version* den Befehl aspnet_regiis.exe -i ausführen. Die verteilbaren Dateien von .NET Framework und J# sind im Ordner \Support der XenApp- und XenDesktop-Installationsmedien enthalten.

Benutzeranforderungen

Aktualisiert: 2014-05-23

Die folgenden Webbrowser-/Betriebssystem-Kombinationen werden für den Zugriff auf Webinterface-Sites unterstützt:

Browser	Betriebssystem
Internet Explorer 11	Windows 8.1 (32 Bit) Windows 8.1 (64 Bit) Windows 8 (32 Bit) Windows 8 (64 Bit) Windows 2012 (64 Bit) Windows 2012 R2 (64 Bit) Windows 7 (32 Bit) mit Service Pack 1 (SP1) Windows 7 (64 Bit) mit Service Pack 1 (SP1) Windows Server 2008 R2 mit Service Pack 1 (SP1) 64 Bit
Internet Explorer 10	Windows 7 (32 Bit) mit Service Pack 1 (SP1) Windows 7 (64 Bit) mit Service Pack 1 (SP1) Windows Server 2008 R2 mit Service Pack 1 (SP1) 64 Bit
Internet Explorer 9.*x* (32-Bit-Modus)	Windows Vista 32-Bit-Editionen mit Service Pack 2 oder höher Windows Vista 64-Bit-Editionen mit Service Pack 2 oder höher Windows 7 32 Bit RTM oder höher Windows 7 64 Bit RTM oder höher Windows Server 2008 32 Bit mit Service Pack 2 oder höher Windows Server 2008 64 Bit mit Service Pack 2 oder höher Windows Server 2008 R2 (64 Bit)

Internet Explorer 8.*x* (32-Bit-Modus)	Windows 7 64-Bit-Editionen Windows 7 32-Bit-Editionen Windows XP Professional mit Service Pack 3 Windows XP Professional x64 Edition mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Server 2008 R2 Windows Server 2008 mit Service Pack 2 Windows Server 2003 mit Service Pack 2
Internet Explorer 7.*x* (32-Bit-Modus)	Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows Server 2008 mit Service Pack 2 Windows Server 2003 mit 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-Bit-Modus)	Windows 7 64-Bit-Editionen Windows 7 32-Bit-Editionen Windows XP Professional mit Service Pack 3 Windows XP Professional x64 Edition mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Server 2003 mit Service Pack 2
Mozilla Firefox 3.*x*	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x64 Edition mit Service Pack 3 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows 7 32-Bit-Editionen Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003 mit Service Pack 2

Mozilla 1.7	Solaris 10

Hinweis: Web Interface 5.4 wird nur für die Softwareversionen unterstützt, die auf dieser Seite aufgeführt werden. Neuere Softwareversionen funktionieren möglicherweise, wurden aber nicht getestet und werden nicht vom technischen Support unterstützt.

Anforderungen für den Zugriff auf Offlineanwendungen

Folgende Kombinationen von Webbrowsern und Betriebssystemen werden unterstützt, damit Benutzer auf Offlineanwendungen zugreifen können:

Browser	Betriebssystem
Internet Explorer 8.*x* (32-Bit-Modus)	Windows 7 64-Bit-Editionen Windows 7 32-Bit-Editionen Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows XP Professional x64 Edition mit Service Pack 2 Windows XP Professional mit Service Pack 3 Windows Server 2008 R2 Windows Server 2008 x64-Editionen mit Service Pack 2 Windows Server 2008 mit Service Pack 2 Windows Server 2003 x64-Editionen mit Service Pack 2 Windows Server 2003 mit Service Pack 2
Internet Explorer 7.*x* (32-Bit-Modus)	Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows XP Professional x64 Edition mit Service Pack 2 Windows XP Professional mit Service Pack 3 Windows Server 2008 x64-Editionen mit Service Pack 2 Windows Server 2008 mit Service Pack 2 Windows Server 2003 x64-Editionen mit Service Pack 2 Windows Server 2003 mit Service Pack 2

Mozilla Firefox 3.*x*	Windows 7 64-Bit-Editionen Windows 7 32-Bit-Editionen Windows Vista 64-Bit-Editionen mit Service Pack 2 Windows Vista 32-Bit-Editionen mit Service Pack 2 Windows XP Professional x64 Edition mit Service Pack 2 Windows XP Professional mit Service Pack 3 Windows Server 2003 mit Service Pack 2

Anforderungen für andere Benutzergeräte

Benutzer können von Thin Clients, Personal Digital Assistants (PDAs) und Handheld-Geräten mit den folgenden Konfigurationen auf das Webinterface zugreifen:

Gerät	Betriebssystem	Browser
iPhone	nicht zutreffend	Safari 5.*x*
iPad	nicht zutreffend	Safari 5.*x*
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSE V90	Windows XP Embedded mit 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-Browser

Benutzergerätanforderungen

Für das Zusammenspiel mit dem Webinterface muss mindestens ein unterstützter Citrix Client oder ein unterstützter Webbrowser mit Java Runtime Environment auf den Benutzergeräten installiert sein. Alle auf den XenApp- und XenDesktop-Installationsmedien enthaltenen Clients sind mit dem Webinterface kompatibel. Die Clients können auch kostenlos von der Citrix Website heruntergeladen werden.

Citrix empfiehlt die Bereitstellung der neuesten Clients, damit die Benutzer die neuesten Funktionen nutzen können. Jeder Client bietet andere Funktionen und Merkmale. Weitere Informationen zu den unterstützten Clientfunktionen finden Sie in der Administratordokumentation des entsprechenden Clients.

Installieren des Webinterface

Das Webinterface wird vom XenApp- oder XenDesktop-Installationsmedium installiert.

Sie können das Webinterface auf den folgenden Plattformen installieren:

- Unterstütztes Windows-Betriebssystem mit folgenden Komponenten:
  - Microsoft Internetinformationsdienste (IIS)
  - Apache Tomcat
- Unterstütztes UNIX-Betriebssystem mit folgenden Komponenten:
  - Apache Tomcat
  - IBM WebSphere
  - Sun GlassFish Enterprise Server

Weitere Informationen zur Installation des Webinterface finden Sie unter Webserveranforderungen.

Durch Befehlszeilenskripte können Sie unbeaufsichtigte Installationen und Siteverwaltung ausführen. Weitere Informationen zur Verwendung der Befehlszeile mit dem Webinterface finden Sie im Knowledge Center.

Weitere Informationen zur Installation des Webinterface finden Sie unter So installieren Sie das Webinterface in Microsoft Internetinformationsdienste und Installieren des Webinterface auf Java-Anwendungsservern.

Sicherheitsüberlegungen

Wenn Sie das Webinterface auf einem Windows-Server installieren möchten, empfiehlt Citrix, dass Sie den Standardrichtlinien von Microsoft zur Konfiguration von Windows-Servern folgen. Für UNIX-Implementierungen sollten Sie die Empfehlungen des Herstellers für das entsprechende Betriebssystem einhalten.

Anzeigen der Citrix XML-Dienst-Portzuordnung

Beim Erstellen der Webinterface-Site (IIS) oder der WAR-Datei (Java) werden Sie aufgefordert, den Port anzugeben, den der Citrix XML-Dienst verwendet. Der Citrix XML-Dienst ist die Kommunikationsverbindung zwischen der Serverfarm und dem Webinterface-Server.

Auf Windows-Plattformen können Sie den Citrix XML-Dienst so konfigurieren, dass er denselben TCP/IP-Port wie Internetinformationsdienste verwendet. Wenn dies der Fall ist, müssen Sie den Port suchen, den der WWW-Dienst von Internetinformationsdienste verwendet, um den Port für den Citrix XML-Dienst zu ermitteln. Der WWW-Dienst verwendet standardmäßig Port 80. Wenn Sie einen dedizierten Port für den Citrix XML-Dienst benötigen, empfiehlt Citrix Port 8080.

Geben Sie auf Windows-Plattformen an einer Eingabeaufforderung netstat -a ein, um eine Liste der verwendeten Ports zu erhalten. Geben Sie auf Servern mit XenApp für UNIX an der Eingabeaufforderung ctxnfusesrv -l ein, um die Portinformationen anzuzeigen.

Hinweis: Falls erforderlich, können Sie den vom Citrix XML-Dienst verwendeten Port auf dem Server ändern. Weitere Informationen finden Sie in der Dokumentation für den Citrix Server.

So installieren Sie das Webinterface in Microsoft Internetinformationsdienste

Bevor Sie das Webinterface installieren, müssen Sie Ihren Server konfigurieren, um die Webserverrolle hinzuzufügen, und IIS und ASP.NET installieren.

Wenn Sie IIS 7.*x* unter Windows Server 2008 verwenden möchten, installieren Sie die Rolle Webserver (IIS) und aktivieren Sie dann die folgenden Rollendienste:

- Webserver > Anwendungsentwicklung > ASP.NET
- Verwaltungsprogramme > IIS 6-Verwaltungskompatibilität > IIS 6-Metabasiskompatibilität

Wenn Sie Passthrough-, Passthrough-mit-Smartcard- und/oder Smartcard-Authentifizierung aktivieren möchten, müssen Sie außerdem die folgenden Rollendienste installieren:

- Aktivieren Sie für die Passthrough- und Passthrough-mit-Smartcard-Authentifizierung Webserver > Sicherheit > Windows-Authentifizierung.
- Aktivieren Sie für Smartcard-Authentifizierung Webserver > Sicherheit > Clientzertifikatzuordnung-Authentifizierung.

Wenn Sie IIS 6.0 unter Windows Server 2003 verwenden möchten, fügen Sie die Rolle Anwendungsserver (IIS, ASP.NET) hinzu und aktivieren Sie ASP.NET.

In IIS wird jede Site einem Anwendungspool zugeordnet. Die Konfiguration des Anwendungspools enthält eine Einstellung, die die Höchstanzahl von Arbeiterprozessen festlegt. Wenn Sie den Standardwert "1" ändern, können Sie das Webinterface unter Umständen nicht ausführen.

Nachdem Sie die Serverrolle konfiguriert haben, müssen Sie sicherstellen, dass .NET Framework 3.5 mit Service Pack 1 und Visual J#.NET 2.0 Second Edition installiert sind.

Wenn Sie ein Upgrade von einer früheren Version des Webinterface, bis einschließlich Version 4.5, vornehmen, fordert das Installationsprogramm Sie zum Sichern Ihrer Sites auf, bevor diese aktualisiert werden.

Wichtig: Zentral konfigurierte Sites und Conferencing Manager-Gastteilnehmersites werden nicht mehr unterstützt. Wenn Sie von einer früheren Webinterface-Version aktualisieren, entfernt das Installationsprogramm die Conferencing Manager-Gastteilnehmersites von Ihrem Webserver. Vorhandene zentral konfigurierte Sites werden aktualisiert und zu Sites mit lokaler Konfiguration konvertiert.

1. Melden Sie sich als Administrator an.

   Wenn Sie das Webinterface vom XenApp- oder XenDesktop-Installationsmedium installieren, legen Sie die Disk in das Laufwerk des Webservers ein.

Wenn Sie das Webinterface von der Citrix Website heruntergeladen haben, kopieren Sie die Datei WebInterface.exe auf Ihren Webserver.

2. Navigieren Sie zur Datei WebInterface.exe und doppelklicken Sie darauf.

3. Wählen Sie eine Sprache aus der Liste aus. Als Standardauswahl wird die Sprache des Betriebssystems angezeigt. Klicken Sie auf OK.

4. Klicken Sie auf der Seite Willkommen auf Weiter.

5. Wählen Sie auf der Seite Lizenzvereinbarung die Option Ich stimme der Lizenzvereinbarung zu und klicken Sie auf Weiter.

6. Gehen Sie auf der Seite Installationsordner zu dem Verzeichnis, in dem das Webinterface installiert werden soll (der Standard ist C:\Programme (x86)\Citrix\Web Interface\). Klicken Sie auf Weiter.

7. Wählen Sie auf der Seite Speicherort der Clients die Option Clients auf diesen Computer kopieren. Klicken Sie auf Durchsuchen, um das Installationsmedium oder das Netzwerk nach Citrix Client-Setupdateien zu durchsuchen.

   Das Setup kopiert den Inhalt des Ordners \Citrix Receiver and Plug-Ins auf dem Installationsmedium oder einer Netzfreigabe in den Webinterface-Ordner \Clients; üblicherweise ist dies C:\Programme (x86)\Citrix\Web Interface*Version*\Clients. Für alle während der Installation erstellten Websites wird angenommen, dass der Webserver die Client-Dateien in dieser Verzeichnisstruktur enthält.

   Wenn die Clients nicht während der Webinterface-Installation auf den Webserver kopiert werden sollen, wählen Sie Diesen Schritt überspringen. Sie können die Clients auch später noch auf den Server kopieren.

8. Klicken Sie auf Weiter, um fortzufahren, und klicken Sie erneut auf Weiter, um zu bestätigen, dass Sie mit der Installation beginnen möchten.

9. Wenn die Installation abgeschlossen ist, klicken Sie auf Fertig stellen.

10. Klicken Sie im Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung, um auf die Citrix Webinterface Management Console zuzugreifen und mit der Erstellung von Sites zu beginnen.

Kompatibilität mit anderen Komponenten auf Windows Server 2003 x64-Editionen

Bei der Installation des Webinterface für Microsoft Internetinformationsdienste auf 64-Bit-Versionen von Windows Server 2003 wird Unterstützung für 32-Bit-Weberweiterungen in IIS 6.0 aktiviert, was die Unterstützung von 64-Bit-Erweiterungen deaktiviert. Wenn Sie das Webinterface für Microsoft Internetinformationsdienste auf einer 64-Bit-Version von Windows Server 2003 installieren, installieren Sie das Webinterface als erste Komponente vor aller anderen Citrix Software, einschließlich XenApp, XenDesktop und der License Management Console. Durch diese Installationsreihenfolge können die Produkte 32-Bit-Unterstützung in IIS 6.0 übernehmen. Wenn Sie diese Produkte in der falschen Reihenfolge installieren, treten beim Zugriff auf dem Webserver u. U. Fehlermeldungen auf, z. B. "Dienst nicht verfügbar".

Wenn das Webinterface für Microsoft Internetinformationsdienste unter 64-Bit-Windows-Server-Betriebssystemen installiert ist, kann es zu Kompatibilitätsproblemen mit Produkten kommen, die 64-Bit-ISAPI-Filter benötigen, z. B. die Windows-Komponente RPC-über-HTTP-Proxy. Sie müssen den RPC-über-HTTP-Proxy vor der Installation des Webinterface deinstallieren.

So deinstallieren Sie RPC-über-HTTP-Proxy

1. Klicken Sie im Windows-Menü Start auf Systemsteuerung > Software.
2. Wählen Sie Windows-Komponenten hinzufügen/entfernen.
3. Wählen Sie Netzwerkdienste und klicken Sie auf Details.
4. Aktivieren Sie das Kontrollkästchen RPC-über-HTTP-Proxy und klicken Sie auf OK.
5. Klicken Sie auf Weiter, um den RPC-über-HTTP-Proxy zu deinstallieren, und starten Sie den Server neu.

Installieren des Webinterface auf Java-Anwendungsservern

Hinweis: Wenn Sie das Webinterface unter IBM WebSphere installieren, wird eine Anwendungssicherheitswarnung angezeigt, die auf ein Problem mit dem Inhalt der Datei was.policy hinweist. Hierbei handelt es sich um eine von WebSphere erstellte Richtliniendatei, wenn Sie unter Security > Global Security die Option Enforce Java 2 Security auswählen. Stellen Sie sicher, dass Sie die Datei was.policy entsprechend der WebSphere Java 2-Sicherheitsrichtlinie modifizieren. Andernfalls funktioniert das Webinterface eventuell nicht ordnungsgemäß. Diese Richtliniendatei wird in folgendem Ordner gespeichert: WEBSPHERE_HOME/AppServer/installedApps/*Knotenname*/*Name der WAR-Datei*.ear/META-INF.

Das Webinterface benötigt auf Java-Anwendungsservern eine Servlet-Engine. Der Apache-Webserver benötigt für die Webinterface-Unterstützung eine zusätzliche Servlet-Engine (z. B. Tomcat). Tomcat kann als eigenständiger Webserver oder als Servlet-Engine verwendet werden.

So installieren Sie das Webinterface unter Tomcat

1. Kopieren Sie die Datei WebInterface.jar aus dem Verzeichnis "Web Interface" auf dem Installationsmedium an einen temporären Speicherort.

2. Navigieren Sie von einer Eingabeaufforderung zu dem Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben, und führen Sie das Installationsprogramm aus, indem Sie java -jar WebInterface.jar eingeben.

3. Drücken Sie zum Lesen der Lizenzvereinbarung die Eingabetaste.

4. Geben Sie J ein, um die Lizenzvereinbarung zu akzeptieren.

5. Wählen Sie einen Sitetyp aus der Liste aus.

6. Geben Sie die Erstkonfiguration für die Site an, indem Sie die Fragen, die auf dem Bildschirm angezeigt werden, beantworten.

7. Es wird eine Zusammenfassung der ausgewählten Optionen angezeigt. Wenn die Siteangaben richtig sind, geben Sie J ein, um die WAR-Datei zu erstellen. Die WAR-Datei wird erstellt und die Citrix Clients werden falls erforderlich vom Installationsmedium kopiert.

8. Folgen Sie den Anweisungen auf dem Bildschirm, um die Installation der WAR-Datei abzuschließen.

So konfigurieren Sie die Sicherheitsrichtlinie auf Sun GlassFish Enterprise Server

Bevor Sie XenApp Web-Sites mit Konto-Self-Service auf einem Server mit Sun GlassFish Enterprise Server erstellen können, müssen Sie die Sicherheitsrichtlinien des Servers manuell konfigurieren.

1. Stellen Sie die WAR-Datei der Site auf dem Server bereit.

2. Halten Sie den Webserver an.

3. Bearbeiten Sie die Datei server.policy im bereitgestellten Domänenkonfigurationsverzeichnis. Beispiel: Wenn Sun GlassFish Enterprise Server unter *Stammverzeichnis von SunGlassFishEnterpriseServer*/AppServer installiert ist und die Site in "Domäne1" bereitgestellt wird, befindet sich die Datei unter *Stammverzeichnis von SunGlassFishEnterpriseServer*/AppServer/domains/Domäne1/config.

4. Fügen Sie die folgende Konfiguration vor allen allgemeinen Berechtigungsblöcken hinzu:

   ```
   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";
   };
   ```

   Name der WAR-Datei ist der erste Teil des Dateinamens der WAR-Datei Ihrer Site, z. B. "XenApp".

5. Bearbeiten Sie die Datei launcher.xml, die sich unter *Stammverzeichnis von SunGlassFishEnterpriseServer*/Anwendungsserver/lib befindet, um javax.wsdl der Liste der Werte im Element sysproperty key="com.sun.enterprise.overrideablejavaxpackages" hinzuzufügen.

6. Starten Sie den Webserver.

Verwenden von Sprachpaketen

Sprachpakete enthalten alle für die Lokalisierung von Sites erforderlichen Informationen für eine bestimmte Sprache (Chinesisch (traditionell und vereinfacht), Deutsch, Englisch, Französisch, Japanisch, Koreanisch, Russisch und Spanisch). Sie enthalten u. a. folgende Komponenten:

- Ressourcendateien für Sites
- Benutzerhilfe
- Lokalisierte Symbole und Bilder

In IIS können Sie Webinterface-Installationen Sprachpakete hinzufügen, indem Sie die Struktur kopieren oder die Dateien im Ordner \languages entpacken, das sich üblicherweise hier befindet: C:\Programme (x86)\Citrix\Web Interface*Version*\languages. Um die Sprache für eine bestimmte Site anzupassen, kopieren Sie das Sprachpaket in den Speicherort der Site und ändern Sie es. Die Site verwendet anschließend das geänderte Sprachpaket, während andere Sites weiter auf das Standardpaket zugreifen.

Hinweis: Damit Windows-Fehlermeldungen in IIS in der richtigen Sprache angezeigt werden, müssen Sie das entsprechende Sprachpaket für Microsoft .NET Framework installieren.

Auf Java-Anwendungsservern können Sie weitere Sprachpakete installieren, indem Sie sie in das entsprechende Verzeichnis auf der Site verschieben und die Dateien extrahieren.

Das englische Sprachpaket wird als Fallback-Sprache verwendet und muss immer auf dem Server vorhanden sein. Sprachpakete sind speziell auf die jeweilige Webinterface-Version, mit der sie geliefert werden, abgestimmt und können nicht mit niedrigeren oder höheren Versionen verwendet werden. Weitere Informationen zur Verwendung von Sprachpaketen finden Sie im Webinterface-SDK.

Entfernen von Sprachpaketen

Manche Geräte, z. B. solche, auf denen Windows CE ausgeführt wird, können bestimmte Sprachen nicht anzeigen (z. B. Japanisch). In diesem Fall werden in der Benutzeroberfläche in der Dropdownliste zum Auswählen der Sprache für nicht verfügbare Sprachen Quadrate angezeigt. Wenn Sie dies vermeiden möchten, können Sie eine Sprache für alle oder für bestimmte Sites entfernen.

Entfernen Sie für Sites in IIS *Sprachcode*.lang (z. B. de.lang) aus dem Verzeichnis \languages, das sich üblicherweise hier befindet: C:\Programme (x86)\Citrix\Web Interface*Version*\languages. Die Sprache wird hiermit aus allen Sites auf dem Server entfernt. Wenn Sie diese Sprache für eine bestimmte Site aktivieren möchten, verschieben Sie die LANG-Datei in das Verzeichnis \languages der Site.

Öffnen Sie für Sites auf Java-Anwendungsservern mit einem entsprechenden Tool die WAR-Datei, nachdem Sie sie erstellt haben, entfernen Sie die LANG-Datei und packen Sie die WAR-Datei erneut. Die Sprache wird hiermit von allen Sites entfernt, die mit dieser WAR-Datei bereitgestellt werden.

Aktualisieren einer bestehenden Installation

Sie können ab Version 4.5 auf die neueste Version des Webinterface aktualisieren, indem Sie das Webinterface entweder vom XenApp- oder XenDesktop-Installationsmedium oder mit aus dem Internet heruntergeladenen Dateien installieren.

Sie können das Webinterface nicht auf eine frühere Version zurückstufen.

Wichtig: Zentral konfigurierte Sites und Conferencing Manager-Gastteilnehmersites werden nicht mehr unterstützt. Wenn Sie von einer früheren Webinterface-Version aktualisieren, entfernt das Installationsprogramm die Conferencing Manager-Gastteilnehmersites von Ihrem Webserver. Vorhandene zentral konfigurierte Sites werden aktualisiert und zu Sites mit lokaler Konfiguration konvertiert.

Die Verzeichnisstruktur des Ordners \Clients, der für die webbasierte Bereitstellung von Clients für Benutzer verwendet wird, ist anders als in Version 5.1 und früheren Versionen des Webinterface. Wenn Sie Ihre Webinterface-Installation mit dem XenApp- oder XenDesktop-Installationsmedium aktualisieren, kopieren Sie die Verzeichnisstruktur vom Installationsmedium. Wenn Sie das Upgrade mit einem Webdownload durchführen, müssen Sie die erforderliche Verzeichnisstruktur für Ihre Webinterface-Installation manuell erstellen. Dann können Sie die gewünschten Clients von der Citrix Website herunterladen. Weitere Informationen zum Verzeichnis \Clients finden Sie unter Kopieren der Installationsdateien für Clients zum Webinterface.

Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Clientinstallationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Clients von der Citrix Website herunterladen oder Sie ältere Clients bereitstellen möchten, überprüfen Sie, ob in den Konfigurationsdateien für Ihre XenApp Web-Sites die richtigen Namen der Clientinstallationsdateien für die Parameter ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 und ClientStreamingWin32 angegeben sind. Weitere Informationen zu den Parametern in Webinterface-Konfigurationsdateien finden Sie unter WebInterface.conf-Parameter.

Nächste Schritte

Nach der Installation müssen Sie den Benutzern das Webinterface bereitstellen. Hierzu verwenden Sie entweder die Citrix Webinterface Management Console, um Sites zu erstellen und zu konfigurieren, oder Sie bearbeiten direkt die Konfigurationsdatei WebInterface.conf.

Darüber hinaus müssen Sie das Webinterface ggf. konfigurieren, um mit anderen installierten Komponenten zusammenzuarbeiten. Sie können die Funktionen des Webinterface auch anpassen oder erweitern.

- Informationen zur Konfiguration des Webinterface mit der Konsole oder der Datei WebInterface.conf finden Sie unter Konfigurieren von Sites mit der Citrix Webinterface Management Console oder Konfigurieren von Sites mit Konfigurationsdateien.
- Informationen zur Konfiguration des Webinterface für Access Gateway oder Secure Gateway mit der Citrix Webinterface Management Console finden Sie unter So konfigurieren Sie Gateway-Einstellungen.
- Informationen zur Konfiguration des Webinterface für die Verwendung von ADFS finden Sie unter Konfigurieren der ADFS-Unterstützung für das Webinterface.
- Informationen zu den Sicherheitsüberlegungen finden Sie unter Konfigurieren der Webinterface-Sicherheit.
- Weitere Informationen zur Erweiterung und Anpassung der Webinterface-Funktionalität finden Sie im Webinterface-SDK.

Problembehandlung bei der Installation des Webinterface

Auf Windows-Plattformen mit IIS können Sie mit der Option Reparieren Probleme bei der Webinterface-Installation beheben. Wenn das Problem nicht mit der Option Reparieren behoben wird oder die Option nicht zur Verfügung steht (z. B. auf Java-Anwendungsserverinstallationen), deinstallieren und installieren Sie das Webinterface neu. Weitere Informationen finden Sie unter Deinstallieren des Webinterface. Nach der Neuinstallation des Webinterface müssen Sie alle Sites neu erstellen.

Verwenden der Option "Reparieren"

Sollten Probleme bei der Webinterface-Installation auftreten, versuchen Sie, das Problem mit der Option Reparieren zu beheben. Mit der Option Reparieren werden gemeinsame Dateien neu installiert. Bestehende Sites werden nicht repariert oder ersetzt.

Wichtig: Wenn Ihre Webinterface-Installation benutzerdefinierten Code enthält und Sie die Option Reparieren wählen, wird der angepasste Code entfernt. Citrix empfiehlt, alle angepassten Dateien zu sichern, bevor Sie diese Option verwenden.

1. Doppelklicken Sie auf die Datei WebInterface.exe.
2. Wählen Sie Reparieren und klicken Sie auf Weiter.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

Deinstallieren des Webinterface

Bei der Deinstallation des Webinterface werden alle Webinterface-Dateien entfernt, einschließlich des Ordners \Clients. Kopieren Sie Webinterface-Dateien, die Sie behalten möchten, vor der Deinstallation des Webinterface in ein anderes Verzeichnis.

Gelegentlich schlägt die Deinstallation des Webinterface fehl. Mögliche Ursachen:

- Unzureichender Registrierungszugriff für das Deinstallationsprogramm
- IIS wurde nach der Webinterface-Installation vom System entfernt

So deinstallieren Sie das Webinterface in Microsoft Internetinformationsdienste

1. Klicken Sie im Windows-Menü Start auf Systemsteuerung > Programme und Funktionen.
2. Wählen Sie Citrix Webinterface und klicken Sie auf Deinstallieren.
3. Folgen Sie den Anweisungen auf dem Bildschirm.

So deinstallieren Sie das Webinterface auf Java-Anwendungsservern

Wenn Ihr Webserver ein Tool für die Deinstallation von Webanwendungen enthält, führen Sie die vom Hersteller empfohlenen Schritte aus, um das Webinterface zu deinstallieren. Sie können das Webinterface auch manuell deinstallieren.

1. Navigieren Sie von einer Eingabeaufforderung in das Verzeichnis, in das Sie ursprünglich die WAR-Datei kopiert haben.
2. Halten Sie den Webserver an und löschen Sie die WAR-Datei.

   Sie müssen ggf. auch das Verzeichnis löschen, in das die WAR-Datei extrahiert wurde. Normalerweise haben diese Verzeichnisse denselben Namen wie die WAR-Datei und befinden sich auch in demselben Verzeichnis. Beispiel: Der Inhalt der Datei MeineSite.war wird in das Verzeichnis /mysite extrahiert.

   Hinweis: Wenn Sie das Webinterface deinstallieren, bleiben eventuell einige Dateien auf dem Server zurück. Weitere Informationen über die verbleibenden Dateien finden Sie in der Datei Citrix XenApp-Readme.

Erste Schritte mit dem Webinterface

Aktualisiert: 2014-11-24

Auswählen einer Konfigurationsmethode

Sie können das Webinterface mit der Citrix Webinterface Management Console oder mit den Konfigurationsdateien konfigurieren und anpassen.

Verwenden der Citrix Webinterface Management Console

Die Citrix Webinterface Management Console ist ein Snap-In für die Microsoft Management Console (MMC) 3.0, mit dem Sie in Microsoft Internetinformationsdienste (IIS) gehostete XenApp Web- und XenApp Services-Sites erstellen und konfigurieren können. Webinterface-Sitetypen werden im linken Bereich angezeigt. Der Ergebnisbereich in der Mitte zeigt die verfügbaren Sites für den im linken Bereich ausgewählten Sitetyp an.

Mit der Citrix Webinterface Management Console können Sie alltägliche Verwaltungsaufgaben schnell und einfach ausführen. Im Bereich Aktionen werden die zurzeit verfügbaren Aufgaben aufgeführt. Im oberen Bereich werden Aufgaben für Objekte, die im linken Bereich ausgewählt sind, angezeigt und darunter werden Aufgaben für Objekte angezeigt, die im Ergebnisbereich ausgewählt sind.

Konfigurationsänderungen in der Konsole werden wirksam, wenn Sie sie anwenden. Daher werden ggf. einige Einstellungen des Webinterface deaktiviert, wenn deren Werte für die aktuelle Konfiguration nicht relevant sind. Die entsprechenden Einstellungen werden auf die Standardwerte in WebInterface.conf zurückgesetzt. Citrix empfiehlt, regelmäßig Sicherungskopien von den Dateien WebInterface.conf und config.xml für Ihre Sites zu erstellen.

Die Citrix Webinterface Management Console wird bei der Installation des Webinterface für Microsoft Internetinformationsidenste automatisch installiert. Starten Sie die Konsole, indem Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Webinterface Management Console klicken.

Hinweis: Sie müssen sicherstellen, dass MMC 3.0 auf dem Server vorhanden ist, auf dem Sie das Webinterface installieren, da dies eine Voraussetzung für die Installation der Citrix Webinterface Management Console ist. MMC 3.0 ist standardmäßig auf allen Windows-Plattformen vorhanden, die die Verwendung des Webinterface unterstützen.

Verwenden von Konfigurationsdateien

Sie können die folgenden Konfigurationsdateien bearbeiten, um Webinterface-Sites zu konfigurieren.

- **Webinterface-Konfigurationsdatei:** Mit der Konfigurationsdatei WebInterface.conf können Sie viele Webinterface-Eigenschaften ändern. Die Datei steht unter Microsoft Internetinformationsdienste und auf Java-Anwendungsservern zur Verfügung. Mithilfe dieser Datei können Sie gängige Verwaltungsaufgaben ausführen und zahlreiche Einstellungen anpassen. Bearbeiten Sie die Werte in der Datei WebInterface.conf und speichern Sie die aktualisierte Datei, um die Änderungen zu übernehmen. Weitere Informationen zur Webinterface-Konfiguration mit WebInterface.conf finden Sie unter Konfigurieren von Sites mit der Konfigurationsdatei.

- **Citrix Online Plug-In-Konfigurationsdatei:** Sie können das Citrix Online Plug-In mit der Datei config.xml auf dem Webinterface-Server konfigurieren.

Erstellen von Sites auf Java-Anwendungsservern

Führen Sie das Installationsprogramm für das Webinterface auf Java-Anwendungsservern aus, um neue Sites zu erstellen. Das Installationsprogramm erstellt eine individuelle WAR-Datei für die Site, die dann installiert wird (üblicherweise indem die WAR-Datei im richtigen Speicherort für die Servlet-Engine abgelegt wird). Sie können Sites ändern, indem Sie den Inhalt der entpackten WAR-Datei bearbeiten, und Sites entfernen, indem Sie die WAR-Datei löschen.

Konfigurieren von Sites mit der Citrix Webinterface Management Console

Die Citrix Webinterface Management Console ist ein Snap-In für die Microsoft Management Console (MMC) 3.0, mit dem Sie in Microsoft Internetinformationsdienste (IIS) gehostete XenApp Web- und XenApp Services-Sites erstellen und konfigurieren können. Webinterface-Sitetypen werden im linken Bereich angezeigt. Der Ergebnisbereich in der Mitte zeigt die verfügbaren Sites für den im linken Bereich ausgewählten Sitetyp an.

Mit der Citrix Webinterface Management Console können Sie alltägliche Verwaltungsaufgaben schnell und einfach ausführen. Im Bereich Aktionen werden die zurzeit verfügbaren Aufgaben aufgeführt. Im oberen Bereich werden Aufgaben für Objekte, die im linken Bereich ausgewählt sind, angezeigt und darunter werden Aufgaben für Objekte angezeigt, die im Ergebnisbereich ausgewählt sind.

Konfigurationsänderungen in der Konsole werden wirksam, wenn Sie sie anwenden. Daher werden ggf. einige Einstellungen des Webinterface deaktiviert, wenn deren Werte für die aktuelle Konfiguration nicht relevant sind. Die entsprechenden Einstellungen werden auf die Standardwerte in WebInterface.conf zurückgesetzt. Citrix empfiehlt, regelmäßig Sicherungskopien von den Dateien WebInterface.conf und config.xml für Ihre Sites zu erstellen.

Die Citrix Webinterface Management Console wird bei der Installation des Webinterface für Microsoft Internetinformationsidenste automatisch installiert. Starten Sie die Konsole, indem Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Webinterface Management Console klicken.

Hinweis: Sie müssen sicherstellen, dass MMC 3.0 auf dem Server vorhanden ist, auf dem Sie das Webinterface installieren, da dies eine Voraussetzung für die Installation der Citrix Webinterface Management Console ist. MMC 3.0 ist standardmäßig auf allen Windows-Plattformen vorhanden, die die Verwendung des Webinterface unterstützen.

Konfigurieren von Sites mit Konfigurationsdateien

Sie können die folgenden Konfigurationsdateien bearbeiten, um Webinterface-Sites zu konfigurieren.

- **Webinterface-Konfigurationsdatei:** Mit der Konfigurationsdatei WebInterface.conf können Sie viele Webinterface-Eigenschaften ändern. Die Datei steht unter Microsoft Internetinformationsdienste und auf Java-Anwendungsservern zur Verfügung. Mithilfe dieser Datei können Sie gängige Verwaltungsaufgaben ausführen und zahlreiche Einstellungen anpassen. Bearbeiten Sie die Werte in der Datei WebInterface.conf und speichern Sie die aktualisierte Datei, um die Änderungen zu übernehmen. Weitere Informationen zur Webinterface-Konfiguration mit WebInterface.conf finden Sie unter Konfigurieren von Sites mit der Konfigurationsdatei.

- **Citrix Online Plug-In-Konfigurationsdatei:** Sie können das Citrix Online Plug-In mit der Datei config.xml auf dem Webinterface-Server konfigurieren.

Gemeinsam verwendete Konfiguration

Für in IIS gehostete Sites können Sie festlegen, dass eine Webinterface-Site ihre Konfiguration von einer "Mastersite" erhält, die Sie so konfiguriert haben, dass ihre Konfigurationsdateien über das Netzwerk gemeinsam genutzt werden können. Nachdem Sie die entsprechenden Dateiberechtigungen eingerichtet haben, können Sie es anderen Sites ermöglichen, die Konfiguration der Mastersite zu verwenden, indem Sie in der Datei bootstrap.conf der lokalen Site den absoluten Pfad zur Konfigurationsdatei der Mastersite (WebInterface.conf) angeben. Bei XenApp Services-Sites, die Konfigurationen gemeinsam verwenden, versucht das Webinterface auch, die Konfigurationsdatei des Citrix Online Plug-Ins (config.xml) zu lesen, die sich im selben Verzeichnis wie WebInterface.conf befindet.

Nachdem Sie eine Site für gemeinsame Verwendung der Konfigurationsdatei konfiguriert haben, können Sie die Konfiguration der Site nicht mehr direkt bearbeiten. Stattdessen müssen Sie die Konfiguration der Mastersite mit der Konsole ändern oder die Konfigurationsdateien auf dem Webserver, auf dem die Mastersite gehostet wird, bearbeiten. Alle Änderungen der Konfiguration der Mastersite wirken sich auch auf alle anderen Sites aus, die diese Konfiguration verwenden. Gemeinsam verwendete Konfigurationen sind nicht verfügbar für Sites, die auf Java-Anwendungsservern gehostet werden.

So geben Sie Sitekonfigurationen frei

1. Richten Sie die entsprechenden Dateifreigabeberechtigungen ein, um den Zugriff über das Netzwerk auf den Ordner \conf (normalerweise C:\inetpub\wwwroot\Citrix*Sitename*\conf) der Hauptsite und auf die Sitekonfigurationsdatei (WebInterface.conf) zu ermöglichen, die normalerweise im Ordner \conf gespeichert ist. Für XenApp Services-Mastersites müssen Sie dieselben Berechtigungen einrichten wie für die Citrix Online Plug-In-Konfigurationsdatei (config.xml), die normalerweise im Ordner \conf der Site ist.

2. Öffnen Sie mit einem Texteditor die Datei bootstrap.conf (normalerweise im Ordner \conf) der Site, die die freigegebene Konfiguration verwenden soll.

3. Ändern Sie den Parameter ConfigurationLocation, um den absoluten Netzwerkpfad zur Konfigurationsdatei der Mastersite anzugeben, z. B.:

   ConfigurationLocation=*ServerName**ShareName*\WebInterface.conf

Erstellen einer Site in Microsoft Internetinformationsdienste

Mit der Aufgabe Site erstellen in der Citrix Webinterface Management Console können Sie folgende Sitetypen erstellen:

- **XenApp Web-Sites:** Für Benutzer, die mit einem Webbrowser auf Ressourcen zugreifen.
- **XenApp Services-Sites:** Für Benutzer, die mit dem Citrix Online Plug-In auf Ressourcen zugreifen.

Sie können mit dieser Aufgabe verschiedene Informationen für die Site angeben: den IIS-Speicherort, von dem die Site gehostet wird, die URL zum Übernehmen von Änderungen und die Authentifizierungseinstellungen für die Site. Diese Einstellungen können Sie später mit den Aufgaben unter Sitewartung aktualisieren. Sie müssen ein lokaler Administrator auf dem System sein, auf dem das Webinterface ausgeführt wird, um Sites erstellen zu können.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf den Container Citrix Webinterface.
3. Klicken Sie im Bereich Aktionen auf Site erstellen.
4. Wählen Sie den Sitetyp aus, den Sie erstellen möchten.
5. Geben Sie die URL und einen Namen für die Site an.
6. Folgen Sie den Anweisungen auf dem Bildschirm, um die Site zu erstellen.

Hosting mit Microsoft Internetinformationsdienste

Mit der Aufgabe IIS-Hosting verwalten unter Sitewartung in der Citrix Webinterface Management Console ändern Sie den Speicherort der Webinterface-Site in IIS.

Festlegen des Authentifizierungspunkts

Aktualisiert: 2014-12-02

Wenn Sie mit der Citrix Webinterface Management Console eine XenApp Web-Site erstellen, müssen Sie den *Authentifizierungspunkt* festlegen. Dies ist der Punkt, an dem die Benutzerauthentifizierung stattfindet.

Authentifizierung am Webinterface

Für die Benutzerauthentifizierung am Webinterface stehen verschiedene integrierte Authentifizierungsmethoden zur Verfügung, einschließlich expliziter, Passthrough- und Smartcard-Authentifizierung. Weitere Informationen über Webinterface-Authentifizierungsmethoden finden Sie unter Konfigurieren der Authentifizierung für das Webinterface.

Authentifizierung an einem ADFS-Kontopartner

Sie können den Kontopartner einer ADFS-Bereitstellung aktivieren, um auf XenApp-Anwendungen zuzugreifen. Hierdurch können Sie Benutzern auf dem Kontopartner Zugriff auf Anwendungen geben.

Wenn Sie vorhaben, Sites mit ADFS-Integration zu erstellen, sollten Sie sich folgender Aspekte bewusst sein:

- XenDesktop unterstützt ADFS-Authentifizierung nicht.
- ADFS-Unterstützung ist mit dem Webinterface für Java-Anwendungsserver nicht verfügbar.
- Der Client für Java und eingebettete Remotedesktopverbindungssoftware (RDP) werden nicht für den Zugriff auf mit ADFS integrierte Sites unterstützt.
- Sites mit ADFS-Integration unterstützen nur die Authentifizierung mit ADFS. Andere Authentifizierungsmethoden werden nicht unterstützt.
- Wenn eine Site mit ADFS-Integration erstellt wurde, können Sie deren Konfiguration nicht mehr ändern, um anstelle von ADFS integrierte Authentifizierung oder Authentifizierung mit Access Gateway zu verwenden.

Weitere Informationen finden Sie unter Konfigurieren der ADFS-Unterstützung für das Webinterface.

Authentifizierung an Access Gateway

Sie können Authentifizierung und Passthrough von Benutzeranmeldeinformationen mit Access Gateway für explizite und Smartcard-Authentifizierung aktivieren. Der Zugriff von Benutzern auf Ressourcen wird mit Richtlinien gesteuert.

Wenn Benutzer sich mit expliziten Anmeldeinformationen an Access Gateway anmelden, wird Passthrough-Authentifizierung standardmäßig aktiviert. Benutzer melden sich an Access Gateway an und müssen sich beim Webinterface nicht erneut authentifizieren, um auf ihre Ressourcen zuzugreifen. Um die Sicherheit zu erhöhen, können Sie die Passthrough-Authentifizierung deaktivieren, damit Benutzer aufgefordert werden, ein Kennwort einzugeben, bevor die Ressourcengruppe angezeigt wird.

Wenn sich Benutzer mit einer Smartcard an Access Gateway anmelden, müssen Sie sich nicht erneut am Webinterface authentifizieren. Standardmäßig werden Benutzer jedoch aufgefordert, eine PIN-Nummer einzugeben, wenn sie auf eine Ressource zugreifen. Sie können die Site so konfigurieren, dass Benutzer auf ihre XenApp-Ressourcen zugreifen können, ohne eine PIN-Nummer eingeben zu müssen. Diese Feature wird von XenDesktop nicht unterstützt

Sie können diese Einstellungen jederzeit mit der Aufgabe Authentifizierungsmethode in der Citrix Webinterface Management Console anpassen.

Authentifizierung an einem Drittanbieter mit Kerberos

Sie können Verbund- oder Single Sign-On-Produkte von Drittanbietern für die Authentifizierung von Benutzern und die Zuordnung ihrer Identitäten zu Active Directory-Benutzerkonten verwenden. Sie können dann Kerberos für Single Sign-On am Webinterface verwenden. Weitere Informationen über Kerberos finden Sie unter Konfigurieren der Kerberos-Anmeldung.

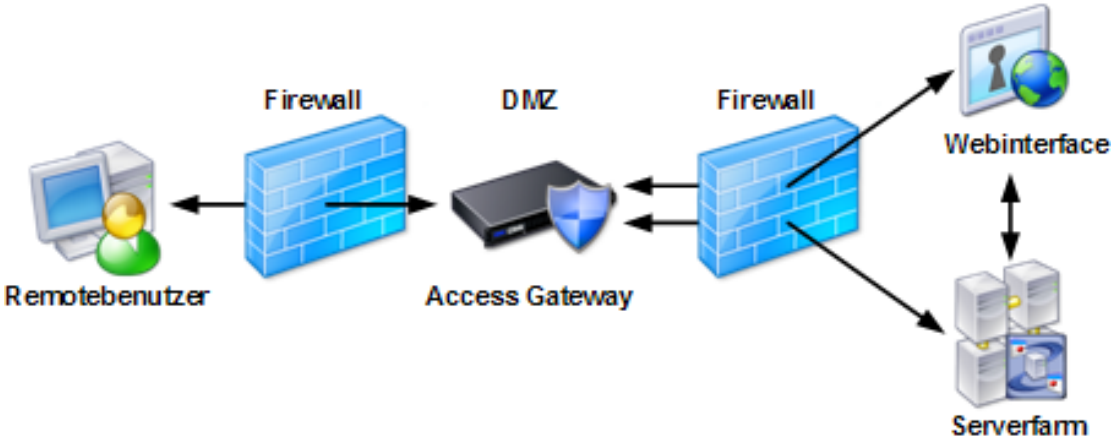
Authentifizierung am Webserver

Sie können die Authentifizierung von Benutzern am Webserver mit Kerberos aktivieren. Weitere Informationen über Kerberos finden Sie unter Konfigurieren der Kerberos-Anmeldung.

Bereitstellen von Access Gateway mit dem Webinterface

Wenn Sie Access Gateway zusammen mit dem Webinterface bereitstellen, empfiehlt Citrix, dass XenApp/XenDesktop und das Webinterface auf Servern im internen Netzwerk installiert sind und sich das Access Gateway-Gerät in der demilitarisierten Zone (DMZ) befindet.

In dieser Abbildung sehen Sie die empfohlene Konfiguration für die Bereitstellung von Access Gateway mit dem Webinterface.



Eine DMZ ist ein Subnetz zwischen dem sicheren internen Netzwerk und dem Internet (oder anderen externen Netzwerken). Wenn Access Gateway in der DMZ bereitgestellt wird, greifen Benutzer mit dem Citrix Secure Access Plug-In oder einem Citrix Client darauf zu. Benutzer melden sich an, werden von Access Gateway authentifiziert und werden dann gemäß den konfigurierten Zugriffsrichtlinien zu ihren Ressourcen geleitet.

Ressourcen Benutzern verfügbar machen

Mit Access Gateway melden sich Benutzer an einem Bereich (für Access Gateway Standard Edition), Anmeldepunkt (für Access Gateway Advanced Edition und Access Gateway 5.0) oder einem virtuellen Server (für Access Gateway Enterprise Edition) an, um Zugriff auf ihre Ressourcen zu erhalten. Sie stellen Ressourcen für Benutzer bereit, indem Sie einen Bereich, Anmeldepunkt oder virtuellen Server für den Zugriff auf eine XenApp Web-Site konfigurieren.

Access Gateway bietet mehrere Methoden für die Integration von XenApp Web-Sites, die mit dem Webinterface erstellt wurden, u. a.:

- Eine XenApp Web-Site, die als Standardhomepage für einen Bereich, Anmeldepunkt oder virtuellen Server konfiguriert ist. Sobald Benutzer angemeldet sind, wird die XenApp Web-Site angezeigt.

- XenApp Web-Sites, die in die Zugriffsoberfläche integriert sind. Wenn die Zugriffsoberfläche als Standardhomepage ausgewählt wird, wird neben den

Dateifreigaben, Access Centers und Webanwendungen eine XenApp Web-Site angezeigt. Das Access Interface ist nur mit Access Gateway Advanced Edition und Enterprise Edition verfügbar.

Integrieren einer XenApp Web-Site mit Access Gateway

Aktualisiert: 2014-10-30

Um eine Site mit Access Gateway zu integrieren, erstellen Sie eine XenApp Web-Site und konfigurieren Sie eine Webressource für die Site in Access Gateway.

So erstellen Sie eine in Access Gateway integrierte Site

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf den Container Citrix Webinterface.

3. Klicken Sie im Bereich Aktionen auf Site erstellen.

4. Wählen Sie XenApp Web und klicken Sie auf Weiter.

5. Geben Sie auf der Seite IIS-Speicherort angeben den Pfad und den Namen für die Site an. Klicken Sie auf Weiter.

6. Wählen Sie auf der Seite Authentifizierungspunkt festlegen die Option Access Gateway und klicken Sie auf Weiter.

7. Geben Sie auf der Seite Access Gateway-Einstellungen festlegen die URL des Access Gateway-Authentifizierungsdienstes im Feld Authentifizierungsdienst-URL ein.

8. Legen Sie fest, wie sich Benutzer an Access Gateway anmelden, und klicken Sie auf Weiter.

   - Wenn die Benutzer sich mit einem Benutzernamen und Kennwort an Access Gateway anmelden, wählen Sie Explizit. Wenn Sie die Sicherheit erhöhen möchten, indem Sie Passthrough der Benutzeranmeldeinformationen von Access Gateway zum Webinterface deaktivieren, aktivieren Sie das Kontrollkästchen Kennwort erforderlich, bevor Anwendungen und Desktops angezeigt werden.

   - Wenn die Benutzer sich mit einer Smartcard an Access Gateway anmelden, wählen Sie Smartcard. Stellen Sie sicher, dass Sie als Domänenadministrator angemeldet sind, bevor Sie die Passthrough-Authentifizierung für Smartcards aktivieren.

   Wichtig: In Access Gateway integrierte XenApp Web-Sites können explizite oder Smartcard-Authentifizierung, aber nicht beide, unterstützen. Wenn sich ein Teil der Benutzer mit expliziter Authentifizierung und ein anderer Teil mit Smartcard-Authentifizierung an Access Gateway anmeldet, müssen Sie für jede Authentifizierungsmethode separate Sites erstellen und konfigurieren. Dann kann Access Gateway Benutzer an die ihrer Authentifizierungsmethode entsprechende Site weiterleiten.

9. Wenn Sie die Site für explizite Authentifizierung konfigurieren, gehen Sie zu Schritt 10. Wenn Sie auf der Seite Smartcard-Einstellungen angeben Smartcard-Authentifizierung konfigurieren, geben Sie an, ob Benutzer eine PIN-Nummer eingeben müssen, um auf Ressourcen zugreifen zu können.

   - Wenn Benutzer jedes Mal, wenn sie auf eine Ressource zugreifen, eine PIN-Nummer eingeben sollen, wählen Sie Benutzer müssen PIN eingeben. Um diese Funktion zu aktivieren, sind weitere Konfigurationsschritte erforderlich. Weitere Informationen finden Sie unter So ermöglichen Sie, dass Smartcard-Benutzer über Access Gateway auf Ressourcen zugreifen können, indem Sie eine PIN-Nummer angeben.

Hinweis: Sie können einrichten, dass Windows XP-Benutzer, die sich an ihren Desktops mit derselben Smartcard wie an Access Gateway anmelden, auf Ressourcen zugreifen können, ohne eine PIN-Nummer eingeben zu müssen. Weitere Informationen finden Sie unter So ermöglichen Sie, dass Smartcard-Benutzer über Access Gateway auf Ressourcen zugreifen können, indem Sie eine PIN-Nummer angeben.

- Wenn Sie möchten, dass alle Benutzer auf ihre XenApp-Ressourcen zugreifen können, ohne eine PIN-Nummer einzugeben, wählen Sie Smartcard-Passthrough aktivieren. Diese Funktion wird von XenDesktop nicht unterstützt und kann nur verwendet werden, wenn der Webserver in derselben Domäne ist wie die Benutzer. Sie müssen u. U. den Webserver neu starten, um den Dienst Passthrough mit Smartcard von Access Gateway zu aktivieren. Um diese Funktion zu aktivieren, sind weitere Konfigurationsschritte erforderlich. Weitere Informationen finden Sie unter So ermöglichen Sie, dass Smartcard-Benutzer über Access Gateway auf Ressourcen zugreifen können, ohne eine PIN-Nummer angeben zu müssen.

  Hinweis: Passthrough mit Smartcard von Access Gateway ist standardmäßig für alle Domänenbenutzer aktiviert. Um die Liste der zugelassenen Benutzer einzuschränken, bearbeiten Sie die Benutzerberechtigungen in der Datei PTSAccess.txt, die sich üblicherweise im Verzeichnis C:\Programme (x86)\Citrix\DeliveryServices\ProtocolTransitionService\ befindet.

10. Bestätigen Sie die Einstellungen für die neue Site und klicken Sie auf Weiter, um die Site zu erstellen.

So ermöglichen Sie Zugriff auf die Site über Access Gateway

Dieser Abschnitt bietet einen Überblick über die Schritte, mit denen Sie den Zugriff auf die Site über Access Gateway ermöglichen. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Access Gateway-Edition.

1. Konfigurieren Sie XenApp oder XenDesktop für die Kommunikation mit Access Gateway.
2. Konfigurieren Sie Access Gateway, um Zugriff auf die XenApp Web-Site zu ermöglichen.

   Wichtig: Geben Sie die Domäne im Format *Domäne* und nicht *Domäne.com* an. Der Webinterface-Dienst Passthrough mit Smartcard von Access Gateway erkennt Domänen im Format *Domäne.com* nicht. Benutzer können sich daher nicht anmelden, wenn Sie die Domäne auf diese Weise angeben.

3. Stellen Sie sicher, dass Einstellungen für Workspace Control (nur Access Gateway Advanced Edition) und Sitzungstimeouts für Access Gateway und das Webinterface richtig konfiguriert sind.

So ermöglichen Sie, dass Smartcard-Benutzer über Access Gateway auf Ressourcen zugreifen können, ohne eine PIN-Nummer angeben zu müssen

Wenn Sie möchten, dass alle Benutzer auf ihre XenApp-Ressourcen zugreifen können, ohne eine PIN-Nummer eingeben zu müssen, müssen Sie Secure Sockets Layer (SSL) für die IIS-Site, die die XenApp Web-Site hostet, aktivieren. Weitere Informationen finden Sie in der Microsoft Dokumentation für IIS 7.*x* und IIS 6.0.

Nachdem Sie SSL aktiviert haben, stellen Sie sicher, dass der Webserver in derselben Domäne wie die Benutzer ist, und konfigurieren Sie Active Directory, um eingeschränkte Delegierung zuzulassen.

So stellen Sie sicher, dass sich die Domäne auf der richtigen Funktionsebene befindet

Wichtig: Zum Heraufstufen der Domänenebene müssen alle Domänencontroller in der Domäne unter Windows Server 2008 oder Windows Server 2003 installiert sein. Stufen Sie die Domänenfunktionsebene nicht auf Windows Server 2008 herauf, wenn Sie einen Domänencontroller besitzen, auf dem Windows Server 2003 ausgeführt wird, oder wenn Sie einen solchen einrichten möchten. Nachdem die Domänenfunktionsebene heraufgesetzt worden ist, kann sie nicht wieder auf eine niedrigere Stufe zurückgesetzt werden.

1. Melden Sie sich als Domänenadministrator am Domänencontroller an und öffnen Sie das MMC-Snap-In Active Directory-Domänen und -Vertrauensstellungen.
2. Wählen Sie im linken Bereich den Domänennamen aus und klicken Sie im Bereich Aktionen auf Eigenschaften.
3. Wenn sich die Domäne nicht auf der höchst möglichen Funktionsebene befindet, wählen Sie den Domänennamen aus und klicken Sie im Bereich Aktionen auf Domänenfunktionsebene heraufstufen.
4. Um die Domänenfunktionsebene heraufzustufen, klicken Sie auf die entsprechende Ebene und klicken Sie auf Heraufstufen.

So vertrauen Sie Servern, auf denen das Webinterface ausgeführt wird, und dem Citrix XML-Dienst für die Delegierung

1. Melden Sie sich als Domänenadministrator am Domänencontroller an und öffnen Sie das MMC-Snap-In Active Directory-Benutzer und -Computer.
2. Klicken Sie im Menü Ansicht auf Erweiterte Funktionen.
3. Klicken Sie im linken Bereich auf den Knoten Computers und wählen Sie den Webserver aus.
4. Klicken Sie im Bereich Aktionen auf Eigenschaften.
5. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Beliebiges Authentifizierungsprotokoll verwenden und klicken Sie dann auf Hinzufügen.
6. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.
7. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst ausgeführt wird, und klicken Sie auf OK.
8. Wählen Sie in der Liste den Diensttyp HTTP aus und klicken Sie auf OK.
9. Überprüfen Sie auf der Registerkarte Delegierung, ob der Diensttyp http für den Server, auf dem der Citrix XML-Dienst ausgeführt wird, in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.
10. Wiederholen Sie Schritte 3 - 9 für jeden Server in der Farm, auf dem der Citrix XML-Dienst ausgeführt wird und zu dem das Webinterface gemäß der Konfiguration eine Verbindung herstellen soll.
11. Klicken Sie im linken Bereich auf den Knoten Computers und wählen Sie den Server aus, auf dem der Citrix XML-Dienst ausgeführt wird, zu dem das Webinterface eine Verbindung herstellen soll.
12. Klicken Sie im Bereich Aktionen auf Eigenschaften.
13. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Nur Kerberos verwenden und klicken Sie dann auf Hinzufügen.
14. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.
15. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst ausgeführt wird, und klicken Sie auf OK.
16. Wählen Sie in der Liste den Diensttyp HOST aus und klicken Sie auf OK.

17. Überprüfen Sie auf der Registerkarte Delegierung, ob der Diensttyp HOST für den Server, auf dem der Citrix XML-Dienst ausgeführt wird, in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.

18. Wiederholen Sie Schritte 11 - 17 für jeden Server in der Farm, auf dem der Citrix XML-Dienst ausgeführt wird und zu dem das Webinterface gemäß der Konfiguration eine Verbindung herstellen soll.

19. Aus Sicherheitsgründen müssen Sie für alle Server in der Farm eingeschränkte Delegierung konfigurieren. Damit Benutzer Zugriff auf Ressourcen auf diesen Servern haben, müssen Sie die betreffenden Dienste, z. B. den Dienst http für einen Webserver, der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann hinzufügen.

    Weitere Informationen finden Sie im Whitepaper *Service Principal Names and Delegation in Presentation Server* (CTX110784) im Citrix Knowledge Center.

So legen Sie fest, auf welche Ressourcen über die Serverfarm zugegriffen werden kann

1. Melden Sie sich als Domänenadministrator am Domänencontroller an und öffnen Sie das MMC-Snap-In Active Directory-Benutzer und -Computer.

2. Klicken Sie im linken Bereich auf den Knoten Computers und wählen Sie einen Server aus der Farm aus.

3. Klicken Sie im Bereich Aktionen auf Eigenschaften.

4. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Nur Kerberos verwenden und klicken Sie dann auf Hinzufügen.

5. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.

6. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein und klicken Sie dann auf OK.

7. Wählen Sie die Diensttypen cifs und ldap aus der Liste aus und klicken Sie auf OK.

    Hinweis: Wenn für den Dienst ldap zwei Optionen angezeigt werden, wählen Sie die Option aus, die mit dem vollqualifizierten Domänennamen des Domänencontrollers übereinstimmt.

8. Überprüfen Sie auf der Registerkarte Delegierung, ob die Diensttypen cifs und ldap für den Domänencontroller in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.

9. Wiederholen Sie den Vorgang für jeden Server in der Farm.

So konfigurieren Sie ein Zeitlimit für den Zugriff auf Ressourcen auf Domänenebene

Vorsicht: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

Standardmäßig können Benutzer 15 Minuten lang auf Ressourcen in einem Netzwerk zugreifen. Sie können diesen Zeitraum erhöhen, indem Sie auf dem Server, auf dem der Citrix XML-Dienst ausgeführt wird, den folgenden Registrierungseintrag ändern:

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

Dieser Wert gibt in Minuten an, wie lange Benutzer nach Beginn einer Sitzung auf Ressourcen zugreifen können.

Die Sicherheitsrichtlinie für Domänen bestimmt den zulässigen Höchstwert für S4ULifetime. Wenn Sie einen Wert für "S4UTicketLifetime" festlegen, der über dem auf der Domänenebene festgelegten Wert liegt, hat die Einstellung auf Domänenebene Vorrang.

1. Melden Sie sich als Domänenadministrator am Domänencontroller an und öffnen Sie das MMC-Snap-In Sicherheitsrichtlinie für Domänen.
2. Klicken Sie im linken Bereich auf Kontorichtlinien > Kerberos-Richtlinie.
3. Aktivieren Sie im Ergebnisbereich Max. Gültigkeitsdauer des Diensttickets.
4. Klicken Sie im Bereich Aktionen auf Eigenschaften.
5. Geben Sie das gewünschte Zeitlimit (in Minuten) im Feld Das Ticket läuft ab in ein.

Wenn Sie für den Zugriff auf Ressourcen über die Serverfarm kein Zeitlimit konfigurieren möchten, wählen Sie die Option Beliebiges Authentifizierungsprotokoll verwenden. Mit dieser Option wird der für "S4UTicketLifetime" angegebene Wert ignoriert. Weitere Informationen finden Sie auf der Microsoft Website unter http://support.microsoft.com/.

So ermöglichen Sie, dass Smartcard-Benutzer über Access Gateway auf Ressourcen zugreifen können, indem Sie eine PIN-Nummer angeben

Aktualisiert: 2014-07-04

Wenn Smartcard-Benutzer jedes Mal eine PIN-Nummer eingeben sollen, wenn sie über Access Gateway auf eine Ressource zugreifen, müssen Sie die Aufzählung von Benutzer-Sicherheits-IDs (SIDs) auf dem Citrix XML-Dienst aktivieren.

Vorsicht: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

1. Wenn sich die Benutzerkonten in einer anderen Domäne befinden als die Serverfarm, stellen Sie sicher, dass eine bidirektionale Vertrauensstellung zwischen den Domänen besteht.

2. Überprüfen Sie, ob der Citrix XML-Dienst die IP-Adresse auflösen und den Domänencontroller der Benutzerkontodomäne kontaktieren kann. Bei Anfragen an den Citrix XML-Dienst kann es zu Zeitüberschreitungen kommen, wenn der Citrix XML-Dienst nicht mit dem Domänencontroller kommunizieren kann.

3. Geben Sie dem Windows-Konto, unter dem der Citrix XML-Dienst ausgeführt wird, Lesezugriff auf das TGGAU-Attribut für alle Domänen in Active Directory. Weitere Informationen zum TGGAU-Attribut finden Sie in Microsoft Knowledge Base-Artikel 331951. Der Citrix XML-Dienst ist standardmäßig für die Ausführung als Netzwerkdienstkonto konfiguriert. Sie können die erforderlichen Berechtigungen gewähren, indem Sie dieses Konto den folgenden in Active Directory integrierten Gruppen hinzufügen:

   - Prä-Windows 2000 kompatibler Zugriff

   - Windows-Autorisierungszugriffsgruppe
4. Gehen Sie auf dem Server, auf dem der Citrix XML-Dienst ausgeführt wird, in der Systemregistrierung zu HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\XMLService\.

5. Fügen Sie unter dem Knoten XMLService einen DWORD-Wert mit dem Namen EnableSIDEnumeration hinzu und setzen Sie den Wert auf 1.

Hinweis: Für XenDesktop 5 und höher ist der Registrierungsschlüssel:
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer]
"EnableXmlServiceSidEnumeration"=REG_DWORD:1

6. Starten Sie IIS auf dem Webserver neu. Wenn die neuen Berechtigungen sofort wirksam werden sollen, anstatt auf den Ablauf des Zeitraums des Kerberos-Ticket-Cache zu warten, starten Sie den Server, auf dem der Citrix XML-Dienst ausgeführt wird, neu.

7. Für Windows XP-Benutzer, die sich an ihren Desktops mit derselben Smartcard wie an Access Gateway anmelden, können Sie einrichten, dass sie auf Ressourcen zugreifen können, ohne eine PIN-Nummer eingeben zu müssen, indem Sie Passthrough-mit-Smartcard-Authentifizierung konfigurieren.

   a. Installieren Sie das Citrix Online Plug-In oder das Citrix Desktop Viewer Plug-In mit einem Administratorkonto auf den Geräten der Benutzer.

   b. Fügen Sie dem Gruppenrichtlinienobjekt-Editor die Clientvorlage hinzu. Weitere Informationen finden Sie unter Schritt 1: Installieren des Plug-Ins für die Smartcard-Authentifizierung.

   c. Aktivieren Sie mit einer Gruppenrichtlinie Passthrough-Authentifizierung für alle Citrix Clients. Weitere Informationen finden Sie unter Schritt 1: Installieren des Plug-Ins für die Smartcard-Authentifizierung.

Koordinieren von Webinterface- und Access Gateway-Einstellungen

Bestimmte XenApp - und XenDesktop-Einstellungen können im Webinterface und Access Gateway konfiguriert werden. Da aber eine in Access Gateway integrierte XenApp Web-Site von mehr als einem Bereich (für Access Gateway Standard Edition), Anmeldepunkt (für Access Gateway Advanced Edition) oder virtuellen Server (für Access Gateway Enterprise Edition) referenziert werden kann, kann ein Bereich, ein Anmeldepunkt oder ein virtueller Server eine XenApp Web-Site in die Zugriffsoberflächenseite einbetten, während ein anderer Bereich, Anmeldepunkt oder virtueller Server die Site als Standardhomepage anzeigt. Dies kann zu Konflikten bei bestimmten Ressourceneinstellungen führen.

Folgen Sie den unten stehenden Anweisungen, um sicherzustellen, dass Ihre Einstellungen wie beabsichtigt funktionieren:

- **Sitzungstimeout:** Stellen Sie sicher, dass alle Bereiche, Anmeldepunkte oder virtuellen Server dieselben Einstellungen wie die XenApp Web-Site verwenden.
- **Workspace Control:** Deaktivieren Sie in Access Gateway Advanced Edition alle Workspace Control-Einstellungen für Anmeldepunkte, die eine XenApp Web-Site als Homepage haben. Dadurch wird sichergestellt, dass die im Webinterface konfigurierten Einstellungen verwendet werden. Für alle anderen Anmeldepunkte kann Workspace Control wie gewünscht konfiguriert werden.

Angeben der Erstkonfiguration für eine Site

Nach der Erstellung einer Site mit der Konsole können Sie die Erstkonfiguration angeben, indem Sie auf der letzten Seite des Assistenten "Site erstellen" das Kontrollkästchen Diese Site jetzt konfigurieren aktivieren. Mit dem Assistenten für die Erstkonfiguration können Sie die Kommunikation mit einer oder mehreren Serverfarmen konfigurieren und die für Benutzer verfügbaren Typen von Ressourcen festlegen.

Angeben von Serverfarmen

Beim Konfigurieren einer neuen Site müssen Sie Angaben zu den Serverfarmen machen, die Ressourcen für die Benutzer der Site zur Verfügung stellen.

Sie können diese Einstellungen jederzeit mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console anpassen. Weitere Informationen zum Konfigurieren der Kommunikation mit Serverfarmen finden Sie unter Verwalten von Servern und Farmen.

Wichtig: Um Kompatibilität mit XenApp 4.0, mit Feature Pack 1, für UNIX zu erreichen, ist ein zusätzlicher manueller Konfigurationsschritt erforderlich. Weitere Informationen finden Sie unter So konfigurieren Sie Unterstützung für XenApp 4.0, mit Feature Pack 1, für UNIX.

Angeben von Authentifizierungsmethoden

Beim Konfigurieren einer XenApp Web-Site, die als Authentifizierungspunkt die Option Webinterface verwendet, können Sie angeben, wie Benutzer sich bei der Anmeldung am Webinterface authentifizieren sollen.

Sie können diese Einstellungen jederzeit mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console anpassen. Weitere Informationen zum Konfigurieren der Authentifizierung finden Sie unter Konfigurieren der Authentifizierung für das Webinterface.

Angeben von Domäneneinschränkungen

Beim Konfigurieren einer XenApp Web-Site, die als Authentifizierungspunkt die Option Webinterface verwendet, können Sie den Zugriff auf Benutzer aus bestimmten Domänen beschränken.

Sie können diese Einstellungen jederzeit mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console anpassen. Weitere Informationen zum Konfigurieren von Domäneneinschränkungen finden Sie unter So konfigurieren Sie Domäneneinschränkungen.

Angeben der Darstellung der Anmeldeseite

Beim Konfigurieren einer XenApp Web-Site können Sie die Darstellung der Anmeldeseiten für Benutzer festlegen. Wählen Sie zwischen einem Minimallayout, bei dem nur die entsprechenden Anmeldefelder angezeigt werden, und einem Layout, das auch die Navigationsleiste umfasst.

Sie können diese Einstellung jederzeit mit der Aufgabe Websitedarstellung in der Citrix Webinterface Management Console anpassen: Weitere Informationen über das Anpassen der Darstellung der Benutzeroberfläche finden Sie unter Anpassen der Darstellung für Benutzer.

Angeben der für Benutzer verfügbaren Ressourcen

Beim Konfigurieren einer neuen Site müssen Sie die Ressourcentypen angeben, die Sie zur Verfügung stellen möchten. Das Webinterface bietet Benutzern über einen Webbrowser oder das Citrix Online Plug-In Zugriff auf Ressourcen (Anwendungen, Inhalte und Desktops). Die Integration der Offlineanwendungsfunktion ermöglicht es Benutzern, Anwendungen auf ihre Desktops zu streamen und diese lokal zu öffnen.

Sie können Benutzern wie im Folgenden beschrieben Zugriff auf Ressourcen gewähren:

- **Online:** Benutzer greifen auf Anwendungen, Inhalte und Desktops auf Remoteservern zu. Benutzer benötigen eine Netzwerkverbindung, um mit ihren Ressourcen arbeiten zu können.

- **Offline:** Benutzer streamen Anwendungen auf ihre eigenen Desktops und öffnen sie lokal. Nach der Bereitstellung von Anwendungen auf XenApp Services-Sites können Benutzer diese Anwendungen jederzeit ausführen, ohne eine Verbindung zum Netzwerk herstellen zu müssen. Bei XenApp Web-Sites benötigen Benutzer eine Verbindung zum Netzwerk, um sich an der Site anmelden und ihre Anwendungen starten zu können. Wenn die Anwendungen ausgeführt werden, muss die Verbindung nicht weiter aufrechterhalten werden.

- **Dual Mode:** Benutzer greifen über dieselbe Site auf Offline- und Onlineanwendungen, Inhalte und Desktops zu. Wenn Offlineanwendungen nicht verfügbar sind, werden wenn möglich Onlineversionen bereitgestellt.

Sie können diese Einstellung jederzeit mit der Aufgabe Ressourcentypen in der Citrix Webinterface Management Console anpassen. Weitere Informationen über Citrix Client-Typen finden Sie unter Verwalten von Clients.

Aktualisieren von vorhandenen Sites

Wenn Sie ein Upgrade von einer früheren Version des Webinterface, bis einschließlich Version 4.5, vornehmen, wird auch die Aktualisierung vorhandener Sites unterstützt (mit Ausnahme von Conferencing Manager-Gastteilnehmersites).

Wichtig: Conferencing Manager-Gastteilnehmersites werden nicht mehr unterstützt. Wenn Sie von einer früheren Webinterface-Version aktualisieren, entfernt das Installationsprogramm die Conferencing Manager-Gastteilnehmersites von Ihrem Webserver.

Vorhandene Access Platform/XenApp Web- und Program Neighborhood Agent-Dienste-/XenApp Services-Sites können folgendermaßen aktualisiert werden:

- **Lokal konfigurierte Sites:** Während der Installation des Webinterface aktualisiert das Installationsprogramm automatisch alle lokal konfigurierten Sites auf die neueste Version.

- **Zentral konfigurierte Sites und Sitegruppen:** Während der Installation konvertiert der Webinterface-Installer automatisch alle vorhandenen zentral konfigurierten Sites zu lokaler Konfiguration. Die konvertierten Sites werden dann auf die neueste Version aktualisiert.

Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Clientinstallationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Clients von der Citrix Website herunterladen oder Sie ältere Clients bereitstellen möchten, überprüfen Sie, ob in den Konfigurationsdateien für Ihre XenApp Web-Sites die richtigen Namen der Clientinstallationsdateien für die Parameter ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 und ClientStreamingWin32 angegeben sind. Weitere Informationen zu den Parametern in Webinterface-Konfigurationsdateien finden Sie unter WebInterface.conf-Parameter.

Verwenden von Siteaufgaben

Um eine Site zu konfigurieren, wählen Sie den Sitetyp im linken Bereich der Citrix Webinterface Management Console aus, klicken Sie dann im Ergebnisbereich auf die Site und wählen Sie eine der Aufgaben im Bereich Aktionen oder im Menü Aktion aus. Sie können auch mit der rechten Maustaste auf einen Sitenamen im Ergebnisbereich klicken und Aufgaben aus dem Kontextmenü auswählen.

Einige Aufgaben sind nur für bestimmte Sitetypen und -konfigurationen verfügbar. In der folgenden Tabelle finden Sie Informationen dazu, welche Aufgaben für die verschiedenen Sitetypen verfügbar sind.

Aufgabe	XenApp Web-Sites		XenApp Services-Sites		Sites mit ADFS-Integration
	Online/Dual Mode	Nur Offline	Online/Dual Mode	Nur Offline	
Authentication Method	*	*			
Authentifizierungsmethoden	*	*	*	*	*
Clientseitiger Proxy	*		*		*
Clientbereitstellung	*	*			*
Ressourcenaktualisierung			*	*	
Ressourcentypen	*	*	*	*	*
Sicherer Zugriff	*		*		*
Serverfarmen	*	*	*	*	*
Servereinstellungen			*	*	
Sitzungsoptionen			*		
Sitzungseinstellungen	*	*			*
Verknüpfungen			*	*	
Sitewartung	*	*	*	*	*
Websitedarstellung	*	*			*
Workspace Control	*				*

Reparieren und Deinstallieren von Sites

Mit den Aufgaben Site reparieren und Site deinstallieren unter Sitewartung in der Citrix Webinterface Management Console reparieren bzw. entfernen Sie Sites. Beim Deinstallieren einer Site wird diese vollständig aus dem System entfernt und Sie können keine Tasks mehr für die Site verwenden.

Wichtig: Mit der Aufgabe Site reparieren werden benutzerdefinierte Skripte und Bilder entfernt, sofern solche vorhanden sind. Benutzerdefinierte Dateien werden auch durch die Aufgabe IIS-Hosting verwalten entfernt. Citrix empfiehlt, alle erstellen Dateien vor dem Ausführen eines dieser Tasks zu sichern.

Bereitstellen des Webinterface für Benutzer

Nach dem Installieren und Konfigurieren des Webinterface teilen Sie den Benutzern die URL der Seite Anmeldung mit. Wenn Benutzer die Seite in ihren Webbrowsern mit einem Lesezeichen versehen möchten, sollte das Lesezeichen auf den folgenden Wert eingestellt werden: http://*Servername*/*Sitepfad*. Verzichten Sie auf die Angabe einer bestimmten Seite wie z. B. login.aspx.

Auf Java-Anwendungsservern wird der Pfad der Site (der Teil der URL nach dem Hostnamen und dem Port) durch die Servlet-Engine bestimmt. Sie können den Pfad beim Installieren der WAR-Datei in der Servlet-Engine ändern. Der Standard ist normalerweise */WARDateiname*, wobei *WARDateiname* der erste Teil des Dateinamens der WAR-Datei der Site ist.

Direkter Zugriff auf Sites

Wenn Benutzer direkt oder über Access Gateway Enterprise Edition mit dem Citrix Secure Access Plug-In auf XenApp Web-Sites zugreifen, können Sie Unterstützung für die URLs veröffentlichter Ressourcen aktivieren. Diese Funktion ermöglicht es Benutzern, dauerhafte Links zu Ressourcen zu erstellen, auf die mit dem Webinterface zugegriffen wird.

Hinweis: Ressourcen-URLs werden nicht für Benutzer unterstützt, die über Access Gateway Standard Edition oder Advanced Edition auf Sites zugreifen oder die Zugriff ohne Client über Access Gateway Enterprise Edition verwenden.

Benutzer können ihren Verknüpfungslisten oder Desktops permanente Links hinzufügen. Um Unterstützung für Ressourcen-URLs mit der Citrix Webinterface Management Console zu aktivieren, klicken Sie im linken Bereich auf XenApp Web-Sites, wählen Sie die Site im Ergebnisbereich aus, klicken Sie im Bereich Aktionen auf Sitzungseinstellungen, klicken Sie auf Permanente URLs und aktivieren Sie das Kontrollkästchen Benutzer können Ressourcen über Browserlesezeichen starten.

Wichtig: Wenn Sie diese Funktion aktivieren, wird der Schutz vor Cross-Site Request Forgery (CSRF)-Angriffen deaktiviert.

Festlegen der Anmeldeseite als Standardwebsite in Microsoft Internetinformationsdienste

Sie können die Seite Anmeldung des Webinterface als Standard für Benutzer des Webservers festlegen, sodass die URL http://*Servername*/ lautet. Aktivieren Sie hierfür das Kontrollkästchen Als Standardseite für die IIS-Site definieren, wenn Sie eine Site erstellen. Mit der Aufgabe IIS-Hosting verwalten unter Sitewartung in der Citrix Webinterface Management Console können Sie dies auch zu einem beliebigen späteren Zeitpunkt ausführen.

Verwalten von Servern und Farmen

Aktualisiert: 2014-11-24

In diesem Abschnitt wird beschrieben, wie Sie das Webinterface für die Kommunikation mit Ihren Serverfarmen konfigurieren. Außerdem wird erläutert, wie Sie Servereinstellungen konfigurieren und verwalten und Load Balancing zwischen Servern, auf denen der Citrix XML-Dienst ausgeführt wird, aktivieren.

Überlegungen zur Kennwortänderung

Sollten Unterschiede zwischen den Serverfarmen bestehen, können Benutzer ihre Kennwörter möglicherweise aufgrund von weiteren Problemen nicht ändern. Beispiel:

- Die Domänenrichtlinie verhindert das Ändern von Kennwörtern durch Benutzer.
- Wenn XenApp für UNIX-Farmen mit XenApp für Windows- und/oder XenDesktop-Farmen in einer Site zusammengefasst sind, kann nur das Windows-Kennwort geändert werden.

Citrix empfiehlt in diesen Situationen, die Kennwortänderung durch Benutzer zu deaktivieren.

Wenn mehrere Farmen zusammengefasst werden, stellen Sie sicher, dass in der ersten Farm, die in der Konfigurationsdatei der Site aufgelistet ist, Presentation Server 4.5 oder höher oder XenDesktop ausgeführt wird.

Bei Bedarf kann die Kennwortänderung in einer gemischten Serverfarmbereitstellung aktiviert werden. Das Webinterface kontaktiert die Serverfarmen in der definierten Reihenfolge, bis eine Serverfarm meldet, dass das Kennwort ordnungsgemäß geändert wurde. An dieser Stelle wird das Verfahren angehalten. Sie können dann die Serverfarm angeben, an die die Anfrage zum Ändern des Kennworts ausgegeben wird. Wenn die Kennwortänderungsanfrage fehlschlägt, wird sie an die nächste Serverfarm in der Reihenfolge ausgestellt. Verwenden Sie geeignete Kennwortreplikationsmethoden zwischen den Serverfarmen, um konsistente Benutzerkennwörter sicherzustellen.

So fügen Sie eine Serverfarm hinzu

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Serverfarmen.
4. Klicken Sie auf Add.
5. Geben Sie einen Namen für die Serverfarm im Feld Farmname ein.
6. Klicken Sie im Bereich Servereinstellungen auf Hinzufügen, um einen Servernamen anzugeben. Wenn Sie einen Servernamen ändern möchten, markieren Sie den Namen in der Liste und klicken Sie auf Bearbeiten. Wenn Sie einen Servernamen entfernen möchten, markieren Sie den Namen und klicken Sie auf Entfernen.
7. Markieren Sie bei der Angabe mehrerer Server einen Namen in der Liste und klicken Sie auf Nach oben oder Nach unten, um die Namen in der entsprechenden Failover-Reihenfolge zu sortieren.

Wichtig: Um Kompatibilität mit XenApp 4.0, mit Feature Pack 1, für UNIX zu erreichen, ist ein zusätzlicher manueller Konfigurationsschritt erforderlich. Weitere Informationen finden Sie unter So konfigurieren Sie Unterstützung für XenApp 4.0, mit Feature Pack 1, für UNIX.

So konfigurieren Sie die Fehlertoleranz

Das Webinterface ermöglicht Fehlertoleranz zwischen Servern, auf denen der Citrix XML-Dienst ausgeführt wird. Mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console können Sie die Fehlertoleranz konfigurieren. Wenn die Kommunikation mit einem Server unterbrochen wird, versucht das Webinterface erst wieder den fehlgeschlagenen Server zu kontaktieren, nachdem die im Feld Ausgefallene Server umgehen angegebene Zeitspanne verstrichen ist. Die Kommunikation wird stattdessen mit den anderen Servern in der Liste Server fortgesetzt.

Standardmäßig wird ein ausgefallener Server für 1 Stunde umgangen. Wenn keiner der Server in der Liste antwortet, versucht das Webinterface alle 10 Sekunden erneut, mit den Servern zu kommunizieren.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Serverfarmen.

4. Klicken Sie auf Hinzufügen, wenn Sie eine Farm hinzufügen, oder wählen Sie einen Namen aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Farm zu konfigurieren.

5. Ordnen Sie die Server in der Liste Server der Priorität nach. Wählen Sie einen Server in der Liste aus und verschieben Sie ihn mithilfe der Schaltflächen Nach oben und Nach unten, um die gewünschte Reihenfolge zu erhalten.

6. Ändern Sie im Feld Ausgefallene Server umgehen die Zeitspanne, die ein ausgefallener Server umgangen wird.

So aktivieren Sie Load Balancing zwischen Servern

Aktualisiert: 2014-11-25

Sie können Load Balancing zwischen Servern aktivieren, auf denen der Citrix XML-Dienst ausgeführt wird. Wenn Sie Load Balancing aktivieren, werden die Verbindungen gleichmäßig auf die Server verteilt, sodass kein Server überlastet wird. Ist Load Balancing standardmäßig deaktiviert.

Sollte bei der Kommunikation mit einem Server ein Fehler auftreten, wird jede weitere Kommunikation auf die verbleibenden Server in der Liste verteilt. Der ausgefallene Server wird für eine bestimmte Zeitspanne umgangen (standardmäßig eine Stunde). Sie können diese Einstellung mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console ändern.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Serverfarmen.

4. Klicken Sie auf Hinzufügen, wenn Sie eine Farm hinzufügen, oder wählen Sie einen Namen aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Farm zu konfigurieren.

5. Fügen Sie der Liste Server die Server hinzu, die Sie für das Load Balancing verwenden wollen.

6. Aktivieren Sie das Kontrollkästchen Serverliste für Load Balancing verwenden.

7. Ändern Sie im Feld Ausgefallene Server umgehen die Zeitspanne, die ein ausgefallener Server umgangen wird.

Konfigurieren von Einstellungen für alle Server in einer Farm

Mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console können Sie festlegen, wie der Citrix XML-Dienst Daten zwischen dem Webinterface und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, überträgt. Der Citrix XML-Dienst ist eine Komponente von XenApp und XenDesktop, die als Kontaktpunkt zwischen der Serverfarm und dem Webinterface-Server dient. Standardmäßig wird die bei der Erstellung der Site angegebene Portnummer verwendet. Diese Portnummer muss dem vom Citrix XML-Dienst verwendeten Port entsprechen.

Sie können außerdem die Gültigkeitsdauer für das vom Server generierte Ticket festlegen. Tickets erhöhen die Authentifizierungssicherheit für explizite Anmeldungen, da die vom Webserver an die Benutzergeräte übermittelten ICA-Dateien keine Anmeldeinformationen der Benutzer enthalten.

Jedes Webinterface-Ticket hat standardmäßig eine Gültigkeitsdauer von 200 Sekunden. Sie können die Gültigkeitsdauer ändern, z. B. um sie der Netzwerkleistung anzupassen, da Benutzer mit ungültigen Tickets nicht ordnungsgemäß bei der Serverfarm authentifiziert werden können. Wenn Sie die IP-Adresse (bzw. Adressen) eines Servers ändern, der den Citrix XML-Dienst ausführt, funktioniert Ticketing erst nach dem Neustart des Servers. Vergessen Sie nach dem Ändern der IP-Adressen eines Servers nicht, den Server neu zu starten.

So legen Sie Einstellungen für alle Server fest

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Serverfarmen.

4. Klicken Sie auf Hinzufügen, wenn Sie eine Farm hinzufügen, oder wählen Sie einen Namen aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Farm zu konfigurieren.

5. Geben Sie im Bereich Kommunikationseinstellungen im Feld XML-Dienst-Port die Portnummer ein. Diese Portnummer muss dem vom Citrix XML-Dienst verwendeten Port entsprechen.

6. Wählen Sie in der Liste Transporttyp eine der folgenden Optionen aus:

   - HTTP: Wählen Sie dieses Protokoll für die Übermittlung von Daten über eine HTTP-Standardverbindung. Verwenden Sie diese Option, wenn Sie bereits andere Vorkehrungen zum Sichern dieser Verbindung getroffen haben.

   - HTTPS: Daten werden über eine sichere HTTP-Verbindung mit SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) gesendet. Der Citrix XML-Dienst muss den Port für Internetinformationsdienste (IIS) freigegeben haben und IIS muss HTTPS unterstützen.

   - SSL-Relay: Daten werden über eine sichere Verbindung gesendet, bei der Hostauthentifizierung und Datenverschlüsselung vom SSL-Relay, das auf dem Server mit XenApp oder XenDesktop ausgeführt wird, durchgeführt werden.

7. Wenn Sie die Option SSL-Relay verwenden, geben Sie den TCP-Port des SSL-Relays im Feld SSL-Relay-Port ein (der Standardport ist 443). Das Webinterface verwendet Stammzertifikate beim Authentifizieren eines Servers, auf dem das SSL-Relay ausgeführt wird. Stellen Sie sicher, dass alle Server, auf denen das SSL-Relay ausgeführt wird, denselben Port abhören.

   Hinweis: Bei Verwendung von SSL-Relay oder HTTPS müssen die angegebenen Servernamen mit den Namen in dem Zertifikat des Servers, auf dem XenApp oder XenDesktop ausgeführt wird, genau übereinstimmen (einschließlich Groß- und Kleinschreibung).

8. Um Ticketing zu konfigurieren, klicken Sie auf Ticketing-Einstellungen.

9. Geben Sie in den Feldern ICA-Ticket-Lebensdauer die Lebensdauer von Tickets für Citrix Clients für Onlineressourcen ein.

10. Geben Sie im Feld Streamingticket-Lebensdauer die Lebensdauer von Tickets für das Citrix Offline Plug-In ein.

Festlegen von erweiterten Servereinstellungen

Aktualisiert: 2014-12-02

Im Dialogfeld Erweiterte Farmeinstellungen können Sie Socketpooling und Inhaltsumleitung aktivieren, die Timeoutdauer des Citrix XML-Dienstes angeben und die Anzahl der Versuche, den XML-Dienst zu kontaktieren, festlegen, bevor der Citrix XML-Dienst als fehlgeschlagen angesehen wird.

So aktivieren Sie Socketpooling

Bei Aktivierung von Socketpooling verwaltet das Webinterface einen Socketpool anstatt Sockets jedes Mal neu zu erstellen. Beim Trennen der Verbindung gibt das Webinterface die Sockets an das Betriebssystem zurück. Das Aktivieren von Socketpooling verbessert die Leistung, besonders für SSL-Verbindungen.

Socketpooling steht nur für Sites zur Verfügung, die als Authentifizierungspunkte Webinterface oder Access Gateway haben, und ist standardmäßig aktiviert. Socketpooling sollte nicht verwendet werden, wenn das Webinterface für die Verwendung von Servern, auf denen XenApp für UNIX ausgeführt wird, konfiguriert ist.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Serverfarmen.
4. Klicken Sie auf Erweitert.
5. Aktivieren Sie im Bereich Socketpooling das Kontrollkästchen Socketpooling aktivieren.

So aktivieren Sie Inhaltsumleitung

Mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console können Sie Inhaltsumleitung vom Plug-In zum Server für einzelne XenApp Services-Sites aktivieren bzw. deaktivieren. Diese Einstellung setzt alle Einstellungen für die Inhaltsumleitung außer Kraft, die für XenApp konfiguriert sind.

Wenn Sie die Plug-In-zu-Server-Inhaltsumleitung aktivieren, öffnen Benutzer, die das Citrix Online Plug-In ausführen, Onlineinhalte und lokale Dateien mit auf Servern veröffentlichten Anwendungen. Ein Citrix Online Plug-In-Benutzer, der z. B. einen E-Mail-Anhang in einem lokal ausgeführten E-Mail-Programm empfängt, öffnet den Anhang in einer Onlineanwendung. Wenn Sie Inhaltsumleitung deaktivieren, öffnen Benutzer Onlineinhalte

und lokale Dateien mit lokal installierten Anwendungen.

Die Inhaltsumleitung ist bei XenApp Services-Sites standardmäßig vom Plug-In zum Server aktiviert.

Sie konfigurieren die Plug-In-zu-Server-Inhaltsumleitung, indem Sie Anwendungen mit Dateitypen verknüpfen. Weitere Informationen zur Dateitypzuordnung finden Sie unter So ordnen Sie Dateitypen veröffentlichten Anwendungen zu.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Serverfarmen.
4. Klicken Sie auf Erweitert.
5. Aktivieren Sie im Bereich Inhaltsumleitung das Kontrollkästchen Inhaltsumleitung aktivieren.

So konfigurieren Sie die Kommunikation mit dem Citrix XML-Dienst

Standardmäßig wird die Verbindung zum Citrix XML-Dienst nach einer Minute beendet. Nach zwei gescheiterten Versuchen, eine Verbindung zu dem Dienst herzustellen, wird dieser als fehlgeschlagen angesehen. Sie können diese Standardeinstellungen mit der Aufgabe Serverfarmen in der Citrix Webinterface Management Console ändern.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Serverfarmen.
4. Klicken Sie auf Erweitert.
5. Um die Timeoutdauer des Citrix XML-Dienstes zu konfigurieren, geben Sie angemessene Werte in die Felder Sockettimeout ein.
6. Um festzulegen, nach wie vielen Versuchen, den Citrix XML-Dienst zu kontaktieren, der Dienst als fehlgeschlagen angesehen wird, geben Sie einen Wert im Feld Versuche, den XML-Dienst zu kontaktieren ein.

Verwalten von Servereinstellungen

Mit der Aufgabe Servereinstellungen in der Citrix Webinterface Management Console konfigurieren Sie, wie das Citrix Online Plug-In mit einer Site kommuniziert und ob Benutzer bei einem Fehlschlag zu alternativen Sites umgeleitet werden.

So konfigurieren Sie Serverkommunikationseinstellungen

Mit den Serverkommunikationseinstellungen erreichen Sie Folgendes:

- **Aktivieren von SSL/TLS für die Kommunikation:** Anmeldung mit Smartcard und sichere SSL/TLS-Kommunikation zwischen Plug-In und Webinterface-Server sind nicht standardmäßig aktiviert. Sie können die SSL/TLS-Kommunikation in diesem Dialogfeld aktivieren und URLs zwingen, das HTTPS-Protokoll automatisch anzuwenden. Sie müssen außerdem auf dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, SSL aktivieren.

- **Benutzer können die Server-URL anpassen:** Die Server-URL verweist das Citrix Online Plug-In auf die richtige Konfigurationsdatei. Der Standardpfad wird auf der Grundlage der Serveradresse bestimmt, die bei der Installation eingegeben wurde. Sie können die Änderung der URL durch Benutzer zulassen. Dadurch wird im Dialogfeld Optionen des Citrix Online Plug-Ins auf der Seite Serveroptionen das Feld Server-URL aktiviert.

- **Konfigurieren der automatischen Aktualisierung:** Legen Sie fest, wie häufig das Plug-In seine Konfigurationseinstellungen aktualisiert.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Servereinstellungen.

4. Um sichere Kommunikation zwischen dem Citrix Online Plug-In und einer Site zu verwenden, wählen Sie SSL/TLS für Kommunikation zwischen Plug-Ins und der Site verwenden.

5. Um es Benutzern zu ermöglichen, die URL zu ändern, die das Citrix Online Plug-In auf die Konfigurationsdatei verweist, wählen Sie die Option Benutzer können die Server-URL anpassen.

6. Um zu konfigurieren, wie oft das Citrix Online Plug-In seine Konfigurationseinstellungen aktualisiert, wählen Sie Automatische Aktualisierung alle aus und geben Sie den Aktualisierungszeitraum in Stunden, Tagen, Wochen oder Jahren ein.

So geben Sie Backup-URLs für das Citrix Online Plug-In an

Sie können Backupserver für das Citrix Online Plug-In angeben, mit denen eine Verbindung hergestellt werden kann, falls der primäre Webinterface-Server nicht verfügbar ist. Mit der Aufgabe Servereinstellungen in der Citrix Webinterface Management Console können Sie URLs für Backupserver angeben. Falls ein Server ausfällt, werden Benutzer automatisch mit dem ersten in der Liste Backupsitepfade angegebenen Backupserver verbunden. Falls dieser Server ebenfalls ausfällt, versucht das Citrix Online Plug-In eine Verbindung zum nächsten Server in der Liste herzustellen.

Wichtig: Alle Backup-URLs müssen auf Sites verweisen, die auf demselben Webservertyp wie die primäre Site gehostet werden. Beispiel: Wenn die primäre Site eine Site für Microsoft Internetinformationsdienste ist, müssen alle Backupsites ebenfalls Sites für Microsoft Internetinformationsdienste sein.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Servereinstellungen.
4. Klicken Sie auf Backup.
5. Klicken Sie auf Add.
6. Geben Sie im Feld Backup-URL die URL für die Site ein, mit der die Benutzer verbunden sind. Sie können maximal fünf Backup-URLs pro Site definieren.
7. Klicken Sie auf OK.
8. Markieren Sie bei der Angabe mehrerer Server einen Namen in der Liste und klicken Sie auf Nach oben oder Nach unten, um die Namen in der entsprechenden Failover-Reihenfolge zu sortieren.

So konfigurieren Sie die Siteumleitung

Mit den Einstellungen für die Umleitung definieren Sie, wann Benutzer zu einer anderen Site umgeleitet werden. Beispiel: Sie erstellen eine neue Site für Ihre Personalabteilung und möchten alle Benutzer von der alten Site auf die neue umleiten, ohne dass diese die URL manuell eingeben müssen. Mit der Aufgabe Servereinstellungen in der Citrix Webinterface Management Console können Sie Details der neuen Site angeben. Benutzer werden sofort oder beim nächsten Start des Citrix Online Plug-Ins zur neuen Site umgeleitet.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Servereinstellungen.

4. Klicken Sie auf Umleitung.

5. Wählen Sie eine der folgenden Optionen:

   - Wenn Sie keine Siteumleitung konfigurieren möchten, wählen Sie Nicht umleiten aus.

   - Wenn Sie die Benutzer sofort zu einer alternativen Site umleiten möchten, wählen Sie Nach der Aktualisierung der Citrix Online Plug-In-Konfiguration umleiten aus.

   - Wenn Sie die Benutzer beim nächsten Start des Clients zu einer alternativen Site umleiten möchten, wählen Sie Beim nächsten Start des Citrix Online Plug-Ins umleiten aus.

6. Geben Sie die URL der alternativen Site im Feld Umleitungs-URL ein.

Konfigurieren der Authentifizierung für das Webinterface

Aktualisiert: 2014-11-25

Authentifizierungsmethoden

Die Authentifizierung findet statt, wenn ein Benutzer auf Ressourcen (Anwendungen, Inhalte und Desktops) zugreift. Nach der erfolgreichen Authentifizierung wird die Ressourcengruppe des Benutzers angezeigt.

Sie können die folgenden Authentifizierungsmethoden für das Webinterface konfigurieren:

- **Explizit (XenApp Web-Sites) oder Zugriff bestätigen (XenApp Services-Sites):** Benutzer müssen bei der Anmeldung einen Benutzernamen und ein Kennwort eingeben. Es stehen Benutzerprinzipalnamen (User Principal Names, UPN), domänenbasierte Authentifizierung von Microsoft und Novell Directory Services (NDS) zur Verfügung. Für XenApp Web-Sites ist auch RSA SecurID- und SafeWord-Authentifizierung verfügbar.

  Hinweis: Novell-Authentifizierung ist nicht für Webinterface für Java-Anwendungsserver verfügbar und wird nicht von XenApp 6.0, XenApp 5.0 für Windows Server 2008 oder XenDesktop unterstützt. XenApp 6.0 ist jedoch mit Novell Domain Services für Windows kompatibel.

- **Passthrough:** Benutzer können mit den Anmeldeinformationen authentifiziert werden, die bei der Anmeldung am Windows-Desktop eingegeben wurden. Sie müssen diese Angaben nicht erneut eingeben und ihre Ressourcengruppe wird automatisch angezeigt. Zur Verbindung mit Serverfarmen kann außerdem die mit Kerberos integrierte Windows-Authentifizierung verwendet werden. Wenn Sie die Kerberos-Authentifizierung festlegen und diese Methode fehlschlägt, schlägt die Passthrough-Authentifizierung ebenfalls fehl und es können sich keine Benutzer anmelden. Informationen über Kerberos finden Sie unter Konfigurieren der Kerberos-Anmeldung.

- **Passthrough mit Smartcard:** Benutzer können sich authentifizieren, indem Sie eine Smartcard in den am Benutzergerät angebrachten Smartcardleser einlegen. Wenn Benutzer das Citrix Online Plug-In installiert haben, werden sie aufgefordert, ihre Smartcard-PIN-Nummer einzugeben, wenn Sie sich am Benutzergerät anmelden. Nach der Anmeldung können Benutzer auf Ihre Ressourcen zugreifen, ohne sich erneut anmelden zu müssen. Benutzer, die eine Verbindung zu XenApp Web-Sites herstellen, werden nicht zur Eingabe einer PIN-Nummer aufgefordert. Wenn Sie eine XenApp Services-Site konfigurieren, können Sie mit Kerberos integrierte Windows-Authentifizierung für die Verbindungsherstellung zum Webinterface festlegen. Hierbei werden Smartcards für die Authentifizierung an der Serverfarm verwendet. Wenn Sie die Kerberos-Authentifizierung festlegen und diese Methode fehlschlägt, schlägt die Passthrough-Authentifizierung ebenfalls fehl und es können sich keine Benutzer anmelden.

Hinweis: Da in Windows Vista die Sicherheit verbessert wurde, müssen Smartcard-Benutzer unter Windows Vista oder Windows 7 beim Zugriff auf Anwendungen ihre PIN-Nummern eingeben. Dies ist auch notwendig, wenn Sie Passthrough-mit-Smartcard-Authentifizierung aktiviert haben.

- **Smartcard:** Benutzer können sich mit einer Smartcard authentifizieren. Sie werden aufgefordert, die PIN-Nummer der Smartcard einzugeben.

  Hinweis: Die Authentifizierungsmethoden Passthrough, Passthrough mit Smartcard und Smartcard stehen auf Servern mit Webinterface für Java-Anwendungsserver nicht zur Verfügung.

- **Anonym:** Benutzer können sich ohne Eingabe von Benutzernamen und Kennwort anmelden und auf Ressourcen zugreifen, die für anonyme Benutzer veröffentlicht wurden.

  Wichtig: Anonyme Benutzer können Secure Gateway-Tickets erhalten, obwohl sie nicht vom Webinterface authentifiziert wurden. Da Secure Gateway davon ausgeht, dass das Webinterface nur authentifizierten Benutzern Tickets ausstellt, wird die Sicherheit von Secure Gateway hierbei gefährdet.

  Hinweis: XenDesktop unterstützt keine anonymen Benutzer.

Empfehlungen für die Authentifizierung

Wenn Sie Passthrough-, Passthrough-mit-Smartcard- oder Smartcard-Authentifizierung aktivieren möchten, müssen Sie folgendes beachten:

- Wenn sich Benutzer mit Smartcards an ihren Computern anmelden und Sie Passthrough-Authentifizierung aktivieren möchten. aktivieren Sie die Option für Kerberos-Authentifizierung.

- Wenn sich Benutzer mit expliziten Anmeldeinformationen an ihren Computern anmelden, aktivieren Sie für diese Benutzer nicht Smartcard- oder Passthrough-mit-Smartcard-Authentifizierung für den Zugriff auf das Webinterface.

  Hinweis: Benutzern, die sich mit expliziten Anmeldeinformationen an Windows anmelden und dann auf eine Site zugreifen, die für Passthrough-mit-Smartcard-Authentifizierung konfiguriert ist, wird ein Dialogfeld Willkommen bei Windows beim Zugriff auf Ressourcen angezeigt. Benutzer müssen die rechte ALT-Taste (ALT GR) und ENTF drücken, um das Dialogfeld zu schließen. Citrix empfiehlt, separate Sites für Benutzer, die sich mit Smartcards anmelden, und für Benutzer, die sich mit expliziten Anmeldeinformationen anmelden, zu erstellen.

Wenn Sie die Webinterface-Authentifizierungsmethoden ändern, erhalten Benutzer die zurzeit angemeldet sind, möglicherweise Fehlermeldungen. Wenn diese Benutzer mit einem Webbrowser auf das Webinterface zugreifen, müssen Sie ihren Browser schließen und neu starten, bevor sie sich erneut anmelden können.

Konfigurieren der Authentifizierung

Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console können Sie konfigurieren, wie Benutzer sich bei XenApp, XenDesktop und dem Citrix Online Plug-In authentifizieren können.

So konfigurieren Sie Domäneneinschränkungen

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und stellen Sie sicher, dass nicht nur anonyme Authentifizierung für Benutzer aktiviert ist.
4. Klicken Sie auf Eigenschaften und wählen Sie Domäneneinschränkung.
5. Geben Sie an, ob Sie den Zugriff auf Benutzer bestimmter Domänen einschränken möchten. Wählen Sie eine der folgenden Optionen:
   - Wenn Sie den Zugriff nicht auf der Grundlage von Domänen einschränken möchten, wählen Sie Alle Domänen zulassen.
   - Wenn Sie den Zugriff auf Benutzer bestimmter Domänen beschränken möchten, wählen Sie Nur folgende Domänen zulassen.
6. Klicken Sie auf Add.
7. Geben Sie die Namen der Domänen, die Sie der Liste der Domäneneinschränkungen hinzufügen möchten, im Feld Anmeldedomäne ein.

   Hinweis: Um den Zugriff auf Benutzer bestimmter Domänen einzuschränken, müssen Sie dieselben Domänennamen in den Listen für Domäne und UPN-Einschränkung eingeben. Weitere Informationen finden Sie unter So verwenden Sie domänenbasierte Authentifizierung.

So konfigurieren Sie Einstellungen für automatische Anmeldung

Konfigurieren Sie mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console Einstellungen für automatische Anmeldung für Benutzer, die mit den Authentifizierungsmethoden "Passthrough", "Passthrough mit Smartcard" und "Smartcard" auf veröffentlichte Ressourcen zugreifen.

Wenn anonyme Authentifizierung als einzige Authentifizierungsmethode für Benutzer aktiviert ist, werden sie automatisch angemeldet, unabhängig von den vom Administrator oder Benutzer konfigurierten Einstellungen.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie eines oder mehr der Kontrollkästchen Passthrough, Passthrough mit Smartcard und Smartcard.

4. Klicken Sie auf Eigenschaften und wählen Sie Automatische Anmeldung.

5. Geben Sie an, ob Sie zulassen möchten, dass Benutzer automatisch angemeldet werden, und ob Benutzer auf der Seite Kontoeinstellungen die Option sehen, mit der sie automatische Anmeldung aktivieren und deaktivieren können.

So verwenden Sie domänenbasierte Authentifizierung

Wenn Sie die Authentifizierungsmethoden "Explizit" oder "Zugriff bestätigen" verwenden, konfigurieren Sie mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console, ob Benutzer sich mit Windows oder Novell Directory Services (NDS) authentifizieren.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie nach Bedarf die Kontrollkästchen Explizit, Zugriff bestätigen und/oder Passthrough.

4. Klicken Sie auf Eigenschaften und wählen Sie Authentifizierungstyp.

5. Wählen Sie Windows oder NIS (UNIX).

6. Geben Sie das Format für Benutzeranmeldeinformationen ein. Wählen Sie eine der folgenden Optionen:

   - Wenn Sie es Benutzern ermöglichen möchten, bei der Anmeldung UPN oder Domänenbenutzernamen zu verwenden, klicken Sie auf Domänenbenutzername und UPN.

   - Wenn Sie festlegen möchten, dass Benutzer bei der Anmeldung nur den Domänenbenutzernamen eingeben können, klicken Sie auf Nur Domänenbenutzername.

   - Wenn Sie festlegen möchten, dass Benutzer bei der Anmeldung nur den UPN verwenden können, klicken Sie auf Nur UPN.

7. Klicken Sie auf Einstellungen.

8. Konfigurieren Sie im Bereich Domänenanzeige die folgenden Einstellungen:

   - Geben Sie an, ob das Feld Domäne auf der Seite Anmeldung angezeigt werden soll.

   - Geben Sie an, ob das Feld Domäne bereits eine Reihe von Domänen enthält, aus denen Benutzer eine Auswahl treffen können, oder ob Benutzer manuell einen Wert in das Feld Domäne eingeben müssen.

     Hinweis: Wenn Benutzer bei der Anmeldung eine Fehlermeldung erhalten, dass eine Domäne angegeben werden muss, kann die Ursache ein leeres Feld Domäne sein. Wählen Sie Domänenfeld ausblenden aus, um dieses Problem zu lösen. Wenn Ihre Farm nur aus Servern besteht, auf denen XenApp für UNIX ausgeführt wird, wählen Sie in der Dropdownliste Domänenliste die Option Bereits ausgefüllt aus und fügen Sie UNIX als Domänenname hinzu.

- Geben Sie die Domänen an, die auf der Seite Anmeldung im Feld Domäne angezeigt werden sollen.

9. Konfigurieren Sie im Bereich UPN-Einschränkung die folgenden Einstellungen:

   - Legen Sie fest, ob alle UPN-Suffixe akzeptiert werden. Standardmäßig sind alle UPN-Suffixe zugelassen.

   - Geben Sie die UPN-Suffixe an, die Sie akzeptieren möchten.

     Hinweis: Um den Zugriff auf Benutzer bestimmter Domänen einzuschränken, müssen Sie dieselben Domänennamen in den Listen für Domäne und UPN-Einschränkung eingeben. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung.

So verwenden Sie Novell Directory Services-Authentifizierung

Wenn Sie die Authentifizierungsmethoden "Explizit" oder "Zugriff bestätigen" verwenden, konfigurieren Sie mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console, ob Benutzer sich mit Windows oder Novell Directory Services (NDS) authentifizieren.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie nach Bedarf die Kontrollkästchen Explizit, Zugriff bestätigen und/oder Passthrough.

4. Klicken Sie auf Eigenschaften und wählen Sie Authentifizierungstyp.

5. Aktivieren Sie die Option NDS.

6. Geben Sie im Feld Standardstrukturname einen Namen ein.

7. Klicken Sie auf Einstellungen und konfigurieren Sie je nach Bedarf Kontexteinschränkung oder kontextlose Authentifizierung.

   Hinweis: Standardmäßig gibt eDirectory keinen anonymen Verbindungszugriff für das cn-Attribut, das für die kontextlose Anmeldung erforderlich ist. Weitere Informationen zur Neukonfiguration von eDirectory finden Sie unter http://developer.novell.com/wiki/index.php/Developer_Home.

8. Wählen Sie für XenApp Services-Sites die Option Windows-Anmeldeinformationen, wenn Citrix Online Plug-In-Benutzer, die den Novell Client installiert haben, ihre Windows-Anmeldeinformationen für die Passthrough-Authentifizierung verwenden sollen.

Aktivieren der expliziten Authentifizierung

Wenn explizite Authentifizierung aktiviert ist, benötigen Benutzer für die Anmeldung ein Benutzerkonto und die entsprechenden Anmeldeinformationen.

Sie können die Einstellungen für die explizite Authentifizierung mit der Konsole ändern. Sie können es Benutzern z. B. ermöglichen, das Kennwort in einer Sitzung zu ändern.

Explizite Authentifizierung steht nur für XenApp Web-Sites zur Verfügung.

So aktivieren Sie explizite Authentifizierung

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Explizit.

4. Klicken Sie auf Eigenschaften, um weitere Einstellungen für die explizite Authentifizierung zu konfigurieren.

So konfigurieren Sie Kennworteinstellungen für die explizite Authentifizierung

Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console konfigurieren Sie, ob Benutzer ihre Kennwörter ändern können und ob Benachrichtigungen vor dem Kennwortablauf angezeigt werden. Einige Kennworteinstellungen werden von anderen Authentifizierungseinstellungen einer Site beeinflusst:

- Die Option Jederzeit ist abgeblendet, wenn Sie auf der Seite Zweifaktorauthentifizierung die Optionen RSA SecurID und Windows-Kennwortintegration verwenden aktivieren.
- Wenn Sie die Option Erinnerungseinstellungen der Active Directory-Gruppenrichtlinie verwenden aktivieren, bedeutet dies, dass Erinnerungseinstellungen basierend auf Ihrer aktuellen Windows-Richtlinie konfiguriert werden. Wenn Ihre aktuelle Windows-Richtlinie keinen Erinnerungszeitraum enthält, werden Benutzer nicht zum Ändern ihres Kennworts aufgefordert, bevor es abläuft.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Explizit.
4. Klicken Sie auf Eigenschaften und wählen Sie Kennworteinstellungen.
5. Wenn Benutzer in der Lage sein sollen, ihre Anmeldekennwörter in einer Webinterface-Sitzung ändern zu können, aktivieren Sie das Kontrollkästchen Benutzer können Kennwörter ändern.
6. Wählen Sie eine der folgenden Optionen aus, um anzugeben, wann Benutzer ihr Kennwort ändern können:
   - Wenn Benutzer ihr Kennwort bei Ablauf ändern können sollen, wählen Sie Nur bei Ablauf aus. Wenn Sie diese Option wählen, werden Benutzer, wenn sie sich aufgrund eines abgelaufenen Kennworts nicht anmelden können, zum Dialogfeld für die Kennwortänderung weitergeleitet. Nach der Kennwortänderung werden Benutzer automatisch mit dem neuen Kennwort angemeldet.
   - Damit Benutzer ihre Kennwörter beliebig oft ändern können, wählen Sie Jederzeit. Wenn Sie diese Option wählen, sehen die Benutzer die Schaltfläche Kennwort ändern auf den Seiten Anwendungen und Kontoeinstellungen. Wenn Benutzer auf diese Schaltfläche klicken, wird ein Dialogfeld eingeblendet, in dem Benutzer das

neue Kennwort eingeben können.

7. Wenn Sie Benutzern vor dem Ablauf des Kennworts eine Erinnerung schicken möchten, wählen Sie eine der folgenden Optionen:

   · Wenn Sie Benutzer nicht benachrichtigen möchten, bevor ihr Kennwort abläuft, wählen Sie Nicht erinnern.

   · Wenn Sie die aktuellen Benachrichtigungseinstellungen der Windows-Richtlinie verwenden möchten, wählen Sie Erinnerungseinstellungen der Active Directory-Gruppenrichtlinie verwenden.

   · Wenn Sie Benutzer erinnern möchten, dass ihr Kennwort in einer bestimmten Anzahl von Tagen abläuft, wählen Sie Benutzerdefinierte Erinnerungseinstellungen verwenden. Geben Sie in den Feldern Benutzer ... vor Ablauf erinnern den gewünschten Zeitraum in Tagen, Wochen oder Jahren ein.

So aktivieren Sie die Zweifaktorauthentifizierung

Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console können Sie bei Bedarf Zweifaktorauthentifizierung aktivieren.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Explizit.

4. Klicken Sie auf Eigenschaften und wählen Sie Zweifaktorauthentifizierung.

5. Wählen Sie in der Liste Zweifaktoreinstellung den Typ der Zweifaktorauthentifizierung, den Sie verwenden möchten, aus und konfigurieren Sie nach Bedarf weitere Einstellungen.

Weitere Informationen zum Konfigurieren von Aladdin SafeWord-, RSA SecurID- und RADIUS-Authentifizierung finden Sie unter Konfigurieren der Zweifaktorauthentifizierung.

Konfigurieren von Konto-Self-Service

Durch die Integration der Password Manager-Funktion Konto-Self-Service können Benutzer, die Password Manager verwenden, ihr Netzwerkkennwort zurücksetzen und die Sperrung ihres Kontos aufheben, indem sie eine Reihe von Sicherheitsfragen beantworten.

Wenn Sie Konto-Self-Service für eine Site aktivieren, werden wichtige Sicherheitsfunktionenen für alle Benutzer verfügbar, die auf die Site zugreifen können. Wenn auf die Site über das Internet zugegriffen werden kann, gibt es keine Beschränkung, wer auf diese Funktionen zugreifen kann. Wenn Ihre Firma über eine Sicherheitsrichtlinie verfügt, die die Verwendung von Benutzerkontoverwaltungsfunktionen auf interne Mitarbeiter beschränkt, müssen Sie sicherstellen, dass ein Zugriff auf die Site von außerhalb ihres internen Netzwerks nicht möglich ist.

Wichtig: Wenn Sie Password Manager einrichten, geben Sie an, welche Benutzer Kennwortrücksetzungen durchführen und die Sperrung ihrer Konten aufheben dürfen. Wenn Sie diese Funktionen für das Webinterface aktivieren, wird Benutzern unter Umständen aufgrund der in Password Manager konfigurierten Einstellungen dennoch die Ausführung dieser Aufgaben verweigert.

Konto-Self-Service steht nur den Benutzern zur Verfügung, die über HTTPS-Verbindungen auf das Webinterface zugreifen. Wenn Benutzer versuchen, über eine HTTP-Verbindung auf das Webinterface zuzugreifen, steht Konto-Self-Service nicht zur Verfügung. Konto-Self-Service ist nicht für in Access Gateway integrierte Sites verfügbar.

Konto-Self-Service unterstützt keine UPN-Anmeldungen, wie z. B. *Benutzername*@*Domäne*.com.

Bevor Sie Konto-Self-Service konfigurieren, müssen Sie Folgendes beachten:

- Die Site ist für explizite Windows-basierte Authentifizierung konfiguriert.
- Die Site ist für die Verwendung von nur einem Password Manager-Dienst konfiguriert. Wenn das Webinterface mehrere Farmen innerhalb derselben oder innerhalb vertrauenswürdiger Domänen verwenden soll, muss Password Manager so konfiguriert sein, dass Anmeldeinformationen von allen diesen Domänen akzeptiert werden.
- Die Site ist so konfiguriert, dass Benutzer jederzeit Kennwörter ändern können. Dies ist Voraussetzung dafür, dass Sie Kennwortzurücksetzung aktivieren können.

So konfigurieren Sie Konto-Self-Service

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Explizit.

4. Klicken Sie auf Eigenschaften und wählen Sie Konto-Self-Service.

5. Geben Sie an, ob Benutzer in der Lage sein sollen, ihre Kennwörter zurückzusetzen und die Sperrung ihrer Konten aufzuheben.

6. Geben Sie die URL für Password Manager im Feld Password Manager-Dienst-URL ein.

Aktivieren der Authentifizierungsmethode "Zugriff bestätigen"

Aktualisiert: 2014-11-24

Wenn Authentifizierung mit Zugriffsbestätigung aktiviert ist, benötigen Benutzer für die Anmeldung ein Benutzerkonto und die entsprechenden Anmeldeinformationen.

Die Authentifizierungsmethode "Zugriff bestätigen" steht nur für XenApp Services-Sites zur Verfügung.

So aktivieren Sie die Authentifizierungsmethode "Zugriff bestätigen"

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Zugriff bestätigen.
4. Klicken Sie auf Eigenschaften, um weitere Einstellungen für die Authentifizierungsmethode "Zugriff bestätigen" zu konfigurieren.

So konfigurieren Sie Kennworteinstellungen für "Zugriff bestätigen für Authentifizierung"

Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console können Sie angeben, ob Benutzer ihre Kennwörter speichern können, und die Optionen für das Ändern von Kennwörtern konfigurieren.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Zugriff bestätigen.
4. Klicken Sie auf Eigenschaften und wählen Sie Kennworteinstellungen.

5. Wenn Benutzer ihre Kennwörter speichern können sollen, wählen Sie die Option Benutzer können Kennwörter speichern.

6. Wenn Sie möchten, dass Benutzer ihre Kennwörter ändern können, wenn diese abgelaufen sind, aktivieren Sie das Kontrollkästchen Benutzer können abgelaufene Kennwörter an folgenden Stellen ändern.

7. Geben Sie den Pfad an, über den Anfragen für Kennwortänderungen ausgeführt werden sollen, indem Sie eine der folgenden Optionen wählen:

   · Wenn Citrix Online Plug-In-Benutzer ihre Kennwörter ändern sollen, indem sie eine Verbindung direkt zum Domänencontroller herstellen, wählen Sie Domänencontroller. Dies ist die sicherste Option, da die Anfrage zum Ändern des Kennworts vom Citrix Online Plug-In direkt an den Domänencontroller gesendet wird und das Webinterface und XenApp/XenDesktop umgangen werden.

   · Wenn Citrix Online Plug-In-Benutzer ihre Kennwörter vorzugsweise über eine direkte Verbindung zum Domänencontroller ändern sollen, Sie aber trotzdem Verbindungen über das Webinterface und XenApp/XenDesktop zulassen möchten für den Fall, dass die bevorzugte Methode fehlschlägt, wählen Sie Domänencontroller mit Fallback auf Serverfarm.

   · Wenn Citrix Online Plug-In-Benutzer ihre Kennwörter ändern sollen, indem Sie über das Webinterface und XenApp/XenDesktop eine Verbindung zum Domänencontroller herstellen, wählen Sie Serverfarm. Mit dieser Option wird sichergestellt, dass das Webinterface plus XenApp und/oder XenDesktop mit dem neuen Kennwort aktualisiert werden, wenn Benutzer Kennwörter ändern. Diese Methode ist allerdings möglicherweise nicht so sicher, da das neue Kennwort über eine größere Anzahl von Netzwerkverbindungen geleitet wird.

Aktivieren der Passthrough-Authentifizierung

Aktualisiert: 2013-02-21

Für Benutzer, die sich mit ihrem Benutzernamen, ihrem Kennwort und ihrer Domäne an ihrem Desktop anmelden, können Sie unter Verwendung der Konsole die Passthrough-Authentifizierung aktivieren. Mit dieser Funktion können Benutzer mit den Anmeldeinformationen authentifiziert werden, die bei der Anmeldung am Windows-Desktop eingegeben wurden. Sie müssen diese Informationen nicht erneut eingeben und ihre Ressourcengruppe wird automatisch angezeigt.

Passthrough-Anforderungen

Damit die Passthrough-Authentifizierung verwendet werden kann, muss das Webinterface in IIS ausgeführt werden und Benutzer müssen unterstützte Versionen von Internet Explorer ausführen. Für XenApp Web-Sites müssen Benutzer die Site in Internet Explorer den Zonen "Vertrauenswürdige Zonen" oder "Lokales Intranet" hinzufügen.

Wenn Sie Internet Explorer Version 7 oder höher verwenden:

1. Fügen Sie die Site den vertrauenswürdigen Sites in Windows hinzu, klicken Sie auf "Internetoptionen" und navigieren Sie zu der Registerkarte "Sicherheit".

2. Markieren Sie die Zone "Vertrauenswürdige Sites" und klicken Sie auf "Stufe anpassen".

3. Navigieren Sie in den Sicherheitseinstellungen zu "Benutzerauthentifizierung", klicken Sie auf "Anmeldung" und stellen Sie "Automatische Anmeldung mit aktuellem Benutzernamen und Kennwort" ein.

Für IIS 7.*x* unter Windows Server 2008 müssen Sie sicherstellen, dass der Rollendienst Webserver > Sicherheit > Windows-Authentifizierung für die Rolle Webserver (IIS) aktiviert ist.

Wichtig: Wird auf den Servern eine frühere Version als Citrix MetaFrame XP Feature Release 2 ausgeführt, werden für die Benutzer bei aktiviertem Passthrough möglicherweise alle Anwendungen angezeigt.

Wenn Benutzer Versionen der Clients für Windows vor 6.30 verwenden und die ICA-Verschlüsselung (SecureICA) aktiviert ist, kann Passthrough nicht verwendet werden. Um Passthrough mit ICA-Verschlüsselung verwenden zu können, müssen die Benutzer die aktuellsten Citrix Clients installiert haben. Passthrough-Authentifizierung ist mit dem Webinterface für Java-Anwendungsserver nicht verfügbar.

Wichtig: Wenn ein Benutzer auf eine Ressource zugreift, wird eine Datei an den Citrix Client gesendet (in einigen Fällen mit dem Webbrowser als Vermittler). Die Datei kann eine Anweisung für den Client enthalten, die Anmeldeinformationen der Benutzer-Arbeitsstationen an den Server zu übermitteln. Der Client ignoriert diese

Einstellung standardmäßig. Ist jedoch Passthrough auf dem Citrix Online Plug-In aktiviert, könnte ein Angreifer dem Benutzer eine Datei senden, die die Anmeldeinformationen des Benutzers an einen nicht autorisierten oder falschen Server weiterleitet. Verwenden Sie Passthrough daher nur in sicheren, vertrauenswürdigen Umgebungen.

Schritt 1: Installieren des Plug-Ins für die Passthrough-Authentifizierung

Aktualisiert: 2014-12-02

Sie müssen das Citrix Online Plug-In oder das Citrix Desktop Viewer mit einem Administratorkonto auf den Geräten der Benutzer installieren. Passthrough-Authentifizierung ist nur in den Plug-Ins verfügbar, die auf den XenApp- und XenDesktop-Installationsmedien enthalten sind. Aus Sicherheitsgründen ist diese Funktion im Citrix Online Web Plug-In nicht enthalten. Aus diesem Grund können Sie Benutzern mit der webbasierten Plug-In-Installation keine Citrix Plug-Ins bereitstellen, die diese Funktion enthalten.

Nach der Installation müssen Sie mit einer Gruppenrichtlinie die Passthrough-Authentifizierung für alle Citrix Clients aktivieren. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX122676 und in der archivierten Dokumentation für das Online Plug-In für Windows.

Schritt 2: Aktivieren von Passthrough für die Plug-Ins

Dieser Vorgang besteht aus zwei Schritten. Zuerst fügen Sie dem Gruppenrichtlinienobjekt-Editor die Clientvorlage hinzu. Anschließend können Sie mit dieser Vorlage Passthrough-Authentifizierung für alle Clients aktivieren.

So fügen Sie dem Gruppenrichtlinienobjekt-Editor die Clientvorlage für die Passthrough-Authentifizierung hinzu

1. Öffnen Sie das MMC-Snap-In Gruppenrichtlinienobjekt-Editor.
2. Wählen Sie das Gruppenrichtlinienobjekt aus, das Sie bearbeiten möchten.
3. Wählen Sie den Knoten Administrative Vorlagen und klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen und gehen Sie zu der Clientvorlagendatei, icaclient.adm. Diese Datei ist im Ordner \Configuration für die Clients installiert, normalerweise unter C:\Programme (x86)\Citrix*Clientname*\Configuration.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und anschließend auf Schließen.

So aktivieren Sie die Passthrough-Authentifizierung für alle Clients

1. Öffnen Sie das MMC-Snap-In Gruppenrichtlinienobjekt-Editor.
2. Wählen Sie das Gruppenrichtlinienobjekt aus, das Sie bearbeiten möchten.
3. Erweitern Sie im linken Bereich den Knoten Administrative Vorlagen.
4. Wählen Sie Klassische administrative Vorlage (ADM) > Citrix Components. Erweitern Sie den Knoten des Clients, den Sie installiert haben, und wählen Sie User authentication.
5. Wählen Sie im Ergebnisbereich die Option Local user name and password aus.
6. Klicken Sie im Menü Aktion auf Eigenschaften.
7. Klicken Sie auf Aktiviert und überprüfen Sie, ob das Kontrollkästchen Enable pass-through authentication aktiviert ist.
8. Stellen Sie sicher, dass diese Schritte für den Benutzer und den Computer im Gruppenrichtlinienobjekt-Editor durchgeführt werden.
9. Melden Sie sich ab und melden Sie sich wieder an, damit Ihre Richtlinienänderungen wirksam werden.

Schritt 3: Aktivieren von Passthrough mit der Konsole

Aktivieren Sie die Passthrough-Authentifizierung mit der Citrix Webinterface Management Console. Ist diese Funktion aktiviert, müssen Benutzer die Anmeldeinformationen nicht erneut eingeben und die Ressourcengruppe wird automatisch angezeigt.

Außerdem können Sie Kerberos mit Passthrough-Authentifizierung für XenApp Web- und XenApp Services-Sites aktivieren. Bei XenApp Services-Sites können Sie auch Kerberos für Passthrough-mit-Smartcard-Authentifizierung festlegen.

So aktivieren Sie Passthrough-Authentifizierung

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie das Kontrollkästchen Passthrough.

4. Klicken Sie auf Eigenschaften und wählen Sie Kerberos-Authentifizierung.

5. Wenn Sie Kerberos-Authentifizierung aktivieren möchten, aktivieren Sie das Kontrollkästchen Kerberos-Authentifizierung für Verbindung zu Servern verwenden (für XenApp Web-Sites) oder Nur Kerberos verwenden (für XenApp Services-Sites).

Aktivieren der Smartcard-Authentifizierung

Aktualisiert: 2014-12-02

Damit die Smartcard-Authentifizierung verwendet werden kann, muss das Webinterface in IIS ausgeführt werden und Benutzer müssen unterstützte Versionen von Internet Explorer oder Firefox ausführen. Um Passthrough-mit-Smartcard-Authentifizierung verwenden zu können, müssen Benutzer eine unterstützte Version von Internet Explorer ausführen; Firefox wird nicht für Passthrough-mit-Smartcard-Authentifizierung unterstützt.

Wenn Sie Passthrough-mit-Smartcard-Authentifizierung für eine XenApp Web-Site aktivieren möchten, müssen Benutzer die Site in Internet Explorer den Zonen "Vertrauenswürdige Sites" oder "Lokales Intranet" hinzufügen.

Wenn IIS 7.*x* unter Windows Server 2008 ausgeführt wird, muss der Rollendienst Webserver > Sicherheit > Clientzertifikatzuordnung-Authentifizierung für die Rolle Webserver (IIS) aktiviert sein. Wenn Sie Passthrough-mit-Smartcard-Authentifizierung aktivieren möchten, müssen Sie sicherstellen, dass der Rollendienst Webserver > Sicherheit > Windows-Authentifizierung aktiviert ist.

Smartcard-Authentifizierung wird vom Webinterface für Java-Anwendungsserver nicht unterstützt.

Auf dem Webserver muss SSL (Secure Sockets Layer) aktiviert sein, da für die Kommunikation zwischen dem Webbrowser und dem Server SSL verwendet wird. Weitere Informationen finden Sie in der Dokumentation Ihres Webservers.

Um Smartcard-Authentifizierung zu aktivieren (mit oder ohne andere Authentifizierungsmethoden), müssen Sie die Seite Anmeldung konfigurieren, damit nur über HTTPS-Verbindungen darauf zugegriffen werden kann. Bei Verwendung von HTTP oder falsch konfiguriertem HTTPS erhalten Benutzer eine Fehlermeldung und können sich nicht anmelden. Um dieses Problem zu vermeiden, stellen Sie die vollständige HTTPS-URL für alle Benutzer zur Verfügung. Beispiel: https://www.*Unternehmen.com*:443/Citrix/XenApp.

Weitere Informationen zu den Anforderungen an Benutzergerät und Server für die Smartcard-Authentifizierung finden Sie unter Verwenden von Smartcards mit XenApp.

Schritt 1: Installieren des Plug-Ins für die Smartcard-Authentifizierung

Um Smartcard-Authentifizierung zu verwenden, müssen Benutzer das Citrix Online Plug-In oder den Citrix Desktop Viewer installieren. Eine andere Möglichkeit ist es, mit der webbasierten Clientinstallation das Citrix Online Plug-In – Web von einer entsprechend konfigurierten XenApp Web-Site herunterzuladen und zu installieren. Um jedoch Passthrough-mit-Smartcard-Authentifizierung verwenden zu können, müssen Sie das Citrix Online Plug-In oder den Citrix Desktop Viewer mit einem Administratorkonto auf den Geräten der Benutzerinstallieren. Passthrough-Authentifizierung ist nur in den Plug-Ins verfügbar, die auf den XenApp- und XenDesktop-Installationsmedien enthalten sind. Aus Sicherheitsgründen ist diese Funktion im Citrix Online Web Plug-In nicht enthalten.

Wenn Sie Passthrough-mit-Smartcard-Authentifizierung aktivieren, müssen Sie nach der Installation der Plug-Ins die Passthrough-Authentifizierung für alle Citrix Clients mit einer Gruppenrichtlinie aktivieren. Dieser Vorgang besteht aus zwei Schritten. Zuerst fügen Sie dem Gruppenrichtlinienobjekt-Editor die Clientvorlage hinzu. Anschließend können Sie mit dieser Vorlage Passthrough-Authentifizierung für alle Clients aktivieren.

So fügen Sie dem Gruppenrichtlinienobjekt-Editor die Clientvorlage für die Passthrough-Authentifizierung hinzu

1. Öffnen Sie das MMC-Snap-In Gruppenrichtlinienobjekt-Editor.
2. Wählen Sie das Gruppenrichtlinienobjekt aus, das Sie bearbeiten möchten.
3. Wählen Sie den Knoten Administrative Vorlagen und klicken Sie im Menü Aktion auf Vorlagen hinzufügen/entfernen.
4. Klicken Sie auf Hinzufügen und gehen Sie zu der Clientvorlagendatei, icaclient.adm. Diese Datei ist im Ordner \Configuration für die Clients installiert, normalerweise unter C:\Programme (x86)\Citrix*Clientname*\Configuration.
5. Klicken Sie auf Öffnen, um die Vorlage hinzuzufügen, und anschließend auf Schließen.

So aktivieren Sie Passthrough-mit-Smartcard-Authentifizierung für alle Clients

1. Öffnen Sie das MMC-Snap-In Gruppenrichtlinienobjekt-Editor.
2. Wählen Sie das Gruppenrichtlinienobjekt aus, das Sie bearbeiten möchten.
3. Erweitern Sie im linken Bereich den Knoten Administrative Vorlagen.
4. Wählen Sie Klassische administrative Vorlage (ADM) > Citrix Components. Erweitern Sie den Knoten des Clients, den Sie installiert haben, und wählen Sie User authentication.
5. Wählen Sie im Ergebnisbereich die Option Smart card authentication.
6. Klicken Sie im Menü Aktion auf Eigenschaften.
7. Klicken Sie auf Aktiviert und aktivieren Sie die Kontrollkästchen Allow smart card authentication und Use pass-through authentication for PIN.

Schritt 2: Aktivieren des Verzeichnisdienst-Zuordnungsprogramms von Windows

Um Smartcard-Authentifizierung zu aktivieren, müssen Sie sicherstellen, dass das Verzeichnisdienst-Zuordnungsprogramm von Windows auf dem Webinterface-Server aktiviert ist.

Bei der Webinterface-Authentifizierung werden Windows-Domänenkonten verwendet, d. h. die Anmeldeinformationen (Benutzername und Kennwort). Smartcards enthalten jedoch Zertifikate. Das Verzeichnisdienst-Zuordnungsprogramm verwendet Windows Active Directory, um ein Zertifikat einem Windows-Domänenkonto zuzuordnen.

So aktivieren Sie das Verzeichnisdienst-Zuordnungsprogramm von Windows in Microsoft Internetinformationsdienste 7.x

1. Stellen Sie auf dem Webinterface-Server sicher, dass der Rollendienst Webserver > Sicherheit > Clientzertifikatzuordnung-Authentifizierung für die Rolle Webserver (IIS) *nicht* installiert ist.

2. Öffnen Sie das MMC-Snap-In Internetinformationsdienste-Manager.

3. Wählen Sie Ihren Webserver im linken Bereich aus und klicken Sie unter Featureübersicht auf Authentifizierung.

4. Aktivieren Sie auf der Seite Authentifizierung die Methode Active Directory-Clientzertifikat-Authentifizierung.

So aktivieren Sie das Verzeichnisdienst-Zuordnungsprogramm von Windows in Microsoft Internetinformationsdienste 6.0

1. Öffnen Sie das MMC-Snap-In Internetinformationsdienste-Manager auf dem Webinterface-Server.

2. Wählen Sie den Knoten Sites unter dem Webinterface-Server aus und klicken Sie im Bereich Aktionen auf Eigenschaften.

3. Klicken Sie auf der Registerkarte Verzeichnissicherheit im Bereich Sichere Kommunikation auf Verzeichnisdienst-Zuordnungsprogramm von Windows aktivieren.

Schritt 3: Aktivieren der Smartcard-Authentifizierung auf dem Webinterface

Sie müssen die Smartcard-Authentifizierung im Webinterface (damit Benutzer auf das Webinterface und ihre Ressourcen zugreifen können) und auf dem Server konfigurieren (damit Benutzer mit dem Webinterface Ressourcen in einer Sitzung starten können).

So aktivieren Sie Smartcard-Authentifizierung für XenApp Web-Sites

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie nach Bedarf das Kontrollkästchen Smartcard oder Passthrough mit Smartcard.

4. Klicken Sie auf Eigenschaften, um weitere Einstellungen für die Smartcard-Authentifizierung zu konfigurieren.

So aktivieren Sie Smartcard-Authentifizierung für XenApp Services-Sites

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden und aktivieren Sie nach Bedarf das Kontrollkästchen Smartcard oder Passthrough mit Smartcard.

4. Klicken Sie auf Eigenschaften und wählen Sie Roaming.

5. Um das Verhalten des Webinterface beim Entfernen einer Smartcard zu konfigurieren, wählen Sie Roaming aktivieren und wählen Sie eine der folgenden Optionen aus:

   - Wenn die Benutzersitzung getrennt werden soll, wenn die Smartcard entfernt wird, wählen Sie Sitzungen nach Entfernen der Smartcard trennen.

   - Wenn die Benutzersitzung abgemeldet werden soll, wenn die Smartcard entfernt wird, wählen Sie Sitzungen nach Entfernen der Smartcard abmelden.

6. Wenn Sie Passthrough-mit-Smartcard-Authentifizierung aktiviert haben und Kerberos-Authentifizierung zwischen dem Plug-In und der XenApp Services-Site verwenden möchten, klicken Sie auf Kerberos-Authentifizierung und aktivieren Sie das Kontrollkästchen Kerberos für die Authentifizierung an der XenApp Services-Site verwenden.

Beispiel: Aktivieren der Smartcard-Authentifizierung für Benutzer

Sie möchten Passthrough-mit-Smartcard-Authentifizierung für einen Benutzer aktivieren. Auf dem Computer des Benutzers wird Windows XP ausgeführt. An den Computer ist ein Smartcardleser angeschlossen und in der Serverfarm ist Smartcard-Unterstützung konfiguriert. Das Webinterface ist im Augenblick nur für explizite Authentifizierung/Authentifizierung mit Zugriff bestätigen konfiguriert (Benutzername und Kennwort).

So aktivieren Sie Passthrough-mit-Smartcard-Authentifizierung

1. Verwenden Sie das entsprechende Installationsmedium, um das Citrix Online Plug-In oder Citrix Desktop Viewer auf dem Computer des Benutzers zu installieren. Die Installation des Plug-Ins wird mit einem Administratorkonto ausgeführt. Fügen Sie für XenApp Web-Sites auf dem Computer des Benutzers die Site in Internet Explorer den Zonen "Vertrauenswürdige Zonen" oder "Lokales Intranet" hinzu.

2. Aktivieren Sie mit einer Gruppenrichtlinie Passthrough-Authentifizierung für alle Citrix Clients. Weitere Informationen finden Sie unter Schritt 1: Installieren des Plug-Ins für die Smartcard-Authentifizierung. Sie müssen auch sicherstellen, dass Passthrough-Authentifizierung in der Farm aktiviert ist. Weitere Informationen finden Sie in der Dokumentation für den Citrix Server.

3. Das Verzeichnisdienst-Zuordnungsprogramm von Windows muss aktiviert sein. Weitere Informationen finden Sie unter Schritt 2: Aktivieren des Verzeichnisdienst-Zuordnungsprogramms von Windows.

4. Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console können Sie Passthrough-mit-Smartcard-Authentifizierung aktivieren. Weitere Informationen finden Sie unter Schritt 3: Aktivieren der Smartcard-Authentifizierung auf dem Webinterface. Benutzer melden sich mit Smartcards an ihren realen Windows-Desktops an. Wenn Benutzer auf ihre Ressourcen zugreifen, werden Sie automatisch angemeldet. Wenn Smartcard-Authentifizierung ohne Passthrough aktiviert ist, müssen Benutzer ihre PIN-Nummer beim Zugriff auf Ressourcen erneut eingeben.

Konfigurieren der Zweifaktorauthentifizierung

Für XenApp Web-Sites können Sie die folgenden Zweifaktorauthentifizierungsmethoden konfigurieren:

- **Aladdin SafeWord for Citrix:** Eine Authentifizierungsmethode, bei der mit alphanumerischen Codes, die aus SafeWord-Token und (optional) PIN-Nummern erzeugt werden, ein Passcode erstellt wird. Benutzer geben die Domänenanmeldeinformationen und SafeWord-Passcodes auf der Seite Anmeldung ein und können dann auf Anwendungen auf dem Server zugreifen.

- **RSA SecurID:** Eine Authentifizierungsmethode, bei der aus von RSA SecurID-Token generierten Nummern (*Tokencodes*) und PIN-Nummern ein *PASSCODE* generiert wird. Benutzer geben die Benutzernamen, Domänen, Kennwörter und RSA SecurID-PASSCODES auf der Seite Anmeldung ein und können dann auf Ressourcen auf dem Server zugreifen. Beim Erstellen von Benutzern auf dem RSA ACE/Server müssen die Anmeldenamen mit den Domänenbenutzernamen übereinstimmen.

  Hinweis: Wenn Sie RSA SecurID-Authentifizierung verwenden, kann vom System eine neue PIN-Nummer für den Benutzer erstellt und angezeigt werden. Diese PIN-Nummer wird für 10 Sekunden angezeigt oder bis der Benutzer auf OK oder Abbrechen klickt. Hierdurch soll sichergestellt werden, dass die PIN-Nummer nicht von anderen Personen eingesehen werden kann. Diese Funktion steht nicht für PDAs zur Verfügung.

- **RADIUS-Server:** Eine Authentifizierungsmethode, die das RADIUS-Authentifizierungsprotokoll (Remote Authentication Dial In User Service) und nicht die herstellerspezifische Agentsoftware verwendet. SafeWord und SecurID können als RADIUS-Server installiert und konfiguriert werden. RADIUS-Authentifizierung ist die einzige Zweifaktorauthentifizierung, die auf Webinterface für Java-Anwendungsservern zur Verfügung steht.

Aktivieren von SafeWord-Authentifizierung in Internetinformationsdienste

In diesem Abschnitt wird die Aktivierung der RSA SecurID 6.0-Unterstützung beschrieben.

Anforderungen für SafeWord

So verwenden Sie SafeWord-Authentifizierung mit dem Webinterface für Microsoft Internetinformationsdienste

- Die neueste Version von SafeWord Agent erhalten Sie von Aladdin Knowledge Systems. Wenn Sie UPN-Authentifizierung unterstützen müssen, stellen Sie sicher, dass alle aktuellen automatischen Updates für den SafeWord Agent auf dem Webinterface- und dem SafeWord-Server angewendet wurden.
- Stellen Sie sicher, dass das Webinterface vor dem SafeWord Agent installiert wird.
- Stellen Sie sicher, dass der SafeWord Agent für das Webinterface auf dem Webinterface-Server installiert ist.

Weitere Informationen zur Konfiguration von SafeWord-Produkten finden Sie unter http://www.aladdin.com/safeword/default.aspx.

Aktivieren der RSA SecurID-Authentifizierung mit der Konsole

Sie müssen im Webinterface die RSA SecurID-Authentifizierung aktivieren, sodass Benutzer auf ihre Ressourcengruppe zugreifen und diese anzeigen können. Verwenden Sie hierzu die Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console.

Aktivieren der Authentifizierung mit RSA SecurID in Microsoft Internetinformationsdienste

Aktualisiert: 2014-11-24

In diesem Abschnitt wird die Aktivierung der RSA SecurID 7.0-Unterstützung beschrieben.

SecurID-Anforderungen

So verwenden Sie SecurID-Authentifizierung mit dem Webinterface für Microsoft Internetinformationsdienste

- Der RSA ACE/Agent für Windows 7.0 oder höher muss auf dem Webserver installiert sein.
- Das Webinterface muss nach der Installation von RSA ACE/Agent installiert werden.
- Das Webinterface muss in Microsoft Internetinformationsdienste 6.0 gehostet werden.

Hinzufügen des Webinterface-Servers als Agent Host

Sie müssen in der RSA ACE/Server-Datenbank einen Agent Host für den Webserver erstellen, damit der RSA ACE/Server dessen Authentifizierungsanfragen erkennt und akzeptiert. Beim Erstellen des Agent-Hosts müssen Sie das Webinterface als NetOS Agent konfigurieren. Diese Einstellung wird vom RSA ACE/Server verwendet, um zu bestimmen, wie die Kommunikation mit dem Webinterface stattfindet.

Kopieren der Datei sdconf.rec

Suchen Sie die Datei sdconf.rec auf dem RSA ACE/Server und kopieren Sie sie in den Ordner \System32 auf dem Webinterface-Server, der sich üblicherweise unter C:\Windows\System32 befindet. Ist die Datei nicht vorhanden, müssen Sie sie erstellen. Diese Datei enthält die Informationen, die das Webinterface zum Herstellen einer Verbindung zum RSA ACE/Server benötigt.

Aktivieren der RSA SecurID-Authentifizierung mit der Konsole

Sie müssen im Webinterface die RSA SecurID-Authentifizierung aktivieren, sodass Benutzer auf ihre Ressourcengruppe zugreifen und diese anzeigen können. Verwenden Sie hierzu die Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console.

Unterstützung mehrerer Domänen mit RSA SecurID

Wenn Sie Benutzerkonten mit identischen Namen in verschiedenen Windows-Domänen haben, müssen Sie diese in der RSA ACE/Server-Datenbank mit einer Standardanmeldung nach folgendem Muster identifizieren: *DOMÄNE\Benutzername* (nur Benutzername ist nicht ausreichend). Außerdem müssen Sie das Webinterface so konfigurieren, dass Domäne und Benutzername an den RSA ACE/Server gesendet werden. Verwenden Sie hierzu die Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console.

Aktivieren der Windows-Kennwort-Integration von RSA SecurID

Das Webinterface unterstützt die Funktion für Windows-Kennwort-Integration von RSA SecurID. Wenn diese Funktion aktiviert ist, können sich Webinterface-Benutzer mit ihrem SecurID-PASSCODE anmelden und auf Ressourcen zugreifen. Benutzer müssen nur bei der ersten Anmeldung am Webinterface ein Windows-Kennwort eingeben oder wenn ihr Kennwort geändert werden muss.

So verwenden Sie SecurID-Windows-Kennwort-Integration mit dem Webinterface für Microsoft Internetinformationsdienste

- Der RSA ACE/Agent Local Authentication Client für Windows muss auf dem Webserver installiert sein (Administratoren müssen sich am Webinterface mit lokalen Administratorrechten anmelden).
- Das Webinterface muss nach der Installation von RSA ACE/Agent installiert werden.
- Der RSA Authentication Agent Offline Local-Dienst muss auf dem Webserver ausgeführt werden.
- Der Agent Host für den Webserver in der RSA ACE/Server-Datenbank muss für die Aktivierung der Windows-Kennwortintegration konfiguriert sein.
- Die Datenbanksystemparameter müssen so konfiguriert sein, dass die Windows-Kennwortintegration auf Systemebene möglich ist.

So setzen Sie das Node Secret auf dem Webserver zurück

Das Node Secret wird verwendet, um sichere Kommunikation zwischen dem Webinterface und dem RSA ACE/Server zu gewährleisten.

Das Node Secret zwischen den beiden Servern kann in den folgenden Situationen abweichen:

- Wenn das Webinterface neu installiert wird.
- Wenn der RSA ACE/Server neu installiert wird.
- Wenn der Agent Host-Eintrag für den Webserver gelöscht und erneut hinzugefügt wurde.
- Wenn der NodeSecret-Registrierungsschlüssel auf dem Webserver gelöscht worden ist.
- Wenn das Kontrollkästchen Node Secret Created im Dialogfeld Edit Agent Host auf dem RSA ACE/Server deaktiviert ist.

Wenn das Node Secret auf dem Webinterface-Server und dem RSA ACE/Server nicht übereinstimmt, schlägt SecurID fehl. Sie müssen das Node Secret auf dem Webinterface-Server und dem RSA ACE/Server zurücksetzen.

Vorsicht: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

1. Wechseln Sie in der Systemregistrierung zu folgendem Eintrag:
    - HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT auf 32-Bit-Servern
    - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SDTI\ACECLIENT auf 64-Bit-Servern
2. Löschen Sie den Node Secret-Schlüssel.

Hinweis: Wenn Sie das Webinterface neu installieren, wird der NodeSecret-Schlüssel nicht gelöscht. Wenn der Agent Host-Eintrag auf dem RSA ACE/Server nicht geändert wird, kann das Node Secret erneut verwendet werden.

Aktivieren der RADIUS-Authentifizierung

Aktualisiert: 2014-11-24

In diesem Abschnitt wird erläutert, wie Sie Aladdin SafeWord installieren und konfigurieren und RSA SecurID als RADIUS-Server einrichten. RADIUS-Authentifizierung ist die einzige Zweifaktorauthentifizierung, die auf Webinterface für Java-Anwendungsservern zur Verfügung steht.

Aktivieren von RADIUS mit SafeWord

Wählen Sie bei der Installation von SafeWord-Serversoftware den IAS RADIUS Agent.

Führen Sie die Anweisungen auf dem Bildschirm für die Installation der RADIUS-Clients mit dem Microsoft Management Console-Snap-In Internetauthentifizierungsdienst aus. Für jeden Webinterface-Server, der Benutzer über den SafeWord-Server authentifiziert, muss ein neuer RADIUS-Client konfiguriert werden.

Jeder RADIUS-Server muss über folgende Informationen verfügen:

- Den vollqualifizierten Domänennamen oder die IP-Adresse des Webinterface-Servers, mit dem der RADIUS-Client verknüpft ist.
- Einen geheimen Schlüssel, der dem verknüpften Webinterface-Server bekannt ist.
- Der Clienttyp muss auf RADIUS standard gesetzt sein.
- Die Option Request must contain the Message Authenticator attribute muss aktiviert sein, um zusätzliche Sicherheit zu bieten.

Aktivieren von RADIUS mit RSA SecurID

RADIUS wird im RSA Authentication Manager mit dem SecurID Configuration Management Tool aktiviert. Weitere Informationen zu diesem Tool finden Sie in der RSA Authentication Manager-Dokumentation.

Hinzufügen der Webinterface- und RADIUS-Server als Authentication Agents

Wenn Sie den RSA Authentication Manager, der Benutzer authentifiziert, auch als RADIUS-Server verwenden möchten, müssen Sie in der RSA Authentication Manager-Datenbank einen Authentication Agent-Datensatz für den lokalen RADIUS-Server erstellen. Geben Sie bei der Erstellung des Authentication Agent-Datensatzes als Namen und IP-Adresse die Daten des lokalen Servers an und konfigurieren Sie diesen Server als einen NetOS Authentication Agent. Der lokale Server muss als der aktive Server eingerichtet werden.

Außerdem müssen Sie in der RSA Authentication Manager-Datenbank einen Authentication Agent-Datensatz für jeden Webinterface-Server erstellen, damit der RSA Authentication Manager Authentifizierungsanfragen vom Webinterface-Server über den RADIUS-Server erkennt und annimmt. Beim Erstellen des Authentication Agent-Datensatzes müssen Sie das Webinterface als Kommunikationsserver konfigurieren und als Verschlüsselungsschlüssel den Wert des gemeinsam mit dem Webinterface verwendeten Geheimschlüssels angeben.

Verwenden des RADIUS-Challengemodus

Der SecurID-RADIUS-Server ist standardmäßig im *RADIUS-Challengemodus*. In diesem Modus gilt für Meldungen Folgendes:

- Das Webinterface zeigt eine generische Challengeseite an, zusammen mit einer Meldung, einem Feld für ein HTML-Kennwort sowie den Schaltflächen OK und Abbrechen.
- Challengemeldungen werden vom Webinterface nicht lokalisiert; sie werden in der Sprache angezeigt, die auf dem SecurID-RADIUS-Server für Challengemeldungen eingestellt ist.

Übermitteln Benutzer keine Antwort (z. B. wenn sie auf Abbrechen klicken), werden sie zur Seite Anmeldung zurückgeleitet.

Citrix empfiehlt, diesen Modus nur zu verwenden, wenn andere Softwarekomponenten oder -produkte als das Webinterface auch den RADIUS-Server zur Authentifizierung verwenden.

Verwenden von benutzerdefinierten Challengemeldungen

Sie können für den SecurID-RADIUS-Server benutzerdefinierte Challengemeldungen erstellen. Wenn Sie benutzerdefinierte Meldungen verwenden, die vom Webinterface erkannt werden, kann der RADIUS-Server dem Benutzer identische Seiten wie im Webinterface für Microsoft Internetinformationsdienste anzeigen. Diese Seiten sind lokalisiert.

Diese Funktion erfordert Änderungen an der RADIUS-Serverkonfiguration. Implementieren Sie sie nur dann, wenn der RADIUS-Server ausschließlich zur Authentifizierung von Webinterface-Benutzern dient.

Zum Ändern von Challengemeldungen starten Sie das RSA RADIUS-Konfigurationsprogramm. Weitere Informationen über die Verwendung dieses Tools finden Sie in der Dokumentation der SecurID-Software. Wenn Sie Benutzern beim Zugriff auf Sites auf IIS- und Java-Anwendungsservern dieselben Meldungen anzeigen möchten, müssen die folgenden Challenges aktualisiert werden:

Meldung	Paket	Aktualisierter Wert
Does User Want a System PIN	Challenge	CHANGE_PIN_EITHER
Is User Ready to Get System PIN	Challenge	SYSTEM_PIN_READY
Is User Satisfied with System PIN	Challenge	CHANGE_PIN_SYSTEM_[%s]
New Numeric PIN of Fixed Length	Challenge	CHANGE_PIN_USER
New Alphanumeric PIN of Fixed Length	Challenge	CHANGE_PIN_USER
New Numeric PIN of Variable Length	Challenge	CHANGE_PIN_USER

New Alphanumeric PIN of Variable Length	Challenge	CHANGE_PIN_USER
New PIN Accepted	Challenge	ERFOLG
Enter Yes or No	Challenge	FEHLER
Next Token Code Required	Challenge	NEXT_TOKENCODE

Erstellen eines gemeinsamen geheimen Schlüssels für RADIUS

Für das RADIUS-Protokoll ist ein gemeinsamer geheimer Schlüssel erforderlich. Dieser Schlüssel ist nur für den RADIUS-Client (d. h. das Webinterface) und den RADIUS-Server, bei dem der Client authentifiziert wird, verfügbar. Das Webinterface speichert diesen gemeinsamen geheimen Schlüssel in einer Textdatei im lokalen Dateisystem. Der Speicherort dieser Datei wird durch den Konfigurationswert RADIUS_SECRET_PATH in der Datei web.config (für in IIS gehostete Sites) oder der Datei web.xml (für auf Java-Anwendungsservern gehostete Sites) angegeben. Der Speicherort ist für in IIS gehostete Sites relativ zum Ordner \conf und für auf Java-Anwendungsservern gehostete Sites relativ zum Verzeichnis /WEB_INF.

Um den gemeinsamen geheimen Schlüssel zu erstellen, erstellen Sie die Textdatei radius_secret.txt, die eine beliebige Zeichenfolge enthält. Verschieben Sie die Textdatei in den in der entsprechenden Konfigurationsdatei angegebenen Speicherort und stellen Sie sicher, dass sie gesichert ist und nur Benutzer oder Prozesse mit entsprechenden Berechtigungen darauf zugreifen können.

Angeben einer Netzwerkzugriffsserver-ID für RADIUS

Das RADIUS-Protokoll erfordert, dass Zugriffsanfragen an RADIUS-Server die IP-Adresse oder eine andere Kennung für den RADIUS-Client (das Webinterface) enthalten. Um RADIUS-Authentifizierung zu aktivieren, müssen Sie entweder die IP-Adresse des Webservers angeben oder einen Wert für das Attribut der RADIUS-Netzwerkzugriffsserver-ID (Network Access Server, NAS) festlegen. Der Wert für das NAS-ID-Attribut kann eine beliebige Zeichenfolge mit mindestens drei Zeichen sein. Obwohl dieses Attribut nicht für jeden RADIUS-Client eindeutig sein muss, kann dies bei der Diagnose von RADIUS-Kommunikationsproblemen helfen.

Um die IP-Adresse des RADIUS-Clients anzugeben, geben Sie in der Datei web.config (für in IIS gehostete Sites) bzw. der Datei web.xml (für auf Java-Anwendungsservern gehostete Sites) die IP-Adresse des Webservers als Wert für den Konfigurationsparameter RADIUS_IP_ADDRESS ein. Um die RADIUS-NAS-ID festzulegen, geben Sie in web.config oder web.xml einen Wert für RADIUS_NAS_IDENTIFIER an.

Aktivieren der RADIUS-Zweifaktorauthentifizierung mit der Konsole

Sie müssen im Webinterface die Zweifaktorauthentifizierung aktivieren, sodass Benutzer auf ihre Ressourcengruppe zugreifen und diese anzeigen können. Verwenden Sie hierzu die Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console. Zusätzlich zum Aktivieren der Zweifaktorauthentifizierung können Sie eine oder mehrere RADIUS-Serveradressen (optional auch Ports), Load Balancing und Failover-Verhalten der Server sowie ein Zeitlimit für die Antwort angeben.

Wichtig: Wenn Sie RADIUS-Authentifizierung aktivieren, müssen Sie auch die IP-Adresse des RADIUS-Clients angeben oder in der Datei web.config (IIS) bzw. der Datei web.xml (Java-Anwendungsserver) einen Wert für das Attribut für die RADIUS-Netzwerkzugriffsserver-ID festlegen.

Verwalten von Clients

Aktualisiert: 2014-11-24

Dieser Abschnitt enthält Informationen zur Bereitstellung und Verwendung der Citrix Clients mit dem Webinterface. Es wird auch erläutert, wie Sie sicheren Zugriff einrichten.

Clients für Onlineressourcen

Folgende Citrix Clients können für den Zugriff auf Onlineressourcen verwendet werden:

- **Nativer Client:** Administratoren installieren den entsprechenden nativen Client auf den Geräten der Benutzer. Benutzer ohne einen nativen Client können mit dem Clienterkennungs- und -bereitstellungsprozess das Citrix Online Plug-In herunterladen und bereitstellen. Seamless-Fenster werden unterstützt. Ressourcen werden in Desktop-Fenstern angezeigt, deren Größe geändert werden kann. Wenn Benutzer über einen PDA auf Ressourcen zugreifen, müssen Sie den nativen Client aktivieren.

- **Client für Java:** Benutzer führen den Client für Java beim Zugriff auf die Ressource aus. Dieser Client wird normalerweise in Situationen verwendet, in denen Benutzer keinen nativen Client installiert haben und das Citrix Online Plug-In nicht herunterladen und bereitstellen können, weil die Konfiguration ihres Geräts oder der XenApp Web-Site dies verhindern. Der Client für Java unterstützt Seamless-Fenster. Ressourcen werden in Desktop-Fenstern gestartet, deren Größe geändert werden kann.

- **Eingebettete Software für Remotedesktopverbindungen (RDP):** Benutzer können die Software für Remotedesktopverbindungen (RDP) verwenden, die bereits als Teil des Windows-Betriebssystems installiert ist, wenn Sie diese Option aktiviert haben. Der Clienterkennungs- und -bereitstellungsprozess stellt die Software für Remotedesktopverbindungen nicht für Benutzer zur Verfügung, die diese Software nicht installiert haben. Seamless-Fenster werden nicht unterstützt. Ressourcen werden in Browserfenster eingebettet angezeigt.

  Hinweis: Der Client für Java und die eingebettete RDP-Software werden auf Geräten, auf denen Windows CE oder Windows Mobile ausgeführt wird, nicht unterstützt. Der Client für Java und die eingebettete Remotedesktopverbindungssoftware (RDP) können nicht mit Sites verwendet werden, die mit ADFS integriert sind.

Konfigurieren des Citrix Online Plug-Ins

Mit dem Citrix Online Plug-In können Benutzer mit einem Webbrowser direkt von ihrem Desktop auf Anwendungen, Inhalte und virtuelle Desktops zugreifen. Sie können remote konfigurieren, dass Links zu Ressourcen im Startmenü, auf dem Windows-Desktop oder im Windows-Infobereich erstellt werden. Die Benutzeroberfläche des Citrix Online Plug-Ins kann auch "gesichert" werden, um eine falsche Konfiguration durch die Benutzer zu verhindern. Sie können das Citrix Online Plug-In mit der Citrix Webinterface Management Console oder der Datei config.xml file konfigurieren.

Verwenden der Citrix Webinterface Management Console für die Konfiguration

Das Citrix Online Plug-In ist mit standardmäßigen Präsentationseinstellungen, Authentifizierungsmethoden und Serververbindungsoptionen konfiguriert. Mit der Citrix Webinterface Management Console können die Standardeinstellungen so konfiguriert werden, dass Benutzer bestimmte Optionen nicht ändern können.

Verwenden der Konfigurationsdateien

Sie können das Citrix Online Plug-In auch mit den Dateien config.xml und WebInterface.conf konfigurieren. Normalerweise sind diese Dateien im Verzeichnis C:\inetpub\wwwroot\Citrix\PNAgent\conf auf dem Webinterface-Server gespeichert.

Verwalten von Plug-In-Konfigurationsdateien

Die Citrix Online Plug-In-Optionen, die mit der Konsole konfiguriert werden, werden in einer Konfigurationsdatei auf dem Webinterface-Server gespeichert. Die Konfigurationsdatei steuert den Umfang der Parameter, die den Benutzern als Optionen im Dialogfeld Optionen des Citrix Online Plug-Ins angezeigt werden. Mit den verfügbaren Optionen können Benutzer ihre Einstellungen für ICA-Sitzungen festlegen, u. a. Anmeldemodus, Bildschirmgröße, Audioqualität und die Speicherorte von Links für Ressourcen.

Bei neuen Sites enthält die installierte Standardkonfigurationsdatei config.xml Standardeinstellungen und kann in den meisten Netzwerkumgebungen ohne Änderungen direkt verwendet werden. Die Datei config.xml ist im Ordner \conf für die Site gespeichert.

Kopieren der Installationsdateien für Clients zum Webinterface

Aktualisiert: 2014-11-24

Um die webbasierte Clientinstallation verwenden zu können, müssen die Clientinstallationsdateien auf dem Webinterface-Server vorhanden sein.

Während der Webinterface-Installation werden Sie vom Setupprogramm zum Zugriff auf das XenApp- oder XenDesktop-installationsmedium aufgefordert. In IIS wird beim Setup der Inhalt des Ordners \Citrix Receiver and Plug-Ins auf dem Installationsmedium in den Ordner \Clients im Stammverzeichnis kopiert, z. B. C:\Programme (x86)\Citrix\Web Interface*Version*\Clients. Auf Java-Anwendungsservern kopiert Setup die Citrix Clients vom Installationsmedium und verpackt sie in einer WAR-Datei.

Wenn Sie die Installationsdateien während der Webinterface-Installation nicht auf den Webserver kopiert haben, müssen Sie diese Dateien auf den Webserver kopieren, bevor Sie die webbasierte Clientinstallation verwenden; kopieren Sie die Dateien beispielsweise vom Ordner "Citrix Receiver and Plug-ins". Wenn das XenApp- oder XenDesktop-Installationsmedium nicht verfügbar ist, müssen Sie die erforderliche Verzeichnisstruktur manuell erstellen und dann die gewünschten Clients von der Citrix Website herunterladen.

Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Clientinstallationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Clients von der Citrix Website herunterladen oder Sie ältere Clients bereitstellen möchten, überprüfen Sie, ob die richtigen Dateinamen der Clientinstallationdateien in den Konfigurationsdateien Ihrer XenApp Web-Sites angegeben sind.

So kopieren Sie die Clientdateien in Microsoft Internetinformationsdienste zum Webinterface

1. Navigieren Sie auf den Ordner \Clients in der Webinterface-Installation, z. B. C:\Programme (x86)\Citrix\Web Interface*Version*\Clients.

2. Legen Sie das Installationsmedium in das Laufwerk des Webservers ein oder navigieren Sie im Netzwerk zu dem freigegebenen Image des Installationsmediums.

3. Gehen Sie zum Ordner \Citrix Receiver and Plug-ins auf dem Installationsmedium. Kopieren Sie den Inhalt des Ordners auf dem Installationsmedium in den Ordner \Clients auf dem Webinterface-Server. Stellen Sie dabei sicher, dass Sie nur den *Inhalt* des Ordners und nicht den Ordner \Citrix Receiver and Plug-ins selbst kopieren.

   Wenn das XenApp- oder XenDesktop-Installationsmedium nicht verfügbar ist, müssen Sie die folgende Verzeichnisstruktur manuell erstellen und dann die gewünschten Clients von der Citrix Website herunterladen.

   C:\Programme (x86)\Citrix\Web Interface*Version*\Clients

   - \de
     - \Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Deutsch in diesem Ordner.
   - \en
     - \Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Englisch in diesem Ordner.
   - \es
     - \Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Spanisch in diesem Ordner.
   - \fr
     - \Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Französisch in diesem Ordner.
   - \ja
     - \Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Japanisch in diesem Ordner.
   - \Java

     Speichern Sie die Dateien für den Client für Java in diesem Ordner.

- \Linux

  Speichern Sie die Installationsdatei für den Citrix Receiver für Linux (linuxx86-*Version*.tar.gz) in diesem Ordner.

- \Mac

  - \Web Online Plug-In

    Speichern Sie die Installationsdatei für das Citrix Online Web Plug-In für Macintosh {Citrix online plug-in (web).dmg} in diesem Ordner.

- \Windows

  - \Offline Plug-in

    Speichern Sie die Installationsdatei für das Citrix Offline Plug-In (CitrixOfflinePlugin.exe) in diesem Ordner.

  - \Online Plug-in

    Speichern Sie die Installationsdatei für das Citrix Online Plug-In – Web (CitrixOnlinePluginWeb.exe) in diesem Ordner.

Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Clientinstallationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Clients von der Citrix Website herunterladen oder Sie ältere Clients bereitstellen möchten, überprüfen Sie, ob in den Konfigurationsdateien für Ihre XenApp Web-Sites die richtigen Namen der Clientinstallationsdateien für die Parameter ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 und ClientStreamingWin32 angegeben sind.

Nachdem Sie die Clientinstallationsdateien in die oben aufgeführte Verzeichnisstruktur kopiert haben, bieten alle XenApp Web-Sites, die für webbasierte Clientinstallation konfiguriert sind, Benutzern, die einen Client benötigen, einen an.

So kopieren Sie die Clientdateien zum Webinterface auf Java-Anwendungsservern

1. Suchen Sie in der entpackten WAR-Datei der Site das Verzeichnis \Clients.

2. Legen Sie das Installationsmedium in das Laufwerk des Webservers ein oder navigieren Sie im Netzwerk zu dem freigegebenen Image des Installationsmediums.

3. Wechseln Sie zum Verzeichnis \Citrix Receiver and Plug-ins auf dem Installationsmedium. Kopieren Sie den Inhalt des Verzeichnisses auf dem Installationsmedium in das Verzeichnis \Clients auf dem Webinterface-Server. Stellen Sie dabei sicher, dass Sie nur den *Inhalt* des Verzeichnisses und nicht das Verzeichnis \Citrix Receiver and Plug-ins selbst kopieren.

   Wenn das XenApp- oder XenDesktop-Installationsmedium nicht verfügbar ist, müssen Sie die folgende Verzeichnisstruktur manuell erstellen und dann die gewünschten Clients von der Citrix Website herunterladen.

   XenAppWebSiteRoot/Clients

   - /de
     - /Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Deutsch in diesem Verzeichnis.
   - /en
     - /Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Englisch in diesem Verzeichnis.
   - /es
     - /Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Spanisch in diesem Verzeichnis.
   - /fr
     - /Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Französisch in diesem Verzeichnis.
   - /ja
     - /Unix

       Speichern Sie die Installationsdateien für die Clients für UNIX (solaris.tar.Z, sol86.tar.Z) mit Unterstützung für Japanisch in diesem Verzeichnis.
   - /Java

     Speichern Sie die Dateien für den Client für Java in diesem Verzeichnis.

- /Linux

  Speichern Sie die Installationsdatei für den Citrix Receiver für Linux (linuxx86-*Version*.tar.gz) in diesem Verzeichnis.

- /Mac

  - /Web Online Plug-in

    Speichern Sie die Installationsdatei für das Citrix Online Web Plug-In für Macintosh {Citrix online plug-in (web).dmg} in diesem Verzeichnis.

- /Windows

  - /Offline Plug-in

    Speichern Sie die Installationsdatei für das Citrix Offline Plug-In (CitrixOfflinePlugin.exe) in diesem Verzeichnis.

  - /Online Plug-in

    Speichern Sie die Installationsdatei für das Citrix Online Plug-In – Web (CitrixOnlinePluginWeb.exe) in diesem Verzeichnis.

Das Webinterface nimmt standardmäßig an, dass die Dateinamen der Clientinstallationsdateien mit den Namen der Dateien auf den XenApp- oder XenDesktop-Installationsmedien identisch sind. Wenn Sie Clients von der Citrix Website herunterladen oder Sie ältere Clients bereitstellen möchten, überprüfen Sie, ob in den Konfigurationsdateien für Ihre XenApp Web-Sites die richtigen Namen der Clientinstallationsdateien für die Parameter ClientIcaLinuxX86, ClientIcaMac, ClientIcaSolarisSparc, ClientIcaSolarisX86, ClientIcaWin32 und ClientStreamingWin32 angegeben sind.

4. Nachdem Sie die Clientinstallationsdateien in die oben aufgeführte Verzeichnisstruktur kopiert haben, starten Sie den Webserver neu.

   Wenn Sie die XenApp Web-Site für webbasierte Clientinstallation konfiguriert haben, wird Benutzern, die einen Client benötigen, einer angeboten.

Konfigurieren von Clientbereitstellung und Installationsmeldungen

Aktualisiert: 2014-11-24

Das Webinterface enthält einen Clienterkennungs- und -bereitstellungsprozess, der ermittelt, welche Citrix Clients in der Benutzerumgebung bereitgestellt werden können, und der die Benutzer bei der Bereitstellung und, falls erforderlich, bei der Neukonfigurierung ihrer Webbrowser unterstützt.

Sie können Benutzern drei Möglichkeiten für den Zugriff auf den Clienterkennungs- und -bereitstellungsprozess geben:

- Sie können den Clienterkennungs- und -bereitstellungsprozess so konfigurieren, dass er automatisch ausgeführt wird, wenn Benutzer auf eine XenApp Web-Site zugreifen. Der Clienterkennungs- und -bereitstellungsprozess wird automatisch gestartet. Er hilft Benutzern, den richtigen Citrix Client für den Zugriff auf ihre Ressourcen auszuwählen. In einigen Umgebungen kann der webbasierte Clienterkennungs- und -bereitstellungsprozess auch erkennen, ob ein Client installiert ist. Dem Benutzer wird in diesem Fall nur dann eine Installationsaufforderung angezeigt, wenn dies erforderlich ist.

- Sie können es Benutzern ermöglichen, einen bevorzugten Client für den Zugriff auf Onlineressourcen auszuwählen. Hierdurch wird die Schaltfläche Clienterkennung ausführen auf der Seite Einstellungen angezeigt, mit der Benutzer den Clienterkennungs- und -bereitstellungsprozess manuell starten können.

- Sie können Installationsmeldungen anzeigen, die Benutzer als Links auf der Seite Meldungen sehen. Durch Klicken auf solch einen Link können sie den Clienterkennungs- und -bereitstellungsprozess starten.

Wenn ein Benutzer auf eine XenApp Web-Site zugreift, versucht der webbasierte Clienterkennungs- und -bereitstellungsprozess zu ermitteln, ob der bevorzugte Citrix Client auf dem Computer des Benutzers installiert ist. Bevor sich der an einer XenApp Web-Site anmeldet, für die automatische Clienterkennung und -bereitstellung konfiguriert ist, startet der Prozess automatisch und hilft dem Benutzer, einen geeigneten Citrix Client, mit dem er auf Ressourcen zugreifen kann, zu finden und bereitzustellen. Der Benutzer wird außerdem, soweit erforderlich, bei der Neukonfigurierung seines Browsers unterstützt.

Benutzer können auch mit Links auf der Seite Meldungen auf den Clienterkennungs- und -bereitstellungsprozess zugreifen. Durch Klicken auf solch einen Link können sie den Clienterkennungs- und -bereitstellungsprozess starten. Diese Links werden *Installationsmeldungen* genannt.

Mit Installationsmeldungen können Sie Benutzern helfen, die über keinen geeigneten Client verfügen, und Benutzer können damit auch auf den Clienterkennungs- und -bereitstellungsprozess zugreifen, um ihre Citrix Clients auf eine neuere Version zu aktualisieren oder um einen anderen Clienttyp zu installieren, der einen erweiterten Funktionsumfang bietet.

Mit der Aufgabe Clientbereitstellung in der Citrix Webinterface Management Console können Sie festlegen, wann und wie Benutzer auf den Clienterkennungs- und -bereitstellungsprozess zugreifen können.

So konfigurieren Sie Meldungen für die Clientbereitstellung und -installation

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Clientbereitstellung. Für Sites, die nur Onlineanwendungen anbieten, aktivieren Sie das Kontrollkästchen Nativer Client und klicken Sie auf Eigenschaften.

4. Klicken Sie auf Clienterkennung.

5. Wenn der Clienterkennungs- und -bereitstellungsprozess automatisch gestartet werden soll, wenn Benutzer ohne geeigneten Citrix Client auf eine XenApp Web-Site zugreifen, aktivieren Sie das Kontrollkästchen Clienterkennung bei Anmeldung durchführen.

6. Wenn Benutzer aufgefordert werden sollen, ihre Clients zu aktualisieren, wenn der Clienterkennungs- und -bereitstellungsprozess neuere Versionen auf der XenApp Web-Site ermittelt hat, aktivieren Sie das Kontrollkästchen Upgrades für Clients anbieten.

7. Legen Sie fest, wann Benutzern Installationsmeldungen angezeigt werden, indem Sie eine der folgenden Optionen auswählen:

   - Wenn Benutzer informiert werden sollen, wenn kein geeigneter Client gefunden wurde oder wenn ein besserer Client verfügbar ist, wählen Sie Immer wenn ein Client erforderlich ist. Dies ist die Standardeinstellung.

   - Wenn Benutzer nur informiert werden sollen, wenn kein geeigneter Client gefunden wurde, wählen Sie Nur wenn Zugriff auf Ressourcen nicht möglich ist.

   - Wenn Installationsmeldungen in keinem Fall angezeigt werden sollen, wählen Sie Nie.

Konfigurieren der Funktion zum Signieren von ICA-Dateien

Aktualisiert: 2014-12-02

Das Webinterface kann ICA-Dateien mit einem von Ihnen gewählten Zertifikat digital signieren, damit kompatible Citrix Clients und Plug-Ins prüfen können, ob die Datei von Ihrer Organisation stammt.

Um ICA-Dateien signieren zu können, sind die folgenden Komponenten erforderlich:

- Webinterface Version 5.4 oder höher
- Merchandising Server Version 1.2 oder höher (für die Bereitstellung von Sicherheitsrichtlinien für nicht verwaltete Clients)
- Gruppenrichtlinienobjekte für die Bereitstellung von Sicherheitsrichtlinien für verwaltete Clients
- Dateiformat für administrative Vorlagen für Windows Server 2003 oder höher

Citrix empfiehlt folgende Reihenfolge von Schritten:

- Sie kaufen ein Codesignaturzertifikat oder ein SSL-Signatur-Zertifikat von einer öffentlichen Zertifizierungsstelle (z. B. VeriSign).
- Wenn das Unternehmen bereits eine private Zertifizierungsstelle hat, erstellen Sie damit ein Codesignaturzertifikat oder ein SSL-Signatur-Zertifikat.
- Verwenden Sie ein vorhandenes SSL-Zertifikat, z. B. das Webinterface- oder Dazzle-Serverzertifikat.
- Erstellen Sie eine neue Stammzertifizierungsstelle und verteilen Sie es mit Gruppenrichtlinienobjekten an die Clients.

Das Zertifikat muss die folgenden Anforderungen erfüllen:

- Das Zertifikat muss den privaten Schlüssel enthalten.
- Das Zertifikat muss noch gültig sein.
- Eine der folgenden Aussagen muss zutreffend sein:
  - Das Zertifikat enthält nicht die Felder "Key Usage" oder "Enhanced Key Usage".
  - Mit dem Feld "Key Usage" kann der Schlüssel für digitale Signaturen verwendet werden.
  - Das Feld "Enhanced Key Usage" ist auf "Code Signing" oder "Server Authentication" gesetzt.

Das Webinterface signiert ICA-Dateien entweder mit dem SHA-1- oder SHA-256-Hash-Algorithmus. Der SHA-256-Hash-Algorithmus ist neuer und sicherer, wird jedoch nur auf Servern unterstützt, auf denen Windows 2008 oder höher ausgeführt wird, und auf Clients, auf denen Windows Vista oder höher ausgeführt wird. Der SHA-1-Hash-Algorithmus kann auf allen unterstützten Server- und Client-Betriebssystemen verwendet werden.

Signieren von ICA-Dateien kann nicht mit dem Client für Java, dem RDP-Client, dem Citrix Streaming Client und für von Netzwerkfreigaben heruntergeladene Dokumente verwendet werden.

Um Signieren von ICA-Dateien zu aktivieren, muss Folgendes konfiguriert werden: die Site verwendet den nativen Client und Onlineanwendungen werden angezeigt. Außerdem muss in der Datei Webinterface.conf "EnableLegacyIcaClientSupport" auf "Off" gesetzt sein.

Weitere Informationen zum Aktivieren von Signieren von ICA-Dateien für das Citrix Online Plug-In finden Sie in der Dokumentation für Citrix Merchandising Server.

So aktivieren Sie das Signieren von ICA-Dateien in der Webinterface Management Console.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Clientbereitstellung.

4. Klicken Sie auf Signieren von ICA-Dateien.

5. Aktivieren Sie die Option Signieren von ICA-Dateien aktivieren und wählen Sie ein Zertifikat aus der Dropdownliste aus. Falls das erforderliche Zertifikat nicht in der Liste vorhanden ist, klicken Sie auf Importieren, um ein Zertifikat in den persönlichen Zertifikatspeicher zu importieren.

6. Wenn Sie Windows 2008 oder höher ausführen, können Sie den Typ des verwendeten Hash-Algorithmus auswählen. Andernfalls wird SHA-1 verwendet. Nachdem Sie das Signieren von ICA-Dateien unter Windows 2003 konfiguriert haben, müssen Sie den Computer neu starten.

Konfigurieren der Überwachung von Streamingsitzungen

Mit der Aufgabe Clientbereitstellung in der Citrix Webinterface Management Console können Sie das Webinterface so konfigurieren, dass dem Citrix Administrator Informationen über Benutzersitzungen zur Verfügung gestellt werden. Das Webinterface stellt diese Informationen über eine Sitzungs-URL bereit, die die Kommunikation mit dem Citrix Offline Plug-In ermöglicht. Meist wird diese URL automatisch erkannt. Unter Umständen muss sie jedoch manuell eingerichtet werden, beispielsweise wenn ein clientseitiger Proxy verwendet wird.

Zum Anzeigen von Sitzungsinformationen können Sie die Delivery Services Management Console verwenden. Sie können Informationen über alle Benutzersitzungen in mehreren Farmen, bestimmte Anwendungen, Sitzungen mit einer Verbindung zu einem bestimmten Server oder die Sitzungen und Anwendungen eines bestimmten Benutzers anzeigen.

So konfigurieren Sie die Überwachung von Streamingsitzungen

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Clientbereitstellung.

4. Klicken Sie auf Citrix Offline Plug-In.

5. Legen Sie fest, wie das Webinterface mit dem Citrix Offline Plug-In kommunizieren soll. Wählen Sie eine der folgenden Optionen:

   - Um die für die Kommunikation mit dem Plug-In verwendete Sitzungs-URL automatisch zu erkennen, aktivieren Sie die Option Sitzungs-URL automatisch erkennen.

   - Um die Sitzungs-URL automatisch zu erkennen, aktivieren Sie die Option Sitzungs-URL angeben und geben Sie die genaue URL ein.

Bereitstellen der Software für Remotedesktopverbindungen

Diese Funktion ist auf 32-Bit-Windows-Systemen, auf denen Internet Explorer ausgeführt wird, verfügbar. Benutzer, die Version 6.0 (Teil von Windows XP Service Pack 3) oder höher der Microsoft-Software für Remotedesktopverbindungen (RDP) installiert haben, können damit auf ihre Ressourcen zugreifen. Wenn Benutzer keine anderen Clients verwenden können, überprüft der Clienterkennungs- und -bereitstellungsprozess, ob die Software für Remotedesktopverbindungen (RDP) verfügbar ist, und hilft Benutzern falls erforderlich beim Aktivieren des Terminaldienste-ActiveX-Steuerelements. Die Option, Software für Remotedesktopverbindungen (RDP) zu verwenden, steht nur für Sites zur Verfügung, die nur Onlineanwendungen anbieten.

Hinweis: Wenn sich die XenApp Web-Site in Internet Explorer nicht in der Zone "Lokales Intranet" oder "Vertrauenswürdige Zonen" befindet, wird eine Fehlermeldung angezeigt. Der Clienterkennungs- und -bereitstellungsprozess des Webinterface bietet Benutzern Anweisungen, wie sie die Site der entsprechenden Windows-Sicherheitszone hinzufügen können.

Bereitstellen des Clients für Java

Wenn Sie Citrix Clients über Netzwerke mit geringer Bandbreite bereitstellen oder die von Benutzern verwendete Plattform nicht kennen, sollten Sie den Client für Java in Erwägung ziehen. Der Client für Java ist ein plattformübergreifendes Applet, das der Webinterface-Server jedem Java-kompatiblen Webbrowser bereitstellen kann.

Da der Client für Java die meisten Benutzerumgebungen, Geräte, Betriebssysteme und Webbrowser unterstützt, kann er als Fallback-Option in Situationen verwendet werden, wenn die Verwendung eines nativen Clients nicht möglich ist. Sie können den Clienterkennungs- und -bereitstellungsprozess so konfigurieren, dass Benutzern, die keinen nativen Client haben oder keinen Client von der XenApp Web-Site herunterladen und bereitstellen können, der Client für Java angeboten wird.

Sie müssen sicherstellen, dass der Client für Java im Ordner \Clients der XenApp Web-Site vorhanden ist, um ihn den Benutzern zur Verfügung stellen zu können.

So konfigurieren Sie Fallback auf den Client für Java

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Clientbereitstellung. Für Sites, die nur Onlineanwendungen anbieten, aktivieren Sie das Kontrollkästchen Nativer Client und klicken Sie auf Eigenschaften.

   Hinweis: Sie müssen den Client für Java nicht für Benutzer verfügbar machen, um die Fallback-Funktion anbieten zu können.

4. Klicken Sie auf Fallback-Verhalten.

5. Legen Sie die Bedingungen fest, unter denen Benutzern ohne einen nativen Client der Client für Java angeboten werden soll, indem Sie eine der folgenden Optionen wählen:

   - Wenn Benutzer ohne einen nativen Client einen passenden Citrix Client herunterladen und bereitstellen sollen, wählen Sie Nativen Client bereitstellen. Dies ist die Standardeinstellung.

   - Wenn Benutzern ohne einen nativen Client der Client für Java angeboten werden soll und sie nur zum Download und zur Bereitstellung eines nativen Clients aufgefordert werden sollen, wenn Sie den Client für Java nicht verwenden können, wählen Sie Nativen Client bereitstellen und Benutzern die Wahl zwischen diesem Client und dem Client für Java überlassen.

   - Wenn Benutzer ohne einen nativen Client zusätzlich dazu, dass ihnen der Client für Java angeboten wird, aufgefordert werden sollen, einen passenden Client herunterzuladen und bereitzustellen, wählen Sie Automatisches Fallback auf Client für Java.

Anpassen der Bereitstellung des Clients für Java

Aktualisiert: 2014-11-25

Sie können die Komponenten konfigurieren, die bei der Bereitstellung des Clients für Java enthalten sind.

Die Größe der des Clients für Java hängt von den enthaltenen Paketen ab. Je weniger Pakete Sie wählen, desto kleiner ist der Client (unter Umständen nur 540 KB). Wenn Sie die Größe des Clients für Java für Benutzer, die langsame Verbindungen verwenden, einschränken möchten, können Sie nur das Minimum der Komponenten bereitstellen. Eine andere Möglichkeit ist es, Benutzern zu erlauben, die benötigten Komponenten selbst auszuwählen. Weitere Informationen zum Client für Java und den Komponenten finden Sie in der Client für Java-Dokumentation.

Hinweis: Einige Komponenten des Clients für Java erfordern weitere Konfigurationsschritte auf den Geräten der Benutzer oder auf dem Server.

In der folgenden Tabelle werden die verfügbaren Optionen erläutert:

Paket	Beschreibung
Audio	Hiermit können Ressourcen, die auf dem Server ausgeführt werden, Audio über die Geräte wiedergeben, die auf den Computern der Benutzer installiert sind. Sie können die von der Clientaudiozuordnung auf dem Server verwendete Bandbreite durch Konfigurieren der Citrix Benutzerrichtlinien steuern.
Zwischenablage	Benutzer können Text und Grafiken zwischen Onlineressourcen und lokal auf ihren Geräten ausgeführten Anwendungen kopieren.
Lokales Textecho	Die Anzeige der Texteingabe auf Benutzergeräten wird beschleunigt.
SSL/TLS	Die Kommunikation wird mit SSL (Secure Sockets Layer) und TLS (Transport Layer Security) gesichert. SSL/TLS bietet Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfung der Nachrichtenintegrität.
Verschlüsselung	Hohe Verschlüsselung für erhöhte Sicherheit der Citrix Client-Verbindungen.

Clientlaufwerkzuordnung	Benutzer können in einer Sitzung auf ihre lokalen Laufwerke zugreifen. Wenn Benutzer eine Verbindung zum Server herstellen, werden die Clientlaufwerke (z. B. Disketten-, Netzwerk- und CD-Laufwerke) automatisch zugeordnet. Benutzer greifen auf lokal gespeicherte Dateien zu, bearbeiten sie in den Sitzungen und speichern sie wieder auf einem lokalen Laufwerk oder einem Laufwerk auf dem Server. Zum Aktivieren dieser Einstellung muss im Dialogfeld Einstellungen für Client für Java die Clientlaufwerkszuordnung konfiguriert sein. Weitere Informationen finden Sie in der Client für Java-Dokumentation.
Druckerzuordnung	Benutzer können in einer Sitzung auf ihren lokalen oder auf Netzwerkdruckern drucken.
Konfigurations-Benutzeroberfläche	Diese Funktion aktiviert das Dialogfeld Einstellungen für Client für Java. In diesem Dialogfeld können Benutzer den Client für Java konfigurieren.

Verwenden von privaten Stammzertifikaten mit dem Client für Java, Version 9.x

Wenn Sie Secure Gateway oder den SSL-Relaydienst mit einem Serverzertifikat konfiguriert haben, das Sie von einer privaten Zertifizierungsstelle erworben haben (z. B. wenn Sie eigene Zertifikate mit den Zertifikatsdiensten von Microsoft ausstellen), müssen Sie das Stammzertifikat in den Java-Schlüsselspeicher jedes Benutzergeräts importieren. Weitere Informationen finden Sie in der Client für Java-Dokumentation.

Verwalten des sicheren Zugriffs

Alle neuen Webinterface-Sites sind standardmäßig für direkten Zugriff konfiguriert, wobei die tatsächliche Adresse des Citrix Servers an alle Citrix Clients übergeben wird. Wenn Sie jedoch Access Gateway, Secure Gateway oder eine Firewall in Ihrer Bereitstellung verwenden, können Sie mit der Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console das Webinterface angemessen konfigurieren. Sie können außerdem unterschiedliche Zugriffsmethoden für verschiedene Benutzergruppen konfigurieren. Beispiel: Interne Benutzer, die sich über das Firmen-LAN anmelden, können direkten Zugriff erhalten, während externe Benutzer, die sich über das Internet anmelden, über Access Gateway Zugriff auf das Webinterface erhalten.

In diesem Abschnitt wird erläutert, wie Sie mit der Aufgabe Sicherer Zugriff Zugriffseinstellungen angeben, Adressübersetzungen bearbeiten und Gateway-Einstellungen konfigurieren können.

So konfigurieren Sie direkte Zugriffsrouten

Wenn die tatsächliche Adresse des Citrix Servers an eine bestimmte Gruppe von Citrix Clients übergeben werden soll, können Sie mit der Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console Adressen und Masken für Benutzergeräte angeben.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Sicherer Zugriff.

4. Klicken Sie auf der Seite Zugriffsmethoden angeben auf Hinzufügen, um eine neue Zugriffsroute hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Route zu bearbeiten.

5. Wählen Sie in der Liste Zugriffsmethode die Option Direkt aus.

6. Geben Sie die Netzwerkadresse und die Subnetzmaske des Clientnetzwerkes ein.

7. Ordnen Sie die Zugriffsrouten in der Tabelle Benutzergerätadressen mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach.

So konfigurieren Sie alternative Adresseinstellungen

Wenn die alternative Adresse des Citrix Servers an eine bestimmte Gruppe von Citrix Clients übergeben werden soll, können Sie mit der Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console Adressen und Masken für Benutzergeräte angeben. Der Server muss mit einer alternativen Adresse und die Firewall muss für Netzwerkadressübersetzung konfiguriert sein.

Hinweis: Auf virtuelle XenDesktop-Desktops kann nicht mit alternativen Adressen zugegriffen werden.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Sicherer Zugriff.

4. Klicken Sie auf der Seite Zugriffsmethoden angeben auf Hinzufügen, um eine neue Zugriffsroute hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Route zu bearbeiten.

5. Wählen Sie in der Liste Zugriffsmethode die Option Alternative Adresse aus.

6. Geben Sie die Netzwerkadresse und die Subnetzmaske des Clientnetzwerkes ein.

7. Ordnen Sie die Zugriffsrouten in der Tabelle Benutzergerätadressen mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach.

So konfigurieren Sie die interne Firewalladressübersetzung

Wenn Sie in Ihrer Bereitstellung eine Firewall verwenden, können Sie mit dem Webinterface Zuordnungen von internen Adressen zu externen Adressen und Ports definieren. Wenn der Citrix Server beispielsweise nicht mit einer alternativen Adresse konfiguriert ist, kann das Webinterface zum Bereitstellen einer alternativen Adresse für den Citrix Client konfiguriert werden. Verwenden Sie hierzu die Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Sicherer Zugriff.

4. Klicken Sie auf der Seite Zugriffsmethoden angeben auf Hinzufügen, um eine neue Zugriffsroute hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Route zu bearbeiten.

5. Wählen Sie in der Liste Zugriffsmethode die Option Übersetzt aus.

6. Geben Sie die Netzwerkadresse und die Subnetzmaske des Clientnetzwerkes ein. Ordnen Sie die Zugriffsrouten in der Tabelle Benutzergerätadressen mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach und klicken Sie auf Weiter.

7. Klicken Sie auf der Seite Adressübersetzungen angeben auf Hinzufügen, um eine neue Adressübersetzung hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Adressübersetzung zu bearbeiten.

8. Wählen Sie im Bereich Zugriffstyp eine der folgenden Optionen:

   - Wenn der Citrix Client über die übersetzte Adresse eine Verbindung zum Citrix Server herstellen soll, wählen Sie Benutzergerätroutenübersetzung.

   - Wenn Sie in der Tabelle Benutzergerätadressen bereits eine übersetzte Gateway-Route konfiguriert haben und möchten, dass der Client und der Gateway-Server beide die übersetzte Adresse für die Verbindungsherstellung mit dem Citrix Server verwenden, wählen Sie Benutzergerät- und Gateway-Routenübersetzung.

9. Geben Sie die internen und externen (übersetzten) Ports und Adressen für den Citrix Server ein. Clients, die eine Verbindung zu dem Server herstellen, verwenden die externe Portnummer und Adresse. Stellen Sie sicher, dass die Zuordnungen, die Sie erstellen, zu den Adresstypen passen, die der Citrix Server verwendet.

So konfigurieren Sie Gateway-Einstellungen

Aktualisiert: 2014-11-25

Wenn Sie Access Gateway oder Secure Gateway in Ihrer Bereitstellung verwenden, müssen Sie das Webinterface für die Gateway-Unterstützung konfigurieren. Verwenden Sie hierzu die Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Sicherer Zugriff.

4. Klicken Sie auf der Seite Zugriffsmethoden angeben auf Hinzufügen, um eine neue Zugriffsroute hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Route zu bearbeiten.

5. Wählen Sie in der Liste Zugriffsmethode eine der folgenden Optionen:

   - Wählen Sie Gateway: direkt, wenn die tatsächliche Adresse des Citrix Servers an das Gateway übergeben werden soll.

   - Wählen Sie Gateway: alternative Adresse, wenn die alternative Adresse des XenApp-Servers an das Gateway übergeben werden soll. Der XenApp-Server muss mit einer alternativen Adresse und die Firewall muss für Netzwerkadressübersetzung konfiguriert sein.

     Hinweis: Auf virtuelle XenDesktop-Desktops kann nicht mit alternativen Adressen zugegriffen werden.

   - Wählen Sie Gateway: übersetzt, wenn die an das Gateway übergebene Adresse von den im Webinterface festgelegten Adressübersetzungszuordnungen bestimmt werden soll.

6. Geben Sie die Netzwerkadresse und die Subnetzmaske des Clientnetzwerkes ein. Ordnen Sie die Zugriffsrouten in der Tabelle Benutzergerätadressen mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach und klicken Sie auf Weiter.

7. Wenn Sie keine Gateway-Adressübersetzung verwenden, fahren Sie mit Schritt 10 fort. Wenn Sie Gateway-Adressübersetzung verwenden, klicken Sie auf der Seite Adressübersetzungen angeben auf Hinzufügen, um eine neue Adressübersetzung hinzuzufügen, oder wählen Sie einen Eintrag aus der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Adressübersetzung zu bearbeiten.

8. Wählen Sie im Bereich Zugriffstyp eine der folgenden Optionen:

- Wenn das Gateway über die übersetzte Adresse eine Verbindung zum Citrix Server herstellen soll, wählen Sie Gateway-Routenübersetzung.

- Wenn Sie in der Tabelle Benutzergerätadressen bereits eine übersetzte Clientroute konfiguriert haben und möchten, dass der Citrix Client und das Gateway beide die übersetzte Adresse für die Verbindungsherstellung mit dem Citrix Server verwenden, wählen Sie Benutzergerät- und Gateway-Routenübersetzung.

9. Geben Sie die internen und externen (übersetzten) Ports und Adressen für den Citrix Server ein und klicken Sie auf OK. Wenn das Gateway eine Verbindung zum Citrix Server herstellt, werden die externe Portnummer und Adresse verwendet. Stellen Sie sicher, dass die Zuordnungen, die Sie erstellen, zu den Adresstypen passen, die die Serverfarm verwendet. Klicken Sie auf Weiter.

10. Geben Sie auf der Seite Gateway-Einstellungen angeben den vollqualifizierten Domänennamen (FQDN) und die Portnummer des Gateways ein, den dieser Client verwenden muss. Der FQDN muss mit dem FQDN auf dem Zertifikat übereinstimmen, das auf dem Gateway installiert ist.

11. Wenn der Citrix Server getrennte Sitzungen aufrechterhalten soll, während der Client eine Wiederverbindung versucht, aktivieren Sie das Kontrollkästchen Sitzungszuverlässigkeit aktivieren.

12. Wenn Sie Sitzungszuverlässigkeit aktiviert haben und Ticketing von zwei Secure Ticket Authoritys (STAs) verwenden möchten, aktivieren Sie das Kontrollkästchen Tickets von zwei STAs anfordern (wenn verfügbar). Wenn diese Option aktiviert ist, ruft das Webinterface Tickets von zwei verschiedenen Secure Ticket Authoritys ab, damit Benutzersitzungen nicht unterbrochen werden, wenn eine Secure Ticket Authority während der Sitzung ausfällt. Wenn das Webinterface aus irgendeinem Grund keine Verbindung zu zwei Secure Ticket Authoritys herstellen kann, wird automatisch nur eine Secure Ticket Authority verwendet. Klicken Sie auf Weiter.

    Hinweis: Sie müssen Access Gateway bereitstellen, um diese Funktion verwenden zu können. Secure Gateway unterstützt zurzeit keine mehrfachen redundanten Secure Ticket Authoritys.

13. Klicken Sie auf der Seite Secure Ticket Authority-Einstellungen angeben auf Hinzufügen, um die URL einer Secure Ticket Authority anzugeben, die das Webinterface verwenden kann, oder wählen Sie einen Eintrag in der Liste aus und klicken Sie auf Bearbeiten, um die Angaben einer vorhandenen Secure Ticket Authority zu bearbeiten. Der Citrix XML-Dienst enthält Secure Ticket Authoritys, z. B. in http[s]://*Servername.Domäne.com*/scripts/ctxsta.dll. Sie können mehr als eine Secure Ticket Authority angeben, um Fehlertoleranz zu erreichen; Citrix rät jedoch davon ab, externe Load Balancing-Programme für diesen Zweck zu verwenden. Ordnen Sie die Secure Ticket Authoritys mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach.

14. Mit der Option Für Load Balancing verwenden können Sie festlegen, ob Load Balancing zwischen Secure Ticket Authoritys verwendet werden soll. Wenn Sie Load Balancing aktivieren, werden die Verbindungen gleichmäßig auf die Server verteilt, sodass kein Server überlastet wird.

15. Geben Sie mit den Feldern Ausgefallene Server umgehen an, wie lange nicht erreichbare Secure Ticket Authoritys umgangen werden sollen. Das Webinterface bietet Fehlertoleranz zwischen den Servern in der Liste Secure Ticket Authority-URLs, sodass im Fall eines Kommunikationsfehlers der ausgefallene Server während der angegebenen

Zeitspanne umgangen wird.

So konfigurieren Sie Standardzugriffseinstellungen

Die Regeln werden in der Reihenfolge angewendet, in der die Einträge in der Tabelle Benutzergerätadressen angezeigt werden. Wenn die Benutzergerätadresse nicht mit den explizit definierten Zugriffsregeln übereinstimmt, wird die Standardregel angewendet. Bei der Erstellung einer Site wird automatisch direkter Zugriff als Standardroute konfiguriert. Mit der Aufgabe Sicherer Zugriff in der Citrix Webinterface Management Console können Sie eine für Ihre Bereitstellung geeignete Standardzugriffsmethode festlegen.

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Sicherer Zugriff.

4. Wählen Sie auf der Seite Zugriffsmethoden angeben den Eintrag Standard aus der Liste aus und klicken Sie auf Bearbeiten.

5. Wählen Sie in der Liste Zugriffsmethode eine der folgenden Optionen:

   - Wählen Sie Direkt, wenn die tatsächliche Adresse des Citrix Servers an den Citrix Client übergeben werden soll.

   - Wenn die alternative Adresse des XenApp-Servers an den Client übergeben werden soll, wählen Sie Alternative Adresse. Der XenApp-Server muss mit einer alternativen Adresse und die Firewall muss für Netzwerkadressübersetzung konfiguriert sein.

     Hinweis: Auf virtuelle XenDesktop-Desktops kann nicht mit alternativen Adressen zugegriffen werden.

   - Wählen Sie Übersetzt, wenn die an den Client übergebene Adresse von den im Webinterface festgelegten Adressübersetzungszuordnungen bestimmt werden soll.

   - Wählen Sie Gateway: direkt, wenn die tatsächliche Adresse des Citrix Servers an das Gateway übergeben werden soll.

   - Wählen Sie Gateway: alternative Adresse, wenn die alternative Adresse des XenApp-Servers an das Gateway übergeben werden soll. Der XenApp-Server muss mit einer alternativen Adresse und die Firewall muss für Netzwerkadressübersetzung konfiguriert sein.

     Hinweis: Auf virtuelle XenDesktop-Desktops kann nicht mit alternativen Adressen zugegriffen werden.

   - Wählen Sie Gateway: übersetzt, wenn die an das Gateway übergebene Adresse von den im Webinterface festgelegten Adressübersetzungszuordnungen bestimmt werden soll.

6. Geben Sie die Netzwerkadresse und die Subnetzmaske des Clientnetzwerkes ein. Ordnen Sie die Zugriffsrouten in der Tabelle Benutzergerätadressen mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach.

7. Wenn Sie Adressübersetzung oder ein Gateway in Ihrer Bereitstellung verwenden, klicken Sie auf Weiter und geben Sie die entsprechenden zusätzlichen Einstellungen für die Standardkonfiguration ein. Weitere Informationen finden Sie unter So konfigurieren Sie die interne Firewalladressübersetzung und So konfigurieren Sie Gateway-Einstellungen.

Bearbeiten von clientseitigen Proxyeinstellungen

Wenn Sie bei der Webinterface-Installation einen clientseitigen Proxyserver verwenden, können Sie konfigurieren, ob die Citrix Clients diesen Proxyserver für die Kommunikation mit dem Server, auf dem XenApp oder XenDesktop ausgeführt werden, verwenden müssen. Hierzu können Sie die Aufgabe Clientseitiger Proxy in der Citrix Webinterface Management Console verwenden.

Ein Proxyserver, der sich auf der Clientseite des Webinterface befindet, bietet die folgenden Sicherheitsvorteile:

- Verbergen von Informationen. Innerhalb der Firewall verwendete Systemnamen werden nicht über DNS (Domain Name System) außerhalb der Firewall bekannt gegeben.
- Weiterleiten (Channeling) verschiedener TCP-Verbindungen über eine Verbindung.

Mit der Citrix Webinterface Management Console können Sie Proxystandardregeln für Citrix Clients festlegen. Sie können jedoch auch Ausnahmen für einzelne Benutzergeräte konfigurieren. Zum Konfigurieren von Ausnahmen verknüpfen Sie die externe IP-Adresse des Proxyservers mit einer Webinterface-Proxyeinstellung.

Sie können auch festlegen, dass das Proxyverhalten vom Client gesteuert wird. Beispiel: Sie möchten die Funktion für die Verwendung eines sicheren Proxys (Secure Proxy) in XenApp und XenDesktop nutzen. Konfigurieren Sie das Webinterface für die Verwendung der im Client angegebenen Proxyeinstellungen und den Client für Secure Proxy. Weitere Informationen zur Verwendung von Citrix Clients zum Steuern des Proxyverhaltens finden Sie in der Dokumentation für den jeweiligen Client.

So konfigurieren Sie Standardproxyeinstellungen

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.
3. Klicken Sie im Bereich Aktionen auf Clientseitiger Proxy.
4. Klicken Sie auf Hinzufügen, um eine neue Zuordnung zu erstellen, oder wählen Sie einen Eintrag in der Liste aus und klicken Sie auf Bearbeiten, um eine vorhandene Zuordnung zu bearbeiten.
5. Geben Sie die externe Adresse des Proxys und die Subnetzmaske des Benutzergeräts in den Feldern IP-Adresse und Subnetzmaske ein.
6. Treffen Sie in der Dropdownliste Proxy eine Auswahl:
   - Wenn der Citrix Client den Webproxy basierend auf der Browserkonfiguration des Benutzergeräts automatisch ermitteln soll, wählen Sie Browsereinstellungen des Benutzers.
   - Wenn der Client den Webproxy mit dem Web Proxy Auto Discovery (WPAD)-Protokoll automatisch ermitteln soll, wählen Sie Automatische Webproxysuche.
   - Wenn die vom Benutzer für den Client konfigurierten Einstellungen verwendet werden sollen, wählen Sie Clienteinstellung verwenden.
   - Wenn ein SOCKS-Proxyserver verwendet werden soll, wählen Sie SOCKS. Wenn Sie diese Option wählen, müssen Sie die Adresse und Portnummer des Proxyservers eingeben. Die Proxyadresse kann eine IP-Adresse oder ein DNS-Name sein.
   - Wenn ein sicherer Proxyserver verwendet werden soll, wählen Sie Secure (HTTPS). Wenn Sie diese Option wählen, müssen Sie die Adresse und Portnummer des Proxyservers eingeben. Die Proxyadresse kann eine IP-Adresse oder ein DNS-Name sein.
   - Wenn kein Proxy verwendet werden soll, wählen Sie Kein Proxy.
7. Wenn Sie mehr als eine Zuordnung eingegeben haben, ordnen Sie die Zuordnungen in der Tabelle mit den Schaltflächen Nach oben und Nach unten ihrer Priorität nach.

Anpassen der Darstellung für Benutzer

Sie können die Darstellung der Benutzeroberfläche anpassen, wenn die Site beispielsweise entsprechend den Unternehmensstandards gestaltet werden soll.

Mit der Aufgabe Websitedarstellung in der Citrix Webinterface Management Console können Sie Folgendes anpassen:

- **Layout:** Legen Sie fest, welche Steuerelemente Benutzern zur Verfügung stehen, und definieren Sie, wie die Website angezeigt wird. Sie haben folgende Möglichkeiten:
    - Wählen Sie "Automatisch", "Kompletter Grafikinhalt" oder "Reduzierter Grafikinhalt" als Layout für die XenApp Web-Site. Die Benutzeroberfläche mit reduziertem Grafikinhalt ist eine kompakte Version für Benutzer, die mit kleinformatigen Geräten oder über langsame Netzwerkverbindungen auf Ressourcen zugreifen. Mit der Option Automatisch wählt das System das am besten geeignete Sitelayout für jeden Benutzer je nach der Größe des Computerbildschirms.
    - Konfigurieren Sie die Funktionen und Steuerelemente, die Benutzer auf der Seite Anwendungen sehen, einschließlich von Suche und Tipps, und legen Sie fest, ob Benutzer ihre eigenen Bildschirme anpassen können.
    - Legen Sie die Standardansichtseinstellungen für die Ressourcengruppen der Benutzer bei reduziertem und komplettem Grafikinhalt fest. Sie können außerdem festlegen, aus welchen Anzeigetypen Benutzer auswählen können.
    - Legen Sie fest, wie Ressourcen auf der Seite Anwendungen der Benutzer gruppiert werden sollen. Sie können entweder getrennte Registerkarten für Anwendungen, Inhalte und Desktops konfigurieren oder Sie können alle Ressourcen auf einer Registerkarte anzeigen.
- **Appearance:** Passen Sie die Benutzeroberfläche durch die Verwendung unterschiedlicher Farben und Grafiken auf der Site an das Branding Ihres Unternehmens an. Sie haben folgende Möglichkeiten:
    - Legen Sie das Aussehen der Anmeldeseite für Benutzer fest. Wählen Sie zwischen einem Minimallayout, bei dem nur die entsprechenden Anmeldefelder angezeigt werden, und einem Layout, das eine Navigationsleiste enthält, mit der Benutzer auf die Seiten Meldungen und Einstellungen zugreifen können.
    - Verwenden Sie individuell angepasste Grafiken für das Sitebranding von Layouts mit komplettem und reduziertem Grafikinhalt. Sie können die Grafiken falls gewünscht auch mit Hyperlinks versehen. Sie können auch das Hintergrundbild, das im Kopfzeilenbereich der Site angezeigt wird, ändern, oder einfach eine bestimmte Farbe verwenden.
- **Inhalte:** Definieren Sie benutzerdefinierte Meldungen und Bildschirmtext und geben Sie lokalisierte Versionen dieses Texts in den Sprachen an, mit denen Ihre Benutzer möglicherweise auf die Site zugreifen. Sie können Seitentitel und Meldungen für die Seiten Anmeldung und Anwendungen festlegen und Fußzeilentext auf allen Seiten anzeigen. Zusätzlich können Sie Haftungsausschlusserklärungen konfigurieren, die Benutzer vor der Anmeldung annehmen müssen.

Verwalten von Ressourcenverknüpfungen und Aktualisierungsoptionen

Aktualisiert: 2014-11-24

Mit der Aufgabe Verknüpfungen in der Citrix Webinterface Management Console können Sie festlegen, wie das Citrix Online Plug-In Verknüpfungen für Ressourcen anzeigt.

Sie können die folgenden Verknüpfungstypen erstellen:

- **Startmenü:** Sie können die mit der Aufgabe Verknüpfungen angegebenen Einstellungen oder die Einstellungen, die bei der Ressourcenveröffentlichung mit XenApp und XenDesktop festgelegt wurden, oder beide verwenden. Zusätzlich können Sie definieren, ob und wie Verknüpfungen im Startmenü angezeigt werden, und das Ändern dieser Einstellung durch Benutzer zulassen. Sie können auch Verknüpfungen im Menü Alle Programme sowie zusätzliche Untermenüs erstellen und/oder das Festlegen von Namen für Untermenüs durch Benutzer zulassen.

- **Desktop:** Sie können die mit der Aufgabe Verknüpfungen angegebenen Einstellungen oder die Einstellungen, die bei der Ressourcenveröffentlichung mit XenApp und XenDesktop festgelegt wurden, oder beide verwenden. Zusätzlich können Sie definieren, ob und wie Verknüpfungen auf dem Desktop angezeigt werden, und das Ändern dieser Einstellung durch Benutzer zulassen. Sie können darüber hinaus einen benutzerdefinierten Ordnernamen verwenden und/oder das Auswählen eines Namens durch Benutzer zulassen.

- **Infobereich:** Sie können Ressourcen im Infobereich anzeigen und/oder zulassen, dass Benutzer festlegen, wie Ressourcen angezeigt werden.

Auch das Entfernen von Verknüpfungen wird mit der Aufgabe Verknüpfungen ausgeführt. Sie können festlegen, zu welchem Zeitpunkt Verknüpfungen entfernt werden (beim Beenden des Citrix Online Plug-Ins oder beim Abmelden der Benutzer von XenApp). Für Benutzer, die Windows CE oder Linux ausführen, können Sie außerdem angeben, ob neben den Citrix Online Plug-In-Verknüpfungen auch von den Benutzern erstellte Verknüpfungen entfernt werden. Wenn Sie festlegen, dass Citrix Online Plug-In-Verknüpfungen und die vom Benutzer erstellten Verknüpfungen entfernt werden sollen, können Sie zur Verbesserung der Leistung auch die Ordnersuchtiefe einschränken.

Optionen zum Aktualisieren von Ressourcen

Geben Sie mit der Aufgabe Ressourcenaktualisierung in der Citrix Webinterface Management Console an, wann die Ressourcenlisten der Benutzer aktualisiert werden und ob Benutzer diese Einstellung ändern können. Sie können die Aktualisierung so konfigurieren, dass sie beim Start des Citrix Online Plug-Ins oder beim Zugriff auf Ressourcen durchgeführt wird, und Sie können die Aktualisierungshäufigkeit angeben.

Verwalten der Sitzungseinstellungen

Mit der Aufgabe Sitzungseinstellungen in der Citrix Webinterface Management Console legen Sie die Einstellungen fest, die Benutzer anpassen können. Mit dieser Aufgabe können Sie auch die Zeitspanne festlegen, nach der nicht aktive Benutzer vom Webinterface abgemeldet werden, und angeben, ob das Webinterface den Benutzergerätnamen bei Clients für Onlineressourcen überschreiben soll.

Für XenApp Web-Sites können Sie folgende Einstellungen für Benutzersitzungen vornehmen:

- **Benutzeranpassungen:** Aktivieren oder deaktivieren Sie den Kioskmodus und legen Sie fest, ob Benutzer die Schaltfläche Einstellungen auf der Seite Anwendungen sehen sollen.
- **Websitzungen:** Geben Sie die Zeitspanne an, in der eine Benutzersitzung inaktiv sein darf, bevor der Benutzer abgemeldet wird.
- **Permanente URLs:** Geben Sie an, ob Benutzer mit Browser-Lesezeichen auf die Site zugreifen können.
- **Verbindungsleistung:** Geben Sie Standardeinstellungen an oder erlauben Sie Benutzern, die Einstellungen für Bandbreitensteuerung, Farbtiefe, Audioqualität und Druckerzuordnung selber anpassen zu können.
- **Anzeige:** Legen Sie fest, ob Benutzer die Fenstergröße in gehosteten Sitzungen steuern können und ermöglichen Sie dem Webinterface die Verwendung von ClearType-Schriftartenglättung. Voraussetzung hierfür ist, dass die entsprechenden Einstellungen in den Windows-Betriebssystemen der Benutzer, der Citrix Client-Software der Benutzer und der Serverfarm konfiguriert sind.
- **Lokale Ressourcen:** Konfigurieren Sie Einstellungen für Windows-Tastenkombinationen, PDA-Synchronisierung und Umleitung spezieller Ordner.
- **Benutzergerätnamen:** Legen Sie fest, ob das Webinterface für Onlineressourcen die Gerätnamen von Benutzern überschreiben soll.

  Wichtig: Sie müssen die Option Benutzergerätnamen überschreiben aktivieren, wenn Sie Workspace Control mit den Versionen 8.*x* und 9.*x* der Clients für Windows verwenden möchten.

Für XenApp Services-Sites, die Onlineressourcen bereitstellen, können Sie mit der Aufgabe Sitzungsoptionen in der Citrix Webinterface Management Console folgende Einstellungen für Benutzersitzungen konfigurieren:

- **Anzeige:** Wählen Sie die für ICA-Sitzungen verfügbaren Fenstergrößen aus und geben Sie benutzerdefinierte Größen in Pixeln oder Prozentwerten der Bildschirmgröße an. Zusätzlich können Sie ClearType-Schriftartenglättung für das Webinterface konfigurieren. Voraussetzung hierfür ist, dass die entsprechenden Einstellungen in den Windows-Betriebssystemen der Benutzer, dem Citrix Online Plug-In und der Serverfarm konfiguriert sind.

- **Farbe und Audio:** Der Benutzer kann aus den in diesem Bereich aktivierten Optionen eine Auswahl treffen.

- **Lokale Ressourcen:** Aktivieren Sie die Ziele der Windows-Tastenkombinationen, die Benutzer auswählen können. Die Windows-Tastenkombinationen betreffen keine Seamlessverbindungen. Sie können folgende Ziele aktivieren:

  - **Lokaler Desktop:** Tastenkombinationen gelten nur für den lokalen Desktop. Sie werden nicht an die ICA-Sitzungen übergeben.

  - **Remotedesktop:** Tastenkombinationen gelten für den virtuellen Desktop in der ICA-Sitzung.

  - **Nur auf Desktops im Vollbildmodus:** Tastenkombinationen gelten für den virtuellen Desktop in der ICA-Sitzung nur im Vollbildmodus.

  Aktivieren Sie die Umleitung spezieller Ordner, damit Benutzer beim Öffnen, Schließen oder Speichern von Dateien in Onlineressourcen zu den Ordnern \Dokumente oder \Desktop auf den lokalen Clientcomputern umgeleitet werden. Weitere Informationen finden Sie unter Umleitung spezieller Ordner.

- **Workspace Control:** Konfigurieren Sie das Wiederverbindungs- und Abmeldeverhalten. Weitere Informationen finden Sie unter Konfigurieren von Workspace Control.

Bandbreitensteuerung

Mit der Bandbreitensteuerung können Benutzer Sitzungseinstellungen auf der Grundlage ihrer Verbindungsbandbreite auswählen. Diese Optionen werden vor oder nach der Anmeldung auf der Seite Einstellungen angezeigt. Mit der Bandbreitensteuerung können Farbtiefe, Audioqualität und Druckerzuordnung gesteuert werden. Sie können auch die Web Interface Management Console verwenden, um Standard- oder benutzerdefinierte Einstellungen für Benutzer anzugeben. Mit der Aufgabe Sitzungseinstellungen verwalten können Sie Bandbreiteneinstellungen mit den Optionen unter Verbindungsleistung anpassen. Wählen Sie in der Dropdownliste Verindungsgeschwindigkeit die Option Benutzerdefiniert, um die Optionen Farbqualität, Audio und Druckerzuordnung aktivieren zu aktivieren.

Bei Verwendung des Clients für Java bestimmt die Bandbreitensteuerung, ob Pakete für Audio und Druckerzuordnung verfügbar sind. Bei Verwendung von Software für Remotedesktopverbindungen (RDP) wird die Audioqualität ein- oder ausgeschaltet. Eine weitere Steuerung der Qualität findet nicht statt. Für drahtlose WAN-Verbindungen werden Einstellungen für niedrige Bandbreite empfohlen.

Hinweis: Bei Verwendung von Software für Remotedesktopverbindungen (RDP) zusammen mit der Bandbreitensteuerung legt das Webinterface die geeigneten Parameter für die ausgewählte Bandbreite fest. Das tatsächliche Verhalten richtet sich aber immer nach der Version der verwendeten Remotedesktopverbindungssoftware, den Terminalservern und der Serverkonfiguration.

Benutzer können standardmäßig die Fenstergröße von Sitzungen anpassen.

Wenn Benutzer eine Einstellung nicht anpassen können, wird die Einstellung nicht in der Benutzeroberfläche angezeigt. Es werden die auf dem Server für die Ressource angegebenen Einstellungen verwendet.

ClearType-Schriftartenglättung

ClearType ist eine Anti-Aliasing-Technologie auf Subpixelbasis, mit der die Darstellung von Text auf LCD-Bildschirmen verbessert wird. Hierdurch werden sichtbare Anzeigefehler reduziert und der Text sieht klarer aus. ClearType-Schriftartenglättung ist eine Funktion, die in Windows XP eingeführt wurde. Schriftartenglättung ist in Windows 7 und Windows Vista standardmäßig aktiviert, aber nicht in Windows XP.

Das Webinterface und das Citrix Online Plug-In unterstützen ClearType-Schriftartenglättung in ICA-Sitzungen. Wenn Benutzer, die Windows XP oder höher ausführen, eine Verbindung zum Server herstellen, ermittelt das Plug-In automatisch die Einstellung für Schriftartenglättung auf ihrem Computer und sendet sie an den Server. Diese Einstellung wird dann für die gesamte Dauer der Sitzung verwendet.

Schriftartenglättung muss in den Betriebssystemen der Benutzer, dem Citrix Online Plug-In, der Webinterface-Site und der Serverfarm aktiviert sein. Mit der Aufgabe Sitzungseinstellungen in der Citrix Webinterface Management Console können Sie die Schriftartenglättung für XenApp Web-Sites aktivieren. Für XenApp Services-Sites verwenden Sie die Aufgabe Sitzungsoptionen.

Schriftartenglättung gilt nur für Onlineressourcen. Für Offlineanwendungen kann diese Funktion nicht verwendet werden.

Umleitung spezieller Ordner

Aktualisiert: 2014-11-24

Mit der Funktion zur Umleitung spezieller Ordner können Benutzer besondere Windows-Ordner den Ordnern auf ihrem lokalen Computer zuordnen, damit sie leichter mit Ressourcen verwendet werden können. Der Begriff *spezielle Ordner* bezieht sich speziell auf Windows-Standardordner, wie z. B. \Dokumente und \Desktop, die unabhängig vom Betriebssystem immer gleich angezeigt werden.

Hinweis: In Windows Vista wurden die Namen dieser Ordner geändert, z. B. hieß der Ordner "Dokumente" in Windows XP "Eigene Dateien".

Wenn Benutzer in einer Sitzung ohne Umleitung spezieller Ordner Dateien öffnen, schließen oder speichern, stehen die Symbole Dokumente und Desktop in den Navigationsdialogfeldern von Onlineressourcen für die jeweiligen Ordner auf dem Server. Bei der Umleitung spezieller Ordner werden Aktionen, wie z. B. das Öffnen oder Speichern von Dateien, umgeleitet, sodass Benutzer beim Öffnen oder Speichern von Dateien ihre lokalen Ordner \Dokumente und \Desktop verwenden. Zurzeit wird die Umleitung nur für die Ordner \Dokumente und \Desktop unterstützt.

Umleitung spezieller Ordner gilt nur für Onlineressourcen. Für Offlineanwendungen kann diese Funktion nicht verwendet werden.

Aktivieren der Umleitung spezieller Ordner

Standardmäßig ist die Umleitung spezieller Ordner für XenApp Web- und XenApp Services-Sites deaktiviert. Wenn Sie die Umleitung spezieller Ordner für eine Site aktivieren, müssen Sie sicherstellen, dass keine der in Ihrer Serverfarm vorhandenen Richtlinienregeln Benutzer daran hindern, auf ihre lokalen Laufwerke zuzugreifen oder darauf zu speichern.

Mit der Aufgabe Sitzungseinstellungen in der Citrix Webinterface Management Console können Sie die Umleitung spezieller Ordner für XenApp Web-Sites aktivieren. Für XenApp Services-Sites verwenden Sie die Aufgabe Sitzungsoptionen. Sie können es auch den Benutzern überlassen, ob sie diese Funktion auf der Seite Einstellungen aktivieren möchten.

Wenn die Umleitung spezieller Ordner aktiviert ist, sollten Benutzer Ressourcen vollständigen Lese- und Schreibzugriff auf lokale Dateien und Ordner gewähren, indem Sie im Citrix Connection Center im Dialogfeld Client-Dateisicherheit die Option Vollzugriff aktivieren. Benutzer müssen sich von allen aktiven Sitzungen abmelden, bevor sie eine neue Sitzung auf einem anderen Gerät starten können. Citrix empfiehlt, die Umleitung spezieller Ordner für Benutzer, die von unterschiedlichen Geräten eine Verbindung zu derselben Sitzung herstellen, nicht zu aktivieren.

Konfigurieren von Workspace Control

Mit der Aufgabe "Workspace Control verwalten" können Benutzer schnell alle Ressourcen (Anwendungen, Inhalte und Desktops) trennen, Verbindungen zu getrennten Ressourcen wiederherstellen und sich von allen Ressourcen abmelden. Dies ermöglicht es Benutzern, zwischen Benutzergeräten zu wechseln und jederzeit beim Anmelden oder manuell Zugriff auf alle Ressourcen zu erhalten (nur getrennte oder getrennte und aktive Anwendungen). Beispiel: Angestellte eines Krankenhauses müssen eventuell verschiedene Arbeitsstationen verwenden und jedes Mal auf dieselbe Gruppe von Ressourcen zugreifen, wenn sie sich anmelden.

Workspace Control-Anforderungen

Die folgenden Funktionen, Anforderungen und Empfehlungen gelten für die Workspace Control-Funktion:

- Um Workspace Control mit den Versionen 8.*x* und 9.*x* der Clients für Windows zu verwenden, müssen Sie mit der Aufgabe Sitzungseinstellungen in der Citrix Webinterface Management Console die Option Benutzergerätnamen überschreiben aktivieren.

- Erkennt das Webinterface, dass von einer Citrix Sitzung darauf zugegriffen wird, wird Workspace Control deaktiviert.

- Je nach den Sicherheitseinstellungen blockt Internet Explorer den Download von Dateien, die scheinbar nicht direkt vom Benutzer angefordert wurden. Aus diesem Grund können Versuche, mit einem nativen Client Verbindungen zu Ressourcen wiederherzustellen, geblockt werden. In Situationen, in denen eine Wiederverbindung nicht möglich ist, wird eine Warnungsmeldung angezeigt und Benutzer haben die Möglichkeit, die Sicherheitseinstellungen von Internet Explorer neu zu konfigurieren.

- Alle Websitzungen werden nach einem gewissen Inaktivitätszeitraum beendet (Standardwert ist 20 Minuten). Wird die HTTP-Sitzung beendet, wird die Abmeldeseite angezeigt. Ressourcen, auf die in dieser Sitzung zugegriffen oder die erneut verbunden wurden, werden jedoch nicht getrennt. Benutzer müssen die Verbindung manuell trennen, sich abmelden oder sich neu am Webinterface anmelden und die Schaltflächen Abmelden oder Trennen verwenden.

- Ressourcen, die für anonyme Benutzer veröffentlicht wurden, werden beendet, wenn sowohl anonyme als auch authentifizierte Benutzer die Verbindung trennen, vorausgesetzt, der Citrix XML-Dienst ist so eingestellt, dass er den Webinterface-Anmeldeinformationen vertraut. Benutzer können daher die Verbindung zu anonymen Ressourcen nicht wiederherstellen, falls diese getrennt wurde.

- Damit Sie Passthrough, Smartcard oder Passthrough mit Smartcard für die Authentifizierung verwenden können, müssen Sie eine Vertrauensstellung zwischen dem Webinterface-Server und dem Citrix XML-Dienst herstellen. Weitere Informationen finden Sie unter Verwenden von Workspace Control mit integrierten Authentifizierungsmethoden für XenApp Web-Sites.

- Ist Passthrough von Anmeldeinformationen für XenApp Services-Sites nicht aktiviert, werden Smartcard-Benutzer aufgefordert, für jede erneut verbundene Citrix Sitzung ihre PIN-Nummer einzugeben. Dies ist bei Passthrough- oder Passthrough-mit-Smartcard-Authentifizierung für XenApp Services-Sites kein Problem, da bei diesen Optionen auch Passthrough von Anmeldeinformationen aktiviert wird.

Workspace Control-Einschränkungen

Wenn Sie Workspace Control aktivieren möchten, beachten Sie Folgendes:

- Workspace Control steht nicht für Sites zur Verfügung, die Offlineanwendungen bereitstellen. Wenn Sie eine Site für Dual Mode-Bereitstellung konfigurieren, funktioniert Workspace Control nur für Onlineressourcen.

- Workspace Control kann nicht mit dem Client für 32-Bit-Windows vor Version 8 oder mit Software für Remotedesktopverbindungen (RDP) verwendet werden. Außerdem ist diese Funktion nur auf Servern verfügbar, die Presentation Server ab Version 4.5 ausführen.

- Workspace Control ermöglicht nur die Wiederverbindung von getrennten virtuellen XenDesktop-Desktops. Benutzer können keine virtuellen Desktops wiederverbinden, die angehalten wurden.

Verwenden von Workspace Control mit integrierten Authentifizierungsmethoden für XenApp Web-Sites

Dieser Abschnitt gilt nur für XenApp Web-Sites Wenn sich Benutzer mit den Authentifizierungsmethoden Passthrough, Smartcard oder Passthrough mit Smartcard anmelden, müssen Sie eine Vertrauensstellung zwischen dem Webinterface-Server und allen Servern herstellen, auf denen der Citrix XML-Dienst ausgeführt wird, zu dem das Webinterface eine Verbindung herstellt. Der Citrix XML-Dienst sendet Informationen über Ressourcen vom Webinterface an die Server, auf denen XenApp und XenDesktop ausgeführt wird, und umgekehrt. Besteht diese Vertrauensstellung nicht, sind die Schaltfläche Trennen, Wiederverbinden und Abmelden für Benutzer deaktiviert, die sich mit Smartcard oder Passthrough anmelden.

Es ist keine Vertrauensstellung erforderlich, wenn die Benutzer von der Serverfarm authentifiziert werden, also wenn sich Benutzer nicht mit den Authentifizierungsmethoden Smartcard oder Passthrough anmelden.

So stellen Sie die Vertrauensstellung her

Wenn Sie einen Server für das Vertrauen von Anfragen konfigurieren, die an den Citrix XML-Dienst gesendet werden, sollten Sie folgende Faktoren berücksichtigen:

- Wenn Sie die Vertrauensstellung herstellen, müssen Sie sich darauf verlassen, dass der Webinterface-Server den Benutzer authentifiziert. Verwenden Sie zur Vermeidung von Sicherheitsrisiken IPSec, Firewalls oder andere Verfahren, die sicherstellen, dass nur vertrauenswürdige Dienste mit dem Citrix XML-Dienst kommunizieren. Wenn Sie die Vertrauensstellung ohne solche Vorkehrungen erstellen, kann ein beliebiges Netzwerkgerät Sitzungen trennen oder beenden. Wenn Sites nur für die explizite Authentifizierung konfiguriert sind, ist keine Vertrauensstellung erforderlich.

- Aktivieren Sie die Vertrauensstellung nur auf Servern, auf die das Webinterface direkt zugreift. Diese Server werden in der Aufgabe Serverfarmen in der Citrix Webinterface Management ManagementConsole aufgeführt.

- Konfigurieren Sie die Komponenten, mit der Sie Ihre Umgebung sichern, so, dass nur der Webinterface-Server auf den Citrix XML-Dienst zugreifen kann. Wenn der Citrix XML-Dienst und Microsoft Internet Information Services (IIS) z. B. einen Port gemeinsam verwenden, können Sie die IP-Adressenbeschränkung in IIS zum Beschränken des Zugriffs auf den Citrix XML-Dienst verwenden.

1. Melden Sie sich an der Serverfarm an und klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix Delivery Services Console.

2. Gehen Sie im linken Bereich der Konsole zu Citrix Ressourcen > XenApp, erweitern Sie den Knoten Ihrer Farm und klicken Sie auf Richtlinien.

3. Wählen Sie im Detailbereich der Konsole die Registerkarte Computer und klicken Sie auf Neu.

4. Geben Sie einen Namen ein und falls gewünscht eine Beschreibung der neuen Richtlinie und klicken Sie auf Weiter.

5. Klicken Sie in der Liste Kategorien auf XML-Dienst, wählen Sie unter Einstellungen die Option XML-Anfragen vertrauen und klicken Sie auf Hinzufügen.

6. Wählen Sie Aktiviert und klicken Sie auf OK. Klicken Sie auf Weiter.

7. Wenden Sie falls erforderlich Filter auf Ihre Richtlinie an, um die Umstände festzulegen, unter denen sie angewendet wird, und klicken Sie auf Weiter.

8. Stellen Sie sicher, dass das Kontrollkästchen Richtlinie aktivieren aktiviert ist und klicken Sie auf Speichern.

So aktivieren Sie automatische Wiederverbindung bei Benutzeranmeldung

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf die Aufgabe für Ihren Sitetyp:

   - Klicken Sie für XenApp-Web-Sites auf Workspace Control.

   - Klicken Sie für XenApp-Services-Sites auf Sitzungsoptionen und wählen Sie Workspace Control.
4. Aktivieren Sie die Option Automatische Wiederverbindung von Sitzungen bei Anmeldung.

5. Wählen Sie eine der folgenden Optionen:

   - Um sowohl getrennte als auch aktive Sitzungen automatisch wiederzuverbinden, aktivieren Sie Alle Sitzungen wiederverbinden.

   - Um nur getrennte Sitzungen automatisch wiederzuverbinden, aktivieren Sie Nur getrennte Sitzungen wiederverbinden.
6. Aktivieren Sie das Kontrollkästchen Benutzerseitig anpassbar, damit Benutzer diese Einstellung auf der Seite "Verbindungseinstellungen" selbst konfigurieren können. Benutzer können diese Einstellung auf der Seite Einstellungen von XenApp Web-Sites oder im Citrix Online Plug-In-Dialogfeld Optionen ändern.

So aktivieren Sie die Schaltfläche "Wiederverbinden"

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites oder XenApp Services-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf die Aufgabe für Ihren Sitetyp:

   - Klicken Sie für XenApp-Web-Sites auf Workspace Control.

   - Klicken Sie für XenApp-Services-Sites auf Sitzungsoptionen und wählen Sie Workspace Control.
4. Aktivieren Sie die Option Schaltfläche 'Wiederverbinden' aktivieren.

5. Wählen Sie eine der folgenden Optionen:

   - Wenn Sie die Schaltfläche Wiederverbinden konfigurieren möchten, um Benutzer wieder mit getrennten und aktiven Sitzungen zu verbinden, aktivieren Sie Alle Sitzungen wiederverbinden.

   - Wenn Sie die Schaltfläche Wiederverbinden konfigurieren möchten, um nur getrennte Sitzungen automatisch wiederzuverbinden, aktivieren Sie Nur getrennte Sitzungen wiederverbinden.
6. Aktivieren Sie das Kontrollkästchen Benutzerseitig anpassbar, damit Benutzer diese Einstellung auf der Seite "Verbindungseinstellungen" selbst konfigurieren können. Benutzer können diese Einstellung auf der Seite Einstellungen von XenApp Web-Sites oder im Citrix Online Plug-In-Dialogfeld Optionen für XenApp Services-Sites ändern.

So konfigurieren Sie das Abmeldeverhalten

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.

2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie Ihre Site im Ergebnisbereich aus.

3. Klicken Sie im Bereich Aktionen auf Workspace Control.

4. Aktivieren Sie das Kontrollkästchen Aktive Sitzungen bei Abmeldung von der Site abmelden, um Benutzer vom Webinterface und allen aktiven Sitzungen abzumelden. Wenn Sie diese Option nicht aktivieren, bleiben Sitzungen aktiv, nachdem Benutzer sich abgemeldet haben.

5. Aktivieren Sie das Kontrollkästchen Benutzerseitig anpassbar, damit Benutzer diese Einstellung auf der Seite Einstellungen der Site selbst konfigurieren können.

Konfigurieren der Webinterface-Sicherheit

Ein umfassender Sicherheitsplan muss Daten an allen Punkten des Bereitstellungsprozesses für Ressourcen schützen. Dieser Abschnitt enthält eine Beschreibung der Sicherheitsprobleme für das Webinterface und Empfehlungen für die folgenden Kommunikationsverbindungen:

- **Kommunikation zwischen Benutzergerät und Webinterface:** Erläutert Probleme, die mit dem Übertragen von Webinterface-Daten zwischen Webbrowsern und Servern verbunden sind, und schlägt Strategien zum Sichern der Daten vor, wenn diese übertragen und auf Benutzergeräte geschrieben werden.

- **Kommunikation zwischen Webinterface und Citrix Server:** Beschreibt das Sichern der Authentifizierung und der Informationen über Ressourcen, die zwischen dem Webinterface-Server und der Serverfarm ausgetauscht werden.

- **Kommunikation zwischen Sitzung und Server:** Erläutert Probleme, die mit dem Übertragen von Sitzungsinformationen zwischen Citrix Clients und Servern verbunden sind, und beschreibt die Implementierung der Webinterface- und XenApp/XenDesktop-Sicherheitsfunktionen zum Schutz dieser Daten.

In dieser Abbildung wird die Interaktion zwischen den Benutzergeräten und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, und dem Webinterface-Server beschrieben.

Allgemeine Sicherheitsüberlegungen

Citrix empfiehlt, dass Sie genauso wie bei jedem Windows-basierten Server die Microsoft Standardrichtlinien für die Konfiguration des Servers einhalten.

Stellen Sie sicher, dass für alle Komponenten immer die neuesten Patches installiert sind. Weitere Informationen und die aktuellen Downloadempfehlungen finden Sie auf der Microsoft Website unter http://support.microsoft.com/.

SSL und TLS

Aktualisiert: 2014-12-02

Das SSL-Protokoll (Secure Sockets Layer) sichert die Datenkommunikation in Netzwerken. SSL bietet Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfung der Nachrichtenintegrität.

SSL verschlüsselt Nachrichten mit Kryptografie, authentifiziert die Identität und gewährleistet die Integrität der Inhalte. Dies schützt vor Abhören, falschem Weiterleiten und Datenmanipulation. SSL prüft die Identität mit Zertifikaten, die öffentliche Schlüssel enthalten und von Zertifizierungsstellen ausgegeben werden. Weitere Informationen zu SSL, Kryptografie und Zertifikate finden Sie unter Sichern von Serverfarmen und Sicheres Unternehmensnetzwerk.

TLS (Transport Layer Security)

TLS (Transport Layer Security) ist die neueste, standardisierte Version des SSL-Protokolls. Die Organisation IETF (Internet Engineering Taskforce) hat das Protokoll nach der Übernahme der Verantwortung für die Entwicklung von SSL als einen offenen Standard in TLS umbenannt. TLS bietet wie SSL Serverauthentifizierung, Verschlüsselung des Datenstroms und Prüfung der Nachrichtenintegrität.

TLS Version 1.0 wird von allen unterstützten Versionen von XenApp für Windows und XenDesktop unterstützt. Da zwischen SSL Version 3.0 und TLS Version 1.0 nur geringfügige technische Unterschiede bestehen, können die Serverzertifikate, die Sie für SSL in Ihrer Installation verwenden, auch für TLS eingesetzt werden.

Einige Organisationen, u. a. amerikanische Regierungsstellen, verlangen das Sichern der Datenkommunikation mit TLS. Diese Organisationen verlangen ggf. auch die Verwendung überprüfter Kryptografie, wie z. B. FIPS 140. FIPS (Federal Information Processing Standard) ist ein Kryptografiestandard.

Hinweis: Das Webinterface für Java-Anwendungsserver unterstützt SSL- bzw. TLS-Zertifikatschlüssel von maximal 2048 Bit.

SSL-Relay

Das SSL-Relay ist eine Komponente, die SSL zum Sichern der Kommunikation zwischen Webinterface-Servern und Serverfarmen verwendet. Das SSL-Relay stellt Serverauthentifizierung, Datenverschlüsselung und Nachrichtenintegrität für TCP/IP-Verbindungen zur Verfügung. Das SSL-Relay wird durch den Citrix XTE-Dienst bereitgestellt.

Das SSL-Relay vermittelt die Kommunikation zwischen dem Webinterface-Server und dem Citrix XML-Dienst. Wenn das SSL-Relay verwendet wird, überprüft der Webserver zuerst die Identität des SSL-Relays, indem das Serverzertifikat des Relays mit einer Liste der vertrauenswürdigen Zertifizierungsstellen verglichen wird.

Nach dieser Authentifizierung handeln der Webserver und das SSL-Relay eine Verschlüsselungsmethode für die Sitzung aus. Der Webserver sendet dann alle Informationsanfragen in verschlüsselter Form an das SSL-Relay. Das SSL-Relay entschlüsselt die Anfragen und übergibt sie an den Citrix XML-Dienst. Bei der Rückgabe der Informationen an den Webserver sendet der Citrix XML-Dienst alle Informationen über den Server, auf dem das SSL-Relay ausgeführt wird, der die Daten verschlüsselt und an den Webserver zur Entschlüsselung weiterleitet. Nachrichtenintegritätsprüfungen stellen sicher, dass die Kommunikation nicht manipuliert wurde.

ICA-Verschlüsselung

Mit der ICA-Verschlüsselung können die zwischen einem Server und einem Citrix Client übermittelten Informationen verschlüsselt werden. Für unbefugte Benutzer ist es daher schwierig, eine verschlüsselte Übertragung zu interpretieren.

ICA-Verschlüsselung sichert Vertraulichkeit und schützt so vor einem möglichen Abhören. Es bestehen jedoch weitere Sicherheitsrisiken und die Verwendung von Verschlüsselung ist nur ein Aspekt einer umfassenden Sicherheitsrichtlinie. Im Gegensatz zu SSL/TLS wird bei ICA-Verschlüsselung der Server nicht authentifiziert. Informationen könnten theoretisch im Netzwerk abgefangen und an einen falschen Server weitergeleitet werden. Bei ICA-Verschlüsselung wird auch die Integrität nicht überprüft.

ICA-Verschlüsselung steht nicht auf Servern mit XenApp für UNIX zur Verfügung.

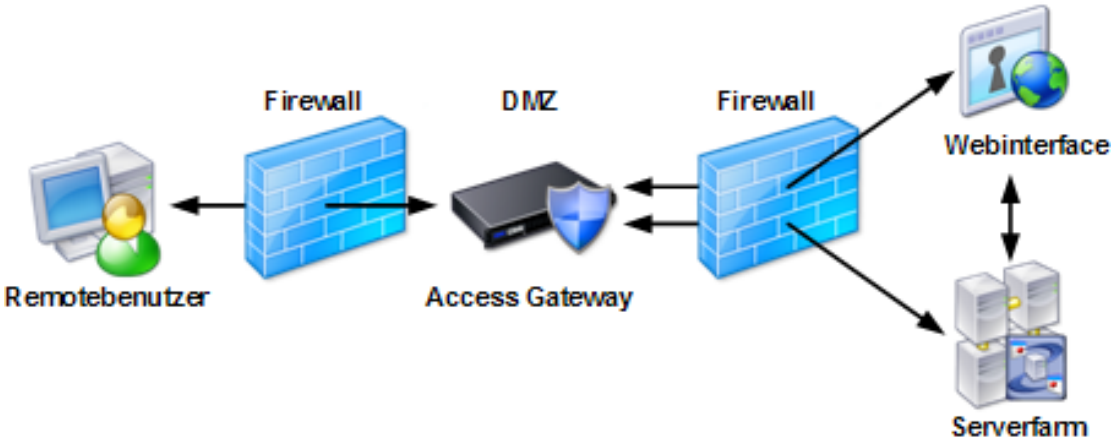
Access Gateway

Sie können Access Gateway mit dem Webinterface und der Secure Ticket Authority (STA) für die Authentifizierung, Autorisierung und Umleitung von Ressourcen (Anwendungen, Inhalte und Desktops) verwenden, die von einem Server mit XenApp oder XenDesktop bereitgestellt werden.

Access Gateway ist ein universelles SSL-VPN-Gerät, das sicheren und zentralen Zugriff auf alle Informationsressourcen ermöglicht, sowohl Daten als auch Sprache. Access Gateway verschlüsselt und unterstützt alle Ressourcen und Protokolle.

Da Access Gateway Remotebenutzern nahtlosen, sicheren Zugriff auf autorisierte Anwendungen, Inhalte, Desktops und Netzwerkressourcen bietet, können die Benutzer so mit Dateien auf Netzwerklaufwerken, E-Mails, Intranet-Sites und Ressourcen arbeiten, als ob sie sich innerhalb der Firewall ihrer Organisation befänden.

In dieser Abbildung wird dargestellt, wie Access Gateway die Kommunikation zwischen SSL/TLS-fähigen Citrix Clients und Servern sichert.



Weitere Informationen über Access Gateway finden Sie in der Access Gateway-Dokumentation. Weitere Informationen zur Konfiguration des Webinterface für Access Gateway mit der Citrix Webinterface Management Console finden Sie unter So konfigurieren Sie Gateway-Einstellungen.

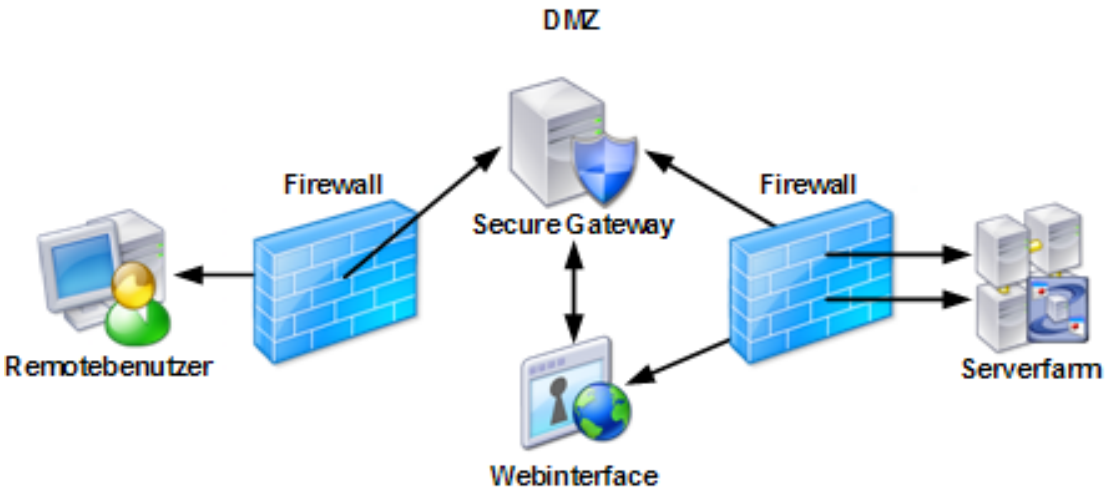
Secure Gateway

Aktualisiert: 2014-11-25

Secure Gateway stellt zusammen mit dem Webinterface einen einzigen sicheren, verschlüsselten Zugangspunkt über das Internet zu Servern in internen Unternehmensnetzwerken bereit.

Secure Gateway ist ein sicheres Internetgateway zwischen SSL/TLS-fähigen Citrix Clients und Servern, das den ICA-Datenverkehr verschlüsselt. Die Datenübertragungen über das Internet zwischen den Benutzergeräten und dem Secure Gateway-Server werden mit SSL/TLS verschlüsselt. Dies ermöglicht es dem Benutzer, ohne Gefährdung der Sicherheit remote auf Informationen zuzugreifen. Secure Gateway vereinfacht auch die Zertifikatverwaltung, da nur der Secure Gateway-Server und nicht jeder Server in der Serverfarm ein Serverzertifikat benötigt.

In dieser Abbildung wird dargestellt, wie Secure Gateway die Kommunikation zwischen SSL/TLS-fähigen Citrix Clients und Servern sichert.



Weitere Informationen zur Konfiguration des Webinterface für Secure Gateway mit der Citrix Webinterface Management Console finden Sie unter So konfigurieren Sie Gateway-Einstellungen.

Sichern des Citrix Online Plug-Ins mit SSL

Wenn Sie die Kommunikation zwischen dem Citrix Online Plug-In und dem Webinterface-Server mit der Citrix Webinterface Management Console mit SSL sichern möchten, klicken Sie im linken Bereich auf XenApp Services-Sites, wählen Sie die Site im Ergebnisbereich aus, klicken Sie im Bereich Aktionen auf Servereinstellungen und aktivieren Sie das Kontrollkästchen SSL/TLS für Kommunikation zwischen Plug-Ins und der Site verwenden.

Stellen Sie sicher, dass in der Delivery Services Console für jede Anwendung im Eigenschaften-Dialogfeld der Anwendung auf der Seite Clientoptionen das Kontrollkästchen SSL- und TLS-Protokoll aktivieren aktiviert ist.

Kommunikation zwischen Benutzergerät und Webinterface

Bei der Kommunikation zwischen Citrix Clients und dem Webinterface-Server werden verschiedene Datentypen übertragen. Wenn sich der Benutzer identifiziert, nach Ressourcen sucht und dann auf eine Ressource zugreift, tauschen der Webbrowser und der Webserver Anmeldeinformationen, Ressourcengruppen und Dateien für die Sitzungsinitialisierung aus. Die folgenden Daten werden im Rahmen dieser Übertragungen auf dem Netzwerk weitergeleitet:

- **HTML-Formulardaten:** Webinterface-Sites übertragen die Anmeldeinformationen des Benutzers bei der Anmeldung mithilfe eines HTML-Standardformulars vom Webbrowser an den Webserver. Das Webinterface-Formular übergibt die Namen und Anmeldeinformationen der Benutzer im Klartext.

- **HTML-Seiten und Sitzungscookies:** Wenn Benutzer ihre Anmeldeinformationen auf der Seite Anmeldung eingegeben haben, werden die Anmeldeinformationen auf dem Webserver gespeichert und von einem Sitzungscookie geschützt. Die HTML-Seiten, die vom Webserver an den Browser gesendet werden, enthalten Ressourcengruppen. Diese Seiten führen die Ressourcen auf, die für den Benutzer verfügbar sind.

- **ICA-Dateien:** Wenn ein Benutzer eine Ressource auswählt, sendet der Webserver eine ICA-Datei für diese Ressource an den Citrix Client (in einigen Fällen mit dem Webbrowser als Vermittler). Die ICA-Datei enthält ein Ticket, das für die Anmeldung am Server verwendet werden kann. ICA-Dateien enthalten keine Tickets für die Passthrough- oder Smartcard-Authentifizierung.

  Beim Start eines Clients wird die ICA-Datei manchmal als Klartextdatei auf der Festplatte des Benutzers gespeichert. Dies verhindert jedoch nicht das erfolgreiche Starten des Clients.

  Mit der Funktion zum Signieren von ICA-Dateien können Benutzer überprüfen, ob sie Anwendungen oder Desktops von einem vertrauenswürdigen Webserver starten. Weitere Informationen finden Sie unter Konfigurieren der Funktion zum Signieren von ICA-Dateien.

Sicherheitsprobleme bei der Datenübertragung zwischen Benutzergerät und Webinterface

Angreifer können Webinterface-Daten abfangen, wenn diese im Netzwerk zwischen dem Webserver und dem Browser übertragen oder auf das Benutzergerät geschrieben werden:

- Angreifer können Anmeldedaten, das Sitzungscookie und HTML-Seiten abfangen, die zwischen dem Webserver und dem Browser übermittelt werden.
- Das vom Webinterface verwendete Sitzungscookie ist temporär und wird entfernt, wenn der Benutzer den Webbrowser schließt. Angreifer mit Zugriff auf den Browser des Benutzers können das Cookie jedoch abrufen und möglicherweise die Anmeldeinformationen verwenden.
- Die ICA-Datei enthält zwar keine Anmeldeinformationen aber ein Einmalticket, das standardmäßig nach 200 Sekunden ungültig wird. Angreifer können theoretisch mit der abgefangenen ICA-Datei eine Verbindung zum Server herstellen, bevor der autorisierte Benutzer mit dem Ticket eine Verbindung herstellt.
- Wenn Benutzer von Internet Explorer, die über eine HTTPS-Verbindung auf den Webserver zugreifen, die Option, mit der verhindert wird, dass verschlüsselte Seiten gespeichert werden, aktivieren, wird die ICA-Datei als Klartextdatei im Windows-Ordner \Temporary Internet Files gespeichert. Angreifer mit Zugriff auf den Internet Explorer-Cache des Benutzers könnten die ICA-Datei abrufen und darüber Netzwerkinformationen erhalten.
- Wenn Passthrough im Citrix Client aktiviert ist, könnten Angreifer dem Benutzer eine ICA-Datei übermitteln, die die Anmeldeinformationen des Benutzers an einen nicht autorisierten oder falschen Server weiterleitet. Dies passiert, wenn der Client die Anmeldeinformationen eines Benutzers bei der Anmeldung an seinem Gerät abfängt und diese an einen beliebigen Server weiterleitet, wenn die entsprechende Einstellung in der ICA-Datei enthalten ist.

Empfehlungen für das Sichern der Kommunikation zwischen Benutzergeräten und dem Webinterface

Die folgenden Empfehlungen kombinieren Sicherheitspraktiken gemäß dem Industriestandard und von Citrix zur Verfügung gestellte Sicherheitsmaßnahmen, um die Daten zu schützen, die zwischen Benutzergeräten und dem Webserver übertragen werden, sowie die Daten, die auf Benutzergeräte geschrieben werden.

Implementieren von SSL/TLS-fähigen Webservern und Browsern

Das Sichern der Webserver-zu-Browser-Komponente der Webinterface-Kommunikation beginnt mit dem Implementieren sicherer Webserver und Browser. Viele sichere Webserver verwenden die SSL/TLS-Technologie zum Sichern des Webverkehrs.

In einer typischen Webserver-zu-Browser-Transaktion überprüft der Browser zuerst die Identität des Servers, indem er das Zertifikat des Servers mit einer Liste der vertrauenswürdigen Zertifizierungsstellen vergleicht. Nach dieser Überprüfung verschlüsselt der Browser Seitenanfragen des Benutzers und entschlüsselt dann die Dokumente, die vom Webserver zurückgegeben werden. Am Ende der Transaktion stellen TLS- oder SSL-Nachrichtenintegritätsprüfungen sicher, dass die Daten bei der Übertragung nicht manipuliert wurden.

In einer Webinterface-Bereitstellung wird durch Authentifizierung und Verschlüsselung mit SSL/TLS eine sichere Verbindung hergestellt, über die der Benutzer Anmeldeinformationen übergeben kann, die auf der Seite Anmeldung eingegeben werden. Daten, die vom Webserver gesendet werden, einschließlich Anmeldeinformationen, Sitzungscookies, ICA-Dateien und der HTML-Ressourcengruppenseiten, sind gleichfalls sicher.

Sie können die SSL/TLS-Technologie nur im Netzwerk implementieren, wenn Sie einen SSL/TLS-fähigen Webserver und SSL/TLS-fähige Webbrowser haben. Die Verwendung dieser Produkte ist für das Webinterface transparent. Webserver oder Webbrowser müssen nicht für das Webinterface konfiguriert werden. Weitere Informationen zur Konfiguration des Webservers für die Unterstützung von SSL/TLS finden Sie in der Webserverdokumentation.

Wichtig: Viele SSL/TLS-fähige Webserver verwenden den TCP/IP-Port 443 für die HTTP-Kommunikation. Standardmäßig verwendet das SSL-Relay ebenfalls diesen Port. Wenn auf Ihrem Webserver gleichzeitig das SSL-Relay ausgeführt wird, stellen Sie sicher, dass der Webserver oder das SSL-Relay einen anderen Port verwendet.

Deaktivieren der Passthrough-Authentifizierung

Passthrough-Authentifizierung darf in sicheren Installationen nicht aktiviert werden, um ein mögliches Weiterleiten der Anmeldeinformationen der Benutzer an einen nicht autorisierten oder falschen Server zu verhindern. Aktivieren Sie diese Funktion nur in einem kleinen, vertrauenswürdigen Umfeld.

Kommunikation zwischen Webinterface und Citrix Server

Die Kommunikation zwischen dem Webinterface und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, beinhaltet Folgendes: Übertragung der Benutzeranmeldeinformationen und Ressourcengruppeninformationen zwischen dem Webinterface und dem Citrix XML-Dienst in der Serverfarm.

In einer typischen Sitzung überträgt das Webinterface die Anmeldeinformationen an den Citrix XML-Dienst für die Benutzerauthentifizierung und der Citrix XML-Dienst gibt Ressourcengruppeninformationen zurück. Der Server und die Farm senden die Informationen über eine TCP/IP-Verbindung unter Verwendung des Citrix XML-Protokolls.

Sicherheitsprobleme bei der Kommunikation zwischen dem Webinterface und dem Citrix Server

Das Webinterface-XML-Protokoll verwendet Klartext für den Austausch aller Daten mit Ausnahme von Kennwörtern, die in schwach verschlüsselter Form übertragen werden. Die Kommunikation hat folgende Schwachstellen:

- Angreifer können den XML-Verkehr abfangen und auf diese Weise Ressourcengruppeninformationen und Tickets erhalten. Angreifer mit der Fähigkeit, die schwache Verschlüsselung aufzulösen, können außerdem Anmeldeinformationen erhalten.
- Angreifer können die Identität des Servers annehmen und Authentifizierungsanfragen abfangen.

Empfehlungen für das Sichern der Kommunikation zwischen dem Webinterface und dem Citrix Server

Citrix empfiehlt die Implementierung einer der folgenden Sicherheitsmaßnahmen, um den zwischen dem Webinterface-Server und der Serverfarm übertragenen XML-Datenverkehr zu sichern:

- Verwenden Sie das SSL-Relay als Sicherheitsbarriere zwischen dem Webinterface-Server und der Serverfarm. Das SSL-Relay führt die Hostauthentifizierung und Datenverschlüsselung aus.
- Installieren Sie in Bereitstellungen, die das SSL-Relay nicht unterstützen, das Webinterface auf dem Server, auf dem XenApp oder XenDesktop ausgeführt wird.
- Verwenden Sie das HTTPS-Protokoll für die Übermittlung von Webinterface-Daten über eine sichere HTTP-Verbindung mit SSL, wenn IIS auf dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, installiert ist.

Verwenden des SSL-Relays

Aktualisiert: 2014-12-02

Das SSL-Relay ist eine Standardkomponente von XenApp und XenDesktop.

Auf der Serverseite müssen Sie ein Serverzertifikat auf dem Server, auf dem SSL-Relay ausgeführt wird, installieren und die Konfiguration des Servers überprüfen. Weitere Informationen zur Installation eines Serverzertifikats und der Konfiguration des SSL-Relays auf Servern finden Sie unter Konfigurieren von SSL/TLS zwischen Server und Client. Sie finden zusätzliche Informationen in der Onlinehilfe für das SSL-Relay-Konfigurationstool. Informationen zu Servern mit XenApp für UNIX finden Sie unter SSL-Relay für UNIX-Administration.

Stellen Sie bei der Konfiguration des SSL-Relays sicher, dass der Server, auf dem das SSL-Relay ausgeführt wird, die Weiterleitung von SSL-Datenübertragungen an die Server zulässt, die Sie als Kontaktpunkt für den Citrix XML-Dienst verwenden. Standardmäßig leitet das SSL-Relay den Datenverkehr nur an den Server weiter, auf dem das Relay installiert ist. Das SSL-Relay kann jedoch für das Weiterleiten von Datenverkehr an andere Server konfiguriert werden. Wenn das SSL-Relay auf einem Server installiert ist, an den Sie keine Webinterface-Daten senden möchten, vergewissern Sie sich, dass der Server, an den Sie Webinterface-Daten weiterleiten möchten, in der Serverliste des SSL-Relays aufgeführt ist.

Sie können das Webinterface für die Verwendung des SSL-Relays mit der Citrix Webinterface Management Console oder der Datei WebInterface.conf konfigurieren. Weitere Informationen dazu, wie Sie das Webinterface mit der Konsole für die Verwendung des SSL-Relays konfigurieren, finden Sie unter Konfigurieren von Einstellungen für alle Server in einer Farm.

So konfigurieren Sie das Webinterface für die Verwendung des SSL-Relays mit der Datei WebInterface.conf

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor.
2. Ändern Sie die Einstellung SSLRelayPort im Parameter **Farm<*n*>** zur Portnummer des SSL-Relays auf dem Server.
3. Ändern Sie den Wert der Einstellung Transport im Parameter **Farm<*n*>** zu SSL.

So fügen Sie dem Webinterface-Server ein neues Stammzertifikat hinzu

Um Unterstützung für eine Zertifizierungsstelle hinzuzufügen, müssen Sie dem Webinterface-Server das Stammzertifikat der betreffenden Zertifizierungsstelle hinzufügen.

Kopieren Sie das Stammzertifikat auf den Webserver.

- In IIS wird das Zertifikat mit dem Snap-In Zertifikate der Microsoft Management Console (MMC) kopiert.
- Verwenden Sie auf Java-Anwendungsservern das Befehlszeilentool keytool, um das Zertifikat in das richtige Schlüsselspeicherverzeichnis auf Ihrer jeweiligen Plattform zu kopieren. Das Zertifikat muss dem Schlüsselspeicher hinzugefügt werden, der mit der Java Virtual Machine verknüpft ist, die die Webseiten bereitstellt. Der Schlüsselspeicher befindet sich üblicherweise an einem der folgenden Speicherorte:
  - {javax.net.ssl.trustStore}
  - {java.home}/lib/security/jssecacerts
  - {java.home}/lib/security/cacerts

Aktivieren des Webinterface auf dem Server, auf dem XenApp oder XenDesktop ausgeführt wird

In Bereitstellungen, die das Ausführen des SSL-Relays nicht unterstützen, kann ein Netzwerkangriff verhindert werden, indem ein Webserver auf dem Server ausgeführt wird, der die Webinterface-Daten zur Verfügung stellt. Wenn Sie die Webinterface-Sites auf einem solchen Webserver hosten, werden alle Webinterface-Anfragen an den Citrix XML-Dienst auf dem lokalen Host geroutet. Auf diese Weise entfällt die Übertragung von Webinterface-Daten über das Netzwerk. Die Vorteile, die sich aus dem Wegfall der Netzwerkübertragung ergeben, müssen gegen das Risiko von Angriffen auf den Webserver abgewogen werden.

Als erstes können Sie sowohl den Webserver als auch den Server, auf dem XenApp oder XenDesktop ausgeführt wird, hinter einer Firewall einrichten, damit die Kommunikation zwischen den Servern nicht im Internet offenbart wird. In diesem Szenario müssen die Benutzergeräte in der Lage sein, durch die Firewall mit dem Webserver und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, zu kommunizieren. Die Firewall muss HTTP-Datenübertragungen für die Kommunikation zwischen Benutzergerät und Webserver zulassen (meist über den HTTP-Standardport 80 oder 443, wenn ein sicherer Webserver verwendet wird). Für die Kommunikation zwischen Client und Servern muss die Firewall eingehende ICA-Datenübertragungen an den Ports 1494 und 2598 zulassen. Weitere Informationen über die Verwendung von ICA mit Netzwerkfirewalls finden Sie in der Dokumentation Ihres Webservers. Weitere Informationen zur Verwendung des Webinterface mit der Netzwerkadressübersetzung finden Sie im Webinterface-SDK.

Hinweis: Bei der Installation von XenApp-Systemen können Sie erzwingen, dass der Citrix XML-Dienst denselben TCP/IP-Port wie IIS verwendet. Bei XenDesktop aktiviert das Installationsprogramm automatisch die Portfreigabe. Wenn die Portfreigabe aktiviert ist, verwenden der Citrix XML-Dienst und der Webserver standardmäßig denselben Port.

Verwenden des HTTPS-Protokolls

Mit dem HTTPS-Protokoll können Sie die zwischen dem Webserver und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, übertragenen Webinterface-Daten sichern. HTTPS bietet mit SSL/TLS starke Datenverschlüsselung.

Der Webserver stellt eine HTTPS-Verbindung zu IIS auf dem Server her, auf dem XenApp oder XenDesktop ausgeführt wird. Hierfür muss der IIS-Port auf dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, freigegeben sein und in IIS auf diesem Server muss SSL aktiviert sein. Der von Ihnen (über die Konsole oder den Parameter **Farm<*n*>** in der Datei WebInterface.conf) angegebene Servername muss ein vollqualifizierter DNS-Name sein, der dem Namen auf dem SSL-Serverzertifikat von IIS entspricht.

Der Citrix XML-Dienst kann über folgende Adresse aufgerufen werden: https://*Servername*/scripts/wpnbr.dll. Weitere Informationen zur Konfiguration des Webinterface für die Verwendung des HTTPS-Protokolls mit der Citrix Webinterface Management Console finden Sie unter Verwalten des sicheren Zugriffs.

So konfigurieren Sie das Webinterface für die Verwendung von HTTPS mit der Datei WebInterface.conf

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor.
2. Ändern Sie den Wert der Einstellung Transport im Parameter **Farm<*n*>** zu HTTPS.

Kommunikation zwischen Benutzersitzung und Server

Bei der Webinterface-Kommunikation zwischen Benutzergeräten und Servern werden verschiedene Typen von Sitzungsdaten übergeben, einschließlich Initialisierungsanfragen und Sitzungsinformationen.

- **Initialisierungsanfragen:** In der ersten Phase der Sitzungsherstellung, die *Initialisierung* genannt wird, fordert der Citrix Client eine Sitzung an und übergibt eine Liste der Konfigurationsparameter für die Sitzung. Diese Parameter steuern zahlreiche Aspekte der Sitzung, u. a. welcher Benutzer angemeldet wird, die Größe des angezeigten Fensters und das in der Sitzung ausgeführte Programm.

- **Sitzungsinformationen:** Nach der Sitzungsinitialisierung werden über verschiedene virtuelle Kanäle Informationen zwischen dem Citrix Client und dem Server übertragen, z. B. Mauseingaben (vom Client zum Server) und grafische Aktualisierungen (vom Server zum Client).

Sicherheitsprobleme bei der Kommunikation zwischen Benutzersitzungen und Servern

Um die Netzwerkkommunikation zwischen dem Client und dem Server abzufangen und zu interpretieren, müssen Angreifer in der Lage sein, das binäre Clientprotokoll zu entschlüsseln. Angreifer, die das binäre Clientprotokoll kennen, können folgende Informationen abfangen:

- Informationen zu den Initialisierungsanforderungen, die vom Citrix Client gesendet werden, einschließlich der Anmeldeinformationen

- Sitzungsinformationen, einschließlich des vom Benutzer eingegebenen Texts und der vom Benutzer eingegebenen Mausklicks, sowie Bildschirmaktualisierungen, die vom Server gesendet werden

Empfehlungen für das Sichern der Kommunikation zwischen Benutzersitzungen und Servern

Aktualisiert: 2014-12-02

Citrix empfiehlt, die Datenübertragungen zwischen den Benutzergeräten und Servern entweder durch Verschlüsselung oder durch Bereitstellen von Access Gateway zu sichern.

Verwenden von SSL/TLS- oder ICA-Verschlüsselung

Citrix empfiehlt die Implementierung von SSL/TLS- oder ICA-Verschlüsselung zum Sichern der Datenübertragungen zwischen den Citrix Clients und den Servern. Beide Verfahren unterstützen die Verschlüsselung des Datenstroms zwischen dem Client und dem Server mit 128 Bit. SSL/TLS unterstützt außerdem die Überprüfung der Identität des Servers.

SSL wird von allen unterstützten Versionen von XenApp und XenDesktop unterstützt. SSL/TLS und ICA-Verschlüsselung werden von allen unterstützten Versionen von XenApp für Windows und XenDesktop unterstützt. Eine Liste der Citrix Clients und welche Methode sie unterstützen, finden Sie in der Dokumentation für die Clients auf der Citrix Downloadsite. Weitere Informationen zur ICA-Verschlüsselung finden Sie unter XenApp-Administration.

Verwenden von Access Gateway

Mit Access Gateway können Sie die Datenübertragung zwischen den Citrix Clients und den Servern über das Internet sichern. Access Gateway ist ein universelles SSL-VPN-Gerät, das sicheren, zentralen Zugriff auf alle Ressourcen ermöglicht. Weitere Informationen über Access Gateway finden Sie in der archivierten Access Gateway-Dokumentation. Weitere Informationen zur Konfiguration des Webinterface für Access Gateway mit der Citrix Webinterface Management Console finden Sie unter So konfigurieren Sie Gateway-Einstellungen.

Steuern der Diagnoseprotokollierung

Mit der Aufgabe Diagnoseprotokollierung unter Sitewartung in der Citrix Webinterface Management Console können Sie die Systemsicherheit für die Fehlerprotokollierung erhöhen. Sie können ein wiederholtes Protokollieren von doppelten Ereignissen unterdrücken oder deren Anzahl und Protokollierungshäufigkeit konfigurieren.

Mit dieser Aufgabe können Sie auch die Weiterleitungs-URL bei Fehlern angeben. Wenn Sie eine benutzerdefinierte Fehlerrückgabe-URL verwenden, müssen Sie alle Fehler-IDs mit dieser URL verarbeiten und Fehlermeldungen für die Benutzer anzeigen. Die Fehlerrückgabe-URL ersetzt außerdem die Abmeldeseiten der Benutzer, auch wenn Benutzer sich erfolgreich ohne Fehler abgemeldet haben.

Konfigurieren von Sites mit der Konfigurationsdatei

Aktualisiert: 2014-11-24

Sitekonfigurationsdateien

Webinterface-Sites enthalten eine Datei namens WebInterface.conf, die die Konfigurationsdaten der jeweiligen Site enthält. Mit dieser Datei können Sie alltägliche Verwaltungsaufgaben ausführen und Einstellungen für eine Site anpassen. Sie können beispielsweise die Einstellungen festlegen, die Benutzer ändern können, oder die Authentifizierung beim Webinterface konfigurieren.

Wenn Sie beim Bearbeiten einer Konfigurationsdatei einen ungültigen Wert für eine Einstellung eingeben und anschließend die Citrix Webinterface Management Console verwenden, ersetzt die Konsole den ungültigen Wert durch den Standardwert, wenn die Datei gespeichert wird.

Wenn die Citrix Webinterface Management Console ausgeführt wird, während Sie eine Konfigurationsdatei manuell bearbeiten, werden diese manuellen Änderungen von Änderungen, die Sie anschließend mit der Konsole ausführen, überschrieben. Citrix empfiehlt, die Citrix Webinterface Management Console zu schließen, bevor Sie die Konfigurationsdateien der Site bearbeiten. Wenn dies nicht möglich ist, sollten Sie die Konsole aktualisieren, um die manuellen Änderungen der Konfigurationsdatei zu übernehmen, bevor Sie weitere Änderungen mit der Konsole vornehmen.

Die Datei WebInterface.conf ist im Konfigurationsverzeichnis der Site gespeichert:

- In Microsoft Internetinformationsdienste (IIS) ist die Datei üblicherweise unter C:\inetpub\wwwroot\Citrix*Sitename*\conf
- Auf Java-Anwendungsservern, z. B. Apache Tomcat, kann dies ./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF sein

Sie können in den Webserverskripten einige Konfigurationswerte in der Datei WebInterface.conf für individuelle Seiten ändern. Weitere Informationen zu Webserverskripts finden Sie im Webinterface-SDK.

Hinweis: Auf Java-Anwendungsservern müssen Sie ggf. den Webserver anhalten und neu starten, damit die Änderungen in WebInterface.conf wirksam werden. Sie müssen außerdem darauf achten, Ihre Änderungen in UTF-8-Codierung zu speichern.

So konfigurieren Sie die Kommunikation mit dem Server

In diesem Beispiel soll der Name eines zusätzlichen Servers angegeben werden, auf dem der Citrix XML-Dienst ausgeführt wird. Der Citrix XML-Dienst fungiert als Kommunikationsverbindung zwischen der Serverfarm und dem Webinterface-Server.

Die Kommunikation erfolgt zurzeit mit einem Server namens "Bremen". Sie möchten den Server "Hamburg" für den Fall hinzufügen, dass "Bremen" ausfällt. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor und suchen Sie die folgende Zeile:

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

2. Schließen Sie in dieser Zeile den zusätzlichen Server folgendermaßen ein:

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

So konfigurieren Sie die SSL-Relay-Kommunikation

In diesem Beispiel möchten Sie die Kommunikation zwischen dem Webserver und dem Server, auf dem XenApp oder XenDesktop ausgeführt wird, mit SSL (Secure Sockets Layer) sichern. Das SSL-Relay wird auf dem Server mit XenApp oder XenDesktop installiert, der den vollqualifizierten Domänennamen "Berlin.Unternehmen.com" hat. Das SSL-Relay hört den TCP-Port 443 ab.

Die Kommunikation erfolgt zurzeit über den Server "Cottbus". Sie möchten jedoch "Cottbus" durch "Berlin.Unternehmen.com" ersetzen. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor und suchen Sie die folgende Zeile:

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

2. Ändern Sie Transport wie folgt zu SSL:

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

Hinweis: Der angegebene Servername muss dem Namen auf dem Serverzertifikat entsprechen.

So konfigurieren Sie die Unterstützung für Citrix Secure Gateway

In diesem Beispiel soll ein Secure Gateway-Server mit dem Namen "csg1.Unternehmen.com" angegeben werden, auf dem die Citrix Clients den Port 443 mit den folgenden beiden Secure Ticket Authority-Adressen verwenden:

- http://Leipzig.Unternehmen.com/scripts/ctxsta.dll
- http://Dresden.Unternehmen.com/scripts/ctxsta.dll

Fügen Sie der Datei WebInterface.conf die folgenden Zeilen hinzu:

```
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
```

Mit der letzten Zeile wird Secure Gateway für alle Benutzer aktiviert.

So konfigurieren Sie Farmen für die Wiederherstellung im Notfall

In diesem Beispiel haben Sie zwei Farmen eingerichtet, die nur verwendet werden, wenn Benutzer aufgrund eines Problems nicht auf die normalen Farmen zugreifen können, z. B. Strom- oder Netzwerkausfall.

Die Namen der Server, auf denen der Citrix XML-Dienst ausgeführt wird, lauten "München" und "Frankfurt". Diese Farmen möchten Sie für die Wiederherstellung im Notfall verwenden. Öffnen Sie dazu mit einem Texteditor die Datei WebInterface.conf und fügen Sie die folgenden Zeilen hinzu. Konfigurieren Sie dabei die Einstellungen für diesen Parameter entsprechend Ihrer Umgebung:

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

Beachten Sie, dass die zweite Farm nur verwendet wird, wenn auf die erste Farm für die Wiederherstellung im Notfall nicht zugegriffen werden kann. Ressourcen werden nicht über beide Notfallfarmen verteilt, da sie nicht ständig im Einsatz sind. Stattdessen versucht das Webinterface, eine Notfallfarm nach der anderen zu kontaktieren, und listet die Anwendungen der Farm auf, zu der als erstes eine Verbindung hergestellt werden konnte.

WebInterface.conf-Parameter

Aktualisiert: 2014-11-25

In der nachstehenden Tabelle sind die Parameter (in alphabetischer Reihenfolge) aufgeführt, die in der Datei WebInterface.conf enthalten sein können. Standardwerte sind **fett** markiert. Ist ein Parameter nicht in der Datei WebInterface.conf angegeben, wird der Standardwert verwendet.

AccountSelfServiceUrl

- Beschreibung: Gibt die URL für den Password Manager-Dienst an.
- Wert: Gültige URL mit HTTPS
- Sitetyp: XenApp Web

AdditionalExplicitAuthentication

- Beschreibung: Gibt die explizite Zweifaktorauthentifizierung an, die zusätzlich zu SAM, ADS oder NDS ausgeführt werden muss.
- Wert: None | SecurID | SafeWord | RADIUS
- Sitetyp: XenApp Web

AddressResolutionType

- Beschreibung: Gibt an, welcher Adresstyp in der ICA-Startdatei zu verwenden ist.
- Wert: dns-port | dns | ipv4-port | ipv4
- Sitetyp: XenApp Web und XenApp Services

AGAuthenticationMethod

- Beschreibung: Gibt die zulässigen Authentifizierungsmethoden für in Access Gateway integrierte Sites an. Dieser Parameter muss auf "Explicit" gesetzt werden, wenn sich Benutzer mit einem Benutzernamen und Kennwort an Access Gateway anmelden. Wenn sich Benutzer mit einer Smartcard an Access Gateway anmelden und dieser Parameter auf "SmartCard" gesetzt wird, müssen Benutzer jedes Mal, wenn sie auf eine Ressource zugreifen, eine PIN-Nummer eingeben. Mit der Option "SmartCardKerberos" können sich Benutzer mit einer Smartcard an Access Gateway anmelden, um auf ihre Ressourcen zuzugreifen, ohne dass sie ihre PIN-Nummer eingeben müssen.
- Wert: Explicit | SmartCard | SmartCard Kerberos
- Sitetyp: XenApp Web

AGEPromptPassword

- Beschreibung: Gibt an, ob Benutzer bei der Anmeldung über die Access Gateway-Anmeldeseite erneut zur Eingabe des Kennworts aufgefordert werden.
- Wert: Off | On
- Sitetyp: XenApp Web

AGEWebServiceURL

- Beschreibung: Gibt die URL für den Access Gateway-Authentifizierungsdienst an.
- Wert: Gültige URL
- Sitetyp: XenApp Web

AllowBandwidthSelection

- Beschreibung: Gibt an, ob Benutzer die Geschwindigkeit ihrer Netzwerkverbindungen angeben können, damit ICA-Einstellungen optimiert werden können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeAudio

- Beschreibung: Gibt an, ob Benutzer die Audioqualität für ICA-Sitzungen anpassen können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeAutoLogin

- Beschreibung: Gibt an, ob Benutzer automatische Anmeldung aktivieren und deaktivieren können.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizeClientPrinterMapping

- Beschreibung: Gibt an, ob Benutzer die Clientdruckerzuordnung aktivieren und deaktivieren können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeJavaClientPackages

- Beschreibung: Gibt an, ob Benutzer auswählen können, welche Client für Java-Pakete sie verwenden möchten.

- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeLayout

- Beschreibung: Gibt an, ob Benutzer auswählen können, ob sie die Benutzeroberfläche mit komplettem oder mit reduziertem Grafikinhalt verwenden möchten.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeLogoff

- Beschreibung: Gibt an, ob Benutzer das Verhalten von Workspace Control ändern können, wenn sie sich vom Server abmelden.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizePersistFolderLocation

- Beschreibung: Gibt an, ob Benutzer die Funktion, mit der sie bei der Anmeldung zu dem Ordner auf der Seite "Anwendungen" gelangen, in dem sie zuletzt gearbeitet haben, aktivieren und deaktivieren können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeReconnectAtLogin

- Beschreibung: Gibt an, ob Benutzer das Verhalten von Workspace Control bei der Anmeldung ändern können.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizeReconnectButton

- Beschreibung: Gibt an, ob Benutzer das Verhalten von Workspace Control ändern können, wenn sie auf die Schaltfläche "Wiederverbinden" geklickt haben.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizeSettings

- Beschreibung: Gibt an, ob Benutzer ihre Webinterface-Sitzungen anpassen können. Wenn dieser Parameter auf "Off" gesetzt ist, wird die Schaltfläche "Einstellungen" nicht auf den Seiten "Anmeldung" und "Anwendungen" der Benutzer angezeigt.

- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizeShowHints

- Beschreibung: Gibt an, ob Benutzer die Tipps auf der Seite "Anwendungen" anzeigen und verbergen können.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowCustomizeShowSearch

- Beschreibung: Gibt an, ob Benutzer die Suchfunktion auf der Seite "Anwendungen" aktivieren und deaktivieren können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeSpecialFolderRedirection

- Beschreibung: Gibt an, ob Benutzer die Funktion zur Umleitung spezieller Ordner aktivieren und deaktivieren können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeTransparentKeyPassthrough

- Beschreibung: Gibt an, ob Benutzer das Passthroughverhalten für Tastenkombinationen auswählen können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeVirtualCOMPortEmulation

- Beschreibung: Gibt an, ob Benutzer die PDA-Synchronisierung aktivieren und deaktivieren können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeWinColor

- Beschreibung: Gibt an, ob Benutzer die Farbtiefe für ICA-Sitzungen ändern können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowCustomizeWinSize

- Beschreibung: Gibt an, ob Benutzer die Fenstergröße für ICA-Sitzungen ändern können.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowDisplayInFrames

- Beschreibung: Gibt an, ob XenApp Web-Sites in Frames angezeigt werden dürfen, die in Drittanbieter-Webseiten eingebettet sind.
- Wert: On | Off
- Sitetyp: XenApp Web

AllowFontSmoothing

- Beschreibung: Gibt an, ob Schriftartenglättung in ICA-Sitzungen zulässig ist.
- Wert: On | Off
- Sitetyp: XenApp Web und XenApp Services

AllowUserAccountUnlock

- Beschreibung: Gibt an, ob Benutzer die Sperrung ihres Kontos mit Konto-Self-Service aufheben können.
- Wert: Off | On
- Sitetyp: XenApp Web

AllowUserPasswordChange

- Beschreibung: Gibt an, unter welchen Bedingungen Benutzer ihr Kennwort ändern können.
- Wert: Never | Expired-Only | Always (nur XenApp Web)
- Sitetyp: XenApp Web und XenApp Services

AllowUserPasswordReset

- Beschreibung: Gibt an, ob Benutzer ihre Kennwörter mit Konto-Self-Service zurücksetzen können.
- Wert: Off | On
- Sitetyp: XenApp Web

AlternateAddress

- Beschreibung: Gibt an, ob die alternative Serveradresse in der ICA-Datei zurückgegeben wird.

- Wert: Off | Mapped | On
- Sitetyp: XenApp Web und XenApp Services

ApplicanceEmbeddedSmartCardSSO

- Beschreibung: Gibt an, ob die Smartcard-Authentifizierung das eingebettete ActiveX-Steuerelement für Single Sign-On verwendet.
- Wert: Off | On
- Sitetyp: Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- Beschreibung: Die Anzahl von Sekunden, die die Seite für die Eingabe der PIN für die eingebettete Smartcard-Authentifizierung wartet, bevor wieder die Anmeldeseite angezeigt wird, wenn keine Eingabe erfolgt.
- Wert: 20
- Sitetyp: Desktop Appliance Connector

ApplianceMultiDesktop

- Beschreibung: Gibt an, ob die Liste mit Desktops angezeigt wird, wenn Benutzern mehrere Desktops zugewiesen sind.
- Wert: Off | On
- Sitetyp: Desktop Appliance Connector

ApplicationAccessMethods

- Beschreibung: Gibt an, ob Benutzer mit einem Client für Onlineressourcen, dem Citrix Offline Plug-In oder beiden auf Anwendungen zugreifen können.
- Wert: Remote, Streaming
- Sitetyp: XenApp Web und XenApp Services

AppSysMessage _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Text an, der unten im Hauptinhaltsbereich der Seite "Anwendungen" angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

AppTab<*n*>

- Beschreibung: Gibt an, welche Registerkarten auf der Seite "Anwendungen" angezeigt werden. Sie können mehrere Instanzen der Werte verwenden, um mehrere

Registerkarten zu definieren. Mit dem Wert AllResources können Sie eine einzige Registerkarte definieren, die alle für den Benutzer verfügbaren Ressourcen enthält.

- Wert: Applications | Desktops | Content | AllResources
- Sitetyp: XenApp Web

AppWelcome Message _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Text an, der oben im Hauptinhaltsbereich der Seite "Anwendungen" angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

AuthenticationPoint

- Beschreibung: Gibt an, wo die Benutzerauthentifizierung stattfindet.
- Wert: WebInterface | ADFS | AccessGateway | 3rdParty | WebServer
- Sitetyp: XenApp Web

AutoLaunchDesktop

- Beschreibung: Gibt an, ob automatischer Zugriff auf Desktops aktiviert ist. Wenn dieser Parameter auf "On" gesetzt ist, startet das Webinterface automatisch den Desktop eines Benutzers, wenn dies die einzige verfügbare Ressource in allen Farmen ist.
- Wert: Off | On
- Sitetyp: XenApp Web

AutoLoginDefault

- Beschreibung: Gibt an, ob automatische Anmeldungen standardmäßig für Benutzer aktiviert sind, die mit Passthrough-, Passthrough-mit-Smartcard- und Smartcard-Authentifizierung auf Ressourcen zugreifen.
- Wert: On | Off
- Sitetyp: XenApp Web

BrandingColor

- Beschreibung: Gibt die Farbe für die Kopfzeilen- und Fußzeilenbereiche an.
- Wert: Hexadezimale Farbnummer oder Farbname
- Sitetyp: XenApp Web

BrandingImage

- Beschreibung: Gibt die URL für die Brandinggrafik im Kopf- und Fußzeilenbereich an.
- Wert: Gültige URL
- Sitetyp: XenApp Web

BypassFailedRadiusServerDuration

- Beschreibung: Gibt die Dauer bis zum nächsten Versuch an, einen RADIUS-Server nach einem Fehlschlagen erneut zu verwenden.
- Wert: Zeit in Minuten (60)
- Sitetyp: XenApp Web

BypassFailedSTADuration

- Beschreibung: Gibt die Dauer bis zum nächsten Versuch an, einen Server, auf dem die Secure Ticket Authority für ein Gateway-Gerät ausgeführt wird, nach einem Fehlschlag erneut zu verwenden.
- Wert: Zeit in Minuten (60)
- Sitetyp: XenApp Web

ClientAddressMap

- Beschreibung: Gibt Paare von Clientadressen/-adresstypen für die serverseitige Firewallkonfiguration an. Das erste Feld des Eintrags ist eine Subnetzadresse und Maske, während das zweite Feld folgende Werte enthalten kann: "Normal", "Alternate", "Translated", "SG", "SGAlternate" und "SGTranslated". Ein Sternchen (*) anstelle einer Clientadresse oder eines Subnetzes gibt für alle ansonsten nicht festgelegten Citrix Clients die Standardeinstellung an.
- Wert: <*Subnetzadresse*>/ <*Subnetzmaske*> |*, Normal | Alternate | Translated | SG | SGTranslated | SGAlternate, …
- Sitetyp: XenApp Web

ClientDefaultURL

- Beschreibung: Gibt die URL an, an die der Clienterkennungs- und -bereitstellungsprozess Benutzer weiterleitet, wenn kein passender Client zum Download bereitsteht.
- Wert: http://www. citrix.com/ download. Gültige URL.
- Sitetyp: XenApp Web

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- Beschreibung: Konfiguriert den Clienterkennungs- und -bereitstellungsprozess für die angegebene Plattform. Wenn der entsprechende Parameter nicht konfiguriert wurde, werden Benutzer an die im Parameter "ClientDefaultURL" festgelegte Webseite weitergeleitet. Standardmäßig sind diese Parameter für die nativen Clients, die auf dem XenApp 6.0-Installationsmedium vorhanden sind, konfiguriert.

  In den ersten beiden Feldern werden der Speicherort und der Dateiname des Client-Installers angegeben. Wenn die Datei nicht gefunden wurde, werden Benutzer an die im Parameter ClientDefaultURL festgelegte Webseite weitergeleitet.

  Im Feld "Mui" wird festgelegt, ob der in den Feldern "Directory" und "Filename" angegebene Client mehrere Sprachen unterstützt. Wenn es auf "No" gesetzt ist, sucht der Clienterkennungs- und -bereitstellungsprozess im Ordner <*Sprachcode*>\<*Ordnername*> nach der angegebenen Datei.

  Das Feld "Version" enthält die kommagetrennte Versionsnummer des in den Feldern "Directory" und "Filename" angegebenen Clients. Wenn keine Versionsnummer angegeben ist, versucht der Clienterkennungs- und -bereitstellungsprozess, die Version aus der angegebenen Datei zu ermitteln.

  Das Feld "ShowEULA" gibt an, ob Benutzer die Citrix Lizenzvereinbarung annehmen müssen, um den angegebenen Client zu installieren.

  Das Feld "ClassID" gibt die Klassen-ID für Clients für Windows an und ist eine erforderliche Einstellung für diese Clients.

  Das Feld "Url" gibt die Webseite an, zu der Benutzer weitergeleitet werden, wenn Sie auf "Herunterladen" klicken und keine Clientdatei mit den Feldern "Directory" und "Filename" angegeben worden ist. Diese Einstellung sollte nur verwendet werden, wenn keine Clientdatei verfügbar ist.

  Im Feld "Description" können Sie eine eigene Meldung angeben, die über der Schaltfläche "Herunterladen" angezeigt wird. Dieser Text wird in der Sprache angezeigt, in der Sie ihn eingeben, und wird nicht automatisch lokalisiert.

- Wert: Directory: <*Ordnername*>, Filename: <*Dateiname*>, [Mui:Yes | No,] [Version: <*Versionsnummer*>,] [ShowEULA: Yes | No,] [ClassID: <*Wert*>,] [Url: <*GültigeURL*>,] [Description: <*Meldung*>]

- Sitetyp: XenApp Web

ClientProxy

- Beschreibung: Gibt eine Liste von Client-Subnetzadressen und -masken und zugehörige Proxyeinstellungen für eine clientseitige Firewall an. Die Clientadresse in der ausgegebenen ICA-Datei wird durch diese Einstellungen bestimmt. Jeder Eintrag besteht aus drei Feldern. Das erste Feld ist eine Subnetzadresse und -maske. Mit einem Sternchen (*) wird die Standardeinstellung für alle ansonsten nicht festgelegten Citrix Clients angegeben. Das zweite Feld enthält einen der sechs Proxytypen. Der Wert des dritten Feldes (Proxyadresse) in jedem Satz, standardmäßig das Minuszeichen (-), muss immer vorhanden sein, wird aber ignoriert, wenn nicht das zweite Feld (Proxytyp) ein expliziter Proxytyp (SOCKS oder Secure) ist.

- Wert: <*Subnetzadesses*>/ <*Subnetzmaske*> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <*Proxyadresse*> | <*Proxyadresse*>: <*Proxyport*>, …
- Sitetyp: XenApp Web und XenApp Services

CompactHeaderImage

- Beschreibung: Gibt die URL für das Kopfzeilenbild für die Benutzeroberflächenversion mit reduziertem Grafikinhalt an.
- Wert: Gültige URL
- Sitetyp: XenApp Web

CompactViewStyles

- Beschreibung: Gibt die Anzeigetypen an, die Benutzern auf der Seite "Anwendungen" der Benutzeroberfläche mit reduziertem Grafikinhalt zur Verfügung stehen.
- Wert: Icons, List
- Sitetyp: XenApp Web

CredentialFormat

- Beschreibung: Gibt die für explizite Windows- und NIS-Anmeldungen akzeptierten Formate für Anmeldeinformationen an.
- Wert: All | UPN | DomainUsername
- Sitetyp: XenApp Web und XenApp Services

CSG_EnableSessionReliability

- Beschreibung: Gibt an, ob Sitzungszuverlässigkeit mit Access Gateway oder Secure Gateway verwendet werden soll.
- Wert: On | Off
- Sitetyp: XenApp Web und XenApp Services

CSG_Server

- Beschreibung: Gibt die Adresse des Access Gateway-Geräts oder des Secure Gateway-Servers an.
- Wert: None Serveradresse als FQDN.
- Sitetyp: XenApp Web und XenApp Services

CSG_ServerPort

- Beschreibung: Gibt den Port des Access Gateway-Geräts oder des Secure Gateway-Servers an.
- Wert: None Serverport.

- Sitetyp: XenApp Web und XenApp Services

CSG_STA_URL<*n*>

- Beschreibung: Gibt die URL des Servers an, auf dem die Secure Ticket Authority für das Gateway-Gerät ausgeführt wird.
- Wert: None URL einer Secure Ticket Authority.
- Sitetyp: XenApp Web und XenApp Services

CSG_UseTwoTickets

- Beschreibung: Gibt an, ob das Webinterface Tickets von zwei verschiedenen Secure Ticket Authority anfordert, wenn auf eine Ressource über Access Gateway zugegriffen wird.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

DefaultAudioQuality

- Beschreibung: Gibt die Standard-Audioqualität für ICA-Verbindungen an.
- Wert: NoPreference | High | Medium | Low | Off
- Sitetyp: XenApp Web

DefaultBandwidthProfile

- Beschreibung: Gibt das Standard-Bandbreitenprofil für ICA-Verbindungen an (d. h. die Sammlung von Einstellungen, die die Bandbreite betreffen, wie z. B. Audioqualität und Farbtiefe).
- Wert: Custom | High | Medium High | Medium | Low
- Sitetyp: XenApp Web

DefaultColorDepth

- Beschreibung: Gibt die Standard-Farbtiefe für ICA-Verbindungen an.
- Wert: NoPreference | TrueColor | High Color
- Sitetyp: XenApp Web

DefaultCompactViewStyle

- Beschreibung: Gibt den Standardanzeigetyp für die Seite "Anwendungen" der Benutzeroberfläche mit reduziertem Grafikinhalt an.
- Wert: List | Icons
- Sitetyp: XenApp Web

DefaultCustomTextLocale

- Beschreibung: Gibt das Standard-Gebietseingabeschema für benutzerdefinierten Text an. Für alle benutzerdefinierten Textparameter (*_<*Sprachcode*>) muss dasselbe Gebietseingabeschema angegeben werden.
- Wert: Kein Wert. en | de | es | fr | ja | Kennung für andere unterstützte Sprachen.
- Sitetyp: XenApp Web

DefaultPrinterMapping

- Beschreibung: Gibt an, ob Druckerzuordnung für ICA-Verbindungen standardmäßig aktiviert ist.
- Wert: On | Off
- Sitetyp: XenApp Web

DefaultViewStyle

- Beschreibung: Gibt den Standardanzeigetyp für die Seite "Anwendungen" der Benutzeroberfläche mit komplettem Grafikinhalt an.
- Wert: Icons | Details | Groups | List | Tree
- Sitetyp: XenApp Web

DefaultWindowSize

- Beschreibung: Gibt den Standard-Fenstermodus für ICA-Sitzungen an. Dies kann als Prozentwert des Gesamtbildschirms im Format X % oder als feste Größe mit individuellen Maßen im Format XxY angegeben werden.
- Wert: FullScreen | Seamless | X% | XxY
- Sitetyp: XenApp Web

DisplayBrandingImage

- Beschreibung: Gibt an, ob die Brandinggrafik in den Kopf- und Fußzeilenbereichen angezeigt wird.
- Wert: On | Off
- Sitetyp: XenApp Web

DomainSelection

- Beschreibung: Gibt die auf der Anmeldeseite für explizite Authentifizierung genannten Domänennamen an.
- Wert: Liste von NetBios-Domänennamen
- Sitetyp: XenApp Web und XenApp Services

DuplicateLogInterval

- Beschreibung: Gibt an, für welche Dauer Protokolleinträge von "DuplicateLogLimit" überwacht werden.
- Wert: Zeit in Sekunden (60)
- Sitetyp: XenApp Web und XenApp Services

DuplicateLogLimit

- Beschreibung: Gibt an, wie viele doppelte Protokolleinträge während der in "DuplicateLogInterval" festgelegten Dauer zulässig sind.
- Wert: Ganzzahl größer als 0 (10)
- Sitetyp: XenApp Web und XenApp Services

EnableFileTypeAssociation

- Beschreibung: Gibt an, ob die Dateitypverknüpfung für eine Site aktiviert ist. Wenn dieser Parameter deaktiviert ist, steht die Inhaltsumleitung für die Site nicht zur Verfügung.
- Wert: On | Off
- Sitetyp: XenApp Web und XenApp Services

EnableKerberosToMPS

- Beschreibung: Gibt an, ob Kerberos-Authentifizierung aktiviert ist.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

EnableLegacyICAClientSupport

- Beschreibung: Gibt an, ob ältere Citrix Clients, die ICA-Dateien im UTF-8-Format nicht lesen können, unterstützt werden. Wenn dieser Parameter deaktiviert ist (Wert = Off), erstellt Presentation Server ICA-Dateien in UTF-8-Codierung.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

EnableLogoffApplications

- Beschreibung: Gibt an, ob Workspace Control aktive Ressourcen abmeldet, wenn sich der Benutzer vom Server abmeldet.
- Wert: On | Off
- Sitetyp: XenApp Web

EnablePassthroughURLs

- Beschreibung: Gibt an, ob Benutzer dauerhafte Links zu Ressourcen erstellen können, auf die mit dem Webinterface zugegriffen wird.
- Wert: Off | On
- Sitetyp: XenApp Web

EnableRadiusServerLoadBalancing

- Beschreibung: Gibt an, ob bei Sitzungen auf den konfigurierten RADIUS-Servern Lastausgleich stattfindet. Unabhängig von der gewählten Einstellung für diesen Parameter findet immer noch Failover zwischen den Servern statt.
- Wert: Off | On
- Sitetyp: XenApp Web

EnableSTALoadBalancing

- Beschreibung: Gibt an, ob bei Anfragen zwischen den konfigurierten Secure Ticket Authority-Servern eines Gateway-Geräts Lastausgleich stattfindet.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

EnableVirtualCOMPortEmulation

- Beschreibung: Gibt an, ob die PDA-Synchronisierung über direkte USB-Verbindungen aktiviert wird.
- Wert: Off | On
- Sitetyp: XenApp Web

EnableWizardAutoMode

- Beschreibung: Gibt an, ob der Clienterkennungs- und -bereitstellungsprozess im automatischen Modus ausgeführt wird.
- Wert: On | Off
- Sitetyp: XenApp Web

EnableWorkspaceControl

- Beschreibung: Gibt an, ob Workspace Control für Benutzer verfügbar ist.
- Wert: On | Off
- Sitetyp: XenApp Web

ErrorCallbackURL

- Beschreibung: Gibt eine URL für das Webinterface zum Weiterleiten bei einem Fehler an. Die Webseite, auf die die URL verweist, muss vier Abfrageparameter annehmen und

verarbeiten:

CTX_MessageType

CTX_MessageKey

CTX_MessageArgs

CTX_LogEventID

- Wert: Gültige URL
- Sitetyp: XenApp Web

Farm<*n*>

- Beschreibung: Gibt alle Informationen zu einer Farm an. Es können maximal 512 Farmen konfiguriert werden.
- Wert: Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Name*>] [,XMLPort: <*Port*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Port*>] [,Bypass Duration: <*Zeit in Minuten* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*Zeit in Sekunden* (200)>] [,RADETicket TimeToLive: <*Zeit in Sekunden* (200)>]
- Sitetyp: XenApp Web und XenApp Services

Farm<*n*>Groups

- Beschreibung: Gibt die Active Directory-Gruppen an, die Ressourcen von Serverfarmen auflisten dürfen. Wenn dieser Parameter angegeben wird, wird das Benutzerroaming aktiviert. Für jede Fam können mit dem Parameter Farm<*n*> maximal 512 Benutzergruppen angegeben werden.
- Wert: None *Domäne*\ *Benutzergruppe*[,...]
- Sitetyp: XenApp Web, XenApp Services und XenDesktop

FooterText _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Fußzeilentext an, der im Fußzeilenbereich aller Seiten angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

HeaderFontColor

- Beschreibung: Gibt die Schriftfarbe für die Kopfzeile an.
- Wert: Hexadezimale Farbnummer oder Farbname
- Sitetyp: XenApp Web

HeadingHomePage

- Beschreibung: Gibt die URL für die Grafik an, die als Überschrift auf der Homepage angezeigt wird.
- Wert: Gültige URL
- Sitetyp: XenApp Web

HeadingImage

- Beschreibung: Gibt die URL für die Grafik an, die als Überschrift des Webinterface angezeigt wird.
- Wert: Gültige URL
- Sitetyp: XenApp Web

HideDomainField

- Beschreibung: Gibt an, ob das Domänenfeld auf der Anmeldeseite angezeigt wird.
- Wert: Off | On
- Sitetyp: XenApp Web

IcaFileSigningCertificateThumbprint

- Beschreibung: Der Fingerabdruck des Zertifikats, das zum Signieren von ICA-Dateien verwendet wird.
- Wert: None Fingerabdruck, der Leerzeichen enthalten kann.
- Sitetyp: XenApp Web und Desktop Appliance Connector

IcaFileSigningEnabled

- Beschreibung: Aktiviert oder deaktiviert das Feature zum Signieren von ICA-Dateien.
- Wert: Off | On
- Sitetyp: XenApp Web und Desktop Appliance Connector

IcaFileSigningHashAlgorithm

- Beschreibung: Der Hash-Algorithmus, der zum Signieren von ICA-Dateien verwendet wird.
- Wert: SHA1 | SHA256
- Sitetyp: XenApp Web und Desktop Appliance Connector

IgnoreClientProvidedClientAddress

- Beschreibung: Gibt an, ob die vom Citrix Client übergebene Adresse ignoriert werden soll.

- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

InternalServerAddressMap

- Beschreibung: Gibt Paare aus normalen und übersetzten Adressen an. Die normale Adresse identifiziert den Server, mit dem das Gateway kommuniziert, und die übersetzte Adresse wird an den Citrix Client zurückgegeben.
- Wert: NormalAddress = Translated Address, …
- Sitetyp: XenApp Web und XenApp Services

JavaClientPackages

- Beschreibung: Gibt den Standardsatz der Pakete für den Client für Java an, die Benutzern zur Verfügung stehen.
- Wert: ClipBoard, ConfigUI, PrinterMapping, SecureICA, SSL, Audio, ClientDrive Mapping, ZeroLatency
- Sitetyp: XenApp Web

JavaFallbackMode

- Beschreibung: Gibt an, ob Fallback auf den Client für Java stattfinden soll, wenn Benutzer keinen nativen Client installiert haben. Dieser Parameter gilt nur, wenn für den Parameter "LaunchClients" der Wert "Ica-Local" angegeben ist. Mit der Einstellung "Manual" können Benutzer wählen, ob sie den Client für Java verwenden möchten.
- Wert: None | Manual | Auto
- Sitetyp: XenApp Web

KioskMode

- Beschreibung: Gibt an, ob Benutzereinstellungen beibehalten werden oder nur für die Dauer der Sitzung bestehen. Bei aktiviertem Kioskmodus werden Benutzereinstellungen nach jeder Sitzung zurückgesetzt.
- Wert: Off | On
- Sitetyp: XenApp Web

LaunchClients

- Beschreibung: Gibt an, aus welchen Citrix Clients Benutzer auswählen können. Dieser Parameter wird für Dual Mode-Sites ignoriert. Für diese Sites gilt immer die Einstellung "Ica-Local". Auch wenn die Einstellung "Ica-Java" nicht verwendet wird, wird Benutzern der Client für Java angeboten. Um dies zu verhindern, müssen Sie auch den Parameter "JavaFallbackMode" auf "None" setzen.
- Wert: Ica-Local, Ica-Java, Rdp-Embedded
- Sitetyp: XenApp Web

LoginDomains

- Beschreibung: Gibt die für die Zugriffsbeschränkung verwendeten Domänennamen an.
- Wert: Liste von NetBios-Domänennamen
- Sitetyp: XenApp Web und XenApp Services

LoginSys Message _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Text an, der unten im Hauptinhaltsbereich der Seite "Anmeldung" angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

LoginTitle _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Text an, der über der Begrüßungsmeldung auf der Seite "Anmeldung" angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

LoginType

- Beschreibung: Gibt den Anmeldeseitentyp an, der Benutzern angezeigt wird. Die Anmeldeseite kann domänenbasiert oder NDS-basiert sein.
- Wert: Default | NDS
- Sitetyp: XenApp Web und XenApp Services

LogoffFederationService

- Beschreibung: Gibt an, ob Benutzer nur von XenApp Web-Sites oder global vom Verbunddienst abgemeldet werden sollen, wenn bei einer Site mit ADFS auf die Schaltfläche "Abmelden" geklickt wird.
- Wert: On | Off
- Sitetyp: XenApp Web

MultiFarmAuthenticationMode

- Beschreibung: Dieser Modus hat drei Optionen, um die zulässige Authentifizierungsmethode festzulegen. Die Option "All" ist die Standardeinstellung, bei der alle Farmen zum Enumerieren aller Anwendungen authentifiziert sind. Die Option "Any" ermöglicht die Enumeration von Anwendungen jeder Farm für den authentifizierten Benutzer. Wenn der Benutzer jedoch die falschen

Anmeldeinformationen eingibt, werden die falschen Anmeldeinformationen jeder Farm zur Authentifizierung präsentiert, ungeachtet der fehlgeschlagenen Authentifizierung bei den anderen Farmen. Dies kann zur Sperrung des Kontos führen. Die Option "Primary" erlaubt die Authentifizierung des Benutzers bei der primären Farm (die erste Farm auf der Liste der für Webinterface konfigurierten Farmen). Danach wird wieder der Modus "Any" ausgeführt. Mit dieser Option wird eine Sperrung von Konten verhindert.

- Wert: All | Any | Primary
- Sitetyp: XenApp Web

MultiLaunchTimeout

- Beschreibung: Gibt die Zeit an, während der Ressourcensymbole inaktiv sind, nachdem ein Benutzer zum ersten Mal darauf geklickt hat, um die Ressource zu starten.
- Wert: Zeit in Sekunden (2)
- Sitetyp: XenApp Web

NDSContextLookupLoadbalancing

- Beschreibung: Gibt an, ob bei NDS-Anfragen auf den konfigurierten LDAP-Servern Lastausgleich stattfindet. Unabhängig von der gewählten Einstellung für diesen Parameter findet immer noch Failover zwischen den Servern statt.
- Wert: Off | On
- Sitetyp: XenApp Web

NDSContextLookupServers

- Beschreibung: Gibt an, welche LDAP-Server verwendet werden sollen. Wenn der Port nicht angegeben ist, wird er anhand des Protokolls ermittelt: wenn dieser Parameter auf "ldap" gesetzt ist, wird der Standard-LDAP-Port (389) verwendet; wenn die Einstellung "ldaps" ist, wird der Standard-LDAP-über-SSL-Port (636) verwendet. Es können maximal 512 LDAP-Server konfiguriert werden.

  Wenn dieser Parameter nicht definiert oder nicht vorhanden ist, wird die kontextlose Anmeldefunktion deaktiviert.
- Wert: None. ldap://[:] | ldaps://[:],
- Sitetyp: XenApp Web

NDSTreeName

- Beschreibung: Gibt bei NDS-Authentifizierung die zu verwendende NDS-Struktur an.
- Wert: None Name der NDS-Struktur.
- Sitetyp: XenApp Web und XenApp Services

OverlayAutologonCredsWithTicket

- Beschreibung: Gibt an, ob ein Anmeldeticket in einem Anmeldeticketeintrag dupliziert oder nur in einem separaten Ticketeintrag der ICA-Startdatei eingefügt werden muss. Wenn Überlagerung von Anmeldeinformationen aktiviert ist, werden Anmeldetickets dupliziert.
- Wert: On | Off
- Sitetyp: XenApp Web

OverrideIcaClientname

- Beschreibung: Gibt an, ob eine vom Webinterface erstellte ID in den Clientnameneintrag einer ICA-Startdatei weitergeleitet werden muss.
- Wert: Off | On
- Sitetyp: XenApp Web

PasswordExpiryWarningPeriod

- Beschreibung: Gibt die Anzahl von Tagen an, bevor ein Kennwort abläuft und Benutzer zur Änderung des Kennworts aufgefordert werden.
- Wert: Ganzzahl zwischen 0 und 999 (14)
- Sitetyp: XenApp Web

PersistFolderLocation

- Beschreibung: Gibt an, ob Benutzer, wenn sie sich das nächste Mal anmelden, zu dem Ordner zurückkehren, mit dem sie auf der Seite "Anwendungen" zuletzt gearbeitet haben.
- Wert: Off | On
- Sitetyp: XenApp Web

PNAChangePasswordMethod

- Beschreibung: Gibt an, wie das Citrix Online Plug-In Anfragen von Benutzern zum Ändern von Kennwörtern verarbeitet. Wenn dieser Parameter auf "Direct-Only" gesetzt ist, ändert das Plug-In das Kennwort, indem er direkt mit dem Domänencontroller Daten austauscht. "Direct-With-Fallback" gibt an, dass das Plug-In erst versucht, Kontakt zum Domänencontroller herzustellen, und dann die XenApp Services-Site verwendet, wenn dies fehlschlägt. Die Option "Proxy" gibt an, dass das Plug-In Kennwörter über die XenApp Services-Site ändert.
- Wert: Direct-Only | Direct-With- Fallback | Proxy
- Sitetyp: XenApp Services

PooledSockets

- Beschreibung: Gibt die Verwendung von Socket-Pooling an.
- Wert: On | Off

- Sitetyp: XenApp Web und XenApp Services

PreLoginMessageButton _<*Sprachcode*>

- Beschreibung: Gibt einen lokalisierten Namen für die Bestätigungsschaltfläche für die Meldung vor der Anmeldung an. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.

- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.

- Sitetyp: XenApp Web

PreLoginMessageText _<*Sprachcode*>

- Beschreibung: Gibt lokalisierten Text an, der auf der Seite "Vor der Anmeldung" angezeigt werden soll. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.

- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.

- Sitetyp: XenApp Web

PreLoginMessageTitle _<*Sprachcode*>

- Beschreibung: Gibt einen lokalisierten Titel für die Seite "Vor der Anmeldung" an. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.

- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.

- Sitetyp: XenApp Web

RADERequestValidation

- Beschreibung: Gibt an, ob bei einkommenden Anfragen vom Citrix Offline Plug-In Textüberprüfung durchgeführt werden soll.

- Wert:

- Sitetyp: XenApp Web und XenApp Services

RADESessionURL

- Beschreibung: Gibt die URL für die RADE-Sitzungsseite an. Wenn dieser Parameter auf "auto" gesetzt ist, wird die URL automatisch erstellt.

- Wert: Auto. Gültige URL.

- Sitetyp: XenApp Web und XenApp Services

RadiusRequestTimeout

- Beschreibung: Gibt das Zeitlimit für das Warten auf eine Antwort vom RADIUS-Server der Sitzung an.

- Wert: Zeit in Sekunden (30)
- Sitetyp: XenApp Web

RadiusServers

- Beschreibung: Gibt die zu verwendenden RADIUS-Server und falls gewünscht die Ports an, die sie abhören. Server können durch IP-Adressen oder Namen angegeben werden. Server und Port für jedes Element sind durch einen Doppelpunkt getrennt. Wenn der Port nicht angegeben ist, wird der Standard-RADIUS-Port (1812) angenommen. Es können maximal 512 Server konfiguriert werden.
- Wert: *Server* [:*Port*] [,…]
- Sitetyp: XenApp Web

ReconnectAtLogin

- Beschreibung: Gibt an, ob Workspace Control bei der Benutzeranmeldung erneut eine Verbindung zu Ressourcen herstellen soll, und falls ja, ob die Verbindung zu allen oder nur zu getrennten Ressourcen wiederhergestellt werden soll.
- Wert: Disconnected AndActive | Disconnected | None
- Sitetyp: XenApp Web

ReconnectButton

- Beschreibung: Gibt an, ob Workspace Control erneut eine Verbindung zu Anwendungen herstellen soll, wenn Benutzer auf die Schaltfläche "Wiederverbinden" klicken, und falls ja, ob die Verbindung zu allen oder nur zu getrennten Ressourcen wiederhergestellt werden soll.
- Wert: Disconnected AndActive | Disconnected | None
- Sitetyp: XenApp Web

RecoveryFarm<*n*>

- Beschreibung: Gibt alle Informationen zu einer Farm für die Wiederherstellung im Notfall an. Es können maximal 512 Farmen konfiguriert werden.
- Wert: Citrix XML Service address [,Citrix XML Service address,] [,Name:<*Name*>] [,XMLPort: <*Port*>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <*Port*>] [,Bypass Duration: <*Zeit in Minuten* (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <*Zeit in Sekunden* (200)>] [,RADETicket TimeToLive: <*Zeit in Sekunden* (200)>]
- Sitetyp: XenApp Web, XenApp Services und XenDesktop

RequestedHighColorIcons

- Beschreibung: Gibt an, ob vom Citrix XML-Dienst 32-Bit-Symbole mit hoher Farbtiefe angefordert werden, und falls ja, listet die Symbolgrößen in Pixeln auf. Wenn dieser Parameter auf "None" gesetzt ist, werden nur Standardsymbole (4-Bit, 32 x 32) angefordert. Die Standardeinstellung variiert je nach Sitetyp und Konfiguration.

- Wert: 16, 32, 48 | None

  Die Standardeinstellung für XenApp Services-Sites ist es, alle Symbole anzufordern. Für XenApp Web-Sites werden standardmäßig nur die Größen 16 x 16 und 32 x 32 angefordert.

- Sitetyp: XenApp Web und XenApp Services

RequestICAClientSecureChannel

- Beschreibung: Gibt TLS-Einstellungen an.

- Wert: Detect-Any Ciphers, TLS- GovCiphers, SSL-AnyCiphers

- Sitetyp: XenApp Web und XenApp Services

RequireLaunchReference

- Beschreibung: Gibt an, ob die Verwendung von Startverweisen erzwungen werden soll. Für die Passthrough-Authentifizierung zu XenApp VM Hosted Apps sind Startverweise erforderlich. Wenn Kompatibilität mit XenApp 4.0, mit Feature Pack 1, für UNIX erforderlich ist, muss dieser Parameter auf "Off" gesetzt sein.

- Wert: On | Off

- Sitetyp: XenApp Web und XenApp Services

RestrictDomains

- Beschreibung: Gibt an, ob der Parameter "LoginDomains" zum Einschränken des Benutzerzugriffs verwendet wird.

- Wert: Off | On

- Sitetyp: XenApp Web und XenApp Services

SearchContextList

- Beschreibung: Gibt Kontextnamen zur Verwendung bei der NDS-Authentifizierung an.

- Wert: None Durch Komma getrennte Liste der Kontextnamen.

- Sitetyp: XenApp Web und XenApp Services

ServerAddressMap

- Beschreibung: Gibt Paare aus normalen und übersetzten Adressen für die serverseitige Firewallkonfiguration an. Die normale Adresse bezeichnet den Server und die übersetzte Adresse wird an den Citrix Client zurückgegeben.

- Wert: NormalAddress, Translated Address, …

- Sitetyp: XenApp Web und XenApp Services

ServerCommunicationAttempts

- Beschreibung: Gibt an, wie oft eine Anforderung an den Citrix XML-Dienst versucht wird, bevor angenommen wird, dass der Dienst nicht erreichbar ist.
- Wert: Ganzzahl größer als 0 (2)
- Sitetyp: XenApp Web und XenApp Services

ShowClientInstallCaption

- Beschreibung: Gibt an, wie und wann Installationsmeldungen angezeigt werden. Wenn dieser Parameter auf "Auto" gesetzt ist, werden Installationsmeldungen angezeigt, wenn Benutzer kein Citrix Client installiert haben oder wenn ein besserer Client verfügbar ist. Wenn der Parameter auf "Quiet" gesetzt ist, werden Installationsmeldungen nur angezeigt, wenn Benutzer keinen Client installiert haben. Das Verhalten der Anmeldeseite ist insofern etwas anders, dass Meldungen nur für Clients für Onlineressourcen und nur dann, wenn kein Client erkannt wurde, angezeigt werden. Es besteht also für die Anmeldeseite kein Unterschied zwischen den Einstellungen "Auto" und "Quiet".
- Wert: Auto | Quiet | Off
- Sitetyp: XenApp Web

ShowDesktopViewer

- Beschreibung: Gibt an, ob das Fenster und die Symbolleiste von Citrix Desktop Viewer standardmäßig aktiviert sind, wenn Benutzer auf ihre Desktops zugreifen.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

ShowHints

- Beschreibung: Gibt an, ob auf der Anwendungsseite Tipps angezeigt werden.
- Wert: On | Off
- Sitetyp: XenApp Web

ShowPasswordExpiryWarning

- Beschreibung: Gibt die Bedingungen an, in denen Benutzern eine Warnung über ablaufende Kennwörter angezeigt wird.
- Wert: Never | WindowsPolicy | Custom
- Sitetyp: XenApp Web

ShowRefresh

- Beschreibung: Gibt an, ob Benutzer die Schaltfläche "Aktualisieren" auf der Seite "Anwendungen" sehen.
- Wert: Off | On

- Sitetyp: XenApp Web

ShowSearch

- Beschreibung: Gibt an, ob Benutzer die Suchfunktion auf der Seite "Anwendungen" sehen.
- Wert: On | Off
- Sitetyp: XenApp Web

SpecialFolderRedirection

- Beschreibung: Gibt an, ob die Umleitung spezieller Ordner aktiviert ist. Wenn dieser Parameter auf "On" gesetzt ist, verwenden Ressourcen die Ordner \Dokumente und \Desktop auf den lokalen Computern der Benutzer. Wird der Parameter auf "Off" gesetzt, werden für die Ordner, die in Anwendungen zur Verfügung stehen, diejenigen auf dem Server verwendet.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

SuppressDuplicateResources

- Beschreibung: Gibt an, ob Ressourcen mit identischen Namen und Speicherorten, die in unterschiedlichen Farmen veröffentlicht sind, verborgen werden sollen.
- Wert: Off | On
- Sitetyp: XenApp Web und XenApp Services

Timeout

- Beschreibung: Gibt das Zeitlimit an, das bei der Kommunikation mit dem Citrix XML-Dienst verwendet werden soll.
- Wert: Zeit in Sekunden (60)
- Sitetyp: XenApp Web und XenApp Services

TransparentKeyPassthrough

- Beschreibung: Gibt den Passthrough-Modus für Windows-Tastenkombinationen an.
- Wert: FullScreen Only | Local | Remote
- Sitetyp: XenApp Web und XenApp Services

TwoFactorPasswordIntegration

- Beschreibung: Gibt an, ob die Kennwortintegration mit RSA SecurID 6.0 aktiviert wird.
- Wert: Off | On
- Sitetyp: XenApp Web

TwoFactorUseFullyQualifiedUserNames

- Beschreibung: Gibt an, ob bei der Zweifaktorauthentifizierung vollqualifizierte Benutzernamen an den Authentifizierungsserver übertragen werden.
- Wert: Off | On
- Sitetyp: XenApp Web

UpgradeClientsAtLogin

- Beschreibung: Gibt an, ob der Clienterkennungs- und -bereitstellungsprozess im automatischen Modus ausgeführt wird, wenn Benutzer sich anmelden und eine aktuellere Version des nativen Clients oder des Citrix Offline Plug-Ins verfügbar ist. Dieser Parameter gilt nur, wenn "EnableWizardAutoMode" auf "On" gesetzt ist.
- Wert: Off | On
- Sitetyp: XenApp Web

UPNSuffixes

- Beschreibung: Gibt Suffixe an, bei denen nur explizite UPN-Authentifizierung möglich ist.
- Wert: Liste von UPN-Suffixen
- Sitetyp: XenApp Web und XenApp Services

UserInterfaceBranding

- Beschreibung: Gibt an, ob die Site für Benutzer, die auf Anwendungen, oder solche, die auf Desktops zugreifen, eingerichtet wurde. Wenn Sie diesen Parameter auf "Desktops" setzen, wird die Funktionalität geändert, um die Erfahrung für XenDesktop-Benutzer zu verbessern. Citrix empfiehlt, diese Einstellung für Bereitstellungen mit XenDesktop zu verwenden.
- Wert: Applications | Desktops
- Sitetyp: XenApp Web

UserInterfaceLayout

- Beschreibung: Gibt an, ob die kompakte Benutzeroberfläche verwendet werden soll.
- Wert: Auto | Normal | Compact
- Sitetyp: XenApp Web

UserInterfaceMode

- Beschreibung: Gibt die Darstellung der Anmeldeseite an. Wenn dieser Parameter auf "Simple" gesetzt ist, werden nur die Anmeldefelder für die ausgewählte Authentifizierungsmethode angezeigt. Wird der Parameter auf "Advanced" gesetzt, wird die Navigationsleiste angezeigt, die Zugriff auf die Seiten "Meldungen" und "Einstellungen" ermöglicht.

- Wert: Simple | Advanced
- Sitetyp: XenApp Web

ViewStyles

- Beschreibung: Gibt die Anzeigetypen an, die Benutzern auf der Seite "Anwendungen" der Benutzeroberfläche mit komplettem Grafikinhalt zur Verfügung stehen.
- Wert: Details | Groups | Icons | List | Tree
- Sitetyp: XenApp Web

WebSessionTimeout

- Beschreibung: Gibt das Zeitlimit für inaktive Browsersitzungen an.
- Wert: Zeit in Minuten (20)
- Sitetyp: XenApp Web

Welcome Message _<*Sprachcode*>

- Beschreibung: Gibt den lokalisierten Text für die Meldung an, die im Willkommensbereich auf der Anmeldeseite angezeigt wird. *Sprachcode* ist en, de, es, fr, ja oder ein anderer unterstützter Sprachcode.
- Wert: None Nur Text plus eine beliebige Anzahl des HTML-Tags
 für neue Zeilen und Hyperlinks.
- Sitetyp: XenApp Web

WIAuthenticationMethods

- Beschreibung: Gibt die zulässigen Authentifizierungsmethoden für Sites an, die nicht in Access Gateway integriert sind. Dies ist eine kommagetrennte Liste und kann folgende Werte in beliebiger Reihenfolge enthalten.
- Wert: Beliebige Kombination von: Explicit, Anonymous, Certificate SingleSignOn, Certificate, SingleSignOn
- Sitetyp: XenApp Web, XenApp Services und Desktop Appliance Connector

Inhalt der Datei config.xml

Aktualisiert: 2014-12-02

Die Datei config.xml enthält einige Parameter, die in verschiedene Kategorien unterteilt sind. Sie können Parameter in den folgenden Kategorien bearbeiten:

- FolderDisplay: Gibt an, wo Symbole für Ressourcen angezeigt werden: im Startmenü, auf dem Windows-Desktop oder im Infobereich. Es gibt einen zusätzlichen Parameter, mit dem Sie einen bestimmten Ordner im Startmenü angeben können. Diese Parameter entsprechen den Steuerelementen auf der Seite Anwendungsanzeige im Dialogfeld Optionen des Citrix Online Plug-Ins.
- DesktopIntegration: Gibt an, ob im Startmenü, auf dem Desktop oder im Infobereich Verknüpfungen hinzugefügt werden sollen.
- ConfigurationFile: Gibt eine andere URL für die Datei config.xml an, die das Plug-In in Zukunft verwenden soll. Dies vereinfacht ein Verlagern der Benutzer auf einen anderen Webinterface-Server.
- Request: Gibt an, von welcher Stelle das Plug-In die Ressourcendaten anfordert und wie oft die Informationen aktualisiert werden.
- Failover: Gibt eine Liste von URLs von Backup-Servern an, die kontaktiert werden sollen, wenn der primäre Server nicht verfügbar ist.
- Anmeldung: Gibt die zu verwendende Anmeldemethode an.
- ChangePassword: Gibt an, in welchen Situationen Citrix Online Plug-In-Benutzer ihre Kennwörter ändern dürfen, sowie den Pfad, über den solche Anfragen geleitet werden.
- UserInterface: Gibt an, ob bestimmte Optionen der Citrix Online Plug-In-Benutzeroberfläche für Benutzer ein- oder ausgeblendet werden.
- ReconnectOptions: Gibt an, ob Workspace Control für Benutzer zur Verfügung steht.
- FileCleanup: Gibt an, ob Verknüpfungen gelöscht werden, wenn Benutzer sich vom Citrix Online Plug-In abmelden.
- ICA_Options: Gibt die Anzeige- und Audiooptionen für Plug-In-Verbindungen an. Dies entspricht den Einstellungen auf der Seite Sitzungsoptionen im Dialogfeld Optionen des Citrix Online Plug-Ins.
- AppAccess: Gibt die Ressourcentypen an, die Benutzern zur Verfügung stehen.

Weitere Informationen zur Verwendung der Datei config.xml finden Sie unter Online Plug-In für Windows.

Überlegungen zum Citrix Online Plug-In

Bestimmte Parametereinstellungen in der Datei WebInterface.conf wirken sich auf die Überprüfung von Citrix Online Plugin-Anfragen aus. Citrix empfiehlt, die Einstellungen in der Datei WebInterface.conf mit den Einstellungen der Datei config.xml für das Citrix Online Plug-In abzugleichen.

Einstellungen in der Datei WebInterface.conf

Die folgende Tabelle enthält die Parameter in der Datei WebInterface.conf, die mit den Parametern in der Datei config.xml übereinstimmen müssen. Sie enthält außerdem Erläuterungen der Parameter, die sich auf das Citrix Online Plug-In sowie die empfohlenen Einstellungen auswirken.

Parameter	Empfohlene Einstellung
LoginType	Wenn dies auf "NDS" gesetzt ist, muss auch Novell-Authentifizierung in config.xml aktiviert sein.
NDSTreeName	Der Parameter DefaultTree im Abschnitt Logon der Datei config.xml muss dieselbe Einstellung haben.
PNAChangePasswordMethod	Der Parameter "Method" im Abschnitt "ChangePassword" der Datei config.xml muss dieselbe Einstellung haben.
WIAuthenticationMethods	Verwenden Sie dieselbe Authentifizierungsmethode, die in der Datei WebInterface.conf festgelegt ist. Die Authentifizierung schlägt fehl, wenn sich diese Methode von der in config.xml unterscheidet.

So konfigurieren Sie das Webinterface bei Verwendung des Citrix Online Plug-Ins

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor.
2. Suchen Sie die folgenden Parameter:
   - LoginType
   - NDSTreeName
   - PNAChangePasswordMethod
   - WIAuthenticationMethods
3. Ändern Sie die Einstellungen dieser Parameter wie unter Inhalt der Datei config.xml beschrieben.
4. Starten Sie den Webinterface-Server neu, um die Änderungen zu übernehmen.

Weitere Informationen zu den Einstellungen in der Datei WebInterface.conf finden Sie unter WebInterface.conf-Parameter.

Einstellungen in der Datei bootstrap.conf

Die folgende Tabelle enthält eine Liste der in der Datei bootstrap.conf enthaltenen Einstellungen.

Parameter	Beschreibung	Werte	Sitetypen
ConfigurationLocation	Gibt die Datei an, von der die Webinterface-Site ihre Konfiguration erhalten soll. Dies kann eine lokale Datei, für in IIS gehostete Sites, oder eine Remotedatei sein, die über das Netzwerk gemeinsam verwendet werden kann.	Absoluter Pfad zur WebInterface -CONF-Datei	XenApp Web XenApp Services
DefaultLocale	Gibt die Standardsprache an, die verwendet werden soll, wenn ein Browser eine nicht unterstützte Sprache anfordert.	en | de | es | fr | ja | Kennung für andere unterstützte Sprachen	XenApp Web XenApp Services
SiteName	Gibt den Namen der Site an, der in der Citrix Webinterface Management Console angezeigt wird. Als Standardeinstellung wird die URL der Site verwendet.	Gültige Zeichenfolge	XenApp Web XenApp Services

So konfigurieren Sie Unterstützung für XenApp 4.0, mit Feature Pack 1, für UNIX

In diesem Beispiel soll eine Site so konfiguriert werden, dass sie mit XenApp 4.0, mit Feature Pack 1, für UNIX kompatibel ist. Neue Webinterface-Sites sind nicht von Anfang an mit diesem Produkt kompatibel; es ist ein zusätzlicher manueller Konfigurationsschritt erforderlich.

1. Öffnen Sie die Datei WebInterface.conf mit einem Texteditor und suchen Sie die folgenden Zeilen:

   OverrideIcaClientname=Off

   RequireLaunchReference=On

2. Ändern Sie die Einstellungen wie im Folgenden angegeben:

   OverrideIcaClientname=On

   RequireLaunchReference=Off

   Hinweis: Wenn der Parameter RequireLaunchReference auf Off gesetzt ist, ist die Passthrough-Authentifizierung für XenApp VM Hosted Apps deaktiviert. Benutzer dieser Site müssen ihre Anmeldeinformationen jedes Mal eingeben, wenn sie auf eine mit VM Hosted Apps veröffentlichte Anwendung zugreifen.

So konfigurieren Sie Benutzerroaming

In diesem Beispiel möchten Sie die Benutzergruppen in der US-Niederlassung Ihres Unternehmens mit bestimmten Serverfarmen verknüpfen, damit sich die Benutzer bei einem Besuch in der japanischen Niederlassung an einem lokalen Webinterface-Server anmelden können und automatisch Ressourcen in englischer Sprache von einer Farm in den USA erhalten.

Eine vorhandene Farm, auf der der Citrix XML-Dienst auf dem Server "Walzer" ausgeführt wird, ist bereits als Farm1 in der Konfigurationsdatei definiert und steht für alle Benutzer zur Verfügung, die sich an dem US-Webinterface-Server anmelden. Die Benutzergruppe "Vertrieb" ist in der Domäne "US-Vertrieb.Unternehmen.com" und die Benutzergruppe "Buchhaltung" ist in der Domäne "Buchhaltung.Unternehmen.com" . Sie möchten Benutzer dieser Gruppen mit Farmen verknüpfen, bei denen die Server, auf denen der Citrix XML-Dienst ausgeführt wird, "Freiburg" und "Erfurt" heißen. Gehen Sie hierzu folgendermaßen vor:

1. Öffnen Sie auf dem US-Webinterface-Server mit einem Texteditor die Datei WebInterface.conf und suchen Sie die folgende Zeile:

   Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance

   Wichtig: Wenn Benutzerroaming aktiviert ist, muss in der ersten Farm, die in der Konfigurationsdatei konfiguriert ist, XenApp 6.0 oder höher oder XenDesktop 4.0 oder höher ausgeführt werden. Wenn in der ersten Farm in der Liste eine frühere Version ausgeführt wird, werden Benutzern keine Ressourcen angezeigt.

2. Definieren Sie neue Farmen, indem Sie folgende Zeilen hinzufügen:

   Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalan
   Farm3=tango,Name:Farm3,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,LoadBalance

3. Weisen Sie den neuen Farmen Benutzergruppen hinzu, indem Sie folgende Zeilen hinzufügen:

   Farm2Groups=ussales.mycompany.com\SalesMgrs,ussales.mycompany.com\SalesTeam,finance.mycompar
   Farm3Groups=ussales.mycompany.com\SalesMgrs

   Wenn Sie einer Farm, die mit **Farm<*n*>** definiert ist, den Parameter **Farm<*n*>Groups** hinzufügen, wird die Benutzerroamingfunktion aktiviert. Dies bedeutet, dass Sie allen Farmen Benutzergruppen zuweisen müssen, und nicht nur denen, die von Roamingbenutzern verwendet werden.
4. Stellen Sie sicher, dass Benutzer weiterhin auf die vorhandene Farm zugreifen können, indem Sie folgende Zeile hinzufügen:

   Farm1Groups=mycompany.com\DomainUsers

   Damit Roamingbenutzer, wenn sie in Japan sind, auf ihre Ressourcen zugreifen können, müssen Sie dieselben Anpassungen in der Konfigurationsdatei des japanischen Webinterface-Servers vornehmen.

5. Öffnen Sie auf dem Webinterface-Server in Japan mit einem Texteditor die Datei WebInterface.conf und fügen Sie die Zeilen aus Schritt 2 und 3 hinzu. Stellen Sie sicher, dass auch allen vorhandenen japanischen Farmen Benutzergruppen zugewiesen werden, damit lokale Benutzer weiter auf sie zugreifen können.

Protokollierte Meldungen und Ereignis-IDs

Aktualisiert: 2014-11-25

Das Webinterface protokolliert Ereignis-IDs für alle Sitetypen und Plattformen auf. Auf Windows-Betriebssystemen können Ereignis-IDs mit der Ereignisanzeige angezeigt werden und sie können von Ctrix EdgeSight oder anderen Überwachungs- und Berichterstellungstools von Drittanbietern verwendet werden. Auf Java-Anwendungsservern sind Ereignis-IDs Teil der Protokollmeldung, die in die Webserver-Protokolldatei geschrieben wird.

Die folgende Tabelle enthält die Webinterface-Ereignis-IDs und die dazugehörigen Protokollmeldungen. Außerdem sind kurze Beschreibungen der Probleme sowie Lösungsvorschläge enthalten.

Ereignis-ID	Message	Schweregrad	Beschreibung
10001	Fehler beim Konfigurationsparsing: <*Fehlerbeschreibung*>.	Fehler	Es liegt ein Problem bei der Konfigurationsdatei der Site vor. Suchen Sie in der Datei WebInterface.conf nach Fehlern.
10002	Fehler beim Laden der Konfiguration.	Fehler	Die Konfigurationsdatei der Site fehlt oder Zugriff darauf ist nicht möglich. Stellen Sie sicher, dass WebInterface.conf nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.
10003	Die Citrix Online Plug-In-Konfiguration konnte nicht abgerufen werden.	Fehler	Die Konfigurationsdatei des Online Plug-Ins fehlt oder Zugriff darauf ist nicht möglich. Stellen Sie sicher, dass config.xml nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.
10004	Die Konfigurationsdaten wurden erfolgreich neu geladen.	Information	Kürzlich vorgenommene Änderungen der Konfigurationsdateien der Site (WebInterface.conf) oder des Online Plug-Ins (config.xml) wurden überprüft und übernommen.

10005	Die folgenden Schlüssel kommen in der Konfigurationsdatei doppelt vor: <*Schlüsselname*>.	Warnung	Die Konfigurationsdatei der Site enthält einen Parameter zweimal. Beheben Sie den Fehler in WebInterface.conf.
10006	Unbekannter Authentifizierungspunkt: <*Authentifizierungspunkt*>.	Fehler	Der Parameter AuthenticationPoint in der Konfigurationsdatei der Site enthält einen inkorrekten Wert. Beheben Sie den Fehler in WebInterface.conf.
10007	Anonyme Anmeldungen können nicht verwendet werden, wenn Roaming aktiviert ist.	Fehler	XenDesktop unterstützt keine anonymen Benutzer. Um Benutzerroaming mit XenDesktop zu verwenden, deaktivieren Sie anonyme Authentifizierung.
10008	Die Konfiguration ist ungültig: NDS-Authentifizierung wird von dieser Version des Webinterface nicht unterstützt.	Fehler	Konfigurieren Sie die Authentifizierungsmethode für die Site neu und wählen Sie entweder Benutzerprinzipalname (UPN) oder domänenbasierte Authentifizierung von Microsoft.
10009	Die Konfiguration ist ungültig: Smartcard- und Passthrough-Authentifizierung werden von dieser Version des Webinterface nicht unterstützt.	Fehler	Dieser Fehler wird angezeigt, wenn Sie die UNIX/JSP-Version des Webinterface ausführen und Webinterface-Authentifizierungspunkte mit Passthrough-, Smartcard- oder Passthrough-mit-Smartcard-Authentifizierung oder Access Gateway-Authentifizierungspunkte mit Smartcard- oder Passthrough-mit-Smartcard-Authentifizierung verwenden.
10010	Es liegt ein Problem bei der Konfiguration der Zweifaktorauthentifizierung vor.	Fehler	Stellen Sie sicher, dass die Authentifizierung mit Aladdin SafeWord for Citrix, RSA SecurID oder einem RADIUS-Server korrekt konfiguriert ist.
10011	Zurzeit sind keine Authentifizierungsmethoden verfügbar.	Fehler	Stellen Sie sicher, dass die Site korrekt konfiguriert ist und dass Sie mindestens eine gültige Authentifizierungsmethode angegeben haben.

10101	Der Protokollübergangsdienst ist nicht richtig konfiguriert. Stellen Sie sicher, dass in der Datei web.config der Eintrag tokenManager definiert ist und dass mindestens ein Tokendienst definiert ist.	Fehler	Überprüfen Sie, ob in der Datei web.config der XenApp Web-Site ein oder mehrere Tokenaussteller mit dazugehörigen Zertifikatsreferenzen angegeben sind, mit denen die Vertrauensstellung mit dem Dienst Passthrough mit Smartcard vom Access Gateway gesichert werden kann.
10201	Die Konfiguration ist ungültig: Signieren von ICA-Dateien wird von dieser Version des Webinterface nicht unterstützt.	Fehler	Sie müssen Webinterface 5.4 oder höher ausführen, um die Funktion zum Signieren von ICA-Dateien verwenden zu können.
10202	Signieren von ICA-Dateien kann nicht verwendet werden, wenn Unterstützung für Legacy-Clients aktiviert ist.	Fehler	Um Signieren von ICA-Dateien zu aktivieren, muss die Site den nativen Client verwenden und in der Datei Webinterface.conf muss "EnableLegacyIcaClientSupport" auf "Off" gesetzt sein.
10203	Signieren von ICA-Dateien kann nicht mit Offlineanwendungen verwendet werden.	Fehler	Stellen Sie sicher, dass die Site Online- oder Dual Mode-Anwendungen anzeigt.
10204	Sie müssen Benutzern erlauben, den nativen Client auszuwählen, um Signieren von ICA-Dateien verwenden zu können.	Information	Um Signieren von ICA-Dateien zu aktivieren, muss die Site den nativen Client verwenden.
10205	Beim Versuch, eine ICA-Datei zu signieren, ist ein Fehler aufgetreten: <*Fehlermeldung*>.	Fehler	Die Fehlermeldung enthält nähere Informationen darüber, welche Schritte jetzt notwendig sind.
10206	Beim Versuch, eine ICA-Datei zu signieren, ist ein Fehler aufgetreten: <>. Starten Sie den Webserver neu, um sicherzustellen, dass der Dienst für das Signieren von ICA-Dateien aktiviert ist.	Fehler	Starten Sie den Webserver neu und überprüfen Sie in der Webinterface Management Console, ob das Signieren von ICA-Dateien aktiviert worden ist.
11001	Ungültige Umleitungs-URL an Clienterkennungs- und -downloadprozess übergeben.	Fehler	Die Umleitungs-URL gibt die Webseite an, zu der Benutzer weitergeleitet werden, wenn sie den Clienterkennungs- und -bereitstellungsprozess abgeschlossen haben. Dieser Fehler zeigt an, dass die Umleitungs-URL im Code der Site geändert wurde.

11002	Der Clienterkennungs- und -bereitstellungsprozess konnte keinen der aktivierten Clients bereitstellen. Überprüfen Sie, ob Browser, Betriebssystem und Zugriffsmethode des Benutzers mit den aktivierten Clients kompatibel sind und ob diese Clients im Ordner \Clients der XenApp Web-Site verfügbar sind.	Fehler	Der Benutzer konnte keinen Client von der Site abrufen. Stellen Sie sicher, dass ein passender Client für das Gerät des Benutzers, das Betriebssystem, den Browser und die Zugriffsmethode auf dem Webserver verfügbar ist und auf der Site aktiviert ist.
11003	Der Clienterkennungs- und -bereitstellungsprozess wird vom Betriebssystem des Benutzercomputers nicht unterstützt.	Fehler	Der Benutzer konnte keinen Client von der Site abrufen, da der Clienterkennungs- und -bereitstellungsprozess das Betriebssystem auf dem Benutzergerät nicht ermitteln konnte.
11004	Die Anfrage von dem Browser, der auf dem Benutzergerät <*IP-Adresse*> ausgeführt wird, kann nicht verarbeitet werden, da der User-Agent-HTTP-Header, der die Plattforminformationen enthält, nicht vorhanden ist.	Fehler	Der Benutzer konnte nicht auf die Site zugreifen, da die vom Browser gesendete Anfrage keinen User-Agent-HTTP-Header enthält, mit dem der Browser und die Plattform identifiziert werden. Überprüfen Sie Ihre Umgebung, um sicherzustellen, dass User-Agent-HTTP-Header nicht aus Benutzeranfragen entfernt werden.
12001	Das Webinterface hat <*Anzahl*> Meldungen mit dieser eindeutigen Protokoll-ID nicht protokolliert. Die Meldungsrate ist gesunken und das Webinterface wird diese Meldungen jetzt wieder protokollieren.	Information	Verhindern Sie mit der Aufgabe Diagnoseprotokollierung unter Sitewartung in der Citrix Webinterface Management Console, dass doppelte Ereignisse wiederholt protokolliert werden, und konfigurieren Sie, wie viele doppelte Ereignisse protokolliert werden und wie oft.
12002	Weitere Meldungen mit dieser eindeutigen Protokoll-ID werden nicht protokolliert, bis die Meldungsrate gesunken ist.	Information	Verhindern Sie mit der Aufgabe Diagnoseprotokollierung unter Sitewartung in der Citrix Webinterface Management Console, dass doppelte Ereignisse wiederholt protokolliert werden, und konfigurieren Sie, wie viele doppelte Ereignisse protokolliert werden und wie oft.

12003	Die Ereignis-ID-Datei konnte nicht geladen werden. Überprüfen Sie in <*Dateiname*>, dass der Pfad zu der Ereignis-ID-Datei korrekt ist.	Warnung	Die Ereignis-ID-Datei fehlt oder Zugriff darauf ist nicht möglich. Überprüfen Sie, ob der Pfad in web.config (für in IIS gehostete Sites) oder web.xml (für auf Java-Anwendungsservern gehostete Sites) korrekt ist. Stellen Sie außerdem sicher, dass WebInterfaceEventIds.txt nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.
12004	Der Nachrichtenschlüssel <*Schlüsselname*> hat keine gültige Ereignis-ID-Entsprechung. Überprüfen Sie, ob die Ereignis-ID-Datei einen gültigen Eintrag für <*Schlüsselname*> hat. Die Ereignis-ID muss eine Ganzzahl zwischen 1 und 65535 sein.	Warnung	Die angegebene Ereignis-ID wurde nicht in der Ereignis-ID-Datei gefunden. Überprüfen Sie, ob diese Ereignis-ID aus der Datei WebInterfaceEventIds.txt entfernt wurde.
13001	Eine SSL-Verbindung mit dem Webdienst unter <*Serveradresse*>:<*Port*> konnte nicht hergestellt werden. Folgende Meldung wurde von der Plattform ausgegeben: <*Fehlerbeschreibung*>.	Fehler	Ein SSL-Fehler ist aufgetreten. Details finden Sie am Ende der Fehlermeldung. Überprüfen Sie, ob die Integration des Webinterface mit Access Gateway oder Password Manager über SSL richtig konfiguriert ist.
13002	Sicherheits-IDs für mindestens eine Gruppe konnten nicht abgerufen werden. Überprüfen Sie, ob der Citrix XML-Dienst verfügbar ist und Roaming von Benutzern unterstützt und ob die Gruppennamen in der Konfigurationsdatei korrekt sind.	Fehler	Bei mindestens einer Benutzergruppe, die für Benutzerroaming konfiguriert ist, ist ein Problem aufgetreten. Überprüfen Sie, ob auf allen Servern in der Farm eine Version von XenApp oder XenDesktop ausgeführt wird, die Benutzerroaming unterstützt. Überprüfen Sie außerdem, ob die angegebenen Gruppennamen gültig sind und die Kommunikation mit den Citrix Servern möglich ist.

14001	Es ist ein Problem mit dem RSA SecurID ACE/Agent aufgetreten. Stellen Sie sicher, dass der ACE/Agent richtig installiert ist und dass der Pfad zu der Datei aceclnt.dll der Umgebungsvariable PATH hinzugefügt wurde.	Fehler	Um SecurID-Authentifizierung mit dem Webinterface für Microsoft Internetinformationsdienste verwenden zu können, muss das Webinterface nach dem RSA Authentication Agent für Web für Internetinformationsdienste installiert werden.
14002	Es ist ein Problem mit dem RSA SecurID ACE/Agent aufgetreten. Stellen Sie sicher, dass die richtige ACE/Agent-Version installiert ist.	Fehler	Überprüfen Sie, ob eine unterstützte Version des RSA Authentication Agent für Web für Internetinformationsdienste auf dem Webserver installiert ist.
14003	Es ist ein Problem mit dem Aladdin SafeWord Agent aufgetreten. Stellen Sie sicher, dass der Agent richtig installiert ist.	Fehler	Stellen Sie sicher, dass der SafeWord Agent für das Webinterface auf dem Webserver installiert ist. Das Webinterface muss vor dem SafeWord Agent installiert werden.
14004	Das von RSA SecurID ACE/Agent zwischengespeicherte Kennwort kann nicht aktualisiert werden. Überprüfen Sie, ob die RSA SecurID ACE/Agent- und ACE/Server-Versionen kompatibel sind und ob ACE/Agent und ACE/Server für Windows-Kennwortintegration konfiguriert sind.	Fehler	Überprüfen Sie, ob die Versionen von RSA Authentication Manager und RSA Authentication Agent für Web für Internetinformationsdienste kompatibel sind. Überprüfen Sie außerdem, ob die RSA Authentication Manager-Datenbanksystemparameter konfiguriert sind, um die Windows-Kennwortintegration auf Systemebene zu aktivieren.
14005	Das von RSA SecurID ACE/Agent zwischengespeicherte Kennwort kann nicht abgerufen werden. Überprüfen Sie, ob die RSA SecurID ACE/Agent- und ACE/Server-Versionen kompatibel sind und ob ACE/Agent und ACE/Server für Windows-Kennwortintegration konfiguriert sind.	Fehler	Überprüfen Sie, ob die Versionen von RSA Authentication Manager und RSA Authentication Agent für Web für Internetinformationsdienste kompatibel sind. Überprüfen Sie außerdem, ob die RSA Authentication Manager-Datenbanksystemparameter konfiguriert sind, um die Windows-Kennwortintegration auf Systemebene zu aktivieren.

14006	Bei der SafeWord-Authentifizierung des Benutzers ist ein Problem aufgetreten.	Fehler	Es liegt ein Problem mit dem SafeWord-Server vor. Weitere Informationen finden Sie in den Protokolldateien auf dem SafeWord-Server.
14007	Es ist ein Problem mit dem RSA SecurID ACE/Agent aufgetreten. Stellen Sie sicher, dass der Webinterface-Anwendungspool je nach der installierten ACE/Agent-Version für 32-Bit- oder 64-Bit-Anwendungen konfiguriert ist.	Fehler	Überprüfen Sie die Anwendungsanforderungen für die Version von ACE/Agent, die Sie ausführen.
15001	Beim Lesen der Clientversion von <*Dateipfad*> ist ein Fehler aufgetreten. Benutzer werden nicht zum Upgrade auf eine höhere Version dieses Clients aufgefordert.	Fehler	Überprüfen Sie, ob die entsprechenden Berechtigungen konfiguriert wurden, damit die angegebene Clientinstallerdatei gelesen werden kann.
15002	Beim Lesen der Sprachpaketdatei <*Dateiname*> ist ein Problem aufgetreten. Stellen Sie sicher, dass auf die Datei zugegriffen werden kann und dass sie das richtige Format verwendet.	Fehler	Stellen Sie sicher, dass die angegebene Datei nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.
15003	Auf das Verzeichnis <*Verzeichnisname*> konnte nicht zugegriffen werden. Sie können die Clients in diesem Verzeichnis nicht Benutzern zur Verfügung stellen. Stellen Sie sicher, dass das Netzwerkdienst-Konto zum Zugriff auf das Verzeichnis berechtigt ist, und starten Sie dann den Webserver neu.	Fehler	Stellen Sie sicher, dass das angegebene Verzeichnis nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass auf dieses Verzeichnis zugegriffen werden kann.
15004	Beim Lesen der Sprachpaketdatei <*Dateiname*> ist ein Problem aufgetreten. Die Versionsdeklaration fehlt in der Datei und das Sprachpaket kann deshalb nicht verwendet werden.	Fehler	Die Sprachpaketdatei enthält keine Versionsnummer. Korrigieren Sie den Fehler in der angegebenen Datei.

15005	Beim Lesen der Sprachpaketdatei <*Dateiname*> ist ein Problem aufgetreten. Die Sprachpaketversion ist <*Versionsnummer*>. Dies ist nicht kompatibel mit der aktuellen Version des Webinterface.	Fehler	Die Versionen des Webinterface und der Sprachpaketdatei passen nicht zusammen. Sprachpakete sind speziell auf die jeweilige Webinterface-Version, mit der sie geliefert werden, abgestimmt und können nicht mit niedrigeren oder höheren Versionen verwendet werden. Aktualisieren Sie die angegebene Datei oder tauschen Sie sie aus.
15006	Es wurde kein Sprachpaket für das Standardgebietsschema <*Installationsgebietsschema*> gefunden. Das Sprachpaket <*Dateiname*> wurde gefunden und wird als Standard verwendet.	Warnung	Wenn das Webinterface kein Sprachpaket für das während der Installation gewählte Gebietsschema findet, verwendet das Webinterface das erste verfügbare Sprachpaket, das kompatibel ist.
16001	RADIUS-Secret-Datei <*Dateipfad*> kann nicht gelesen werden.	Fehler	Die RADIUS-Secret-Datei fehlt oder Zugriff darauf ist nicht möglich. Überprüfen Sie, ob der Pfad in web.config (für in IIS gehostete Sites) oder web.xml (für auf Java-Anwendungsservern gehostete Sites) korrekt ist. Stellen Sie außerdem sicher, dass die RADIUS-Secret-Datei nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.
16002	Die RADIUS-Geheimschlüssel-Datei <*Dateipfad*> ist leer.	Fehler	Für das RADIUS-Protokoll ist ein gemeinsamer geheimer Schlüssel erforderlich. Dieser Schlüssel ist nur für den RADIUS-Client (das Webinterface) und den RADIUS-Server, bei dem der Client authentifiziert wird, verfügbar. Die RADIUS-Secret-Datei kann eine beliebige Zeichenfolge enthalten, aber sie darf nicht leer sein.
16003	Bei der RADIUS-Authentifizierung des Benutzers ist ein Problem aufgetreten.	Fehler	Es liegt ein Problem mit dem RADIUS-Server vor. Weitere Informationen finden Sie in den Protokolldateien auf dem RADIUS-Server.

16004	Die Werte RADIUS_NAS_IDENTIFIER und/oder RADIUS_IP_ADDRESS müssen in der Webkonfigurationsdatei der Site vorhanden sein. Werte für RADIUS_NAS_IDENTIFIER müssen mindestens 3 Zeichen enthalten. RADIUS_IP_ADDRESS muss eine gültige IP-Adresse sein.	Fehler	Das RADIUS-Protokoll erfordert, dass Zugriffsanfragen an RADIUS-Server die IP-Adresse oder eine andere Kennung für den RADIUS-Client (das Webinterface) enthalten. Stellen Sie sicher, dass web.config (für in IIS gehostete Sites) oder web.xml (für auf Java-Anwendungsservern gehostete Sites) eine gültige RADIUS-NAS-ID oder IP-Adresse enthält.
17001	Fehler bei der Kontextsuche auf Server <*Serveradresse*>:<*Ausnahme*>. Dieser Server wurde vorübergehend von der Liste der aktiven Server entfernt.	Fehler	Es liegt ein Problem mit dem angegebenen NDS-Server vor. Dieser Server wird umgangen, bis das Problem behoben wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem NDS-Server.
17002	Alle NDS-Server sind ausgefallen. Kontextsuche ist daher nicht möglich. Versuchen Sie, sich mit einem vollqualifizierten Benutzernamen anzumelden, d. h. *.benutzername.unternehmen.com*.	Fehler	Keiner der NDS-Server konnte kontaktiert werden. Versuchen Sie, die Anmeldeinformationen im Format *.benutzername.unternehmen.com* einzugeben. Weitere Informationen finden Sie in den Protokolldateien auf den NDS-Servern.
18001	Bei der Kommunikation mit dem Advanced Access Control-Authentifizierungsdienst unter <*URL*> ist ein Kommunikationsfehler aufgetreten. Überprüfen Sie, ob der Authentifizierungsdienst ausgeführt wird. Folgende Meldung wurde von der Plattform ausgegeben: <*Fehlerbeschreibung*>.	Fehler	Es liegt ein Problem mit der Verbindungsherstellung zum Access Gateway-Authentifizierungsdienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien des Access Gateway-Geräts.
18002	Beim Schließen der Sitzung mit dem Access Gateway-Authentifizierungsdienst unter <*URL*> ist ein Kommunikationsfehler aufgetreten. Überprüfen Sie, ob der Authentifizierungsdienst ausgeführt wird. Folgende Meldung wurde von der Plattform ausgegeben: <*Fehlerbeschreibung*>.	Fehler	Es liegt ein Problem mit der Verbindungsherstellung zum Access Gateway-Authentifizierungsdienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien des Access Gateway-Geräts.

18003	Der Access Gateway-Authentifizierungsdienst konnte den Benutzer nicht authentifizieren. Folgende Meldung wurde von dem Dienst ausgegeben: <*Fehlerbeschreibung*> [Statuscode: <*Codenummer*>].	Fehler	Es liegt ein Problem mit dem Access Gateway-Authentifizierungsdienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien des Access Gateway-Geräts.
18004	Der Access Gateway-Authentifizierungsdienst konnte die Sitzung nicht schließen. Folgende Meldung wurde von dem Dienst ausgegeben: <*Fehlerbeschreibung*> [Statuscode: <*Codenummer*>].	Fehler	Es liegt ein Problem mit dem Access Gateway-Authentifizierungsdienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien des Access Gateway-Geräts.
18005	Ungültige URL für Access Gateway-Authentifizierungsdienst in der Sitekonfiguration: <*URL*>.	Fehler	Der Parameter AGEWebServiceURL in der Konfigurationsdatei der Site enthält eine ungültige URL. Beheben Sie den Fehler in WebInterface.conf.
18006	Benutzer <*Benutzername*> konnte sich nicht an der Site anmelden: <*Sitename*>. Starten Sie den Webserver neu, um sicherzustellen, dass der Dienst Passthrough mit Smartcard vom Access Gateway aktiviert ist.	Fehler	Der Smartcard-Benutzer konnte sich nicht an der in Access Gateway integrierten Site anmelden. Starten Sie den Webserver neu, um sicherzustellen, dass der Dienst Passthrough mit Smartcard vom Access Gateway ausgeführt wird.
18007	Diese Access Gateway-Version unterstützt keine Anfragen zum Ändern von Webinterface-Kennwörtern. Damit Benutzer ihre Kennwörter ändern können, müssen Sie ein Upgrade auf eine Access Gateway-Version, die dieses Feature unterstützt, durchführen.	Fehler	Dieser Fehler wird angezeigt, wenn das Feature zur Kennwortänderung in Ihrer Site aktiviert ist, Sie aber eine Access Gateway-Version verwenden, die dieses Feature nicht unterstützt. Deaktivieren Sie das Feature zur Kennwortänderung oder aktualisieren Sie Access Gateway auf eine Version, die dieses Feature unterstützt.
19001	Beim Trennen der Ressourcen eines Benutzers ist ein Fehler aufgetreten. Dies kann folgende Ursachen haben: Workspace Control ist nicht aktiviert, der Benutzer ist anonym oder beim Abrufen der Anmeldeinformationen oder des Clientnamens ist ein Fehler aufgetreten.	Fehler	Es liegt ein Problem mit Workspace Control vor. Überprüfen Sie, ob Workspace Control für die Site aktiviert ist und ob der Benutzer sich mit einer anderen Authentifizierungsmethode als anonyme Authentifizierung angemeldet hat.

19002	Beim Wiederverbinden der Ressourcen eines Benutzers ist ein Fehler aufgetreten. Dies kann folgende Ursachen haben: Workspace Control ist nicht aktiviert, der Benutzer ist anonym oder beim Abrufen der Anmeldeinformationen oder des Clientnamens ist ein Fehler aufgetreten.	Fehler	Es liegt ein Problem mit Workspace Control vor. Überprüfen Sie, ob Workspace Control für die Site aktiviert ist und ob der Benutzer sich mit einer anderen Authentifizierungsmethode als anonyme Authentifizierung angemeldet hat.
20001	Bei der Kommunikation mit dem Password Manager-Dienst unter <*URL*> ist ein Kommunikationsfehler aufgetreten. Überprüfen Sie, ob der Dienst ausgeführt wird. Folgende Meldung wurde von der Plattform ausgegeben: <*Fehlerbeschreibung*>.	Fehler	Es liegt ein Problem mit der Verbindungsherstellung zum Password Manager-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Password Manager-Server.
20002	Ungültige URL für Password Manager-Dienst in der Sitekonfiguration: <*URL*>.	Fehler	Der Parameter AccountSelfServiceUrl in der Konfigurationsdatei der Site enthält eine ungültige URL. Beheben Sie den Fehler in WebInterface.conf.
21001	Ein schwerwiegender Serverfehler ist aufgetreten.	Fehler	In einem der Skripte, die auf der Webseite ausgeführt werden, ist eine Java-Ausnahme aufgetreten. Versuchen Sie, die Seite neu zu laden. Sie können auch mit der Aufgabe Site reparieren unter Sitewartung in der Citrix Webinterface Management Console die Skripte für die Site neu installieren.
21002	Schwerwiegender Serverfehler: <*.NET-Fehlerbeschreibung*>.	Fehler	In einem der Skripte, die auf der Webseite ausgeführt werden, ist eine .NET-Ausnahme aufgetreten. Versuchen Sie, die Seite neu zu laden. Sie können auch mit der Aufgabe Site reparieren unter Sitewartung in der Citrix Webinterface Management Console die Skripte für die Site neu installieren.

21003	Der Datei-Watcher konnte aufgrund eines Fehlers nicht unter Pfad <*Sitekonfigurationsverzeichnis*> erstellt werden.	Fehler	Überprüfen Sie, ob der Pfad zu dem Sitekonfigurationsordner korrekt ist und ob die Berechtigungen so konfiguriert sind, dass das Verzeichnis gelesen werden kann. Sie können auch versuchen, IIS neu zu starten, um die Site mit den aktuellen Konfigurationsänderungen zu aktualisieren.
21004	Ein Benutzer kann nicht auf die Site zugreifen, da der vollqualifizierte Domänenname des Webservers Unterstriche (_) enthält. Benennen Sie den Webserver und/oder die Domäne um, um die Unterstriche zu entfernen. Wenn dies nicht möglich ist, konfigurieren Sie eine alternative Adresse für den Webserver, die keine Unterstriche enthält, oder weisen Sie Benutzer an, mit der IP-Adresse des Webservers auf die Site zuzugreifen.	Fehler	Zugriff auf Sites, deren Namen nicht erkannte Zeichen, z. B. Unterstriche, enthalten, ist nicht möglich. Überprüfen Sie, ob der Webservername Unterstriche enthält, und ändern Sie den Servernamen ggf. mit der Webinterface Management Console.
21005	Das ActiveX-Steuerelement für das Citrix Online Plug-In mit der Klassen-ID <*ID*> konnte nicht gestartet werden. Überprüfen Sie, ob in der Konfigurationsdatei der Site die richtige Klassen-ID angegeben wurde.	Fehler	Überprüfen Sie, ob die ActiveX-Klassen-ID mit der ID in der Datei Webinterface.conf übereinstimmt.
21006	Das ActiveX-Steuerelement für das Citrix Online Plug-In mit der Klassen-ID <*ID*> konnte nicht gestartet werden. Überprüfen Sie, ob in der Konfigurationsdatei der Site die richtige Klassen-ID angegeben wurde.	Fehler	Überprüfen Sie, ob die ActiveX-Klassen-ID mit der ID in der Datei Webinterface.conf übereinstimmt.
22001	Die Dateien für den Client für Java können nicht auf dem Server gefunden werden. Überprüfen Sie, ob diese Dateien im Ordner \Clients der XenApp Web-Site vorhanden sind.	Fehler	Die Client-für-Java-Pakete fehlen oder Zugriff darauf ist nicht möglich. Stellen Sie sicher, dass die Dateien nicht gelöscht wurden und dass die Berechtigungen so konfiguriert wurden, dass diese Dateien gelesen werden können.

23001	Beim Versuch, auf den Desktop für Benutzer <*Benutzername*> zuzugreifen, ist ein ICA-Fehler aufgetreten.	Fehler	Das Citrix Online Plug-In konnte nicht auf den Benutzerdesktop zugreifen. Stellen Sie sicher, dass der Desktop ausgeführt wird und Zugriff darauf möglich ist.
23002	Internet Explorer konnte Benutzer <*Benutzername*> keinen Zugriff auf den Desktop geben. Überprüfen Sie, ob auf dem Gerät des Benutzers Citrix Desktop Appliance Lock installiert ist und ob die Desktop Appliance Connector-Site der entsprechenden Windows-Sicherheitszone in Internet Explorer hinzugefügt wurde.	Fehler	Der Desktopgerätbenutzer konnte nicht auf einen Desktop im Vollbildmodus zugreifen. Überprüfen Sie, ob das Citrix Online Plug-In auf dem Benutzergerät korrekt installiert und konfiguriert wurde.
23003	Benutzer <*Benutzername*> hat Zugriff auf <*Anzahl*> Desktops erhalten. Benutzer, die mit einem Desktop Appliance Connector auf Desktops im Vollbildmodus zugreifen, sollten immer nur Zugriff auf einen einzigen Desktop erhalten.	Warnung	Es wurde mehr als ein Desktop für den Desktopgerätbenutzer zur Verfügung gestellt. Der Benutzer kann auf einen Desktop zugreifen. Da es jedoch nicht möglich ist, den erforderlichen Desktop auszuwählen, kann der Benutzer bei der nächsten Anmeldung möglicherweise keine Verbindung zu demselben Desktop herstellen. Konfigurieren Sie den Desktop Appliance Connector so, dass der Benutzer nur berechtigt ist, auf einen einzelnen Desktop zuzugreifen.
23004	Die angegebene Authentifizierungsmethode ist ungültig. Sie müssen entweder 'Explicit' oder 'Certificate' aber nicht beide gleichzeitig angeben.	Fehler	In der Sitekonfigurationsdatei wurden für den Parameter WIAuthenticationMethods Werte für Explicit und Certificate angegeben. Sie können nicht gleichzeitig explizite und Smartcard-Authentifizierung für denselben Desktop Appliance Connector angeben. Beheben Sie den Fehler in WebInterface.conf.

23005	Die Konfiguration für SSO-Authentifizierung mit eingebetteter Smartcard ist ungültig. Die Authentifizierungsmethode muss 'Certificate' enthalten.	Fehler	In der Site-Konfigurationsdatei für den Desktop Appliance Connector muss für den Parameter WIAuthenticationMethods der Wert Certificate angegeben werden. Beheben Sie den Fehler in WebInterface.conf.
23006	Die angegebenen Authentifizierungsmethoden sind ungültig. Die Kombination von Authentifizierungsmethoden wird nicht unterstützt.	Fehler	Die Authentifizierungsmethoden, die für Desktop Appliance Connector in der Site-Konfigurationsdatei im Parameter WIAuthenticationMethods angegeben wurden, können nicht zusammen verwendet werden. Beheben Sie den Fehler in WebInterface.conf.
24001	Ein nicht authentifizierter Benutzer hat versucht, sich anzumelden. Überprüfen Sie, ob für alle vorgesehenen Benutzer des Systems Schattenkonten angelegt wurden. Wenn das Problem weiterhin auftritt, versuchen Sie, die Site mit der Webinterface Management Console zu reparieren.	Fehler	Es liegt ein Problem mit der Site mit ADFS-Integration vor. Der Benutzer konnte nicht authentifiziert werden. Überprüfen Sie, ob für den Benutzer in der Ressourcenpartnerdomäne ein Schattenkonto erstellt wurde. Sie können auch mit der Aufgabe Site reparieren unter Sitewartung in der Citrix Webinterface Management Console die Site neu installieren.
24002	Ein nicht authentifizierter Benutzer hat versucht, sich anzumelden. Wenn das Problem weiterhin auftritt, versuchen Sie, die Site mit der Webinterface Management Console zu reparieren.	Fehler	Es liegt ein Problem mit der XenApp Web- oder XenApp Services-Site vor. Der Benutzer konnte nicht authentifiziert werden. Überprüfen Sie, ob in der Domäne ein Benutzerkonto für den Benutzer erstellt wurde. Sie können auch mit der Aufgabe Site reparieren unter Sitewartung in der Citrix Webinterface Management Console die Site neu installieren.

30001	Ein Fehler trat beim Versuch auf, Informationen von den Citrix Servern zu lesen: <*Farmname*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30002	Ein Fehler trat beim Versuch auf, Informationen auf die Citrix Server zu schreiben: <*Farmname*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30003	Ein Fehler trat beim Versuch auf, eine Verbindung zum Server <*Serveradresse*> auf Port <*Port*> herzustellen. Überprüfen Sie, ob der Citrix XML-Dienst ausgeführt wird und den richtigen Port verwendet. Wenn der XML-Dienst so konfiguriert ist, denselben Port wie Microsoft Internetinformationsdienste (IIS) zu verwenden, überprüfen Sie, ob IIS ausgeführt wird. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Überprüfen Sie, ob der XML-Dienst für die gemeinsame Verwendung der TCP/IP-Ports mit IIS konfiguriert wurde. Wenn dies der Fall ist, überprüfen Sie, ob IIS ausgeführt wird. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30004	Der Servername <*Serveradresse*> kann nicht aufgelöst werden. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30005	Die Citrix Server übermittelten falsch formatierte HTTP-Syntax. Überprüfen Sie, ob die aktuelle Webinterface-Version mit den verwendeten Servern kompatibel ist. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass in der Serverfarm XenDesktop oder Presentation Server 4.5 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30006	Die Citrix Server sendeten eine falsche oder unerwartete Antwort. Überprüfen Sie, ob die aktuelle Webinterface-Version mit den verwendeten Servern kompatibel ist. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass in der Serverfarm XenDesktop oder Presentation Server 4.5 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30008	Die Citrix Server haben die Verbindung unerwartet getrennt. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30009	Die Citrix Server übermittelten HTTP-Header, die das Auftreten eines Fehlers angeben: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30010	Die Citrix Server können die Anforderung zurzeit nicht verarbeiten. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30011	Folgender Fehler ist auf den Citrix Servern beim Versuch aufgetreten, die Anforderung abzuschließen: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30012	Die Citrix Server haben eine nicht übereinstimmende Version gefunden. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30013	Die Citrix Server haben eine falsche Anforderung erhalten. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30014	Beim Parsen der Anforderung ist ein Fehler auf den Citrix Servern aufgetreten. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30015	Der Citrix XML-Dienst unter der Adresse <*Dateipfad*> kann keine Anfragen verarbeiten.	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30016	Das Citrix XML-Dienstobjekt wurde nicht gefunden: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30017	Die Citrix XML-Dienstmethode wird nicht unterstützt: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30018	Die Citrix XML-Dienstantwort ist nicht akzeptabel: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30019	Die Länge der Citrix XML-Dienstanforderung ist erforderlich: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30020	Die Citrix XML-Dienstanforderung ist zu kurz: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30021	Die Citrix XML-Dienstanforderung überschreitet die maximale Größe: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30022	Der Citrix XML-Dienst oder die Citrix Server sind möglicherweise nicht verfügbar oder momentan überlastet: <*Details*>. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30023	Das von den Citrix Servern übermittelte XML-Dokument konnte nicht verarbeitet werden. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30024	Das von den Citrix Servern übermittelte XML-Dokument konnte nicht verarbeitet werden, da es ungültigen XML-Code enthält. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30025	Ein Fehler trat beim Versuch auf, Informationen von den Citrix Servern zu lesen: <*Farmname*>. Dieser Fehler ist möglicherweise das Ergebnis eines Versuchs, mit einer anderen Komponente als einem SSL-Relay zu kommunizieren. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Um bei Verbindungen zu der Serverfarm SSL/TLS-Verschlüsselung zu verwenden, müssen Sie mit dem SSL-Relay Unterstützung auf allen Servern konfigurieren. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30026	Ein Fehler trat beim Versuch auf, eine Verbindung mit dem SSL-Relay herzustellen: <*Serveradresse*>:<*Port*>. Bitte stellen Sie sicher, dass ein SSL-Relay aktiv ist und dass es einen gültigen Port abhört. Der Name im Serverzertifikat, das für das SSL-Relay konfiguriert ist, muss genau mit dem Namen des Servers übereinstimmen, zu dem eine Verbindung hergestellt werden soll. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass das SSL-Relay aktiv ist und den richtigen Port abhört (üblicherweise Port 443) und dass das Zertifikat des SSL-Relay-Servers den vollqualifizierten Namen des Servers (unter Beachtung von Groß- und Kleinschreibung) enthält, zu dem die Verbindung hergestellt werden soll. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30027	Ticketing wird möglicherweise von mindestens einem Citrix Server nicht unterstützt. Um diese Funktion verwenden zu können, müssen Sie die Server aktualisieren, auf denen der XML-Dienst ausgeführt wird, oder deaktivieren Sie Ticketing. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass auf allen Servern in der Farm XenDesktop oder MetaFrame XP 1.0 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30028	Der Name des SSL-Relays <*Serveradresse*> konnte nicht aufgelöst werden. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30029	Eine SSL-Verbindung konnte nicht hergestellt werden: <*SSL-Fehler-Beschreibung*>. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30030	Eine Verbindung zum SSL-Relay konnte nicht hergestellt werden: <*SSL-Fehler-Beschreibung*>. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30031	Der Citrix XML-Dienst unter der Adresse <*Dateipfad*> unterstützt nicht die Funktion <*Funktionsname*>.	Fehler	Überprüfen Sie, ob auf allen Servern in der Farm eine Version von XenApp oder XenDesktop ausgeführt wird, die die angegebene Funktion unterstützt. Weitere Informationen finden Sie unter Mindestanforderungen für die Software.

30101	Bei dem Versuch, das Kennwort zu ändern, ist ein Fehler aufgetreten.	Fehler	Aus Sicherheitsgründen konnte der Benutzer nicht das Windows-Kennwort ändern. Weitere Informationen finden Sie in den Protokolldateien der Citrix Server und/oder des Domänencontrollers.
30102	Die Citrix Server meldeten einen unspezifizierten Fehler vom XML-Dienst unter der Adresse <*Dateipfad*>.	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30103	Die Citrix Server meldeten, dass keine alternative Adresse gefunden wurde. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30104	Beim Herstellen einer Verbindung zum Citrix Server, um auf die Ressource zuzugreifen, ist ein Fehler aufgetreten. Überprüfen Sie, ob der Server aktiv ist und das Netzwerk ordnungsgemäß funktioniert. Dieser Fehler wurde für einen XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Überprüfen Sie, ob in der Serverfarm oder im Netzwerk Probleme vorliegen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30105	Die Citrix Server vertrauen dem Server nicht. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Überprüfen Sie, ob zwischen dem Webinterface-Server und dem Citrix XML-Dienst eine Vertrauensstellung besteht. Weitere Informationen finden Sie unter Verwenden von Workspace Control mit integrierten Authentifizierungsmethoden für XenApp Web-Sites.

30106	Die Citrix Server sind nicht für die Unterstützung des angeforderten Vorgangs lizenziert. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass der Citrix Lizenzserver ausgeführt wird und Zugriff darauf möglich ist. Citrix empfiehlt, den Lizenzserver auf die aktuelle Version zu aktualisieren, um Kompatibilität mit neuen Produkten zu gewährleisten. Weitere Informationen finden Sie in den Protokolldateien des Citrix Servers und/oder des Lizenzservers.
30107	Die Citrix Server sind zu ausgelastet, um Zugriff auf die ausgewählte Ressource zu ermöglichen. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Überprüfen Sie, ob die Serverfarm überlastet ist. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30108	Die Ticketing-Funktion ist auf dem Citrix Server deaktiviert. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass alle Server in der Farm denselben Port für die Kommunikation mit dem XML-Dienst verwenden. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30109	Der Citrix XML-Dienst unter Adresse <*Dateipfad*> hat einen Registrierungsfehler gemeldet. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30110	Ein Fehler des Typs <*Fehlertyp*> mit einer Fehler-ID von <*Fehler-ID*> wurde vom Citrix XML-Dienst unter der Adresse <*Dateipfad*> gemeldet. Wie viele Informationen im Ereignisprotokoll des Servers zur Verfügung stehen, hängt davon ab, auf welchem Server der XML-Dienst ausgeführt wird. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30111	Die Citrix Server unterstützen den angegebenen Adresstyp nicht. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30112	Beim Zugriff auf Desktopgruppe <*Gruppenname*> wurde keine verfügbare Ressource für Benutzer <*Benutzername*> gefunden. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Überprüfen Sie, ob der Benutzer der angegebenen Desktopgruppe zugewiesen wurde und ob unbenutzte Desktops in der Gruppe vorhanden sind. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30113	Eine Verbindungsanfrage des Citrix Servers wurde abgelehnt, während die Initialisierung der Desktopgruppe <*Gruppenname*> für Benutzer <*Benutzername*> verarbeitet wurde. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30114	Die Citrix Server sind nicht zum Abrufen von Sicherheits-IDs für den Benutzer berechtigt. Gewähren Sie dem XML-Dienst Leserechte für das Attribut 'Token-Groups-Global-And-Universal' in Active Directory oder deaktivieren Sie die Auflistung von Sicherheits-IDs im XML-Dienst. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Wenn der XML-Dienst konfiguriert wurde, Sicherheits-IDs für Benutzer aufzuzählen, überprüfen Sie, ob die entsprechenden Berechtigungen in Active Directory gewährt wurden. Weitere Informationen finden Sie in Artikel CTX117489 und den Protokolldateien auf dem Citrix-Server.
30115	Die Citrix Server konnten keine Sicherheits-IDs für den Benutzer abrufen. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in Artikel CTX117489 und den Protokolldateien auf dem Citrix-Server.
30116	Beim Initialisieren der Desktopgruppe <*Gruppenname*> ist keine Verbindung zu einem Desktop im Wartungsmodus für Benutzer <*Benutzername*> möglich. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass der Desktop des Benutzers nicht in den Wartungsmodus versetzt wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30117	Die Citrix Server unterstützen keine Desktopneustarts. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass in der Serverfarm XenDesktop 3.0 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

30118	Die Citrix Server haben das Zeitlimit überschritten, weil das Herunterfahren eines Computers in der Desktopgruppe <*Gruppenname*> für Benutzer <*Benutzername*> zu lange gedauert hat. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30119	Ein Computer im Wartungsmodus in der Desktopgruppe <*Gruppenname*> für Benutzer <*Benutzername*> konnte nicht heruntergefahren werden. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Stellen Sie sicher, dass der Desktop des Benutzers nicht in den Wartungsmodus versetzt wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30120	Benutzer <*Benutzername*> wurde nicht gefunden. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30201	Ungültige Secure Ticket Authority-Adresse: <*URL*>. <*Fehlerbeschreibung*>	Fehler	Der Parameter **CSG_STA_ URL<*n*>** in der Konfigurationsdatei der Site enthält eine ungültige URL. Beheben Sie den Fehler in WebInterface.conf.
30202	Die Secure Ticket Authority <*URL*> unterstützt keine Anfragen von Version 4. Die gesamte Secure Ticket Authority-Kommunikation greift jetzt auf Version 1 zurück. Dies bedeutet, dass neue Verbindungen über Secure Gateway keine Sitzungszuverlässigkeit verwenden.	Fehler	Die verwendete Secure Gateway-Version unterstützt nicht die Secure Ticket Authority-Redundanzfunktion. Aus diesem Grund wird diese Funktion deaktiviert.

30203	Die Secure Ticket Authority <*URL*> gab ein Ticket mit einer unerwarteten Autorität bzw. einem unerwarteten Typ zurück - <*Fehlertyp*>, <*Fehler-ID*>, <*SSL-Fehler-Beschreibung*>, <*Details*>. <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit der Secure Ticket Authority vor. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30204	Es konnte keine Verbindung zur Secure Ticket Authority hergestellt werden. Sie wurde vorübergehend von der Liste der aktiven Dienste entfernt.	Fehler	Es liegt ein Problem mit der Secure Ticket Authority vor. Dieser Dienst wird umgangen, bis das Problem behoben wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
30205	Keine der konfigurierten Secure Ticket Authoritys hat auf diese XML-Transaktion geantwortet.	Fehler	Es konnte keine Verbindung zu einer Secure Ticket Authority hergestellt werden. Versuchen Sie, den Webserver neu zu starten. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
30301	Die HTTP-Antwort zeigt an, dass die zugrundeliegende Verbindung geschlossen wurde.	Fehler	Stellen Sie sicher, dass in der Serverfarm XenDesktop oder Presentation Server 4.5 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen.
30401	Ein Socket wurde von der Transaktionsebene zerstört.	Fehler	Überprüfen Sie, ob der Farmdatenspeicher beschädigte Anwendungen enthält. Weitere Informationen finden Sie unter CTX114769.
31001	Es konnte keine Verbindung zum angegebenen Citrix XML-Dienst hergestellt werden. Er wird vorübergehend von der Liste der aktiven Dienste entfernt.	Fehler	Es liegt ein Problem mit dem Citrix XML-Dienst vor. Dieser Server wird umgangen, bis das Problem behoben wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
31002	Diese XML-Dienst-Transaktion ist fehlgeschlagen, aber der XML-Dienst wurde nicht von der Liste der aktiven Dienste entfernt.	Fehler	Obwohl auf den Citrix XML-Dienst zugegriffen werden kann, konnte die Anfrage oder Anweisung nicht abgeschlossen werden. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.

31003	Keiner der für die Farm <*Farmname*> konfigurierten Citrix XML-Dienste antwortete auf diese XML-Dienst-Transaktion.	Fehler	Keiner der Citrix XML-Dienst-Hosts für die angegebene Farm konnte kontaktiert werden. Versuchen Sie, den Webserver neu zu starten. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
31004	Der XML-Protokoll-Fehler <*Fehler-ID*> konnte nicht in einen Zugriffsstatusfehler umgewandelt werden.	Fehler	Stellen Sie sicher, dass der Benutzer Active Directory-Anmelderechte für die Citrix Server hat.
31005	<*Anzahl*> von <*Anzahl*> Ressourcen wurden ignoriert, da sie ungültig sind.	Fehler	Der Citrix XML-Dienst konnte nicht alle verfügbaren Ressourcen aufzählen. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
31006	Die Anmeldung von Benutzer <*Benutzername*> wurde abgelehnt, weil der Benutzer nicht lizenziert ist.	Fehler	Der Benutzer konnte nicht angemeldet werden, da keine Citrix Lizenzen oder Microsoft Remotedekstopdienste-Clientzugriffslizenzen verfügbar sind. Stellen Sie sicher, dass der Citrix Lizenzserver ausgeführt wird und Zugriff darauf möglich ist. Citrix empfiehlt, den Lizenzserver auf die aktuelle Version zu aktualisieren, um Kompatibilität mit neuen Produkten zu gewährleisten. Weitere Informationen finden Sie in den Protokolldateien der Citrix Server und/oder des Lizenzservers.
31007	Die Citrix Server sind nicht für die Unterstützung von Workspace Control lizenziert. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>.	Fehler	Stellen Sie sicher, dass die Citrix Lizenzen eine Produktedition aktivieren, die die Workspace Control-Funktion enthält. Stellen Sie außerdem sicher, dass der Citrix Lizenzserver ausgeführt wird und Zugriff darauf möglich ist. Citrix empfiehlt, den Lizenzserver auf die aktuelle Version zu aktualisieren, um Kompatibilität mit neuen Produkten zu gewährleisten. Weitere Informationen finden Sie in den Protokolldateien des Citrix Servers und/oder des Lizenzservers.

31008	Die Citrix Server sind nicht zum Starten der Ressource <*Ressourcenname*> lizenziert. Diese Meldung wurde vom XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>.	Fehler	Stellen Sie sicher, dass die Citrix Lizenzen eine Produktedition aktivieren, die diesen Ressourcentyp enthält. Stellen Sie außerdem sicher, dass der Citrix Lizenzserver ausgeführt wird und Zugriff darauf möglich ist. Citrix empfiehlt, den Lizenzserver auf die aktuelle Version zu aktualisieren, um Kompatibilität mit neuen Produkten zu gewährleisten. Weitere Informationen finden Sie in den Protokolldateien des Citrix Servers und/oder des Lizenzservers.
31009	Die Kontodaten für die folgenden Konten können nicht abgerufen werden: <*Liste der Kontonamen*>. Überprüfen Sie, ob der Name richtig geschrieben ist. Diese Meldung wurde vom Citrix XML-Dienst unter folgender Adresse ausgegeben: <*Dateipfad*>.	Fehler	Der Citrix XML-Dienst kann nicht auf die angegebenen Konten zugreifen. Überprüfen Sie, ob die Konten gelöscht wurden und ob die richtigen Berechtigungen konfiguriert wurden, damit der XML-Dienst die Konten lesen kann. Überprüfen Sie außerdem, ob die Kontonamen richtig eingegeben wurden. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
31101	Der Benutzer <*Benutzername*> hat eine Serversitzung, <*Sitzungs-ID*>, hat aber keinen Zugriff auf <*Ressourcenname*>, die Ressource, die die Sitzung erstellt hat. Aus diesem Grund kann der Benutzer nicht auf diese Sitzung zugreifen.	Fehler	Die Zugriffsberechtigungen des Benutzers wurden geändert, während die Benutzersitzung noch aktiv war. Setzen Sie die Sitzung zurück. Beachten Sie, dass dies zu Datenverlust für den Benutzer führt. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
31201	Die Farm <*Farmname*> wurde für Ticketing konfiguriert. Es wurde jedoch kein Tag für ein Ticket empfangen. Prüfen Sie, ob die Farm Ticketing unterstützt.	Fehler	Stellen Sie sicher, dass auf allen Servern in der angegebenen Farm XenDesktop oder MetaFrame XP 1.0 oder höher ausgeführt wird. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.

31202	Ein Benutzer hat versucht, die Ressource <*Ressourcenname*> zu starten, die zurzeit deaktiviert ist.	Fehler	Überprüfen Sie, ob die angegebene Ressource auf dem Server, auf dem sie gehostet wird, aktiviert ist.
31203	Die Farm <*Farmname*> wurde konfiguriert, Startreferenzen zu verwenden. Es wurde aber keine Startreferenz vom Citrix XML-Dienst empfangen. Überprüfen Sie, ob die Farm Startreferenzen unterstützt, oder deaktivieren Sie Startreferenzanfragen.	Fehler	Um Startreferenzen zu verwenden, muss auf allen Servern in der angegebenen Farm XenDesktop oder Presentation Server 4.5 oder höher ausgeführt werden. Citrix empfiehlt, dass alle Server in einer Farm dasselbe Produkt mit derselben Version ausführen. Wenn in der Farm XenApp 4.0, mit Feature Pack 1, für UNIX oder Presentation Server 4.0 und früher ausgeführt wird, stellen Sie sicher, dass in der Konfigurationsdatei der XenApp Web-Site, WebInterface.conf, die Parameter RequireLaunchReference auf Off und OverrideIcaClientname auf On gesetzt sind.
31301	Die Konfiguration der Farm <*Farmname*> ist ungültig.	Fehler	Es liegt ein Problem mit der angegebenen Serverfarm vor. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
32001	Die Konfiguration enthält keine Informationen für Citrix Server.	Fehler	Für den Parameter **Farm<*n*>** in der Konfigurationsdatei der XenApp Services-Site wurde kein Wert angegeben. Beheben Sie den Fehler in WebInterface.conf.
32002	Parsing der Provider Chain-Konfiguration nicht möglich.	Fehler	Es liegt ein Problem mit der XenApp Services-Site vor. Suchen Sie in den Sitekonfigurationsdateien nach Fehlern.
32003	<*Fehlerursache*> Der folgende Systemfehler ist aufgetreten: <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit der XenApp Services-Site vor. Details finden Sie am Ende der Fehlermeldung. Suchen Sie in den Sitekonfigurationsdateien nach Fehlern.

33001	Citrix Streaming-Dienst: Der angegebene Citrix XML-Dienst konnte nicht kontaktiert werden und wurde vorübergehend von der Liste aktiver Dienste entfernt.	Fehler	Das Citrix Offline Plug-In hat ein Problem mit dem Citrix XML-Dienst festgestellt. Dieser Dienst wird umgangen, bis das Problem behoben wurde. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
33002	Citrix Streaming-Dienst: Diese Citrix XML-Dienst-Transaktion ist fehlgeschlagen, aber der XML-Dienst wurde nicht von der Liste aktiver Dienste entfernt.	Fehler	Obwohl das Citrix Offline Plug-In auf den Citrix XML-Dienst zugreifen kann, konnte die Anfrage oder Anweisung nicht abgeschlossen werden. Weitere Informationen finden Sie in den Protokolldateien auf dem Citrix-Server.
33003	Citrix Streaming-Dienst: Keiner der für die Farm <*Farmname*> konfigurierten Citrix XML-Dienste antwortete auf diese XML-Dienst-Transaktion.	Fehler	Das Citrix Offline Plug-In konnte keinen der Citrix XML-Dienst-Hosts für die angegebene Farm kontaktieren. Versuchen Sie, den Webserver neu zu starten. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
33004	Citrix Streaming-Dienst: Die Konfiguration der Farm <*Farmname*> ist ungültig.	Fehler	Das Citrix Offline Plug-In hat ein Problem mit der angegebenen Serverfarm festgestellt. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
33005	Citrix Streaming-Dienst: Die Konfiguration enthält keine Informationen für Citrix Server.	Fehler	Für den Parameter **Farm<*n*>** in der Sitekonfigurationsdatei wurde kein Wert angegeben. Beheben Sie den Fehler in WebInterface.conf.
33006	Die Konfigurationsdatei RadeValidationRules.conf konnte nicht geladen werden. Überprüfen Sie, ob die Datei im Konfigurationsordner der Site zur Verfügung steht	Fehler	Die Konfigurationsdatei RadeValidationRules.conf fehlt oder Zugriff darauf ist nicht möglich. Stellen Sie sicher, dass die Datei nicht gelöscht wurde und dass die Berechtigungen so konfiguriert wurden, dass diese Datei gelesen werden kann.

33007	Die Konfigurationsdatei RadeValidationRules.conf kann nicht verwendet werden, da sie ungültige Regeln enthält. Überprüfen Sie, ob alle Regeln eine Syntax mit gültigen regulären Ausdrücken verwenden.	Fehler	Es liegt ein Problem bei der Konfigurationsdatei RadeValidationRules.conf vor. Alle Regeln in dieser Datei sollten in einer Syntax mit gültigen regulären Ausdrücken angegeben werden. Suchen Sie in der Datei nach Fehlern. Sie können auch mit der Aufgabe Site reparieren unter Sitewartung in der Citrix Webinterface Management Console die Site neu installieren. Alle Änderungen, die Sie in der Datei gemacht haben, werden verworfen.
34001	Die Konfiguration enthält keine Informationen für Citrix Server.	Fehler	Für den Parameter **Farm<*n*>** in der Konfigurationsdatei der Desktop Appliance Connector- oder XenApp Web-Site wurde kein Wert angegeben. Beheben Sie den Fehler in WebInterface.conf.
34002	Parsing der Provider Chain-Konfiguration nicht möglich.	Fehler	Es liegt ein Problem mit der Desktop Appliance Connector- oder XenApp Web-Site vor. Suchen Sie in der Datei WebInterface.conf nach Fehlern.
34003	<*Fehlerursache*> Der folgende Systemfehler ist aufgetreten: <*Fehlerbeschreibung*>	Fehler	Es liegt ein Problem mit der XenApp Services-Site vor. Details finden Sie am Ende der Fehlermeldung. Suchen Sie in der Datei WebInterface.conf nach Fehlern.
40001	Beim Auflisten der Ressourcen eines Benutzers ist ein Fehler aufgetreten. Es wurde eine nicht erkannte XML-Nachricht von einem Benutzergerät empfangen	Fehler	Das Citrix Online Plug-In hat ein Problem bei der Verbindungsherstellung zu den Citrix Servern festgestellt. Überprüfen Sie, ob das Citrix Online Plug-In auf dem Benutzergerät richtig konfiguriert ist.
40002	Beim Auflisten der Ressourcen eines Benutzers ist ein Fehler aufgetreten. Es wurde eine nicht erkannte XML-Nachricht von einem Benutzergerät empfangen	Fehler	Das Citrix Online Plug-In hat ein Problem bei der Verbindungsherstellung zu den Citrix Servern festgestellt. Überprüfen Sie, ob das Citrix Online Plug-In auf dem Benutzergerät richtig konfiguriert ist.

40003	Beim Wiederverbinden der Ressourcen eines Benutzers ist ein Fehler aufgetreten. Es wurde eine nicht erkannte XML-Nachricht von einem Benutzergerät empfangen	Fehler	Das Citrix Online Plug-In hat ein Problem bei der erneuten Verbindungsherstellung zu den Citrix Servern festgestellt. Überprüfen Sie, ob das Citrix Online Plug-In auf dem Benutzergerät richtig konfiguriert ist.
40004	<*IP-Adresse*> hat Citrix Online Plug-In-Konfiguration <*Dateiname*> angefordert. Diese existiert nicht.	Fehler	Stellen Sie sicher, dass die URL der Konfigurationsdatei im Dialogfeld Optionen des Citrix Online Plug-Ins auf dem Benutzergerät richtig eingegeben wurde .
40005	Beim Starten der Ressource eines Benutzers ist ein Fehler aufgetreten: <*Fehlerbeschreibung*>	Fehler	Das Citrix Online Plug-In hat ein Problem festgestellt. Details finden Sie am Ende der Fehlermeldung. Weitere Informationen finden Sie in den Protokolldateien auf den Citrix-Servern.
40006	Bei einer Desktopsteuerungsoperation ist ein Fehler aufgetreten. Es wurde eine nicht erkannte XML-Nachricht von einem Benutzergerät empfangen	Fehler	Das Citrix Online Plug-In hat beim Neustart des Desktops des Benutzers ein Problem festgestellt. Überprüfen Sie, ob das Citrix Online Plug-In auf dem Benutzergerät richtig konfiguriert ist.

Deaktivieren von Fehlermeldungen

In IIS können Sie die im Webinterface enthaltenen Fehlermeldungen deaktivieren und den zugrunde liegenden Fehler anzeigen. Bearbeiten Sie dazu die Datei web.config, die sich im Stammordner der Site befindet. Ändern Sie die folgende Zeile:

<customErrors mode="On" defaultRedirect="~/html/serverError.html">

in

<customErrors mode="Off" defaultRedirect="~/html/serverError.html">

Sie können auch eigene angepasste Fehlermeldungen anzeigen. Ändern Sie hierzu die Zeile zu:

<customErrors mode="On" defaultRedirect="~/html/*CustomErrorPage*">

wobei *EigeneFehlerSeite* der Name Ihrer angepassten Fehlerseite ist.

Konfigurieren der ADFS-Unterstützung für das Webinterface

Aktualisiert: 2014-11-24

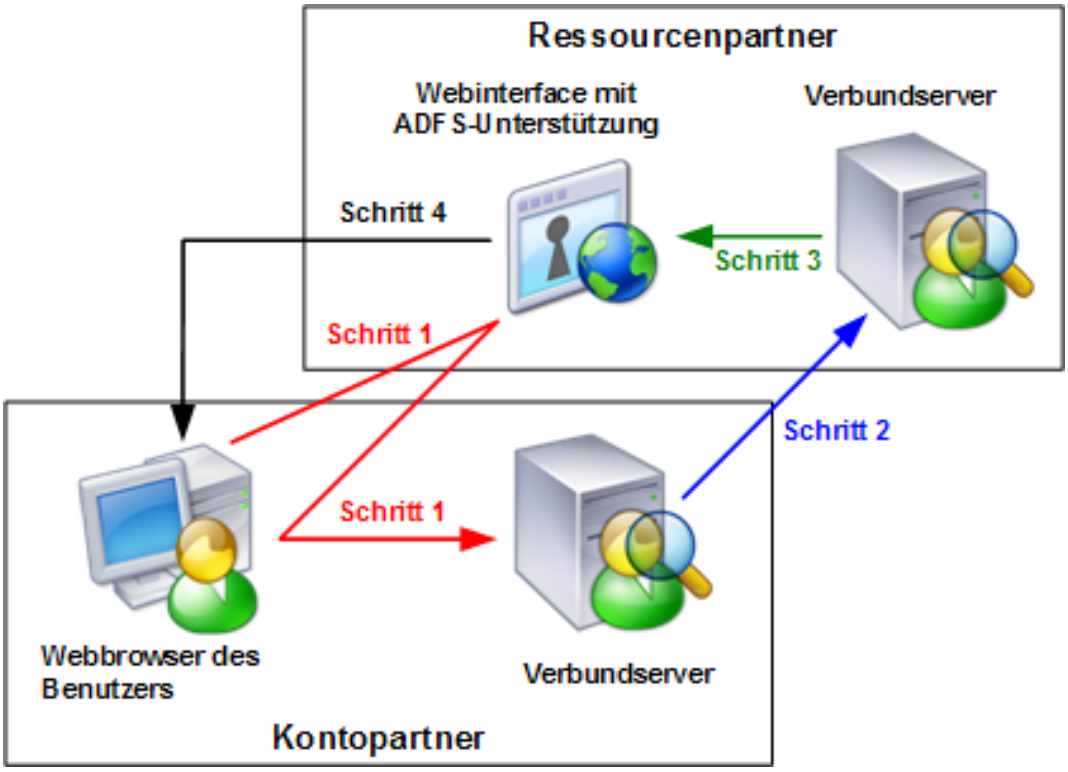
Active Directory-Verbunddienste-Unterstützung für das Webinterface ermöglicht dem Ressourcenpartner einer ADFS-Bereitstellung die Verwendung von XenApp. Administratoren können ADFS-Sites erstellen, damit Benutzer Zugriff auf Anwendungen und Inhalte auf dem Ressourcenpartner haben.

Wichtig: Für ADFS ist eine sichere Datenübertragung zwischen Webbrowser, Webserver und Verbundservern erforderlich. Webinterface-Benutzer müssen HTTPS/SSL für den Zugriff auf die Site verwenden.

Funktionsweise von ADFS-Sites

Wenn ein Benutzer auf einem Kontopartner auf eine Anwendung auf einem Ressourcenpartner zugreift, werden die folgenden Schritte ausgeführt:

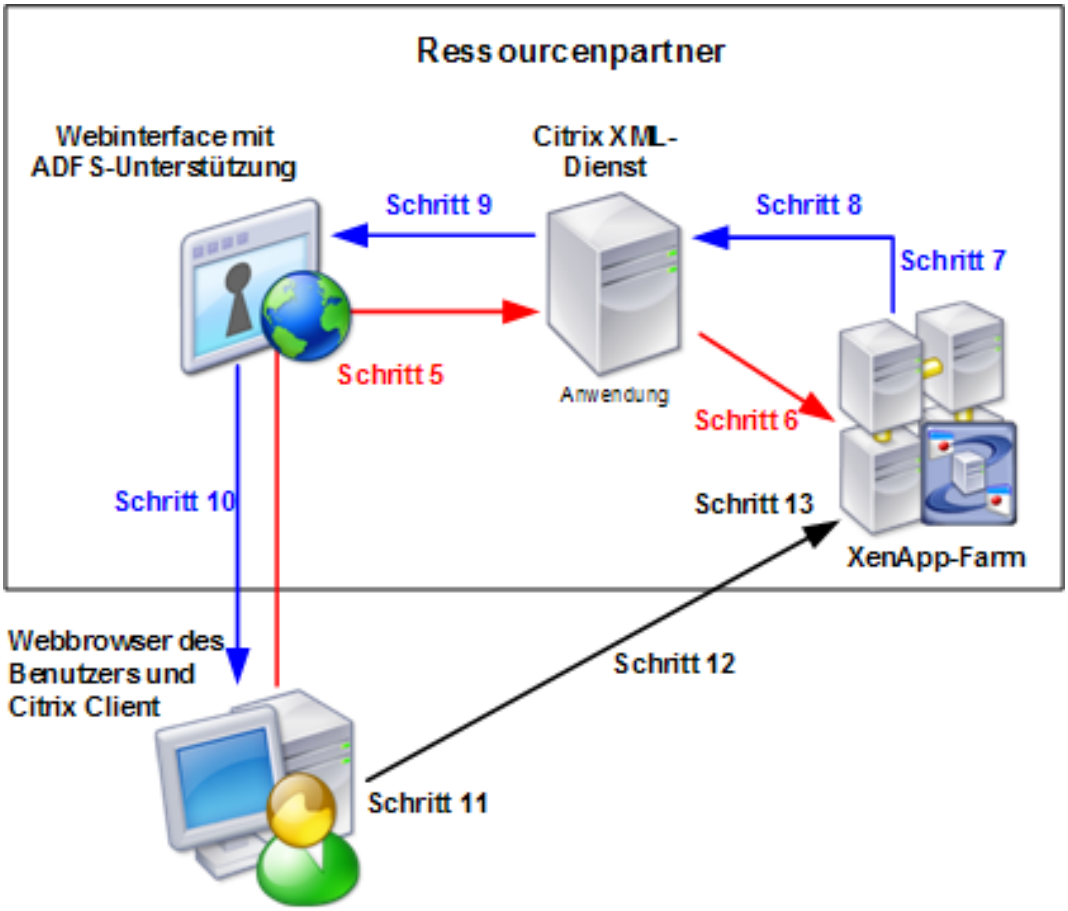
- **Schritt 1:** Ein Benutzer, der die Webinterface-Homepage auf dem Ressourcenpartner öffnet, wird an die Authentifizierungsseite des Kontopartners weitergeleitet.
- **Schritt 2:** Der Kontopartner authentifiziert den Benutzer und sendet ein Sicherheitstoken an den Ressourcenpartner zurück.
- **Schritt 3:** ADFS auf dem Ressourcenpartner überprüft das Sicherheitstoken, wandelt es in eine Windows-Identität um (die ein Schattenkonto darstellt) und leitet den Benutzer an die Webinterface-Seite Anmeldung weiter.



Schritt 4: Das Webinterface zeigt die Anwendungsgruppe an. Diese Abbildung veranschaulicht die Schritte, wenn Benutzer sich von der Kontopartnerdomäne anmelden, um auf ihre Anwendungsgruppen zuzugreifen.

- **Schritt 5:** Der Benutzer greift auf eine Anwendung zu, indem er auf einen Link auf der Seite klickt. Das Webinterface sendet eine Zugriffsanforderung an den Citrix XML-Dienst.
- **Schritt 6:** Der Citrix XML-Dienst erstellt Security Support Provider-Schnittstellen-Daten und sendet diese an einen XenApp-Server.
- **Schritt 7:** Der Server verwendet die Security Support Provider-Schnittstellen-Daten zur Authentifizierung des Benutzers und speichert zur späteren Authentifizierung ein Anmeldetoken.
- **Schritt 8:** Der Server erstellt ein Startticket zur eindeutigen Darstellung des gespeicherten Anmeldetokens und sendet dieses Ticket an den Citrix XML-Dienst zurück.
- **Schritt 9:** Der Citrix XML-Dienst sendet das Startticket an das Webinterface zurück.
- **Schritt 10:** Das Webinterface erstellt eine ICA-Datei mit dem Startticket und sendet diese an den Webbrowser des Benutzers.
- **Schritt 11:** Das Benutzergerät öffnet die ICA-Datei und versucht, eine ICA-Verbindung zum Server herzustellen.
- **Schritt 12:** Der Citrix Client sendet das Startticket an den XenApp-Server.

.



Schritt 13: Bei Eingang des Starttickets prüft der Server, ob das Ticket mit dem zuvor erstellten Anmeldetoken übereinstimmt, und verwendet dieses Anmeldetoken, um den Benutzer an der ICA-Sitzung auf dem Server anzumelden. Die ICA-Sitzung wird mit der Identität des Schattenkontos ausgeführt.Diese Abbildung veranschaulicht die Schritte, wenn Benutzer von der Kontopartnerdomäne auf Anwendungen zugreifen.

Je nach den für eine Site konfigurierten Einstellungen werden Benutzer, wenn sie sich abmelden, vom Webinterface oder dem Webinterface und ADFS abgemeldet. Wenn sie sich vom Webinterface *und* ADFS abmelden, werden sie von allen ADFS-Anwendungen abgemeldet.

Vor dem Erstellen von ADFS-Sites

Vor dem Erstellen einer ADFS-Site müssen Sie die nachstehend beschriebenen Schritte ausführen. Das Auslassen von Schritten kann zur Folge haben, dass Sie keine Sites erstellen können.

- Synchronisieren Sie die Uhrzeit auf den Verbundservern des Kontopartners und des Ressourcenpartners mit einem Zeitunterschied von maximal fünf Minuten. Andernfalls werden die vom Kontopartner erstellten Sicherheitstoken unter Umständen nicht vom Ressourcenpartner akzeptiert, weil die Token scheinbar abgelaufen sind. Zur Vermeidung dieses Problems müssen beide Organisationen ihre Server mit demselben Internetzeitserver synchronisieren. Weitere Informationen finden Sie unter Herstellen einer Vertrauensstellung zwischen Domänen.

- Vergewissern Sie sich, dass Verbund- und Webserver des Ressourcenpartners auf die Zertifikatsperrlisten (Certificate Revocation List, CRL) der Zertifizierungsstelle zugreifen können. ADFS kann fehlschlagen, wenn die Server nicht garantieren können, dass ein Zertifikat nicht gesperrt wurde. Weitere Informationen finden Sie unter Herstellen einer Vertrauensstellung zwischen Domänen.

- Stellen Sie sicher, dass alle Server in der Bereitstellung für den Verbund als vertrauenswürdig angesehen werden. Weitere Informationen finden Sie unter Konfigurieren der Delegierung für die Server in der Bereitstellung.

- Richten Sie in der Domäne des Ressourcenpartners Schattenkonten für jeden externen Benutzer ein, der sich beim Webinterface über ADFS authentifizieren kann. Weitere Informationen finden Sie unter Einrichten von Schattenkonten.

- Installieren Sie XenApp und stellen Sie sicher, dass der Citrix XML-Dienst den Port für IIS freigegeben hat und IIS HTTPS unterstützt.

- Stellen Sie eine Vertrauensstellung zwischen dem Webinterface-Server und anderen Servern in der Farm her, auf denen der Citrix XML-Dienst ausgeführt wird, den das Webinterface kontaktiert. Weitere Informationen finden Sie unter Verwenden von Workspace Control mit integrierten Authentifizierungsmethoden für XenApp Web-Sites.

Wichtig: Die Installation von ADFS wird in diesem Abschnitt nicht beschrieben. Sie müssen über eine funktionstüchtige ADFS-Installation und externe Benutzerkonten verfügen, die auf ADFS-fähige Anwendungen auf einem Ressourcenpartner zugreifen können, bevor Sie versuchen, eine ADFS-Site zu erstellen.

Softwareanforderungen für ADFS

Folgende Software muss in Ihrer Umgebung installiert und konfiguriert sein:

- Windows Server 2008 oder Windows Server 2003 R2 für den Verbund- und Webserver. Für den Webserver werden nur 32-Bit-Versionen von Windows Server 2008 und Windows Server 2003 R2 unterstützt.

- Active Directory-Verbunddienste (ADFS) auf dem Ressourcen- und dem Kontopartner. Der Ansprüche unterstützende Web Agent und der tokenbasierte ADFS-Web Agent müssen installiert sein.

Herstellen einer Vertrauensstellung zwischen Domänen

Die hier beschriebene Bereitstellung besteht aus zwei Domänen (in eigenen Gesamtstrukturen), d. h. einer Domäne für den Kontopartner und einer Domäne für den Ressourcenpartner. Hinweis: Die erforderlichen Komponenten müssen nicht auf separaten Computern installiert sein.

So stellen Sie eine Vertrauensstellung zwischen Domänen her

1. Vergewissern Sie sich, dass die folgenden Komponenten vorhanden sind. Kontopartner:

   - Domänencontroller
   - Verbundserver
   - Benutzergeräte

   Ressourcenpartner:

   - Domänencontroller
   - Verbundserver
   - Webserver
   - Einen oder mehrere Server für eine XenApp-Farm

   Die Verbundserver müssen auf Computern gehostet werden, auf denen Windows Server 2008 oder Windows Server 2003 R2 ausgeführt wird und auf denen die Serverrolle Active Directory-Verbunddienste installiert ist.

   Der Webserver muss auf einem Computer gehostet werden, auf dem eine 32-Bit-Version von Windows Server 2008 oder Windows Server 2003 R2 ausgeführt wird. Die Rollendienste Ansprüche unterstützender Agent und Windows-Token-basierter Agent müssen ebenso wie *alle* Rollendienste für die Serverrolle Webserver (IIS) installiert sein.

2. Fordern Sie separate Serverzertifikate für den Webserver und beide Verbundserver an.

   - Die Zertifikate müssen von einer vertrauenswürdigen Organisation, einer sogenannten Zertifizierungsstelle, signiert sein.
   - Da das Serverzertifikat einen bestimmten Computer identifiziert, müssen Sie den vollqualifizierten Domänennamen (FQDN) jedes Servers kennen, beispielsweise "xenappserver1.domäne.com".
   - Installieren Sie das Webserverzertifikat in Microsoft Internetinformationsdienste (IIS), um die IIS-Standardwebsite für SSL-Verkehr zu aktivieren.
   - Installieren Sie Verbundserverzertifikate mit dem Zertifikate-Snap-In der Microsoft Management Console (MMC). Weitere Informationen finden Sie in der *Schrittweisen Anleitung zur Microsoft Management Console* unter http://technet.microsoft.com/.

3. Um sicherzustellen, dass der Verbundserver des Ressourcenpartners dem Verbundserver des Kontopartners vertraut, installieren Sie das Verbundzertifikat des Kontopartners im Speicher "Vertrauenswürdige Stammzertifizierungsstellen" auf dem Verbundserver des Ressourcenpartners.

4. Um sicherzustellen, dass der Webserver dem Verbundserver des Ressourcenpartners vertraut, installieren Sie das Verbundzertifikat des Ressourcenpartners im Speicher "Vertrauenswürdige Stammzertifizierungsstellen" des Webservers.

   Wichtig: Der Ressourcenverbund- und der Webserver müssen in der Lage sein, auf die Zertifikatsperrlisten (CRLs) der Zertifizierungsstelle zuzugreifen. Der

Ressourcenverbundserver muss Zugriff auf die Zertifizierungsstelle des Kontopartners haben, während der Webserver Zugriff auf die Zertifizierungsstelle des Ressourcenpartners benötigt. ADFS kann fehlschlagen, wenn die Server nicht garantieren können, dass ein Zertifikat nicht gesperrt wurde.

5. Öffnen Sie auf dem Verbundserver des Ressourcenpartners das MMC-Snap-In Active Directory-Verbunddienste.

6. Wählen Sie im linken Bereich Verbunddienst > Vertrauensrichtlinie > Partnerorganisationen > Kontopartner und wählen Sie dann den Namen des Kontopartners aus.

7. Klicken Sie im Bereich Aktionen auf Eigenschaften.

8. Aktivieren Sie auf der Registerkarte Ressourcenkonten die Option Ressourcenkonten sind für alle Benutzer vorhanden und klicken Sie auf OK.

9. Synchronisieren Sie mit dem gleichen Internetzeitserver die Uhrzeit auf den Verbundservern des Kontopartners und des Ressourcenpartners mit einem Zeitunterschied von maximal fünf Minuten. Andernfalls werden die vom Kontopartner erstellten Sicherheitstoken unter Umständen nicht vom Ressourcenpartner akzeptiert, weil die Token scheinbar abgelaufen sind. Ressourcen- und Kontopartner können sich in unterschiedlichen Zeitzonen befinden, müssen zeitlich jedoch richtig synchronisiert sein. Beispiel: Der Kontopartner befindet sich in New York und ist auf 16 Uhr EST (Eastern Standard Time) eingestellt. Der Ressourcenpartner befindet sich in Kalifornien und ist auf zwischen 12.55 und 13.05 Uhr PST (Pacific Standard Time) eingestellt. (Der Zeitunterschied zwischen den beiden Zeitzonen (EST und PST) beträgt drei Stunden.)

10. Öffnen Sie auf dem Webserver das MMC-Snap-In Internetinformationsdienste-Manager.

11. Wählen Sie Ihren Webserver im linken Bereich aus und klicken Sie unter Ansicht "Features" auf Verbunddienst-URL.

12. Geben Sie auf der Seite Verbunddienst-URL die URL des Ressourcenpartner-Verbundservers ein und klicken Sie im Bereich Aktionen auf Übernehmen.

Konfigurieren der Delegierung für die Server in der Bereitstellung

Aktualisiert: 2014-11-24

Sie müssen sicherstellen, dass allen von Ihnen bereitgestellten Servern für die Delegierung vertraut wird. Führen Sie zu diesem Zweck die folgenden Aufgaben aus. Sie müssen dabei auf dem Domänencontroller der Ressourcenpartnerdomäne als Domänenadministrator angemeldet sein.

So stellen Sie sicher, dass sich die Ressourcenpartnerdomäne auf der richtigen Funktionsebene befindet

Wichtig: Zum Heraufstufen der Domänenebene müssen alle Domänencontroller in der Domäne unter Windows Server 2008 oder Windows Server 2003 installiert sein. Stufen Sie die Domänenfunktionsebene nicht auf Windows Server 2008 herauf, wenn Sie einen Domänencontroller besitzen, auf dem Windows Server 2003 ausgeführt wird, oder wenn Sie einen solchen einrichten möchten. Nachdem die Domänenfunktionsebene heraufgesetzt worden ist, kann sie nicht wieder auf eine niedrigere Stufe zurückgesetzt werden.

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Domänen und -Vertrauensstellungen.

2. Wählen Sie im linken Bereich den Domänennamen des Ressourcenpartners aus und klicken Sie im Bereich Aktionen auf Eigenschaften.

3. Wenn sich die Domäne nicht auf der höchst möglichen Funktionsebene befindet, wählen Sie den Domänennamen aus und klicken Sie im Bereich Aktionen auf Domänenfunktionsebene heraufstufen.

4. Um die Domänenfunktionsebene heraufzustufen, klicken Sie auf die entsprechende Ebene und klicken Sie auf Heraufstufen.

So vertrauen Sie dem Webinterface-Server für die Delegierung

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Benutzer und -Computer.
2. Klicken Sie im Menü Ansicht auf Erweiterte Funktionen.
3. Klicken Sie im linken Bereich unter dem Domänennamen des Ressourcenpartners auf den Knoten Computers und wählen Sie den Webinterface-Server aus.
4. Klicken Sie im Bereich Aktionen auf Eigenschaften.Klicken Sie im Bereich Aktionen auf Eigenschaften.
5. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Beliebiges Authentifizierungsprotokoll verwenden und klicken Sie dann auf Hinzufügen.
6. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.
7. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst ausgeführt wird, und klicken Sie auf OK.
8. Wählen Sie in der Liste den Diensttyp HTTP aus und klicken Sie auf OK.
9. Überprüfen Sie auf der Registerkarte Delegierung, ob der Diensttyp HTTP für den XenApp-Server in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.
10. Wiederholen Sie den Vorgang für jeden Server in der Farm, auf dem der Citrix XML-Dienst ausgeführt wird und zu dem das Webinterface gemäß der Konfiguration eine Verbindung herstellen soll.

So vertrauen Sie dem Citrix XML-Dienst-Server für die Delegierung

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Benutzer und -Computer.

2. Klicken Sie im linken Bereich unter dem Domänennamen des Ressourcenpartners auf den Knoten Computers und wählen Sie den Server aus, auf dem der Citrix XML-Dienst ausgeführt wird, zu dem das Webinterface eine Verbindung herstellen soll.

3. Klicken Sie im Bereich Aktionen auf Eigenschaften.

4. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Nur Kerberos verwenden und klicken Sie dann auf Hinzufügen.

5. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.

6. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Servers ein, auf dem der Citrix XML-Dienst ausgeführt wird, und klicken Sie auf OK.

7. Wählen Sie in der Liste den Diensttyp HOST aus und klicken Sie auf OK.

8. Überprüfen Sie auf der Registerkarte Delegierung, ob der Diensttyp HOST für den Server, auf dem der Citrix XML-Dienst ausgeführt wird, in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.

9. Wiederholen Sie den Vorgang für jeden Server in der Farm, auf dem der Citrix XML-Dienst ausgeführt wird und zu dem das Webinterface gemäß der Konfiguration eine Verbindung herstellen soll.

So legen Sie fest, auf welche Ressourcen über den XenApp-Server zugegriffen werden kann

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Benutzer und -Computer.
2. Klicken Sie im linken Bereich unter dem Domänennamen des Ressourcenpartners auf den Knoten Computers und wählen Sie den XenApp-Server aus.
3. Klicken Sie im Bereich Aktionen auf Eigenschaften.
4. Klicken Sie auf der Registerkarte Delegierung auf Computer bei Delegierungen angegebener Dienste vertrauen und Nur Kerberos verwenden und klicken Sie dann auf Hinzufügen.
5. Klicken Sie im Dialogfeld Dienste hinzufügen auf Benutzer oder Computer.
6. Geben Sie im Dialogfeld Benutzer oder Computer auswählen im Feld Geben Sie die zu verwendenden Objektnamen ein den Namen des Ressourcenpartner-Domänencontrollers ein und klicken Sie dann auf OK.
7. Wählen Sie die Diensttypen cifs und ldap aus der Liste aus und klicken Sie auf OK.

   Hinweis: Wenn für den Dienst ldap zwei Optionen angezeigt werden, wählen Sie die Option aus, die mit dem vollqualifizierten Domänennamen des Domänencontrollers übereinstimmt.
8. Überprüfen Sie auf der Registerkarte Delegierung, ob die Diensttypen cifs und ldap für den Domänencontroller des Ressourcenpartners in der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann angezeigt wird, und klicken Sie auf OK.
9. Wiederholen Sie den Vorgang für jeden XenApp-Server in der Farm.

Konfigurieren von Servern für eingeschränkte Delegierung

Aus Sicherheitsgründen müssen Sie alle XenApp-Server für eingeschränkte Delegierung konfigurieren. Damit Benutzer Zugriff auf Ressourcen auf diesen Servern haben, müssen Sie die betreffenden Dienste mit dem MMC-Snap-In Active Directory-Benutzer und -Computer der Liste Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann hinzufügen. Damit sich Benutzer beispielsweise bei einem Webserver auf Host "Adam" authentifizieren können, fügen Sie den Dienst http für Server "Adam" hinzu. Damit sich Benutzer bei einem SQL-Server auf Host "Eva" authentifizieren können, fügen Sie den Dienst MSSQLSvc für Server "Eva" hinzu.

Weitere Informationen finden Sie im Whitepaper *Service Principal Names and Delegation in Presentation Server* (CTX110784) im Citrix Knowledge Center.

Konfigurieren eines Zeitlimits für den Zugriff auf Ressourcen

Vorsicht: Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die nur durch eine Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr.

Standardmäßig können ADFS-Benutzer 15 Minuten lang auf Ressourcen in einem Netzwerk zugreifen. Sie können diesen Zeitraum erhöhen, indem Sie auf dem Server, auf dem der Citrix XML-Dienst ausgeführt wird, den folgenden Registrierungseintrag ändern:

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

Dieser Wert gibt in Minuten an, wie lange Benutzer nach Beginn einer Sitzung auf Ressourcen zugreifen können.

Die Sicherheitsrichtlinie für Domänen bestimmt den zulässigen Höchstwert für S4ULifetime. Wenn Sie einen Wert für "S4UTicketLifetime" festlegen, der über dem auf der Domänenebene festgelegten Wert liegt, hat die Einstellung auf Domänenebene Vorrang.

So konfigurieren Sie ein Zeitlimit für den Zugriff auf Ressourcen auf Domänenebene

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Sicherheitsrichtlinie für Domänen.
2. Klicken Sie im linken Bereich auf Kontorichtlinien > Kerberos-Richtlinie.
3. Aktivieren Sie im Ergebnisbereich Max. Gültigkeitsdauer des Diensttickets.
4. Klicken Sie im Bereich Aktionen auf Eigenschaften.
5. Geben Sie das gewünschte Zeitlimit (in Minuten) im Feld Das Ticket läuft ab in ein.

Wenn Sie für den Zugriff auf Ressourcen über den XenApp-Server kein Zeitlimit konfigurieren möchten, wählen Sie die Option Beliebiges Authentifizierungsprotokoll verwenden. Mit dieser Option wird der für "S4UTicketLifetime" angegebene Wert ignoriert. Weitere Informationen finden Sie auf der Microsoft Website unter http://support.microsoft.com/.

Einrichten von Schattenkonten

Um Zugriff auf Anwendungen zu geben, benötigt XenApp echte Windows-Konten. Daher müssen Sie in der Ressourcenpartnerdomäne für jeden externen Benutzer, der sich beim Webinterface über ADFS authentifiziert, manuell ein Schattenkonto erstellen.

Wenn in der Kontopartnerdomäne viele Benutzer sind, die auf Anwendungen und Inhalte in der Ressourcenpartnerdomäne zugreifen, können Sie ein Drittanbieterprodukt zum raschen Erstellen von Schattenkonten für Benutzer in Active Directory verwenden.

Zum Erstellen von Schattenkonten führen Sie die folgenden Aufgaben aus. Sie müssen dabei auf dem Domänencontroller der Ressourcenpartnerdomäne als Domänenadministrator angemeldet sein.

So fügen Sie UPN-Suffixe hinzu

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Domänen und -Vertrauensstellungen.
2. Markieren Sie im linken Bereich Active Directory-Domänen und -Vertrauensstellungen.
3. Klicken Sie im Bereich Aktionen auf Eigenschaften.
4. Fügen Sie für jeden externen Kontopartner ein UPN-Suffix hinzu. Wenn sich der Kontopartner beispielsweise in der Active Directory-Domäne "Domäne.com" befindet, fügen Sie Domäne.com als UPN-Suffix hinzu.

So definieren Sie den Benutzer des Schattenkontos

1. Öffnen Sie auf dem Domänencontroller des Ressourcenpartners das MMC-Snap-In Active Directory-Benutzer und -Computer.
2. Wählen Sie im linken Bereich den Domänennamen des Ressourcenpartners aus.
3. Klicken Sie im Bereich Aktionen auf Neu > Benutzer.
4. Geben Sie den Vornamen, die Initialen und den Nachnamen des Benutzers in den entsprechenden Feldern ein.
5. Geben Sie im Feld Benutzeranmeldename den Kontonamen ein. Vergewissern Sie sich, dass dieser Name mit dem Namen auf dem Kontopartner des Domänencontrollers übereinstimmt.
6. Wählen Sie in der Liste das externe UPN-Suffix aus und klicken Sie auf Weiter.
7. Geben Sie in den Feldern Kennwort und Kennwort bestätigen ein Kennwort ein, das Ihrer Kennwortrichtlinie entspricht. Dieses Kennwort wird niemals verwendet, weil sich der Benutzer über ADFS authentifiziert.
8. Deaktivieren Sie das Kontrollkästchen Benutzer muss Kennwort bei der nächsten Anmeldung ändern.
9. Aktivieren Sie die Kontrollkästchen Benutzer kann das Kennwort nicht ändern und Kennwort läuft nie ab.
10. Klicken Sie auf Weiter und dann auf Fertig stellen.

Erstellen von ADFS-Sites

Führen Sie in der Citrix Webinterface Management Console die Aufgabe Site erstellen aus und konfigurieren Sie die Webinterface-Site zur Verwendung von ADFS für die Authentifizierung.

Hinweis: Die Bereitstellung von virtuellen XenDesktop-Desktops wird in ADFS-Umgebungen nicht unterstützt. Außerdem werden der Client für Java und die eingebettete Remotedesktopverbindungssoftware (RDP) nicht für den Zugriff auf mit ADFS integrierte Sites unterstützt.

So erstellen Sie ADFS-Sites

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf den Container Citrix Webinterface.
3. Klicken Sie im Bereich Aktionen auf Site erstellen.
4. Wählen Sie XenApp Web und klicken Sie auf Weiter.
5. Geben Sie auf der Seite IIS-Speicherort angeben den Pfad und den Namen für die Site an. Klicken Sie auf Weiter.
6. Wählen Sie auf der Seite Authentifizierungspunkt festlegen die Option Microsoft ADFS-Kontopartner. Legen Sie die Rückgabe-URL für das Webinterface fest und klicken Sie auf Weiter.
7. Bestätigen Sie die Einstellungen für die neue Site und klicken Sie auf Weiter, um die Site zu erstellen.

Konfigurieren von Sites als Active Directory-Verbunddienste-Anwendungen

Nach dem Erstellen einer Site müssen Sie diese als ADFS-Anwendung konfigurieren, damit sie vom Verbundserver erkannt wird.

So konfigurieren Sie Sites als Active Directory-Verbunddienste-Anwendungen

1. Öffnen Sie auf dem Verbundserver des Ressourcenpartners das MMC-Snap-In Active Directory-Verbunddienste.
2. Wählen Sie im linken Bereich Verbunddienst > Vertrauensrichtlinie > Eigene Organisation > Anwendungen.
3. Klicken Sie im Bereich Aktionen auf Neu > Anwendung.
4. Klicken Sie auf Weiter, wählen Sie Ansprüche unterstützende Anwendung und klicken Sie erneut auf Weiter.
5. Geben Sie einen Namen für die Site im Feld Anwendungsanzeigename ein.
6. Geben Sie im Feld Anwendungs-URL die URL der Webinterface-Site *genau so* ein, wie sie im Feld Webinterface-Rückgabe-URL bei der Siteerstellung angezeigt wurde, und klicken Sie auf Weiter.

   Hinweis: Achten sie darauf, dass Sie HTTPS und den vollqualifizierten Domänennamen des Webservers verwenden.
7. Aktivieren Sie das Kontrollkästchen UPN (User Principal Name) und klicken Sie auf Weiter.
8. Stellen Sie sicher, dass das Kontrollkästchen Diese Anwendung aktivieren aktiviert ist, und klicken Sie auf Weiter.
9. Klicken Sie auf Fertig stellen, um Ihre Site als ADFS-Anwendung hinzuzufügen.

Testen der Bereitstellung

Aktualisiert: 2014-12-02

Nach dem Konfigurieren der Site als ADFS-Anwendung sollten Sie die Bereitstellung testen, um sicherzustellen, dass die Verbindung zwischen Kontopartner und Ressourcenpartner einwandfrei funktioniert.

So testen Sie die Webinterface-ADFS-Bereitstellung

1. Melden Sie sich auf einem Benutzergerät in der Kontopartnerdomäne an.
2. Öffnen Sie einen Webbrowser und geben Sie die URL mit dem vollqualifizierten Domänennamen der zuvor erstellten Webinterface-Site mit ADFS-Integration ein.

   Die Anwendungsgruppe wird angezeigt.

   Hinweis: Wenn Sie ADFS nicht für die integrierte Authentifizierung konfiguriert haben, werden Sie unter Umständen zur Eingabe der Anmeldeinformationen oder zum Einlegen einer Smartcard aufgefordert.
3. Wenn Sie das Citrix Online Plug-In noch nicht installiert haben, tun Sie dies jetzt. Weitere Informationen finden Sie in der archivierten Dokumentation für das Online Plug-In für Windows.
4. Klicken Sie auf eine Anwendung, um darauf zuzugreifen.

Abmelden von ADFS-Sites

Mit der Aufgabe Authentifizierungsmethoden in der Citrix Webinterface Management Console geben Sie an, ob sich Benutzer durch Klicken auf die Schaltflächen Abmelden oder Trennen auf der Website wie folgt abmelden:

- nur vom Webinterface
- vom Webinterface und vom ADFS-Verbunddienst

Wenn Sie angeben, dass sich Benutzer nur vom Webinterface abmelden, werden sie an die Webinterface-Abmeldeseite weitergeleitet. Wenn Sie angeben, dass sich Benutzer vom Webinterface und vom ADFS-Verbunddienst abmelden, werden sie zur Abmeldeseite des Verbunddienstes weitergeleitet und bei allen ADFS-Anwendungen abgemeldet.

Hinweis: Benutzer, die sich über ADFS authentifizieren, können ihre XenApp-Sitzungen nicht entsperren, da sie ihre Kennwörter nicht kennen. Um Sitzungen zu entsperren, müssen sich Benutzer vom Webinterface abmelden, sich dann erneut mit ADFS-Authentifizierung anmelden und ihre Anwendungen neu starten. Hierdurch wird die Sperrung der vorherigen Sitzung aufgehoben und das neue Fenster wird geschlossen.

So geben Sie an, von welchen Diensten sich Benutzer abmelden

1. Klicken Sie im Windows-Menü Start auf Alle Programme > Citrix > Managementkonsolen > Citrix Webinterface-Verwaltung.
2. Klicken Sie im linken Bereich der Citrix Webinterface Management Console auf XenApp Web-Sites und wählen Sie im Ergebnisbereich Ihre Site mit ADFS-Integration aus.
3. Klicken Sie im Bereich Aktionen auf Authentifizierungsmethoden.
4. Um anzugeben, dass sich Benutzer vom Webinterface und dem ADFS-Verbunddienst abmelden, aktivieren Sie das Kontrollkästchen Globale Abmeldung durchführen. Um anzugeben, dass sich Benutzer nur vom Webinterface abmelden, deaktivieren Sie das Kontrollkästchen Globale Abmeldung durchführen.