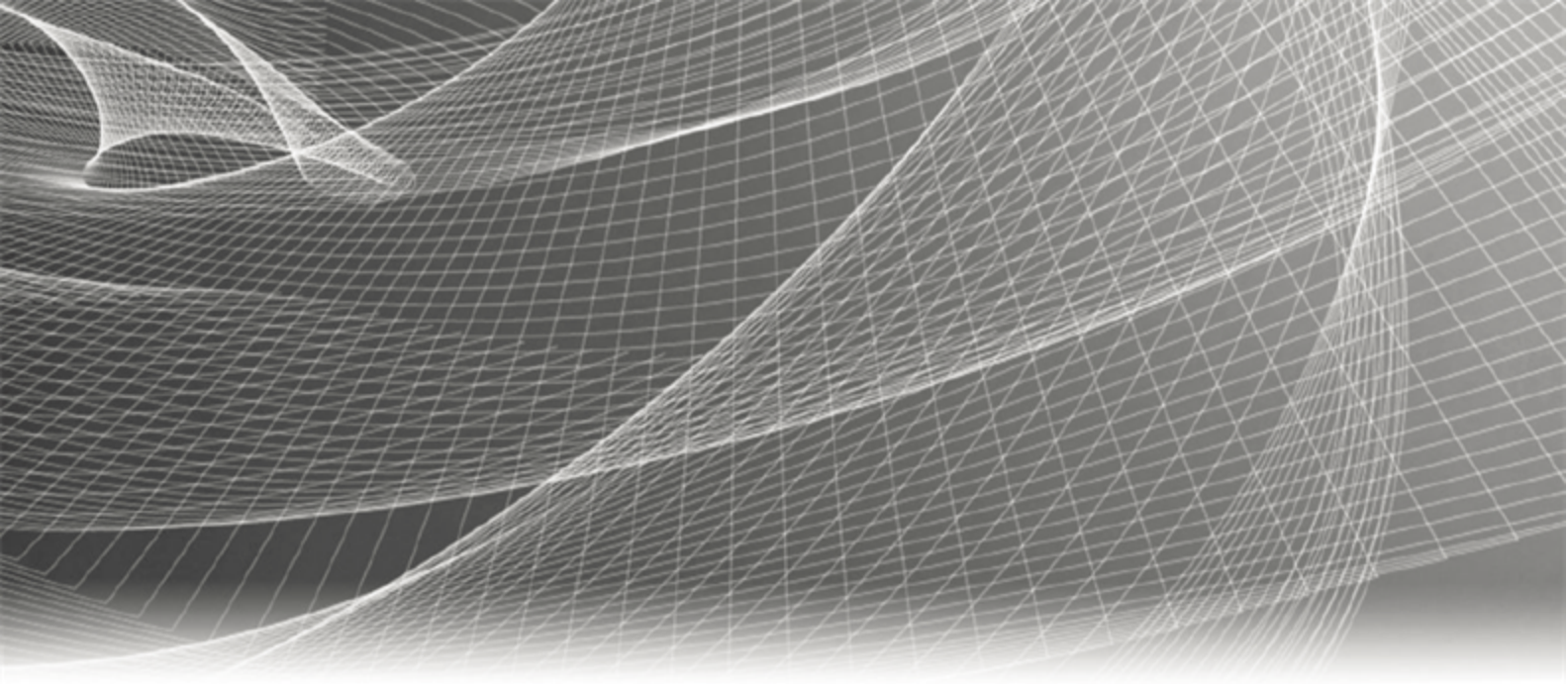

RSA SECURID® ACCESS

RSA® Authentifizierungs-Agent 2.0 für Citrix StoreFront

Administratorhandbuch

Kontaktinformationen

RSA Link (https://community.rsa.com) enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Dell, RSA, das RSA-Logo, EMC und andere Marken sind Marken von Dell Inc. oder ihren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein. Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell Inc. oder ihren Tochtergesellschaften und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens Dell Inc. ausgelegt werden.

Lizenzen von Drittanbietern

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen,die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Nutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von Dell ist eine entsprechende Softwarelizenz erforderlich.

Dell Inc. ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. DELL INC. MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.

März 2019

Inhalt

Vorwort

Zielgruppe

Dieses Handbuch richtet sich an Netzwerk- und Systemadministratoren, die RSA Authentication Agent for Citrix StoreFront bereitstellen, konfigurieren und verwalten.

In diesem Dokument wird davon ausgegangen, dass Sie Erfahrung mit Citrix StoreFront haben. Außerdem setzt es voraus, dass Sie Erfahrung mit RSA Authentication Manager oder dem Cloudauthentifizierungsservice haben oder dass Sie mit einem Administrator für diese Produkte zusammenarbeiten.

Support und Service

Sie können auf RSA Link unter https://community.rsa.com auf die Community- und Supportinformationen zugreifen. RSA Link enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

RSA Ready Partner Program

Die Website des RSA Ready Partner Program unter www.rsaready.com enthält Informationen über Hardware- und Softwareprodukte von Drittanbietern, die für den Einsatz mit RSA-Produkten zertifiziert sind. Die Website stellt Leitfäden für die Implementierung mit detaillierten Anweisungen sowie weitere Informationen zur Interoperabilität von RSA- und Drittanbieterprodukten bereit.

Kapitel 1: RSA Authentication Agent for Citrix StoreFront

Übersicht über RSA Authentication Agent for Citrix StoreFront

RSA Authentication Agent for Citrix StoreFront ist Authentifizierungssoftware, die Citrix StoreFront um zusätzliche Methoden zur Authentifizierung von Nutzern innerhalb oder außerhalb der Unternehmens-Firewall erweitert. Beim Versuch, auf einen StoreFront-Store zuzugreifen, geben Nutzer ihre Nutzernamen und Passwörter für die primäre Authentifizierung an und Agent for Citrix StoreFront fordert Sie auf, je nach konfiguriertem Authentifizierungsmodus eine oder mehrere zusätzliche Authentifizierungsmethoden abzuschließen. Der Agent unterstützt die folgenden Authentifizierungsmodi:

- **RSA Cloudauthentifizierungsservice (CAS-Modus)**. Der Agent stellt eine Verbindung zu Ihrer vorhandenen Cloudauthentifizierungsservice-Bereitstellung her, die folgende Authentifizierungsmethoden unterstützt:
  - Genehmigen
  - Authenticate Tokencode
  - Gerätebiometrie
  - SMS-Tokencode
  - Telefonischer Tokencode
  - RSA SecurID-Token (erfordert Integration zwischen Cloudauthentifizierungsservice und RSA Authentication Manager)
- **RSA Authentication Manager Mit REST-Protokoll (AM REST-Modus)**. Der Agent stellt eine Verbindung zu Ihrer vorhandenen RSA Authentication Manager-Bereitstellung mithilfe des REST-Protokolls her, die folgende Authentifizierungsmethoden unterstützt:
  - RSA SecurID-Token
  - Authenticate Tokencode (erfordert Integration zwischen Cloudauthentifizierungsservice und RSA Authentication Manager)
- **RSA Authentication Manager Mit UDP-Protokoll (AM UDP-Modus)**. Der Agent stellt eine Verbindung zu Ihrer vorhandenen RSA Authentication Manager-Bereitstellung mithilfe des UDP-Protokolls her, das RSA SecurID Token und Risk-Based Authentication (RBA) unterstützt: Weitere Informationen finden Sie unter Risk-based Authentication Auf der gegenüberliegenden Seite.

Eine vollständige Dokumentation für RSA Authentication Manager und den Cloudauthentifizierungsservice ist auf RSA Linkverfügbar.

Wenn Sie die Authentifizierung auf Nutzer außerhalb der Unternehmens-Firewall ausdehnen möchten, müssen Sie den Agent in Verbindung mit Citrix NetScaler Gateway und Citrix Delegated Forms Authentication (DFA) verwenden. Weitere Informationen finden Sie unter Citrix Delegated Forms Authentication auf Seite 59.

Agent for Citrix StoreFront ist mit FIPS (Federal Information Processing Standard) kompatibel, einem Computersicherheitsstandard der US-Regierung, der zur Genehmigung von Verschlüsselungsmodulen verwendet wird. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren von FIPS auf Windows Server-Betriebssystemen auf Seite 44.

RSA SecurID

RSA SecurID schützt den Zugriff mithilfe von Zwei-Faktor-Authentifizierung mit hardware- und softwarebasierten Token. Wenn der Agent for Citrix StoreFront Nutzer mit RSA SecurID authentifiziert, werden die Nutzer beim Versuch, sich bei einem StoreFront-Laden anzumelden, nach einem RSA SecurID-Passcode

gefragt. Der Agent überprüft den Passcode mithilfe von RSA Authentication Manager. Verläuft die Authentifizierung erfolgreich, gewährt StoreFront dem Nutzer Zugriff auf die geschützte Ressource.

Anweisungen zum Konfigurieren der SecurID-Authentifizierung finden Sie unter Vom Agent verwendete Citrix StoreFront-Nutzername- und Passwort-Funktionen auf Seite 39.

Risk-based Authentication

Risk-Based Authentication (RBA) nutzt Wissen über das Clientgerät und Nutzerverhalten, um das potenzielle Risiko einer Authentifizierungsanforderung zu bewerten. Bei Authentifizierungsversuchen mit erhöhtem Risiko müssen Nutzer ihre Identität weiter bestätigen. Wenn RBA zusammen mit Windows-Passwortintegration (WPI) aktiviert ist, wird ein Nutzer, der sich erfolgreich authentifiziert, bei einem Storefront-Store angemeldet und muss keine separaten Anmeldedaten eingeben. Weitere Informationen zu WPI finden Sie unter Windows-Passwortintegration (WPI) unten.

RBA wird nur unterstützt, wenn Agent for Citrix StoreFront im AM UDP-Modus konfiguriert ist. Weitere Informationen zur Integration des Agent mit RBA finden Sie unter Aktivieren der RSA Authentication Manager Risk-Based Authentication auf Seite 65.

Dienstprogramm für die automatische Registrierung des RSA Authentication Agent

Bei der Konfiguration im AM UDP-Modus muss Agent for Citrix StoreFront bei RSA Authentication Manager zur Authentifizierung von Nutzern registriert werden. Authentication Manager identifiziert Agents nach IP-Adresse und verwendet einen Node-Schlüssel, der für jeden Agent spezifisch ist, um Authentifizierungsinformationen während der Übertragung zu schützen.

Das Dienstprogramm für die automatische Registrierung des RSA Authentication Agent ist eine optionale Funktion von Agent for Citrix StoreFront, die nur im AM UDP-Modus unterstützt wird. Dieses Dienstprogramm registriert den Agent bei Authentication Manager und aktualisiert die IP-Adresse und den Node-Schlüssel nach Bedarf ohne manuelle Intervention.

Ziehen Sie die automatische Registrierung in Betracht, wenn Ihr Netzwerk DHCP (Dynamic Host Configuration Protocol) verwendet, um IP-Adressen zuzuweisen, oder in Umgebungen, die drahtlose und VPN-Verbindungen (Virtual Private Network) für den Zugriff auf das Unternehmensnetzwerk verwenden. Installationsanweisungen für das Dienstprogramm zur automatischen Registrierung werden unter Installieren des Agent auf Seite 27beschrieben.

Sie können das Dienstprogramm für die automatische Registrierung so konfigurieren, dass bestimmte Netzwerkadapter von der automatischen Registrierung von IP-Adressen ausgeschlossen werden. Weitere Informationen finden Sie unter Ausschließen bestimmter Netzwerkadapter von der automatischen Registrierung auf Seite 39.

Hinweis: Das Dienstprogramm zur automatischen Registrierung wird in einer Citrix StoreFront-Servergruppe nicht unterstützt. Wählen Sie das Dienstprogramm zur automatischen Registrierung nur aus, wenn die StoreFront-Bereitstellung aus einem einzigen Server ohne Load Balancer besteht.

Windows-Passwortintegration (WPI)

Die Windows-Passwortintegration ist eine optionale RSA Authentication Manager-Funktion, die Sie für Agent for Citrix StoreFront aktivieren können, wenn der Agent im AM UDP- oder AM REST-Modus konfiguriert ist.

Wenn die Funktion aktiviert ist, kann der Agent for Citrix StoreFront ein Windows-Passwort aus dem Authentication Manager abrufen und es bei der Anmeldung an Citrix StoreFront verwenden. Nutzer geben Windows-Passwörter nur bei der ersten Authentifizierung an. Zu diesem Zeitpunkt speichert der Agent die Windows-Passwörter mit Nutzerauthentifizierungsdaten im Authentication Manager. Bei späteren Authentifizierungen geben die Nutzer nur ihre Nutzernamen und RSA SecurID-Passcodes ein. Der Agent for Citrix StoreFront verwendet gespeicherte Passwörter zur Authentifizierung gegenüber Active Directory.

Wenn Nutzer das Windows-Passwort innerhalb einer Citrix StoreFront-Sitzung ändern, synchronisiert der Agent for Citrix StoreFront automatisch das Passwort in den entsprechenden Konten in der Authentication Manager-Datenbank. Wenn ein Nutzerpasswort außerhalb einer solchen Sitzung geändert wird, wird das im Authentication Manager gespeicherte Passwort nicht aktualisiert. Wenn jedoch später der Agent for Citrix StoreFront das gespeicherte Passwort abruft, wird der Nutzer aufgefordert, das richtige Passwort einzugeben, und das Passwort wird im Authentication Manager gespeichert.

Sie aktivieren WPI über die Einstellungen der Offline-Authentifizierungs-Policy in der Sicherheitskonsole. Sie können die Windows-Passwortintegration für alle Agent for Citrix StoreFront-Computer in der Datenbank aktivieren oder bestimmte Computer auswählen. Wenn der Agent im AM UDP-Modus konfiguriert ist, ist dies der einzige erforderliche Schritt.

Wenn der Agent im AM REST-Modus konfiguriert ist, müssen Sie auch die Sicherheitskonfigurationsdatei (**sdconf.rec**) und die Node-Schlüsseldatei (**<AgentName>_NodeSecret.zip**) aus dem Authentication Manager beziehen, sie auf jeden Agent-Computer kopieren und bei der Installation oder Konfiguration des Agent die jeweiligen Dateipfade angeben.

Hinweis: Wenn RSA Authentication Agent for Microsoft Windows bereits mit einem Node-Schlüssel auf dem Citrix StoreFront-Server installiert und konfiguriert ist, enthält Agent for Citrix StoreFront eine Option zur Verwendung desselben Node-Schlüssels, um WPI im AM REST-Modus zu aktivieren.

Weitere Informationen finden Sie in der Authentication Manager-Dokumentation auf RSA Link.

RSA Authentication Agent – Lokaler Offline-Service

Agent for Citrix StoreFront unterstützt die Offline-Authentifizierungsfunktion nicht, die von RSA Authentication Agent for Microsoft Windows bereitgestellt wird. Wenn Agent for Citrix StoreFront jedoch im AM UDP-Modus installiert ist, hängt die Windows-Passwortintegration vom lokalen Offline Service des RSA Authentication Agent ab. Wenn Sie Windows-Passwortintegration für einen der Agents verwenden, deaktivieren Sie diesen Service nicht.

Hinweis: Agent for Citrix StoreFront konfiguriert den Offline Local Service so, dass Nutzer-Offlinedaten nicht heruntergeladen werden.

Koexistenz mit RSA Authentication Agent for Microsoft Windows

RSA Authentication Agent for Microsoft Windows (der Windows-Agent) ist eine Authentifizierungssoftware, die die Anmeldung bei Windows Computern schützt, indem sie erfordert, dass Nutzer sich mit RSA SecurID authentifizieren. Agent for Citrix StoreFront und der Windows-Agent verwenden mehrere Produktkomponenten: Automatische Agent-Registrierung, SecurID-Authentifizierung und Offlineservice.

Beide Agents können auf einem Citrix StoreFront-Server mit den folgenden Einschränkungen installiert werden:

- Wenn Sie beide Agents installieren, empfiehlt RSA, zuerst den Windows-Agent zu installieren.
- Die Funktion der automatischen Agent-Registrierung kann nur von einem Agent gleichzeitig installiert werden.
- Wenn beide Produkte installiert sind, ist die Funktion zur Offline-Authentifizierung des Windows-Agent nicht verfügbar, da der Agent für Citrix StoreFront den Download von Offlinedaten deaktiviert. Dieser kann erneut aktiviert werden, indem ein Registrierungswert wie folgt geändert wird:
    1. Um den Registry Editor zu öffnen, klicken Sie auf **Start**, geben Sie **regedit** in das Suchfeld ein und klicken Sie auf **regedit** in der Ergebnisliste unter **Programme**.
    2. Öffnen Sie den Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT**
    3. Ändern Sie den Wert von **NoDADownload** (ein REG_DWORD) von **1** in **0**.

Hinweis: Wenn der Windows-Agent bereits mit einem Node-Schlüssel auf dem Citrix StoreFront-Server installiert und konfiguriert ist, enthält Agent for Citrix StoreFront eine Option zur Verwendung desselben Node-Schlüssels, um WPI im AM REST-Modus zu aktivieren. RSA empfiehlt, diese Option während der Erstinstallation auszuwählen, wenn Sie WPI aktivieren müssen, und die **WPI managen**-Einstellungen nur dann im Menü „SecurID-Optionen managen" zu verwenden, wenn Sie nach der Erstinstallation vom AM UDP-oder CAS-Modus in den AM REST-Modus wechseln.

Citrix StoreFront-Support für RSA Authentication Manager-Funktionen

Agent for Citrix StoreFront unterstützt diese Authentication Manager, wenn sie in AM UDP- oder AM REST-Modus installiert sind:

- RSA SecurID-Authentifizierung mit nativem RSA SecurID-Protokoll
- On-Demand-Authentifizierung (ODA) mit nativem RSA SecurID-Protokoll
- Risk-Based Authentication (RBA)
- RBA mit Single Sign-On
- Passwortintegration
- Support für RSA Authentication Manager-Replikate

Die folgenden Funktionen werden nicht unterstützt:

- RSA SecurID-Authentifizierung mit RADIUS-Protokoll
- ODA mit RADIUS-Protokoll
- Sekundären RADIUS-Serversupport
- RSA SecurID-Softwaretoken-Automatisierung
- RSA SecurID 800-Authentifikator-Automatisierung
- RSA SecurID-Schutz der administrativen Schnittstelle

Sprachsupport

Agent for Citrix StoreFront stellt lokalisierte (übersetzte), dem Nutzer zugewandte Citrix StoreFront Authentifizierungs-Webseiten bereit, die gemäß den Spracheinstellungen angezeigt werden, die vom

Webbrowser des Nutzers angezeigt werden. Lokalisierte Seiten werden in den folgenden Sprachen bereitgestellt:

- Englisch USA (en-us)
- Deutsch (de)
- Chinesisch (zh-cn)
- Chinesisch (zh-tw)
- Französisch (fr)
- Japanisch (ja)
- Koreanisch (ko)
- Spanisch (Lateinamerika) (es)
- Russisch (ru)

Kapitel 2: Vorbereiten der Installation

Systemanforderungen

RSA Authentication Agent for Citrix StoreFront erfordert die folgenden Systemkomponenten:

- Eines der folgenden Windows-Betriebssysteme:
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2

  Hinweis: Windows Server Core-Modus wird nicht unterstützt.
- Eine der folgenden Citrix StoreFront-Versionen:
  - 3.13 (alle oben aufgeführten Windows Betriebssysteme)
  - 3.16 (nur Windows Server 2012 R2 und 2016)
- Microsoft PowerShell 3.0 oder höher

  Hinweis: Windows 2008 R2 enthält standardmäßig PowerShell 2.0, aber Sie können Windows Management Framework 3.0 von Microsoft herunterladen, das PowerShell 3.0 enthält.
- Microsoft .NET Framework 4.5 oder höher

  Hinweis: Windows Server 2008 R2 enthält nicht Microsoft .NET Framework 4.5, aber Sie können ein Installationsprogramm von Microsoft herunterladen.

Zusätzlich zu den Hardwareanforderungen, die von den oben genannten Komponenten auferlegt werden, erfordert Agent for Citrix StoreFront mindestens 50 MB freien Festplattenspeicherplatz.

Sicherheitshinweise

Agent for Citrix StoreFront stellt Authentifizierungsservices für Citrix StoreFront über eine von Citrix definierte Programmierschnittstelle bereit. Um die Nutzeranmeldedaten zu schützen, die über diese Schnittstelle fließen, empfiehlt RSA Folgendes:

- Konfigurieren Sie Ihre Citrix-Umgebung (StoreFront und, falls zutreffend, NetScaler Gateway), um HTTPS für die sichere Kommunikation zwischen Citrix StoreFront und Nutzern zu verwenden.
- Konfigurieren Sie Microsoft Internet Information Services (IIS), auf dem die Citrix StoreFront-Services gehostet werden, und den Microsoft TLS/SSL-Sicherheitsanbieter (von IIS verwendet) zur Verwendung von TLS (Transport Layer Security) Version 1.2 oder höher.

Konfigurationsanweisungen finden Sie unter den folgenden Referenzen.

Aufgabe	Referenz	Schlüsselwörter suchen
Konfigurieren von Citrix StoreFront zur Verwendung von HTTPS	https://www.citrix.com/support/	*https*, *StoreFront*
Konfigurieren des Microsoft TLS/SSL-Sicherheitsanbieters zur Verwendung von TLS	http://support.microsoft.com	*So beschränken Sie die Verwendung bestimmter kryptografischer*

Aufgabe	Referenz	Schlüsselwörter suchen
Version 1.2		*Algorithmen und Protokolle in Schannel.dll*
Konfigurieren von TLS	http://csrc.nist.gov/publications/PubsSPs.html	*Richtlinien für die Auswahl, Konfiguration und Verwendung von TLS-Implementierungen (Transport Layer Security)*

Erforderliche TCP/IP-Ports

Die folgenden TCP/IP-Ports müssen für Agent for Citrix StoreFront verfügbar sein.

Port	Authentifizierungsmodus	Beschreibung
5500/udp	AM UDP	Authentication Manager verwendet diesen Port zur Überwachung. Agent for Citrix StoreFrontstellt während der Authentifizierung eine Verbindung zu diesem Port her.
5550/tcp	AM UDP	Die automatische Registrierung des RSA Authentication Agent verwendet diesen Port zur automatischen Registrierung von Agent for Citrix StoreFront mit Authentication Manager.
5580/tcp	AM UDP/AM REST	Muss verfügbar sein, wenn eine Passwortintegration erforderlich ist. Authentication Manager verwendet diesen Port, um Änderungen an den Windows-Passwörtern der Nutzer zu unterstützen. Der lokale Offline-Service des RSA Authentication Agent stellt eine Verbindung zu diesem Port her.
5555/tcp	AM REST	Wird standardmäßig für die Kommunikation mit REST-Protokoll zwischen dem Agent und primären Instanzen und Replikatinstanzen von Authentication Manager verwendet. Der Authentication Manager-Administrator kann ändern, welcher Port für diesen Zweck verwendet wird.
443/tcp	CAS	Verwendet für die Kommunikation mit REST-Protokoll zwischen dem Agent und dem Cloudauthentifizierungsservice.

Unterstützte Webbrowser

Agent for Citrix StoreFront unterstützt die folgenden Webbrowser:

- Edge (41) auf Windows 10
- Internet Explorer (11)
- Google Chrome (71)
- Mozilla Firefox (64)
- Safari auf OS X

- Android Webbrowser auf Android 9
- Safari auf iOS 12.0.1

Hinweis: JavaScript muss im Browser aktiviert werden.

RSA Authentication Manager-Anforderungen

Agent for Citrix StoreFront erfordert RSA Authentication Manager 8.4 oder höher.

Anforderungen zur Nutzerauthentifizierung

Für den AM UDP-Modus müssen Nutzer über ein RSA SecurID-Hardware- oder Softwaretoken verfügen, um sich erfolgreich zu authentifizieren. Nutzer müssen für die Risk-Based Authentication (RBA) aktiviert sein, um sich bei Citrix StoreFront-Ressourcen, die mit RBA geschützt sind, zu authentifizieren.

Für den AM REST-Modus müssen Nutzer über ein RSA SecurID-Hardware- oder Softwaretoken oder ein registriertes mobiles Gerät verfügen, auf dem die RSA SecurID Authenticate-APP installiert ist.

Für den CAS-Modus gelten die folgenden Anforderungen:

- Um Approve, Device Biometrics oder Authenticate Tokencode verwenden zu können, müssen Nutzer die RSA SecurID Authenticate-App installieren und ein kompatibles mobiles Gerät registrieren.
- Um SMS Tokencode und Voice Tokencode zu verwenden, muss die Telefonnummer des Nutzers in einer Identitätsquelle aufgezeichnet werden, die mit dem Cloudauthentifizierungsservice verbunden ist, und das Attribut „Telefonnummer" muss mit dem Cloudauthentifizierungsservice synchronisiert werden.
- Um RSA SecurID-Token zu verwenden, muss der Authentication Manager mit dem Cloudauthentifizierungsservice integriert sein und Nutzer müssen über SecurID-Hardware- oder Softwaretoken verfügen.
- Die für den Agent konfigurierte Zugriffs-Policy muss die Authentifizierungsmethoden zulassen, die Sie für Citrix StoreFront-Nutzer verfügbar machen möchten.

Hinweis: Der RSA SecurID 800-Hybridauthentifikator (SecurID 800) kann nur im Offlinemodus verwendet werden.

Aufgaben vor der Installation

Bevor Sie die Installation von Agent for Citrix StoreFront vornehmen, Importieren des vertrauenswürdigen Stammzertifikats für Authentication Manager oder den Cloudauthentifizierungsservice auf Seite 22 und führen Sie dann die Aufgaben für den Authentifizierungsmodus aus, den Sie konfigurieren möchten.

Aufgaben vor der Installation für AM UDP-Modus

- Abrufen der RSA Authentication Manager-Konfigurationsdatei Auf der gegenüberliegenden Seite (**sdconf.rec**).
- (Optional) Wenn sie das Dienstprogramm zur automatischen Registrierung des Authentifizierungs-Agent verwenden möchten, Herunterladen des RSA Authentication Manager-Serverzertifikats für die automatische Registrierung auf Seite 21 **(server.cer)**.

- Vergewissern Sie sich, dass Ihre Nutzer mit dem RSA SecurID-Token oder dem RBA-Authentifizierungsprozess vertraut sind.

Aufgaben vor der Installation für AM REST-Modus

- Abrufen der REST Authentifizierungs-URL für die primäre Instanz von Authentication Manager Auf der nächsten Seite.
- (Optional) Rufen Sie die REST Authentifizierungs-URL für alle Authentication Manager-Replikatinstanzen ab, die Sie mit dem Agent verbinden möchten.
- Rufen Sie den REST Authentifizierungs-API-Zugriffsschlüssel für Authentication Manager ab. Anweisungen dazu finden Sie unter Konfigurieren der RSA SecurID Authentication-API für Authentifizierungs-Agents auf RSA Link.
- (Optional) Wenn Sie beabsichtigen, WPI zu aktivieren:
  - Abrufen der RSA Authentication Manager-Konfigurationsdatei unten (**sdconf.rec**).
  - Rufen Sie die Node-Schlüsseldatei über die Sicherheitskonsole ab. Anweisungen finden Sie unter Managen des Node-Schlüssels auf RSA Link.
- Wenn Sie den Agent über die Befehlszeile installieren möchten, Erstellen einer Konfigurationseingabedatei für die Installation über Befehlszeile auf Seite 22.
- Vergewissern Sie sich, dass Ihre Nutzer mit dem RSA SecurID-Token-Authentifizierungsprozess vertraut sind.

Aufgaben vor der Installation für CAS-Modus

- Abrufen der REST-Authentifizierungs-URL für den Cloudauthentifizierungsservice Auf der nächsten Seite
- Rufen Sie den REST Authentifizierungs-API-Zugriffsschlüssel für den Cloudauthentifizierungsservice ab. Anweisungen dazu finden Sie unter Hinzufügen eines RSA SecurID-Authentifizierungs-API-Schlüssels auf RSA Link.
- Wenn Sie den Agent über die Befehlszeile installieren möchten, Erstellen einer Konfigurationseingabedatei für die Installation über Befehlszeile auf Seite 22.
- Vergewissern Sie sich, dass Ihre Nutzer mit dem Cloudauthentifizierungsservice vertraut sind. Weitere Informationen finden Sie unter Cloud Authentication Service-Rollout für Nutzer auf RSA Link.

Abrufen der RSA Authentication Manager-Konfigurationsdatei

Um Agent for Citrix StoreFront im AM UDP-Modus zu installieren oder um WPI im AM REST-Modus zu konfigurieren, müssen Sie die RSA Authentication Manager-Konfigurationsdatei (**sdconf.rec**) in Authentication Manager erzeugen, sie auf den Agent-Hostcomputer kopieren und ihren Verzeichnisort bei der Installation von Konfiguration des Agent festlegen.

Die Datei **sdconf.rec** enthält einen Snapshot der Serverinformationen, die zum Zeitpunkt der Erstellung der Datei verfügbar sind.

Vorbereitung

Verwenden Sie eine Kopie von **sdconf.rec**, die von einem Authentication Manager-Server erzeugt wurde, der die Authentifizierung durchführt. (Der Authentifizierungsservice muss auf diesem Server ausgeführt werden.)

Verfahren

1. Melden Sie sich als Administrator bei der Sicherheitskonsole an.
2. Wählen Sie **Zugriff > Authentifizierungs-Agent > Konfigurationsdatei erzeugen**.
3. Wählen Sie mit den Standardeinstellungen die Option **Konfigurationsdatei erzeugen** aus.
4. Klicken Sie auf den Link **Jetzt herunterladen** und speichern Sie die Datei an einem Speicherort, auf den der Agent während der Installation oder Konfiguration zugreifen kann.
5. Entpacken Sie die Datei **AM_Config. zip**, damit die Inhalte verwendet werden können.

Abrufen der REST Authentifizierungs-URL für die primäre Instanz von Authentication Manager

Um Agent for Citrix StoreFront im REST-Modus zu konfigurieren, müssen sie die REST-Authentifizierungs-URL für Ihre primäre Authentication Manager-Instanz mit dem folgenden Format angeben:

`https://<hostname>:<port>/mfa/v1_1/`

Sie erhalten den Wert *<hostname>* aus dem Feld **Vollständig qualifizierter Domainname** auf der Seite **Administration > Netzwerk > Appliance-Netzwerkeinstellungen** der Authentication Manager-Betriebskonsole. Der Standard *<port>* ist 5555.

Abrufen der REST-Authentifizierungs-URL für den Cloudauthentifizierungsservice

Um Agent for Citrix StoreFront im CAS-Modus zu konfigurieren, müssen sie die REST-Authentifizierungs-URL für den Cloudauthentifizierungsservice mit dem folgenden Format angeben:

`https://<hostname>:<port>/mfa/v1_1/`

Entnehmen Sie den *<Hostnamen>* dem Feld **Authentifizierungsservicedomain** auf der Registerkarte **Registrierung** der Einstellungsseite für jeden Identitätsrouter auf der Seite **Plattform > Identitätsrouter** der Cloudadministrationskonsole. Der Standard *<port>* ist 443.

Herunterladen des RSA Authentication Manager-Serverzertifikats für die automatische Registrierung

Die Authentication Manager-Serverzertifikatdatei (**server.cer**) ist für die Installation des Dienstprogramms für die automatische Registrierung des RSA Authentication Agent erforderlich.

Wenn Sie Agent for Citrix StoreFront im AM UDP-Modus installieren und Sie das Dienstprogramm zur automatischen Registrierung nicht installieren, müssen Sie den Agent in der Authentication Manager-Datenbank manuell registrieren. Weitere Informationen erhalten Sie unter Registrieren des Agent in RSA Authentication Manager auf Seite 32.

Vorbereitung

Um das Dienstprogramm zur automatischen Registrierung des Authentication Agent zu verwenden, muss Authentication Manager so konfiguriert werden, dass die automatische Agent-Host-Registrierung zugelassen wird. Weitere Informationen finden Sie unter Automatische Agent-Registrierung auf RSA Link.

Verfahren

1. Melden Sie sich als Administrator bei der Sicherheitskonsole an.
2. Klicken Sie auf **Zugriff > Authentifizierungs-Agenten > Serverzertifikatsdatei herunterladen**.

3. Klicken Sie auf **Jetzt herunterladen** und speichern Sie die Datei an einem Speicherort, auf den Sie während der Installation von Agent for Citrix StoreFront zugreifen können.

Importieren des vertrauenswürdigen Stammzertifikats für Authentication Manager oder den Cloudauthentifizierungsservice

Bevor Sie den Agent installieren, müssen Sie je nach dem Authentifizierungsmodus, den Sie für den Agent konfigurieren, das vertrauenswürdige Root-CA-Zertifikat von RSA Authentication Manager oder dem Cloudauthentifizierungsservice importieren.

Führen Sie dieses Verfahren auf jedem Computer aus, auf dem Agent for Citrix StoreFront installiert wird.

Vorbereitung

Rufen Sie das vertrauenswürdige Root-CA-Zertifikat von Ihrem Authentication Manager- oder Cloudauthentifizierungsservice-Administrator ab und kopieren Sie es an einen Speicherort auf dem Computer, auf dem Sie den Agent installieren. Anweisungen hierzu finden Sie im Wissensdatenbankartikel How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.

Verfahren

1. Melden Sie sich an dem Computer an, auf dem Sie den Agent installieren werden.
2. Führen Sie **mmc.exe** aus, um die Microsoft Management Console zu öffnen.
3. Wählen Sie **Datei > Snap-In hinzufügen/entfernen**.
4. Doppelklicken Sie auf **Certificates**.
5. Wählen Sie **Computerkonto** aus und klicken Sie anschließend auf **Weiter**.
6. Wählen Sie **Lokaler Computer** aus und klicken Sie anschließend auf **Fertigstellen**.
7. Klicken Sie auf **OK**.
8. Navigieren Sie zu **Zertifikate (Lokaler Computer) > Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate**.
9. Klicken Sie mit der rechten Maustaste auf **Zertifikate** und wählen Sie **Alle Aufgaben > Importieren** aus.
10. Klicken Sie auf **Weiter**.
11. Klicken Sie auf **Durchsuchen**, wählen Sie dann das Zertifikat aus, das Sie importieren möchten, und klicken Sie auf **Öffnen**.
12. Klicken Sie auf **Weiter**.
13. Wählen Sie **Place all certificates in the following store**.
14. Klicken Sie auf **Durchsuchen**, wählen Sie dann **Vertrauenswürdige Stammzertifizierungsstellen** aus und klicken Sie auf **OK**.
15. Klicken Sie auf **Weiter**.
16. Klicken Sie auf **Fertigstellen und OK**.

Erstellen einer Konfigurationseingabedatei für die Installation über Befehlszeile

Bevor Sie Agent for Citrix StoreFront im AM REST- oder im CAS-Modus über die Befehlszeile installieren, müssen Sie eine Eingabedatei erstellen, um Konfigurationseingaben an das Installationsprogramm zu übergeben. Die Eingabedatei ist eine Textdatei, die Schlüsselwertpaare enthält, die Agent-Installationsparameter angeben.

Vorbereitung

Führen Sie die Aufgaben vor der Installation auf Seite 19 für den Authentifizierungsmodus aus, den Sie konfigurieren möchten.

Verfahren

1. Erstellen Sie eine Textdatei mit beliebigem Dateinamen und Erweiterung. Z. B. **input.txt**.
2. Öffnen Sie die Datei zur Bearbeitung.
3. Fügen Sie die folgende Zeichenfolge hinzu, um den Authentifizierungsmodus anzugeben:
   `AUTHENTICATION_MODE= <#>`
   wobei `<#>` entweder `1` für AM REST-Modus oder `2` für CAS-Modus ist.
4. Fügen Sie die folgende Zeichenfolge hinzu, um die Server-URL anzugeben:
   `hERVER_URL= https://<Hostname>:<port>/mfa/v1_1/`
   wobei `<hostname>` die URL für die REST-Authentifizierung für entweder den Cloudauthentifizierungsservice oder die primäre Authentication Manager-Instanz in Ihrer Bereitstellung ist, je nach dem Authentifizierungsmodus, den Sie angegeben haben. Der Standard-`<port>` ist entweder 5555 für AM REST-Modus oder 443 für den CAS-Modus.
5. Fügen Sie die folgende Zeichenfolge hinzu, um den Agent-Namen anzugeben:
   `AGENT_NAME= <examplename>`
   wobei `<examplename>` der Name ist, den Sie auswählen, um den Agent in Authentication Manager oder in mobilen Benachrichtigungen, die über den Cloudauthentifizierungsservice gesendet wurden, zu identifizieren.
6. Fügen Sie die folgende Zeichenfolge hinzu, um den Zugriffsschlüssel anzugeben:
   `ACCESS_KEY= <accesskey>`
   wobei `<accesskey>` der Zugriffsschlüssel ist, den Sie für entweder RSA Authentication Manager oder den Cloudauthentifizierungsservice abgerufen haben, je nach Authentifizierungsmodus.
7. (Optional) Für AM REST-Modus, fügen Sie die folgende Zeichenfolge hinzu, um Replikatserver-URLs anzugeben:
   `REPLICA_URLS= <https://hostname2:port/mfa/v1_1, https://hostname3:port/mfa/v1_1, https://hostname4:port/mfa/v1_1>`
   wobei `<https://hostname2:port/mfa/v1_1, https://hostname3:port/mfa/v1_1, https://hostname4:port/mfa/v1_1>` eine kommagetrennte Liste von URLs für die Replikatserver in Ihrer Bereitstellung ist.
8. (Optional) Für AM REST-Modus, führen Sie einen der folgenden Schritte aus, wenn Sie WPI aktivieren müssen:
   - Fügen Sie die folgenden Zeichenfolgen hinzu, um eine Node-Schlüsseldatei anzugeben, die von Authentication Manager erzeugt wird:
     `NSFILENAME=<nodesecretfilename>`
     `NSPASSWORD=<nodesecretpassword>`
     wobei `<nodesecretfilename>` der Dateiname der Node-Schlüsseldatei ist, die Sie in das Installationsverzeichnis des Agent kopiert haben, und `<nodesecretpassword>` das Passwort ist, das verwendet wurde, um die Node-Schlüsseldatei zu verschlüsseln.
   - Fügen Sie die folgende Zeichenfolge hinzu, um anzugeben, ob die vorhandene Node-Schlüsseldatei von Agent for Microsoft Windows verwendet werden soll, wenn sie bereits auf dem Citrix StoreFront-Server installiert ist:
     `USE_LAC_NODESECRET=<true>`
9. Für CAS-Modus, fügen Sie die folgende Zeichenfolge hinzu, um die Zugriffs-Policy anzugeben, die der Agent verwenden soll:
   `ACCESS_POLICY= <accesspolicy>`

wobei *<accesspolicy>* der genaue Name (einschließlich Unterscheidung nach Groß-/Kleinschreibung) der Zugriffs-Policy ist, wie in der Cloudadministrationskonsole angegeben.

10. (Optional) Für CAS-Modus, fügen Sie die folgende Zeichenfolge hinzu, wenn Sie die Sammlung von Risikodaten während der Authentifizierung deaktivieren müssen:
    `RISK_COLLECTION_ENABLED=false`
    Wenn Sie diese Zeichenfolge nicht hinzufügen, ist die Sammlung von Risikodaten standardmäßig aktiviert.

    Hinweis: Wenn Sie Risikodatensammlung deaktivieren, können Sie das Zugriffsrichtlinienattribut der Identitätszuverlässigkeit nicht verwenden, um Anforderungen für die Nutzerauthentifizierung zu bestimmen.

11. (Optional) Für CAS-Modus, fügen Sie die folgende Zeichenfolge hinzu, wenn Sie die Sammlung von Standortdaten während der Authentifizierung deaktivieren müssen:
    `LOCATION_COLLECTION_REQUIRED= false`
    Wenn Sie diese Zeichenfolge nicht hinzufügen, ist die Sammlung von Standortdaten standardmäßig aktiviert.

    Hinweis: Wenn Sie Standortdatensammlung deaktivieren, können Sie das Zugriffsrichtlinienattribut der vertrauenswürdigen Standorte nicht verwenden, um Anforderungen für die Nutzerauthentifizierung zu bestimmen.

12. Speichern Sie die Datei auf dem Citrix StoreFront-Server, auf dem Sie den Agent installieren möchten.

Nach Abschluss

Verweisen Sie auf die Eingabedatei, die Sie erstellt haben, indem Sie Folgendes in den Konsolenbefehl einschließen, wenn Sie den Agent über die Befehlszeile installieren:
`INPUTFILE=`*<absolute\file\path\input.txt>*
wobei *<absolute\file\path\input.txt>* der absolute Dateipfad für die Eingabedatei ist.

Kapitel 3: Installieren von Agent for Citrix StoreFront

Hinweise zur Installation für Citrix StoreFront-Servergruppen

Wenn Sie Agent for Citrix StoreFront in einer Citrix StoreFront-Servergruppe installieren, beachten Sie die folgenden Richtlinien:

- Sie können ein Skript erstellen, um die Befehlszeileninstallation auf jeden Server in der Servergruppe zu übertragen.
- Das Dienstprogramm zur automatischen Registrierung wird in einer Citrix StoreFront-Servergruppe nicht unterstützt.
- Sie müssen den Agent for Citrix StoreFront auf jedem Server installieren, bevor Sie Änderungen über die Servergruppe weitergeben können.

Installieren des Agent

Das Installationsprogramm installiert die folgenden Elemente abhängig nach den Optionen, die Sie während der Installation auswählen:

- RSA Authentication Agent for Citrix StoreFront
- (Optional) Dienstprogramm zur automatischen Registrierung
- (Optional) Windows-Passwortintegration

Sie können entweder den Installationsassistenten verwenden, der Sie durch den Installationsprozess führt, oder die Befehlszeile verwenden, die eine automatische Installation ermöglicht und mit benutzerdefinierten Skripten verwendet werden kann, um den Agent auf mehreren Servern zu installieren.

Installieren über den Installationsassistenten

Der Installationsassistent bietet eine einfache grafische Benutzeroberfläche für die Installation von Agent for Citrix StoreFront. Führen Sie den Installationsassistenten auf jedem Citrix StoreFront-Server aus, auf dem Sie den Agent installieren möchten.

Vorbereitung

- Sie müssen über Administratorrechte für den Citrix StoreFront-Server verfügen, auf dem Sie Agent for Citrix StoreFront installieren.
- Schließen Sie die Citrix StoreFront-Managementkonsole.
- Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem System, auf dem Sie den Agent installieren möchten.
- Sie müssen das Installationsprogramm vom ursprünglichen Downloadspeicherort aus ausführen oder sicherstellen, dass die Verzeichnisstruktur beibehalten wird, wenn Sie die Installationsdateien verschieben.
- Kopieren Sie die folgenden Dateien in denselben Ordner wie das Installationsprogramm:
  - **sdconf.rec** (für AM UDP-Modus oder wenn Sie WPI für AM REST-Modus konfigurieren möchten)
  - **server.cer** (für AM UDP-Modus, wenn Sie die automatische Registrierung installieren möchten)
  - **<AgentName>_NodeSecret.zip** (für AM REST-Modus, wenn Sie WPI konfigurieren möchten)

Hinweis: Der Installationsassistent fordert Sie auf, die Dateien während der Installation zu durchsuchen und auszuwählen.

Verfahren

1. Melden Sie sich an dem Citrix StoreFront-Server an, auf dem Sie Agent for Citrix StoreFront installieren möchten.
2. Doppelklicken Sie in dem Ordner, in den Sie die Installationsdateien kopiert haben, auf **RSA Authentication Agent for Citrix Storefront x64.msi**, um den Installationsassistenten zu starten.
3. Klicken Sie auf **Next**, um fortzufahren.
4. Lesen und bestätigen Sie die Lizenzvereinbarung oder klicken Sie auf **Drucken**, um Sie zu drucken. Klicken Sie auf **Weiter**.
5. Wählen Sie den Authentifizierungsmodus aus, den Sie für den Agent konfigurieren möchten, und klicken Sie auf **Weiter**.
6. Führen Sie die Schritte für Ihren Authentifizierungsmodus aus:
   - Für **RSA Cloudauthentifizierungsservice (CAS-Modus**):
     a. Geben Sie im Feld **Server-URL** die REST-Authentifizierungs-URL für den Cloudauthentifizierungsservice ein.
     b. Geben Sie im Feld **Zugriffsschlüssel** den REST-Authentifizierungs-API-Zugriffsschlüssel Cloudauthentifizierungsservicefür die ein.
     c. Geben Sie im Feld **Zugriffs-Policy** den Namen der Zugriffs-Policy ein, die der Agent verwenden soll, wie er in Cloudadministrationskonsole angezeigt wird.
     d. Geben Sie im Feld **Agent-Name** einen Namen für den Agent ein. Der Name, den Sie angeben, wird verwendet, um den Agent in mobilen Benachrichtigungen zu identifizieren, die über den Cloudauthentifizierungsservice gesendet werden.
     e. (Optional) Wählen Sie **Erfassung von Standortdaten während der Authentifizierung aktivieren** aus, um dem Agent die Erfassung von HTML5-Geostandortdaten während der Authentifizierung von Nutzern zu erlauben, die Längengrad, Breitengrad und einen Zeitstempel umfassen.
     f. (Optional) Wählen Sie **Erfassung von Risikodaten während der Authentifizierung aktivieren** aus, um dem Agent die Erfassung von Gerätefingerabdruckdaten und anderen Informationen während der Authentifizierung zu erlauben.
     g. Klicken Sie auf **Weiter**.
   - Für **RSA Authentication Manager Mit REST-Protokoll (AM REST-Modus)**:
     a. Geben Sie im Feld **Server-URL** die REST-Authentifizierungs-URL für die primäre Authentication Manager-Instanz ein.
     b. Geben Sie im Feld **Zugriffsschlüssel** den REST-Authentifizierungs-API-Zugriffsschlüssel für Authentication Manager ein.
     c. Geben Sie im Feld **Agent-Name** einen Namen für den Agent ein. Der von Ihnen angegebene Name wird verwendet, um den Agent in Authentication Manager zu identifizieren.
     d. (Optional) Geben Sie im Feld **Replikat-URLs** die REST-Authentifizierungs-URL für eine Authentication Manager-Replikatinstanz ein und klicken sie auf **+**, um sie der Liste der Replikatserver hinzuzufügen. Wiederholen Sie diesen Schritt, um bis zu 15 Replikatserver hinzuzufügen.

e. Klicken Sie auf **Weiter**.

f. (Optional) Wählen Sie **Windows-Passwortintegration aktivieren** aus, um WPI zu aktivieren, und gehen Sie dann wie folgt vor:

i. (Optional) Wenn Agent for Windows auf dem Citrix StoreFront-Server installiert ist und Sie den vorhandenen Node-Schlüssel für Agent for Citrix StoreFront verwenden möchten, wählen Sie **Node-Schlüssel vom Agent for Windows verwenden** aus und fahren Sie mit Schritt **g** fort.

ii. Klicken Sie auf **Durchsuchen**, um den Speicherort der Konfigurationsdatei **sdconf.rec** festzulegen.

iii. Klicken Sie auf **Durchsuchen** und legen Sie den Verzeichnisort der Node-Schlüsseldatei **<AgentName>_NodeSecret.zip** fest.

iv. Geben Sie das Passwort ein, mit dem die Node-Schlüsseldatei verschlüsselt wurde.

g. Klicken Sie auf **Weiter**.

- Für **RSA Authentication Manager Mit UDP-Protokoll (AM UDP-Modus)**:

a. (Optional) Um das Dienstprogramm zur automatischen Registrierung zu installieren, wählen Sie **Wird auf der lokalen Festplatte installiert** aus der Drop-down-Liste **Dienstprogramm für automatische Registrierung** aus.

b. Klicken Sie auf **Weiter**.

c. Klicken Sie auf **Durchsuchen**, um die Systemkonfigurationsdatei (**sdconf.rec**) zu suchen und zu öffnen.

d. Klicken Sie auf **Weiter**.

e. Wenn Sie das Dienstprogramm zur automatischen Registrierung installieren, klicken Sie auf **Durchsuchen**, um die Serverzertifikatdatei (**server.cer**) zu suchen und zu öffnen.

f. Klicken Sie auf **Weiter**.

7. Klicken Sie auf **Installieren**.
8. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.

Installieren mithilfe von Befehlszeilenoptionen

Sie können das Befehlszeilen-Installationsprogramm verwenden, um eine automatische Installation durchzuführen oder um den Befehl mithilfe eines Skripts oder eines Drittanbieterprodukts auf mehreren Servern gleichzeitig auszuführen.

Vorbereitung

- Sie müssen über Administratorrechte für den Citrix StoreFront-Server verfügen, auf dem Sie Agent for Citrix StoreFront installieren.
- Sie sollten mit den Grundlagen der Softwareinstallation mithilfe der msiexec-Befehlszeilenoptionen vertraut sein. Weitere Informationen finden Sie unter http://technet.microsoft.com
- Wenn Sie den Agent im AM REST- oder CAS-Modus installieren, müssen Sie Erstellen einer Konfigurationseingabedatei für die Installation über Befehlszeile auf Seite 22 erstellen.
- Schließen Sie die Citrix StoreFront-Managementkonsole.
- Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem System, auf dem Sie den Agent installieren möchten.

- Sie müssen das Installationsprogramm vom ursprünglichen Downloadspeicherort aus ausführen oder sicherstellen, dass die Verzeichnisstruktur beibehalten wird, wenn Sie die Installationsdateien verschieben.
- Kopieren Sie die folgenden Dateien in denselben Ordner wie das Installationsprogramm:
  - **sdconf.rec** (für AM UDP-Modus oder wenn Sie WPI für AM REST-Modus konfigurieren möchten)
  - **server.cer** (für AM UDP-Modus, wenn Sie die automatische Registrierung installieren möchten)
  - **<AgentName>_NodeSecret.zip** (für AM REST-Modus, wenn Sie WPI konfigurieren möchten)

  Hinweis: Die Befehlszeileninstallation erfasst die Dateien aus dem Ordner, in dem Sie ausgeführt wird.

Verfahren

1. Öffnen Sie eine Administrator-Eingabeaufforderung.
2. Navigieren Sie zu dem Verzeichnis, das die Paketdatei **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, oder geben Sie den vollständigen Pfadnamen zu der Paketdatei in der Befehlszeile ein.

Führen Sie je nach dem Authentifizierungsmodus und den optionalen Funktionen, die Sie für den Agent konfigurieren möchten, einen der folgenden Schritte aus:

- Für **AM UDP-Modus**, verwenden Sie einen Befehl ähnlich dem folgenden:
  `msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi"`
- Für **AM UDP-Modus und das Dienstprogramm zur automatischen Registrierung**, verwenden Sie einen Befehl ähnlich dem folgenden:
  `msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi" ADDLOCAL=AgentAutoRegistration`
- Für **AM REST- oder CAS-Modus**, verwenden Sie einen Befehl ähnlich dem folgenden:
  `msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi" INPUTFILE= <absolute\file\path\input.txt>`
  wobei *<absolute\file\path\input.txt>* der absolute Dateipfad der Konfigurationseingabedatei ist, die Sie erstellt haben. Die Parameter in der Eingabedatei geben den Authentifizierungsmodus und andere Funktionen an, die vom Installationsprogramm konfiguriert werden.

Hinweis: In den vorherigen Beispielen weist der `/qn`-Switch das Installationsprogramm an, im unbeaufsichtigten Modus ausgeführt zu werden, wobei alle Elemente der Benutzeroberfläche unterdrückt werden. Um Fehler zu protokollieren, fügen Sie die Option `/lv` (log verbose) am Ende des Befehls hinzu. Speichern Sie die Protokolldatei, z. B. **install.log**, an einem bekannten Speicherort, wie etwa **%USERPROFILE**.

Nach Abschluss

Wenn Sie den Agent mithilfe einer Konfigurationseingabedatei installiert haben, sichern oder löschen Sie die Datei, da sie sensible Daten enthält.

Upgrade von Agent for Citrix StoreFront 1.5

Wenn Agent for Citrix StoreFront Version 1.5 bereits auf Ihrem Citrix Storefront-Server installiert ist, bewahrt das Installationsprogramm die vorherigen Einstellungen auf, aktualisiert den Agent auf Version 2.0 und konfiguriert den AM UDP-Modus automatisch.

Sie können eine Installation des Upgrades mithilfe des Installationsassistenten oder über die Befehlszeile

durchführen. Der Installationsassistent erkennt die vorhandene Agent-Version und zeigt eine Warnmeldung an, die Sie akzeptieren müssen, um fortzufahren. Bei der Befehlszeileninstallation wird das Upgrade automatisch durchgeführt, wenn Sie den Befehl ausführen, den Agent im UDP-Modus zu installieren.

Nachinstallation

Führen Sie nach der Installation von Agent for Citrix StoreFront die Aufgaben für den ausgewählten Authentifizierungsmodus in der angegebenen Reihenfolge aus.

Aufgaben nach der Installation für AM UDP-Modus

1. Registrieren Sie den Agent in Authentication Manager:
   - Wenn Sie das Dienstprogramm zur automatischen Registrierung installiert haben, wird der Agent während der Installation automatisch registriert.
   - Wenn Sie das Dienstprogramm zur automatischen Registrierung nicht installiert haben, registrieren Sie den Agent manuell als Agent-Host in Authentication Manager. Anweisungen dazu finden Sie unter Registrieren des Agent in RSA Authentication Manager Auf der gegenüberliegenden Seite.
2. Führen Sie eine Testauthentifizierung durch, um die Verbindung mit Authentication Manager zu überprüfen und einen Node-Schlüssel zu erzeugen, falls noch keiner vorhanden ist. Anweisungen dazu finden Sie unter Durchführen einer Testauthentifizierung. auf Seite 54.
   Sie können optional den Node-Schlüssel mit dem Dienstprogramm zum Laden des Node-Schlüssels einrichten. Diese Methode ist nützlich für das Troubleshooting oder die Behebung von Problemen mit Node-Schlüsseln, wenn Agent for Citrix StoreFront und Agent for Microsoft Windows auf demselben Computer installiert sind. Anweisungen dazu finden Sie unter Manuelles Laden des Node-Schlüssels auf Seite 40.
3. Konfigurieren Sie Citrix StoreFront für die **RSA SecurID**-Authentifizierung. Anweisungen dazu finden Sie unter Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.

Aufgaben nach der Installation für AM REST-Modus

1. Registrieren des Agent in RSA Authentication Manager Auf der gegenüberliegenden Seite.
2. Konfigurieren Sie Citrix StoreFront für die **RSA SecurID**-Authentifizierung. Anweisungen dazu finden Sie unter Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
3. (Optional) Konfigurieren Sie zusätzliche Einstellungen wie „Lastenausgleichsschema", „Anforderungs-Timeout", „Lese-Timeout" und „Anzahl der erneuten Versuche" mithilfe der Seite „SecurID-Optionen managen". Anweisungen dazu finden Sie unter Managen von Agent-Einstellungen auf Seite 47.
4. (Optional) Testen Sie die Verbindung zum Cloudauthentifizierungsservice durch Eingabe von `https://HOSTNAME:PORT/mfa/v1_1` in einem Browser oder HTTP-Client.

   Da Sie sich derzeit nicht authentifizieren, wird eine Meldung angezeigt, dass die Website verboten oder nicht autorisiert ist. Dies wird für den Test erwartet.

Aufgaben nach der Installation für den CAS-Modus

1. Konfigurieren Sie Citrix StoreFront für die **RSA SecurID**-Authentifizierung. Anweisungen dazu finden Sie unter Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
2. (Optional) Konfigurieren Sie zusätzliche Einstellungen wie „Anforderungs-Timeout", „Lese-Timeout" und „Anzahl der erneuten Versuche" mithilfe der Seite „SecurID-Optionen managen". Anweisungen dazu finden Sie unter Managen von Agent-Einstellungen auf Seite 47.
3. (Optional) Testen Sie die Verbindung zum Cloudauthentifizierungsservice durch Eingabe von `https://HOSTNAME:PORT/mfa/v1_1` in einem Browser oder HTTP-Client.

   Da Sie sich derzeit nicht authentifizieren, wird eine Meldung angezeigt, dass die Website verboten oder nicht autorisiert ist. Dies wird für den Test erwartet.

Registrieren des Agent in RSA Authentication Manager

Nach der Installation von Agent for Citrix StoreFront im AM UDP- oder AM REST-Modus müssen Sie ihn bei Authentication Manager registrieren.

Hinweis: Wenn der Agent im AM UDP-Modus ist und Sie das Dienstprogramm zur automatischen Registrierung installiert haben, müssen Sie den Agent nicht manuell registrieren.

Vorbereitung

Ermitteln Sie Folgendes:

Für AM UDP-Modus:

- Hostname
- IP-Adressen für Netzwerkschnittstellen

  Hinweis: Wenn Sie Agent for Citrix StoreFront mit einer Citrix StoreFront-Servergruppe verwenden, registrieren Sie eine StoreFront-Servergruppe mit Lastenausgleich als einen einzelnen RSA SecurID-Agent in Authentication Manager, indem Sie die IP-Adresse und den Hostnamen des Load Balancer verwenden. Registrieren Sie die IP-Adresse von jedem StoreFront-Server als alternative IP-Adresse für den Agent.

  Weitere Informationen zur Registrierung des Agent im AM UDP-Modus finden Sie unter https://community.rsa.com/docs/DOC-77208 auf RSA Link.

Für AM REST-Modus:

- Name des logischen Agent
- **<AgentName>_NodeSecret.zip** (nur wenn WPI aktiviert ist)
- **sdconf.rec** (nur, wenn WPI aktiviert ist)

  Weitere Informationen zur Registrierung des Agent im AM REST-Modus finden Sie unter https://community.rsa.com/docs/DOC-76818 auf RSA Link.

Verfahren

1. Melden Sie sich bei der Sicherheitskonsole an.
2. Klicken Sie auf **Zugriff > Authentifizierungs-Agent > Neu hinzufügen**.

3. Geben Sie die erforderlichen Informationen ein. Stellen Sie sicher, dass der Agent-Typ auf **Standard-Agent** (Standardeinstellung) festgelegt ist.
   Authentication Manager verwendet diese Einstellung, um die Kommunikation mit Citrix StoreFront festzulegen.
4. Klicken Sie auf **Speichern**.

Erstellen des Agent-Node-Schlüssels

Wenn Agent for Citrix StoreFront im AM UDP-Modus oder im AM REST-Modus mit aktivierter WPI installiert ist und Ihre Bereitstellung eine Citrix StoreFront-Servergruppe enthält, in der mehrere Server den Agent ausführen, muss der Node-Schlüssel für alle Agents in der Gruppe identisch sein. Für AM REST-Modus, geben Sie die Node-Schlüsseldatei an, wenn Sie WPI im Installationsprogramm oder auf der Seite „SecurID-Optionen managen" aktivieren. Im UDP-Modus müssen Sie das Dienstprogramm zum Laden des Node-Schlüssels verwenden, um den Node-Schlüssel auf jedem StoreFront-Server in der Gruppe zu installieren. Weitere Informationen finden Sie unter Manuelles Laden des Node-Schlüssels auf Seite 40.

Eine Anleitung zum Erzeugen des Node-Schlüssels in der Sicherheitskonsole finden Sie unter Managen des Node-Schlüssels auf RSA Link.

Ändern einer Installation

Wenn Sie den Agent im AM UDP-Modus installiert haben, können Sie die Installation ändern, um das Dienstprogramm für die automatische Registrierung von RSA Authentication Agent hinzuzufügen oder zu entfernen. Sie können die Installation mithilfe des Installationsassistenten oder über Befehlszeilenoptionen ändern.

Ändern der Installation mithilfe des Installationsassistenten

Verwenden Sie dieses Verfahren, um die Installation mithilfe des Installationsassistenten zu ändern.

Vorbereitung

- Kopieren Sie das Downloadpaket mit **RSA Authentifizierungs-RSA Authentication Agent for Citrix StoreFront x64.msi** in einen Ordner auf dem System, in dem Sie die Installation ändern möchten.
- Wenn Sie das Dienstprogramm zur automatischen Registrierung hinzufügen, kopieren Sie die Datei **server.cer** in den Ordner, der die MSI-Datei enthält. Während der Änderung erfasst das Installationsprogramm diese Datei aus dem Ordner, aus dem es ausgeführt wird.
- Wenn Sie das Dienstprogramm zur automatischen Registrierung entfernen, gehen Sie folgendermaßen vor:
  - Entfernen Sie die RSA SecurID-Authentifizierungsmethode. Siehe Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
  - Schließen Sie die Citrix StoreFront-Managementkonsole.

Verfahren

1. Doppelklicken Sie in dem Ordner, in den Sie die Paketdatei kopiert haben, auf **RSA Authentication Agent for Citrix Storefront x64.msi**, um das Installationsprogramm zu starten.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie **Ändern** aus und klicken Sie dann auf **Weiter**.

4. Wählen Sie aus der Drop-down-Liste **Dienstprogramm zur automatischen Registrierung des Agent-Hosts** eine der folgenden Optionen aus:
    - Wird auf lokaler Festplatte installiert
    - Gesamte Funktion wird auf lokaler Festplatte installiert
    - Gesamte Funktion wird nicht verfügbar sein
5. Klicken Sie auf **Weiter**.
6. Wenn Sie das Dienstprogramm zur automatischen Registrierung hinzufügen, klicken Sie auf **Durchsuchen**, um die Datei **server.cer**, die Sie verwenden möchten, zu suchen und zu öffnen.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Installieren**.
9. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.

Ändern der Installation mithilfe der Befehlszeile

Verwenden Sie dieses Verfahren, um eine Agent-Installation über die Befehlszeile zu ändern.

Vorbereitung

- Erfahren Sie, wie Sie Software mithilfe der msiexec-Befehlszeile installieren. Weitere Informationen zu msiexec-Befehlen finden Sie unter http://technet.microsoft.com.
- Kopieren Sie das Downloadpaket mit **RSA Authentifizierungs-RSA Authentication Agent for Citrix StoreFront x64.msi** in einen Ordner auf dem System, in dem Sie die Installation ändern möchten.
- Wenn Sie das Dienstprogramm zur automatischen Registrierung hinzufügen, kopieren Sie die Datei **server.cer** in den Ordner, der die MSI-Datei enthält. Während der Änderung erfasst das Installationsprogramm diese Datei aus dem Ordner, aus dem es ausgeführt wird.
- Wenn Sie das Dienstprogramm zur automatischen Registrierung entfernen, gehen Sie folgendermaßen vor:
    - Entfernen Sie die RSA SecurID-Authentifizierungsmethode. Siehe Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
    - Schließen Sie die Citrix StoreFront-Managementkonsole.

Verfahren

1. Öffnen Sie eine Eingabeaufforderung und führen Sie einen der folgenden Schritte aus:
2. Um das Dienstprogramm zur automatischen Registrierung hinzuzufügen, verwenden Sie einen msiexec-Befehl (mit Unterscheidung zwischen Groß- und Kleinschreibung) ähnlich dem folgenden Beispiel:
```
msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi"
ADDLOCAL=AgentAutoRegistration
```
3. Um das Dienstprogramm zur automatischen Registrierung zu entfernen, verwenden Sie einen msiexec-Befehl (mit Unterscheidung zwischen Groß- und Kleinschreibung) ähnlich dem folgenden Beispiel:
```
msiexec /qn /i "RSA Authentication Agent for Citrix StoreFront x64.msi"
REMOVE=AgentAutoRegistration
```

Hinweis: In den vorherigen Beispielen weist der `/qn`-Switch das Installationsprogramm an, im unbeaufsichtigten Modus ausgeführt zu werden, wobei alle Elemente der Benutzeroberfläche unterdrückt werden.

Reparieren einer Installation

Das Reparieren einer Installation ersetzt fehlende Dateien in einer beschädigten Installation. Sie können die Agent for Citrix StoreFront-Installation entweder mithilfe des Installationsassistenten, der Sie durch den Änderungsprozess führt, oder mithilfe von Befehlszeilenoptionen reparieren.

Reparieren der Installation mithilfe des Installationsassistenten

Der Installationsassistent bietet eine einfache grafische Benutzeroberfläche für die Reparatur der Agent-Installation.

Vorbereitung

Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem System, wo Sie die Installation reparieren möchten.

Verfahren

1. Doppelklicken Sie in dem Ordner, in den Sie das Paket kopiert haben, auf **RSA Authentication Agent for Citrix Storefront x64.msi**, um das Installationsprogramm zu starten.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie **Reparieren** aus und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf **Reparieren**.
5. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.

Reparieren der Installation mithilfe der Befehlszeile

Sie können eine Agent-Installation mithilfe der Befehlszeile reparieren. Verwenden Sie die Befehlszeile, um eine automatische Installation durchzuführen oder um den Befehl mithilfe eines Skripts oder eines Drittanbieterprodukts auf mehreren Servern gleichzeitig auszuführen.

Vorbereitung

- Erfahren Sie, wie Sie Software mithilfe der msiexec-Befehlszeile installieren. Weitere Informationen zu msiexec-Befehlen finden Sie unter http://technet.microsoft.com.
- Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem System, wo Sie die Installation reparieren möchten.

Verfahren

1. Öffnen Sie eine Eingabeaufforderung.
2. Navigieren Sie zu dem Verzeichnis, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, oder geben Sie den vollständigen Pfadnamen zu der Paketdatei in der Befehlszeile ein.
3. Geben Sie den folgenden Befehl ein:
   ```
   msiexec /qn /fvomus "RSA Authentication Agent for Citrix StoreFront x64.msi"
   ```

Hinweis: Im vorherigen Beispiel weist der `/qn`-Switch das Installationsprogramm an, im unbeaufsichtigten Modus ausgeführt zu werden, wobei alle Elemente der Benutzeroberfläche unterdrückt werden.

Deinstallieren des Agent

Sie können Agent for Citrix StoreFront entweder über das Windows Control Panel deinstallieren, oder indem Sie das Installationsprogramm über die Befehlszeile ausführen. Um das Produkt von mehreren Servern zu deinstallieren, müssen Sie die Befehlszeile verwenden.

Deinstallieren über das Windows Control Panel

Führen Sie das folgende Verfahren aus, um den Agent über das Windows Control Panel zu deinstallieren.

Vorbereitung

- Wenn Sie DFA (Delegated Forms Authentication) so konfiguriert haben, dass sie die RSA SecurID-Authentifizierung verwendet, setzen Sie die DFA-Authentifizierung wieder auf die Standard-Citrix-Methode **Nutzername und Passwort** zurück. Siehe Aktivieren der RSA SecurID-Authentifizierung für DFA auf Seite 59.
- Entfernen Sie die RSA SecurID-Authentifizierungsmethode. Siehe Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
- Schließen Sie die Citrix StoreFront-Managementkonsole.

Verfahren

1. Klicken Sie im Startmenü auf **Systemsteuerung > Programme > Programme und Funktionen**.
2. Klicken sie in der Programmliste auf **RSA Authentication Agent for Citrix StoreFront**.
3. Klicken Sie auf **Deinstallieren**.
4. Starten Sie den Server neu, wenn Sie dazu aufgefordert werden. Wenn Sie die Deinstallation abbrechen, wird die Anwendung in den vorherigen Zustand zurückgesetzt.

Deinstallieren über den Installationsassistenten

Führen Sie die folgenden Schritte aus, um den Agent mithilfe des Installationsassistenten zu deinstallieren.

Vorbereitung

- Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem Computer, auf dem Sie den Agent deinstallieren möchten.
- Wenn Sie DFA (Delegated Forms Authentication) so konfiguriert haben, dass sie die RSA SecurID-Authentifizierung verwendet, setzen Sie die DFA-Authentifizierung wieder auf die Standard-Citrix-Methode **Nutzername und Passwort** zurück. Siehe Aktivieren der RSA SecurID-Authentifizierung für DFA auf Seite 59.
- Entfernen Sie die RSA SecurID-Authentifizierungsmethode. Siehe Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
- Schließen Sie die Citrix StoreFront-Managementkonsole.

Verfahren

1. Doppelklicken Sie in dem Ordner, in den Sie die Installationsdateien kopiert haben, auf **RSA Authentication Agent for Citrix Storefront x64.msi**, um den Installationsassistenten zu starten.
2. Klicken Sie auf **Weiter**.

3. Wählen Sie **Entfernen** aus und klicken Sie anschließend auf **Weiter**.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.

Deinstallieren mit der Befehlszeile

Führen Sie das folgende Verfahren aus, um den Agent über die Befehlszeile zu deinstallieren.

Vorbereitung

- Kopieren Sie das Downloadpaket, das **RSA Authentication Agent for Citrix StoreFront x64.msi** enthält, in einen Ordner auf dem System, wo Sie das Produkt deinstallieren möchten.
- Wenn Sie DFA (Delegated Forms Authentication) so konfiguriert haben, dass sie die RSA SecurID-Authentifizierung verwendet, setzen Sie die DFA-Authentifizierung wieder auf die Standard-Citrix-Methode **Nutzername und Passwort** zurück. Siehe Aktivieren der RSA SecurID-Authentifizierung für DFA auf Seite 59.
- Entfernen Sie die RSA SecurID-Authentifizierungsmethode. Siehe Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher auf Seite 46.
- Schließen Sie die Citrix StoreFront-Managementkonsole.

Verfahren

1. Öffnen Sie eine Eingabeaufforderung.
2. Geben Sie einen Befehl ein ähnlich dem folgenden, mit der Option `/x` (REMOVE=ALL) und dem vollständig qualifizierten Pfadnamen:
   ```
   msiexec /qn /x "RSA Authentication Agent for Citrix StoreFront x64.msi" /lv uninstall.log
   ```

   Hinweis: Im vorherigen Beispiel weist der `/qn`-Switch das Installationsprogramm an, im unbeaufsichtigten Modus ausgeführt zu werden, wobei alle Elemente der Benutzeroberfläche unterdrückt werden. Verwenden Sie die Option `/lv` (log verbose), um alle Fehler bei der Entfernung zu protokollieren. Speichern Sie die Protokolldatei, z. B. **uninstall.log**, an einem bekannten Speicherort, wie etwa %USERPROFILE.
3. (Optional) Um das Produkt von mehreren Servern zu deinstallieren, führen Sie den Befehl auf den Servern mithilfe eines Skripts oder eines Drittanbieterprodukts aus, z. B. System Center Configuration Manager (ConfigMgr) von Microsoft oder IBM Tivoli.

Kapitel 4: Konfigurieren und Verwalten des Agent for Citrix StoreFront

Vom Agent verwendete Citrix StoreFront-Nutzername- und Passwort-Funktionen

Sie können die folgenden Funktionen der Citrix StoreFront-Authentifizierungsmethode **Nutzername und Passwort** mit dem Agent for Citrix StoreFront verwenden:

- Konfigurieren Sie vertrauenswürdige Domains, aus denen sich Nutzer anmelden können, und fügen Sie optional die Liste der Domains in ein Drop-down-Menü im Passcode-Dialogfeld ein.
- Legen Sie fest, ob und wann Nutzer Ihre Passwörter ändern können.

Hinweis: Wenn Sie Citrix StoreFront und den Agent auf einem Server installieren und diesen Server einer vorhandenen Servergruppe hinzufügen, gibt der autorisierende StoreFront in der Gruppe die Serverkonfiguration, einschließlich der RSA SecurID-Einstellungen, an den neuen StoreFront-Server weiter.

Anweisungen zur Verwendung dieser Citrix StoreFront-Funktionen finden sie in der Citrix-Dokumentation unter http://docs.citrix.com

Ausschließen bestimmter Netzwerkadapter von der automatischen Registrierung

Wenn Agent for Citrix StoreFront im AM UDP-Modus installiert und die automatische Registrierung aktiviert ist, können Sie das Dienstprogramm für die automatische Registrierung so konfigurieren, dass bestimmte Netzwerkadapter von der automatischen Registrierung von IP-Adressen ausgeschlossen werden. In einigen Fällen kann dies den Netzwerkdatenverkehr reduzieren und die Performance maximieren. Sie können beispielsweise angeben, dass Änderungen an den IP-Adressen von Geräten wie VMware Hosts oder Wireless-Routern keine automatische Registrierung auslösen.

Das Dienstprogramm zur automatischen Registrierung ignoriert Änderungen an den IP-Adressen von Geräten, die in der Zeichenfolgenwerteliste „ExcludeAdapters" aufgeführt sind.

Verfahren

1. Melden Sie sich beim Citrix StoreFront-Server an, auf dem Agent for Citrix StoreFront gehostet wird.
2. Klicken Sie auf **Start** > **Apps** > **Ausführen**.
3. Geben Sie in das Feld **Öffnen** den Befehl **regedit** ein und klicken Sie auf **OK**.
4. Navigieren Sie zu **HKLM\ SOFTWARE\RSA\RSA Authentication Agent\AgentAutoRegistration**.
5. Klicken Sie mit der rechten Maustaste auf **AgentAutoRegistration** und wählen Sie**Neu > Zeichenfolgenwert** aus.
6. Geben Sie als Namen für den neuen Zeichenfolgenwert **ExcludeAdapters** ein.
7. Klicken Sie im rechten Bereich des Fensters des Registry-Editors mit der rechten Maustaste auf **ExcludeAdapters** und klicken Sie auf **Ändern**.
8. Geben Sie Datenwerte für jeden Netzwerkadapter ein, den das Dienstprogramm zur automatischen Registrierung von der Überwachung ausschließen soll.
   Bei Datenwerten wird die Groß-/Kleinschreibung berücksichtigt. Trennen Sie die Werte für jeden Adapter mithilfe von Semikolons. Beispiel: Wenn Sie `VPN;VMware` eingeben, werden alle Adapter, deren

Namen „VPN" und alle Adapter, deren Namen „VMware" enthalten, von der automatischen Registrierung ausgeschlossen.

Verwalten der primären IP-Adresse des Agent

Wenn Agent for Citrix StoreFront im AM UDP-Modus installiert ist, muss die primäre IP-Adresse jedes Agent-Hosts in seinem Agent-Datensatz in der Authentication Manager-Datenbank identifiziert werden. Sie können auch andere IP-Adressen für den Agent als „sekundäre Nodes" für Failover auflisten.

Wenn Sie das Dienstprogramm für die automatische Registrierung des RSA Authentication Agent für einen Agent installieren und aktivieren, wird die primäre IP-Adresse des Agent automatisch in den Authentication Manager-Agent-Datensatz eingegeben und automatisch bei jeder Änderung aktualisiert.

Wenn Ihre Authentication Manager-Umgebung nicht für die automatische Registrierung von Agents konfiguriert ist, muss der Authentication Manager-Administrator die primären und sekundären IP-Adressen des Agent manuell in Authentication Manager notieren. Wenn die Adresse eines Agent geändert wird, muss der Administrator den Authentication Manager-Agent-Datensatz entsprechend aktualisieren.

Wenn Agents manuell registriert werden, muss der Authentication Manager-Administrator sicherstellen, dass die primäre IP-Adresse im Authentication Manager-Agent-Datensatz mit der primären IP-Adresse übereinstimmt, die auf der Seite „SecurID-Optionen managen" angegeben ist (und in der Datei **sdopts.rec**, die die Lastenausgleichsoptionen enthält, wenn Sie den automatischen Lastenausgleich verwenden, wie in Automatischer Lastenausgleich auf Seite 81 beschrieben). Wenn die Adressen nicht übereinstimmen, wird die Kommunikation zwischen Agent for Citrix StoreFront und Authentication Manager fehlschlagen. Wenn sekundäre IP-Adressen für den Agent angegeben sind, müssen diese Adressen auch im Agent-Datensatz eingegeben werden und alle Adressen müssen aktualisiert werden, wenn Sie geändert werden.

Weitere Informationen finden Sie unter Aktivieren einer Außerkraftsetzung einer IP-Adresse auf Seite 52.

Manuelles Laden des Node-Schlüssels

Bei der Installation im AM UDP-Modus ist jede Instanz des Agent mit einem eindeutigen Node-Schlüssel verknüpft. Der Node-Schlüssel ermöglicht es dem Agent und dem Authentication Manager-Server, während des SecurID-Authentifizierungsprozesses eine verschlüsselte Kommunikation zu verwenden.

Wenn der Node-Schlüssel zuvor noch nicht eingerichtet wurde, erstellt Authentication Manager ihn automatisch und lädt ihn auf den Agent-Host herunter, wenn sich ein Nutzer zum ersten Mal erfolgreich mit einem SecurID-Passcode authentifiziert.

In dieser Aufgabe wird beschrieben, wie Sie den Node-Schlüssel manuell auf den Agent-Host laden, bevor Nutzer sich mit RSA SecurID authentifizieren.

Hinweis: Sie müssen das Dienstprogramm zum Laden des Node-Schlüssels verwenden, wenn Sie den Agent in einer Citrix StoreFront-Servergruppe installieren.

Vorbereitung

Erzeugen Sie den Node-Schlüssel. Anweisungen finden Sie unter Managen des Node-Schlüssels auf RSA Link.

Verfahren

1. Stellen Sie den Node-Schlüssel von Authentication Manager mithilfe einer sicheren Methode bereit.
2. Stellen Sie das Passwort, mit dem der Node-Schlüssel verschlüsselt wurde, separat bereit und verwenden Sie dabei eine sichere Methode.
3. Kopieren Sie die Node-Schlüsseldatei und das Dienstprogramm **agent_nsload.exe** in das Verzeichnis **C:\Program Files\Common Files\RSA Shared\Auth API** auf dem Agent-Host.
4. Öffnen Sie eine Eingabeaufforderung und navigieren Sie zum Verzeichnis **C:\Program Files\RSA Shared\Auth API**.
5. Führen Sie das Dienstprogramm zum Laden des Node-Schlüssels mit der folgenden Syntax aus:
   `agent_nsload -f path -d "..\Auth Data"`
   wobei *path* der Verzeichnisort und Name der Node-Schlüsseldatei ist und auf `-d` (Ziel) der Zieldateipfad folgt, wo Sie den Node-Schlüssel speichern möchten. Schließen Sie den Dateipfad in Anführungszeichen ein.
6. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort ein, das zum Verschlüsseln der Node-Schlüsseldatei verwendet wird. Das Dienstprogramm zum Laden des Node-Schlüssels lädt die neue Node-Schlüsseldatei auf den Agent-Host.
7. Wiederholen Sie dieses Verfahren für jeden Agent, der während der ersten RSA SecurID-Authentifizierung zusätzlichen Verschlüsselungsschutz erfordert.

Hinweis: Laden Sie für eine StoreFront-Servergruppe mit Lastenausgleich den Node-Schlüssel von Authentication Manager herunter und installieren Sie ihn auf jedem Storefront-Server in der Gruppe. Derselbe Node-Schlüssel funktioniert auch für RSA Authentication Agent for Microsoft Windows, wenn er auf den StoreFront-Servern installiert ist.

Konfigurieren von Protokollierungsoptionen für AM REST-Modus oder CAS-Modus

Die Protokollierung ist standardmäßig aktiviert, wenn Sie Agent for Citrix StoreFront im AM REST-Modus oder im CAS-Modus installieren. Sie können die Protokollierungsoptionen anpassen, indem sie die Datei **C:\<*AgentInstallDirectory*>\config\log4net.config** manuell bearbeiten. Sie können die folgenden Parameter mithilfe der bereitgestellten Syntax der Protokolldatei ändern.

Hinweis: Sie müssen Microsoft Internet Information Services (IIS) neu starten, nachdem Sie **log4net.config** geändert haben.

Standardmäßiges Protokollformat

Sie können das Protokollierungsformat angeben. Geben Sie `SizeBasedRotation`, `TimeBasedRotation` oder `CompositeRotation` wie gezeigt an:

```
<root>

<level value="ALL" />

<appender-ref ref="SizeBasedRotation"/>

</root>
```

Das Standardformat ist größenbasierte Protokollierung.

Optionen für größenbasierte Protokollierung

Konfigurieren Sie Optionen für größenbasierte Protokollierung, indem Sie die folgenden Parameter bearbeiten.

Protokollrotation

Sie können die Protokollrotation aktivieren, indem Sie den Appender-Tag wie gezeigt festlegen:

```
<appender name="SizeBasedRotation" type="log4net.Appender.RollingFileAppender">
```

Protokolldateiname

Sie können den Namen der Protokolldatei angeben. Beispiel:

```
<file value="C:\kit\SizeBasedLogFile.log"/>
```

Größe von Protokolldateien

Sie können die maximale Protokolldateigröße angeben. Beispiel:

```
<maximumFileSize value="10MB" />
```

Standardmäßig beträgt die maximale Größe der Protokolldatei 10 MB.

Anzahl der Protokolldateien

Sie können die maximale Anzahl von Protokolldateien, die gespeichert werden sollen, angeben. Wenn die maximale Anzahl von Protokolldateien erreicht ist, werden ältere Protokolldateien überschrieben.

```
<maxSizeRollBackups value="10" />
```

Standardmäßige Anzahl der Protokolldateien ist 10.

Protokollebenen

Der Agent weist Protokollebenen in der folgenden Reihenfolge auf: Debug > Info > Warn > Error > Fatal

Der Agent protokolliert alle Meldungen zwischen den festgelegten minimalen und maximalen Ebenen. Die folgenden Beispielwerte werden alle Meldungen für die Ebenen Info, Warn, Error und Fatal protokollieren, nicht jedoch Debug-Meldungen:

```
<filter type="log4net.Filter.LevelRangeFilter">

<levelMin value="INFO" />

<levelMax value="FATAL" />

</filter>
```

Optionen für die zeitbasierte Protokollierung

Konfigurieren Sie Optionen für zeitbasierte Protokollierung, indem Sie die folgenden Parameter bearbeiten.

Protokollrotation

Sie können die Protokollrotation aktivieren, indem Sie den Appender-Tag wie gezeigt festlegen:

```
<appender name="TimeBasedRotation" type="log4net.Appender.RollingFileAppender">
```

Protokollebenen

Der Agent weist Protokollebenen in der folgenden Reihenfolge auf: Debug > Info > Warn > Error > Fatal

Der Agent protokolliert alle Meldungen zwischen den festgelegten minimalen und maximalen Ebenen. Die folgenden Beispielwerte werden alle Meldungen für die Ebenen Info, Warn, Error und Fatal protokollieren, nicht jedoch Debug-Meldungen:

```
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
```

Protokolldateiname

Sie können den Namen der Protokolldatei angeben. Beispiel:

```
<file value="C:\kit\DateBasedLogFile.log"/>
```

Protokolldatei-Datumsmuster

Dem Namen der Protokolldatei wird das Datum in dem Format angehängt, das Sie festgelegt haben. Beispiel:

```
<datePattern value="-yyyyMMdd-HHmm" />
```

Optionen für zusammengesetzte Protokollierung

Wenn die zusammengesetzte Protokollierung konfiguriert ist, werden Protokolldateien basierend entweder auf Datum oder auf Größe überschrieben, je nachdem, welche Bedingung zuerst erfüllt ist. Verwenden Sie die folgende Syntax als grundlegende Vorlage zur Konfiguration der zusammengesetzten Protokollierung und ändern Sie dann die Parameter nach Bedarf für Ihre Bereitstellung.

```
<appender name="TimeBasedLogFile" type="log4net.Appender.RollingFileAppender">
<file value="C:\kit\DateBasedLogFile.log"/>
<lockingModel type="log4net.Appender.FileAppender+MinimalLock" />
<encoding value="utf-8" />
<appendToFile value="true" />
<rollingStyle value="Composite" />
<datePattern value=".yyMMddHHmm.'log'" />
<preserveLogFileNameExtension value="true" />
<maximumFileSize value="1MB" />
<staticLogFileName value="true" />
<maxSizeRollBackups value="5" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern value="%d %-5p %c - %m%n" />
</layout>
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
</appender>
```

Protokollrotation

Sie können die Protokollrotation aktivieren, indem Sie den Appender-Tag wie gezeigt festlegen:

```
<appender name="TimeBasedLogFile" type="log4net.Appender.RollingFileAppender">
```

Protokollebenen

Der Agent weist Protokollebenen in der folgenden Reihenfolge auf: Debug > Info > Warn > Error > Fatal

Der Agent protokolliert alle Meldungen zwischen den festgelegten minimalen und maximalen Ebenen. Die folgenden Beispielwerte werden alle Meldungen für die Ebenen Info, Warn, Error und Fatal protokollieren, nicht jedoch Debug-Meldungen:

```
<filter type="log4net.Filter.LevelRangeFilter">
<levelMin value="INFO" />
<levelMax value="FATAL" />
</filter>
```

Protokolldateiname

Sie können den Namen der Protokolldatei angeben. Beispiel:

```
<file value="C:\kit\DateBasedLogFile.log"/>
```

Protokolldatei-Datumsmuster

Dem Namen der Protokolldatei wird das Datum in dem Format angehängt, das Sie festgelegt haben. Beispiel:

```
<datePattern value=".yyMMddHHmm.'log'" />
```

Hinweis: In dieser Konfiguration der zusammengesetzten Protokollierung haben Ihre Protokolldateien das folgende Benennungsformat: 2010-11-02_15_05.log.0, 2010-11-02_15_05.log.1 etc.

Aktivieren oder Deaktivieren von FIPS auf Windows Server-Betriebssystemen

FIPS (Federal Information Processing Standard) ist ein Computersicherheitsstandard der US-Regierung, der zur Genehmigung von Verschlüsselungsmodulen verwendet wird. Agent for Citrix StoreFront ist mit FIPS kompatibel. Führen Sie dieses Verfahren durch, um den FIPS-Modus auf allen Windows Server-Versionen zu aktivieren, die von Agent for Citrix StoreFront unterstützt werden.

Verfahren

1. Melden Sie sich beim Citrix StoreFront-Server als Administrator an.
2. Klicken Sie auf **Start > Systemsteuerung > Verwaltungstools > Lokale Sicherheitsrichtlinie**. Das Fenster **Lokale Sicherheitseinstellungen** wird angezeigt.
3. Klicken Sie im Navigationsbereich auf **Lokale Richtlinien** und anschließend auf **Sicherheitsoptionen**.
4. Doppelklicken Sie im rechten Fensterbereich auf **Systemkryptographie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden.**
5. Klicken Sie im Dialogfeld, das angezeigt wird, auf **Aktiviert** oder **Deaktiviert**, basierend auf Ihren Anforderungen für die Bereitstellung, und klicken Sie dann auf **Anwenden**.
6. Klicken Sie auf **OK**.
7. Schließen Sie das Fenster **Lokale Sicherheitseinstellungen**.

Managen von RSA SecurID-Authentifizierung mithilfe der Citrix StoreFront-Managementkonsole

Die Citrix StoreFront-Managementkonsole (MMC) ist die primäre Schnittstelle für die Aktivierung, Deaktivierung und Konfiguration RSA SecurID-Authentifizierungs- und Agent-Einstellungen auf dem Storefront-Server, nachdem der Agent for Citrix StoreFront installiert ist.

Informationen zum Ändern der folgenden Einstellungen finden Sie unter Öffnen Sie die Citrix StoreFront-Managementkonsole unten.

Verwenden Sie die Citrix StoreFront-MMC, um die folgenden Aufgaben durchzuführen:

- Hinzufügen oder Entfernen von RSA SecurID aus der Liste der Authentifizierungsmethoden, die aktiviert und deaktiviert werden können. Weitere Informationen finden Sie unter Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher Auf der gegenüberliegenden Seite.
- Aktivieren oder Deaktivieren der RSA SecurID-Authentifizierung Die Aktivierung von RSA SecurID-Authentifizierung setzt die Citrix-Authentifizierung mit **Nutzername und Passwort** automatisch außer Kraft. Wenn RSA SecurID-Authentifizierung deaktiviert ist, können Sie andere verfügbare Methoden verwenden. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der RSA SecurID-Authentifizierung auf Seite 47.
- Hinzufügen oder Entfernen eines StoreFront-Servers in einer Servergruppe, die für die Verwendung von RSA SecurID-Authentifizierung konfiguriert ist Auf der gegenüberliegenden Seite.
- Greifen Sie auf zusätzliche Agent for Citrix StoreFront-Konfigurationseinstellungen auf der „SecurID-Optionen managen" zu. Weitere Informationen finden Sie unter Managen von Agent-Einstellungen auf Seite 47.

Hinweis: Konfigurieren Sie für eine StoreFront-Servergruppe mit Lastenausgleich RSA SecurID-Authentifizierungseinstellungen auf einem StoreFront-Server und übertragen Sie diese dann auf die Servergruppe.

Öffnen Sie die Citrix StoreFront-Managementkonsole

Öffnen Sie die Citrix StoreFront-Management Konsole, um auf Optionen zur Aktivierung, Deaktivierung und Konfiguration von RSA SecurID-Authentifizierungs- und Agent-Einstellungen auf dem StoreFront-Server zuzugreifen.

Verfahren

Führen Sie je nach Betriebssystem auf dem StoreFront-Server einen der folgenden Schritte aus:

- Auf Windows 2008 R2, klicken Sie auf **Start > Alle Programme > Citrix > Citrix StoreFront**.
- Auf Windows 2012, klicken Sie auf **Start > Citrix StoreFront**.
- Auf Windows 2012 R2, klicken Sie auf **Start > Apps > Citrix StoreFront**.
- Auf Windows Server 2016, klicken Sie auf **Start > Apps > Citrix StoreFront**.

Hinweis: Bei den Verfahren in diesem Dokument wird davon ausgegangen, dass die Citrix StoreFront MMC so konfiguriert ist, dass drei Bereiche angezeigt werden. Ein linker Bereich **Konsolenstruktur**, ein mittlerer Bereich **Ergebnisse** und ein rechter Bereich **Aktionen**.

Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher

Bei diesem Verfahren wird RSA SecurID-Authentifizierung aus der Liste der Authentifizierungsanbieter hinzugefügt oder entfernt, die für Citrix StoreFront aktiviert und deaktiviert werden kann. Wenn Sie RSA SecurID-Authentifizierung aus der Liste entfernen, wird der Agent nicht von Ihrem System deinstalliert.

Hinweis: Sie müssen RSA SecurID-Authentifizierung für jeden Speicher installieren, den der Agent schützen soll.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole Auf der vorherigen Seite.
2. Wählen Sie **Speicher** in der **Konsolenstruktur** aus.
3. Wählen Sie in der **Speicherliste** den Speicher aus, für den Sie die RSA SecurID-Authentifizierungsmethode installieren oder deinstallieren möchten.
4. Klicken Sie auf **Authentifizierungsmethoden managen** im **Aktionsbereich**.
5. Klicken Sie im Drop-down-Menü **Erweitert** auf **Authentifizierungsmethoden installieren oder deinstallieren**.
6. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für **RSA SecurID**, um RSA SecurID-Authentifizierung zu installieren.
   - Deaktivieren Sie das Kontrollkästchen für **RSA SecurID**, um RSA SecurID-Authentifizierung zu deinstallieren.
7. Klicken Sie auf **OK**, um das Dialogfeld **Authentifizierungsmethoden installieren oder deinstallieren** zu schließen.
8. Klicken Sie auf **OK**, um das Dialogfeld **Authentifizierungsmethoden managen** zu schließen.
9. (Optional) So übertragen Sie die Änderungen auf Mitglieder einer StoreFront-Servergruppe:
   a. Wählen Sie **Servergruppe** in der **Konsolenstruktur** aus.
   b. Verwenden Sie die Aktion **Änderungen weitergeben**, um die Einstellungen an die Mitglieder der Servergruppe weiterzugeben.

   Hinweis: Agent for Citrix StoreFront muss auf allen Mitgliedern der Servergruppe installiert sein.

Hinzufügen oder Entfernen eines StoreFront-Servers in einer Servergruppe, die für die Verwendung von RSA SecurID-Authentifizierung konfiguriert ist

Wenn Sie Citrix StoreFront und den Agent auf einem Server installieren und diesen Server zu einer bestehenden Servergruppe hinzufügen, überträgt der autorisierende StoreFront in der Gruppe die Serverkonfiguration, einschließlich der RSA SecurID-Authentifizierungseinstellungen, auf den neuen StoreFront-Server.

Vorbereitung

Der Agent für Citrix StoreFront muss auf dem StoreFront-Server installiert sein, den Sie der Gruppe hinzufügen.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole Auf der vorherigen Seite auf einem der Storefront-Server in der Servergruppe.

2. Wählen Sie in der Konsolenstruktur **Servergruppe** aus und fügen Sie den neuen Server mithilfe der Aktion **Server hinzufügen** zur Storefront-Servergruppe hinzu.
3. Verwenden Sie die Aktion **Änderungen weitergeben**, um die Serverkonfiguration, einschließlich RSA SecurID-Authentifizierungseinstellungen, auf den neuen Server zu übertragen.

Aktivieren oder Deaktivieren der RSA SecurID-Authentifizierung

Die Aktivierung von RSA SecurID-Authentifizierung setzt die Citrix-Authentifizierung mit **Nutzername und Passwort** automatisch außer Kraft. Wenn RSA SecurID-Authentifizierung deaktiviert ist, können Sie andere verfügbare Methoden verwenden.

Vorbereitung

Installieren oder Deinstallieren von RSA SecurID-Authentifizierung für einen Speicher Auf der vorherigen Seite. **RSA SecurID** muss in der Citrix Storefront-Managementkonsolenliste der verfügbaren Authentifizierungsanbieter angezeigt werden.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Wählen Sie **Speicher** in der **Konsolenstruktur** aus.
3. Wählen Sie in der **Speicherliste** den Speicher aus, für den Sie RSA SecurID-Authentifizierung aktivieren oder deaktivieren möchten.
4. Klicken Sie auf **Authentifizierungsmethoden managen** im **Aktionsbereich**.
5. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen für **RSA SecurID**, um RSA SecurID-Authentifizierung zu aktivieren.
   - Deaktivieren Sie das Kontrollkästchen für **RSA SecurID**, um RSA SecurID-Authentifizierung zu deaktivieren.
6. Klicken Sie auf **OK**.

Managen von Agent-Einstellungen

Verwenden Sie die Seite „SecurID-Optionen managen", um die Authentifizierungsmodi zu ändern und andere Agent for Citrix StoreFront-Funktionen zu konfigurieren. Die Seite zeigt je nach ausgewähltem Authentifizierungsmodus verschiedene Optionen an.

Informationen zum Ändern dieser Einstellungen finden Sie unter Öffnen Sie die Seite „SecurID-Optionen managen" auf Seite 52.

AM UDP-Modus – Optionen

Option	Beschreibung
Vollständiger Pfad der Datei sdconf.rec	Klicken Sie auf **Durchsuchen**, um den Speicherort der Authentication Manager-Konfigurationsdatei **sdconf.rec** festzulegen. Beschaffen Sie sich diese Datei vom Authentication Manager-Administrator.
Automatische Registrierung aktivieren	Falls aktiviert, registriert die automatische Registrierung den Agent bei Authentication Manager und aktualisiert die IP-Adresse und den Node-Schlüssel nach Bedarf ohne manuelle Intervention. Das Dienstprogramm für die automatische Registrierung des RSA Authentication Agent muss installiert sein, bevor Sie diese Funktion aktivieren können.

Option	Beschreibung
Vollständiger Pfad der Datei server.cer:	Klicken Sie auf **Durchsuchen**, um den Speicherort der Serverzertifikatdatei **server.cer**festzulegen. Beschaffen Sie sich diese Datei vom Authentication Manager-Administrator.
Erweiterte Tools	Dieses Untermenü enthält die folgenden Optionen: • Testen der Authentifizierung: Sendet RSA SecurID-Nutzernamen und -Passcode an Authentication Manager, um zu überprüfen, ob Agent for Citrix StoreFront authentifiziert werden kann. Befolgen Sie die Anweisungen auf dem Bildschirm, um Authentifizierungsinformationen bereitzustellen und bei Bedarf eine RSA SecurID-PIN zu erstellen. Weitere Informationen finden Sie unter Durchführen einer Testauthentifizierung. auf Seite 54. • Ablaufverfolgung: Erzeugt Protokolldateien für das Troubleshooting von Authentifizierungsproblemen. In der Regel aktivieren Sie die Ablaufverfolgung nur, wenn Sie vom RSA Kundensupport dazu aufgefordert werden. Dieser gibt an, welche Stufe der Ablaufverfolgung eingestellt werden soll und welche Komponenten verfolgt werden sollen. Weitere Informationen finden Sie unter Aktivieren der Nachverfolgung auf Seite 55. • IP-Adresse überschreiben: Gibt die primäre IP-Adresse an zur Identifizierung von Agent for Citrix StoreFront, wenn der Server, auf dem der Agent gehostet wird, mehrere IP-Adressen hat. Sie müssen diese Adresse auch angeben, wenn Sie den Agent in der Authentication Manager-Sicherheitskonsole registrieren. Diese Funktion ist nicht verfügbar, wenn die automatische Registrierung aktiviert ist. Weitere Informationen finden Sie unter Aktivieren einer Außerkraftsetzung einer IP-Adresse auf Seite 52.
Serverumgebung	Zeigt Informationen über Ihre Authentication Manager-Serverumgebung an, sodass Sie die primären Instanzen und Replikatinstanzen prüfen und sicherstellen können, dass Agent for Citrix StoreFront mit dem richtigen Authentication Manager-Server kommuniziert.
Node-Schlüssel löschen	Löscht den Node-Schlüssel vom Agent. Möglicherweise müssen Sie im Falle einer Nichtübereinstimmung den Node-Schlüssel löschen und ersetzen. Beispiel: Wenn ein Administrator die Registrierung des Agent in der Authentication Manager-Sicherheitskonsole aufhebt. Weitere Informationen finden Sie unter Löschen des Node-Schlüssels auf Seite 53.
Domain- und Nutzernamen an Authentication Manager senden	Gibt an, ob der Agent bei der Kontaktaufnahme mit Authentication Manager für eine Authentifizierungsanforderung die Domain zusammen mit dem Nutzernamen eines Nutzers sendet. Aktivieren Sie diese Option, wenn Nutzerkonten in Ihrer Bereitstellung ein Domain\Nutzername-Format verwenden. **Hinweis:** Der Agent unterstützt keine Authentication Manager-Konten im UPN-Format (nutzername@domainname).

AM REST-Modus – Optionen

Option	Beschreibung
Server-URL	Gibt die REST-Authentifizierungs-URL für Ihre primäre Authentication Manager-Instanz mit dem folgenden Format an:

Option	Beschreibung
	`https://`*`HOSTNAME`*`:`*`PORT`*`/mfa/v1_1/` Sie erhalten den Wert *`HOSTNAME`* aus dem Feld **Vollständig qualifizierter Domainname** auf der Seite **Administration > Netzwerk > Appliance-Netzwerkeinstellungen** der Betriebskonsole. Der Standard*`port`* ist 5555.
Zugriffsschlüssel	Gibt den REST-Authentifizierungs-API-Zugriffsschlüssel für RSA Authentication Manager an. Informationen zum Abrufen des API-Zugriffsschlüssels finden Sie unter Konfigurieren der RSA SecurID Authentication-API für Authentifizierungs-Agents auf RSA Link.
Name des Agent	Gibt einen Namen an, der verwendet wird, um den Agent in Authentication Manager zu identifizieren.
Replikat-URLs	Gibt die REST-Authentifizierungs-URLs für ihre Authentication Manager-Replikatinstanzen an. Geben Sie eine URL ein und klicken Sie auf **+**, um Sie zur Liste hinzuzufügen. Wählen Sie eine URL aus der Liste aus und klicken Sie auf **-**, um sie zu entfernen. Sie können bis zu 15 Replikat-URLs hinzufügen.
Timeout bei Anforderung	Gibt die maximal zulässige Anzahl von Sekunden an, in denen der Agent jede Transaktion mit Authentication Manager abschließen kann. Bereich: 1–180 Standard: 180 **Hinweis:** Wenn eine Authentication Manager-Instanz nicht mehr verfügbar ist, bemerken Nutzer möglicherweise eine Verzögerung während der Authentifizierung, während der Agent versucht, eine Replikatinstanz zu kontaktieren. Die Einstellung eines niedrigeren Timeout-Werts bei Anforderungen kann diese Verzögerung reduzieren.
Lese-Timeout	Gibt die maximal zulässige Anzahl von Sekunden an, in denen der Agent die Verbindung mit dem Authentication Manager-Server herstellen und die Antwort lesen kann. Bereich: 1–180 Standard: 60
Anzahl der erneuten Versuche	Gibt an, wie oft der Agent versucht, eine Authentication Manager-Instanz zu kontaktieren, wenn der erste Versuch nicht erfolgreich ist. Wenn Replikate konfiguriert sind, versucht der Agent, das nächste Replikat zu kontaktieren, wenn die Anzahl der erneuten Versuche erreicht ist. Bereich: 1–5 Standard: 1
Serveraktualisierungsintervall	Gibt die Anzahl der Minuten an zwischen Polling-Versuchen zur Feststellung, ob der Authentication Manager-Service verfügbar ist. Minimum: 5

Option	Beschreibung
	Standard: 5
Lastenausgleich	Gibt die Methode an, mit der Authentifizierungsanforderungen unter konfigurierten Authentication Manager-Replikatservern verteilt werden. Der Agent unterstützt diese Modi: • Round Robin mit Gewichtung (Standard) Der Agent misst regelmäßig die Zeit, die jeder Server für die Verarbeitung einer Authentifizierungsanforderung benötigt, und verteilt mehr Anforderungen an schnellere Server und weniger Anforderungen an langsamere Server. • Round Robin Der Agent verteilt Anforderungen an jeden Server nacheinander in der Reihenfolge, in der die Server vom Administrator hinzugefügt wurden.
Aktivieren von WPI	Aktiviert oder deaktiviert Windows-Passwortintegration. Wenn WPI aktiviert und konfiguriert ist, geben Nutzer Windows-Passwörter nur bei der ersten Authentifizierung an. Der Agent ruft bei nachfolgenden Authentifizierungen gespeicherte Passwörter ab und fordert nicht dazu auf, ein Windows-Passwort einzugeben. Klicken Sie auf **WPI managen** für zusätzliche Konfigurationseinstellungen, die zur Aktivierung von WPI erforderlich sind. **Hinweis:** Sie müssen auch WPI über die Einstellungen für Policys zur Offlineauthentifizierung in der Sicherheitskonsole aktivieren, damit diese Einstellung funktioniert.
WPI managen	Dieses Untermenü enthält die folgenden WPI-Einstellungen: • Node-Schlüssel von UDP verwenden: Wenn der Agent zuvor im UDP-Modus konfiguriert wurde, aktivieren Sie dieses Kontrollkästchen, um den zuvor generierten Node-Schlüssel zu verwenden. • Vollständiger Pfad der Datei **sdconf.rec**: Klicken Sie auf **Durchsuchen**, um den Speicherort der Authentication Manager-Konfigurationsdatei **sdconf.rec** festzulegen. • Vollständiger Pfad der Datei ***<AgentName>*_NodeSecret.zip**: Klicken Sie auf **Durchsuchen**, um den Speicherort der Authentication Manager-Konfigurationsdatei ***<AgentName>*_NodeSecret.zip** festzulegen. • Geben Sie das Passwort ein, mit dem ***<AgentName>*_NodeSecret.zip** verschlüsselt wird: Dies ist das Passwort, das angegeben wurde, als die Node-Schlüsseldatei in der Sicherheitskonsole erzeugt wurde. • Node-Schlüssel erzeugen: Klicken Sie auf diese Schaltfläche, um den während der verschlüsselten Kommunikation zwischen dem Agent und Authentication Manager verwendeten Node-Schlüssel zu erzeugen.
Domain- und Nutzernamen an	Gibt an, ob der Agent bei der Kontaktaufnahme mit Authentication Manager für

Option	Beschreibung
Authentication Manager senden	eine Authentifizierungsanforderung die Domain zusammen mit dem Nutzernamen eines Nutzers sendet. Aktivieren Sie diese Option, wenn Nutzerkonten in Ihrer Bereitstellung ein Domain\Nutzername-Format verwenden. **Hinweis:** Der Agent unterstützt keine Authentication Manager-Konten im UPN-Format (nutzername@domainname).

CAS-Modus-Optionen

Option	Beschreibung
Server-URL	Gibt die REST-Authentifizierungs-URL für den Cloudauthentifizierungsservice mit dem folgenden Format an: `https://hostname:port/mfa/v1_1/` Entnehmen Sie den *Hostnamen* dem Feld **Authentifizierungsservicedomain** auf der Registerkarte **Registrierung** der Einstellungsseite für jeden Identitätsrouter auf der Seite **Plattform > Identitätsrouter** der Cloudadministrationskonsole. Der Standardport ist *443*.
Zugriffsschlüssel	Gibt den Zugriffsschlüssel für die REST-Authentifizierungs-API für den Cloudauthentifizierungsservice an. Informationen darüber, wie Sie den API-Zugriffsschlüssel erhalten, finden Sie unter Hinzufügen eines RSA SecurID Authentication-API-Schlüssels auf RSA Link.
Name des Agent	Gibt einen Namen an, der verwendet wird, um den Agent in mobilen Benachrichtigungen zu identifizieren, die über den Cloudauthentifizierungsservice gesendet werden.
Zugriffs-Policy	Gibt den genauen Namen (einschließlich Beachtung von Groß- und Kleinschreibung) der Cloudadministrationskonsole-Zugriffs-Policy an, die der Agent verwenden soll. Informationen zum Anzeigen und Hinzufügen von Zugriffsrichtlinien finden Sie unter Verwalten von Zugriffsrichtlinien auf RSA Link.
Timeout bei Anforderung	Gibt die maximal zulässige Anzahl von Sekunden an, in denen der Agent jede Transaktion mit dem Cloudauthentifizierungsservice abschließen kann. Bereich: 1–180 Standard: 180
Lese-Timeout	Gibt die maximal zulässige Anzahl von Sekunden an, in denen der Agent die Verbindung mit dem Cloudauthentifizierungsservice herstellen und die Antwort lesen kann. Bereich: 1–180 Standard: 60
Anzahl der erneuten Versuche	Gibt an, wie oft der Agent versucht, den Cloudauthentifizierungsservice zu kontaktieren, wenn der erste Versuch nicht erfolgreich ist. Bereich: 1–5 Standard: 1
Eingabeaufforderung für Windows-Passwort nach RSA	Gibt an, ob der Agent die Nutzer nach Abschluss aller erforderlichen SecurID-Authentifizierungsmethoden zur Eingabe Ihres Windows-Passworts auffordert. Standardmäßig fordert der Agent zuerst zur Eingabe des Windows-Passworts auf.

Option	Beschreibung
SecurID-Authentifizierung	
Risikosammlung aktivieren	Gibt an, ob die Erfassung von Geräte-Fingerabdruckdaten und anderen Informationen während der Authentifizierung aktiviert werden soll, die der Cloudauthentifizierungsservice verwenden kann, um eine Stufe der Identitätssicherheit für einen Nutzer festzulegen. Zugriffsrichtlinien können das Attribut der Identitätszuverlässigkeit verwenden, um Benutzern mit hoher Identitätszuverlässigkeit die Authentifizierung zu erleichtern. Weitere Informationen finden Sie unter Bedingungsattribute für Zugriffsrichtlinien auf RSA Link. **Hinweis:** Ungeachtet dieser Einstellung erfasst der Agent immer initiierende IP-Adresse, Nutzer-Agent und HTTP-Header-Informationen während der Nutzerauthentifizierung, die der Cloudauthentifizierungsservice verwenden kann, um Authentifizierungsanforderungen gemäß der konfigurierten Zugriffs-Policy festzustellen.
Standortsammlung aktivieren	Gibt an, ob die Erfassung von HTML5-Geostandortdaten während der Authentifizierung von Nutzern aktiviert werden soll, die Längengrad, Breitengrad und Zeitstempel umfasst. Zugriffsrichtlinien können das Attribut „Vertrauenswürdiger Standort" verwenden, um Benutzern von bestimmten Standorten die Authentifizierung zu erleichtern. Weitere Informationen finden Sie unter Bedingungsattribute für Zugriffsrichtlinien auf RSA Link. **Hinweis:** Ungeachtet dieser Einstellung erfasst der Agent immer initiierende IP-Adresse, Nutzer-Agent und HTTP-Header-Informationen während der Nutzerauthentifizierung, die der Cloudauthentifizierungsservice verwenden kann, um Authentifizierungsanforderungen gemäß der konfigurierten Zugriffs-Policy festzustellen.

Öffnen Sie die Seite „SecurID-Optionen managen"

Öffnen Sie die Seite „SecurID-Optionen managen", um auf Einstellungen zuzugreifen, mit denen Sie Authentifizierungsmodi ändern und andere Agent for Citrix StoreFront-Funktionen konfigurieren können.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Wählen Sie in der **Speicherliste** einen Speicher aus, für den Agent for Citrix StoreFront als Authentifizierungsmethode konfiguriert ist.
3. Klicken Sie auf **Authentifizierungsmethoden managen** im **Aktionsbereich**.
4. Wählen Sie **SecurID-Optionen managen** im Drop-down-Menü in der Spalte **Einstellungen** für RSA SecurID aus.

Aktivieren einer Außerkraftsetzung einer IP-Adresse

Wenn Agent for Citrix StoreFront im AM UDP-Modus auf einem Server installiert ist, der über mehrere Netzwerkschnittstellenkarten und mehrere IP-Adressen verfügt, und Sie beabsichtigen, verschiedene Adressen zu verwenden, um eine Verbindung zu Authentication Manager vom Agent-Host zu unterschiedlichen Zeitpunkten herzustellen, müssen Sie Folgendes tun:

- Registrieren Sie eine IP-Adresse als primäre in Authentication Manager und legen Sie diese als außer Kraft setzende IP-Adresse auf der Seite „SecurID-Optionen managen" fest.
- Registrieren Sie die anderen IP-Adressen, die dem Agent-Host angehören, als sekundäre Adressen in Authentication Manager.

Informationen zum Registrieren von IP-Adressen in Authentication Manager finden Sie unter Hinzufügen eines Authentifizierungs-Agent auf RSA Link.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen" Auf der vorherigen Seite.
3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Klicken Sie auf **Erweiterte Tools**.
5. Klicken Sie auf **IP-Adresse überschreiben**:
6. Geben Sie in das Feld **IP-Adresse überschreiben** die IP-Adresse ein, die als primäre Adresse in Authentication Manager angegeben ist.
7. Klicken Sie auf **OK**.

Löschen des Node-Schlüssels

Wenn der Agent im AM UDP-Modus installiert wird und der Node-Schlüssel des Agent nicht mit dem Node-Schlüssel im Authentication Manager übereinstimmt, kann keine verschlüsselte Kommunikation zwischen Agent for Citrix StoreFront und Authentication Manager stattfinden. In diesem Fall müssen Sie den Node-Schlüssel auf dem Agent und auf Authentication Manager löschen.

Wenn der Service für die automatische Registrierung des RSA Authentication Agent installiert und Authentication Manager so konfiguriert ist, dass Agents automatisch registriert werden können, ist es in der Regel nicht erforderlich, den Node-Schlüssel auf dem Agent zu löschen. Allerdings kann es in bestimmten Situationen zu einer Nichtübereinstimmung der Node-Schlüssel kommen. Wenn ein Administrator beispielsweise die Sicherheitskonsole verwendet, um eine Instanz des Agent for Citrix StoreFront im Authentication Manager abzumelden, wird der Node-Schlüssel nicht übereinstimmen und Sie müssen den Node-Schlüssel löschen.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen" Auf der vorherigen Seite.
3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Klicken Sie auf **Node-Schlüssel löschen**.
5. Klicken Sie auf **Ja**.
6. Wenn der Service zur automatischen Registrierung deaktiviert oder nicht installiert ist, löschen Sie den Node-Schlüssel für diesen Agent aus Authentication Manager. Anweisungen finden Sie unter Aktualisieren des Node-Schlüssels auf RSA Link.

Anzeigen der Informationen zur Serverumgebung

Sie können Informationen über Ihre RSA Authentication Manager-Serverumgebung in den Agent-Optionen anzeigen, um zu überprüfen, ob die Umgebung ordnungsgemäß eingerichtet ist.

Administratoren zeigen in der Regel Informationen zur Umgebung an, um die Authentication Manager Server, primäre und Replikatserver, zu prüfen und um zu prüfen, ob Agent for Citrix StoreFront mit dem richtigen Authentication Manager Server kommuniziert.

Verfahren

1. Auf dem Citrix StoreFront-Server, Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen“ auf Seite 52.
3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Klicken Sie auf **Serverumgebung**.
5. Belassen Sie im Feld **Anzuzeigenden Server auswählen** den Standardserver oder wählen Sie ggf. einen anderen Server aus der Drop-down-Liste aus. Wenn Sie einen anderen Server auswählen, klicken Sie auf **Aktualisieren**, um die Informationen für diesen Server anzuzeigen.

Durchführen einer Testauthentifizierung.

Wenn Agent for Citrix StoreFront im AM UDP-Modus konfiguriert ist, können Sie eine Testauthentifizierung durchführen, um zu überprüfen, ob der Agent erfolgreich authentifiziert werden kann. Eine Testauthentifizierung sendet einen Nutzernamen und ein RSA SecurID-Passcode an den konfigurierten Authentication Manager-Server. Eine Testauthentifizierung erzeugt auch einen Node-Schlüssel, wenn noch keiner vorhanden ist, und lädt ihn auf den Agent-Host herunter.

Vorbereitung

Agent for Citrix StoreFront muss über eine Netzwerkverbindung mit Authentication Manager verfügen.

Verfahren

1. Auf dem Citrix StoreFront-Server, Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen“ auf Seite 52.
3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Klicken Sie auf **Erweiterte Tools**.
5. Klicken Sie auf **Test Authentication**.
6. Im Feld **Nutzername**, behalten Sie den aktuellen Nutzernamen bei oder geben Sie einen entsprechenden Namen ein.
7. Gehen Sie im Feld **SecurID-Passcode** auf eine der folgenden Weisen vor:
   - Wenn Sie keine SecurID-PIN festgelegt haben, geben Sie den aktuellen Tokencode ein. Klicken Sie auf **OK**. Das Dialogfeld „Neue RSA SecurID-PIN festlegen“ wird geöffnet. Weiter mit Schritt 8.
   - Wenn Sie bereits eine SecurID-PIN haben, geben Sie den Passcode ein. Klicken Sie auf **OK**. Fahren Sie bei Bedarf mit Schritt 10 fort.
8. Um eine PIN festzulegen, befolgen Sie die Anweisungen im Dialogfeld „Neue RSA SecurID-PIN festlegen“.
   - Wenn Authentication Manager so konfiguriert ist, dass systemgenerierte PINs ausgegeben werden, werden Sie aufgefordert, sich Ihre neue PIN zu merken. Klicken Sie dann auf **OK**. Wenn Sie auf **Abbrechen** klicken, wird die neue PIN nicht festgelegt.
   - Wenn Sie aufgefordert werden, Ihre PIN zu erstellen, geben Sie eine PIN in das Feld **SecurID PIN** ein. Geben Sie dieselbe PIN erneut in das Feld **SecurID-PIN bestätigen** ein. Klicken Sie auf **Fertigstellen**.
9. Sobald Ihr PIN festgelegt wurde, geben Sie den PIN gefolgt von dem Tokencode im Feld **Nächster Passcode** ein. Wenn der Authentifikator über ein PIN-Eingabefeld verfügt, geben Sie die PIN in das Gerät ein, um einen Passcode zu erzeugen, und geben Sie dann den Passcode ein. Klicken Sie auf **OK**.

10. Wenn Sie aufgefordert werden, den nächsten Tokencode einzugeben, um ihren Besitz des Authentifikators zu bestätigen und ihn mit Authentication Manager zu synchronisieren, warten Sie, bis der Tokencode auf Ihrem Authentifikator geändert wurde. Geben Sie den neuen Tokencode in das Feld **Nächster Tokencode** ein und klicken Sie auf **OK**.

Wenn Sie sich nicht authentifizieren können, überprüfen Sie Ihre Authentication Manager-Einstellungen auf dem Bildschirm „Serverumgebung" der Seite „SecurID-Optionen managen".

Aktivieren der Nachverfolgung

Wenn Agent for Citrix StoreFront im AM UDP-Modus installiert ist, können Sie die Ablaufverfolgung aktivieren, um Authentifizierungsprobleme zu diagnostizieren. In der Regel aktivieren Sie die Trace-Protokollierung nur, wenn Sie von RSA Kundensupport dazu aufgefordert werden. Der Kundensupport informiert Sie auch darüber, welche Komponenten nachverfolgt werden und welche Level für die Nachverfolgung festgelegt werden müssen.

Hinweis: Die Nachverfolgung ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, werden die Ausgabedateien der Ablaufverfolgung nach **C:\ProgramData\RSA\Logfiles** geschrieben. Sie können diesen Speicherort ändern.

Informationen zum Konfigurieren der Protokollierung, wenn der Agent im AM REST- oder CAS-Modus installiert ist, finden Sie unter Konfigurieren von Protokollierungsoptionen für AM REST-Modus oder CAS-Modus auf Seite 41.

Verfahren

1. Auf dem Agent-Host, auf dem Probleme auftreten, Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen" auf Seite 52.
3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Klicken Sie auf **Erweiterte Tools**.
5. Klicken Sie auf **Nachverfolgen**.
6. Konfigurieren Sie die Nachverfolgungseinstellungen gemäß den Anweisungen des Kundensupports.
7. Klicken Sie auf **OK**.

Ändern des Authentifizierungsmodus nach Erstinstallation

Sie können den Authentifizierungsmodus für Agent for Citrix StoreFront nach der Erstinstallation ändern.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45
2. Öffnen Sie die Seite „SecurID-Optionen managen" auf Seite 52
3. Wählen Sie im Drop-down-Menü **Authentifizierungsmodus** den Authentifizierungsmodus aus, den Sie konfigurieren möchten.
4. Konfigurieren Sie die Agent-Einstellungen für den ausgewählten Authentifizierungsmodus nach Bedarf für Ihre Bereitstellung. Weitere Informationen finden Sie unter Managen von Agent-Einstellungen auf Seite 47.

Aktivieren von WPI für AM REST-Modus nach der Erstinstallation

Wenn Sie WPI bei der Erstinstallation des Agent im AM REST-Modus nicht aktiviert haben oder wenn Sie nach der Erstinstallation in den AM REST-Modus gewechselt haben, können Sie sie jederzeit aktivieren.

Verfahren

1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45.
2. Öffnen Sie die Seite „SecurID-Optionen managen" auf Seite 52.
3. Vergewissern Sie sich, dass AM REST im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist.
4. Wählen Sie **Windows-Passwortintegration (WPI) aktivieren** aus.
5. Klicken Sie auf **WPI managen**.
6. Wenn der Agent zuvor im AM UDP-Modus installiert und konfiguriert wurde und immer noch denselben Agent-Namen verwendet, wählen Sie **Node-Schlüssel im UDP-Modus verwenden** aus und fahren Sie mit Schritt 10 fort. Fahren Sie andernfalls mit Schritt 7 fort.
7. Klicken Sie auf **Durchsuchen**, um den Speicherort der Konfigurationsdatei **sdconf.rec** festzulegen.
8. Klicken Sie auf **Durchsuchen** und legen Sie den Verzeichnisort der Node-Schlüsseldatei **<*AgentName*>_NodeSecret.zip** fest.
9. Geben Sie im Feld **Eingeben des Passworts, mit dem _NodeSecret.zip verschlüsselt wurde** das Verschlüsselungspasswort ein.
10. Klicken Sie auf **OK**.

Hinweis: Sie müssen auch WPI für Agent for Citrix StoreFront über die Einstellungen der Offline-Authentifizierungs-Policy in der Sicherheitskonsole aktivieren.

Kapitel 5: Citrix Delegated Forms Authentication

Citrix Delegated Forms Authentication

Das Citrix Delegated Forms Authentication (DFA)-Protokoll ermöglicht, dass StoreFront Authentifizierungsservices für den NetScaler-Gateway bereitstellt. DFA ist eine Voraussetzung für die Erweiterung von Agent for Citrix StoreFront, um Nutzer entweder mit RSA SecurID oder RBA zu authentifizieren.

Führen Sie diese übergeordneten Schritte aus, damit DFA für Citrix StoreFront die RSA SecurID-Authentifizierungsservices für das Citrix NetScaler-Gateway bereitstellen kann.

1. Schützen Sie die Anmeldung an StoreFront mit RSA SecurID-Authentifizierung mit dem Agent for Citrix StoreFront. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der RSA SecurID-Authentifizierung auf Seite 47.
2. Aktivieren Sie DFA auf Citrix StoreFront und schützen Sie DFA mit RSA SecurID, wie unter Aktivieren der RSA SecurID-Authentifizierung für DFA unten beschrieben.
3. Wenden Sie angepasste Skripte an, um NetScaler-Designs zur Unterstützung von RSA SecurID-Authentifizierung zu aktivieren. Siehe Anwenden von RSA SecurID-Authentifizierungsskripten auf NetScaler-Designs auf Seite 61.
4. Konfigurieren Sie den NetScaler-Gateway, um DFA zur Authentifizierung bei Citrix StoreFront zu verwenden.
   Weitere Informationen finden Sie in den DFA-Konfigurationsschritten, die im *SecurID Access Implementierungsleitfaden für Citrix Netscaler Gateway* von RSA Ready-Technologieintegrationen auf RSA Link unter https://community.rsa.com/docs/DOC-66800 beschrieben sind.
5. Konfigurieren Sie StoreFront, um Remotezugriff über NetScaler-Gateway bereitzustellen.
   Anleitungen zur Konfiguration von DFA auf NetScaler-Gateway finden Sie auf der Citrix-Dokumentationswebsite unter http://docs.citrix.com und indem Sie nach „Configure NetScaler Gateway connection settings" suchen.

Hinweis: Wenn Sie DFA auf einem StoreFront-Server in einer StoreFront-Servergruppe konfigurieren, müssen Sie Änderungen an alle Server in der Gruppe weitergeben.

Hinweis: Wenn Sie den optionalen Parameter `-tenantID` bei der Ausführung des Befehls `Install-DFAServer` festlegen, müssen Sie diese tenantID in den `-VirtualPath`, der in allen Befehlen in diesem Kapitel verwendet wird, wie folgt einbeziehen:

```
-VirtualPath /Citrix/DelegatedForms/<tenantID>/Default
```

Diese PowerShell-Befehle werden auch im Dokument *Konfigurieren von Citrix Storefront für Delegierte Formularauthentifizierung mit RSA SecurID* beschrieben. Sie können über die Citrix StoreFront-Managementkonsole auf dieses Dokument zugreifen oder die neueste Version von RSA Link herunterladen.

Aktivieren der RSA SecurID-Authentifizierung für DFA

Führen Sie das folgende Verfahren aus, um die SecurID-Authentifizierung für DFA zu aktivieren.

Vorbereitung

Installieren und konfigurieren Sie den DFA-Server auf Citrix StoreFront. Befolgen Sie die Anweisungen im von

Citrix bereitgestellten Readme-Dokument *StoreFront Services Delegated Forms Server Management* unter ***<Citrix StoreFront-Installationsverzeichnis>*\Management\Cmdlets\DFAServerFPReadMe.rtf**.

Verfahren

1. Öffnen Sie ein PowerShell-Befehlsfenster und laden Sie die Citrix StoreFront-Module mit dem von Citrix bereitgestellten Skript **ImportModules.ps1**, wie in der Readme-Datei *Storefront Services Delegated Forms Server Management* beschrieben.
2. Geben Sie den folgenden Befehl ein, um das Protokoll „Nutzerdefinierte Formulare" zu DFA hinzuzufügen:

   ```
   Add-STFAuthenticationServiceProtocol -Name CustomForms -AuthenticationService
   (Get-STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/Default)
   ```

3. Um DFA mit RSA SecurID-Authentifizierung zu schützen, geben Sie den folgenden Befehl ein:

   ```
   Set-DSDFAProperty -conversationfactory SecurIDAuthentication
   ```

4. (Optional) Wenn die Namen Ihrer vertrauenswürdigen Nutzer nicht vollständig qualifiziert sind und Sie DFA mit RBA schützen möchten, müssen Sie vertrauenswürdige Domains für DFA konfigurieren. Geben Sie den folgenden Befehl ein:

   ```
   Set-STFExplicitCommonOptions -authenticationservice (Get-
   STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/Default) -Domains
   @("domain1”, “domain2") -DefaultDomain "domain1"
   ```

Deaktivieren der RSA SecurID-Authentifizierung für DFA

Führen Sie das folgende Verfahren aus, um die SecurID-Authentifizierung für DFA zu deaktivieren.

Hinweis: Sie müssen RSA SecurID-Authentifizierung für DFA deaktivieren, bevor Sie Agent for Citrix StoreFront deinstallieren können.

Verfahren

1. Öffnen Sie ein PowerShell-Befehlsfenster und laden Sie die Citrix StoreFront-Module mit dem von Citrix bereitgestellten Skript **ImportModules.ps1**, wie in der Readme-Datei *Storefront Services Delegated Forms Server Management* beschrieben.
2. Geben Sie zum Zurücksetzen des DFA-Schutzes auf die standardmäßige Authentifizierung mit Citrix-Nutzername und Passwort den folgenden Befehl ein:

   ```
   Set-DSDFAProperty -conversationfactory ExplicitAuthentication
   ```

3. Geben Sie den folgenden Befehl ein, um das Protokoll „Nutzerdefinierte Formulare" aus DFA zu entfernen:

   ```
   Remove-STFAuthenticationServiceProtocol -Name CustomForms -
   AuthenticationService (Get-STFAuthenticationService -VirtualPath
   /Citrix/DelegatedForms/Default)
   ```

4. (Optional) Um die vertrauenswürdigen Domains für DFA zu löschen, geben Sie den folgenden Befehl ein:

   ```
   Set-STFExplicitCommonOptions -authenticationservice (Get-
   STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/Default) Domains @
   () -DefaultDomain ""
   ```

Anwenden von RSA SecurID-Authentifizierungsskripten auf NetScaler-Designs

Bevor Agent for Citrix StoreFront RSA SecurID-Authentifizierung über Citrix NetScaler bereitstellen kann, müssen Sie die Nutzerportal-Designdateien und -skripte auf der NetScaler-Appliance manuell ändern.

Hinweis: Agent for Citrix StoreFront unterstützt nur die NetScaler-Designs „RfWebUI" und „X1" oder angepasste Designs, die mithilfe dieser Designs als Vorlagen erstellt wurden.

Vorbereitung

- Kopieren Sie **open-sans.woff**, **SecurID.js** und **SecurID.css** aus dem NetScaler-Ordner im Installationsverzeichnis des Agent auf dem Citrix StoreFront-Server an einen Speicherort auf der NetScaler-Appliance.
- (Optional) Wenn Sie ein benutzerdefiniertes Design verwenden möchten, erstellen Sie ein neues Portal-Design auf der NetScaler-Appliance, indem Sie entweder „RfWebUI" oder „x1" als Designvorlage (Theme-Copy) verwenden, das Thema dann an den virtuellen Server binden und es anwenden. Weitere Informationen hierzu finden Sie in Ihrer Citrix-Dokumentation.

Verfahren

1. Melden Sie sich bei der NetScaler-Appliance an.
2. Kopieren Sie **open-sans.woff** je nach Ihrem Design in eines der folgenden Verzeichnisse:
   - Für Standarddesigns: **/var/netcscaler/logon/LogonPoint/custom/**
   - Für benutzerdefinierte Designs: **/var/netcscaler/logon/themes/theme-copy/**

3. Hängen Sie im selben Verzeichnis die Inhalte von **SecurID.css** und **SecurID.js** an die **Dateien Style. CSS** und **Script. js** an.

Kapitel 6: Aktivieren von RSA Authentication Manager Risk-Based Authentication

Aktivieren der RSA Authentication Manager Risk-Based Authentication

Wenn Agent for Citrix StoreFront im AM UDP-Modus installiert ist, können Sie RSA Authentication Manager Risk-Based Authentication (RBA) aktivieren, um die Anmeldung bei Citrix Storefront von Nutzern zu schützen, die sich über das NetScaler-Gateway authentifizieren. Nutzer, die sich mit RBA authentifizieren, werden über StoreFront angemeldet und müssen die Anmeldedaten nicht ein zweites Mal eingeben.

Die Aktivierung von RBA zum Schutz von StoreFront umfasst die folgenden Schritte:

1. Schützen Sie die Anmeldung bei StoreFront mit RSA SecurID-Authentifizierung mit dem Agent for Citrix StoreFront. Weitere Informationen finden Sie unter Managen von RSA SecurID-Authentifizierung mithilfe der Citrix StoreFront-Managementkonsole auf Seite 45.
2. Aktivieren Sie Citrix Delegated Forms Authentication (DFA), um die RSA SecurID-Authentifizierung über das NetScaler-Gateway zu erweitern. Weitere Informationen finden Sie unter Citrix Delegated Forms Authentication auf Seite 59.
3. Installieren Sie die Webanwendung „RSA Risk-Based Authentication Helper", um einen Verbindungspunkt zwischen der RBA-Authentifizierung und Agent for Citrix StoreFront bereitzustellen. Weitere Informationen finden Sie unter Installieren von RBA Helper unten.
4. Integrieren Sie RSA Authentication Manager und NetScaler-Gateway mit Agent for Citrix StoreFront. Anweisungen dazu finden Sie im *RBA-Implementierungsleitfaden*, der auf RSA Link unter https://community.rsa.com/docs/DOC-66800 verfügbar ist.

RSA Authentication Manager Risk-Based Authentication Helper

Der RSA Authentication Manager Risk-Based Authentication Helper (RBA Helper) ist eine Webanwendung, die RSA Authentication Manager RBA und Agent for Citrix StoreFront miteinander verbindet. Das RBA Helper-Installationsprogramm ist als Teil von Agent for Citrix StoreFront verfügbar.

Der RBA Helper macht Folgendes:

- Er stellt ein Formular bereit, in dem Authentication Manager die Ausgabe einer erfolgreichen RBA-Authentifizierung schreiben kann.
- Er leitet die Authentifizierung an einen virtuellen NetScaler-Server weiter, der DFA für Citrix StoreFront aufruft.

Installieren von RBA Helper

Zum Installieren des RBA Helper können Sie den Installationsassistenten oder die Befehlszeile verwenden.

Hinweis: Agent for Citrix StoreFront unterstützt RBA Helper Version 1.5 oder höher. Sie müssen keine neue Version von RBA Helper installieren, wenn Version 1.5 oder höher bereits installiert ist.

Sicherheitsempfehlungen

Auf den RBA Helper muss über HTTPS zugegriffen werden, um Authentication Manager RBA mit Agent for Citrix

StoreFront zu integrieren und die Nutzer-RBA-Anmeldeinformationen während der Übertragung zu schützen.

RSA empfiehlt, dass Sie Microsoft Internet Information Services (IIS), die den RBA Helper hosten, für die Verwendung von HTTPS konfigurieren. Informationen zur Konfiguration von IIS für die Verwendung von HTTPS finden Sie auf der Website der Microsoft IIS-Dokumentation unter http://www.iis.net. Suchen Sie nach *TLS/SSL*.

RSA empfiehlt auch, dass Sie den Microsoft TLS/SSL Security Provider (der vom IIS verwendet wird) für die Verwendung von Transport Layer Security (TLS) v1.2 oder höher konfigurieren. Informationen zur Konfiguration des Microsoft TLS/SSL Security Provider für die Verwendung von TLS v1.2 finden Sie in der Microsoft-Dokumentation unter http://support.microsoft.com. Suchen Sie nach *Beschränken der Verwendung bestimmter kryptografischer Algorithmen und Protokolle in "Schannel.dll"*. Hinweise zur Konfiguration von TLS finden Sie in den Veröffentlichungen des National Institute of Standards and Technology über Computersicherheit unter http://csrc.nist.gov/publications/PubsSPs.html. Suchen Sie nach *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

Installieren über den Installationsassistenten

Um RBA Helper mit dem Installationsassistenten zu installieren, führen Sie die folgenden Schritte aus:

Vorbereitung

- Bestätigen Sie, dass Sie die Sicherheitsempfehlungen beachtet haben.
- Sie müssen über Administratorrechte für den Server verfügen, auf dem Sie RBA Helper installieren.
- Überprüfen Sie, ob der Server, auf dem Sie RBA Helper installieren, die folgenden Anforderungen erfüllt:
  - .NET Framework 4.5 oder höher
  - ASP.NET 4.5 fähig
  - Internet Information Services (IIS)
  - Version 7.5, 8.0, 8.5 oder 10.0
  - Webserverrolle mit aktiviertem ASP.NET 4.5
  - HTTPS aktiviert
- Kopieren Sie das Downloadpaket, das **RSA Authentication Manager Risk-Based Authentication Helper x64.msi** enthält, in einen Ordner auf dem Computer, in dem Sie RBA Helper installieren möchten.

Hinweis: Der Installationsassistent installiert den RBA Helper auf der Standardwebsite. Installieren Sie RBA Helper über die Befehlszeile, um RBA Helper auf einer anderen Website zu installieren.

Verfahren

1. Doppelklicken Sie in dem Ordner, in den Sie die Installationsdatei kopiert haben, auf **RSA Authentication Manager Risk-Based Authentication Helper x64.msi**, um den Installationsassistenten zu starten.
2. Klicken Sie auf **Weiter**, um fortzufahren.
3. Lesen und bestätigen Sie die Lizenzvereinbarung oder klicken Sie auf **Drucken**, um Sie zu drucken. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Installieren**.
5. Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.

Nach Abschluss

Überprüfen, ob RBA Helper funktioniert unten

Installieren mithilfe von Befehlszeilenoptionen

Sie können den RBA Helper über die Befehlszeile installieren.

Vorbereitung

- Bestätigen Sie, dass Sie die Sicherheitsempfehlungen beachtet haben.
- Sie müssen über Administratorrechte für den Server verfügen, auf dem Sie RBA Helper installieren.
- Überprüfen Sie, ob der Server, auf dem Sie RBA Helper installieren, die folgenden Anforderungen erfüllt:
  - .NET Framework 4.5 oder höher
  - ASP.NET 4.5 fähig
  - Internet Information Services (IIS)
  - Version 7.5, 8.0, 8.5 oder 10.0
  - Webserverrolle mit aktiviertem ASP.NET 4.5
  - HTTPS aktiviert
- Kopieren Sie das Downloadpaket, das **RSA Authentication Manager Risk-Based Authentication Helper x64.msi** enthält, in einen Ordner auf dem Computer, in dem Sie RBA Helper installieren möchten.

Verfahren

1. Öffnen Sie eine Administrator-Eingabeaufforderung.
2. Navigieren Sie zu dem Ordner, in den Sie die Installationsdatei kopiert haben, oder geben Sie den vollständigen Pfadnamen zur Installationsdatei in der Befehlszeile an.
3. Führen Sie einen der folgenden Schritte aus:
   - Um RBA Helper auf der Standardwebsite zu installieren, verwenden Sie einen Befehl ähnlich dem folgenden:
     ```
     msiexec /qn /i "RSA Authentication Manager Risk-Based Authentication
     Helper x64.msi"
     ```
   - Um RBA Helper auf einer anderen Website zu installieren, verwenden Sie einen Befehl ähnlich dem folgenden:
     ```
     msiexec /qn /i "RSA Authentication Manager Risk-Based Authentication
     Helper x64.msi" PARENT_WEBSITE="<Nicht-Standardwebsite>"
     ```

   Wenn der angegebene Speicherort nicht vorhanden ist, installiert das Installationsprogramm den RBA Helper auf der Standardwebsite.

Nach Abschluss

Überprüfen, ob RBA Helper funktioniert unten

Überprüfen, ob RBA Helper funktioniert

Führen Sie nach der Installation von RBA Helper das folgende Verfahren durch, um zu überprüfen, ob er funktioniert.

Vorbereitung

Vergewissern Sie sich, dass die Webanwendung RBA Helper ausgeführt wird.

Verfahren

1. Öffnen Sie Internet Information Services (IIS) Manager.
2. Öffnen Sie im Bereich „Verbindungen" **Websites > Standardwebsite** (oder die Website, auf der RBA Helper installiert wurde).
3. Überprüfen Sie, ob RBA Helper als Webanwendung installiert wurde.
4. Klicken Sie mit der rechten Maustaste auf **RSAAuthMgrRbaHelper**.
5. Bestätigen Sie, dass **Anwendung managen** als Option im Kontextmenü angezeigt wird.

Kapitel 7: Troubleshooting

Troubleshooting

Dieses Kapitel enthält Informationen zum Troubleshooting und Details zu Fehlermeldungen. Melden Sie sich bei RSA Link unter https://community.rsa.com an, um weitere Informationen zum Troubleshooting zu erhalten.

Probleme bei der Installation und Deinstallation

Wenn die Installation oder Deinstallation nicht erfolgreich ist, überprüfen Sie Ihre Protokolldatei (z. B. **%USERPROFILE%\install.log**), um festzustellen, welches Problem den Fehler verursacht haben könnte. Wenn Sie eine interaktive Installation verwenden, stoppt das Installationsprogramm und eine Fehlermeldung wird angezeigt.

Problem	Lösung
Citrix StoreFront ist nicht installiert.	Wenden Sie sich an Citrix, um Citrix StoreFront herunterzuladen und zu installieren. Führen Sie das Installationsprogramm aus.
Microsoft .NET Framework 4.5 oder höher ist nicht installiert.	Wenden Sie sich an Microsoft, um .NET Framework 4.5 herunterzuladen und zu installieren. Führen Sie das Installationsprogramm aus.
Die Installation schlägt fehl, wenn Sie das Dienstprogramm zur automatischen Registrierung mit RSA Authentication Agent für Citrix StoreFront installieren, es jedoch bereits mit RSA Authentication Agent für Windows installiert ist.	Das Dienstprogramm für die automatische Registrierung kann nur von einem Authentifizierungs-Agent installiert werden. Wählen Sie das Dienstprogramm zur automatischen Registrierung nicht aus, wenn es bereits mit RSA Authentication Agent für Windows installiert ist. Führen Sie das Installationsprogramm aus.
Agent for Citrix StoreFront kann nicht deinstalliert werden, wenn Citrix StoreFront bereits deinstalliert wurde.	Installieren Sie Citrix StoreFront neu und schließen Sie die Citrix StoreFront MMC (die automatisch geöffnet wird). Deinstallieren Sie Agent for Citrix StoreFront und deinstallieren Sie anschließend Citrix Storefront.
Die Citrix StoreFront-Managementkonsole reagiert nicht mehr, wenn Sie während der Installation von Agent for Citrix StoreFront ausgeführt wird.	Schließen Sie die Citrix StoreFront-Managementkonsole, bevor Sie Agent for Citrix StoreFront installieren.

Probleme mit Schnittstellen

In diesem Abschnitt werden Probleme im Zusammenhang mit Schnittstellenkomponenten, die von Agent for Citrix StoreFront verwendet werden, beschrieben.

Problem	Lösung
Freigegebene Citrix StoreFront Speicher zeigen die aktualisierte Agent for Citrix StoreFront-Konfigurationsschnittstelle nicht an, nachdem	Gehen Sie wie folgt vor: Deaktivieren Sie die RSA SecurID-Authentifizierung für den freigegebenen Speicher und aktivieren Sie diese

Problem	Lösung
der Agent von Version 1.5 auf 2.0 aktualisiert wurde.	anschließend erneut. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der RSA SecurID-Authentifizierung auf Seite 47.

Probleme bei der Koexistenz mit RSA Authentication Agent for Microsoft Windows

In diesem Abschnitt werden Probleme beschrieben, die auftreten können, wenn der RSA Authentication Agent for Microsoft Windows (Windows-Agent) und der RSA Authentication Agent for Citrix StoreFront (Citrix-Agent) beide auf einem Citrix Storefront-Server installiert sind.

Problem	Lösung
Die Offline-Authentifizierung für den Windows-Agent ist nicht verfügbar, wenn beide Agents installiert sind.	Agent for Citrix StoreFront deaktiviert den Download von Offlinedaten. So aktivieren Sie diese Funktion erneut: 1. Öffnen Sie den Registrierungs-Editor: Klicken Sie auf **Start**. Geben Sie **regedit** in das Suchfeld ein und klicken Sie in der Ergebnisliste unter „Programme" auf **regedit**. 2. Öffnen Sie den Schlüssel: **HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT** 3. Ändern Sie den Wert von **NoDADownload** (a REG_DWORD) von **1** auf **0**.
Nach der Deinstallation eines der Agents kann der Service **OASVC_LOCAL** nicht neu gestartet werden.	Reparieren Sie die Installation für den Authentifizierungs-Agent, der noch auf dem Citrix StoreFront-Server installiert ist. Informationen zum Reparieren von Agent for Citrix StoreFront finden Sie unter Reparieren einer Installation auf Seite 35.
Nachdem ein Administrator den Node-Schlüssel mithilfe von RSA Control Center für den Windows-Agent gelöscht hat, schlägt die Citrix StoreFront-Authentifizierung im AM UDP-Modus fehl und der Citrix-Agent zeigt einen Nichtübereinstimmungsfehler des Node-Schlüssels an.	Gehen Sie wie folgt vor: 1. Starten Sie **AuthAPIService** und **sdadmreg** auf dem Citrix Storefront-Server neu. 2. Führen Sie eine Testauthentifizierung mithilfe von RSA Control Center für den Windows-Agent durch.
Nachdem ein Administrator den Node-Schlüssel mithilfe von RSA Control Center für den Windows-Agent gelöscht hat, funktioniert WPI für den Citrix-Agent im AM REST-Modus nicht mehr. Dieses Problem tritt nur auf, wenn der Windows-Agent und der Citrix-Agent den gleichen Agent-Namen verwenden.	Gehen Sie wie folgt vor: 1. Führen Sie eine Testauthentifizierung mithilfe von RSA Control Center für den Windows-Agent durch. 2. Klicken Sie auf der Seite „SecurID-Optionen für den Citrix-Agent managen" auf **WPI managen** und wählen Sie dann **Node-Schlüssel vom UDP-Modus verwenden** aus.
Nachdem ein Administrator den	Starten Sie sdadmreg auf dem Citrix Storefront-Server neu.

Problem	Lösung
Node-Schlüssel für den Citrix-Agent im AM UDP-Modus gelöscht hat, schlägt die Authentifizierung des Windows-Agent fehl. Dieses Problem tritt nur auf, wenn die automatische Registrierung von Agents für den Windows-Agent installiert ist.	
Wenn ein Administrator den Node-Schlüssel löscht oder einen neuen Node-Schlüssel für den Citrix-Agent im AM REST-Modus generiert, schlägt die Windows-Agent-Authentifizierung fehl und der Windows-Agent zeigt die Fehlermeldung „Node-Schlüssel stimmt nicht überein: gelöscht auf dem Agent, aber nicht auf dem Server" an. Dieses Problem tritt nur auf, wenn der Windows-Agent und der Citrix-Agent den gleichen Agent-Namen verwenden.	Gehen Sie wie folgt vor: 1. Deaktivieren Sie den Node-Schlüssel für den Windows-Agent in Authentication Manager. 2. Führen Sie eine Testauthentifizierung mithilfe von RSA Control Center für den Windows-Agent durch. 3. Klicken Sie auf der Seite „SecurID-Optionen für den Citrix-Agent managen" auf **WPI managen** und wählen Sie dann **Node-Schlüssel vom UDP-Modus verwenden** aus.
Windows Agent-Services werden nach dem Ändern des Citrix-Agent-Authentifizierungsmodus beendet.	Reparieren Sie die Installation des Windows-Agent.

Probleme bei Delegated Forms Authentication (DFA)

In diesem Abschnitt werden Probleme in Zusammenhang mit DFA beschrieben.

Problem	Lösung
Wenn bei der Installation des DFA-Servers eine optionale tenantID festgelegt wurde, schlagen PowerShell Befehle, die auf VirtualPath basieren, fehl.	Schließen Sie die tenantID bei Befehlen ein, die auf VirtualPath basieren. Beispiel: Ersetzen: (Get-STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/Default) durch: (Get-STFAuthenticationService -VirtualPath /Citrix/DelegatedForms/[tenantID]/Default)

Probleme beim Protokollieren

In diesem Abschnitt werden Probleme beschrieben, die im Zusammenhang mit von Agent for Citrix StoreFront

erzeugten Protokollen auftreten.

Problem	Lösung
Änderungen an der Protokollierungskonfiguration oder an Optionen in der Citrix StoreFront-Managementkonsole werden in den Agent-Protokollen nicht angezeigt, wenn benutzerdefinierte Formulare aktiviert werden.	Deaktivieren Sie angepasste Formulare und aktivieren Sie diese anschließend erneut.
Wenn Agent for Citrix StoreFront im AM UDP-Modus konfiguriert ist und die Ablaufverfolgung so festgelegt ist, dass Protokolle an einem angepassten Speicherort gespeichert werden, wird der Protokollordner nicht automatisch gelöscht, wenn der Agent deinstalliert wird.	Löschen Sie nach der Deinstallation des Agent das angepasste Protokollverzeichnis manuell.

Probleme bei der Authentifizierung

In diesem Abschnitt werden Probleme im Zusammenhang mit der Authentifizierung beschrieben sowie Verfahren, mit denen Sie diese beheben können.

Problem	Lösung
RSA Authentication Manager und der Agent-Host können nicht kommunizieren. Der Agent for Citrix StoreFront ist im AM UDP-Modus installiert.	Authentication Manager und der Agent-Host verfügen möglicherweise nicht über kompatible Kopien der Systemkonfigurationsdatei (**sdconf.rec**). Vergewissern Sie sich, dass Sie die richtige **sdconf.rec**-Datei haben. 1. Öffnen Sie die Citrix StoreFront-Managementkonsole auf Seite 45. 2. Öffnen Sie die Seite „SecurID-Optionen managen“ auf Seite 52. 3. Vergewissern Sie sich, dass AM UDP im Drop-down-Menü **Authentifizierungsmodus** ausgewählt ist. 4. Klicken Sie auf **Serverumgebung**. Auf der linken Seite des Dialogfelds werden Informationen über den Status des Authentication Manager-Servers und die Kommunikation mit dem Agent angezeigt.
Sie erhalten die Fehlermeldung „Die Serverumgebung konnte nicht abgerufen werden“, wenn Sie versuchen, die Systemkonfigurationsdatei (**sdconf.rec**) mithilfe der Option „Serverumgebung“ auf der Seite „SecurID-Optionen managen“ zu überprüfen und die Agent for Citrix StoreFront im AM UDP-Modus	Die Datei **sdconf.rec** ist beschädigt und muss ersetzt werden. 1. Rufen Sie eine neue **sdconf.rec**-Datei von RSA Authentication Manager ab. 2. Navigieren Sie zum Verzeichnis **C:\Program Files\Common Files\RSA Shared\Auth Data**, in dem die vorhandene **sdconf.rec**-Datei auf dem Agent-Host gespeichert ist. 3. Ersetzen Sie die vorhandene **sdconf.rec**-Datei durch die neue

Problem	Lösung
installiert ist.	Datei. **Hinweis:** Stellen Sie sicher, dass Ihre Spyware oder Virenschutzsoftware den Node-Schlüssel oder die Datei **sdconf.rec** nicht automatisch entfernt.
Es treten Probleme bei der Authentifizierung auf, wenn Agent for Citrix StoreFront im AM UDP-Modus installiert wird.	Möglicherweise müssen Sie eine beschädigte **server.cer**-Datei ersetzen, um Probleme bei der Authentifizierung zu beheben. 1. Rufen Sie eine neue **server.cer**-Datei von RSA Authentication Manager ab. 2. Öffnen Sie **Verwaltungsprogramme > Services** und beenden Sie den Service **Automatische Registrierung des RSA Authentication Agent**. 3. Navigieren Sie zu dem Verzeichnis **C:\Program Files\RSA\RSA Authentication Agent\Agenthost Autoreg Utility**, wo die vorhandene Datei **server.cer** gespeichert ist. 4. Ersetzen Sie die vorhandene **server.cer**-Datei durch die neue Datei. 5. Starten Sie den Service für die **automatische Registrierung des RSA Authentication Agent**.
Der Agent protokolliert keine Standortdetails, wenn sich Nutzer mit Mozilla Firefox authentifizieren.	Weisen Sie Nutzer an, mithilfe der folgenden Schritte die Sammlung von Geostandortdaten in FireFox zu aktivieren: 1. Geben Sie in der Adressleiste „about:config" ein. 2. Ändern Sie den Wert für geo.wifi.ui zu: https://location.services.mozilla.com/v1/geolocate?key=test
Nach dem Ändern des Authentifizierungsmodus von AM REST auf AM UDP schlägt die Authentifizierung fehl und der Agent zeigt folgende Fehlermeldung an: „Node-Schlüssel stimmt nicht überein: gelöscht auf dem Agent, aber nicht auf dem Server".	Deaktivieren Sie den Node-Schlüssel für den Agent in der Authentication Manager-Sicherheitskonsole und führen Sie dann eine Testauthentifizierung auf der Seite „SecurID-Optionen managen" der Citrix StoreFront-Managementkonsole aus. Weitere Informationen finden Sie unter Durchführen einer Testauthentifizierung. auf Seite 54.
Die Authentifizierung schlägt im AM REST-Modus fehl und Citrix StoreFront zeigt die Fehlermeldung an: „Ihre Anforderung kann nicht abgeschlossen werden".	Gehen Sie wie folgt vor: • Prüfen Sie die Agent-Protokolle auf Fehler bei der Zertifikatvalidierung und importieren Sie bei Bedarf gültige vertrauenswürdige Stammzertifikate. Weitere Informationen finden Sie unter Importieren des vertrauenswürdigen Stammzertifikats für Authentication Manager oder den Cloudauthentifizierungsservice auf Seite 22. • Überprüfen Sie die Agent-Protokolle auf Fehler der REST-Konfigurationsdatei und reparieren Sie die Agent-Installation bei Bedarf Weitere Informationen finden Sie unter Reparieren einer Installation auf Seite 35.

Diagnose von Problemen mit RSA Authentication Manager mit Risk-Based Authentication Helper

Sie können Aufgaben zur Diagnose von Problemen ausführen, die bei der Unterstützung der Integration mit Authentication Manager Risk-Based Authentication (RBA) auftreten können.

Eine erste Aufgabe ist die Aktivierung der Ablaufverfolgung. Weitere Informationen finden Sie unter Aktivieren der Nachverfolgung auf Seite 55. Weitere Aufgaben werden nachfolgend beschrieben.

Anzeige des RSAAuthMgrRbaHelper-Formulars aktivieren

Standardmäßig wird in RSAAuthMgrRbaHelper nicht das Formular angezeigt, das zur Unterstützung der Integration mit RBA verwendet wird. Sie können die Anzeige des Formulars in RSAAuthMgrRbaHelper aktivieren, wenn Sie vom RSA Kundensupport dazu aufgefordert werden.

Verfahren

1. Öffnen Sie Internet Information Services (IIS) Manager.
2. Öffnen Sie im Bereich „Verbindungen" **Websites > Standardwebsite** oder die Website, auf der RSAAuthMgrRbaHelper installiert ist.
3. Wählen Sie **RSAAuthMgrRbaHelper** aus.
4. Wählen Sie im Bereich „Aktionen" die Option **Erkunden** aus.
5. Verwenden Sie im Explorer-Fenster, das geöffnet wird, einen Texteditor, um die Datei **web.config** zu öffnen.
6. Suchen Sie das Attribut `<add key="allowHttpGet" value="false"/>` unter dem Element `<appSettings>`.
7. Ändern Sie den Wert von **false** auf **true**.
8. Speichern Sie die Datei **web.config**.
9. Um zu überprüfen, ob das Formular angezeigt werden kann, wählen Sie im Bereich „Aktionen" **Durchsuchen*:80 (http)** oder **Durchsuchen*:443 (https)** aus. Internet Explorer zeigt das RBA Helper-Formular an.

Hinweis: Wenn Sie durch **Durchsuchen*:443 (https)** auswählen, wird möglicherweise eine Zertifikatwarnung angezeigt, da IIS Manager einen Servernamen **localhost** verwendet, der wahrscheinlich nicht mit dem Serverattribut im SSL-Zertifikat übereinstimmt. Sie können diese Warnmeldung ignorieren.

Fehler- und Event Viewer-Protokollmeldungen

Wenn Agent for Citrix StoreFront im AM UDP-Modus installiert ist, werden Fehler- und Ereignismeldungen in den folgenden Kategorien in den Windows Event Viewer geschrieben:

- ACECLIENT
- AuthAPIService
- Automatische Registrierung von RSA Agents
- Automatische Registrierung des RSA Authentication Agent
- RSA SecurID-Authentifikator

Meldung	Beschreibung
AVOID-Befehl hat ungültige IP-Adresse in SDOPTS.REC-Datei.	Die IP-Adresse, die mit dem Parameter „AVOID" in der Datei **sdopts.rec** verknüpft ist, ist ungültig. Informationen zum Erstellen einer korrekt formatierten **sdopts.rec**-Datei finden Sie in Automatischer Lastenausgleich auf Seite 81.
Standard-IP-Adresse kann in SDOPTS.REC-Dateiadresse nicht vermieden werden.	Der Parameter „AVOID" funktioniert nicht mit der in der Datei **sdopts.rec** angegebenen Standard-IP-Adresse. Informationen zum Erstellen einer korrekt formatierten **sdopts.rec**-Datei finden Sie in Automatischer Lastenausgleich auf Seite 81.
Doppelte AVOID-Anweisungen in SDOPTS.REC-Datei	Es gibt zwei identische AVOID-Anweisungen in der Datei **sdopts.rec**. Informationen zum Erstellen einer korrekt formatierten **sdopts.rec**-Datei finden Sie in Automatischer Lastenausgleich auf Seite 81.
Falsche Größe für Datei: sdconf.rec	Die Datei **sdconf.rec** wurde wahrscheinlich nicht im binären Modus kopiert. Fragen Sie den Authentication Manager-Administrator nach einer neuen Kopie von **sdconf.rec**.
Datei nicht gefunden: aceclnt.dll	Die Software wurde möglicherweise falsch installiert oder **aceclnt.dll** wurde gelöscht. Installieren sie die Citrix Agent-Software erneut aus der MSI-Datei (**RSA Authentication Agent for Citrix StoreFront x64.msi**).
Datei nicht gefunden: sdconf.rec	Die Datei **sdconf.rec** ist nicht im Verzeichnis **HKLM\Software\RSA\RSA Authentication Agent\AuthDataDir**. Sie wurde entweder entfernt oder nie von Authentication Manager kopiert. Fragen Sie Ihren Authentication Manager-Administrator nach einer neuen Kopie von **sdconf.rec**.
Netzwerk-Timeout: Authentication Manager hat reagiert, wurde aber jetzt beendet.	Vergewissern Sie sich, dass der Authentication Manager-Prozess auf dem-Server ausgeführt wird. Prüfen Sie auf ein Netzwerkproblem, wie z. B. eine Routerfehlfunktion oder ein nicht eingestecktes Netzwerkkabel.
Nutzer <*Nutzername*> hat die neue PIN-Routine abgebrochen.	Der Nutzer hat den Authentifizierungsversuch im neuen PIN-Modus abgebrochen.
Nutzer <*Nutzername*> hat die Authentifizierungsroutine abgebrochen.	Der Nutzer hat abgebrochen, ohne einen Nutzernamen einzugeben.
Nutzer <*Nutzername*>: ZUGRIFF VERWEIGERT.	Dem Nutzer wurde der Zugriff verweigert. Prüfen Sie das Authentication Manager-Aktivitätsprotokolls, um den spezifischen Grund zu erfahren.
Nutzer <*Nutzername*>: ZUGRIFF VERWEIGERT. Nächster Tokencode fehlgeschlagen.	Der Nutzer konnte sich im Modus „Nächster Tokencode" nicht authentifizieren und muss versuchen, sich erneut zu authentifizieren.
Nutzer <*Nutzername*>: ZUGRIFF VERWEIGERT. Serversignatur ungültig.	Die Identität des Authentication Manager konnte nicht durch den Authentifizierungs-Agent verifiziert werden. Wenden Sie sich an den RSA Kundensupport.
Nutzer <*Nutzername*> hat die „Nächster Tokencode"-Routine abgebrochen.	Der Nutzer hat den „Nächster Tokencode"-Prozess abgebrochen.
Nutzer <*Nutzername*>: Neue PIN wurde	Die neue RSA SecurID-PIN des Nutzers wurde überprüft.

Meldung	**Beschreibung**
akzeptiert	
Nutzer <*Nutzername*>: Neue PIN wurde abgelehnt	Die RSA SecurID-PIN wurde vom Authentication Manager abgelehnt. Der Nutzer muss sich erneut authentifizieren, um die RSA SecurID-PIN festzulegen. Überprüfen Sie das Authentication Manager-Aktivitätsprotokoll.
Nutzer <*Nutzername***>**: PASSCODE akzeptiert	Der Passcode des Nutzers wurde akzeptiert.
Nutzer <*Nutzername***>**: Erfolgreiche Anmeldung MIT „Nächster Tokencode"	Authentication Manager hat den nächsten Tokencode akzeptiert und dem Nutzer Zugriff gewährt.
USESERVER und AVOID können nicht beide in der sdopts-Datei verwendet werden.	Die Datei **sdopts.rec** versucht, sowohl USESERVER als auch AVOID zu verwenden. Informationen zum Erstellen einer korrekt formatierten **sdopts.rec**-Datei finden Sie in Automatischer Lastenausgleich auf Seite 81.

Anhang A: Konfigurieren des automatischen Lastenausgleichs für den AM UDP-Modus

Automatischer Lastenausgleich

Wenn der Agent for Citrix StoreFront im AM UDP-Modus installiert ist, konfigurieren Sie den Authentifizierungs-Agent so, dass er die Lasten der Authentifizierungsanfragen automatisch ausgleicht, indem er eine Datei mit Optionen für den Lastenausgleich (**sdopts.rec**) erstellt. Die Datei **sdopts.rec** ist eine Textdatei, die auf dem Host des Authentifizierungs-Agent gespeichert ist (dem Computer, auf dem ein Agent installiert ist). In der Datei können Sie einen dynamischen oder manuellen Lastenausgleich angeben. Sie müssen sich als Administrator anmelden, wenn Sie die Datei **sdopts.rec** ändern möchten.

Hinweis: Der Lastenausgleich kann im CAS-Modus nicht konfiguriert werden. Im AM REST-Modus, wählen Sie ein Lastenausgleichsschema aus, wenn Sie den Agent installieren oder die Agent-Einstellungen konfigurieren. Weitere Informationen finden Sie unter Managen von Agent-Einstellungen auf Seite 47.

Dynamischer Lastenausgleich

Bei dynamischem Lastenausgleich sendet der Authentifizierungs-Agent eine Zeitanforderung an jeden RSA Authentication Manager-Server im Bereich und bestimmt eine Prioritätenliste basierend auf der Antwortzeit der einzelnen Server. Der Authentication Manager-Server mit der schnellsten Antwortzeit erhält die höchste Priorität und erhält die größte Anzahl von Authentifizierungsanforderungen. Andere Authentication Manager-Server erhalten niedrigere Prioritäten und weniger Anforderungen. Diese Anordnung dauert an, bis der Authentifizierungs-Agent eine andere Zeitanforderung oder eine Zeitüberschreitung eintritt.

Um einen dynamischen Lastenausgleich durchzuführen, verbindet sich Authentifizierungs-Agent mit dem Authentication Manager-Server über Firewalls mithilfe alternativer IP-Adressen (Aliase) für die Authentication Manager Server her. Die Authentication Manager-Server stellen dem Authentifizierungs-Agent die Aliase auf Anfrage zur Verfügung. Die Adressen werden in der Konfigurationsdatensatzdatei (**sdconf.rec**) auf dem Authentifizierungs-Agent-Host gespeichert.

Sie legen den dynamischen Lastenausgleich fest, indem Sie die Anweisung **USESERVER** aus der Datei **sdopts.rec** ausschließen. Weitere Informationen finden Sie unter Erstellen einer sdopts.rec-Datei Auf der gegenüberliegenden Seite.

Manueller Lastenausgleich

Mit manuellem Lastenausgleich bestimmen Sie den Authentication Manager-Server, den jeder Authentifizierungs-Agent-Host verwendet. Außerdem weisen Sie jedem Authentication Manager-Server eine Priorität zu, damit der Authentifizierungs-Agent Authentifizierungsanforderungen an einige Authentication Manager-Server häufiger als an andere leiten kann. Sie legen den manuellen Lastenausgleich fest, indem Sie die Anweisung **USESERVER** in die Datei **sdopts.rec** einschließen und Prioritätseinstellungen mit jedem Authentication Manager-Server verknüpfen, den Sie zur Verwendung angeben. Weitere Informationen finden Sie unter Erstellen einer sdopts.rec-Datei Auf der gegenüberliegenden Seite.

Managen der Lastenausgleichs-Konfigurationsdatei (sdopts.rec)

In diesem Abschnitt werden die Komponenten beschrieben, die Sie verwenden können, um eine **sdopts.rec**-

Datei zu erstellen. Es werden auch Beispiele dafür angeführt, wie Sie die Komponenten verwenden können, um den Lastenausgleich einzurichten.

Erstellen einer sdopts.rec-Datei

Sie können eine **sdopts.rec** -Datei mit einem beliebigen Texteditor erstellen und bearbeiten. Nachdem Sie die Datei erstellt haben, speichern Sie sie in dem Verzeichnis, das in der folgenden Registrierungseinstellung angegeben ist: Wert **AuthDataDir** unter dem Schlüssel **HKLM\Software\RSA\RSA Authentication Agent**. Um die Datei vor unbefugten Änderungen zu schützen, ändern Sie die Berechtigungseinstellungen so, dass nur Administratoren die Datei ändern können.

Hinweis: Jedes Mal, wenn Sie die Datei **sdopts.rec** ändern, starten Sie den Authentifizierungs-Agent neu, um die Änderungen zu registrieren.

Die Datei kann Folgendes enthalten:

- Kommentarzeilen, denen jeweils ein Semikolon vorangestellt wird.
- Schlüsselwort-Wert-Paare, die wie folgt aussehen können:
  - **CLIENT_IP=ip_address**. Gibt eine außer Kraft setzende IP-Adresse für den Authentifizierungs-Agent-Host an. Das Schlüsselwort **CLIENT_IP** darf nur einmal in der Datei vorkommen. Weitere Informationen finden Sie unter Angeben einer außer Kraft setzenden IP-Adresse auf Seite 87. Der Authentifizierungs-Agent ignoriert diese Einstellung, wenn die IP-Außerkraftsetzung bereits über die Option **Erweiterte Tools** auf der Seite „SecurID-Optionen managen" festgelegt ist.
  - **USESERVER=ip_address**, **Priorität**. Gibt einen Authentication Manager-Server an, der Authentifizierungsanforderungen vom Authentifizierungs-Agent-Host gemäß einem angegebenen Prioritätswert empfängt. Verwenden Sie eine Einstellung für jeden Authentication Manager-Server, den der Authentifizierungs-Agent-Host verwendet. Die kombinierte maximale Anzahl von Authentication Manager-Servern, die Sie in den Dateien **sdopts.rec** und **sdconf.rec** angeben können, ist 11. Sie müssen jedem Authentication Manager-Server, den Sie der Datei **sdopts rec** hinzufügen, eine Priorität zuweisen. Andernfalls ist der Eintrag ungültig.

    Hinweis: Wenn dieser Wert in der Datei **sdopts.rec** eingeschlossen ist, wird der manuelle Lastenausgleich aktiviert.

    Jeder **USESERVER**-Schlüsselwortwert muss aus der tatsächlichen Authentication Manager-IP-Adresse bestehen, getrennt durch ein Komma von der zugewiesenen Priorität. Die Priorität gibt an, ob oder wie oft ein Authentication Manager-Server Authentifizierungsanforderungen empfängt. In der folgenden Tabelle werden die Prioritätswerte aufgelistet, die Sie festlegen können.

Priorität	Bedeutung
2–10	Senden Sie Authentifizierungsanforderungen an diesen Authentication Manager-Server mithilfe einer randomisierten Auswahl, basierend auf der zugewiesenen Priorität des Authentication Manager-Servers. Sie kann zwischen 2 und 10 liegen. Je höher der Wert ist, desto mehr Anforderungen empfängt der Authentication Manager-Server. Ein Authentication Manager-Server mit der Priorität 10 empfängt etwa 24-mal so viele Anforderungen wie ein Authentication Manager-Server mit der Priorität 2.
1	Verwenden Sie diesen Authentication Manager-Server nur, wenn keine Authentication Manager-Server mit höherer Priorität verfügbar sind.

Priorität	Bedeutung
0	Ignorieren Sie diesen Authentication Manager-Server. Verwenden Sie nur unter diesen Umständen Priorität 0: • Der Server muss einer der vier Authentication Manager-Server sein, die in der Datei **sdconf.rec** aufgeführt sind. • Der Server wird nur für die erstmalige Authentifizierung von Authentifizierungs-Agent verwendet, es sei denn, alle Authentication Manager-Server mit den Prioritäten 1 bis 10 in der Datei **sdopts.rec** sind als unbrauchbar für Authentifizierungs-Agent bekannt. • Im Allgemeinen erlaubt Ihnen die Priorität 0, einen Eintrag in die Datei für einen Authentication Manager-Server vorzunehmen, ohne ihn zu verwenden. Sie können den Prioritätswert ändern, wenn Sie sich entscheiden, den Authentication Manager-Server zu verwenden. **Hinweis:** Sie müssen Schlüsselwörter in Großbuchstaben eingeben. • Wenn keiner der Server mit **USESERVER**-Anweisungen antwortet, ist der Standardserver entweder der Master (falls vorhanden) oder der Authentication Manager-Server, mit dem die **sdconf.rec**-Datei erstellt wird.

Die IP-Adressen in der Datei werden anhand der Liste der gültigen Authentication Manager-Server überprüft, die Authentifizierungs-Agent im Rahmen der erstmaligen Authentifizierung empfängt.

- **ALIAS=ip_address, alias_ip_address_1, alias_ip_address_2, alias_ip_address_3**. Gibt eine oder mehrere alternative IP-Adressen (Aliase) für einen Authentication Manager-Server an, zusätzlich zu den Aliasen, die für den Authentication Manager-Server in der Datei **sdconf.rec** aufgeführt sind. Sie können in der Datei **sdopts.rec** bis zu drei Aliase angeben.

  Der Schlüsselwortwert **ALIAS** enthält die tatsächliche IP-Adresse für den Authentication Manager-Server, gefolgt von bis zu drei Aliasen für diesen Authentication Manager-Server. Der Authentifizierungs-Agent sendet Zeitanforderungen an die tatsächliche sowie an die Alias-Adressen.

  Nur die tatsächliche IP-Adresse, die durch das **ALIAS**-Schlüsselwort angegeben wird, muss dem angegebenen Authentication Manager-Server bekannt sein. Darüber hinaus muss die tatsächliche IP-Adresse auf jeder Authentication Manager-Serverliste enthalten sein, die vom Authentifizierungs-Agent empfangen wird. Die Authentication Manager-Serverliste enthält die tatsächlichen und Alias-IP-Adressen für alle bekannten Authentication Manager-Server im Bereich. Der Authentifizierungs-Agent empfängt die Liste vom Authentication Manager-Server, nachdem Authentication Manager eine Authentifizierungsanforderung validiert hat.

- **ALIASES_ONLY=ip_address**. Wenn Sie eine tatsächliche IP-Adresse eines Authentication Manager-Servers als Wert angeben, weist dieses Schlüsselwort den Authentifizierungs-Agent an, nur die Alias-IP-Adressen zu verwenden, um Authentication Manager zu kontaktieren.

  Wenn Sie keinen Wert angeben, weist dieses Schlüsselwort den Authentifizierungs-Agent an,

Anforderungen nur an die Authentication Manager-Server zu senden, denen Alias-IP-Adressen zugewiesen sind. Sie können Ausnahmen erstellen, indem Sie nicht mehr als 10 **IGNORE_ ALIASES**-Schlüsselwörter in die Datei **sdopts.rec** aufnehmen, um anzugeben, welche Authentication Manager-Server über Ihre tatsächlichen IP-Adressen kontaktiert werden müssen. Ein Beispiel für diese Ausnahmen finden Sie unter Angeben von Alias-IP-Adressen für die Verwendung oder den Ausschluss Auf der nächsten Seite. (Wenn Sie dieses Schlüsselwort verwenden, stellen Sie sicher, dass für mindestens einen Authentication Manager-Server eine Alias-IP-Adresse in der Datei **sdconf.rec** oder in der Datei **sdopts.rec** angegeben ist.)

- **IGNORE_ALIASES=ip_address**. Wenn Sie keinen Wert angeben, gibt dieses Schlüsselwort an, dass alle Alias-IP-Adressen in den Dateien **sdopts.rec** und **sdconf.rec** oder in der Authentication Manager-Serverliste ignoriert werden. Sie können Ausnahmen erstellen, indem Sie nicht mehr als 10 **ALIASES_ONLY**-Schlüsselwörter in die Datei **sdopts.rec** aufnehmen, um anzugeben, welche Authentication Manager-Server über Ihre tatsächlichen IP-Adressen kontaktiert werden müssen. Ein Beispiel für diese Ausnahmen finden Sie unter Angeben von Alias-IP-Adressen für die Verwendung oder den Ausschluss Auf der nächsten Seite.

  Geben Sie eine tatsächliche IP-Adresse als Wert an, um den Authentifizierungs-Agent anzuweisen, nur die tatsächliche IP-Adresse zu verwenden, um Authentication Manager zu kontaktieren.

- **AVOID=ip_address**. Geben Sie eine tatsächliche IP-Adresse eines Authentication Manager-Servers an, um den Authentifizierungs-Agent anzuweisen, diesen Authentication Manager-Server während des dynamischen Lastenausgleichs von der Verwendung auszuschließen.

  Hinweis: Verwenden Sie das Schlüsselwort **AVOID** nur für den dynamischen Lastenausgleich. Verwenden Sie es nicht mit dem Schlüsselwort **USESERVER** für den manuellen Lastenausgleich.

Ausschließen eines Authentication Manager-Servers während des dynamischen Lastenausgleichs

Beim dynamischen Lastenausgleich können Sie das Schlüsselwort **AVOID** in der Datei **sdopts.rec** mit einer tatsächlichen IP-Adresse eines Authentication Manager-Servers als Wert verwenden, um den Authentifizierungs-Agent anzuweisen, diesen Authentication Manager-Server während des dynamischen Lastenausgleichs von der Verwendung auszuschließen.

Hinweis: Verwenden Sie das Schlüsselwort **AVOID** nur für den dynamischen Lastenausgleich. Verwenden Sie es nicht mit dem Schlüsselwort **USESERVER** für den manuellen Lastenausgleich. Wenn das Schlüsselwort **AVOID** in einer **sdopts.rec**-Datei enthalten ist, die eine **USESERVER**-Anweisung enthält, wird die Anweisung **AVOID** als Fehler betrachtet.

Wenn Sie die Anweisung **AVOID** mit der IP-Adresse des Authentication Manager-Standardservers verwenden, wird die Anweisung ignoriert, es sei denn, ein anderer Authentication Manager-Server ist verfügbar. Der Authentication Manager-Standardserver ist der Speicherort, an dem die Datei **sdconf.rec** erstellt wurde. Wenn aber ein Authentication Manager-Server als Master bestimmt wurde, wird der Master zum Authentication Manager-Standardserver, unabhängig davon, wo die Datei **sdconf.rec** erstellt wurde.

Das folgende Beispiel zeigt, wie Sie die **AVOID**-Schlüsselwörter in der Datei **sdopts.rec** verwenden:

```
AVOID=192.100.123.5
```

In diesem Beispiel wird der Authentication Manager-Server mit der IP-Adresse 192.100.123.5 nicht für die Authentifizierung verwendet.

Konfigurieren des manuellen Lastenausgleichs

Sie konfigurieren manuellen Lastenausgleich, indem Sie das Schlüsselwort **USESERVER** in die Datei **sdopts.rec** aufnehmen, um die IP-Adressen der Authentication Manager-Server anzugeben, die für jeden Agent-Host verwendet werden sollen.

Sie können die IP-Adressen in der Datei **sdopts.rec** in beliebiger Reihenfolge auflisten, aber Sie müssen jede jeweils einzeln auflisten, jeweils eine pro Zeile.

Das folgende Beispiel zeigt, wie Sie die **USESERVER**-Schlüsselwörter verwenden, um die IP-Adressen anzugeben.

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).

;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.

USESERVER=192.168.10.23, 10

USESERVER=192.168.10.22, 2

USESERVER=192.168.10.20, 1

USESERVER=192.168.10.21, 0
```

In diesem Beispiel empfängt der Authentication Manager-Server, der durch die IP-Adresse 192.168.10.23 identifiziert wird, mehr Authentifizierungsanforderungen als Authentication Manager-Server 192.168.10.22. Authentication Manager-Server 192.168.10.20 wird nur verwendet, wenn die Authentication Manager-Server mit höherer Priorität nicht verfügbar sind. Authentication Manager-Server 192.168.10.21 wird ignoriert, außer in seltenen Fällen, wie unter Erstellen einer sdopts.rec-Datei auf Seite 82 beschrieben.

Hinweis: Sie können die Schlüsselwörter **USESERVER** und **ALIAS** in der Datei **sdopts.rec** zusammen verwenden. **USESERVER**-Schlüsselwörter wirken sich jedoch nicht auf die Alias-Adressen aus, die für die Verbindung mit den Authentication Manager-Servern verwendet werden, und **ALIAS**-Schlüsselwörter wirken sich nicht darauf aus, welche Authentication Manager-Server für die Verwendung angegeben sind.

Angeben von Alias-IP-Adressen für die Verwendung oder den Ausschluss

Sie können die Datei **sdopts.rec** verwenden, um Alias-IP-Adressen zur Verwendung oder zum Ausschluss anzugeben.

Hinweis: Der Authentifizierungs-Agent ignoriert diese Einstellung, wenn die IP-Außerkraftsetzung bereits über die Option **Erweiterte Einstellungen** auf der Seite „SecurID-Optionen managen" festgelegt ist. Weitere Informationen finden Sie unter Managen von Agent-Einstellungen auf Seite 47.

Sie können die Einstellungen in der Datei **sdopts.rec** in beliebiger Reihenfolge auflisten, aber Sie müssen jede Einstellung jeweils einzeln auflisten, jeweils eine Einstellung pro Zeile.

Das folgende Beispiel zeigt, wie Sie die **ALIAS**-Schlüsselwörter in der Datei **sdopts.rec** verwenden.

Standardmäßig werden Alias- oder tatsächliche IP-Adressen verwendet, mit einigen Ausnahmen. Für den Authentication Manager-Server mit der tatsächlichen IP-Adresse 192.168.10.23 sind drei Alias-Adressen angegeben, während Authentication Manager-Server 192.168.10.20 und 192.168.10.21 jeweils nur einen Alias haben. Authentication Manager-Server 192.168.10.22 hat zwei Alias-Adressen. Die durch die **ALIAS**-Schlüsselwörter angegebenen Aliase sind Ergänzungen zu allen Aliasnamen, die in der Datei **sdconf.rec** und im Authentication Manager-Server angegeben sind.

In diesem Beispiel wird außerdem gezeigt, wie Sie die Schlüsselwörter **USESERVER** und **ALIAS** in der Datei **sdopts.rec** zusammen verwenden. **USESERVER**-Schlüsselwörter wirken sich jedoch nicht auf die Alias-Adressen aus, die für die Verbindung mit den Authentication Manager-Servern verwendet werden, und **ALIAS**-Schlüsselwörter haben keine Auswirkung darauf, welche Authentication Manager-Server für die Verwendung angegeben sind. Die Standardeinstellung ist die Verwendung von Aliasnamen, mit zwei Ausnahmen. Authentication Manager-Server 192.168.10.23, wie durch das **ALIASES_ONLY**-Schlüsselwort angegeben, wird nur über die Alias-IP-Adressen kontaktiert. Authentication Manager-Server 192.168.10.22, angegeben durch das **IGNORE_ALIASES**-Schlüsselwort, wird nur über die tatsächliche IP-Adresse kontaktiert.

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).

;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.

USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0

ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.1
ALIAS=192.168.10.21, 0, 192.168.1.1

ALIAS_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

Im folgenden Beispiel werden standardmäßig Aliasnamen ignoriert, mit zwei Ausnahmen:

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

Die **ALIASES_ONLY**-Ausnahmen weisen den Authentifizierungs-Agent an, Anforderungen an die Authentication Manager-Server 192.168.10.23 und 192.168.10.22 nur über Alias-IP-Adressen zu senden.

Im folgenden Beispiel werden standardmäßig Aliasnamen verwendet, mit zwei Ausnahmen:

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

Die **IGNORE_ALIASES**-Ausnahmen weisen den Authentifizierungs-Agent an, Anforderungen an die Authentication Manager-Server 192.168.10.23 und 192.168.10.22 nur über tatsächliche IP-Adressen zu senden.

Angeben einer außer Kraft setzenden IP-Adresse

Wenn Authentifizierungs-Agent auf einem Host ausgeführt wird, der über mehrere Netzwerkschnittstellenkarten und daher über mehrere IP-Adressen verfügt, müssen Sie eine primäre Agent-Host-IP-Adresse angeben, die für die verschlüsselte Kommunikation zwischen Authentifizierungs-Agent und Authentication Manager verwendet werden soll. Agent-Hosts versuchen in der Regel, ihre eigenen IP-Adressen zu erkennen. Ein Agent-Host mit mehreren Adressen wählt möglicherweise eine aus, die für Authentication Manager unbekannt ist, wodurch die Kommunikation zwischen Authentifizierungs-Agent und Authentication Manager unmöglich gemacht wird. Sie können eine außer Kraft setzende primäre IP-Adresse angeben, indem Sie das Schlüsselwort **CLIENT_IP** in eine **sdopts.rec**-Datei auf dem Authentifizierungs-Agent-Host aufnehmen.

Hinweis: Das DHCP (Dynamic Host Configuration Protocol) weist den Agent-Hosts dynamisch IP-Adressen zu. Um Adresskonflikte zu vermeiden, installieren Sie das Dienstprogramm zur automatischen Registrierung, wenn Sie Authentifizierungs-Agent installieren. Weitere Informationen erhalten Sie unter Installieren des Agent auf Seite 27.

Gehen Sie folgendermaßen vor, um eine IP-Adresse in der Datei **sdopts.rec** außer Kraft zu setzen:

```
CLIENT_IP=192.168.10.19
```

Mit dieser Anweisung wird sichergestellt, dass der Authentifizierungs-Agent-Host immer die angegebene IP-Adresse für die Kommunikation mit Authentication Manager verwendet.

Hinweis: Der Authentifizierungs-Agent ignoriert diese Einstellung, wenn die Option zur Außerkraftsetzung der IP-Adresse auf der Seite „SecurID-Optionen managen" festgelegt ist. Wenn Sie jedoch das Dienstprogramm zur automatischen Registrierung installiert haben, überschreibt die Adresse, die das Dienstprogramm registriert, die IP-Einstellung auf der Seite „SecurID-Optionen managen". (Das Feld **Einstellung zur Außerkraftsetzung der IP-Adresse** wird nach der Installation des Dienstprogramms für die automatische Registrierung auch inaktiv angezeigt.) Weitere Informationen finden Sie unter Managen von Agent-Einstellungen auf Seite 47.
