Single Sign-On 5.0

Dec 11, 2015

Überblick

Oct 05, 2015

Neue Funktionen

Single Sign-On 5.0 integriert das Single Sign-On Plug-in in Citrix Receiver, vereinfacht die Benutzererfahrung, ermöglicht die Bereitstellung des Single Sign-On Plug-ins mit Merchandising Server und enthält vereinfachtes Chinesisch als unterstützte Single Sign-On Plug-in-Sprache.

- **Benutzer greifen auf das Single Sign-On Plug-in über das Symbol von Citrix Receiver zu.** Benutzern wird statt mehreren Single Sign-On Plug-in-Symbolen nur das Citrix Receiver-Symbol im Windows-Infobereich angezeigt. Das Citrix Receiver-Symbol wird nur einmal im Windows-Infobereich angezeigt, unabhängig von der Zahl der aktiven Single Sign-On-Sitzungen des Benutzers. Benutzer verwalten Anmeldeinformationen, halten das Single Sign-On an und setzen es fort, stellen fest, ob Single Sign-On angehalten wurde und senden Kennwörter manuell über Menüoptionen, auf die sie über das Citrix Receiver-Symbol zugreifen.
  Hinweis: Wenn ältere Versionen des Plug-ins installiert sind, können weitere Symbole im Windows-Infobereich angezeigt werden. Weitere Informationen finden Sie unter Installieren des Single Sign-On Plug-ins.
- **Das Single Sign-On Plug-in muss auf den Benutzergeräten installiert sein, damit alle Funktionen zur Verfügung stehen.** Das Single Sign-On Plug-in muss auf dem Benutzergerät installiert sein, sonst können Benutzer Anmeldeinformationen nicht verwalten, Single Sign-On nicht anhalten und fortsetzen, nicht feststellen, ob Single Sign-On angehalten wurde oder Kennwörter manuell senden. Weitere Informationen finden Sie unter Bereitstellungsszenarios für die Single Sign-On Plug-in-Software.
- **Benutzer beenden das Single Sign-On Plug-in, wenn sie Citrix Receiver beenden**. Benutzer beenden Single Sign-On mit der Option "Beenden" im Menü des Citrix Receiver-Symbols. Die Benutzeroberfläche von Citrix Receiver und alle Plug-ins, auf die über die Benutzeroberfläche zugegriffen werden, werden geschlossen.
- **Benutzer verwalten Anmeldeinformationen mit dem Dialogfeld "Kennwörter verwalten".** Der Anmeldungsmanagers wurde in das Dialogfeld "Kennwörter verwalten" umbenannt und neu gestaltet, um die Benutzererfahrung zu vereinfachen:
  - Benutzer greifen auf das Dialogfeld "Kennwörter verwalten" über eine Menüoption im Citrix Receiver-Symbol zu. Ein Dialogfeld "Kennwörter verwalten" wird angezeigt und enthält Anmeldeinformationen für die Anwendungen aller Sitzungen des Benutzers.
  - Sie konfigurieren im Dialogfeld "Kennwörter verwalten" die angezeigten Spalten für diese Attribute der gespeicherten Anmeldeinformationen: Name, Beschreibung, Gruppe, Uhrzeit und Datum der letzten Verwendung und Uhrzeit und Datum der letzten Änderung. Benutzer können nach jedem dieser Attribute sortieren.
  - Das Dialogfeld "Kennwörter verwalten" hat keine Dropdownmenüs. Der Zugriff auf die Funktionalität, auf die früher mit den Optionen in diesen Menüs im Anmeldungsmanager zugegriffen wurde, hat sich geändert oder ist nicht mehr möglich:

Menü	Option	Was ist mit dieser Funktionalität in Single Sign-On 5.0 passiert?
Datei	Neue Anmeldung oder Neue Anmeldung > Eine Anmeldung hinzufügen	Benutzer speichern Authentifizierungsinformationen manuell mit der Option "Kennwort senden" im Menü des Citrix Receiver-Symbols.

Menü	Option	Was ist mit dieser Funktionalität in Single Sign-On 5.0 passiert?
	Neue Anmeldung > Mehrere Anmeldungen hinzufügen	Benutzer erstellen mehrere Gruppen der Anmeldeinformationen für dieselbe Anwendung, indem sie die erste Gruppe erstellen, sie kopieren und die Kopie bearbeiten.
	Kopieren	Ersetzt durch die Schaltfläche "Kopieren" im Dialogfeld "Kennwörter verwalten".
	Löschen	Ersetzt durch die Schaltfläche "Entfernen" im Dialogfeld "Kennwörter verwalten".
	Properties	Ersetzt durch die Schaltfläche "Bearbeiten" im Dialogfeld "Kennwörter verwalten".
	Beenden	Benutzer schließen das Dialogfeld "Kennwörter verwalten" mit der Windows-Schaltfläche "Schließen".
View	Symbol, Liste und Detail	Diese Funktionalität wurde entfernt, um die Benutzererfahrung zu vereinfachen.
	Symbole sortieren	Diese Funktionalität steht nicht zur Verfügung; Benutzer können jedoch auf die Spaltenüberschrift im Dialogfeld "Kennwörter verwalten" klicken, um die Spalten zu sortieren.
	Refresh	Ersetzt durch den Link "Aktualisieren" im Dialogfeld "Kennwörter verwalten".
	Kennwörter anzeigen	Benutzer können jeweils ein Kennwort mit der Schaltfläche "Anzeigen" im Dialogfeld "Kennwörter verwalten" anzeigen. Benutzer können nur jeweils ein Kennwort anzeigen.
Tools	Kontozuordnung	Benutzer können die Kontozuordnung nicht mit dem Single Sign-On Plug-in aktivieren. Damit Benutzer die Kontozuordnung aktivieren können, geben Sie ihnen Zugriff auf das Dienstprogramm AccAssoc.exe als veröffentlichte Anwendung.
	Registrierung der Sicherheitsfragen	Benutzer können die Antworten auf die Sicherheitsfragen nur mit dem Single Sign-On Plug-in neu registrieren, wenn Sie sie zur Neuregistrierung auffordern. Damit Benutzer die Antworten auf die Sicherheitsfragen neu registrieren können, geben Sie ihnen Zugriff auf das Dienstprogramm QBAEnroll.exe als veröffentlichte Anwendung.
	Optionen > Beenden	Die Bestätigung beim Beenden wird über Citrix Receiver gesteuert. Das Single

Menü	Option	Was ist mit dieser Funktionalität in Single Sign-On 5.0 passiert?
	bestätigen	Sign-On Plug-in fordert nicht zu einer Bestätigung beim Beenden auf.
Help	Anmeldungsmanager-Hilfe	Ersetzt durch den Link "Hilfe" im Dialogfeld "Kennwörter verwalten".
	Überblick	Ersetzt durch den Link "Info" im Dialogfeld "Kennwörter verwalten".

- Das Dialogfeld "Kennwörter verwalten" hat kein Kontextmenü. Der Zugriff auf die Funktionalität, auf die früher mit diesem Menü im Anmeldungsmanager zugegriffen wurde, hat sich geändert:

Option	Was ist mit dieser Funktionalität in Single Sign-On 5.0 passiert?
Kopieren	Ersetzt durch die Schaltfläche "Kopieren" im Dialogfeld "Kennwörter verwalten".
Löschen	Ersetzt durch die Schaltfläche "Entfernen" im Dialogfeld "Kennwörter verwalten".
Properties	Ersetzt durch die Schaltfläche "Bearbeiten" im Dialogfeld "Kennwörter verwalten".

- **Benutzer können nicht bei der Erstverwendung von Single Sign-On zum Speichern der Anmeldeinformationen aufgefordert werden.** Die Option für die Ersteinrichtung der Anmeldeinformationen wurde entfernt.
- **Das Single Sign-On Plug-in kann mit Merchandising Server bereitgestellt und verwaltet werden.** Wenn Citrix Receiver Updater auf den Benutzergeräten installiert ist, können Sie das Single-Sign-On Plug-in mit Merchandising Server bereitstellen und verwalten.
- **Das Single Sign-On Plug-in kann vereinfachtem Chinesisch bereitgestellt werden.**

Bekannte Probleme

Weitere Informationen zu bekannten Problemen in Single Sign-On 5.0 finden Sie unter Bekannte Probleme in XenApp 6.5 für Windows Server 2008 R2.

Erste Schritte

Oct 05, 2015

Single Sign-On hat folgende Hauptkomponenten:

- Zentraler Speicher
- Single Sign-On-Komponente von Citrix AppCenter
- Single Sign-On Plug-in
- Single Sign-On-Dienst (optional)

Zentraler Speicher

Der zentrale Speicher ist ein zentrales Repository, das von Single Sign-On zum Speichern und Verwalten von Benutzerdaten und administrativen Daten verwendet wird. Benutzerdaten sind zum Beispiel die Anmeldeinformationen der Benutzer, Antworten auf Sicherheitsfragen und andere auf Benutzer bezogene Daten. Administrative Daten sind zum Beispiel Kennwortrichtlinien, Anwendungsdefinitionen, Sicherheitsfragen und andere allgemeine Daten. Wenn sich ein Benutzer anmeldet, vergleicht Single Sign-On die Anmeldeinformationen des Benutzers mit den Daten im zentralen Speicher. Wenn der Benutzer kennwortgeschützte Anwendungen oder Webseiten öffnet, werden die entsprechenden Anmeldeinformationen aus dem zentralen Speicher abgerufen.

Single Sign-On-Komponente von Citrix AppCenter

Die Single Sign-On-Komponente von Citrix AppCenter ist das Befehlszentrum von Single Sign-On. Hier konfigurieren Sie neben weiteren wichtigen kennwortbezogenen Einstellungen wie Single Sign-On funktioniert, welche Features bereitgestellt werden und welche Sicherheitsmaßnahmen verwendet werden.

Die Komponente enthält im linken Bereich vier Elemente oder Knoten. Durch Auswählen eines Knotens werden die Aufgaben für diesen Knoten angezeigt. Es gibt die folgenden Knoten:

- Mit Benutzerkonfigurationen können Sie bestimmte Einstellungen für Benutzer anpassen, die auf den geografischen Standorten oder den Unternehmensrollen der Benutzer basieren.
- Mit Anwendungsdefinitionen stellen Sie die Informationen bereit, damit das Single Sign-On Plug-In die Anmeldeinformationen der Benutzer an die Anwendungen senden und auftretende Fehlerzustände erkennen kann. Verwenden Sie die Anwendungsdefinitionsvorlagen, die mit Single Sign-On ausgeliefert werden, um Zeit zu sparen, oder erstellen Sie benutzerdefinierte Definitionen für Anwendungen, die diese Vorlagen nicht verwenden können.
- Kennwortrichtlinien steuern die Kennwortlänge, den Typ und die Zeichenvielfalt, die in benutzerdefinierten und automatisch generierten Kennwörtern verwendet werden. In Kennwortrichtlinien legen Sie auch fest, welche Zeichen nicht in Kennwörtern verwendet werden dürfen, und ob alte Kennwörter wieder verwendet werden dürfen. Durch das Erstellen von Kennwortrichtlinien gemäß der Sicherheitsrichtlinien Ihres Unternehmens stellen Sie sicher, dass die Kennwortsicherheit von Single Sign-On richtig verwaltet wird.
- Mit der Identitätsprüfung erstellen Sie Sicherheitsfragen, die dem Sign-On Plug-In eine weitere Sicherheitsebene bieten. Sicherheitsfragen schützen vor Identitätswechsel des Benutzers, vor nicht autorisierten Kennwortänderungen und dem nicht autorisierten Sperren des Kontos. Benutzer, die sich registrieren und die Sicherheitsfragen beantworten, können die Identität bestätigen, indem sie dieselben Antworten eingeben. Nach der Prüfung können Benutzer die Self-Service-Aufgaben für ihr Konto durchführen, z. B. Zurücksetzen des primären Kennworts oder Entsperren des Kontos. Sicherheitsfragen werden auch für die Schlüsselwiederherstellung verwendet.

Single Sign-On Plug-in

Das Single Sign-On Plug-in sendet die relevanten Anmeldeinformationen an die Anwendungen, die auf dem Clientgerät des

Benutzers ausgeführt werden, erzwingt die Kennwortrichtlinien, stellt die Self-Service-Funktionalität bereit und ermöglicht das benutzerseitige Verwalten der Anmeldeinformationen mit dem Dialogfeld "Kennwörter verwalten" (früher Anmeldungsmanager). Außerdem stellt das Plug-in den Benutzern zahlreiche Features bereit, abhängig von den administrativen Einstellungen, die Sie in den Benutzerkonfigurationen vornehmen.

Single Sign-On-Dienst

Der Single Sign-On-Dienst wird auf einem Webserver ausgeführt, der das Fundament für optionale Features bereitstellt, die in diesem Release enthalten sind. Installieren Sie den Single Sign-On-Dienst, wenn Sie mindestens eines der folgenden Module implementieren möchten:

- Konto-Self-Service: Ermöglicht das benutzerseitige Zurücksetzen der Windows-Kennwörter und das Aufheben der Sperrung der eigenen Windows-Konten.
- Datenintegrität: Schützt die Daten bei der Übertragung vom zentralen Speicher zum Single Sign-On Plug-in vor Manipulation.
- Schlüsselverwaltung: Benutzer können bei einer Änderung des primären Kennworts die sekundären Anmeldeinformationen wiederherstellen, entweder mit der automatischen Schlüsselwiederherstellung oder durch das Beantworten von Sicherheitsfragen mit der fragenbasierten Authentifizierung.
- Provisioning: Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Single Sign-On-Benutzerdaten und -Anmeldeinformationen mit der Single Sign-On-Komponente von Citrix AppCenter.
- Synchronisierung der Anmeldeinformationen: Synchronisiert die Anmeldeinformationen der Benutzer über einen Webdienst.

Wenn Sie die oben angeführten Module nicht implementieren, sollten Sie den Single Sign-On-Dienst nicht installieren.

Evaluierung

Oct 05, 2015

Wenn Sie XenApp 6.5 für Windows Server 2008 R2 verwenden, um Anwendungen zu veröffentlichen, und Single Sign-On 5.0 zur Kennwortsicherung und zur Bereitstellung von Single Sign-On-Zugriff auf die Anwendungen einsetzen möchten, erhalten Sie in diesem Abschnitt eine Anleitung zur schnellen Bereitstellung von Single Sign-On. Die hier beschriebene Single Sign-On-Bereitstellung kann zur Evaluierung von Single Sign-On oder als Pilotversuch verwendet werden, der später um weitere Benutzer und Anwendungen erweitert wird.

Hinweis: Der hier dargestellte Bereitstellungsvorgang ist vereinfacht und enthält deshalb einige Komponenten, Features und Optionen nicht, die bei der Verwendung von Single Sign-On 5.0 mit XenApp 6.5 verfügbar sind.
Die hier beschriebene Bereitstellung enthält die folgenden Komponenten von Single Sign-On:

- **Zentraler Speicher** Der zentrale Speicher ist ein zentrales Repository, das von Single Sign-On zum Speichern und Verwalten von Benutzerdaten und administrativen Daten verwendet wird. Benutzerdaten sind zum Beispiel die Anmeldeinformationen der Benutzer, Antworten auf Sicherheitsfragen und andere auf Benutzer bezogene Daten. Administrative Daten sind zum Beispiel Kennwortrichtlinien, Anwendungsdefinitionen, Sicherheitsfragen und andere allgemeine Daten. Wenn sich ein Benutzer anmeldet, vergleicht Single Sign-On die Anmeldeinformationen des Benutzers mit den Daten im zentralen Speicher. Wenn der Benutzer kennwortgeschützte Anwendungen oder Webseiten öffnet, werden die entsprechenden Anmeldeinformationen aus dem zentralen Speicher abgerufen.
- **Single Sign-On-Komponente von Citrix AppCenter** In dieser Bereitstellung können Sie die Single Sign-On-Komponente von Citrix AppCenter zum Definieren von Kennwortrichtlinien und Erstellen von Benutzerkonfigurationen einsetzen sowie Single Sign-On zur Erkennung von Anwendungen konfigurieren.
- **Anwendungsdefinitionstool** Das Anwendungsdefinitionstool bietet die selben Features wie das Modul der Single Sign-On-Komponente von Citrix AppCenter, der zum Konfigurieren von Single Sign-On zur Erkennung von Anwendungen verwendet wird.
- **Single Sign-On Plug-In** Bei dem Single Sign-On Plug-In handelt es sich um die Komponente von Single Sign-On, mit der Benutzer interagieren. Das Plug-In sendet die relevanten Anmeldeinformationen an die Anwendungen, die auf dem Clientgerät des Benutzers ausgeführt werden, erzwingt die Einhaltung von Kennwortrichtlinien und ermöglicht das benutzerseitige Verwalten der Anmeldeinformationen im Fenster zum Verwalten von Kennwörtern. In dieser Bereitstellung wird es auf jedem Benutzergerät installiert.

Die Bereitstellung enthält jedoch nicht den Single Sign-On-Dienst oder die von ihm unterstützten optionalen Features:
- Konto-Self-Service: Ermöglicht das benutzerseitige Zurücksetzen der Windows-Kennwörter und das Entsperren der eigenen Windows-Konten.
- Datenintegrität: Schützt die Daten bei der Übertragung vom zentralen Speicher zum Single Sign-On Plug-In vor Manipulation.
- Schlüsselverwaltung: Benutzer können bei einer Änderung des primären Kennworts die sekundären Anmeldeinformationen wiederherstellen, entweder mit der automatischen Schlüsselwiederherstellung oder durch das Beantworten von Sicherheitsfragen mit der fragenbasierten Authentifizierung.
- Provisioning: Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Single Sign-On-Benutzerdaten und -Anmeldeinformationen mit der Single Sign-On-Komponente von Citrix AppCenter.
- Synchronisierung der Anmeldeinformationen: Synchronisiert die Anmeldeinformationen der Benutzer über einen Webdienst.

Führen Sie die Aufgaben in diesem Abschnitt in der Reihenfolge aus, in der sie hier aufgeführt sind.

Planen der Bereitstellung

- Prüfen Sie die Systemanforderungen für den zentralen Speicher, die Single Sign-On-Komponente von AppCenter, das Anwendungsdefinitionstool und das Plug-In: Systemanforderungen.
- Prüfen Sie die Lizenzierungsanforderungen für Single Sign-On und installieren bzw. aktualisieren Sie die Lizenzen, falls erforderlich: Systemanforderungen.
- Wählen Sie die Anwendungen aus, die Sie einschließen möchten. Wählen Sie für diese Bereitstellung nur mit XenApp veröffentlichte Windows- und Webanwendungen aus:
  - Windows-Anwendungen: 32-Bit-Windows-Anwendungen (einschließlich Java-Anwendungen), z. B. Microsoft Outlook, Lotus Notes, SAP oder jede andere kennwortaktivierte Windows-Anwendung. In Single Sign-On ist jede Anwendung, die von einer Datei mit einer EXE-Erweiterung gestartet wird, als Windows-Anwendung klassifiziert.
  - Webanwendungen: Webanwendungen (einschließlich Java-Applets und SAP), auf die über Microsoft Internet Explorer zugegriffen wird. Im Allgemeinen wird jede Anwendung, die in einem Webbrowser ausgeführt wird, in Single Sign-On als Webanwendung angesehen. Single Sign-On unterstützt Webanwendungen, die mit Internet Explorer-Versionen 6.0, 7.0. 8.0 und 9.0 ausgeführt werden.
- Wählen Sie die Benutzer aus, die Sie einschließen möchten. Vergewissern Sie sich, dass die Benutzergeräte dieser Benutzer das Single Sign-On Plug-In unterstützen.
- Legen Sie den Installationsort für den zentralen Speicher fest. Der zentrale Speicher ist in dieser Bereitstellung eine NTFS-Netzwerkfreigabe.
- Legen Sie den Installationsort für die Single Sign-On-Komponente von Citrix AppCenter fest. Sie können ein bereits installiertes AppCenter verwenden oder ein neues AppCenter installieren.
- Legen Sie fest, ob das Anwendungsdefinitionstool installiert werden soll, und falls ja, wo. Ist Citrix AppCenter nicht installiert auf einem Computer, auf dem eine Anwendung ausgeführt wird, die Sie in die Bereitstellung einschließen möchten, müssen Sie das Anwendungsdefinitionstool auf diesem Computer installieren. Beim Konfigurieren von Single Sign-On für die Erkennung von Anwendungen starten Sie die Anwendungen und lassen die Assistenten im Tool Informationen über sie sammeln.
- Planen Sie die Kennwortrichtlinien. Bei Kennwortrichtlinien handelt es sich um Regeln, die das Erstellen, Übermitteln und Verwalten von Kennwörtern steuern. Kennwortrichtlinien werden auf alle Benutzer oder spezifische Anwendungsgruppen angewendet. Single Sign-On enthält zwei Standard-Kennwortrichtlinien: die Standardrichtlinie und die Domänenrichtlinie. Wenn die in diesen Standardrichtlinien festgelegten Standardwerte Ihren Zwecken in dieser Bereitstellung entsprechen, können Sie sie ohne Änderungen verwenden. Sonst können Sie auf ihnen basierende neue Richtlinien erstellen und Änderungen an den Werten vornehmen.
  - Einen Überblick über Kennwortrichtlinien finden Sie unter Kennwortrichtlinien.
  - Hinweise für das Erstellen von sicheren und benutzerfreundlichen Kennwortrichtlinien finden Sie unter Kennwortrichtlinien.
  - Weitere Informationen dazu, wie Single Sign-On Kennwortrichtlinien erzwingt, finden Sie unter Erzwingen von Kennwortrichtlinien.
  - Sie können überprüfen, ob die Standardwerte der Kennwortrichtlinien für Ihre Anwendungen und Benutzer angemessen sind, indem Sie die Standardwerte für jede Einstellung im Referenzabschnitt Kennwortrichtlinien (und den Unterabschnitten) einsehen. Beide Standard-Kennwortrichtlinien (Standard- und Domänenrichtlinie) enthalten diese Standardwerte.
- Planen der Benutzerkonfigurationen Eine Benutzerkonfiguration ist eine eindeutige Zusammenstellung von Einstellungen, Kennwortrichtlinien und Anwendungen, die Sie auf Benutzer anwenden, die Active Directory-Hierarchien (Organisationseinheiten oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind. Mit Benutzerkonfigurationen können Sie das Verhalten und die Darstellung der Plug-In-Software für Benutzer steuern.
  - Einen Überblick über die Benutzerkonfigurationseinstellungen in dieser Bereitstellung und ihre Standardwerte finden Sie Einstellungsreferenz für Single Sign-On 5.0. Beachten Sie, dass einige der dort beschriebenen Optionen und

Features in dieser Bereitstellung nicht verwendet werden. Der Überblick enthält die folgenden Informationen:

- Grundlegendes Plug-in-Verhalten
- Plug-in-Benutzeroberfläche
- Synchronisierung
  Hinweis: Wählen Sie nicht die Option Zugriff auf Anmeldeinfo über das Modul 'Synchronisierung der Anmeldeinformationen' zulassen. Das Modul "Synchronisierung der Anmeldeinfo" ist in der Bereitstellung der Benutzerkonfigurationen nicht eingeschlossen.
- Anwendungsunterstützung
- Lizenzierung

- Informationen zum Schutz der Benutzeranmeldeinformationen finden Sie unter Datenschutzmethoden.
  Hinweis: Verwenden Sie die Standardwerte für die sekundären Datenschutzeinstellungen. Für andere Werte als die Standardwerte ist das Modul "Schlüsselverwaltung" erforderlich, das nicht in dieser Bereitstellung eingeschlossen ist.
  Bei dieser Bereitstellung können Sie anfänglich die Standard-Benutzerkonfigurationseinstellungen (mit Ausnahme der Lizenzierungseinstellungen) in den meisten Umgebungen verwenden. Sollten sich die Anforderungen ändern, wenn die Bereitstellung genutzt wird, können Sie die Benutzerkonfigurationswerte entsprechend ändern.

  Die Einstellungen für Features, die in dieser Bereitstellung nicht verwendet werden, sind standardmäßig nicht aktiviert.

Erstellen des zentralen Speichers

Beim zentralen Speicher von Single Sign-On kann es sich um einen von zwei Typen handeln: Active Directory oder eine NTFS-Netzwerkfreigabe. In dieser Bereitstellung werden Sie einen zentralen Speicher auf einer NTFS-Netzwerkfreigabe erstellen, da weniger Berechtigungen für sie erforderlich sind als für einen zentralen Active Directory-Speicher. Informationen über die Vorteile von NTFS-Netzwerkfreigaben und Hinweise zu ihrer Verwendung finden Sie unter Auswählen einer NTFS-Netzwerkfreigabe.

Falls nötig können Sie die Benutzer später in einen zentralen Active Directory-Speicher migrieren.

Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe

1. Laden Sie das XenApp-Medium.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Serverkomponenten > Sonstiges > Single Sign-On.
3. Klicken Sie auf Zentraler Speicher.
4. Wählen Sie NTFS-Netzwerkfreigabe.

Der zentrale Speicher wird als %SystemDrive%\CITRIXSYNC$ erstellt.

Installieren der Single Sign-On-Komponente vom AppCenter

In der Standardinstallation umfasst AppCenter die Single Sign-On-Komponente.

Wenn Sie eine bestehende Instanz von AppCenter mit Single Sign-On verwenden möchten, konfigurieren Sie Discovery entsprechend und führen Sie es aus, nachdem der zentrale Speicher erstellt wurde.

Wenn Sie eine neue Instanz von AppCenter mit Verwendung von Single Sign-On installieren möchten, stellen Sie sicher, dass die erforderlichen Microsoft Visual C++ Redistributable Packages und Microsoft Primary Interoperability Assemblies installiert sind, wie unter Systemanforderungen beschrieben.

Installieren von AppCenter

1. Laden Sie das XenApp-Medium.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Gemeinsame Komponenten > Managementkonsolen.

Folgen Sie den Anweisungen.
3. Wählen Sie Discovery konfigurieren und durchführen und folgen Sie den Anweisungen.

Nach der Konfiguration ist die Single Sign-On-Komponente von AppCenter mit dem zentralen Speicher verbunden, so dass Sie sie zum Definieren von Kennwortrichtlinien und Erstellen von Benutzerkonfigurationen verwenden können sowie Single Sign-On zum Ermitteln von Anwendungen konfigurieren können.

Installieren des Anwendungsdefinitionstools

Ist Citrix AppCenter nicht installiert auf einem Computer, auf dem eine Anwendung ausgeführt wird, die Sie in die Bereitstellung einschließen möchten, müssen Sie das Anwendungsdefinitionstool installieren, um Anwendungsdefinitionen für die Anwendung zu erstellen.

1. Laden Sie das XenApp-Medium.
2. Suchen Sie die Datei "ASC_PasswordManager" im Order "Administration" und führen Sie sie aus.
3. Wählen Sie Anwendungsdefinitionstool. Folgen Sie den Anweisungen.

Definieren von Kennwortrichtlinien

Wenn Sie entschieden haben, dass die Standardwerte der Standard-Kennwortrichtlinien Ihren Zwecken in dieser Bereitstellung entsprechen, ist es nicht erforderlich, weitere Richtlinien zu erstellen. Andernfalls können Sie neue Richtlinien erstellen, die auf den Standardrichtlinien basieren.

Erstellen einer neuen Kennwortrichtlinie

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Kennwortrichtlinien.
3. Klicken Sie im Menü Aktionen auf Kennwortrichtlinie erstellen.
4. Folgen Sie den Anweisungen des Assistenten für Kennwortrichtlinien.

Konfigurieren von Single Sign-On für die Erkennung von Anwendungen

Single Sign-On erkennt und reagiert auf Anwendungen basierend auf den Einstellungen in den Anwendungsdefinitionen. Anwendungsdefinitionen stellen die Informationen bereit, mit denen das Single Sign-On Plug-In die Anmeldeinformationen der Benutzer an Anwendungen senden und auftretende Fehlerzustände erkennen kann.

Anwendungsdefinitionen bestehen aus Formulardefinitionen. Über Formulardefinitionen analysiert das Single Sign-On Plug-In jede Anwendung beim Starten, erkennt Identifizierungsmerkmale und stellt fest, ob für die startende Anwendung eine bestimmte Aktion ausgeführt werden muss, beispielsweise:

- Senden von Anmeldeinformationen des Benutzers bei Anmeldeaufforderung
- Aushandeln einer Oberfläche zum Ändern von Anmeldeinformationen
- Verarbeiten einer Oberfläche zum Bestätigen von Anmeldeinformationen

Obwohl die meisten Anwendungen und die entsprechenden Anwendungsdefinitionen nur zwei Formulare für das Verwalten der Anmeldeinformationen der Benutzer verwenden, können Sie beliebig viele Formulare in einer Anwendungsdefinition definieren.

Sie können die folgenden Typen von Verwaltungsformularen für Benutzeranmeldeinformationen erstellen:

- Anmeldeformular
  Identifiziert die Anmeldeoberfläche für eine Anwendung und verwaltet die Aktionen, die für den Zugriff auf die zugeordnete Anwendung benötigt werden.

- Kennwortänderungsformular

Identifiziert die Kennwortänderungsoberfläche für eine Anwendung und verwaltet die Aktionen, die für das Ändern des Benutzerkennworts für die zugeordnete Anwendung benötigt werden.

- Formular für eine erfolgreiche Kennwortänderung
  Identifiziert die Oberfläche für eine erfolgreiche Änderung des Kennworts für eine Anwendung und verwaltet die Aktionen, die für das Bestätigen einer erfolgreichen Kennwortänderung für die zugeordnete Anwendung benötigt werden.

- Formular für eine fehlgeschlagene Kennwortänderung
  Identifiziert die Oberfläche für eine fehlgeschlagene Kennwortänderung für eine Anwendung und legt die Aktionen fest, die bei einer fehlgeschlagenen Kennwortänderung ausgeführt werden müssen.

Sie können Anwendungsdefinitionen mit den in AppCenter verfügbaren Assistenten oder dem Anwendungsdefinitionstool erstellen. Wenn die Anwendung, die Sie definieren möchten, ausgeführt wird oder in einem Browserfenster verfügbar ist, sammeln diese Assistenten die Informationen, die Sie für die Anwendungsdefinition benötigen. Für das Erstellen einer Anwendungsdefinition müssen Sie vom Computer, auf dem die Anwendungsdefinition erstellt wird, auf die Anwendung zugreifen können.

Da sich Anwendungssignaturen abhängig von dem Betriebssystem, auf dem die Anwendung ausgeführt wird, unterscheiden können, sollten Sie Anwendungsdefinitionen auf allen Betriebssystemen testen, auf denen sie verwendet werden sollen.

Für einige Anwendungen stehen Anwendungsvorlagen zur Verfügung. Diese Vorlagen vereinfachen Ihnen das Hinzufügen von Anwendungsdefinitionen zur Single Sign-On-Bereitstellung, indem sie die meisten der für die Anwendungsdefinition erforderlichen Informationen bereitstellen. Weitere Informationen über Anwendungsvorlagen finden Sie unter Anwendungsvorlagen.

Erstellen einer Windows-Anwendungsdefinition

Wenn Sie eine Anwendungsdefinition für eine Windows-Anwendung erstellen möchten, führen Sie die Anwendung auf einem Computer aus, auf dem Sie gleichzeitig den Assistenten für Anwendungsdefinitionen von Citrix AppCenter oder das Anwendungsdefinitionstool starten. Navigieren Sie innerhalb der Anwendung, für die ein Ereignis zur Verwaltung von Benutzeranmeldeinformationen (Benutzeranmeldung, Kennwortänderung, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) erforderlich ist, zum entsprechenden Formular, während Sie den Assistenten ausführen.

Einen Überblick über die Überlegungen für Windows-Anwendungsdefinitionen finden Sie unter Windows-Anwendungsdefinitionen.

1. Starten Sie die Anwendung.
2. Bereiten Sie den Start des Assistenten für Anwendungsdefinitionen vor:
   - In AppCenter: Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter. Erweitern Sie den Knoten Single Sign-On und wählen Sie Anwendungsdefinitionen.
   - Im Anwendungsdefinitionstool: Klicken Sie auf Start > Alle Programme > Citrix > Single Sign-On > Anwendungsdefinitionstool.
3. Wählen Sie Anwendungsdefinition erstellen.
4. Stellen Sie sicher, dass Windows und Neu erstellen ausgewählt sind und klicken Sie auf Assistent starten.
5. Geben Sie den Namen der Anwendung ein, wie er im zentralen Speicher angezeigt werden soll. Sie können wahlweise auch eine Beschreibung angeben. Klicken Sie auf Next.
6. Klicken Sie auf Formular hinzufügen. Der Assistent für Formulardefinitionen wird gestartet.

7. Starten Sie ggf. nun das Programm und navigieren Sie zum Formular für die Benutzeranmeldung, Kennwortänderung bzw. die erfolgreiche oder fehlgeschlagene Kennwortänderung.
8. Klicken Sie auf der Seite Formular identifizieren im Assistenten für Formulardefinitionen auf Auswählen.
9. Wählen Sie unter Programmfenster auswählen die Anwendung, für die Sie eine Definition erstellen möchten. Ein blinkender Rand wird um die Eingabeaufforderung der Anwendung herum angezeigt.
10. Geben Sie auf der Seite Formular benennen einen Namen für das Formular ein und wählen Sie den Formulartyp. Klicken Sie auf Next.
11. Klicken Sie unter Programmfenster auswählen auf OK.
12. Klicken Sie auf der Seite Formular identifizieren auf Weiter.
13. Konfigurieren Sie auf der Seite Formularaktionen definieren die Felder und Schaltflächen für die Anmeldeinformationen, die im Formular angezeigt werden sollen.
    1. Klicken Sie auf den Link Festlegen/Ändern, der bestimmten Anmeldeinformationen des Benutzers zugeordnet ist. Dadurch wird das Dialogfeld Steuerelementtext konfigurieren geöffnet, in dem das Steuerelement identifiziert wird, das die ausgewählten Anmeldeinformationen des Benutzers erhalten soll.
    2. Wählen Sie den Steuerelementtyp aus, der die Anmeldeinformationen erhalten soll. Je nach den Kandidaten, die Sie auswählen, wird in der Anwendung ein blinkender Rand um den entsprechenden Steuerelementtyp angezeigt.
    3. Wiederholen Sie diese Aktion für alle Anmeldeinformationen des Benutzers, die für das Formular erforderlich sind, sowie für die erforderliche Schaltfläche zum Senden des Formulars.
       Für einige Formulare sind Domänen- oder andere benutzerdefinierte Anmeldeinformationen erforderlich, die erfolgreich gesendet werden müssen, um das Formular zu verarbeiten. Zwei benutzerdefinierte Felder sind verfügbar, um diese Anforderungen zu erfüllen. Weisen Sie diesen Feldern die Sonderanmeldeinformationen zu. Die diesen Feldern zugeordneten Namen werden auf der Seite Benutzerdefinierte Felder benennen des Assistenten für Anwendungsdefinitionen nach der Definition des Formulars festgelegt.

       Hinweis: Nicht alle Anmeldeinformationen, die oben auf der Seite Formularaktionen definieren angegeben sind, müssen konfiguriert werden.
14. Wenn für die Anwendungen zusätzliche Formulare erforderlich sind, verwenden Sie die Assistenten, um sie zu erstellen.

Erstellen einer Webanwendungsdefinition

Wenn Sie eine Anwendungsdefinition für eine Webanwendung erstellen möchten, führen Sie die Anwendung auf einem Computer aus, auf dem Sie gleichzeitig den Assistenten für Anwendungsdefinitionen von Citrix AppCenter oder das Anwendungsdefinitionstool starten. Navigieren Sie innerhalb der Anwendung, für die ein Ereignis zur Verwaltung von Benutzeranmeldeinformationen (Benutzeranmeldung, Kennwortänderung, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) erforderlich ist, zum entsprechenden Formular, während Sie den Assistenten ausführen.

1. Starten Sie die Anwendung.
2. Bereiten Sie den Start des Assistenten für Anwendungsdefinitionen vor:
   - In AppCenter: Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter. Erweitern Sie den Knoten Single Sign-On und wählen Sie Anwendungsdefinitionen.
   - Im Anwendungsdefinitionstool: Klicken Sie auf Start > Alle Programme > Citrix > Single Sign-On > Anwendungsdefinitionstool.
3. Wählen Sie Anwendungsdefinition erstellen.
4. Stellen Sie sicher, dass Web und Neu erstellen ausgewählt sind und klicken Sie auf Assistent starten.
5. Geben Sie auf der Seite Anwendung festlegen den Namen der Anwendung ein, wie er im zentralen Speicher angezeigt werden soll. Sie können wahlweise auch eine Beschreibung angeben. Klicken Sie auf Next.

6. Klicken Sie auf Formular hinzufügen. Der Assistent für Formulardefinitionen wird gestartet.
7. Klicken Sie auf der Seite Formular benennen auf Weiter.
   1. Geben Sie einen Namen für das Formular ein.
   2. Wählen Sie den Formulartyp aus.
   3. Stellen Sie sicher, dass Keine spezielle Aktion ausgewählt wurde.
   4. Klicken Sie auf Next.
8. Starten Sie ggf. nun das Programm und navigieren Sie zum Formular für die Benutzeranmeldung, Kennwortänderung bzw. die erfolgreiche oder fehlgeschlagene Kennwortänderung.
9. Klicken Sie auf der Seite Formular identifizieren auf Auswählen. Der Assistent für Webformulare wird gestartet.
10. Wählen Sie unter Webseite auswählen die Anwendung, für die Sie eine Definition erstellen möchten. Klicken Sie auf OK. Ein blinkender Rand wird rund um die Webseite angezeigt, in der das Anmeldeformular der Anwendung angezeigt wird.
11. Geben Sie einen Namen für das Formular ein und wählen Sie den Formulartyp. Klicken Sie auf Next.
12. Zum Verwalten der Interpretation der identifizierten URLs sind auf der Seite Formular identifizieren zwei Kontrollkästchen verfügbar: Aktivieren Sie die relevanten Kontrollkästchen und klicken Sie auf Weiter.
    - Strenge URL-Zuordnung
      Wenn Sie dieses Kontrollkästchen aktivieren, werden Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers nur erkannt, wenn sie von Webanwendungen stammen, die über die angegebenen URLs gestartet wurden. Einige URLs enthalten unter Umständen dynamische Daten wie Kennungen zur Sitzungsverwaltung, Anwendungsparameter oder andere Kennungen, die für jede Instanz unterschiedlich sein können. In diesem Fall wird die URL beim Verwenden der strengen URL-Zuordnung möglicherweise nicht erkannt.

    - URL (Groß-/Kleinschreibung)
      Aktivieren Sie dieses Kontrollkästchen, um URLs mit genau übereinstimmender Schreibweise zu verwenden.

13. Konfigurieren Sie auf der Seite Formularaktionen definieren die Felder und Schaltflächen für die Anmeldeinformationen, die im Formular angezeigt werden sollen.
    1. Klicken Sie auf den Link Festlegen/Ändern, der bestimmten Anmeldeinformationen des Benutzers zugeordnet ist. Das Dialogfeld Feldtext konfigurieren wird geöffnet, in dem das Feld identifiziert wird, das diese Anmeldeinformationen erhält. Bei bereits geöffnetem Formular enthält dieses Dialogfeld alle möglichen Steuerelemente für den Feldtyp, der den ausgewählten Anmeldeinformationen des Benutzers oder der Sendeoption zugeordnet ist.
    2. Wenn das Formular für die Anmeldeinformationen für die Anwendung nicht geöffnet ist, starten Sie die Anwendung und rufen Sie das richtige Formular für die Anmeldeinformationen des Benutzers auf. Wählen Sie dann Aktualisieren. Nach der Auswahl des Anwendungsformulars werden in diesem Dialogfeld die möglichen Feldtypen angezeigt, die den ausgewählten Anmeldeinformationen des Benutzers entsprechen.
    3. Wählen Sie den Feldtyp aus, der die Anmeldeinformationen erhält. Bei der Auswahl der verschiedenen möglichen Optionen wird der zugeordnete Feldtyp in der Anwendung markiert, damit der Feldtyp, der die identifizierten Anmeldeinformationen des Benutzers bzw. die Schaltfläche "Senden" erhalten soll, leichter identifiziert werden kann.
    4. Wiederholen Sie diese Aktion für alle Anmeldeinformationen des Benutzers, die für das Formular erforderlich sind, sowie für die erforderliche Schaltfläche zum Senden des Formulars.
       Für einige Formulare sind Domänen- oder andere benutzerdefinierte Anmeldeinformationen erforderlich, die erfolgreich gesendet werden müssen, um das Formular zu verarbeiten. Zwei benutzerdefinierte Felder sind verfügbar, um diese Anforderungen zu erfüllen. Weisen Sie diesen Feldern die Sonderanmeldeinformationen zu. Die diesen Feldern zugeordneten Namen werden auf der Seite Benutzerdefinierte Felder benennen des Assistenten für Anwendungsdefinitionen nach der Definition des Formulars festgelegt.

       Hinweis: Nicht alle Anmeldeinformationen, die oben auf der Seite Formularaktionen definieren angegeben sind, müssen konfiguriert werden.

14. Wenn für die Anwendungen zusätzliche Formulare erforderlich sind, verwenden Sie die Assistenten, um sie zu erstellen.

Hinzufügen einer Anwendungsdefinition für eine Anwendung mit einer verfügbaren Vorlage

Der Assistent für Anwendungsdefinitionen hilft Ihnen dabei, Anwendungsvorlagen zu finden und sie Ihrer Bereitstellung hinzuzufügen.

1. Bereiten Sie den Start des Assistenten für Anwendungsdefinitionen vor:
   - In AppCenter: Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter. Erweitern Sie den Knoten Single Sign-On und wählen Sie Anwendungsdefinitionen.
   - Im Anwendungsdefinitionstool: Klicken Sie auf Start > Alle Programme > Citrix > Single Sign-On > Anwendungsdefinitionstool.
2. Wählen Sie Vorlagen verwalten.
3. Sehen Sie in der Liste der Anwendungen nach, ob die gewünschte Anwendung angezeigt wird. Sie können auch den Link verwenden, um weitere Anwendungen aus dem Internet herunterzuladen und sie in die Liste zu importieren.
4. Wählen Sie die hinzuzufügende Anwendungsvorlage aus und klicken Sie auf Anwendungsdefinition erstellen.
5. Verwenden Sie den Assistenten, um die Formulare für die Anwendung zu bearbeiten oder die Standardwerte anzunehmen.

Erstellen von Benutzerkonfigurationen

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie auf Benutzerkonfiguration hinzufügen.
4. Geben Sie den Namen der Anwendung ein, wie er im zentralen Speicher angezeigt werden soll. Sie können wahlweise auch eine Beschreibung angeben.
5. Geben Sie an, wie Sie diese Benutzerkonfiguration den Benutzern zuordnen möchten.
   Sie haben zwei Optionen: Benutzer können entsprechend einer Active Directory-Hierarchie (Organisationseinheit oder Einzelbenutzer) oder einer Active Directory-Gruppe zugeordnet werden. Bei Bedarf können Sie die Benutzerkonfiguration später einer anderen Hierarchie oder Gruppe zuordnen, indem Sie im Menü Aktion auf Benutzerkonfiguration verschieben klicken.

   Wichtig: Die Organisation der Active Directory-Umgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Wenn Sie sowohl Active Directory-Hierarchien als auch Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.
   Wenn ein Benutzer zu zwei verschiedenen Active Directory-Gruppen gehört und jede der Gruppen einer Benutzerkonfiguration zugeordnet ist, hat die Benutzerkonfiguration mit der höchsten Priorität Vorrang und wird verwendet.

   Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

6. Fügen Sie auf der Seite Anwendungen auswählen die Anwendungen für die Benutzerkonfiguration hinzu. Wenn Sie auf die Schaltfläche Hinzufügen klicken, werden die bereits erstellten Anwendungsdefinitionen in einem Dialogfeld angezeigt.
7. Legen Sie auf der Seite Single Sign-On Plug-In-Verhalten konfigurieren das Verhalten der Plug-In-Software für alle Benutzer in der Umgebung fest.

8. Wählen Sie auf der Seite Lizenzierung konfigurieren einen Lizenzserver und ein Lizenzierungsmodell aus.
9. Auf der Seite Datenschutzmethoden auswählen können Sie die Datenschutzmethoden zum Schutz der Anmeldeinformationen der Benutzer auswählen, je nachdem, welche der Authentifizierungsmethoden die Benutzer verwenden dürfen.

Installieren des Single Sign-On Plug-Ins

Das Single Sign-On Plug-In wird auf dem XenApp-Server ausgeführt und stellt Anmeldeinformationen und Zugriff auf veröffentlichte Anwendungen bereit. Das Plug-In wird auch auf jedem Benutzergerät ausgeführt, um die Anmeldeinformationen an Anwendungen weiterzureichen und es den Benutzern zu ermöglichen, ihre Anmeldeinformationen zu verwalten.

Berücksichtigungen für die Installation:

- Nach der Installation des Plug-Ins unter unterstützten Betriebssystemen, die die Windows-Komponente Microsoft Graphical Identification and Authentication (GINA) verwenden, muss das Gerät neu gestartet werden. Hierzu gehören Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 und Microsoft Windows Server 2003 mit Service Pack 2.
  WinLogon verwendet die GINA-Steuerelemente für das Dialogfeld, das Benutzern angezeigt wird, wenn sie die Tastenkombination STRG+ALT+ENTF drücken. Das Dialogfeld sammelt alle für die Authentifizierung erforderlichen Daten. XenApp, das Single Sign-On Plug-In und der Novell NetWare-Client interagieren alle mit der GINA-DLL (Dynamic Link Library) bzw. machen eine Ersetzung erforderlich. Unter Umständen müssen Sie Software in einer bestimmten Reihenfolge installieren oder deinstallieren, damit die richtige GINA-Kette erhalten bleibt. Wenn Sie das Single Sign-On Plug-In als letztes Programm installieren, stellen Sie sicher, dass Single Sign-On-GINA als erstes vom Winlogon-Prozess aufgerufen wird.

- Nach dem Abschluss der Installation (und ggf. dem Neustart des Geräts) wird das Citrix Receiver-Symbol in der Taskleiste angezeigt.
- Wenn Sie nach der Installation des Plug-Ins die Citrix Lizenzierungsinformationen konfigurieren oder ändern, starten Sie das Plug-In neu, um die Änderungen zu übernehmen.

Installieren des Single Sign-On Plug-Ins auf einem Benutzergerät oder einem XenApp-Server

1. Laden Sie das XenApp-Medium auf dem Computer oder Server.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Serverkomponenten > Sonstiges > Single Sign-On > Single Sign-On Plug-In.
3. Folgen Sie den Anweisungen.

Anleiten der Benutzer zum Verwenden von Single Sign-On

Bevor die Endbenutzer beginnen, Single Sign-On zu verwenden, überprüfen Sie, dass die Hilfe für Endbenutzer in der Benutzeroberfläche von Single Sign-On zur Verfügung steht. Informieren Sie die Benutzer darüber, wie Single Sign-On funktioniert und welche Funktionen in dieser Bereitstellung verfügbar sind.

Systemanforderungen

Oct 05, 2015

Auf den Computern in der Single Sign-On-Umgebung muss folgende Systemsoftware installiert sein:

Softwarekomponente	Erforderlich für	Bezugsquelle
Microsoft Windows Installer 3.0 oder höher (automatisch Teil der Installation mit Autorun)	Alle	• Ordner "Support" auf dem Single Sign-On-Installationsmedium • http://www.microsoft.com
Microsoft .NET Framework 3.5 (automatisch Teil der Installation mit Autorun)	• Single Sign-On-Dienst • Single Sign-On-Komponente im AppCenter • Anwendungsdefinitionstool	Ordner "Support" auf dem Single Sign-On-Installationsmedium
Microsoft Internet Explorer Version 6.0, 7.0, 8.0 oder 9.0 (nicht geschützter Modus)	Benutzer, die auf Single Sign-On-aktivierte Webanwendungen zugreifen	http://www.microsoft.com
ASP.NET	Single Sign-On-Dienst	http://www.asp.net/

• 32-Bit-Computer: Microsoft Visual C++ 2005 Redistributable Package (x86) Service Pack 1
  • vc80_vcredist_x86.exe
• 64-Bit-Computer: Microsoft Visual C++ 2005 Redistributable Package (x64) Service Pack 1
  • vc80_vcredist_x86.exe
  • vc80_vcredist_x64.exe
	Single Sign-On-Konsole, Dienst oder Plug-in: Beim Installieren der Konsolenkomponente, des Dienstes oder Plug-ins an einer Befehlszeile unter Windows Vista, Windows Server 2008 oder Windows Server 2008 R2	Ordner "Support" auf dem Single Sign-On-Installationsmedium

• 32-Bit-Computer: Microsoft Visual C++ 2008 Redistributable Package (x86) Service Pack 1
  • vc90_vcredist_x86.exe
• 64-Bit-Computer: Microsoft Visual C++ 2008 Redistributable Package (x86) Service Pack 1
  • vc90_vcredist_x86.exe
  • vc90_vcredist_x64.exe
	Single Sign-On-Konsole, Dienst oder Plug-in: Beim Installieren der Konsolenkomponente, des Dienstes oder Plug-ins an einer Befehlszeile unter Windows Vista, Windows Server 2008 oder Windows Server 2008 R2	Ordner "Support" auf dem Single Sign-On-Installationsmedium

Microsoft Primary Interoperability	Single Sign-On-Konsole: Beim	Ordner "Support" auf dem Single Sign-

Softwarekomponente	Erforderlich für	Bezugsquelle
Assemblies • vs90_piaredist.exe	Installieren der Konsolenkomponente an einer Eingabeaufforderung unter Windows Vista, Windows Server 2008 oder Windows Server 2008 R2	On-Installationsmedium
Verstärkte Sicherheitskonfiguration für Internet Explorer	Single Sign-On Plug-in: Deaktivieren Sie die verstärkte Sicherheitskonfiguration für Internet Explorer, wenn Sie das Plug-in auf einem Computer mit Windows Server 2003, Windows Server 2008 oder Windows Server 2008 R2 installieren. Bei Aktivierung reagiert das Plug-in nicht auf Webanwendungsdefinitionen.	

Anforderungen für die Single Sign-On-Komponente

Single Sign-On-Komponente	Unterstützte Umgebung oder Microsoft Windows-Betriebssysteme	Unterstützte Sprachen	Hardwareanforderungen
Zentraler Speicher	• Active Directory • NTFS-Dateifreigabe	• Englisch • Deutsch • Französisch • Spanisch • Japanisch	30 KB Speicherplatz auf der Festplatte pro Benutzer
Single Sign-On-Komponente im AppCenter	• Microsoft Windows 7 Service Pack 1 (32 Bit und 64 Bit) • Microsoft Windows 7 (32 Bit und 64 Bit) • Microsoft Windows Vista Service Pack 2 (Business Edition, Ultimate Edition, Enterprise Edition) (32 Bit und 64 Bit) • Microsoft Windows Vista (Business Edition, Ultimate Edition, Enterprise Edition) (32 Bit und 64 Bit) • Windows XP Service Pack 3 (32 Bit) • Microsoft Windows XP Professional, Service Pack 2 (32 Bit) • Microsoft Windows XP Professional	• Englisch • Deutsch • Französisch • Spanisch • Japanisch	• 64 MB RAM • 60 Speicherplatz auf der Festplatte

Single Sign-On-Komponente	Unterstützte Umgebung oder Microsoft Windows-Betriebssysteme	Unterstützte Sprachen	Hardwareanforderungen
	x64 Edition (64 Bit) • Windows Server 2008 R2 Service Pack 1 (64 Bit) • Microsoft Windows Server 2008 R2 (64 Bit) • Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit)		
Plug-in	• Microsoft Windows 7 Service Pack 1 (32 Bit und 64 Bit) • Microsoft Windows 7 (32 Bit und 64 Bit) • Microsoft Windows Vista Service Pack 2 (Business Edition, Ultimate Edition, Enterprise Edition) (32 Bit und 64 Bit) • Microsoft Windows Vista (Business Edition, Ultimate Edition, Enterprise Edition) (32 Bit und 64 Bit) • Windows XP Service Pack 3 (32 Bit) • Microsoft Windows XP Professional, Service Pack 2 (32 Bit) • Microsoft Windows XP Professional x64 Edition (64 Bit) • Microsoft Windows XP Embedded • Windows Server 2008 R2 Service Pack 1 (64 Bit) • Microsoft Windows Server 2008 R2 (64 Bit) • Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64	• Englisch • Deutsch • Französisch • Spanisch • Japanisch • Vereinfachtes Chinesisch	• 10 MB RAM • 25 MB Speicherplatz auf der Festplatte (keine Installation der optionalen Features) • 35 MB Speicherplatz auf der Festplatte (Installation der optionalen Features)

Single Sign-On-Komponente	Unterstützte Umgebung oder Microsoft Windows-Betriebssysteme	Unterstützte Sprachen	Hardwareanforderungen
	Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit)		
Dienst	• Windows Server 2008 R2 Service Pack 1 (64 Bit) • Microsoft Windows Server 2008 R2 (64 Bit) • Microsoft Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit) • Microsoft Windows Server 2003 R2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit)	• Englisch • Deutsch • Französisch • Spanisch • Japanisch	• 128 MB RAM • 30 Speicherplatz auf der Festplatte
Anwendungsdefinitionstool	Entspricht Plug-in	• Englisch • Deutsch • Französisch • Spanisch • Japanisch	Entspricht Plug-in

Hinweis: Single Sign-On wird nicht unter Microsoft Windows XP Home Edition unterstützt.
Hotdesktop wird nur unter den folgenden Betriebssystemen unterstützt:

- Microsoft Windows XP Professional, Service Pack 2 (32 Bit)
- Microsoft Windows XP Embedded

Hotdesktop wird nicht unter 64-Bit-Betriebssystemen oder Serverbetriebssystemen unterstützt.

Lizenzierungsanforderungen

Installieren Sie zuerst den Lizenzserver und fügen Sie Lizenzen hinzu, bevor Sie Single Sign-On installieren.

Für dieses Release muss die aktuelle Version des Lizenzservers installiert sein. Wenn Sie frühere Versionen des Lizenzservers ausführen, müssen Sie den Lizenzserver aktualisieren.
Wichtig: Für lokal installierte Instanzen des Single Sign-On Plug-Ins wird keine separate Lizenz für Benutzer benötigt, die auf gehostete Anwendungen in einer Umgebung mit Citrix XenApp, Platinum Edition, zugreifen können.

Getrennter Modus

Wenn Sie Benutzer haben, deren Verbindung zum Lizenzserver für längere Zeit getrennt ist, z. B. mobile Benutzer mit Laptops, müssen Sie für diese Benutzer einen Zeitraum für den getrennten Modus angeben. Der Zeitraum für den getrennten Modus wird in den Lizenzierungseinstellungen in der Benutzerkonfiguration angegeben. Der Zeitraum für den

getrennten Modus gibt zwei Aspekte des Lizenzierungsverhalten an:

- Die Dauer, für die eine Benutzerverbindung zum Lizenzserver getrennt sein kann, ohne in den Lizenzierungskulanzzeitraum überzugehen. Nach dem Ablauf des Zeitraums für den getrennten Modus gehen die Benutzerverbindungen, die der Benutzerkonfiguration zugeordnet sind, in den Lizenzierungskulanzzeitraum von 30 Tagen über.
- Der Zeitraum, bis eine ausgecheckte Lizenz, die im getrennten Modus ist, an den Pool verfügbarer Lizenzen auf dem Lizenzserver zurückgegeben wird, unabhängig davon, ob das Produkt erneut eine Verbindung zum Lizenzserver herstellt. Wenn eine Lizenz ausgecheckt ist, und der Zeitraum für den getrennten Modus, der dieser Lizenz zugeordnet ist, vor dem Einchecken der Lizenz abläuft, checkt der Lizenzserver die Lizenz wieder ein, damit sie zur Verfügung steht. Beispiel: Wenn ein Laptop mit Single Sign-On verloren geht und nie wieder eine Verbindung zum Unternehmensnetzwerk herstellt, checkt der Lizenzserver die Lizenz automatisch am Ende des Zeitraums für den getrennten Modus ein.

Wenn Sie den Zeitraum für den getrennten Modus festlegen, geben Sie an, wie lange Sie warten, bis die Lizenz an den Pool der verfügbaren Lizenzen zurückgegeben wird.

Sie sollten lange Zeiträume für den getrennten Modus für Benutzer angeben, die nicht regelmäßig eine Verbindung zum Unternehmensnetzwerk herstellen, z. B. Verkaufsmitarbeiter, die remote arbeiten. Beachten Sie jedoch, dass Sie ausgecheckte Lizenzen für die Dauer dieses Zeitraums nicht wieder dem Pool hinzufügen können, selbst wenn das Gerät verloren oder kaputt ist.

Gemischte Lizenztypen

Je nach den Anforderungen in der Single Sign-On-Umgebung bzw. im Unternehmen verwenden Sie ggf. früher erworbene eigenständige Single Sign-On-Lizenzen. Sie könnten beispielsweise für mobile Benutzer, die über Desktopcomputer und Laptop auf das Single Sign-On Plug-in zugreifen, Benutzerkonfigurationen nach dem Lizenzierungsmodell für benannte Benutzer erstellen. Außerdem könnten Sie Benutzerkonfigurationen nach dem CCU-Lizenzierungsmodell für Hotdesktop-Benutzer erstellen.

In einigen Fällen könnten alle benannten Benutzerlizenzen verwendet werden, und Single Sign-On steht einigen Benutzern daher nicht mehr zur Verfügung. Unter diesen Umständen können Sie gleichzeitige Benutzerlizenzen in der Benutzerkonfiguration festlegen, die offline verwendet werden.

Planen

Oct 05, 2015

Vor der Installation von Single Sign-On sollten Sie Ihre Umgebung planen. Hierzu gehören folgende Aufgaben: Festlegen des Typs für den zentralen Speicher, der Single Sign-On-aktivierten Anwendungen im Unternehmen, für die Single Sign-On aktiviert werden soll, der verwendeten Single Sign-On-Features und Einrichten von Kennwortrichtlinien.

Eine Single Sign-On-Umgebung kann die folgenden Elemente enthalten:

- Freigegebene Netzwerkordner oder Active Directory mit dem zentralen Speicher.
- Mindestens einen Computer, auf dem die Single Sign-On-Komponente des Citrix AppCenters ausgeführt wird.
- Benutzercomputer, auf denen das Single Sign-On Plug-in ausgeführt wird.
- Einen dedizierten Server, auf dem der Single Sign-On-Dienst ausgeführt wird und auf dem ein oder mehrere Module installiert sind.
- Citrix XenApp-Umgebung, in der das Single Sign-On Plug-in gehostet wird.
- Authentifizierungsgeräte, z. B. Smartcards.
- Single Sign-On-Features, z. B. Hotdesktop und Schlüsselverwaltung.

Typen des zentralen Speichers

Oct 05, 2015

Single Sign-On verwendet ein Repository, den sogenannten zentralen Speicher, um Informationen zu Benutzern und der Umgebung zu speichern und abzurufen. Single Sign-On führt mit den Daten im zentralen Speicher alle standardmäßigen und konfigurierten Single Sign-On-Funktionen aus. Sie können einen zentralen Speicher im Rahmen der Installation von Single Sign-On automatisch oder mit dem Dienstprogramm zum Setup des zentralen Speichers manuell erstellen.

Der zentrale Speicher enthält Benutzerdaten und administrative Daten:

- Benutzerdaten im zentralen Speicher sind u. a. die sekundären Anmeldeinformationen des Benutzers, Sicherheitsfragen und Antworten, dienstspezifische Daten (z. B. Provisioningdaten, fragenbasierte Authentifizierungsdaten, Registrierung für die Schlüsselwiederherstellung usw.) sowie die Single Sign-On zugeordneten Benutzerdaten der Windows-Registrierung.
- Administrative Daten im zentralen Speicher sind u. a. Anwendungsdefinitionen, Kennwortrichtlinien, Sicherheitsfragen und weitere Einstellungen, die in der Konsole für Features und Komponenten von Single Sign-On festgelegt werden.

Im Wesentlichen ermöglicht der zentrale Speicher die Kommunikation der auf einem Computer des Benutzers oder einem Computer mit XenApp ausgeführten Plug-in-Software mit dem zentralen Speicher und den Diensten, um Anmeldeinformationen des Benutzers an Anwendungen bereitzustellen, auf die der Benutzer zugreifen darf.

Die Plug-in-Software verwaltet einen lokalen Speicher auf dem Computer des Benutzers. Im lokalen Speicher werden lediglich die sekundären Anmeldeinformationen des Benutzers, die Informationen zur Schlüsselwiederherstellung und ggf. die Sicherheitsfragen und Antworten gespeichert. Die Agentsoftware ist mit dem zentralen Speicher synchronisiert. So können sich die Benutzer frei im Unternehmen bewegen und haben jederzeit Zugriff auf die gespeicherten Anmeldeinformationen.

Typen des zentralen Speichers sind:

- Active Directory
  Der zentrale Speicher verwendet die Active Directory-Umgebung und -Objekte zum Speichern und Aktualisieren von Single Sign-On-Daten.

- NTFS-Netzwerkfreigabe
  Der zentrale Speicher verwendet eine Windows-Netzwerkfreigabe zum Speichern von Single Sign-On-Daten.

Sie können Benutzer ggf. von einem Typ des zentralen Speichers auf einen anderen migrieren.

Auswählen eines zentralen Speichers unter Active Directory

Wenn Sie einen zentralen Speicher unter Active Directory auswählen, können Sie die Vorteile der bestehenden Active Directory-Benutzerauthentifizierung und -Objektverwaltung nutzen. Sie können z. B. benutzerspezifische Einstellungen auf jede Domänenstufe (Domäne, Organisationseinheit, Gruppe oder Benutzer) anwenden.

Wenn Sie den zentralen Speicher unter Active Directory erstellen, werden dem Active Directory-Schema zwei neue Klassen und zwei Attribute hinzugefügt:

Klasse	Beschreibung
citrix-SSOConfig	Beschreibt das Objekt, das Daten für die Einstellungen der Plug-in-Software enthält, den Synchronisierungszustand und die Anwendungsdefinitionen sowie die Ersteinrichtung der Plug-in-Software. Diese Klasse umfasst die folgenden Attribute:

Klasse	Beschreibung
	citrix-SSOConfigData: Enthält die eigentlichen Daten, citrix-SSOConfigType: Gibt den Datentyp an
citrix-SSOSecret	Beschreibt das geheime Datenobjekt, das für die Authentifizierung eines Single Sign-On-Benutzers verwendet wird. Diese Klasse enthält das folgende Attribut: citrix-SSOSecretData: Enthält verschlüsselte Anmeldeinformationsdaten für eine Anwendung sowie Daten für das benutzerseitige Zurücksetzen des Kennworts

Hinweis: Weitere Informationen zu diesen Klassen und Attributen finden Sie auf dem Installationsmedium in der Datei CitrixMPMSchema.xml im Ordner \Tools.
Wählen Sie Active Directory als zentralen Speicher aus, wenn Folgendes zutrifft:

- Sie können das Active Directory-Schema ohne Auswirkungen auf das Unternehmen erfolgreich erweitern.
- Sie haben bereits die von Microsoft empfohlenen optimalen Verfahren zum Active Directory-Backup und der Active Directory-Wiederherstellung implementiert (obwohl dies keine Voraussetzung ist).
- Sie möchten die in Active Directory integrierte hohe Verfügbarkeit auf die Daten des zentralen Speichers ausdehnen.

Vorteile einen zentralen Speichers unter Active Directory

Die Verwendung eines zentralen Speichers unter Active Directory hat folgende Vorteile:

- Active Directory bietet integriertes Failover und integrierte Redundanz. Zusätzliche Maßnahmen für die Wiederherstellung im Notfall sind nicht erforderlich.
- Mit der Active Directory-Replikation können Sie die im zentralen Speicher enthaltenen administrativen Daten und Benutzerdaten im Unternehmen verteilen.
- Beim Verwenden von Active Directory als zentralen Speicher ist keine weitere Hardware erforderlich.

Überlegungen zu einem zentralen Speicher unter Active Directory

Vor dem Verwenden eines zentralen Speichers unter Active Directory sollten Sie Folgendes berücksichtigen:

- Die Verwendung von Active Directory als zentralen Speicher erfordert die Erweiterung des Schemas und damit eine sorgfältige Planung und Implementierung. Das Erweitern des Schemas wirkt sich auf die komplette Gesamtstruktur aus.
- Es empfiehlt sich, die Erweiterung des Schemas und Erstellung des zentralen Active Directory-Speichers außerhalb der Spitzenauslastungszeiten vorzunehmen. Die Active Directory-Replikationszykluslatenz hat Auswirkungen auf die Geschwindigkeit, mit der die Änderungen auf alle Domänencontroller in der Gesamtstruktur kopiert werden.
- Für die standortübergreifende Replikation von Daten des zentralen Speichers in großen Unternehmen mit WANs muss die Replikation richtig konfiguriert werden, um die Latenz zur verringern. (Die Replikation innerhalb eines Standorts dagegen führt normalerweise zu einer geringeren Latenz.)

Auswählen einer NTFS-Netzwerkfreigabe

Wenn Sie eine NTFS-Netzwerkfreigabe als zentralen Speicher verwenden, können Sie die Vorteile der bestehenden Active Directory-Benutzerauthentifizierung und Struktur nutzen, ohne das Active Directory-Schema erweitern zu müssen. Sie können z. B. benutzerspezifische Einstellungen auf jede Domänenstufe (Domäne, Organisationseinheit, Gruppe oder Benutzer) anwenden.

Wichtig: Verwenden Sie in diesem Fall eine versteckte Freigabe für den zentralen Speicher.
Single Sign-On erstellt einen freigegebenen Ordner mit dem Namen "CITRIXSYNC$" sowie die beiden Unterordner "People" und "CentralStoreRoot".

Der Ordner People enthält für jeden Benutzer einen Unterordner mit den entsprechenden Lese- und Schreibberechtigungen. Der Ordner CentralStoreRoot enthält administrative Daten.

Vorteile einer NTFS-Netzwerkfreigabe

Die Verwendung einer NTFS-Netzwerkfreigabe hat folgende Vorteile:

- Sie können die Darstellungsweise eines zentralen Active Directory-Speichers emulieren, ohne das Active Directory-Schema erweitern zu müssen. Sie können jedoch die Vorteile der bestehenden Active Directory-Hierarchie oder -Gruppen nutzen.
  Hinweis: Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.
- Die Benutzerdaten sind immer aktuell, da sie an einem zentralen Speicherort aufbewahrt werden und die mit Active Directory einhergehende Latenz bei der Datenreplikation vermieden wird.
- Um eine höhere Verfügbarkeit zu gewährleisten, können Sie einen Lastausgleich der Freigaben auf mehreren Computern ausführen, die NTFS-Netzwerkfreigaben hosten können.
- Eine NTFS-Netzwerkfreigabe reduziert die Arbeitslast im Zusammenhang mit den Authentifizierungsaufgaben in der Active Directory-Umgebung.
- Mit Single Sign-On können Sie den zentralen Speicher auf einer NTFS-Netzwerkfreigabe auf einen zentralen Speicher unter Active Directory migrieren, wenn Sie später einen zentralen Speicher unter Active Directory implementieren möchten.

Überlegungen zu einer NTFS-Netzwerkfreigabe

Vor der Verwendung einer NTFS-Freigabe sollten Sie Folgendes berücksichtigen:

- Unter Umständen wird zusätzliche Hardware zum Hosten des zentralen Speichers benötigt.
- Die Dateien und Ordner des zentralen Speichers (einschließlich der dazugehörigen Berechtigungen) müssen regelmäßig gesichert werden. Sie sollten auch Wiederherstellungspläne für den Notfall bereithalten und implementieren, wenn Sie die Replikation von Dateien und Ordnern für die Wiederherstellung von Sites benötigen.
- Die Netzwerktopologie des Unternehmens macht es u. U. für Benutzer (und die Single Sign-On Plug-In-Software) erforderlich, Benutzerdaten über eine oder mehrere WAN-Verbindungen hinweg zu übermitteln. In diesem Fall sollten Sie die Implementierung des verteilten Dateisystems erwägen, das Teil von Microsoft Windows Server 2003 und 2008 ist. Weitere Informationen zum verteilten Dateisystem finden Sie auf der Microsoft Website unter http://support.microsoft.com.

Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen

Administratoren können in Unternehmen mit mehreren Domänen mehrere zentrale Speicher einrichten. In einer solchen Umgebung ist es sogar möglich, mehrere Typen des zentralen Speichers zu verwenden. So können Sie z. B. Benutzerkonfigurationen in einer Domäne dem Speichertyp NTFS-Netzwerkfreigabe zuweisen und in einer anderen Domäne dem Speichertyp Active Directory.

Unternehmen haben möglicherweise mehrere Windows-Domänen, und Benutzer können daher mehrere Windows-Konten haben. Mit dem Feature "Kontozuordnung" in Single Sign-On kann sich ein Benutzer von einem oder mehreren Windows-Konten aus an jeder Anwendung anmelden. Da Single Sign-On normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert.

Administratoren können jedoch die Kontozuordnung konfigurieren und die Anmeldeinformationen des Benutzers mit dem Modul "Synchronisierung der Anmeldeinformationen" synchronisieren. Benutzer mit konfigurierter Kontozuordnung können mit allen Konten in der Single Sign-On-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Ohne die Kontozuordnung muss ein Benutzer, der mehrere Windows-Konten besitzt, die Anmeldeinformationen manuell für jedes Windows-Konto ändern.

Geben Sie Benutzern Zugriff auf AccAssoc.exe als veröffentlichte Anwendung, damit sie die Anmeldeinformationen mit der Kontozuordnung synchronisieren können.

Vorteile der Verwendung der Kontozuordnung

- Die Kontozuordnung steigert die Produktivität und verringert die Inanspruchnahme des Helpdesks, da die Anmeldeinformationen des Benutzers synchronisiert werden und damit das Verwalten oder das Fehlschlagen der Anmeldungen verringert wird.
- Konten können über verschiedene Typen des zentralen Speichers synchronisiert werden. Das heißt, das ein Benutzerkonto, das Active Directory als zentralen Speicher verwendet, mit einem zugeordneten Konto synchronisiert werden kann, das als zentralen Speicher eine NTFS-Netzwerkfreigabe verwendet.
- Konten können auch über verschiedene Benutzerkonfigurationszuordnungen synchronisiert werden. Sie können z. B. eine Benutzerkonfiguration in einer Domäne einer Active Directory-Hierarchie (OU oder Benutzer) und in einer anderen Domäne einer Active Directory-Gruppe zuordnen.
- Konten können über verschiedene Benutzerkonfigurationszuordnungen in derselben Domäne und demselben zentralen Speicher synchronisiert werden.
- Für die Kontozuordnung müssen keine vertrauenswürdigen Beziehungen zwischen Domänencontrollern bestehen.

Vor der Konfiguration der Kontozuordnung sollten Sie Folgendes berücksichtigen:

- Die Kontozuordnung ist nicht mit Smartcards kompatibel, wenn Smartcards als primäre Authentifizierungsmethode für die Anmeldung an Windows verwendet werden.
  Hinweis: Die Benutzerkonfigurationen in jeder Domäne haben möglicherweise unterschiedliche Kennwortrichtlinien, wodurch der Zugriff auf eine Ressource blockiert werden könnte. Mit der Kontozuordnung werden jedoch nur die Anmeldeinformationen der Benutzer synchronisiert, nicht die Konfigurationsrichtlinien. Überlegen Sie sich, wie Sie Kennwortrichtlinien im Unternehmen abfassen.
- Jedes zugeordnete Domänenkonto muss Single Sign-On verwenden.
- Anwendungsdefinitionsnamen müssen in jeder Benutzerkonfiguration identisch sein, damit die Anmeldeinformationen von der Kontozuordnung synchronisiert werden können.
- Anmeldeinformationen der Benutzer werden nur für Anwendungen gemeinsam verwendet, die in Anwendungsdefinitionen angegeben sind, die vom Single Sign-On-Administrator erstellt wurden.
- Als Teil des Single Sign-On-Dienstes ist das Modul "Synchronisierung der Anmeldeinformationen" ein Webdienst, der über eine sichere HTTP-Verbindung verfügbar ist. Alle Computer im Unternehmen, die die Kontozuordnung verwenden, müssen auf dieses Modul zugreifen können.

Kennwortrichtlinien

Oct 05, 2015

Kennwortrichtlinien sind Regeln, mit denen festgelegt wird, wie Kennwörter erstellt, gesendet und verwaltet werden. Single Sign-On enthält zwei Standardkennwortrichtlinien: Standardrichtlinie und Domänenrichtlinie. Beide Richtlinien können nicht gelöscht werden. Sie können die Richtlinien kopieren und Änderungen vornehmen, um sie dem Unternehmen und Vorschriften anzupassen.

Standardkennwortrichtlinie

Single Sign-On wendet die Standardrichtlinie auf kennwortgeschützte Anwendungen an, die im Unternehmen verwendet werden (außer den Anwendungen, die Anmeldeinformationen eines Domänenbenutzers benötigen). Die Richtlinie wird auf alle Anwendungen angewendet, die nicht von einem Administrator (mit dem Feature "Anwendungsdefinitionen" in der Konsole) definiert wurden, bzw. auf alle Anwendungen, die nicht Teil einer Anwendungsgruppe sind.

Wenn ein Benutzer im Dialogfeld "Kennwörter verwalten" (früher Anmeldungsmanager) Anmeldeinformationen für eine Anwendung hinzufügt, die keine entsprechende Anwendungsdefinition hat, verwaltet Single Sign-On die Anwendung mit der Standardrichtlinie.

Domänenkennwortrichtlinie

Normalerweise erstellt ein Administrator eine Anwendungsgruppe und weist dann den Anwendungen in dieser Gruppe die Domänenrichtlinie zu. Single Sign-On weist daraufhin denjenigen Anwendungen die Domänenrichtlinie zu, welche die Domänenanmeldeinformationen des Benutzers für den Zugriff benötigen. Sie können die Domänenrichtlinie ändern oder kopieren, sodass sie die für Active Directory bzw. NT geltenden Domänenrichtlinien für Benutzerkonten im Unternehmen widerspiegeln.

Wenn Sie eine Anwendungsgruppe als Domänenkennwortgruppe behandeln möchten, müssen Sie die Domänenrichtlinie auf diese Anwendungsgruppe anwenden. Eine Anwendungsgruppe ist eine Sammlung von definierten Anwendungen mit mindestens einer dazugehörigen Benutzerkonfiguration, einschließlich der Richtlinie für die Verwaltung der Anwendungen.

Benutzerdefinierte Kennwortrichtlinien

Sie können Kennwortrichtlinien nach Bedarf erstellen: Sie können eine Richtlinie auf die gesamte Domänengruppe anwenden, einzelne Richtlinien erstellen und diese zum besseren Schutz der Anwendungen auf einzelne Anwendungsgruppen anwenden usw.

Achten Sie beim Erstellen oder Ändern von benutzerdefinierten Kennwortrichtlinien darauf, dass diese zu den Unternehmens- und Anwendungsanforderungen passen. Wenn Sie z. B. eine Richtlinie erstellen, die absolut nicht mit den Anforderungen einer Anwendung übereinstimmt, können sich die Benutzer möglicherweise nicht an dieser Anwendung authentifizieren.

Mit Kennwortrichtlinien legen Sie im Wesentlichen die folgenden Einschränkungen fest:

- Mindest- und Höchstanzahl der Zeichen im Kennwort
- Verwendung von Buchstaben und Ziffern
- Höchstanzahl wiederholter Zeichen
- Nicht erlaubte bzw. benötigte Zeichen oder Sonderzeichen
- Benutzerseitiges Anzeigen der gespeicherten Kennwörter
- Anzahl der Anmeldeversuche

- Parameter für den Ablauf der Kennwörter
- Kennwortverlauf und Ausnahmen

Überlegungen zu Kennwortrichtlinien

Beachten Sie vor der Erstellung von Kennwortrichtlinien Folgendes:

- Denken Sie bei den Überlegungen zu den Sicherheitsanforderungen immer auch an die Benutzerfreundlichkeit. Zu restriktive Kennwörter können von den Benutzern möglicherweise zu schwer erstellt, implementiert oder behalten werden.
- Da Single Sign-On inhärent sicher ist, definiert die Standardrichtlinie das Mindestmaß an Kennwortsicherheit, das von Citrix zur Sicherung der meisten Anwendungen mit aktiviertem Single Sign-On empfohlen wird. Diese Einstellungen können Sie gemäß den im Unternehmen geltenden Richtlinien und Vorschriften ändern.
- Da Single Sign-On die Standardrichtlinie auf vom Benutzer hinzugefügte Anwendungen anwendet, sollte die Standardrichtlinie so weit wie möglich gefasst werden, damit Kennwörter für Anwendungen angenommen werden, für die die Benutzer Kennwörter speichern dürfen.
- Für den Fall eines Kennwortwechsels durch den Benutzer kann die Benutzerkonfiguration in Single Sign-On so eingestellt werden, dass Single Sign-On das alte Kennwort mit dem neuen vergleicht. Dies verhindert, dass Benutzer identische Kennwörter für dieselbe Anwendung zweimal hintereinander verwenden.
- Manchmal haben Benutzer ein Kennwort, das für mehrere Anwendungen verwendet wird (z. B. bei einer Produktsuite). Dies wird als gemeinsame Kennwortverwendung bezeichnet. Dabei wird dieselbe Authentifizierungsstelle für die Anwendungen verwendet.
  Die anderen Anmeldeinformationen für diese Anwendungen (z. B. Benutzername und benutzerdefinierte Felder) können unterschiedlich sein, das Kennwort des Benutzers ist jedoch gleich. Erstellen Sie in diesem Fall eine Anwendungsgruppe, die eine Kennwortgruppe ist. So stellen Sie sicher, dass die Plug-in-Software das Kennwort für alle Anwendungen in der Gruppe als Einheit verwaltet. Bei der Änderung des Kennworts in einer Anwendung stellt die Plug-in-Software sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe widergespiegelt wird.

- Domänenkennwortgruppen unterscheiden sich von anderen Kennwortgruppen, da das Domänenkennwort des Benutzers als primäres Kennwort für die Anwendungsgruppe verwendet wird. Wenn der Benutzer das Domänenkennwort ändert, stellt die Plug-in-Software sicher, dass die Änderung in den Anmeldeinformationen für alle anderen Anwendungen in der Gruppe widergespiegelt wird. Es kann nur das Domänenkennwort geändert werden. Benutzer können nur dann Kennwortänderungen für eine der anderen Anwendungen in der Gruppe vornehmen, wenn der Administrator die Anwendung aus der Domänenkennwortgruppe entfernt.

Anwendungsdefinitionen

Oct 05, 2015

Als Administrator von Single Sign-On können Sie für jede Anwendung, die Single Sign-On für die Benutzer verwalten soll, eine Anwendungsdefinition erstellen bzw. eine Anwendungsdefinitionsvorlage ändern. Sie können Anwendungsdefinitionen mit der Konsole oder mit dem eigenständigen Anwendungsdefinitionstool erstellen, das auf Arbeitsstationen ohne Konsole installiert werden kann.

Sie können auch zulassen, dass Benutzer in Single Sign-On die ermittelten Anmeldeinformationen für alle clientseitigen Anwendungen anhand der Einstellungen in den Benutzerkonfigurationen hinzufügen können. Die Plug-in-Software kann bei den meisten Anwendungen Anmeldeänderungen erkennen und darauf reagieren, darunter bei den folgenden Anwendungstypen:

Anwendungstypen	Beschreibung
Windows	32-Bit-Windows-Anwendungen (einschließlich Java-Anwendungen), z. B. Microsoft Outlook, Lotus Notes, SAP oder jede andere kennwortaktivierte Windows-Anwendung.
Web-	Webanwendungen (einschließlich Java-Applets und SAP), auf die über Microsoft Internet Explorer zugegriffen wird.
Terminalemulator	Anwendungen, auf die Sie über einen HLLAPI-kompatiblen Terminalemulator zugreifen. (Single Sign-On unterstützt keine 64-Bit-Terminalemulatorsoftware.)

Die Plug-in-Software reagiert entsprechend der Anwendungsdefinitionen, die Sie selbst erstellen oder von bestehenden Anwendungsdefinitionsvorlagen kopieren. Anwendungsdefinitionen haben die folgenden Funktionen:

- Sie ermöglichen es der Plug-in-Software, Anwendungen und die von den Anwendungen für die Verarbeitung der Anmeldeinformationen des Benutzers verwendeten Formulare zu erkennen und darauf zu reagieren.
- Sie enthalten eine Reihe von Kennungen zum Festlegen von Parametern, mit denen die Plug-in-Software Anwendungen erkennt und darauf reagiert.

In jeder Definition erstellen Sie Anmeldeformulare und mit Kennwörtern verbundene Formulare, die erforderlich sind, um den Zugriff auf die Anwendung zu aktivieren. Wenn Sie eine Anwendung öffnen, helfen Ihnen die Assistenten für Anwendungsdefinitionen beim Erstellen der Definition. Über die Fensterzuordnungsfunktion von Single Sign-On erkennen die Assistenten die Formulare und Felder der meisten Anwendungen.

Tipp: Single Sign-On bietet Standardanwendungsdefinitionsvorlagen für verschiedene Anwendungen bzw. Anwendungsfeatures von Citrix. Weitere Vorlagen finden Sie auf der Citrix Support-Website.

Smartcards

Oct 05, 2015

Citrix hat Smartcards getestet, die der ISO-Norm 7816 (International Organization for Standardization) entsprechen. Diese Karten haben elektrische Kontakte (werden auch als Kontaktkarten bezeichnet), die über einen Smartcardleser eine Schnittstelle zum Computersystem herstellen. Das Lesegerät kann über einen seriellen, einen USB- oder einen PC-Karten-Port (PCMCIA) am Computer angeschlossen sein.

Citrix unterstützt die Verwendung von PC/SC-basierten kryptographischen Smartcards. Diese Karten bieten eine Unterstützung für kryptographische Funktionen, wie beispielsweise digitale Signaturen und Verschlüsselung. Kryptographische Karten eignen sich für die sichere Speicherung privater Schlüssel, wie etwa in PKI-Sicherheitssystemen (Public Key Infrastructure).

Die eigentlichen kryptographischen Vorgänge finden auf der Smartcard selbst statt, sodass der private Schlüssel nie die Karte verlässt. Außerdem bieten Smartcards Zweifaktorauthentifizierung für erhöhte Sicherheit: die Karte und die PIN-Nummer des Benutzers. Wenn diese Elemente zusammen verwendet werden, beweisen sie, dass der Karteninhaber der rechtmäßige Eigentümer der Smartcard ist.

Softwareanforderungen für Smartcards

Welche Voraussetzungen im Hinblick auf die Konfiguration für Ihre spezielle Smartcard-Implementierung zu erfüllen sind, erfahren Sie im Smartcard-Fachhandel. Auf dem Server oder Client werden folgende Komponenten benötigt:

- PC/SC-Software
- CSP-Software (Cryptographic Service Provider)
- Softwaretreiber für den Smartcardleser

Unter Umständen sind auf den Windows Server- und Clientbetriebssystemen bereits PC/SC, CSP oder Treiber für einen Smartcardleser installiert bzw.verfügbar. Ob diese Softwarekomponenten unterstützt werden oder durch eine herstellerspezifische Software ersetzt werden müssen, erfahren Sie im Smartcard-Fachhandel.

Wenn Sie Smartcards in einer Windows Server 2008- oder Windows Vista-Umgebung verwenden möchten, muss der zentrale Speicher mit einer Single Sign-On Console (früher Password Manager Console) der Version 4.5 oder höher erstellt oder aktualisiert werden; außerdem müssen Sie Microsoft Data Protection API (erfordert servergespeicherte Profile) in den Benutzerkonfigurationen wählen.

Vorschreiben der Identitätsprüfung

Oct 05, 2015

Je nach den Einstellungen in der Benutzerkonfiguration sollten Sie jedoch die Identität der Benutzer in den folgenden Fällen prüfen:

- Benutzer ändern die Authentifizierungstypen, beispielsweise wechselt ein Benutzer zwischen der Authentifizierung mit Smartcard und mit Kennwort. (Sie können eine Benutzerkonfiguration erstellen, die nur beim Wechsel zwischen Authentifizierungstypen eine anfängliche Prüfung erfordert.)
- Der Administrator ändert das primäre Kennwort eines Benutzers.
- Benutzer setzen das primäre Kennwort mit dem Konto-Self-Service zurück.
- Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.
- Benutzer ändern das primäre Kennwort auf einem Computer, auf dem die Plug-in-Software nicht installiert ist, und melden sich dann an einem Gerät an, auf dem die Plug-in-Software installiert ist.

Single Sign-On kann so konfiguriert werden, dass die Identität des Benutzers geprüft wird, um so sicherzustellen, dass der Benutzer zur Verwendung von Single Sign-On berechtigt ist. Sie können eine der beiden folgenden Identitätsprüfungsmethoden auswählen:

Methode	Beschreibung
Altes Kennwort	Bei dieser Methode bestätigen Benutzer ihre Identität durch Eingabe des alten primären Kennwortes.
Sicherheitsfragen (auch fragenbasierte Authentifizierung genannt)	Bei dieser Methode erstellen Sie einen Fragenkatalog, der beliebig viele Fragen und Fragengruppen enthält, die Sie den Benutzern bereitstellen möchten. Sie können die von Single Sign-On bereitgestellten Standardfragen verwenden oder eigene Fragen erstellen.

Achtung: Wenn Benutzern nur das alte Kennwort als Methode zur Identitätsprüfung zur Verfügung steht, werden Benutzer ausgesperrt, die das alte primäre Kennwort vergessen. Der Administrator muss dann in der Single Sign-On-Komponente die Aufgabe zum Zurücksetzen der Benutzerdaten ausführen, damit sich die Benutzer wieder registrieren können. Möglicherweise muss der Administrator auch die Kennwörter in den Anwendungen des Benutzers zurücksetzen.

Prüfen der Benutzeridentität mit Sicherheitsfragen (fragenbasierte Authentifizierung)

Single Sign-On ermöglicht die fragenbasierte Authentifizierung zur Prüfung der Identität des Benutzers. Single Sign-On stellt vier Fragen (in Englisch, Französisch, Deutsch, Japanisch und Spanisch) zur Verfügung, die Sie für diese Zwecke verwenden können.

Sie können die fragenbasierte Authentifizierung in den folgenden Fällen verwenden:

- Als Teil der benutzerseitigen Sicherheitsfragenregistrierung bei der Erstverwendung der Plug-in-Software.
- Nach der Registrierung, wenn Sie das Konto-Self-Service-Feature so konfiguriert haben, dass Benutzer die primären Anmeldeinformationen ändern oder die Sperrung der Konten aufheben können.

Wenn ein Benutzer sein primäres Kennwort ändert, können Sie die Identität des Benutzers bestätigen, indem der Benutzer die Sicherheitsfragen im Fragenkatalog beantwortet, den Sie erstellen. Dieser Fragenkatalog wird beim ersten Starten der Plug-in-Software angezeigt. Benutzer beantworten die erforderliche Anzahl der Sicherheitsfragen und werden bei

bestimmten Kennwortänderungsereignissen ggf. zur erneuten Eingabe dieser Informationen aufgefordert.

Damit Benutzer die Antworten auf die Sicherheitsfragen neu registrieren können, geben Sie ihnen Zugriff auf QBAEnroll.exe als veröffentlichte Anwendung.

Wenn Sie keine Sicherheitsfragen einrichten, werden die Benutzer aufgefordert, das alte Kennwort anzugeben, wenn sie sich das erste Mal anmelden oder das primäre Kennwort ändern. Sie können Password Manager auch so konfigurieren, dass Benutzer die bevorzugte Authentifizierungsmethode (altes Kennwort oder Sicherheitsfragen) selbst auswählen können.

Automatisches Wiederherstellen oder Entsperren der Anmeldeinformationen des Benutzers

Wichtig: Die automatische Schlüsselverwaltung ist nicht so sicher wie andere Methoden zur Schlüsselwiederherstellung, z. B. Sicherheitsfragen und altes Kennwort.
Sie können Single Sign-On so konfigurieren, dass die Identitätsprüfung umgangen wird und die Anmeldeinformationen des Benutzers (d. h. die den Benutzerdaten zugeordneten Verschlüsselungsschlüssel) automatisch wiederhergestellt werden. Hierfür müssen Sie den Single Sign-On-Dienst installieren und das Schlüsselverwaltungsmodul verwenden.

Der Arbeitsablauf für die automatische Schlüsselverwaltung sieht im Wesentlichen wie folgt aus:

1. Installieren Sie den Single Sign-On-Dienst mit dem Schlüsselverwaltungsmodul.
2. Erstellen oder bearbeiten Sie die Benutzerkonfigurationen und wählen Sie die Schlüsselwiederherstellungsmethode, die die automatische Schlüsselverwaltung ohne Identitätsprüfung ermöglicht. Diese Option ist als Teil der Eigenschaften "Sekundäre Datenschutzmethode" in der Benutzerkonfiguration verfügbar.

Planen der Benutzerkonfigurationen für das Single Sign-On Plug-in

Oct 05, 2015

Eine Benutzerkonfiguration ist eine einmalige Sammlung von Einstellungen, Kennwortrichtlinien und Anwendungen, die Sie auf Benutzer anwenden, die einer Active Directory-Hierarchie (Organisationseinheit oder einzelner Benutzer) oder einer Active Directory-Gruppe zugeordnet sind (Ausnahme: Verteilergruppen und lokale Gruppen der Domäne im gemischten Modus von Active Directory, welche nicht unterstützt werden). Mit Benutzerkonfigurationen können Sie das Verhalten und die Darstellung der Plug-In-Software für Benutzer steuern.

Benutzerkonfigurationen legen unter anderem die Benutzerinformationen, Anwendungsdefinitionen, Kennwortrichtlinien und Methoden zur Identitätsprüfung fest. Darüber hinaus müssen Sie in jeder Benutzerkonfiguration Lizenzierungsinformationen (Lizenzserver und Lizenztyp) angeben. Aus diesem Grund können die Benutzer die Plug-in-Software erst dann verwenden, wenn Sie die entsprechenden Benutzerkonfigurationen erstellt haben.

Vor dem Erstellen von Benutzerkonfigurationen müssen Sie Folgendes erstellt bzw. definiert haben:

- Zentraler Speicher
- Dienstmodule (optional)
- Anwendungsdefinitionen
- Kennwortrichtlinien
- Sicherheitsfragen (optional)

Benutzerkonfigurationen enthalten die folgenden Elemente:

- Benutzer, die einer Active Directory-Domänenhierarchie (Organisationseinheit oder einzelner Benutzer) oder einer Gruppe zugeordnet sind.
- Datenschutzmethoden.
- Erstellte Anwendungsdefinitionen, die Sie bei der Erstellung einer Benutzerkonfiguration in einer Anwendungsgruppe zusammenfassen können.
- Kennwortrichtlinien, die für bestimmte Anwendungsgruppen gelten. (Beim Erstellen einer Benutzerkonfiguration können Sie Anwendungsgruppen erstellen, die Sie einer Benutzerkonfiguration zuordnen. Sie können auch nach dem Erstellen einer Benutzerkonfiguration eine Anwendungsgruppe hinzufügen.)
- Self-Service-Features (Entsperren des Kontos und Zurücksetzen des Kennworts) und Schlüsselverwaltungsoptionen (Verwenden von alten Kennwörtern, Sicherheitsfragen, die Sie für die Benutzer erstellen, und automatische Schlüsselverwaltung).
- Einstellungen für Optionen, wie z. B. Hotdesktop, Provisioning von Anmeldeinformationen und Anwendungssupport.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

Berücksichtigen Sie bei der Planung der Benutzerumgebung für das Single Sign-On Plug-in Folgendes:

- Wenn Sie dieselben Einstellungen der Benutzerkonfiguration auf eine andere Benutzergruppe anwenden müssen, duplizieren Sie die Benutzerkonfiguration in der Konsole und nehmen Sie die entsprechenden Einstellungsänderungen vor.
- Die Organisation der Single Sign-On-Benutzerumgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Das heißt, dass Benutzerkonfigurationen in der Single Sign-On-Umgebung einer Active Directory-Hierarchie (OU oder Benutzer) oder einer Active Directory-Gruppe zugeordnet werden. Wenn Sie sowohl Hierarchien als auch

Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.

- Die Benutzerkonfigurationsdaten im zentralen Speicher haben Vorrang vor denen im lokalen Speicher (d. h. den Benutzerdaten, die auf dem Computer eines Benutzers gespeichert sind). Die Benutzerdaten im lokalen Speicher werden in der Regel dann verwendet, wenn der zentrale Speicher nicht verfügbar oder offline ist.

Gemeinsames Verwenden von Ressourcen oder Arbeitsstationen durch mehrere Benutzer (Hotdesktop)

Oct 05, 2015

Mit dem Hotdesktop-Feature können Benutzer Arbeitsstationen effizient und sicher gemeinsam verwenden. Hotdesktop bietet ein bequemes und schnelles Wechseln der Benutzer und Single Sign-On-Funktionalität durch Single Sign-On.

Bevor Sie Hotdesktop implementieren können, müssen Sie folgende Schritte ausführen:

- Erstellen von Hotdesktop-relevanten Konfigurationen.
- Konfigurieren eines Hotdesktop-Kontos.
- Bearbeiten der Skripte, mit denen definiert wird, welche Anwendungen auf den Hotdesktop-Geräten ausgeführt werden und wie sich diese beim Starten und Beenden verhalten.

Das Hotdesktop-Feature wird nicht standardmäßig installiert. Sie können das Feature bei der Installation der Plug-in-Software auswählen. Bestehende Bereitstellungen können auch für die Verwendung von Hotdesktop aktualisiert werden.

Wenn Sie Hotdesktop in einer Umgebung bereitstellen, in der sich Benutzer mit Smartcards anmelden und die ausgewählte Smartcardschlüsselquelle DPAPI mit Profil ist, wählen Sie für diese Benutzer nicht Benutzer zur Eingabe des alten Kennworts auffordern als einzige Schlüsselwiederherstellung für diese Benutzer. Benutzer in solchen Umgebungen können nicht das richtige alte Kennwort eingeben und würden somit unwiderruflich aus dem System ausgeschlossen. Wählen Sie zur Vermeidung dieses Problems die Option zur automatischen Schlüsselverwaltung aus oder stellen Sie die fragenbasierte Authentifizierung als eine Option zur Verfügung.

Anwendungssteuerung mit Hotdesktop

Mit Hotdesktop werden Benutzer schnell mit den Windows-Anmeldeinformationen oder einer starken Smartcard-Authentifizierungsmethode authentifiziert. Als Administrator können Sie Hotdesktop so konfigurieren, dass Anwendungen in der Hotdesktop-Umgebung gestartet werden, damit Benutzer nicht die Anwendungen suchen und auf den Anwendungsstart warten müssen.

Darüber hinaus können Sie Hotdesktop so konfigurieren, dass alle Anwendungen richtig beendet werden und die nächste Benutzersitzung in einer sauberen Umgebung gestartet wird.

Benutzererfahrung bei Hotdesktop

Bei der Anmeldung des Hotdesktop-Kontos wird das Gerät in einen Modus für die schnelle Benutzerumschaltung gesetzt, der die Anzeige einer standardmäßigen Windows-Authentifizierungsaufforderung auslöst. Das Hotdesktop-Konto bleibt unabhängig von der Aktivität des Hotdesktop-Benutzers angemeldet.

Wenn sich Benutzer authentifizieren, melden sie sich an Hotdesktop nicht im traditionellen Sinne an. Hotdesktop startet mit den Windows-Anmeldeinformationen der Benutzer eine Hotdesktop-Sitzung. Da Benutzer nicht richtig angemeldet sondern nur authentifiziert sind, treten die zeitintensiven Ereignisse nicht auf, die normalerweise mit der Anmeldung verbunden sind, z. B. Anwenden der Gruppenrichtlinie, Initialisierung des Druckers usw. Dies führt dazu, dass Benutzer bei der Ausführung von Hotdesktop eine schnelle Benutzerumschaltung wahrnehmen. Ein Benutzer kann eine Sitzung starten, alle berufsbezogenen Aufgaben ausführen, und die Sitzung beenden, damit sich der nächste Benutzer am System anmelden und Aufgaben durchführen kann. Das Umschalten von Benutzer zu Benutzer erfolgt schnell und mühelos.

Die Single Sign-On Plug-in-Software wird beim Start der Hotdesktop-Sitzung gestartet. Nach dem Herstellen der Sitzung greift Hotdesktop auf die Windows-Anmeldeinformationen des Benutzers zu und startet Anwendungen in der normalen Benutzeroberfläche. Diese Clientanwendungen fordern die Benutzer normalerweise zur Eingabe der Anmeldeinformationen auf, die vom Plug-in gesendet werden können. Die Plug-in-Software verwendet die Einstellungen, die dem Windows-Konto zugeordnet sind.

Planen optionaler Single Sign-On-Dienst-Features

Oct 05, 2015

Der Single Sign-On-Dienst ist ein Webdienst, der die Daten, die vom Single Sign-On-Dienst, der Konsole und der Plug-In-Software verwendet werden, mit SSL (Secure Sockets Layers) verschlüsselt. Der Dienst verwendet einen dedizierten Webserver als Host für die optionalen Features von Single Sign-On.

Installieren Sie den Single Sign-On-Dienst, wenn Sie mindestens eines der folgenden Module implementieren möchten:

- Schlüsselverwaltung
- Datenintegrität
- Provisioning
- Self-Service
- Synchronisierung der Anmeldeinfo

Wichtig: Der Server mit dem Single Sign-On-Dienst enthält sehr vertrauliche Benutzerdaten. Sie sollten einen dedizierten Server verwenden, der an einem physisch sicheren Standort installiert ist.

Schlüsselverwaltung

Mit der Schlüsselverwaltung können sich Benutzer am Netzwerk anmelden und sofort auf Anwendungen zugreifen, die von Single Sign-On verwaltet werden; das Prüfen der Identität mit der fragenbasierten Authentifizierung (auch automatische Schlüsselverwaltung genannt) entfällt. Die automatische Schlüsselverwaltung verwendet die Schlüsselaufteilung (das Aufteilen eines privaten Schlüssels in zwei Teile), um Sicherheitsrisiken zu verringern.

Allerdings schützt die automatische Schlüsselverwaltung nicht vor einem unbefugten Benutzer oder Administrator, der die Identität eines Benutzers annimmt, da es kein nur dem Benutzer bekanntes Geheimnis gibt, mit dem das Netzwerkkennwort des Benutzers geschützt wird. Um dieses potenzielle Problem zu vermeiden, sollten Sie die automatische Schlüsselverwaltung zusammen mit dem Konto-Self-Service-Modul und der fragenbasierten Authentifizierung implementieren.
Wichtig: Abhängig von der Sicherheitsrichtlinie der Organisation können Systemadministratoren auf Kennwörter für von Single Sign-On verwaltete Anwendungen zugreifen. Überprüfen Sie die Sicherheitsrichtlinie der Organisation, bevor Sie Single Sign-On die Handhabung von Kennwörtern erlauben, die Benutzer eigentlich vollständig vertraulich halten möchten. Das Deaktivieren von automatischen Schlüsselverwaltungsfeatures in der Einstellung Datenschutzmethoden der Benutzerkonfiguration kann ebenfalls zur Vermeidung von nicht autorisierten Zugriffen beitragen.

Datenintegrität

Das Modul "Datenintegrität" enthält die Dateien mit den öffentlichen und privaten Schlüsseln, die für das Signieren von Daten verwendet werden. Das Modul verwendet Kryptografie mit öffentlichem Schlüssel per RSA, um sicherzustellen, dass die Plug-in-Software nur Konfigurationsdaten erhält, die von einer autorisierten Quelle stammen. Das Modul "Datenintegrität" verteilt nie den privaten Schlüssel.

Nach der Signatur der Daten sendet die Konsole die Daten und die Signatur an den zentralen Speicher. Bei der Synchronisierung erhält die Plug-in-Software die Daten und die Signatur vom zentralen Speicher. Die Plug-in-Software kontaktiert dann den Single Sign-On-Dienst, um eine Kopie des öffentlichen Schlüssels zu erhalten, der zur Prüfung der Signatur benötigt wird, die vom zentralen Speicher empfangen wurde.

Installieren Sie das Modul "Datenintegrität", wenn Sie sicherstellen möchten, dass die in den Komponenten von Single Sign-On übertragenen Daten von einer sicheren und autorisierten Quelle stammen. Dieses Modul ist optional und für Benutzer gedacht, die keine vertrauenswürdigen Netzwerke haben.

Wenn die Plug-in-Software für die Verwendung des Moduls "Datenintegrität" konfiguriert ist, werden alle Daten abgelehnt, die die Prüfung der Datenintegrität nicht bestanden haben. Wenn eine Prüfung fehlschlägt, protokolliert die Plug-in-Software das Ereignis und zeigt den Benutzern eine Fehlermeldung an, in der sie aufgefordert werden, sich an den Administrator zu wenden. Die Plug-in-Software verwendet dann standardmäßig vorherige Konfigurationen oder kehrt in einen Offlinestatus zurück.

Wenn Sie bereits einen Sicherheitsrahmen implementiert haben, mit dem die gesendeten Daten geschützt werden, z. B. IPsec (Internet Protocol Security) oder SMB-Signatur (Server Message Block), brauchen Sie das Modul "Datenintegrität" nicht zu installieren.

Provisioning

Mit dem Provisioning (auch Provisioning der Anmeldeinformationen genannt) können Sie bestimmte Prozesse für das Verwalten von Anmeldeinformationen automatisieren. Sie haben folgende Möglichkeiten:

- Hinzufügen, Ändern und Löschen von Anmeldeinformationen im zentralen Speicher
- Zurücksetzen der Anmeldeinformationen der Benutzer
- Entfernen von Benutzern und ihren Anwendungsanmeldeinformationen von Single Sign-On

Das Provisioning von Anmeldeinformationen wird erreicht, wenn Sie mit den Informationen über die Umgebung eine Vorlage erstellen, mit der Sie Anmeldeinformationen im zentralen Speicher hinzufügen, entfernen oder ändern können.

Self-Service

Sie können in den Self-Service-Features von Single Sign-On konfigurieren, dass Benutzer ohne Beteiligung des Administrators oder des Helpdeskpersonals das primäre Kennwort zurücksetzen oder die Windows-Domänenkonten entsperren können. Je nach Bedarf können Sie eine oder beide Konto-Self-Service-Features (Kennwort zurücksetzen und Kontosperrung aufheben) sicher in der Single Sign-On-Umgebung implementieren.
Hinweis: Sie können den Konto-Self-Service nur in einer Active Directory-Umgebung verwenden, um die benutzerseitige Zurücksetzung des primären Kennwortes sowie die Aufhebung der Sperrung der Windows-Domänenkonten zu ermöglichen. Diese Kontofunktionen werden durch die fragenbasierte Authentifizierung geschützt. So wird sichergestellt, dass Benutzer zum Zurücksetzen der Kennwörter oder Aufheben der Kontosperrung berechtigt sind. Wenn Benutzer den Konto-Self-Service aktivieren, müssen sie sich registrieren und die Sicherheitsfragen beantworten, die Sie erstellt und ausgewählt haben. Diese Sicherheitsfragen werden den Benutzern angezeigt, wenn sie das Kennwort zurücksetzen oder das Konto entsperren möchten. Werden die Fragen richtig beantwortet, können die Benutzer die Kennwörter zurücksetzen oder die Kontosperrung aufheben.

Synchronisierung der Anmeldeinfo

Mit der Synchronisierung der Anmeldeinformationen (auch Kontozuordnung genannt) kann sich ein Benutzer mit jedem Windows-Konto an jeder Anwendung anmelden. Da Single Sign-On normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert. Administratoren können jedoch die Kontozuordnung konfigurieren und die Anmeldeinformationen des Benutzers synchronisieren. Benutzer mit konfigurierter Kontozuordnung können mit allen Konten in der Single Sign-On-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Bereitstellungsszenarios für die Single Sign-On Plug-In-Software

Oct 05, 2015

Sie können Single Sign-On in Umgebungen mit gehosteten XenApp-Anwendungen, lokal installierten Anwendungen oder beiden verwenden.

In einer XenApp-Bereitstellung installieren Sie die Single Sign-On Plug-In-Software auf jedem Server in der XenApp-Farm, die Anwendungen hostet, für die eine Authentifizierung der Anmeldeinformationen erforderlich ist. Benutzer greifen über Citrix Verbindungen auf diese Anwendungen zu. Die Plug-In-Software auf dem Server stellt den Anwendungstyp fest (Windows, Web oder Terminalemulator) und ruft die entsprechenden Anmeldeinformationen von dem im Benutzerprofil gespeicherten lokalen Speicher der Anmeldeinformationen ab.

Sie können das Single Sign-On Plug-In auch auf jedem Benutzergerät installieren. Für eine XenApp-Bereitstellung lesen Sie bitte die unten beschriebenen Überlegungen. Wenn Benutzer Anwendungen ausführen, die lokal auf den Geräten installiert ist, muss das Single Sign-On Plug-In auf dem Benutzergerät installiert sein, um die Anmeldeinformationen bereitzustellen und den Zugriff auf lokale Anwendungen zu ermöglichen.

Unabhängig davon, ob das Single Sign-On Plug-auf dem Benutzergerät installiert ist, können Benutzer die Antworten auf die Sicherheitsfragen ohne Aufforderung neu registrieren oder die Anmeldeinformationen mit der Kontozuordnung synchronisieren, wenn sie veröffentlichte Anwendungen verwenden, zu denen Sie ihnen Zugriff geben, nachdem das Plug-in auf einem XenApp-Server installiert wird.

Single Sign-On kann mit Folgendem verwendet werden:

- Access Gateway Advanced Edition (Anwendungen stehen von XenApp über einen Webbrowser zur Verfügung)
- Citrix XenApp-Features:
  - Citrix Receiver für Windows
  - Citrix Offline Plug-in
  - Webinterface

Bereitstellen des Single Sign-On Plug-ins auf Benutzergeräten in einer XenApp-Umgebung

Die Entscheidung, ob das Single Sign-On Plug-in auf dem Benutzergerät installiert wird oder ob es veröffentlicht wird, hängt davon ab, was Benutzer tun können. In allen Fällen werden Anmeldeinformationen an veröffentlichte Anwendungen gesendet.

- Wenn Sie das Single Sign-On Plug-in nicht auf dem Benutzergerät installieren, können Benutzer Folgendes tun:
  - Registrieren der Antworten auf Sicherheitsfragen
  - Automatisches Speichern der Anmeldeinformationen, wenn Single Sign-On dazu auffordert
  - Ändern des Kennworts für ein Programm oder eine Website, wenn Single Sign-On dazu auffordert
- Wenn Sie die Anwendung "Kennwörter verwalten" (LogonManager.exe, wird bei der Installation des Single Sign-On Plug-ins installiert) veröffentlichen, können Benutzer Folgendes tun:
  - Registrieren der Antworten auf Sicherheitsfragen
  - Automatisches Speichern der Anmeldeinformationen, wenn Single Sign-On dazu auffordert
  - Ändern des Kennworts für ein Programm oder eine Website, wenn Single Sign-On dazu auffordert
  - Bearbeiten, Löschen oder Anzeigen der in Single Sign-On gespeicherten Kennwörter
- Wenn Sie das Single Sign-On Plug-in auf dem Benutzergerät installieren, können Benutzer alle verfügbaren Single Sign-On-Aufgaben ausführen:

- Registrieren der Antworten auf Sicherheitsfragen
- Automatisches Speichern der Anmeldeinformationen, wenn Single Sign-On dazu auffordert
- Ändern des Kennworts für ein Programm oder eine Website, wenn Single Sign-On dazu auffordert
- Bearbeiten, Löschen oder Anzeigen der in Single Sign-On gespeicherten Kennwörter
- Manuelles Senden von Anmeldeinformationen, wenn Single Sign-On dazu auffordert
- Hinzufügen weiterer Kennwörter für bereits in Single Sign-On gespeicherte Programme und Websites
- Anhalten von Single Sign-On, Fortsetzen von Single Sign-On oder Feststellen, ob Single Sign-On angehalten ist
- Verwenden des Konto-Self-Service

Mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer

Oct 05, 2015

Beim Erstellen oder Bearbeiten einer Benutzerkonfiguration können Sie abhängig von dem im Unternehmen verwendeten Authentifizierungsschema verschiedene Methoden zum Schutz der Anmeldeinformationen des Benutzers auswählen.

Mit den folgenden Eigenschaften-Dialogfeldern der Benutzerkonfiguration optimieren Sie das Verhalten der Single Sign-On Plug-in-Software und passen die Methode zum Schutz der Anmeldeinformationen an, wenn Benutzer eine oder mehrere primäre Authentifizierungsmethoden implementieren.

Seite "Datenschutzmethoden"

Im Eigenschaften-Dialogfeld für die Benutzerkonfiguration Datenschutzmethoden können Sie als Datenschutzmethode eine oder mehrere primäre Authentifizierungsmethoden auswählen. Darüber hinaus können Sie auch den Administratorzugriff auf die Anmeldeinformationen des Benutzers steuern, um zu verhindern, dass Administratoren die Identität eines Benutzers annehmen und unberechtigt auf Benutzerdaten zugreifen.

Seite "Sekundäre Datenschutzmethode"

Wenn Benutzer die primäre Authentifizierung ändern (z. B. ein Domänenkennwort ändern oder eine Smartcard ersetzen), können Sie zum Erhöhen der Sicherheit im Eigenschaften-Dialogfeld der Benutzerkonfiguration eine Sekundäre Datenschutzmethode festlegen, dass sich die Benutzer neu authentifizieren und einer Identitätsprüfung unterziehen müssen, bevor die Sperrung der Anwendungsanmeldeinformationen aufgehoben wird.

Sicherheit und Benutzerfreundlichkeit

Um zu entscheiden, welche Optionen Sie in den beiden Dialogfeldern für diese Benutzerkonfigurationseigenschaften auswählen, stellen Sie sich die folgenden beiden Fragen:

- Welche Authentifizierungstypen werden in der Umgebung für die Benutzer verwendet, die Sie mit dieser Benutzerkonfiguration verwalten?
- Wie können die Sicherheitsanforderungen des Unternehmens und eine umfassende Benutzerfreundlichkeit miteinander in Einklang gebracht werden?

Bedenken Sie auch, dass die folgenden Optionen sich nicht gegenseitig ausschließen und Sie verschiedene Möglichkeiten im Unternehmen miteinander kombinieren können (mehrere primäre Authentifizierungsmethoden). Ihre Entscheidung hängt letztendlich davon ab, wie stark Sie die Sicherheit der Benutzer im Unternehmen gegenüber der Benutzerfreundlichkeit gewichten.

Annahme der Identität des Benutzers

Wenn Sie den Zugriff des Administrators auf die Anmeldeinformationen des Benutzers unterbinden möchten, wählen Sie Ja für die Option Möchten Sie den Administratorkontozugriff auf Benutzerdaten beschränken? . Die Anmeldeinformationen sind nun vor Administratoren geschützt, die die Identität eines Benutzers annehmen und auf Benutzerdaten zugreifen möchten.

Ja ist die Standardeinstellung für die Seite Datenschutzmethoden. Mit dieser Konfiguration haben Administratoren, wie z. B.

der Kontoadministrator, keinen Zugriff auf die Benutzerkennwörter oder die Benutzerdaten. Damit wird verhindert, dass ein Administrator die Identität eines Benutzers annimmt. Mit dieser Standardeinstellung kann der Administrator sich nicht als Benutzer anmelden und möglicherweise auf Daten zugreifen, die im lokalen Speicher der Anmeldeinformationen des Benutzers gespeichert sind.

Mit der Einstellung Ja wird die Verwendung der Option Microsoft Data Protection API auf dieser Seite und der Option Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt auf der folgenden Seite Sekundäre Datenschutzmethode deaktiviert. Smartcards und servergespeicherte Profile sind in diesem Fall nicht zugelassen, und Anmeldeinformationen werden bei einer Kennwortänderung ohne Authentifizierung oder Identitätsprüfung nicht automatisch wiederhergestellt.

Wählen Sie Nein, wenn Sie die Verwendung aller Features für die mehrfache Authentifizierung auf dieser Seite und der Seite Sekundäre Datenschutzmethode zulassen möchten (einschließlich das automatische Wiederherstellen der Anmeldeinformationen ohne erneute Authentifizierung oder Identitätsprüfung).

Benutzername und Kennwort

Die einfachste Implementierung ist die Standardeinstellung für die Seite Datenschutzmethoden: eine Umgebung nur mit Kennwort. Bei dieser Standardeinstellung verwenden Benutzer einfach den Benutzernamen und das Kennwort zum Schutz der Anmeldeinformationen vor nicht autorisiertem Zugriff durch Administratoren.

Wichtig: Die Sicherheit dieser Methode hängt von der relativen Stärke der Domänenkennwortrichtlinie ab. Je strenger (oder komplexer) die Anforderungen an das Kennwort sind, desto sicherer ist diese Methode.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Siehe *— Annahme der Identität des Benutzers* .
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort. Die Kennwortsicherheit ergibt sich aus dem Domänenkennwort, das der Benutzer eingegeben hat, oder einem einmaligen Kennwort aus Tokens, Proximitykarten oder biometrischen Geräten.

Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer

Verwenden Sie Smartcardzertifikat und Authentifizierungsdaten der Benutzer, wenn Sie im Unternehmen Smartcards mit eingebetteten Zertifikaten oder digitalen Signaturen und Authentifizierungsdaten der Benutzer kombinieren möchten. Die Kombination von Smartcards mit einem Benutzernamen und Kennwort für die Authentifizierung ist die sicherste Methode zum Schutz von Authentifizierungsdaten der Benutzer.

Wählen Sie die Option Smartcardzertifikat, wenn Sie Smartcards mit Hotdesktop verwenden.

Wenn Sie Smartcards in einer Windows Server 2008- oder Windows Vista-Umgebung verwenden möchten, muss der zentrale Speicher mit einer Single Sign-On Console (früher Password Manager Console) der Version 4.5 oder höher erstellt oder aktualisiert werden; außerdem müssen Sie Microsoft Data Protection API (erfordert servergespeicherte Profile) in den Benutzerkonfigurationen wählen.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Siehe *— Annahme der Identität des Benutzers* .
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort. Die Kennwortsicherheit ergibt sich aus dem Domänenkennwort, das der Benutzer eingegeben hat, oder einem einmaligen Kennwort aus Tokens, Proximitykarten oder biometrischen Geräten.
Smartcardzertifikat	Ausgewählt. In diesem Fall ist das nur dem Benutzer bekannte Geheimnis durch die von dem Sicherheitszertifikat der Smartcard bereitgestellte Ver- und Entschlüsselung geschützt.

Smartcards mit PIN-Nummern

Wenn Sie Smartcards verwenden, die keine Sicherheitszertifikate als primäre Authentifizierung in Windows-Domänen unterstützen, oder wenn Sie keine servergespeicherten Profile verwenden, wählen Sie die Option Smartcard-PINs zulassen. Wenn diese Option gewählt wurde, werden die Verschlüsselungsschlüssel für den Schutz der sekundären Anmeldeinformationen aus der PIN-Nummer der Smartcard abgeleitet.

Achten Sie darauf, dass starke PIN-Nummern verwendet werden. In manchen Unternehmen werden als PIN vierstellige Zahlen verwendet; diese bieten einen weniger starken Schutz als beispielsweise längere Kennwörter. Verwenden Sie die Option "PIN-Nummer als Kennwort" nur dann, wenn die PINs sowohl aus Ziffern als auch aus Buchstaben bestehen und eine Mindestlänge von acht Zeichen haben.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Siehe *— Annahme der Identität des Benutzers* .
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um eine persönliche Identifikationsnummer (PIN).
Smartcard-PINs zulassen	Ausgewählt. Die PIN-Nummer der Smartcard wird als das nur dem Benutzer bekannte Geheimnis verwendet, um die Benutzerdaten zu schützen. Verwenden Sie diese Option

Option	Beschreibung
	nur, wenn die Richtlinien des Unternehmens bzw. die Umgebung starke PINs fordern.

Diese Option wird vom Single Sign-On Version 4.1 (vormals Password Manager) Plug-in unterstützt, wenn Sie Datenschutz wie in Single Sign-On 4.1 und vorherigen Versionen verwenden und PIN-Nummer als Kennwort, wenn Sie alte Versionen der Plug-ins verwenden möchten.

Servergespeicherte Profile (Microsoft DPAPI)

Wählen Sie Nein für die Option Möchten Sie den Administratorkontozugriff auf Benutzerdaten beschränken?, um die Verwendung von servergespeicherten Profilen und Microsoft Data Protection API in der Umgebung zu aktivieren. Diese Option ist nach Smartcards mit Zertifikaten und Benutzerauthentifizierungsdaten die nächstsichere Option.

Aktivieren Sie diese Option, wenn Sie servergespeicherte Profile mit einem Kerberos-Netzwerkauthentifizierungsprotokoll für die Benutzer verwenden. Diese Option funktioniert nur, wenn servergespeicherte Profile verfügbar sind. Wenn Sie servergespeicherte Profile auf Arbeitsstationen speichern, müssen Sie diese Option auswählen.

Single Sign-On leitet die Verschlüsselungsschlüssel für den Schutz der sekundären Anmeldeinformationen aus dem primären Kennwort des Benutzers ab. Wenn jedoch ein Benutzer eine Smartcard für die primäre Authentifizierung verwendet, gibt es kein primäres Kennwort. Somit kann es auch nicht verwendet werden. In diesem Fall ist Microsoft Data Protection API die beste Option in Plug-in. Diese Option verwendet die Microsoft DPAPI, um die Verschlüsselungsschlüssel abzuleiten und die sekundären Anmeldeinformationen zu schützen. Diese Verschlüsselungsmethode verwendet die Windows- oder Domänenanmeldeinformationen des Benutzers zum Ermitteln der Verschlüsselungsschlüssel.

Wenn Benutzer mit Kennwörtern auf den Computer und mit einem Kerberos-Netzwerkauthentifizierungsprotokoll auf die XenApp-Server zugreifen, wählen Sie die folgenden Optionen:

- Nein für die Option Möchten Sie den Administratorkontozugriff auf Benutzerdaten beschränken?
- Authentifizierungsdaten der Benutzer
- Microsoft Data Protection API

Mit dieser Methode können Benutzer sich auch mit Anmeldeinformationen und Smartcards anmelden.

Wenn Sie Smartcards in einer Windows Server 2008- oder Windows Vista-Umgebung verwenden möchten, muss der zentrale Speicher mit einer Single Sign-On Console (früher Password Manager Console) der Version 4.5 oder höher erstellt oder aktualisiert werden; außerdem müssen Sie Microsoft Data Protection API (erfordert servergespeicherte Profile) in den Benutzerkonfigurationen wählen.

Diese Methode wird von Version 4.1 des Single Sign-On Plug-ins sowie von den Plattformen Windows XP, Windows 2000 und Windows Server 2003 unterstützt. Wählen Sie Datenschutz wie in Single Sign-On 4.1 und vorherigen Versionen verwenden und DPAPI mit Profil, wenn Sie alte Versionen der Plug-In-Software verwenden möchten.

Leere Kennwörter

Das Zulassen von leeren Kennwörtern sollte als Spezialfall angesehen und nur in Umgebungen mit geringen Sicherheitsanforderungen verwendet werden, die aber extrem benutzerfreundlich sein sollen. Ein denkbares Szenario ist z. B., wenn eine Arbeitsstation in einer Fabrikhalle aufgestellt und von vielen Benutzern verwendet wird. Single Sign-On kann nach wie vor verwendet werden, um den Zugriff auf Anwendungen zu steuern, aber die Anmeldeinformationen der Benutzer für den Zugriff auf die Arbeitsstation enthalten ein leeres Kennwort.

Wichtig: Wenn Sie diese Option nicht auswählen und ein leeres Kennwort in der Umgebung zulässig ist, kann die Plug-In-Software kein nur dem Benutzer bekanntes Geheimnis ermitteln und keine weiteren Datenschutzmaßnahmen mit dem

leeren Kennwort vornehmen.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Siehe *— Annahme der Identität des Benutzers* .
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort.
Schutz mit leeren Kennwörtern zulassen	Ausgewählt. Wenn Sie diese Option auswählen und die Plug-in-Software ein leeres Kennwort bei einem Benutzer entdeckt, wird zum Schutz der Daten ein nur dem Benutzer bekanntes Geheimnis aus der Benutzer-ID ermittelt.

Installieren und Upgrade

Oct 05, 2015

Single Sign-On sollte in der folgenden Reihenfolge installiert werden:

1. Erstellen Sie den zentralen Speicher.
2. Installieren Sie das Citrix AppCenter, das die Single Sign-On-Konsolenkomponente enthält.
3. Installieren Sie den Single Sign-On-Dienst, wenn Sie mindestens eines der folgenden Module verwenden möchten:
   - Schlüsselverwaltung
   - Self-Service
   - Provisioning
   - Synchronisierung der Anmeldeinformationen
   - Datenintegrität
     Wenn Sie das Datenintegritätsmodul später oder nach der Installation von Citrix AppCenter und des Single Sign-On Plug-ins installieren möchten, müssen Sie die Daten im vorhandenen zentralen Speicher digital mit dem Datensignierungstool CtxSignData.exe signieren. (Dieses Tool steht nach der Installation des Moduls "Datenintegrität" zur Verfügung.) Umgekehrt müssen Sie die Signatur der Daten im zentralen Speicher aufheben, wenn Sie das Modul "Datenintegrität" deinstallieren.
4. Wenn Sie nur Anwendungsdefinitionen erstellen möchten, installieren Sie das Anwendungsdefinitionstool auf den Computern in der Umgebung. (Wenn Sie die XenApp-Serverrolle mit den Standardkomponenten installieren, ist das Anwendungsdefinitionstool enthalten.)
5. Installieren Sie das Single Sign-On Plug-in auf jedem Benutzergerät und auf dem XenApp-Server.

Wichtig: Die Server, auf denen der Single Sign-On-Dienst und der zentrale Speicher auf einer NTFS-Freigabe ausgeführt werden, enthalten sehr vertrauliche Benutzerinformationen. Verwenden Sie einen dedizierten Server, der an einem sicheren Standort installiert ist.
Die folgenden Installationen sind nicht empfehlenswert und werden nicht unterstützt:

- Installieren Sie den Dienst und das Plug-in nicht auf demselben Computer.
- Installieren Sie den Dienst und die XenApp-Serverrolle nicht auf demselben Server.
- Installieren Sie Single Sign-On nicht auf einem Domänencontroller. Die Installation des Plug-ins oder Dienstes, der Konsole oder das Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe auf einem Domänencontroller wird nicht unterstützt.

Upgrade auf Single Sign-On 5.0

Sie können die ganze Umgebung auf Single Sign-On Version 5.0 aktualisieren oder ein Upgrade in Phasen durchführen.

Upgrade der ganzen Umgebung

1. Citrix empfiehlt, obwohl es ist keine Voraussetzung ist, dass Sie ein Upgrade auf die aktuelle Version des Lizenzservers durchführen und die benötigten Lizenzen hinzufügen, bevor Sie Single Sign-On aktualisieren.
2. Wenn Sie eines der folgenden Module verwenden, müssen Sie den Single Sign-On-Dienst aktualisieren. Zu diesem Zeitpunkt können Sie auch zusätzliche Module installieren.
   - Schlüsselverwaltung
   - Self-Service
   - Provisioning

- Synchronisierung der Anmeldeinformationen
- Datenintegrität

Hinweis: Wenn Sie das Modul "Datenintegrität" zu einem späteren Zeitpunkt oder nach der Installation der Single Sign-On-Komponente im Citrix AppCenter und des Single Sign-On Plug-Ins installieren, müssen Sie die Daten im vorhandenen zentralen Speicher digital mit dem Datensignaturtool CtxSignData.exe signieren. (Dieses Tool steht nach der Installation des Moduls "Datenintegrität" zur Verfügung.) Umgekehrt müssen Sie die Signatur der Daten im zentralen Speicher aufheben, wenn Sie das Modul "Datenintegrität" deinstallieren.

3. Aktualisieren Sie die Single Sign-On-Komponente im Citrix AppCenter (früher Delivery Services Console) auf den Computern in der Umgebung.
   Hinweis:
   - Sie sollten die gleiche Versionsstufe des Single Sign-On-Dienstes und der Konsolenkomponente verwenden.
   - Beim Upgrade der Konsolenkomponente auf Version 5.0 wird auch der zentrale Speicher von Single Sign-On aktualisiert. Nach dem Upgrade einer Single Sign-On 4.8-Konsole auf Version 5.0 können andere Konsolen der Version 4.8 keine Änderungen am zentralen Speicher vornehmen.
4. Wenn Sie nur Anwendungsdefinitionen erstellen müssen, aktualisieren oder installieren Sie das Anwendungsdefinitionstool auf den Computern in der Umgebung. (Wenn Sie die XenApp-Serverrolle mit den Standardkomponenten installieren, ist das Anwendungsdefinitionstool enthalten.)
5. Führen Sie ein Upgrade des zentralen Speichers von Single Sign-On durch.
   - Zentrale Speicher auf NTFS-Netzwerkfreigabebasis:
     - Sichern Sie den Netzwerkfreigabeordner ab, bevor Sie den zentralen Speicher von Single Sign-On aktualisieren.
     - Wählen Sie den Knoten "Single Sign-On" aus und führen Sie den Assistenten Discovery konfigurieren und durchführen vom Citrix AppCenter aus, um den zentralen Speicher von Single Sign-On zu aktualisieren.
     - Geben Sie im Assistenten den UNC-Pfad der vorhandenen NTFS-Netzwerkfreigabe ein, normalerweise \\Servername\CITRIXSYNC$, wobei Servername der Name des Servers ist, auf dem Sie den zentralen Speicher erstellt haben.
   - Wählen Sie für zentrale Speicher auf Active Directory-Basis den Knoten "Single Sign-On" aus und führen Sie den Assistenten Discovery konfigurieren und durchführen im Citrix AppCenter aus, um den zentralen Speicher von Single Sign-On automatisch zu aktualisieren.
   - Wenn Sie von einer Citrix Password Manager-Version aktualisieren, in der freigegebene Novell Ordner unterstützt werden (z. B. Version 4.6), müssen Sie die Freigabe ggf. absichern und administrative Daten exportieren und importieren, um die Einstellungen weiter zu verwenden, die in diesem Typ des zentralen Speichers konfiguriert sind. Weitere Informationen zum Verschieben von Daten im zentralen Speicher finden Sie in der Administrations- und Installationsdokumentation für Password Manager 4.6. Die Dokumentation steht im Citrix Knowledge Center zur Verfügung.
6. Nach dem Konfigurieren der Single Sign-On-Features im Citrix AppCenter können Sie das Single Sign-On Plug-In auf jedem Benutzergerät in der Umgebung installieren oder aktualisieren.

Upgrade in Phasen

1. Fügen Sie zuerst der vorhandenen Umgebung (Single Sign-On 4.8) Benutzergeräte hinzu, auf denen das Single Sign-On 5.0-Plug-In ausgeführt wird.
2. Führen Sie dann ein Upgrade des Single Sign-On-Dienstes und der Konsole auf Version 5.0 aus.
3. Stellen Sie den restlichen Benutzergeräten dann das Single Sign-On 5.0-Plug-In bereit.

Einrichten der Sicherheit und Konten vor der Installation von Single Sign-On

Oct 05, 2015

Stellen Sie vor der Installation des Single Sign-On-Dienstes sicher, dass die entsprechenden Konten und Komponenten für die Unterstützung des Dienstes verfügbar sind. Da der Dienst HTTP (HTTPS) verwendet, wird ein Serverauthentifizierungszertifikat für die Kommunikation per SSL (Secure Sockets Layer) mit der Konsole und dem Plug-in benötigt.

Abrufen und Installieren eines Serverauthentifizierungszertifikats

Besorgen Sie sich für die SSL-Kommunikation ein Serverauthentifizierungszertifikat bei einer Zertifizierungsstelle (CA) oder laden Sie ein eigenes Zertifikat auf den Server herunter, wenn Sie eine vorhandene PKI (Public Key Infrastructure) verwenden.

Mit dem SSL-Zertifikat können Sie sicherstellen, dass die Datenübertragung vom Dienst zur Konsole und zum Plug-in sicher ist, und dass das Plug-in und die Konsole mit dem richtigen Dienstserver kommunizieren.

- Da dieses Zertifikat für die SSL-Kommunikation verwendet wird, muss der allgemeine Name des Zertifikats mit dem vollqualifizierten Domänennamen des Dienstservers (FQDN) übereinstimmen. Geben Sie eine Mindestschlüssellänge von 1024 an.
- Installieren Sie das Zertifikat im Zertifikatsspeicher des lokalen Computers und erstellen Sie eine entsprechende Vertrauensstellung für die Single Sign-On-Komponente im Citrix AppCenter und für das Plug-in.
- Installieren Sie dieses Zertifikat auf den Computern, auf denen die Single Sign-On-Komponente des Citrix AppCenters, der Single Sign-On-Dienst und das Plug-in ausgeführt werden.
- In einer Umgebung mit Lastausgleich und Clusterdienst können Sie ein Zertifikat für mehrere Dienstserver verwenden, wenn der allgemeine Name des SSL-Zertifikats ein Platzhalterzeichen (in der Regel ein Sternchen) enthält. Verwenden Sie beispielsweise für eine Umgebung, die Server mit den Namen server1.meineFirma.com, server2.meineFirma.com und server3.meineFirma.com umfasst, ein SSL-Zertifikat mit dem allgemeinen Namen server*.meineFirma.com. Sie können in diesem Fall auch ein SSL-Zertifikat mit dem allgemeinen Namen *.meineFirma.com verwenden, wobei der allgemeine Name nicht mit dem vollqualifizierten Namen des Servers übereinstimmt.

Wichtig: Wenn Sie das Zertifikat von einer Zertifizierungsstelle beziehen, die standardmäßig als nicht vertrauenswürdig gilt (z. B. eine im Unternehmen installierte Zertifizierungsstelle), müssen Sie das Stammzertifikat im vertrauenswürdigen Stammzertifikatspeicher des lokalen Computers installieren, um die Vertrauensstellung herzustellen.
Wenn Sie SSL-Fehler feststellen, wird das Serverzertifikat wahrscheinlich nicht als vertrauenswürdig angesehen. Weitere Informationen zum Extrahieren und Bereitstellen von Stammzertifikaten einer Zertifizierungsstelle finden Sie auf der Website von Microsoft.

Die Signatur- und Verifizierungszertifikate, die während der Single Sign-On-Installation erstellt werden, haben nichts mit dem SSL-Zertifikat zu tun.

Für die Dienstmodule erforderliche Konten

Für den Single Sign-On-Dienst können in der Umgebung bis zu drei verschiedene Systemkontotypen zum Lesen und Schreiben von Daten erforderlich sein. Die Anzahl und der Typ der benötigten Konten hängt von den verwendeten Dienstmodulen ab. In der Tabelle sind die Konten aufgeführt, die Sie für jedes Dienstmodul benötigen. Wenn für unterschiedliche Module derselbe Kontotyp benötigt wird, können Sie dasselbe Konto für mehrere Module verwenden bzw.

für jedes Modul eigene benutzerdefinierte Konten angeben.

Modul	Benötigte Konten		
	Dienst	Datenproxy	Self-Service
Datenintegrität	Ja	Nein	Nein
Schlüsselverwaltung	Ja	Ja	Nein
Provisioning	Ja	Ja	Nein
Self-Service	Ja	Ja	Ja
Synchronisierung der Anmeldeinfo	Ja	Nein	Nein

Anforderungen für Dienstkonten

Verwenden Sie auf dem Server mit dem Single Sign-On-Dienst die vorhandenen Konten für den Netzwerkdienst und den lokalen Dienst

In dieser Version von Single Sign-On können keine lokalen Benutzerkonten als Dienstkonto definiert werden. Sie können das integrierte Konto "Lokaler Dienst" angeben.

Wenn Sie ein Domänenkonto als Dienstkonto erstellen, müssen Sie mit dem Dienstprogramm setspn.exe einen Dienstprinzipalnamen für dieses Domänenkonto und den Dienstserver in Active Directory registrieren. Bei Verwendung eines Domänenbenutzerkontos sollte das Konto die Rechte "Als Dienst anmelden" haben. Der Computer, auf dem der Dienst ausgeführt wird, muss für die Delegierung als vertrauenswürdig angesehen werden.

Weitere Informationen zu Dienstprinzipalnamen finden Sie auf der Website von Microsoft.

Anforderungen für Datenproxykonten

Erstellen Sie auf dem Server mit dem Single Sign-On-Dienst ein Domänenadministratorkonto mit den folgenden Einstellungen und verwenden Sie es für die Datenproxykommunikation mit dem Dienst.

Das Konto muss Lese- und Schreibzugriff auf den zentralen Speicher haben. Die Kontoanforderungen hängen vom Typ des zentralen Speichers ab, der implementiert wird.

Typ des zentralen Speichers	Kontobeschreibung
NTFS-Netzwerkfreigabe	Für das Konto gilt: • Konto benötigt Lese- und Schreibzugriff auf den zentralen Speicher. • Konto ist Mitglied der Domäne. Gehen Sie nach dem Erstellen des zentralen Speichers wie folgt vor: • Erteilen Sie dem Konto die Berechtigung "Volle Kontrolle" für die Freigabe CITRIXSYNC$. • Erteilen Sie dem Konto die Berechtigung "Volle Kontrolle" für den Ordner "CITRIXSYNC" und die Unterordner: CentralStoreRoot und People. • Erteilen Sie dem Konto die Berechtigung "Volle Kontrolle" für alle Objekte im Ordner

Typ des zentralen Speichers	Kontobeschreibung
	CITRIXSYNC und den Unterordnern ● Stellen Sie sicher, dass die Gruppe "Authentifizierte Benutzer" Ordner im Ordner "People" erstellen können.
Active Directory	Für das Konto gilt: ● Konto benötigt Lese- und Schreibzugriff auf den zentralen Speicher. ● Es ist Mitglied der Gruppe "Domänenadministratoren".

Anforderungen für Self-Service

Wenn Sie die Features des Moduls "Konto-Self-Service" zum benutzerseitigen Zurücksetzen des Kennworts bzw. zum Entsperren des Kontos verwenden, benötigen Sie ein Konto, das Mitglied der Gruppe "Domänenadministratoren" ist.

Für das Installieren und Verwenden von Single Sign-On benötigte Konten

Der Benutzer, der den Single Sign-On-Dienst installiert und den Assistenten für die Dienstkonfiguration ausführt, muss ein Mitglied der Domäne (ein Domänenbenutzer) sowie ein Mitglied der lokalen Gruppe "Administratoren" auf dem Dienstcomputer sein. (Fügen Sie der lokalen Gruppe "Administratoren" ein Domänenbenutzerkonto hinzu.)

Der Benutzer, der die Single Sign-On-Konsole installiert, eine Discovery und Konfiguration durchführt und die Konsole verwendet, muss ein Domänenadministrator und Mitglied der lokalen Gruppe "Administratoren" auf dem Konsolencomputer sein. Für dieses Benutzerkonto ist Lese- und Schreibzugriff auf den zentralen Speicher erforderlich. Ein Benutzerkonto ohne Administratorrechte kann die Verwaltungsrechte für die Konsolenkomponente und die zugehörigen Funktionen über eine Delegierung bzw. begrenzte Delegierung mit Active Directory erhalten.

Der Benutzer, der das Single Sign-On Plug-in installiert, muss ein Mitglied der Domäne (ein Domänenbenutzer) sowie ein Mitglied der lokalen Gruppe "Administratoren" auf dem Benutzergerät sein. Der Benutzer, der das Plug-in installiert, muss ein Mitglied der Domäne (ein Domänenbenutzer) sowie ein Mitglied der lokalen Gruppe "Administratoren" auf dem Benutzergerät sein. Der Benutzer, der das Plug-in ausführt, muss ein Mitglied der Domäne (ein Domänenbenutzer) sein.

Installieren von Java Runtime Environment

Oct 05, 2015

Single Sign-On unterstützt Java Runtime Environment (JRE), Versionen 1.4.x, 5 (1.5.x) und 6 (1.6.x). Laden Sie die aktuell unterstützte Version von der Sun Microsystems Website (http://java.sun.com) herunter.

Installieren oder Upgrade der JRE nach Installation der Single Sign-On-Komponenten

Wenn Sie die JRE nach der Installation der Single Sign-On-Komponente der Delivery Services Console, des Anwendungsdefinitionstools oder des Plug-Ins installieren oder aktualisieren, ordnen Sie die aktuelle JRE der Single Sign-On-Komponente zu.

1. Navigieren Sie in der Systemsteuerung auf den Bereich "Programme" und wählen Sie die Single Sign-On-Komponente.
2. Klicken Sie auf Ändern.
3. Klicken Sie im Setupdialogfeld auf Reparieren.

Problembehandlung bei Java-bezogenen Fehlermeldungen beim Installieren oder Deinstallieren des Plug-Ins

Unter Umständen wird beim Installieren bzw. Deinstallieren des Plug-Ins die folgende Fehlermeldung angezeigt:

"Citrix Single Sign-On hat erkannt, dass mehrere Java-Softwareprogramme oder Dateien aktuell verwendet werden. Schließen Sie alle Programme und halten Sie alle Java-bezogenen Dienste an, bevor Sie den Vorgang fortsetzen. "

Dieser Fehler tritt meist dann auf, wenn Sie das Plug-In auf einem Computer installieren, auf dem auch ein Webserverdienst, z. B. Apache Tomcat oder Apache HTTP-Server, ausgeführt wird. Die Fehlermeldung kann auch angezeigt werden, wenn Sie das Plug-In auf einem XenApp-Server mit installierter License Management Console installieren.

Gehen Sie in diesem Fall wie folgt vor:

1. Beenden Sie den Dienst.
2. Installieren oder deinstallieren Sie das Plug-In.
3. Starten Sie den Dienst.

Erstellen eines zentralen Speichers

Oct 05, 2015

1. Laden Sie das XenApp-Medium.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Serverkomponenten > Sonstiges > Single Sign-On.
3. Klicken Sie auf Zentraler Speicher.
4. Wählen Sie den Typ des zentralen Speichers: NTFS-Netzwerkfreigabe oder Active Directory.
   - Wenn Sie NTFS-Netzwerkfreigabe wählen, wird der zentrale Speicher als "%SystemDrive%\CITRIXSYNC$" erstellt.
   - Bei Auswahl von Active Directory:
     1. Wählen Sie Schritt 1: Active Directory erweitern. Das Active Directory-Schema wird erweitert.
     2. Wählen Sie Schritt 2: Zentralen Speicher erstellen.
     3. Nachdem Sie den zentralen Speicher erstellt haben, starten Sie den Server neu, auf dem die Single Sign-On-Konsole installiert ist. Andernfalls schlägt die Discovery für den zentralem Speicher fehl.

     Wichtig: Stellen Sie sicher, dass der aktuelle Server zur Active Directory-Domäne gehört und der aktuelle Benutzer ein Mitglied der Gruppe "Schemaadministratoren" und der Gruppe "Domänenadministratoren" ist. Stellen Sie sicher, dass der Active Directory-Schemamaster so konfiguriert ist, dass Updates zulässig sind. Wenn der Server, auf dem Sie das Active Directory-Schema erweitern, kein Domänencontroller ist, müssen Sie auch sicherstellen, dass das Microsoft Windows Dienstprogramm Ldifde.exe vor dem Ausführen dieses Schrittes installiert ist. Sie finden das Dienstprogramm auf dem Windows-Installationsmedium oder auf der Microsoft Website. Sie können den Vorgang nicht abschließen, wenn die Datei "Ldifde.exe" nicht installiert ist.

Installieren der Konsolenkomponente

Oct 05, 2015

Die Single Sign-On-Konsolenkomponente wird mit dem Citrix AppCenter installiert.

Wichtig: Sie können den Assistenten für das Konfigurieren und Durchführen der Discovery nur erfolgreich abschließen und Single Sign-On verwenden, wenn Sie bereits den zentralen Speicher für Single Sign-On erstellt haben.

1. Führen Sie die Schritte für die Installation der XenApp-Serverrolle aus. In der Standardeinstellung ist das AppCenter Teil der Installation.
2. Wählen Sie Discovery konfigurieren und durchführen und folgen Sie den Anweisungen.

Stellen Sie sicher, dass die erforderlichen Microsoft Visual C++ Redistributable Packages und Microsoft Primary Interoperability Assemblies installiert sind, wie unter Systemanforderungen beschrieben.

1. Laden Sie das XenApp-Medium.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Gemeinsame Komponenten > Managementkonsolen. Folgen Sie den Anweisungen.
3. Wählen Sie Discovery konfigurieren und durchführen und folgen Sie den Anweisungen.

Installieren und Konfigurieren der Dienstmodule

Oct 05, 2015

Der Installations- und Konfigurationsarbeitsablauf umfasst Folgendes:

1. Erwerben und installieren Sie ein SSL-Zertifikat auf den Computern, auf denen der Single Sign-On-Dienst, die Konsole und das Plug-in ausgeführt werden.
2. Erstellen Sie den erforderlichen Kontotyp für die zu installierenden Dienstmodule.
3. Installieren Sie die Dienstmodule.
4. Konfigurieren Sie die Dienstmodule.

Bei den folgenden Schritten wird davon ausgegangen, dass das Installationsmedium in den Computer eingelegt ist, auf dem die Single Sign-On-Dienstmodule ausgeführt werden, und dass der XenApp-Autorun-Bildschirm angezeigt wird.

1. Laden Sie das XenApp-Medium.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Serverkomponenten > Sonstiges > Single Sign-On > Single Sign-On-Dienst.
3. Folgen Sie den Anweisungen.

Der Assistent für die Dienstkonfiguration wird nach dem Abschluss der Dienstmodulinstallation gestartet. Sie können den Assistenten später über Start > Alle Programme > Citrix > Single Sign-On > Dienstkonfiguration aufrufen.

Folgen Sie den Anweisungen.

- Seite Dienstkonfiguration:

Verbindungseinstellung	Geben Sie die Portnummer für die Dienstverbindung an; der Standardwert ist 443. Sie können den Dienst an jedem verfügbaren Port auf dem Server ausführen. Wenn Sie später Dienstmodule installieren, müssen Sie die Portnummer verwenden, die bei der Erstinstallation des Dienstes festgelegt wurde. Der Dienst kann nicht an mehreren Ports ausgeführt werden. Wenn Sie den falschen Port angeben, kann dies später zu Fehlermeldungen wie beispielsweise "Fehler bei der Kommunikation bzw. beim Herstellen einer Verbindung zum Single Sign-On-Dienst" führen. Geben Sie die richtige Dienstportnummer an, wenn Sie das Signaturtool für die Datenintegrität an der Befehlszeile verwenden.
SSL-Zertifikat	Wählen Sie das auf dem Dienstcomputer installierte SSL-Zertifikat aus, das für die Kommunikation mit Clientcomputern verwendet wird. Aktivieren Sie das Kontrollkästchen Ausführlichen Namen anzeigen, um die im Zertifikat enthaltenen LDAP-Informationen Connection Setting anzuzeigen.

Name des virtuellen Hosts	Standardwert verwenden ist standardmäßig aktiviert, wenn der Name des SSL-Zertifikats mit dem Namen des virtuellen Hosts übereinstimmt. Der Name des virtuellen Hosts muss mit dem Namen des SSL-Zertifikats übereinstimmen. Der virtuelle Host ist der Rechnername, der Benutzern beim Erstellen des Zertifikats angezeigt wurde. Dies muss nicht der tatsächliche Rechnername sein. Der Zertifikatsname kann beispielsweise ein Platzhalterzeichen (Sternchen) enthalten oder einen Domänennamen, dessen Groß- bzw. Kleinschreibung nicht mit dem Domänennamen des Zertifikats übereinstimmt. Diese Einstellung ist sinnvoll in Umgebungen mit Lastausgleich oder Clusterdienst.
Kontoanmeldeinformationen	Wählen Sie das Konto des lokalen Computers aus, das für den Dienst verwendet wird. Normalerweise können Sie das Netzwerkdienst-Konto auswählen.

- Seite Domänen konfigurieren:
  1. Aktivieren Sie das Optionsfeld neben jeder Domäne, für die Sie die Dienstunterstützung aktivieren möchten.
  2. Wählen Sie die Domänen aus und klicken Sie auf Eigenschaften, um das Dialogfeld Konfiguration bearbeiten anzuzeigen.
  3. Wenn Sie einen zentralen Speicher unter Active Directory erstellt haben, wählen Sie Domänencontroller und wählen Sie dann den richtigen Domänencontroller aus der Liste aus.
  4. Wählen Sie Datenproxykonto und geben Sie den Benutzernamen, das Kennwort und die Domäne des Datenproxykontos ein, das für die Kommunikation mit dem zentralen Speicher verwendet wird.
  5. Wenn Sie das Self-Service-Modul installiert haben, wählen Sie Self-Service-Konto und geben Sie die Anmeldeinformationen für dieses Feature ein. Klicken Sie auf OK, um das Dialogfeld Konfiguration bearbeiten zu schließen.
     Wichtig: Wenn der Dienst unter Windows Server 2008 oder Windows Server 2008 R2 mit einem zentralen Speicher auf einer NTFS-Freigabe ausgeführt wird, müssen Sie mit dem Dienstprogramm CtxFileSyncPrep.exe das Konto für den Datenproxy als Administrator dem zentralen Speicher hinzufügen. Geben Sie Folgendes ein:
     CtxFileSyncPrep [/Admin:Kontoname]

     Wenn der Dienst unter Windows Server 2008 oder Windows Server 2008 R2 mit einem zentralen Speicher unter Active Directory ausgeführt wird, müssen Sie das Konto für den Datenproxy als Administrator dem zentralen Speicher hinzufügen. Weitere Informationen hierzu finden Sie auf der Citrix Website (http://support.citrix.com/article/ctx107690)

Der Single Sign-On-Dienst kann Dienstanfragen von Benutzern in verschiedenen vertrauenswürdigen Domänen verarbeiten. Ein Administrator kann das Citrix AppCenter mit der Single Sign-On-Komponente auf Computern in verschiedenen Domänen installieren und mehrere Benutzerkonfigurationen in jeder Domäne erstellen.

Beispiel: Der Computer mit dem Single Sign-On-Dienst befindet sich in DomäneA. Benutzer, die einer Benutzerkonfiguration in DomäneA zugeordnet sind, können mit dem Konto-Self-Service die Konten entsperren. Benutzer, die einer Benutzerkonfiguration in DomäneB zugeordnet sind, können das vom Dienstcomputer der DomäneA bereitgestellte

Feature auch verwenden. In dieser Situation bestehen mehrere Benutzerkonfigurationen in mehreren Domänen, die einen Computer mit dem Dienst für dieses Feature verwenden.

Anforderungen für das Mehrdomänendienstfeature

Vor der Implementierung des Mehrdomänendienstfeatures müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

Komponente	Anforderungen
Domänen	Jede Domäne, die den Dienst gemeinsam verwendet, muss zu derselben Domänenstruktur gehören. Die Domänen in der Struktur müssen eine gegenseitige Vertrauensbeziehung haben.
Zentraler Speicher	Dieses Features kann implementiert werden, wenn als zentraler Speicher Active Directory oder eine NTFS-Netzwerkfreigabe verwendet wird. Alle Benutzer, die denselben Dienstcomputer verwenden, müssen mit demselben Typ des zentralen Speichers implementiert werden: Active Directory oder freigegebener NTFS-Ordner. Mehrere Typen des zentralen Speichers werden nicht unterstützt. In dieser Situation kann als zentraler Speicher kein freigegebener NTFS-Ordner pro Domäne verwendet werden. Sie können jedoch als zentralen Speicher einen freigegebenen NTFS-Ordner pro Struktur verwenden.
Datenintegrität	Die Datenintegrität muss konsistent domänenübergreifend verwendet werden. Das heißt, das Feature ist entweder in der Konfiguration des Dienstes und des Single Sign-On Plug-ins für alle Domänen aktiviert oder deaktiviert. Beispiel: Sie können dieses Feature nicht in der Dienstkonfiguration aktivieren und bei der Installation des Plug-ins deaktivieren.
Single Sign-On-Komponente in Citrix AppCenter	Jede Konsole kann nur einen zentralen Speicher und nicht mehrere zentrale Speicher anzeigen. Der Single Sign-On-Administrator sollte eine Konsole in jeder Domäne mit einem Benutzerkonto installieren, das administrative Rechte in der Domäne hat. Der Administrator kann auch eine Konsole installieren, die auf andere Domänen zugreifen kann. Er kann dann ggf. zu einer dieser Domänen wechseln, wenn er sich mit den Anmeldeinformationen für diese Domäne anmeldet.
Datenproxy und Self-Service-Konten	Sie können einen Datenproxy und ein Self-Service-Konto konfigurieren, das Lese- und Schreibrechte für den zentralen Speicher und ausreichende Privilegien für das Zurücksetzen der Benutzerkennwörter und das Entsperren des Kontos hat. Sie können diese Konten auch für jede Domäne im Dienstkonfigurationstool angeben.

Komponente	Anforderungen

Konfigurieren des Diensts für mehrere Domänen

1. Melden Sie sich als Administrator am Computer an, auf dem der Dienst installiert ist.
2. Starten Sie das Tool zur Dienstkonfiguration; klicken Sie auf Start > Alle Programme > Citrix > Password Manager > Dienstkonfiguration.
3. Klicken Sie in der Dienstkonfiguration im linken Bereich auf Domänenkonfigurationen.
4. Markieren Sie das Optionsfeld neben jeder Domäne, um die Dienstunterstützung für diese Domäne zu aktivieren.
5. Wählen Sie die Domänen aus und klicken Sie auf Eigenschaften, um das Dialogfeld Konfiguration bearbeiten anzuzeigen.
6. Seite Konfiguration bearbeiten:
    1. Wenn Sie einen zentralen Speicher unter Active Directory erstellt haben, klicken Sie auf Domänencontroller und wählen Sie aus der Liste den Domänencontroller aus, an den sich Single Sign-On bei Schreibvorgängen zum zentralen Speicher bindet, oder wählen Sie Jeder nicht schreibgeschützte Domänencontroller.
    2. Klicken Sie auf Datenproxykonto und geben Sie den Benutzernamen, das Kennwort und die Domäne des Datenproxykontos ein, das für die Kommunikation mit dem zentralen Speicher verwendet wird.
    3. Wenn Sie das Self-Service-Modul installiert haben, klicken Sie auf Self-Service-Konto und geben Sie die Anmeldeinformationen für dieses Feature ein.

Installieren des Single Sign-On Plug-ins

Oct 05, 2015

Das Single Sign-On Plug-In wird auf dem XenApp-Server ausgeführt und stellt Anmeldeinformationen und Zugriff auf veröffentlichte Anwendungen bereit. Das Plug-in wird auch auf jedem Benutzergerät ausgeführt und stellt Anmeldeinformationen, Zugriff auf Anwendungen, die lokal auf dem Benutzergerät ausgeführt werden, und Steuern der Single Sign-On-Abläufe bereit.

Hinweis: Wenn Sie diese Version des Plug-Ins mit XenApp verwenden und für Single Sign-On aktivierte Anwendungen veröffentlichen, sollte das Plug-In auch auf den Benutzergeräten installiert sein. Wenn das Plug-in nicht auf dem Benutzergerät installiert ist, sendet Single Sign-On die Anmeldeinformationen automatisch an mit XenApp veröffentlichten Anwendungen; der Benutzer kann jedoch das Kennwort nicht bearbeiten, löschen oder anzeigen, Sign-On anhalten oder fortsetzen, feststellen, ob Sign-On angehalten wurde oder Kennwörtern manuell senden.
Berücksichtigungen für die Installation:

- Wenn Sie diese Version des Single Sign-On Plug-ins auf einem Benutzergerät installieren, wird Version 4.8 aktualisiert.
- Nach der Installation des Plug-Ins unter unterstützten Betriebssystemen, die die Windows-Komponente Microsoft Graphical Identification and Authentication (GINA) verwenden, muss das Gerät neu gestartet werden. Hierzu gehören Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 und Microsoft Windows Server 2003 mit Service Pack 2.
  WinLogon verwendet die GINA-Steuerelemente für das Dialogfeld, das Benutzern angezeigt wird, wenn sie die Tastenkombination STRG+ALT+ENTF drücken. Das Dialogfeld sammelt alle für die Authentifizierung erforderlichen Daten. XenApp, das Single Sign-On Plug-In und der Novell NetWare-Client interagieren alle mit der GINA-DLL (Dynamic Link Library) bzw. machen eine Ersetzung erforderlich. Unter Umständen müssen Sie Software in einer bestimmten Reihenfolge installieren oder deinstallieren, damit die richtige GINA-Kette erhalten bleibt. Wenn Sie das Single Sign-On Plug-In als letztes Programm installieren, stellen Sie sicher, dass Single Sign-On-GINA als erstes vom Winlogon-Prozess aufgerufen wird.
- Nach dem Abschluss der Installation (und ggf. dem Neustart des Geräts) wird das Citrix Receiver-Symbol in der Taskleiste angezeigt.
- Wenn Sie nach der Installation des Plug-Ins die Citrix Lizenzierungsinformationen konfigurieren oder ändern, starten Sie das Plug-In neu, um die Änderungen zu übernehmen.

1. Folgen Sie den Anweisungen unter
   — Installieren von XenApp mit dem assistentengestützten Serverrollen-Manager
   . Wählen Sie aus der Liste der optionalen Komponenten Single Sign-On Plug-in.
2. Bei der Konfiguration von XenApp mit dem assistentengestützten Serverkonfigurationstool werden Sie zur Auswahl des Typs des zentralen Speichers aufgefordert: Microsoft Active Directory (Standardwert) oder NTFS-Netzwerkfreigabe; geben Sie auch den Pfad ein.

1. Folgen Sie den Anweisungen unter
   — Installieren von XenApp an der Befehlszeile
   . Schließen Sie die Option SSONAgentFeature ein (/install:XenApp,SSONAgentFeature).
2. Bei der Konfiguration von XenApp an der Befehlszeile können Sie die Option /SSOPluginUncPath:Pfad einschließen und den UNC-Pfad zum zentralen Speicher auf der NTFS-Netzwerkfreigabe angeben. Wenn Sie diese Option auslassen, wird

Active Directory angenommen.

1. Laden Sie das XenApp-Medium auf dem Computer oder Server.
2. Wählen Sie im Autorun-Menü Komponenten manuell installieren > Serverkomponenten > Sonstiges > Single Sign-On > Single Sign-On Plug-In.
3. Folgen Sie den Anweisungen. Sie werden aufgefordert, den Typ des zentralen Speichers und die zu installierenden Komponenten auszuwählen (z. B. Sprachpakete, Self-Service und Datenintegrität).

Folgen Sie den Anweisungen zum Download oder der Bereitstellung von Plug-ins in der Merchandising Server-Dokumentation.

Wenn nur diese Version des Single Sign-On Plug-ins für alle XenApp-Sitzungen auf jedem Benutzergerät verwendet wird, wird im Microsoft Windows-Infobereich auf jedem Benutzergerät nur ein Receiver-Symbol mit einem integrierten Single Sign-On-Menü angezeigt, das alle Sitzungen konsolidiert.

Wenn XenApp oder auf dem Benutzergerät eine frühere Plug-in-Version verwendet wird, können im Windows-Infobereich auch Single Sign-On-Symbole angezeigt werden. In der folgenden Tabelle werden mehrere Szenarios beschrieben.

Benutzergerät		XenApp-Server		Windows-Infobereich	Menü "Kennwörter" über das Receiver-Symbol verfügbar?
Citrix Receiver	Single Sign-On Plug-in	Citrix Receiver	Single Sign-On Plug-in		
Aktuell*	5.0	Aktuell	5.0	Ein Receiver-Symbol	Ja
Aktuell	-	Aktuell	5.0	Ein Receiver-Symbol	Nein
Aktuell	5.0	-	4.8	Ein Receiver-Symbol und ein Single Sign-On-Symbol für jede verbundene XenApp-Sitzung. **	Ja
Aktuell	4.8	Aktuell	5.0	Ein Receiver-Symbol und ein Single Sign-On-Symbol	Nein
Aktuell	4.8	Aktuell	4.8	Ein Receiver-Symbol und ein Single Sign-On-Symbol, und ein Single Sign-On-Symbol für jede verbundene XenApp-Sitzung. **	Nein
Früher Online Plug-in	4.8	Aktuell	5.0	Ein Single Sign-On-Symbol und ein Online Plug-in-Symbol	Nein

* Aktuell = Receiver für Windows,der das Online Plug-in enthält

Benutzergerät		XenApp-Server		Windows-Infobereich	Menü "Kennwörter" über das Receiver-Symbol verfügbar?
Citrix Receiver	Single Sign-On Plug-in	Citrix Receiver	Single Sign-On Plug-in		

** Wenn auf den XenApp-Servern eine frühere Version des Single Sign-On Plug-ins ausgeführt wird und die aktuelle Receiver-Version auf dem Benutzergerät installiert ist (unabhängig davon, ob ein Single Sign-On Plug-in auf dem Benutzergerät installiert ist), enthält der Windows-Infobereich auf dem Benutzergerät ein Single Sign-On-Symbol für alle XenApp-Server (auf denen die frühere Plug-in-Version ausgeführt wird), zu denen eine Verbindung besteht.

Verwaltung

Oct 05, 2015

Sie können mit Kennwortrichtlinien Regeln definieren, die die Eigenschaften der von Benutzern gespeicherten Kennwörter steuern. Diese Regeln sind die Kennwortrichtlinien die Sie, abhängig vom Unternehmen, auf alle Benutzer oder auf bestimmte Gruppen von Anwendungen anwenden.

Hinweis: Citrix XenApp bietet Richtlinienregeln, mit denen Sie konfigurieren und steuern können, welche Benutzer Single Sign-On verwenden können, wenn sie eine Verbindung mit Servern und veröffentlichten Anwendungen in der Serverfarm herstellen. Trotz der ähnlichen Namen sind diese zwei Richtlinientypen nicht miteinander verwandt.
Single Sign-On enthält zwei Standardkennwortrichtlinien: Standardrichtlinie und Domänenrichtlinie. Sie können diese Richtlinien unverändert verwenden, kopieren oder ändern, um sie den im Unternehmen geltenden Richtlinien und Vorschriften anzupassen. Die Standardrichtlinie und die Domänenrichtlinie können nicht gelöscht werden.

Wenn ein Benutzer im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) Anmeldeinformationen für eine Anwendung hinzufügt, die nicht von einem Administrator definiert wurde, verwaltet Single Sign-On die Anwendung mit der Standardrichtlinie. Wenn Sie eine Anwendungsgruppe als Domänenkennwortgruppe behandeln möchten, wenden Sie die Domänenrichtlinie auf diese Anwendungsgruppe an.

Da Single Sign-On die Standardrichtlinie auf vom Benutzer hinzugefügte Anwendungen anwendet, legen Sie die Standardrichtlinie so großzügig wie möglich an, damit Kennwörter für Anwendungen angenommen werden, für die die Benutzer Kennwörter speichern können.

Sie können im Unternehmen beliebig viele Richtlinien erstellen. So können Sie z. B. eine Richtlinie auf die gesamte Domänengruppe anwenden und einzelne Richtlinien erstellen, die Sie auf einzelne Anwendungsgruppen anwenden, um die Anforderungen weiter zu definieren. Mit Kennwortrichtlinien können Sie folgende Aktionen ausführen:

- Automatische Kennwortänderung für Anwendungen.
- Implementieren von Sicherheitsschemas wie komplexe Kennwörter und anwendungsspezifische Kennwörter, die von Benutzern nicht angezeigt werden können.
- Definieren des Kennwortablaufs für Anwendungen, selbst wenn die Anwendung keine Funktion für den Kennwortablauf hat.
- Dies verhindert, dass Benutzer identische Kennwörter für dieselbe Anwendung zweimal hintereinander verwenden.

Manchmal haben Benutzer ein Kennwort, das für mehrere Anwendungen verwendet wird (z. B. bei einer Produktsuite). Dies wird als gemeinsame Kennwortverwendung bezeichnet. Dabei wird dieselbe Authentifizierungsstelle für die Anwendungen verwendet.

Die anderen Anmeldeinformationen für diese Anwendungen (z. B. Benutzername und benutzerdefinierte Felder) können unterschiedlich sein, das Kennwort des Benutzers ist jedoch gleich. Erstellen Sie in diesem Fall eine Anwendungsgruppe, die eine Kennwortgruppe ist. So stellen Sie sicher, dass das Single Sign-On Plug-In das Kennwort für alle Anwendungen in der Gruppe als Einheit verwaltet. Bei der Änderung des Kennworts in einer Anwendung stellt das Single Sign-On Plug-In sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe widergespiegelt wird.

Domänenkennwortgruppen unterscheiden sich von anderen Kennwortgruppen, da das Domänenkennwort des Benutzers

das primäre Kennwort für die Anwendungsgruppe ist. Wenn der Benutzer das Domänenkennwort ändert, übernimmt das Single Sign-On Plug-in die Änderung in den Anmeldeinformationen für alle anderen Anwendungen in der Gruppe. Es kann nur das Domänenkennwort geändert werden. Benutzer können nur dann Kennwortänderungen für eine der anderen Anwendungen in der Gruppe vornehmen, wenn der Administrator die Anwendung aus der Domänenkennwortgruppe entfernt.

Single Sign-on erzwingt die Einhaltung von Kennwortrichtlinien, unabhängig davon, ob das Kennwort benutzerdefiniert oder automatisch von Single Sign-On generiert wurde.

Das Einhalten einer Kennwortrichtlinie wird in den folgenden Situationen nicht erzwungen:

- Ein Benutzer registriert sich bei Single Sign-On (bei der Erstverwendung).
- Ein Benutzer bearbeitet ein Kennwort im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager)).
- Ein Administrator erstellt eine Anwendungsdefinition.

Single Sign-On erzwingt die Einhaltung einer Kennwortrichtlinie nicht für bestehende Kennwörter (d. h. Kennwörter, die vor der Single Sign-On-Implementierung im Unternehmen erstellt wurden), da Benutzern sonst der Zugriff auf bereits verwendete Anwendungen oder Ressourcen verweigert werden könnte.

Konfigurieren von Single Sign-On für die Erkennung von Anwendungen

Oct 05, 2015

Single Sign-On erkennt und reagiert auf Anwendungen basierend auf den Einstellungen in den Anwendungsdefinitionen.

Mit den Formularen, die in den Anwendungsdefinitionen enthalten sind, analysiert das Single Sign-On Plug-In jede Anwendung beim Start, erkennt bestimmte Identifizierungsmerkmale und stellt fest, ob für die startende Anwendung eine bestimmte Aktion ausgeführt werden muss, beispielsweise:

- Senden von Anmeldeinformationen des Benutzers bei Anmeldeaufforderung
- Aushandeln einer Oberfläche zum Ändern von Anmeldeinformationen
- Verarbeiten einer Oberfläche zum Bestätigen von Anmeldeinformationen

Anwendungsdefinitionen bestehen aus Formulardefinitionen und Konfigurationsoptionen, die für alle Formulare in der Konfiguration gelten. Formulardefinitionen sind Sätze bestimmter Erkennungs- und Aktionsmerkmale von Formularen für Anmeldeinformationen des Benutzers.

Die Einstellungen in der Formulardefinition legen die Aktionen fest, die Single Sign-On ausführt, wenn eine Anwendung eine bestimmte Aktion für die Anmeldeinformationen des Benutzers fordert.

Eine Anwendungsdefinition enthält alle Formulare zum Verwalten von Anmeldeinformationen des Benutzers, die einer einzelnen Anwendung zugeordnet sind.

Obwohl die meisten Anwendungen und die entsprechenden Anwendungsdefinitionen nur zwei Formulare für das Verwalten der Anmeldeinformationen der Benutzer verwenden, können Sie beliebig viele Formulare in einer Anwendungsdefinition definieren.

Single Sign-On unterstützt eine Vielzahl von Anwendungen, einschließlich Windows-, Web- und Terminalemulator-Anwendungen. Das Programm ist kompatibel mit Java-Anwendungen, SAP-Lösungen und Anwendungen, die auf einem Mainframe-, AS/400-System- oder UNIX-Server gehostet werden.

Verwenden Sie die Assistenten, um Anwendungsdefinitionen für Anwendungen zu erstellen, für die keine vordefinierten Anwendungsvorlagen bestehen. Im Assistenten für Anwendungsdefinitionen konfigurieren Sie die Merkmale, die allen in der Definition enthaltenen Formularen zugeordnet werden. Der Assistent für Formulardefinitionen leitet Sie schrittweise an, Unterstützung für Windows-, Web- und Terminalemulator-Anwendungen zu definieren.

Single Sign-On unterstützt außerdem die externe Anwendungserkennung und Aktionsverarbeitung. Mit diesem Feature können Implementierer von Drittanbietern die einem Formular zugeordneten Aufgaben zur Anwendungserkennung und Anmeldeinformationsübertragung erweitern, da während der Anwendungserkennung und Aktionsübertragungsverarbeitung im Single Sign-On Plug-In auf externe Prozesse zugegriffen werden kann.

Die Kombination dieser Features stellt Ihnen eine flexible und anpassbare Entwicklungsumgebung für Anwendungsdefinitionen bereit, mit der Sie Benutzern einen sicheren und flexiblen Single Sign-On-Zugriff auf wichtige Anwendungen bieten können.

Achtung: Single Sign-On hängt vom sicheren Betrieb des Computers ab, auf dem die Produktkomponenten ausgeführt werden. Wenn das Benutzergerät mit bösartigem Code infiziert wird, kann dieser Code die von Single Sign-On bereitgestellte Sicherheit gefährden. Sie sollten immer die optimalen Verfahren zum Erhalten der Sicherheit in der

Infrastruktur des Unternehmens einhalten, um dieses Risiko zu verringern.

Anwendungsvorlagen sind XML-Dateien, mit denen Sie Anwendungsdefinitionen zwischen verschiedenen Single Sign-On-Umgebungen gemeinsam verwenden können. Anwendungsvorlagen verringern den Zeit- und Arbeitsaufwand, da sie ohne größeren Bearbeitungs- oder Konfigurationsbedarf in Anwendungsdefinitionen umgewandelt werden können. Für Vorlagen müssen Sie Informationen eingeben, um die Anwendungsdefinition abzuschließen, u. a. URL oder Name der ausführbaren Datei, Kennwortablauf und erweiterte Erkennungseinstellungen.

Sie installieren Anwendungsvorlagen über den Knoten "Single Sign-On" im Citrix AppCenter oder im Anwendungsdefinitionstool. Beide Programme enthalten Anwendungsvorlagen für häufig verwendete Windows- und Webanwendungen.

Wichtig: Unter Windows Server 2008, Windows Server 2008 R2, Windows Vista oder Windows 7 müssen Sie dem Anwendungsdefinitionstool eine Integritätsebene von "hoch" geben, damit Schreibvorgänge zum zentralen Speicher von Active Directory möglich sind. Melden Sie sich mit einem Konto an, dass ein Mitglied der Gruppe "Lokaler Administrator" ist, um das Tool auf dem Systemcomputer zu starten. Das Konto muss auch Mitglied der Gruppe "Domänenadministrator sein und Schreibrechte zu Active Directory-Objekten im zentralen Speicher haben. Geben Sie diese Anmeldeinformationen bei der Ausführung des Tools entweder an der Eingabeaufforderung der Benutzerkontensteuerung oder bei der Erstanmeldung am System ein. Dem Tool wird eine hohe Integritätsebene zugeordnet und es hat Schreibrechte für Active Directory-Objekte.
Wenn Sie keine Anwendungsvorlage für eine Anwendung finden, erstellen Sie eine im Knoten "Single Sign-On" im Citrix AppCenter oder mit dem Anwendungsdefinitionstool.

Identifizieren von Anwendungen und Ereignissen zur Verwaltung von Benutzeranmeldeinformationen durch das Single Sign-On Plug-in

Jul 22, 2016

Die Benutzeroberfläche einer Anwendung umfasst verschiedene Formulare, mit denen anwendungsspezifische Ereignisse für Anmeldeinformationen des Benutzers verwaltet werden.

Beispielsweise gibt ein Formular die Anmeldeinformationen ein, ein zweites Formular ändert das Anwendungskennwort und ein drittes Formular bestätigt die erfolgreiche Änderung der Anmeldeinformationen des Benutzers.

Je nach Typ der zu definierenden Anwendung (Windows, Web oder Terminalemulator) werden in Single Sign-On eine Vielzahl unterschiedlicher Kennungen in Anwendungsdefinitionen gesammelt, um Formulare eindeutig zu erkennen und auf sie zu reagieren. Dazu gehören unter anderem der Anwendungstyp, der Fenstertitel und der Dateiname der ausführbaren Datei.

Sobald das Single Sign-On Plug-in die Anwendung und das Formular erkennt, werden die Benutzer je nach den vorgegebenen Einstellungen aufgefordert, die Anmeldeinformationen einzugeben oder zu speichern. Danach werden die gespeicherten Anmeldeinformationen gesendet oder die Benutzer aufgefordert, die Anmeldeinformationen zu aktualisieren.

Sie erstellen Anwendungsdefinitionen mit dem AppCenter oder dem Anwendungsdefinitionstool.

Eine Anwendungsdefinition unterstützt sämtliche Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers, die einer Anwendung zugeordnet sind. Dazu gehören:

- Authentifizieren des Benutzers
- Ändern der Anmeldeinformationen des Benutzers
- Bestätigen der geänderten Anmeldeinformationen

Anwendungsdefinitionen sind in drei Haupttypen klassifiziert, mit denen die gesammelten Informationen festgelegt werden:

- Windows-Anwendungen (einschließlich Java-Anwendungen und SAP Logon Pad)
- Webanwendungen (einschließlich Java-Applets)
- HLLAPI-kompatible, terminalemulator-basierte Anwendungen

Anwendungsdefinitionen bestehen aus folgenden Komponenten:

- Anwendungsmerkmale, die für alle Formulare in der Definition gelten. Diese werden mit dem Assistenten für Anwendungsdefinitionen definiert.
- Formularspezifische Daten zum Erkennen der einzelnen Ereignisse zum Verwalten von Anmeldeinformationen, die der Anwendung zugeordnet sind. Diese Formulare und Ereignisse definieren Sie mit dem Assistenten für Formulardefinitionen. Dieser Assistent wird im Assistent für Anwendungsdefinitionen ausgeführt.

Die Anwendungsmerkmale für alle Anwendungstypen enthalten ähnliche Konfigurationsinformationen. Die in der Anwendungsdefinition enthaltenen formularspezifischen Daten können jedoch je nach Anwendungstyp stark variieren.

Für das Erstellen einer Anwendungsdefinition müssen Sie vom Computer, auf dem die Anwendungsdefinition erstellt wird, auf die Anwendung zugreifen können. Da sich Anwendungssignaturen abhängig vom Betriebssystem unterscheiden können, sollten Sie Anwendungsdefinitionen unter allen Betriebssystemen testen, die in der Organisation verwendet werden.

Testen Sie immer Änderungen oder Upgrades einer Anwendung, die nach dem Entwickeln und Bereitstellen einer Anwendungsdefinition vorgenommen werden, um sicherzustellen, dass die Anwendungsdefinition aufgrund geänderter Anwendungssignaturen modifiziert werden muss.

Wichtig: Als Sicherheitsmaßnahme ist die Benutzeroberflächen-Rechteisolierung (UIPI) unter Windows Server 2008, Windows Server 2008 R2, Windows Vista und Windows 7 in der Standardeinstellung aktiviert. UIPI verhindert, dass Anwendungen Nachrichten an andere Anwendungen senden, die eine höhere Integritätsebene haben. Das Single Sign-On Plug-in, das in der Standardeinstellung mit einer mittleren Integritätsebene ausgeführt wird, erkennt und sendet dann keine Anmeldeinformationen für Anwendungen, die mit einer hohen Integritätsebene ausgeführt werden. Ändern Sie diese Standardeinstellungen nicht, um das beabsichtigte Sicherheitsniveau von diesen Betriebssysteme und von Single Sign-On zu erhalten.

Assistent für Anwendungs- und Formulardefinitionen im Überblick

Jul 22, 2016

Alle Anwendungsdefinitionen werden mit dem Assistenten für Anwendungsdefinitionen und dem integrierten Assistenten für Formulardefinitionen erstellt.

Mit dem Assistenten für Formulardefinitionen legen Sie die Merkmale jedes Formulars für die Verwaltung der Anmeldeinformationen der Benutzer fest, das in einer Anwendungsdefinition enthalten ist.

Zum Starten des Assistenten für Anwendungsdefinitionen markieren Sie den Knoten "Anwendungsdefinitionen" im AppCenter und klicken dann im Menü Aktion auf Anwendungsdefinition erstellen.

Der Assistent für Anwendungsdefinitionen sammelt Daten für jeden Anwendungstyp (Windows-, Web- oder Teminalemulator-Anwendungen).

Gesammelte Daten	Windows	Web-	Terminalemulator
Anwendung festlegen	X	X	X
Formulare verwalten	X	X	X
Benutzerdefinierte Felder benennen	X	X	X
Symbol angeben	X		
Erweiterte Erkennung konfigurieren	X	X	X
Kennwortablauf konfigurieren	X	X	X
Einstellungen bestätigen	X	X	X

Die meisten Anwendungen verwenden unterschiedliche Formulare für die Anmeldung und Kennwortänderungen. Einige Anwendungen haben auch separate Formulare, mit denen Benutzer über eine erfolgreiche Änderung des Kennworts informiert werden.

Auf der Seite Formulare verwalten fügen Sie der Anwendungsdefinition Formulare hinzu. Auf dieser Seite können Sie auch Formulare bearbeiten oder löschen.

Bei Auswahl von Formular hinzufügen wird der Assistent für Formulardefinitionen gestartet, mit dem die Formulardaten für ein Formular gesammelt werden. Verwenden Sie den Assistenten für Formulardefinitionen für jedes Formular in der Anwendungsdefinition.

Single Sign-On enthält die Felder für den Benutzernamen und das Kennwort für jedes Anmeldungsformular. Für einige Anwendungen werden weitere Informationen für die Authentifizierung des Benutzers benötigt, u. a. Datenbankname, Domänenname oder Systemname.

Mit dem Assistenten für Formulardefinitionen können Sie maximal zwei benutzerdefinierte Felder hinzufügen. Benennen Sie diese Felder dann auf der Seite Benutzerdefinierte Felder benennen im Assistenten für Anwendungsdefinitionen.

Um eine Zugriffstaste für den Namen des benutzerdefinierten Feldes festzulegen, fügen Sie im Feldnamen direkt vor dem zu verwendenden Buchstaben ein kaufmännisches Und-Zeichen (&) ein. Ohne Zugriffstaste legt das Single Sign-On Plug-in dynamisch einen numerischen Wert als Zugriffstaste für das Steuerelement fest. Dies wird auf der Schaltfläche je nach der Anzahl der benutzerdefinierten Felder als (1) oder (2) angezeigt.

Single Sign-On verwendet in der Standardeinstellung unterschiedliche Symbole, um Windows-, Web- und Terminalemulator-Anwendungen im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) zu unterscheiden. Sie können ein benutzerdefiniertes Symbol für Windows-Anwendungen auf der Seite Symbol angeben festlegen, damit Benutzer bestimmte Anwendungen leichter erkennen. Wenn Sie die Option für ein benutzerdefiniertes Symbol verwenden, sollten Sie die Symboldatei in demselben Verzeichnis wie die Anwendung speichern.

Mit den Optionen auf der Seite Erweiterte Erkennung konfigurieren verringern Sie Schleifen beim Senden und Ändern der Anmeldeinformationen.

Manchmal gehen Benutzer auf eine Website mit einer Schleife beim Senden von Anmeldeinformationen. In diesen Fällen melden sich die Benutzer von einer Anwendung ab und kehren auf die Anmeldeseite zurück. Das Single Sign-On Plug-in erkennt die Anmeldeseite und sendet die Anmeldeinformationen der Benutzer und meldet sie automatisch wieder an. Aktivieren Sie Nur die erste Anmeldung für diese Anwendung verarbeiten, um zu verhindern, dass die Anmeldeinformationen erneut automatisch gesendet werden.

Wenn eine vordefinierte Anwendung das erste Mal gestartet wird und diese Option ausgewählt ist, sendet das Single Sign-On Plug-in die Anmeldeinformationen bei der ersten Instanz des Anmeldeformulars, ohne dass ein weiterer Benutzereingriff erforderlich ist. Wenn der Benutzer sich abmeldet und das Anmeldedialogfeld erneut angezeigt wird, wird ein Fenster für ungefähr 10 Sekunden angezeigt. Benutzer haben drei Optionen:

- Fenster schließen: Es werden keine Anmeldeinformationen gesendet.
- Fenster ignorieren: Es werden keine Anmeldeinformationen gesendet.
- Auf den Link klicken: Die Anmeldeinformationen werden gesendet.

Beim Schließen der Anwendung wird die Sitzung beendet und Single Sign-On sendet die Anmeldeinformationen, wenn die Anwendung das nächste Mal geöffnet wird.

Aktivieren Sie die Option Nur die erste Anmeldung für diese Anwendung verarbeiten, um eine Schleife beim Ändern des Kennworts zu vermeiden. Wenn diese Option aktiviert ist und Benutzer versuchen, das Kennwort mehrmals beim Zugriff auf eine bestimmte Anwendung zu ändern, müssen sie nachfolgende Kennwortänderungen bestätigen.

Die Seite Kennwortablauf konfigurieren enthält folgende Optionen:

- Identifizieren eines Skripts, das beim Kennwortablauf ausgeführt wird

- Verwenden der Single Sign-On-Ablaufwarnung

Mit diesem Skript können Sie oder eine Person im Unternehmen Benutzer auffordern, Kennwörter für bestimmte oder alle Anwendungen regelmäßig zu ändern oder die Kennwörter automatisch zu ändern, um die Sicherheits- und Gesetzesvorschriften einzuhalten. Diese Prozesse lassen sich auch kombinieren. Wenn Sie solch ein Skript ausführen möchten, wenn das Kennwort abläuft, das der Anwendungsdefinition zugeordnet ist (wie in der Kennwortrichtlinie definiert), aktivieren Sie die Option "Skript ausführen" und geben Sie den absoluten Pfad für das Skript ein. Alle Benutzer müssen auf den Skriptpfad zugreifen können. Verwenden Sie keinen UNC-Pfad.

In der Regel ruft das Skript eine zugeordnete Anwendung über eine Befehlszeile mit einem Kennwortänderungsparameter auf.

Sie können auch die Option Citrix Single Sign-On-Ablaufwarnung verwenden aktivieren Beim Aktivieren dieser Option wird eine Warnmeldung zum Ablauf des Single Sign-On-Kennworts angezeigt, wenn die Kennwortrichtlinie für die Anwendung angibt, dass das Kennwort abgelaufen ist. Es wird wiederholt eine Meldung angezeigt, dass der festgelegte Zeitraum abgelaufen ist, jedoch keine Änderung des Kennworts erzwungen.

Mit dem Assistenten für Formulardefinitionen können Sie Folgendes ausführen:

- Definieren eines Formulars mit dem Assistenten für Anwendungsdefinitionen
- Bearbeiten eines vorhandenen Formulars
- Hinzufügen eines Formulars zu einer vorhandenen Anwendungsdefinition

Mit dem Assistenten für Formulardefinitionen legen Sie mehrere Standardformulare für die Verwaltung der Anmeldeinformationen des Benutzers fest:

- Anmeldeformular
  Identifiziert die Anmeldeoberfläche für eine Anwendung und verwaltet die Aktionen, die für den Zugriff auf die zugeordnete Anwendung benötigt werden.

- Kennwortänderungsformular
  Identifiziert die Kennwortänderungsoberfläche für eine Anwendung und verwaltet die Aktionen, die für das Ändern des Benutzerkennworts für die zugeordnete Anwendung benötigt werden.

- Formular für eine erfolgreiche Kennwortänderung
  Identifiziert die Oberfläche für eine erfolgreiche Änderung des Kennworts für eine Anwendung und verwaltet die Aktionen, die für das Bestätigen einer erfolgreichen Kennwortänderung für die zugeordnete Anwendung benötigt werden.

- Formular für eine fehlgeschlagene Kennwortänderung
  Identifiziert die Oberfläche für eine fehlgeschlagene Kennwortänderung für eine Anwendung und legt die Aktionen fest, die bei einer fehlgeschlagenen Kennwortänderung ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Die Daten, die für jedes Formular gesammelt sind, erfüllen zwei Funktionen:

- Eindeutiges Identifizieren beim Starten eines anwendungsspezifischen Formulars
- Ausführen der erforderlichen Aktionen zum Verarbeiten der Anmeldeinformationen des Benutzers, die dem Formular zugeordnet sind

Sie starten den Assistenten für Formulardefinitionen auf der Seite Formulare verwalten im Assistenten für Anwendungsdefinitionen, wenn Sie Formular hinzufügen auswählen.

In der folgenden Tabelle finden Sie die Formularinformationen, die vom Assistenten für Formulardefinitionen für jeden Anwendungstyp (Windows, Web und Terminalemulator) gesammelt werden.

Gesammelte Daten	Windows	Web-	Terminalemulator
Formular benennen	X	X	X
Formular identifizieren	X	X	X
Formularaktionen definieren	X	X	
Regeln für Felderkennung einstellen			X
Sonstige Einstellungen konfigurieren	X	X	X
Einstellungen bestätigen	X	X	X

Windows-Anwendungsdefinitionen

Jul 22, 2016

Mit Windows-Anwendungsdefinitionen identifizieren Sie Windows-Anwendungen, Java-Anwendungen und Anwendungen, die über SAP Logon Pad gestartet werden.

Für die Definition einer Anwendungsdefinition können Sie jede Anwendung, die von einer Datei mit einer EXE-Erweiterung gestartet wird, als Windows-Anwendung klassifizieren.

Am besten können Sie die für Windows-Anwendungsdefinitionen erforderlichen Informationen erfassen, wenn Sie die Anwendung starten und zum Formular navigieren, für das ein Ereignis zum Verwalten der Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche oder fehlgeschlagene Kennwortänderung) erforderlich ist, während gleichzeitig der Assistent für Formulardefinitionen über die Konsole oder vom Anwendungsdefinitionstool ausgeführt wird. Der Assistent enthält Anweisungen zum Suchen und Identifizieren der erforderlichen Bestandteile der Anwendung.

Geben Sie beim Erstellen von Anwendungsdefinitionen für Windows-Anwendungen auf der Seite Formular identifizieren die Informationen ein, mit denen das Single Sign-On Plug-in das definierte Formular eindeutig erkennt.

Zu diesen Informationen gehören der Fenstertitel und der Name der ausführbaren Datei. Wenn das Single Sign-On Plug-in den Namen der ausführbaren Datei erkennt, überwacht es die Anwendung auf die definierten Fenstertitel.

Wenn ein Fenstertitel erkannt wird, führt das Single Sign-On Plug-in die für das Formular definierten Aktionen aus.

Identifizieren eines Formulars

1. Starten Sie ggf. das Windows-Programm und navigieren auf das Formular für die Benutzeranmeldung, Kennwortänderung, die erfolgreiche oder fehlgeschlagene Kennwortänderung.
2. Klicken Sie auf der Seite Formular identifizieren im Assistenten für Formulardefinitionen auf Auswählen.
3. Wenn das gewünschte Programm nicht markiert ist, wählen Sie im Dialogfeld Programmfenster auswählen eines der verfügbaren Programme aus.

Identifizieren von dynamischen Fenstertiteln

Auf der Seite Formular identifizieren können Sie im Feld Fenstertitel für dieses Formular die Titel bearbeiten, um dynamische Fenstertitel zu verwalten, u. a. eine Datums- oder Sitzungskennung. Ersetzen Sie hierfür Platzhalterzeichen für dynamische Daten, die im Fenstertitel angezeigt werden, wie folgt:

Wildcard	Beschreibung
?	Platzhalter für ein einzelnes Zeichen in dynamischen/sich ändernden Fenstertiteln
*	Platzhalter für dynamische Fenstertiteldaten für ein oder mehrere Zeichen. Dieser Wert empfiehlt sich nicht für leere Fenstertitel. Verwenden Sie in diesen Fällen den Wert NULL.
NULL	Platzhalter für leere Fenstertitel (das Wort NULL muss großgeschrieben sein)

Im Bereich Namen und Pfade der ausführbaren Datei werden der Name der ausführbaren Datei und Informationen zum sicheren Pfad angezeigt.

Bei sicheren Pfaden werden nur Programminstanzen der Anwendung erkannt, die über die hier definierten Pfade initiiert werden. Wenn mehrere sichere Pfade identifiziert werden, sendet das Single Sign-On Plug-in nur dann Anmeldeinformationen, wenn das identifizierte Programm über den definierten Pfad ausgeführt wird und alle anderen definierten Formularkennungen vorliegen.

Sie können einen sicheren Pfad festlegen, indem Sie im Dialogfeld Programmfenster auswählen die Option Kompletten Pfad der ausführbaren Datei verwenden aktivieren.

Wenn keine Pfadangaben definiert sind, wird Keine Angabe angezeigt und das Single Sign-On Plug-in sendet Anmeldeinformationen an jedes Programm, das den anderen Formularkennungen entspricht.

Trennen Sie mehrere Pfade mit Strichpunkten. Sie können Pfade mit absoluten Pfadangaben oder Umgebungsvariablen identifizieren.

Hinweis: Mit Anwendungsdefinitionen, die einen sicheren Pfad enthalten, können Vorlagen für Anwendungsdefinitionen erstellt werden. Der sichere Pfad ist jedoch nicht in der Vorlage enthalten.

Auf der Seite Formularaktionen definieren können Sie definieren, welche Aktionen vom Single Sign-On Plug-in ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular gesendet werden können.

Am oberen Rand werden alle Anmeldeinformationen des Benutzers angezeigt, die dem betreffenden Formular zugeordnet sind.

	Anmeldeformular	Kennwortänderungsformular	Formular für eine erfolgreiche Kennwortänderung	Formular für eine fehlgeschlagene Kennwortänderung
Username/ID	X	X	X	X
Password	X		X	X
Altes Kennwort		X		
Neues Kennwort		X		
Kennwort bestätigen		X		
Benutzerdefiniertes Feld 1	X		X	X
Benutzerdefiniertes Feld 2	X		X	X
OK	X	X	X	X

Unten auf der Seite wird die definierte Aktionsfolge angezeigt.

Auf dieser Seite werden die Aktionen definiert, die vom Plug-in ausgeführt werden, um die erforderlichen Anmeldeinformationen des Benutzers erfolgreich an das identifizierte Formular zu senden.

Definieren von Formularaktionen

Die folgenden Schritte reichen für die meisten Windows-Anwendungen aus:

1. Klicken Sie auf den Link Festlegen/Ändern, der bestimmten Anmeldeinformationen des Benutzers zugeordnet ist. Dadurch wird das Dialogfeld Steuerelementtext konfigurieren geöffnet, in dem das Steuerelement identifiziert wird, das die ausgewählten Anmeldeinformationen des Benutzers erhalten soll.
2. Wählen Sie den Steuerelementtyp aus, der die Anmeldeinformationen erhalten soll. Bei der Auswahl der verschiedenen möglichen Optionen wird der zugeordnete Steuerelementtyp in der Anwendung markiert, damit der Steuerelementtyp, der die identifizierten Anmeldeinformationen des Benutzers bzw. die Schaltfläche "Senden" erhalten soll, leichter identifiziert werden kann.
3. Wiederholen Sie diese Aktion für alle Anmeldeinformationen des Benutzers, die für das Formular erforderlich sind, sowie für die erforderliche Schaltfläche zum Senden des Formulars.
   Für einige Formulare sind Domänen- oder andere benutzerdefinierte Anmeldeinformationen erforderlich, die erfolgreich gesendet werden müssen, um das Formular zu verarbeiten. Zwei benutzerdefinierte Felder sind verfügbar, um diese Anforderungen zu erfüllen. Weisen Sie diesen Feldern die Sonderanmeldeinformationen zu. Die diesen Feldern zugeordneten Namen werden auf der Seite Benutzerdefinierte Felder benennen des Assistenten für Anwendungsdefinitionen nach der Definition des Formulars festgelegt.

   Hinweis: Nicht alle Anmeldeinformationen, die oben auf der Seite Formularaktionen definieren angegeben sind, müssen konfiguriert werden.

Auf der Seite "Fensterkennung" definieren Sie eine Fenstersteuerelement-ID, mit der ein Formular eindeutig identifiziert wird, wenn mehr als ein Fenster identifiziert ist. Dazu wird lediglich der definierte Fenstertitel und der Name der ausführbaren Datei verwendet. Dies ist nur sinnvoll, wenn mit der Fenstersteuerelement-ID zwischen mehreren identifizierbaren Formularen unterschieden werden kann.

Aktivieren Sie das Kontrollkästchen Zuordnen nach Fenstersteuerelement-ID aktivieren und geben Sie die Steuerelement-ID an, mit der das zu definierende Formular eindeutig von allen anderen Formularen unterschieden werden kann.

Identifizierungserweiterungen sind Teil der Anwendungsdefinitionserweiterungen. Mit diesen Erweiterungen können neben der Plug-in-Software externe Anwendungen verwendet werden, um zu erkennen, ob Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers vorliegen und um Anmeldeinformationen zu senden.

Obwohl Single Sign-On-Administratoren normalerweise Anwendungsdefinitionen in der Single Sign-On-Konsolenkomponente und im Anwendungsdefinitionstool erstellen, sind für einige Anwendungen aufgrund spezieller Anforderungen alternative Verfahren erforderlich, um die Anwendung zu erkennen und Anmeldeinformationen des Benutzers zu senden bzw. ähnliche Aktionen auszuführen.

Um diese Anwendungen zu unterstützen, können Single Sign-On-Administratoren mit Anwendungsdefinitionserweiterungen eine Abstraktion für die Anwendungssteuerelemente und die zugeordneten Dateneingabemechanismen schaffen.

Identifizierungserweiterungen werden von Implementierern von Drittanbietern entwickelt. Die Implementierung erfolgt anwendungsspezifisch. Aus diesem Grund sind die erforderlichen Verfahren zum Konfigurieren ihrer Verwendung ebenfalls anwendungsspezifisch.

Im Allgemeinen sind Single Sign-On-Administratoren nicht an der Entwicklung dieser Erweiterungen beteiligt. Erweiterungen werden von Implementierern von Drittanbietern erstellt. Da die Konfiguration dieser Erweiterungen erweiterungsspezifisch ist, sind der Erweiterung in der Regel Konfigurationsanleitungen beigefügt.

Auf der Seite Formularaktionen definieren definieren Sie die Aktionen, die von der Plug-in-Software ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular für die Verwaltung der Benutzerinformationen gesendet werden

können.

Für viele Windows-Anwendungen reichen die grundlegenden Informationen aus, die im Assistenten für Formulardefinitionen gesammelt werden, um das Formular zu definieren. Für einige Formulare sind jedoch weitere Informationen, Schritte, Sondertasten oder andere Aktionen erforderlich, um eine Aufgabe zum Verwalten von Anmeldeinformationen des Benutzers abzuschließen. Klicken Sie für diese Formulare auf der Seite Formularaktionen definieren auf Aktionseditor, um das Dialogfeld Aktionseditor zu öffnen.

Das Dialogfeld Aktionseditor enthält Folgendes:

- Aktionen auswählen
  Zeigt alle verfügbaren Aktionsfolgeaktionen an:
- Aktionen konfigurieren
  Definieren aktionsspezifischen Optionen in der Aktionsfolge.
- Aktionsfolgen
  Zeigt die Reihenfolge an, in der definierte Aktionen ausgeführt werden müssen, um das spezifische Formular zum Verwalten von Anmeldeinformationen des Benutzers zu verarbeiten.

Unten im Dialogfeld Aktionseditor finden Sie die Schaltfläche Erweiterte Einstellungen, mit der Sie auf das Dialogfeld Erweiterte Einstellungen zugreifen. Das Dialogfeld Erweiterte Einstellungen hat zwei Optionsfelder:

- Ordinalzahlen für Steuerelemente
  Aktivieren Sie dieses Kontrollkästchen, um keine Steuerelement-ID-Nummern sondern Ordinalzahlen für Steuerelemente (häufig als Z-Reihenfolge bezeichnet) zu verwenden. Ordinalzahlen für Steuerelemente werden bei der Definition unabhängig (und von der Plug-in-Software) festgelegt, um die Steuerelemente unabhängig von den Steuerelement-ID-Nummern, die von der Anwendung definiert werden, eindeutig zu identifizieren.

  Sie sollten dieses Feature bei der Definition von .NET-Anwendungen, die dynamische Nummern für Steuerelement-IDs generieren, oder für Anwendungen mit duplizierten Nummern für Steuerelement-IDs auswählen.
- Anfängliche Verzögerung
  Wählen Sie diese Option aus und definieren Sie, wie lange die Plug-in-Software wartet, bevor die Aktionsfolge initiiert wird. Sie können eine Verzögerung auch konfigurieren, indem Sie die Aktionsfolge mit der Aktion Verzögerung einfügen verzögert starten.

  Im Gegensatz zur Option Verzögerung einfügen, auf die Sie im Bereich Aktionen auswählen im Dialogfeld Aktionseditor zugreifen (als SendKeys-Vorgang definiert) können Sie mit einer an dieser Stelle definierten anfänglichen Verzögerung das Erstellen einer Anwendungsdefinition vermeiden, die nur von den Versionen 4.5, 4.6 und 4.6 mit Service Pack 1, 4.8 und 5.0 des Single Sign-On Plug-Ins unterstützt werden.

1. Wählen Sie eine Aktion unter den Auswahlen in Aktionen auswählen.
2. Konfigurieren Sie die Aktion mit den Optionen unter Aktionen konfigurieren. Wenn Sie die gewünschten Konfigurationseinstellungen gewählt haben, klicken Sie auf Einfügen. Die konfigurierte Aktion wird unter Aktionsfolge aufgeführt.
3. Wiederholen Sie die Schritte 1 und 2 für alle Aktionen, die für das Formular für Anmeldeinformationen des Benutzers erforderlich sind.
4. Wählen Sie Aktionen unter Aktionsfolge und klicken Sie auf Auf oder Ab, um sie in der richtigen Ausführungsreihenfolge anzuordnen, die für das Verwaltungsformular für die Anmeldeinformationen des Benutzers benötigt werden.
5. Wenn die Aktionsfolge richtig und vollständig ist, klicken Sie auf OK. Sie gehen dann auf die Seite Formularaktionen definieren zurück, und die definierte Aktionsfolge wird im Bereich Aktionsfolge angezeigt.

6. Klicken Sie auf Weiter, um die Definition des Formulars auf der Seite Sonstige Einstellungen konfigurieren fortzusetzen. Wenn eine Kombination der Formularaktionen die definierte Folge nur auf das Plug-in bzw. die Agentsoftware von Single Sign-On 4.5, Password Manager 4.6, Password Manager 4.6 mit Service Pack 1, Single Sign-On 4.8 und Single Sign-On 5.0 beschränkt, wird eine Meldung angezeigt, und Sie können fortfahren oder zurückgehen und die Konfiguration bearbeiten.

Beachten Sie beim Definieren von Windows-Anwendungsdefinitionen die folgenden Punkte:

- Anwendungsvorlagen erleichtern das Erstellen von Anwendungsdefinitionen.
- Testen Sie die Anwendungsdefinitionen mit der Plug-In-Software, bevor Sie sie Benutzern zur Verfügung stellen.
- Von den meisten Anwendungsdefinitionen werden nur die grundlegenden Informationen verwendet. Wenn eine Anwendungsdefinition in der Testumgebung nicht wie erwartet funktioniert, kann dies auf eindeutige Features wie dynamische Fenstertitel, dynamische Steuerelement-IDs oder andere spezielle Kennungen oder Aktionen zurückzuführen sein, die in die Anwendung programmiert wurden.
- Mit der Aufgabe Administrative Daten exportieren der Single Sign-On-Komponente im Citrix AppCenter exportieren Sie Anwendungsdefinitionen aus der Testumgebung in die Produktionsumgebung.
- Einstellungen, die auf Anwendungsdefinitionsebene ausgewählt sind, gelten für alle Formulare innerhalb der Anwendungsdefinition.
- Einige Einstellungen, die auf Anwendungsdefinitionsebene ausgewählt sind, können jedoch auf Formularebene überschrieben werden. Für eine Anwendung mit drei definierten Formularen kann beispielsweise auf Anwendungsdefinitionsebene das automatische Senden aktiviert werden. Jedes Mal, wenn die Plug-In-Software auf eines dieser drei Formulare für diese Anwendung trifft, werden die Anmeldeinformationen des Benutzers automatisch bereitgestellt und gesendet. Das automatische Senden kann jedoch auf Formularebene für eines der Formulare deaktiviert werden, sodass die Plug-In-Software die Informationen für dieses bestimmte Formular nicht automatisch sendet. In diesem Fall muss der Benutzer für das ausgewählte Formular auf Senden oder OK klicken.
- Um eine Zugriffstaste für den Namen des benutzerdefinierten Feldes festzulegen, fügen Sie im Feldnamen direkt vor dem zu verwendenden Buchstaben ein kaufmännisches Und-Zeichen (&) ein.
  Ohne Zugriffstaste legt die Plug-In-Software dynamisch einen numerischen Wert als Zugriffstaste für das Steuerelement fest. Diese Ziffer wird auf der Schaltfläche je nach der Anzahl der benutzerdefinierten Felder als (1) oder (2) angezeigt.

  Testen Sie das fertige Formular, um sicherzustellen, dass der definierte Name für das benutzerdefinierte Feld nicht zu groß ist.

Wenn im Assistenten für Webformulare kein Formular für die Webanwendung erkannt wird, muss die Formulardefinition umgeleitet werden, sodass eine für eine Windows-Anwendung erstellte Formulardefinition verwendet wird.

Formulare werden unter Umständen nicht erkannt, wenn in der Webanwendung ActiveX-Steuerelemente, Flash-basierte Steuerelemente, bestimmte Ajax-Steuerelementtypen oder andere nicht auf HTML basierende Steuerelemente für Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden.

Stellen Sie in diesen Situationen sicher, dass das Kontrollkästchen Zu Windows-Anwendung umleiten auf der Seite Formular benennen aktiviert ist. Klicken Sie auf Weiter, um die restlichen Seiten im Assistenten für die Formulardefinition zu durchlaufen, und klicken Sie dann auf der Seite Einstellungen bestätigen auf Fertig stellen.

Die Merkmale für die Formularerkennung und die Aktionen für die Anmeldeinformationen müssen jetzt mit einer Windows-Anwendungsdefinition und SendKeys-Aktionen definiert werden.

Identifizieren von Windows-Formularen mit der erweiterten Zuordnung

Jul 22, 2016

Die Seite Formular identifizieren im Assistenten für Formulardefinitionen enthält für die meisten Windows-Anwendungen ausreichende Identifizierungszuordnungen. Für einige Formulare für die Verwaltung von Anmeldeinformationen werden zusätzliche Kennungen benötigt. Single Sign-On bietet für diese Formulare die erweiterte Zuordnung. Dieses Feature steht auf der Seite Formular identifizieren des Assistenten für Formulardefinitionen zur Verfügung; klicken Sie auf Erweiterte Zuordnung.

Die erweiterte Zuordnung bietet fünf erweiterte Kennungen für Windows-Anwendungen:

- Klasseninformationen
- Steuerelementzuordnung
- SAP-Sitzungsinformationen
- Fensterkennung
- Identifizierungserweiterungen

Auf der Seite Klasseninformationen können Sie Formulare angeben, die von Single Sign-On ignoriert werden sollen. Wenn Sie eine Fensterklasse in das Feld Diese Fensterklasse ignorieren eingeben, reagiert das Single Sign-On Plug-in nicht, wenn ein Formular mit diesen Klasseninformationen angezeigt wird.

Verwenden Sie diesen Zuordnungstyp nicht für .NET-Anwendungen bzw. für Anwendungen, die die Fensterklasse 32770 (Standardklasse) verwenden.

Diese Einstellung ist bei dynamischen Fensterklassen von Nutzen. Verwenden Sie in diesem Fall Platzhalterzeichen, um eine Kennung für dynamische Fensterklassen zuzuordnen.

Wildcard	Beschreibung
?	Platzhalter für einzelnes dynamisches/sich änderndes Zeichen.
*	Platzhalter für dynamische Kennungsdaten für ein oder mehrere Zeichen. Dieser Wert empfiehlt sich nicht für leere Fensterklassenkennungen. Verwenden Sie in diesen Fällen den Wert NULL.
NULL	Platzhalter für leere Fensterklassenkennungen (das Wort NULL muss großgeschrieben sein).

Verwenden Sie Fensterklassenkennungen, wenn Sie eine Fensterklasse unter vielen möglichen Fensterklassenzielen identifizieren möchten. Es gelten die folgenden Bedingungen:

- Der angegebene Fenstertitel und die zugeordnete ausführbare Datei führen zu mehreren möglichen Entsprechungen. Dieser Fall tritt häufig auf, wenn der Fenstertitel dynamische Daten enthält und Platzhalter angegeben sind.
- Das Zielformular muss einer eindeutigen Fensterklassenkennung zugeordnet sein und für alle anderen möglichen Entsprechungen müssen andere Fensterklassenkennungen gelten.

Identifizieren von Klasseninformationen

Starten Sie auf der Seite Formular identifizieren im Assistenten für Formulardefinitionen.

1. Klicken Sie auf Erweiterte Zuordnung und wählen Sie dann die Option Klasseninformationen aus.
2. Klicken Sie auf Auswählen, um die Zielanwendung unter den Anwendungen auszuwählen, die zurzeit auf dem Computer geöffnet sind.
   Hinweis: Aktivieren Sie das Kontrollkästchen Ausgeblendete Programmfenster anzeigen oder das Kontrollkästchen Untergeordnete Fenster anzeigen, um weitere Auswahlen anzuzeigen.

In einigen Anwendungen werden Steuerelementbeschriftungen dynamische Informationen zugewiesen. In diesen Fällen können der Fenstertitel, die ihm zugeordnete ausführbare Anwendung und die Steuerelement-ID(s) für mehrere Formulare zum Verwalten von Anmeldeinformationen des Benutzers identisch sein, während sich die Textbeschriftungen oder andere Eigenschaften auf dem Formular infolge anwendungsspezifischer Ereignisse ändern.

Verwenden Sie für diese Formulartypen die Konfigurationsoptionen zur Steuerelementzuordnung, um ein Formular für eine bestimmte Plug-in-Aktion eindeutig zu identifizieren. Dies erfolgt auf der Grundlage eindeutiger Klassen-, Stil- oder Textwerte, die der Steuerelement-ID (bzw. mehreren Steuerelement-IDs, wenn mehrere Definitionen zur eindeutigen Identifizierung des Formulars erforderlich sind), zugeordnet sind.

Definieren von Zuordnungskriterien

Starten Sie auf der Seite Formular identifizieren im Assistenten für Formulardefinitionen.

1. Klicken Sie auf Erweiterte Zuordnung und wählen Sie dann die Option Steuerelementzuordnung aus.
2. Klicken Sie auf Zuordnung hinzufügen.
   Hinweis: Definieren Sie nur so viele Kriterien zur Steuerelementzuordnung wie für die Identifizierung des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.
3. Klicken Sie im Dialogfeld Zuordnungskriterien definieren auf Auswählen.
4. Klicken Sie mit der rechten Maustaste auf einen Steuerelement-ID-Eintrag.
5. Wählen Sie Klasse, Stil oder Text, um ein Merkmal auszuwählen, mit dem das Formular für die ausgewählte Steuerelement-ID identifiziert wird.
6. Wiederholen Sie die Schritte 4 und 5 für jede Steuerelement-ID, die zur eindeutigen Identifizierung des Formulars verwendet wird.

Ältere SAP-Versionen werden über die Standarddefinitionen für Windows- und Webanwendungen verwaltet. Das Dialogfeld Erweiterte Zuordnung bietet jedoch Unterstützung für SAP-Anwendungen, bei denen mehrere SAP-Systeme dieselbe SAP GUI-Anmeldebenutzeroberfläche (z. B. SAP Logon Pad) verwenden.

Zum Unterstützen der SAP-Sitzungsinformationen muss vom SAP-Administrator das GUI-Skripting auf dem Server aktiviert sein. Dann können die Konsole und die Single Sign-On Plug-in-Software Daten vom SAP Logon Pad abfragen und die System-ID oder den Servernamen (oder beide) bestimmen, die für die eindeutige Identifizierung des bestimmten Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.

Mit der Option SAP-Sitzungsinformationen können die Sitzungsinformationen aus einem SAP-Fenster extrahiert werden, um SAP-Anmeldefenster eindeutig zu identifizieren und voneinander zu unterscheiden.

Manuelles Definieren von SAP-Sitzungsinformationen

Sie können die SAP-System-ID und den Servernamen eingeben. Sie können in beiden Feldern reguläre Ausdrücke als Werte verwenden. Dies ist sinnvoll, wenn Sie mehrere Server zuordnen möchten.

Ein weiterer Grund für die manuelle Eingabe von Werten ist die Zuordnung von DNS- und NetBIOS-Namen eines Servers.

Verwenden Sie das folgende Format für reguläre Ausdrücke, um DNS und NetBIOS zu unterstützen.

^Servername(\.Domäne\.com)?$

Generieren einer SAP GUI-Skriptmeldung

SAP GUI-Skriptmeldungen können erstellt werden, wenn vom Programm versucht wird, über die SAP GUI eine Verbindung zu SAP Logon Pad herzustellen. In diesem Fall können Sie eine Registrierungseinstellung ändern und das Anzeigen der Meldung verhindern.

Der Schlüssel lautet HKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security\WarnOnAttach. Dies ist ein DWORD-Wert. Wenn dieser Schlüsselwert auf 0 gesetzt wird, wird die Meldung nicht angezeigt. Der Standardwert ist 1.

Webanwendungsdefinitionen

Jul 22, 2016

Mit Webanwendungsdefinitionen werden webbasierte Anwendungen, einschließlich Java-Applets, identifiziert.

In der Regel wird jede Anwendung, die in einem Browser ausgeführt wird, beim Definieren einer Anwendungsdefinition als Webanwendung eingestuft. Single Sign-On unterstützt Webanwendungen, die mit Internet Explorer-Versionen 6.0, 7.0. 8.0 und 9.0 ausgeführt werden.

Webanwendungsdefinitionen werden zum Teil durch Identifizieren von Teilen der aktiven Webanwendung erstellt. Am besten (und einfachsten) können Sie die für Webanwendungsdefinitionen erforderlichen Informationen sammeln, wenn Sie die Anwendung starten und zum Formular navigieren, für das ein Ereignis zum Verwalten der Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) erforderlich ist, während gleichzeitig der Assistent für Formulardefinitionen in der Konsole oder vom Anwendungsdefinitionstool ausgeführt wird. Der Bildschirmtext des Assistenten enthält Anweisungen zum Suchen und Identifizieren der erforderlichen Bestandteile der Anwendung.

Beim Erstellen von Anwendungsdefinitionen für Webanwendungen wird die Seite Formular benennen des Assistenten für Formulardefinitionen für Folgendes verwendet:

- Zuweisen eines benutzerdefinierten Namens für das zu erstellende Formular
- Identifizieren des zu erstellenden Formulartyps
- Identifizieren aller speziellen Aktionen

Bedenken Sie, dass der Name, den Sie dem Formular zuweisen, auf der Seite Formulare verwalten des Assistenten für Anwendungsdefinitionen angezeigt wird. Weisen Sie daher einen aussagekräftigen Namen für den zu definierenden Formulartyp zu.

Verschiedene Standardformulartypen zum Verarbeiten von Anmeldeinformationen des Benutzers können mit dem Assistenten für Formulardefinitionen definiert werden. Dazu gehören:

- Anmeldeformular
  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.
- Kennwortänderungsformular
  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.
- Formular für eine erfolgreiche Kennwortänderung
  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.
- Formular für eine fehlgeschlagene Kennwortänderung
  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwortänderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare

enthalten.

Verwenden Sie den Bereich Spezielle Aktionen, um ggf. spezielle Formularaktionen für das zu definierende Formular zu identifizieren:

- Keine spezielle Aktion
  Wählen Sie diese Option für die normale Webformularverarbeitung.
- Zu Windows-Anwendung umleiten
  Wählen Sie diese Option aus, wenn im Assistenten für Webformulare kein Formular für die Webanwendung erkannt wurde. Dies tritt auf, wenn in der Webanwendung ActiveX-Steuerelemente, Flash-basierte Steuerelemente, bestimmte Ajax-Steuerelementtypen oder andere nicht auf HTML basierende Steuerelemente für Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden.
- Dieses Formular ignorieren, wenn es von der Plug-in-Software erkannt wird
  Wählen Sie diese Option, damit die Plug-in-Software das Formular ignoriert.

Beim Erstellen von Anwendungsdefinitionen für Webanwendungen werden auf der Seite Formular identifizieren die Informationen eingegeben, die erforderlich sind, damit das zu definierende Formular von der Single Sign-On Plug-In-Software eindeutig erkannt wird.

Webanwendungen werden über die URL-Adresse identifiziert, die dem Formular zum Verwalten von Anmeldeinformationen des Benutzers zugeordnet ist, das definiert wird.

Klicken Sie auf Auswählen, um das Dialogfeld "Webseite auswählen" zu öffnen. Geben Sie im Dialogfeld "Webseite auswählen" die Webseite an, die Sie dem Formular zuordnen möchten.

Nach Abschluss der Webseitenauswahl gehen Sie auf diese Seite zurück. Zum Verwalten der Interpretation der identifizierten URLs sind zwei Kontrollkästchen verfügbar:

- Strenge URL-Zuordnung
  Wenn Sie dieses Kontrollkästchen aktivieren, werden Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers nur erkannt, wenn sie von Webanwendungen stammen, die über die angegebenen URLs gestartet wurden. Einige URLs enthalten unter Umständen dynamische Daten wie Kennungen zur Sitzungsverwaltung, Anwendungsparameter oder andere Kennungen, die für jede Instanz unterschiedlich sein können. In diesem Fall wird die URL beim Verwenden der strengen URL-Zuordnung möglicherweise nicht erkannt.
- URL (Groß-/Kleinschreibung)
  Aktivieren Sie dieses Kontrollkästchen, um URLs mit genau übereinstimmender Schreibweise zu verwenden.

Auf der Seite Formularaktionen definieren können Sie definieren, welche Aktionen vom Single Sign-On Plug-in ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular gesendet werden können.

Am oberen Rand werden alle Anmeldeinformationen des Benutzers angezeigt, die dem betreffenden Formular zugeordnet sind.

	Anmeldeformular	Kennwortänderungsformular	Formular für eine erfolgreiche Kennwortänderung	Formular für eine fehlgeschlagene Kennwortänderung
Username/ID	X	X	X	X
Password	X		X	X

Altes Kennwort Neues Kennwort	Anmeldeformular	Kennwortänderungsformular X X	Formular für eine erfolgreiche Kennwortänderung	Formular für eine fehlgeschlagene Kennwortänderung
Kennwort bestätigen		X		
Benutzerdefiniertes Feld 1	X		X	X
Benutzerdefiniertes Feld 2	X		X	X
OK	X	X	X	X

Unten auf der Seite wird die definierte Aktionsfolge angezeigt.

Auf dieser Seite werden die Aktionen definiert, die von der Plug-in-Software ausgeführt werden, um die erforderlichen Anmeldeinformationen des Benutzers erfolgreich an das identifizierte Formular zu senden.

Für zahlreiche Webanwendungen ist nur Folgendes erforderlich:

1. Klicken Sie auf den Link Festlegen/Ändern, der bestimmten Anmeldeinformationen des Benutzers zugeordnet ist. Das Dialogfeld Feldtext konfigurieren wird geöffnet, in dem das Feld identifiziert wird, das diese Anmeldeinformationen erhält. Bei bereits geöffnetem Formular enthält dieses Dialogfeld alle möglichen Steuerelemente für den Feldtyp, der den ausgewählten Anmeldeinformationen des Benutzers oder der Sendeoption zugeordnet ist.
   Wenn das Formular für die Anmeldeinformationen für die Anwendung nicht geöffnet ist, starten Sie die Anwendung und rufen Sie das richtige Formular für die Anmeldeinformationen des Benutzers auf. Wählen Sie dann Aktualisieren. Nach der Auswahl des Anwendungsformulars werden in diesem Dialogfeld die möglichen Feldtypen angezeigt, die den ausgewählten Anmeldeinformationen des Benutzers entsprechen.

2. Wählen Sie den Feldtyp aus, der die Anmeldeinformationen erhält. Bei der Auswahl der verschiedenen möglichen Optionen wird der zugeordnete Feldtyp in der Anwendung markiert, damit der Feldtyp, der die identifizierten Anmeldeinformationen des Benutzers bzw. die Schaltfläche "Senden" erhalten soll, leichter identifiziert werden kann.
3. Wiederholen Sie diese Aktion für alle Anmeldeinformationen des Benutzers, die für das Formular erforderlich sind, sowie für die erforderliche Schaltfläche zum Senden des Formulars.
   Für einige Formulare sind Domänen- oder andere benutzerdefinierte Anmeldeinformationen erforderlich, die erfolgreich gesendet werden müssen, um das Formular zu verarbeiten. Zwei benutzerdefinierte Felder sind verfügbar, um diese Anforderungen zu erfüllen. Weisen Sie diesen Feldern die Sonderanmeldeinformationen zu. Die diesen Feldern zugeordneten Namen werden auf der Seite Benutzerdefinierte Felder benennen des Assistenten für Anwendungsdefinitionen nach der Definition des Formulars festgelegt.

   Hinweis: Nicht alle Anmeldeinformationen, die oben auf der Seite Formularaktionen definieren angegeben sind, müssen konfiguriert werden.

Nachdem Sie definiert haben, welche Formularfelder die identifizierten Anmeldeinformationen des Benutzers erhalten sollen und welche Schaltfläche zum Senden des Formulars ausgewählt werden soll, ist für viele Webanwendungen die Definition der Formularaktionen abgeschlossen und Sie können mit der nächsten Seite im Assistenten fortfahren.

Für einige Formulare sind jedoch weitere Informationen, Schritte, Sondertasten oder andere Aktionen erforderlich, um eine Aufgabe zur Verwaltung der Anmeldeinformationen erfolgreich abzuschließen. Klicken Sie für diese Formulare auf Aktionseditor, um das Dialogfeld Aktionseditor zu öffnen.

Definieren von Aktionsfolgen für Webformulare mit dem Aktionseditor

Auf der Seite Formularaktionen definieren definieren Sie die Aktionen, die von der Plug-in-Software ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular für die Verwaltung der Benutzerinformationen gesendet werden können.

Für viele Webanwendungen reichen die grundlegenden Informationen aus, die im Assistenten für Formulardefinitionen gesammelt werden, um das Formular zu definieren. Für einige Formulare sind jedoch weitere Informationen, Schritte, Sondertasten oder andere Aktionen erforderlich, um eine Aufgabe zum Verwalten von Anmeldeinformationen des Benutzers abzuschließen. Klicken Sie für diese Formulare auf der Seite Formularaktionen definieren auf Aktionseditor, um das Dialogfeld Aktionseditor zu öffnen.

Das Dialogfeld Aktionseditor enthält Folgendes:

- Aktionen auswählen
  Zeigt alle verfügbaren Aktionsfolgeaktionen an:
- Aktionen konfigurieren
  Definieren aktionsspezifischen Optionen in der Aktionsfolge.
- Aktionsfolgen
  Zeigt die Reihenfolge an, in der definierte Aktionen ausgeführt werden müssen, um das spezifische Formular zum Verwalten von Anmeldeinformationen des Benutzers zu verarbeiten.

Für Webdefinitionen geben Sie auf der Seite Sonstige Einstellungen konfigurieren an, ob die Plug-in-Software die Schaltfläche "Senden" automatisch aktiviert, oder ob der Benutzer auf die Schaltfläche klicken muss.

Wählen Sie Dieses Formular automatisch senden, um das Formular ohne Benutzereingriff zu senden.

Dialogfeld "Erweiterte Einstellungen" für Webanwendungen

Jul 22, 2016

Einige Webanwendungen verwenden dynamische URLs. In diesem Fall müssen zusätzliche Formulardefinitionskriterien (so genannte Erkennungszuordnungseinträge) verwendet werden, um ein bestimmtes Formular zum Verwalten von Anmeldeinformationen des Benutzers eindeutig zu identifizieren.

Diese Erkennungszuordnungen werden im Dialogfeld Zuordnungsdetail definiert und werden im Dialogfeld Erweiterte Einstellungen angezeigt. Klicken Sie zum Öffnen des Dialogfelds Zuordnungsdetail auf der Seite Sonstige Einstellungen konfigurieren auf Erweitert, um das Dialogfeld Erweiterte Einstellungen zu öffnen, und klicken dann auf Hinzufügen.

Definieren Sie mit den Optionen und Steuerelementen im Dialogfeld Zuordnungsdetail die Kriterien, die zum eindeutigen Identifizieren eines bestimmten Formulars zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden. Bei dieser Methode wird der mit Tags markierte Inhalt des HTML-Formulars, mit dem eine bestimmte Aktion zum Verwalten von Anmeldeinformationen des Benutzers ausgeführt werden soll, nach bestimmten Werten durchsucht. Sie müssen lediglich so viele Zuordnungsbedingungen definieren, wie für die Identifizierung des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.

Geben Sie im Feld "Suchen" den Typ des Webelements ein, den Sie zuordnen möchten. Wenn das Element nicht gefunden wird, erweitern Sie den Abschnitt "Erweiterte "Einstellungen" und identifizieren Sie das Element manuell.

Der Abschnitt Zusätzliche Einstellungen ist wie folgt unterteilt:

- Tag
  In diesem Feld suchen Sie das angegebene HTML-Tag. Wenn die bestimmte Instanz des Tags bekannt ist, aktivieren Sie Diese Instanz zuordnen und geben die Instanz im Dokument an, die Sie verwenden möchten. Wenn keine bestimmte Instanz identifiziert ist, werden alle Instanzen im Dokument ausgewertet. Sie müssen nur den Tag und nicht das Trennzeichen angeben (beispielsweise p statt

). Wählen Sie nach Möglichkeit das Tag aus, das dem zuzuordnenden Inhalt am nächsten ist.

  Hinweis: Da die Option Diese Instanz zuordnen je nach Browser variieren kann, sollten Sie dieses Feature nur bei Bedarf verwenden und die Konfiguration eingehend testen.
- Werttyp
  In diesem Bereich definieren Sie die Zuordnungskriterien. Wählen Sie eines der folgenden Kriterien aus:

Kriterien	Beschreibung
Text	Beliebiger Text im HTML-Code
HTML	Beliebiger bestimmter Code im angegebenen Tag
Attribut	Jedes Attribut des HTML-Codes (z B. Attribut "Name" oder ein Formulartag)

- Wert
  Geben Sie in dieses Feld den Zuordnungswert ein. Aktivieren Sie Ganzen Wert zuordnen, um eine strenge Wertzuordnung zu erzwingen (jeder nicht angegebene Text im Tagelement lässt die Zuordnung fehlgeschlagen). Geben Sie alle

Trennzeichen und Anführungszeichen ein, die auftreten können.

Hinweis: Ganzen Wert zuordnen sollte nur aktiviert werden, wenn es mehrere Instanzen eines ähnlichen Zuordnungskriteriums gibt.

- Operator
  In diesem Bereich können Sie definieren, in welcher Beziehung dieser Zuordnungseintrag zu anderen Einträgen auf diesem Formular steht. Die folgenden Optionen sind verfügbar:

Optionen	Beschreibung
UND	Wählen Sie diese Option aus, wenn nicht nur dieser Zuordnungseintrag, sondern mehrere Zuordnungen erforderlich sind, um das Formular zu identifizieren. Wenn Sie diese Option auswählen, wird das aktuelle Zuordnungsergebnis mit dem nächsten Zuordnungsergebnis verglichen. Wenn beide zutreffen, ist die Zuordnung erfolgreich.
ODER	Wählen Sie diese Option aus, wenn diese Zuordnung ausreicht, um das Formular zu identifizieren. Wenn Sie diese Option auswählen, wird das aktuelle Zuordnungsergebnis mit dem nächsten Zuordnungsergebnis verglichen. Wenn eins der beiden zutrifft, ist die Zuordnung erfolgreich. Diese Option wird für Definitionen mit Einzelzuordnung verwendet.
NICHT	Verwenden Sie diesen Vorgang, um negative Logik auf den Operator anzuwenden. Dieser Operator wird verwendet, um Zuordnungskriterien zu definieren, die nicht auf der Seite angezeigt werden sollen.

Terminalemulator-Anwendungsdefinitionen

Jul 22, 2016

Mit Terminalemulator-Anwendungsdefinitionen identifizieren Sie terminalemulator-basierte Anwendungen, u a. Mainframe, AS/400, OS/390 oder UNIX. Single Sign-On bietet Single Sign-On-Funktionalität für terminalemulator-basierte Anwendungen, die HLLAPI implementieren oder über eine interne Skriptsprache verfügen, mit der ein Dialogfeld angezeigt werden kann.

Am besten (und einfachsten) können Sie die für Terminalemulator-Anwendungsdefinitionen (HLLAPI) erforderlichen Informationen sammeln, indem Sie die Anwendung starten.

Terminalemulator-basierte Anwendungsdefinitionen werden mit dem Assistenten für Formulardefinitionen erstellt. Mit dem Assistenten werden eine oder mehrere Textzeichenfolgen identifiziert, die für ein bestimmtes Formular zum Verwalten von Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) auf den Terminalemulator-Anwendungsbildschirmen vorhanden sein müssen (bzw. nicht vorhanden sein dürfen).

Zeichnen Sie beim Aufrufen des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers alle Benutzeraktionen auf, die für den Formularzugriff erforderlich sind. Diese Aktionen sind in der Formulardefinition für jedes Formular erforderlich, wenn der Assistent für Formulardefinitionen über die Konsole bzw. das Anwendungsdefinitionstool ausgeführt wird.

Nach dem Identifizieren des richtigen Formulars zum Verwalten von Anmeldeinformationen des Benutzers werden die Koordinaten der Dateneintragsfelder definiert, die zum Senden der entsprechenden Anmeldeinformationen des Benutzers an die Anwendung verwendet werden. Diese werden durch Festlegen der Aktionsfolge bzw. Tastatureingaben definiert, die zum Wechsel zwischen Feldern oder Bildschildschirmen und zur Texteingabe erforderlich sind.

Definieren von Formularen

Jul 22, 2016

Bei der Formulardefinition werden die formularspezifischen Identifizierungs- und Aktionsinformationen gesammelt. Dabei werden die folgenden Seiten des Assistenten für Formulardefinitionen für Windows-Anwendungen verwendet:

- Formular benennen
- Formular identifizieren
- Sonstige Einstellungen konfigurieren
- Einstellungen bestätigen

Klicken Sie nach Abschluss der Aktionen, die für eine bestimmte Seite erforderlich sind, auf Weiter. Mit der Schaltfläche Zurück, die normalerweise auf jeder Seite verfügbar ist, gehen Sie auf vorher konfigurierte Optionen zurück. Unter Umständen ist es jedoch erforderlich, nachfolgende Einstellungen anzupassen, wenn Sie zuvor konfigurierte Optionen ändern.

Beim Erstellen von Anwendungsdefinitionen für Terminalemulatoranwendungen wird die Seite Formular benennen des Assistenten für Formulardefinitionen für Folgendes verwendet:

- Zuweisen eines benutzerdefinierten Namens für das zu erstellende Formular
- Identifizieren des zu erstellenden Formulartyps

Bedenken Sie, dass der Name, den Sie dem Formular zuweisen, auf der Seite Formulare verwalten des Assistenten für Anwendungsdefinitionen angezeigt wird. Weisen Sie daher einen aussagekräftigen Namen für den zu definierenden Formulartyp zu.

Verschiedene Standardformulartypen zum Verarbeiten von Anmeldeinformationen des Benutzers können mit dem Assistenten für Formulardefinitionen definiert werden. Dazu gehören:

- Anmeldeformular
  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.

- Kennwortänderungsformular
  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- Formular für eine erfolgreiche Kennwortänderung
  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- Formular für eine fehlgeschlagene Kennwortänderung
  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwortänderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Wenn der verwendete Terminalemulator mehr als eine Anmeldungs- oder Kennwortänderungsseite anzeigt, müssen Sie für jede Seite ein Formular erstellen.

Beim Erstellen von Anwendungsdefinitionen für Terminalemulatoranwendungen (HLLAPI) werden auf der Seite Formular identifizieren die Informationen eingegeben, die erforderlich sind, damit das zu definierende Formular von der Single Sign-On Plug-in-Software eindeutig erkannt wird.

Terminalemulator-basierte Anwendungen werden durch das Suchen von Textzeichenfolgen identifiziert, die an bestimmten Stellen in Zeilen oder Spalten auf dem Bildschirm der Terminalemulatoranwendung angezeigt werden. Es müssen nur so viele Textzeichenfolgezuordnungen definiert werden, wie für eine eindeutige Identifizierung des Hosts erforderlich sind.

Hinzufügen eines qualifizierenden Eintrag für eine Textzuordnung

1. Stellen Sie sicher, dass die Terminalemulatoranwendung gestartet ist, und dass Sie die Textzeichenfolgen ermittelt haben, mit denen die Zielanwendung eindeutig festgelegt wird.
2. Klicken Sie im Assistenten für Formulardefinitionen auf der Seite Formular identifizieren auf Hinzufügen, um der Liste der Textzuordnungseinträge einen Eintrag hinzuzufügen, mit dem die Anwendung qualifiziert wird. Das Dialogfeld Text für Zuordnung wird geöffnet.
3. Geben Sie die Felder im Dialogfeld Text für Zuordnung ein:
   - Textzeichenfolge
     Geben Sie den genauen Text ein, der zur Identifizierung der Anwendung verwendet werden soll.
   - Zeile
     Geben Sie die genaue Zeilennummer für die Zeichenfolge ein.
   - Spalte
     Geben Sie die genaue Spaltennummer für die Zeichenfolge ein.

   Hinweis: Wenn die Terminalemulatoranwendung von der Plug-in-Software durchsucht wird, wird im Bildschirm nach der exakten Textzeichenfolge in der definierten Zeile und Spalte gesucht. Wenn der Text unter den definierten Koordinaten nicht genau mit dem angegebenen Text übereinstimmt, wird der Bildschirm ignoriert.
4. Klicken Sie auf OK. Der definierte Eintrag unter Text für Zuordnung wird auf der Seite Formular identifizieren angezeigt.

Oft müssen zur Identifizierung des fehlerfreien Starts der Ziel-Terminalemulatoranwendung mehrere Textzeichenfolgen definiert werden. Wiederholen Sie Schritte 2 und 4 für jede Zeichenfolge, wenn mehrere Zeichenfolgen unter Text für Zuordnung erforderlich sind.

Auf der Seite Regeln für Felderkennung einstellen werden der Speicherort und die Tastenaktionen identifiziert, die zum Verwalten des zu definierenden Formulars für Anmeldeinformationen des Benutzers erforderlich sind.

Dabei sollen Feldeingaben erstellt werden, mit denen festgelegt wird, welche Anmeldeinformationen des Benutzers verarbeitet werden, an welcher Stelle sie auf dem Bildschirm eingefügt werden (Zeilen- und Spaltenkoordinaten) und welche Tastatureingaben zum Bewegen des Mauszeigers zu den nächsten Anmeldeinformationen bzw. zur nächsten Sendeaktion erforderlich sind.

Hinzufügen einer Feldeingabe

1. Klicken Sie auf Hinzufügen, um das Dialogfeld Feld definieren zu öffnen.

2. Füllen Sie die folgenden Felder im Dialogfeld Feld definieren aus:
   - Feldfunktionen
     Wählen Sie im Listenfeld die Anmeldeinformationen des Benutzers aus, die gesendet werden sollen.
   - Zeile
     Geben Sie die genaue Zeilennummer für die Zeichenfolge ein.
   - Spalte
     Geben Sie die genaue Spaltennummer für die Zeichenfolge ein.
   - Tasten nach
     Geben Sie die Tastencodes ein, die erforderlich sind, um zum nächsten Anmeldeinformationsfeld zu wechseln oder um eine Sendeaktion auszuführen.

   Hinweis: Wählen Sie den Link "Virtuelle Tastencodes" aus, um Hilfeinformationen zu gültigen Tastencodes anzuzeigen.
3. Klicken Sie auf OK. Die definierte Feldeingabe wird auf der Seite Regeln für Felderkennung einstellen angezeigt.
4. Wiederholen Sie die Schritte 1 bis 3 für alle Anmeldeinformationen für Benutzer, die für das Formular definiert werden müssen.
5. Die auf der Seite Regeln für Felderkennung einstellen angezeigten Feldeingaben werden entsprechend ihrer Position auf der Seite von oben nach unten verarbeitet. Ordnen Sie die Einträge mit den Pfeiltasten "Auf" und "Ab" in der Reihenfolge an, die für die Verarbeitung des Formulars für Anmeldeinformationen des Benutzers erforderlich ist.

Die Seite Sonstige Einstellungen konfigurieren enthält erweiterte Einstellungsoptionen für das zu definierende Formular. Folgende Optionen sind möglich:

- Definieren einer anfänglichen Verzögerung bei der Formularverarbeitung
- Definieren der erforderlichen Tastatureingaben zum Aufrufen des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers
- Definieren der Kriterien für eine Zuordnung von Textzeichenfolgen, sodass sie nicht von der Plug-In-Software verarbeitet werden

Wenn das Formular zum Verwalten der Anmeldeinformationen des Benutzers noch weiter konfiguriert werden muss, klicken Sie auf Erweitert, um das Dialogfeld Erweiterte Einstellungen zu öffnen.

Erweiterte Einstellungen für Terminalemulatoranwendungen

Jul 22, 2016

Für einige Terminalemulatoranwendungen ist eine zusätzliche Konfiguration erforderlich, um sicherzustellen, dass das richtige Formular zum Verwalten von Anmeldeinformationen des Benutzers identifiziert wird. Beispiele:

- Festlegen einer Wartezeit zum Starten der Terminalemulatoranwendung, bevor versucht wird, die Anwendung zu identifizieren
- Verarbeiten einer Reihe von Tastatureingaben zum Aufrufen der Erstanmeldungs- oder Kennwortänderungsseite
- Ignorieren einer Seite bei der Verarbeitung, wenn bestimmter Text angezeigt wird

Wenn erweiterte Konfigurationseinstellungen für das Formular zum Verwalten der Anmeldeinformationen des Benutzers benötigt werden, klicken Sie auf der Seite Sonstige Einstellungen konfigurieren im Assistenten für Formulardefinitionen auf Erweitert, um das Dialogfeld Erweiterte Einstellungen zu öffnen.

Das Dialogfeld Erweiterte Einstellungen enthält zwei Konfigurationsseiten, die über den linken Seitenbereich aufgerufen werden:

- Aktivieren Sie die Option Zusätzliche Einstellungen für Hostformular, um auf die Optionen für Zusätzliche Einstellungen zuzugreifen:
  - Feldeingaben verzögern (ms): Geben Sie die Verzögerung für den Abschluss des Ladevorgangs der Anwendung in Millisekunden ein, bevor das Formular verarbeitet wird.
  - Tasten vorher: Geben Sie die virtuellen Tastencodes ein, die eingegeben werden müssen, um auf das erste Feld des Formulars zum Verwalten von Anmeldeinformationen des Benutzers zuzugreifen, das verarbeitet wird. Wählen Sie den Link Virtuelle Tastencodes, um die Hilfe für die gültigen Tastencodes anzuzeigen.
- Aktivieren Sie die Option Zuordnung ignorieren, um auf die Option Textzuordnung, die das Senden von Anmeldeinformationen beendet zuzugreifen. Mit dieser Option können Textzeichenfolgen definiert werden, die auf der Anwendungsseite für Formulare angezeigt werden, die zu ignorieren sind.

Überlegungen zu Terminalemulator-Anwendungsdefinitionen

Jul 22, 2016

Berücksichtigen Sie die folgenden Faktoren, wenn Sie Anwendungsdefinitionen für Terminalemulator (HLLAPI) definieren:

- Für jede Benutzerkonfiguration mit Terminalemulatoranwendungen muss die Unterstützung von Terminalemulationsprogrammen aktiviert sein.
- Stellen Sie sicher, dass der Terminalemulator HLLAPI-kompatibel ist.
- Stellen Sie sicher, dass das Terminalemulatorprogramm in der Datei mfrmlist.ini der Plug-in-Software definiert ist.
- Sparen Sie Zeit, indem Sie einen Terminalemulator verwenden, in dem die Zeilen- und Spaltenkoordinaten der Mauszeigerposition angezeigt werden. Damit erkennen Sie leichter die Position des Textes und der Felder für die Identifizierung der Hostanwendung und der zugehörigen Anmeldeformulare.
- Für die HLLAPI-Erkennung muss der Terminalemulator für jede Sitzung einen Kurznamen festlegen. Die Plug-in-Software kann eine Anwendung nicht ohne den Kurznamen der Terminalemulatorsitzung erkennen.
- Die Dokumentation für die Terminalemulatoranwendung enthält unter Umständen eindeutige Kennungen (z. B. Bildschirmnummern) für die Bildschirme, die zum Senden der Anmeldeinformationen des Benutzers verwendet werden. Verwenden Sie in diesem Fall die Bildschirmnummer als eindeutige Kennung, um sicherzustellen, dass die Anmeldeinformationen für das richtige Formular von der Plug-in-Software identifiziert und gesendet werden.

Unterstützung für Terminalemulatoren

Jul 22, 2016

Die unterstützten Terminalemulatoren sind in der Datei Mfrmlist.ini enthalten. Diese Datei umfasst alle Terminalemulatoren, die von Citrix getestet wurden.

Die Liste kann um weitere Terminalemulatoren erweitert werden. Neue Definitionen sollten jedoch getestet und geprüft werden, bevor Sie sie in Ihre Produktionsumgebung integrieren. Im Folgenden finden Sie einen Beispielabschnitt dieser Datei:

```
[Emulators] Ver=20021101 EMU1=Rumba6 EMU2=Attachmate myExtra! EMU3=Attachmate Extra! 6,3 EMU4=Attachmate Extra! 6,4 EMU5=Attachmate Extra! 6.5 EMU7=Attachmate Extra! 7.1 EMU8=Re
```

Die Terminalemulatoreinträge im Abschnitt [Emulators] der Datei Mfrmlist.ini müssen numerisch von "EMU1" bis "EMU99" geordnet sein. Jede Unterbrechung der Reihenfolge führt dazu, dass der Prozess Ssomho.exe beendet wird, bevor alle Einträge gelesen wurden.

Durch Entfernen oder Auskommentieren nicht verwendeter Terminalemulatoren kann der Startprozess verbessert werden. Ssomho.exe verschwendet dann keine Ressourcen oder Zeit mit der Suche nach dem Speicherort nicht benötigter HLLAPI-DLLs.

Zum Auskommentieren eines Eintrags verschieben Sie den entsprechenden Eintrag an das Ende der Liste, setzen Sie vor den Eintrag ein Semikolon und nummerieren die restlichen EMU-Einträge neu, sodass kein Nummerierungswert ausgelassen wird.

Single Sign-On kann die Datei mfrmlist.ini nicht global aktualisieren. Sie müssen die Datei daher nach dem Installieren des Plug-ins manuell überschreiben. Bei großen Bereitstellungen sollten Sie die Verwendung von Batchdateien oder Skripten erwägen, die über eine System Management Server (SMS)-, CA-Unicenter- oder Active Directory-Softwareinstallation ausgeführt werden.

Felddefinitionen in Mfrmlist.ini

Jul 22, 2016

Terminalemulatoren, die der Datei Mfrmlist.ini hinzugefügt wurden, funktionieren nur, wenn sie dem HLLAPI-Standard entsprechen. Die Felddefinitionen für die Datei Mfrmlist.ini können Sie der Tabelle unten entnehmen. Wenn Sie eine Terminalemulatordefinition hinzufügen müssen, erkundigen Sie sich beim Hersteller des Terminalemulators, ob der Terminalemulator HLLAPI unterstützt, und besorgen Sie sich dort die richtigen Felddefinitionseinträge. Um festzustellen, ob ein Terminalemulator mit Single Sign-On funktioniert, testen Sie ihn außerhalb der Produktionsumgebung.

Feld	Definitionen
[EmulatorName]	Der Wert für "EmulatorName" muss mit dem Wert der Zeile "EMUnn=EmulatorName" im Abschnitt "[Emulators]" übereinstimmen.
GroupName	Nur für den internen Gebrauch.
DisplayName	Anzeigename des Terminalemulators. Einer von zwei Parametern, der verwendet wird, wenn ein neuer Prozess für die Sitzung initiiert wird. Muss innerhalb der Datei Mfrmlist.ini eindeutig sein.
RegistryLoc	Registrierungsschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE, der auf den Pfad verweist, in dem die HLLAPI-DLL gespeichert ist. Wenn das Programm diese Information nicht unter HKEY_LOCAL_MACHINE\SOFTWARE speichert, verwenden Sie statt der Einstellung "RegistryLoc" die Einstellung "ExplicitPath". Wenn sowohl die Einstellung "RegistryLoc" als auch die Einstellung "ExplicitPath" definiert wurde, hat die Einstellung "ExplicitPath" Vorrang.
ExplicitPath	Expliziter Pfad zu der HLLAPI-DLL-Datei, die dieser Emulator verwendet. Diese Einstellung wird anstelle der Einstellung "RegistryLoc" verwendet, wenn das Emulatorprogramm den Speicherort der HLLAPI-DLL nicht in der Systemregistrierung speichert. Wenn sowohl die Einstellung "RegistryLoc" als auch die Einstellung "ExplicitPath" definiert wurde, hat die Einstellung "ExplicitPath" Vorrang.
ValueName	Name des Wertes im Schlüssel "RegistryLoc", der den tatsächlichen Pfadwert enthält.
DLLFile	Name der HLLAPI-DLL-Datei.
StripFileName	Gibt an, dass der in ValueName gespeicherte Wert einen umgekehrten Schrägstrich (\) enthält, der beim Zusammenstellen des HLLAPI-DLL-Pfades aus den Einträgen ValueName und DLLFile entfernt werden muss.
IntSize	Definiert die vom Terminalemulator unterstützte Ganzzahlgröße (16 Bit oder 32 Bit).
WindowClass	Fensterklassenname für den Terminalemulator. Wird mit der Single Sign-On Console bzw. dem Anwendungsdefinitionstool abgerufen.

Feld	Definitionen
WindowTitle	Teil des Fenstertitels, mit dem Single Sign-On feststellen kann, dass dieses Fenster mit dem Terminalemulator verknüpft ist. Muss mindestens ein Wort enthalten. Dieses wird immer im Fenstertitel angezeigt. Auf beiden Seiten des Textes werden Platzhalterzeichen angenommen.
UseSendKeys	Weist Single Sign-On an, für die Kommunikation mit dem Terminalemulator SendKeys zu verwenden. Die Option ist nicht mit der für Windows-Anwendungen verwendeten Option identisch.

Erstellen von Benutzerkonfigurationen

Oct 05, 2015

Mit Benutzerkonfigurationen können Sie das Verhalten und die Darstellung der Plug-In-Software für Benutzer steuern. Das Erstellen einer oder mehrerer Benutzerkonfigurationen ist der letzte Schritt, den Sie ausführen müssen, bevor Sie die Single Sign-On Plug-in-Software den Benutzern in der Umgebung bereitstellen. Es können jedoch auch nachträglich noch jederzeit Benutzerkonfigurationen hinzugefügt oder bearbeitet werden.

Eine Benutzerkonfiguration ist eine eindeutige Zusammenstellung von Einstellungen, Kennwortrichtlinien und Anwendungen, die Sie auf Benutzer anwenden, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind.

Eine Benutzerkonfiguration beinhaltet Folgendes:

- Benutzer, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind.
  Wichtig: Verteilergruppen und lokale Gruppen der Domänen im gemischten Modus von Active Directory werden nicht unterstützt.
- Lizenztyp und für die Benutzer geltende Einstellungen (Lizenzierungsmodell: Gleichzeitige oder benannte Benutzer).
- Datenschutzmethoden.
- Erstellte Anwendungsdefinitionen, die Sie bei der Erstellung einer Benutzerkonfiguration in einer Anwendungsgruppe zusammenfassen können.
- Kennwortrichtlinien, die für bestimmte Anwendungsgruppen gelten.
- Konto-Self-Service-Features (Entsperren des Kontos und Zurücksetzen des Kennworts) und Schlüsselverwaltungsoptionen (Verwendung von alten Kennwörtern, Sicherheitsfragen und automatische Schlüsselverwaltung).
- Einstellungen für Optionen wie z. B. Provisioning von Anmeldeinformationen und Anwendungssupport.

Vor dem Erstellen von Benutzerkonfigurationen müssen Sie Folgendes erstellt bzw. definiert haben:

- Zentraler Speicher
- Anwendungsdefinitionen
- Kennwortrichtlinien
- Sicherheitsfragen

Sie müssen Benutzerkonfigurationen erstellen, bevor Sie die Single Sign-On Plug-in-Software den Benutzern bereitstellen. Unter anderem werden in einer Benutzerkonfiguration der Lizenzserver und die Lizenzierungsinformationen festgelegt, die die Plug-in-Software für den Betrieb benötigt.

Weitere Informationen zu den Standardeinstellungen und Details finden Sie in den Abschnitten
— Single Sign-On - Einstellungsreferenz > Benutzerkonfigurationen
.

In Umgebungen mit einem Active Directory-basierten zentralen Speicher und mehreren Domänencontrollern können Sie auswählen, an welchen Domänencontroller eine Benutzerkonfiguration beim Schreiben in den zentralen Speicher gebunden werden.

Durch diese Bindung werden die durch die Active Directory-Replikation verursachten Synchronisierungsverzögerungen verringert. Diese Verzögerungen können auftreten, wenn Benutzer gleichzeitig an mehreren Active Directory-Standorten auf Single Sign-On zugreifen.

Bei der Discovery, die über die Konsole gestartet wird, ermittelt Single Sign-On alle Domänencontroller in der Domäne. Anschließend können Sie die erstellten Benutzerkonfigurationen an bestimmte Domänencontroller binden, indem Sie den jeweiligen Controller bei der Erstellung der Benutzerkonfiguration auswählen.

So können Sie zum Beispiel festlegen, dass die Benutzer im lokalen Netzwerk an einen Domänencontroller gebunden werden. Nach der Angabe eines Domänencontrollers binden sich Benutzer bei der nächsten Anmeldung an Single Sign-On an diesen Domänencontroller.

In der Standardeinstellung binden sich Benutzer an jeden nicht schreibgeschützten Domänencontroller, wenn Sie nicht einen Domänencontroller festlegen. Sie können die Einstellung für den Domänencontroller jederzeit ändern, ohne die Integrität der Benutzerdaten zu gefährden, indem Sie die Benutzerkonfiguration ändern.

Hinweis: Stellen Sie bei der Auswahl eines Domänencontrollers sicher, dass die verfügbaren Ressourcen auf dem Domänencontroller den Datenverkehr handhaben können, den Benutzer generieren, wenn sie zu Zeiten starker Auslastung eine Verbindung mit dem Domänencontroller herstellen.
Wenn der angegebene Domänencontroller nicht verfügbar oder offline ist, verwendet die Plug-in-Software die Benutzerdaten aus dem lokalen Speicher (d. h. die Benutzerdaten auf dem Computer des Benutzers). Wenn der Domänencontroller über einen bestimmten (von Ihnen festgelegten) Zeitraum offline ist, können Sie in der Konsole die Aufgabe Benutzerkonfiguration bearbeiten starten und einen anderen Domänencontroller auswählen oder die Option Jeder nicht schreibgeschützte Domänencontroller aktivieren.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie eine Benutzerkonfiguration aus.
4. Klicken Sie im Menü Aktion auf Benutzerkonfiguration bearbeiten.
5. Wählen Sie links auf der Seite des Assistenten für das Bearbeiten von Benutzerkonfigurationen die Option Domänencontroller.
6. Wählen Sie einen verfügbaren Domänencontroller aus oder aktivieren Sie Jeder nicht schreibgeschützte Domänencontroller.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie im Menü Aktion auf Benutzerkonfiguration hinzufügen.

Benennen der Benutzerkonfiguration

Auf der Seite Benutzerkonfiguration benennen des Assistenten für Benutzerkonfigurationen können Sie die Benutzerkonfiguration benennen und festlegen, wie Sie diese den Benutzern zuordnen.

- Name
  Sie sollten die Benutzerkonfigurationen nach der geplanten Gruppierung der Benutzer und Zuordnung von Anwendungen benennen. Beispiel: Benutzer Marketing, Benutzer Softwareentwicklung, Benutzer Nordamerika usw.

- Benutzerkonfigurationszuordnung

Sie haben zwei Optionen: Benutzer können entsprechend einer Active Directory-Hierarchie (Organisationseinheit oder Einzelbenutzer) oder einer Active Directory-Gruppe zugeordnet werden. Bei Bedarf können Sie die Benutzerkonfiguration später einer anderen Hierarchie oder Gruppe zuordnen, indem Sie im Menü Aktion auf Benutzerkonfiguration verschieben klicken.

Wichtig: Die Organisation der Active Directory-Umgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Wenn Sie sowohl Active Directory-Hierarchien als auch Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.
Wenn ein Benutzer zu zwei verschiedenen Active Directory-Gruppen gehört und jede der Gruppen einer Benutzerkonfiguration zugeordnet ist, hat die Benutzerkonfiguration mit der höchsten Priorität Vorrang und wird verwendet.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

Angeben eines Domänencontrollers

Wenn Sie einen zentralen Speicher unter Active Directory verwenden, können Sie auf der Seite Domänencontroller angeben des Assistenten für Benutzerkonfigurationen einen verfügbaren oder Jeder nicht schreibgeschützte Domänencontroller auswählen.

Auswählen von Anwendungen und Konfigurieren von Benutzereinstellungen

Oct 05, 2015

Auf der Seite Anwendungen auswählen des Assistenten für Benutzerkonfigurationen fügen Sie die Anwendungen für die Benutzerkonfiguration hinzu. Wenn Sie auf die Schaltfläche Hinzufügen klicken, werden die bereits erstellten Anwendungsdefinitionen in einem Dialogfeld angezeigt. Diese Anwendungsdefinitionen können jetzt in einer Anwendungsgruppe zusammengefasst werden. Eine Anwendungsgruppe kann mehrere Anwendungen oder nur eine Anwendung enthalten.

Sie können auch eine Kennwortgruppe erstellen und so die Kennwortänderung automatisieren und vereinfachen. Wenn das Kennwort für eine zu einer Kennwortgruppe gehörenden Anwendungsdefinition geändert wird, stellt die Plug-in-Software sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe umgesetzt wird.

Durch die Verwendung von Kennwortgruppen kann die Plug-in-Software mehrere Anmeldeinformationen für Anwendungen verwalten, die dieselbe Authentifizierungsstelle verwenden. Wenn Sie zwei Anwendungen haben, beispielsweise eine Finanzanwendung und eine Personalanwendung, die zum Authentifizieren dieselbe Oracle-Datenbank verwenden, können Sie diese beiden Anwendungen in dieselbe Kennwortgruppe einordnen. Sobald ein Benutzer sein Kennwort für eine der Anwendungen ändert, werden die Anmeldeinformationen in der anderen Anwendung automatisch aktualisiert.

Wichtig: Stellen Sie sicher, dass alle Kennwörter in der Kennwortgruppe von derselben Authentifizierungsstelle verwaltet werden. Das Implementieren einer Kennwortgruppe ist zum Beispiel dann sinnvoll, wenn die Anwendungen in einer Kennwortgruppe dieselbe Back-End-Authentifizierungsstelle (wie z. B. eine Datenbank) verwenden, und der Benutzer für jede Anwendung die gleichen Anmeldeinformationen eingeben würde, um sich an der Datenbank zu authentifizieren. Nicht in Zusammenhang stehende Anwendungen (z. B. ein E-Mail-Programm, eine Webanwendung und ein benutzerdefiniertes Programm im Intranet, für das Single Sign-On aktiviert ist), für die ein Benutzer potenziell jeweils verschiedene Anmeldeinformationen eingeben könnte und nur durch Zufall dieselben, würden nicht in einer Gruppe zusammengefasst werden. Wenn ein Benutzer in einem solchen Fall seine Anmeldeinformationen für eine Anwendung in dieser Kennwortgruppe ändert, folgt daraus nicht zwingend, dass diese Anmeldeinformationen auch für die anderen beiden Anwendungen gültig sind.

Auf den folgenden Seiten konfigurieren Sie die Benutzereinstellungen. Weitere Informationen finden Sie in den Abschnitten *— Single Sign-On - Einstellungsreferenz > Benutzerkonfigurationen*

.

- Auf der Seite Single Sign-On Plug-in-Verhalten konfigurieren des Assistenten für Benutzerkonfigurationen legen Sie das Verhalten der Plug-in-Software für alle Benutzer fest.
- Auf der Seite Lizenzierung konfigurieren des Assistenten für Benutzerkonfigurationen wählen Sie einen Lizenzserver und ein Lizenzierungsmodell aus.
  Wichtig: Wenn Sie die Benutzerkonfiguration nachträglich bearbeiten und die Produktedition ändern, ändert sich auch das Lizenzierungsmodell. Wenn Sie zum Beispiel die Produktedition von Single Sign-On Enterprise in Single Sign-On Advanced ändern, ändert sich das Lizenzierungsmodell von "Gleichzeitige Benutzer" in "Benannte Benutzer".
- Auf der Seite Datenschutzmethoden auswählen des Assistenten für Benutzerkonfigurationen wählen Sie die Datenschutzmethoden zum Schutz der Anmeldeinformationen der Benutzer aus, je nachdem, welche Authentifizierungsmethoden die Benutzer verwenden dürfen. In einigen Umgebungen können die Benutzer mehrere

Methoden verwenden.

- Wenn Benutzer die primäre Authentifizierung ändern (z. B. ein Domänenkennwort ändern oder eine Smartcard ersetzen), können Sie auf der Seite Sekundäre Datenschutzoptionen auswählen des Assistenten für Benutzerkonfigurationen Optionen für sekundäre Datenschutzmethoden festlegen, bevor Sie die Sperrung der Anmeldeinformationen der Benutzer aufheben. Hier können Sie auch einstellen, dass die Benutzer ihre Identität nachweisen müssen, um eine höhere Sicherheit zu gewährleisten. Alternativ können Sie einstellen, dass Anmeldeinformationen automatisch wiederhergestellt werden. Dazu wird das Schlüsselverwaltungsmodul implementiert.
- Für die Optionen auf der Seite Self-Service-Features aktivieren des Assistenten für Benutzerkonfigurationen muss das Modul "Schlüsselverwaltung" installiert sein. Dieses Feature erweitert die Dialogfelder Anmelden an Windows und Sperrung des Computers aufheben um eine Schaltfläche Konto-Self-Service, mit der die Administrationskosten oder die Kosten für die Unterstützung durch den Helpdesk im Unternehmen gesenkt werden können.
- Auf den Seiten Schlüsselverwaltungsmodul und Provisioningmodul des Assistenten für Benutzerkonfigurationen müssen Sie die URL und den Dienstport für installierte Dienstmodule angeben.

Synchronisieren der Anmeldeinformationen mit der Kontozuordnung

Oct 05, 2015

In Unternehmen, in denen mehrere Windows-Domänen verwendet werden, können Benutzer daher mehrere Windows-Konten haben. Single Sign-On umfasst für die Aktivierung der Kontozuordnung den Dienst "Synchronisierung der Anmeldeinformationen".

Mit der Kontozuordnung kann sich ein Benutzer mit jedem Windows-Konto an jeder Anwendung anmelden. Da Single Sign-On normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert. Administratoren können jedoch die Kontozuordnung konfigurieren und die Anmeldeinformationen des Benutzers synchronisieren. Benutzer mit konfigurierter Kontozuordnung können mit allen Konten in der Single Sign-On-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Ohne die Kontozuordnung muss ein Benutzer, der mehrere Windows-Konten besitzt, die Anmeldeinformationen manuell für jedes Windows-Konto ändern.

Für die Konfiguration der Kontozuordnung müssen Windows-Domänenadministratoren des Unternehmens die folgenden Schritte der Reihe nach ausführen:

1. Wählen Sie eine Domäne, in der Sie das Modul "Synchronisierung der Anmeldeinformationen" installieren und ausführen, das Teil des Single Sign-On-Dienstes ist.
2. Stellen Sie das vertrauenswürdige Stammzertifikat allen Computern im Unternehmen bereit, die die Kontozuordnung verwenden.
3. Synchronisieren Sie manuell alle Anwendungsdefinitionen zwischen den Domänen.
4. Konfigurieren Sie die Benutzereinstellungen für die Kontozuordnung in anderen Domänen, die mit dem Modul "Synchronisierung der Anmeldeinformationen" verbunden sind.
5. Stellen Sie den Benutzern die Kontozuordnung als veröffentlichte Anwendung bereit.

Jeder Benutzer muss die Kontozuordnung in der Plug-in-Software aktivieren.

Wählen Sie die Domäne, die die Konten aller Benutzer im Unternehmen enthält, die die Kontozuordnung verwenden. Das Modul "Synchronisierung der Anmeldeinformationen" agiert als Netzknoten für alle Anmeldeinformationen im Unternehmen. Installieren Sie dieses Modul wie jeden anderen Single Sign-On-Dienst in dieser Domäne.

Wichtig: Wenden Sie sich an den Netzwerkadministrator, um festzustellen, ob Firewalländerungen erforderlich sind, und ob diese Änderungen die Unternehmensrichtlinien einhalten.
Erstellen oder bearbeiten Sie nach der Installation des Moduls "Synchronisierung der Anmeldeinformationen" Benutzerkonfigurationen im Citrix AppCenter, um einzelne Benutzerkonten zur Verwendung des Moduls "Synchronisierung der Anmeldeinformationen" zu berechtigen, wie nachfolgend beschrieben.

Konfigurieren der Synchronisierung der Anmeldeinformationen in der Hostdomäne

Öffnen Sie die Konsole von der Domäne, in der das Modul "Synchronisierung der Anmeldeinformationen" ausgeführt wird.

Einige Domänen können auf mehrere zentrale Speicher zugreifen. Stellen Sie sicher, dass die Konsole, die Sie verwenden, eine Verbindung zu demselben zentralen Speicher wie das Modul "Synchronisierung der Anmeldeinformationen" herstellt.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie eine vorhandene Benutzerkonfiguration aus oder erstellen Sie eine neue.
   - Beim Erstellen einer neuen Benutzerkonfiguration stehen die folgenden Optionen über die Schaltfläche Erweiterte Einstellungen auf der Seite Plug-in-Verhalten konfigurieren im Assistenten für Benutzerkonfigurationen zur Verfügung.
   - Zum Bearbeiten einer vorhandenen Benutzerkonfiguration stehen die folgenden Optionen auf der Eigenschaftenseite Benutzerkonfiguration bearbeiten zur Verfügung.
4. Klicken Sie auf Synchronisierung und wählen Sie Zugriff auf Anmeldeinfo über das Modul 'Synchronisierung der Anmeldeinformationen' zulassen.
5. Klicken Sie auf OK und wiederholen Sie die Schritte 3 und 4 für alle vorhandenen und neuen Benutzerkonfigurationen.

Manuelles Synchronisieren der Anwendungsdefinitionen zwischen Domänen

Konten können auch synchronisiert werden, wenn die Benutzerkonfigurationen unterschiedlich zugeordnet sind. Sie können z. B. eine Benutzerkonfiguration in einer Domäne einer Active Directory-Hierarchie (OU oder Benutzer) und in einer anderen Domäne einer Active Directory-Gruppe zuordnen. Solange die Namen der Anwendungsdefinitionen in jeder Benutzerkonfiguration identisch sind, werden die Anmeldeinformationen mit der Kontozuordnung synchronisiert.

Anmeldeinformationen der Benutzer werden nur für Anwendungen gemeinsam verwendet, die vom Single Sign-On-Administrator definiert wurden. Administratoren müssen sicherstellen, dass jede Anwendungsdefinition in jeder Domäne denselben Namen in jedem zentralen Speicher hat.

Beispiel: Wenn die Anwendungsdefinition für SAP in einer Domäne SAP-Anmeldung heißt, SAP in einer anderen Domäne und SAP Launch Pad in einer weiteren, werden die Anmeldeinformationen des Benutzers nicht für diese Anwendungen zwischen den Konten für diese Domäne synchronisiert.

Bei der Erstellung einer neuen domänenübergreifenden Anwendungsdefinition verwenden Sie am besten die Aufgaben Anwendungsdefinitionen exportieren und Administrative Daten importieren in der Konsole. Mit diesen Aufgaben exportieren Sie gerade erstellte Anwendungsdefinitionen, die Sie in jeden zentralen Speicher importieren. Bestehende, bereits definierte Anwendungen müssen manuell umbenannt werden.

Konfigurieren von Benutzereinstellungen für die Kontozuordnung in anderen Domänen

Installieren und öffnen Sie die Konsole auf einer Arbeitsstation in jeder Domäne, auf der das Modul "Synchronisierung der Anmeldeinformationen" ausgeführt wird. Einige Domänen haben mehrere zentrale Speicher. Stellen Sie daher sicher, dass Sie jeden zentralen Speicher konfigurieren.

Alle Domänenadministratoren müssen die Domänenbenutzer berechtigen, die Konten ihrem Hostdomänenkonto zuzuordnen. Bearbeiten Sie in der Konsole den Abschnitt "Kontozuordnung" für die entsprechenden Benutzerkonfigurationen.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie eine vorhandene Benutzerkonfiguration aus oder erstellen Sie eine neue.
   - Beim Erstellen einer neuen Benutzerkonfiguration stehen die folgenden Optionen über die Schaltfläche Erweiterte

Einstellungen auf der Seite Plug-in-Verhalten konfigurieren im Assistenten für Benutzerkonfigurationen zur Verfügung.
- Zum Bearbeiten einer vorhandenen Benutzerkonfiguration stehen die folgenden Optionen auf der Eigenschaftenseite Benutzerkonfiguration bearbeiten zur Verfügung.

4. Klicken Sie auf Kontozuordnung.
5. Wählen Sie Benutzer können Konten zuordnen.
   Die folgenden Optionen sind nicht erforderlich, ergeben jedoch eine nahtlose Benutzererfahrung.
6. Aktivieren Sie die Option Standarddienstadresse angeben und geben Sie die Adresse und den Port des Single Sign-On-Dienstes für die Domäne an, in der das Modul "Synchronisierung der Anmeldeinformationen" ausgeführt wird.
7. Deaktivieren Sie die Option Benutzer können Dienstadresse bearbeiten.
8. Aktivieren Sie die Option Standarddomäne angeben und geben Sie den Namen der Domäne ein, in der das Modul "Synchronisierung der Anmeldeinformationen" ausgeführt wird. Wenn Sie die Domäne nicht angeben, wissen die Benutzer möglicherweise nicht, welche Anmeldeinformationen für welches Domänenkonto eingegeben werden sollen.
9. Deaktivieren Sie die Option Benutzer können Domäne bearbeiten.
10. Aktivieren Sie abhängig von den Sicherheitsrichtlinien des Unternehmens Benutzer können Kennwort speichern.
11. Klicken Sie auf OK und wiederholen Sie Schritte für jede Benutzerkonfiguration.

Da diese Version des Single Sign-On Plug-ins keine Menüoption bietet, über die Benutzer die Kontozuordnung aktivieren können, stellen Sie den Benutzern ein Tool bereit, mit dem sie die Kontozuordnung als eine veröffentlichte Anwendung aktivieren können:

1. Installieren Sie das Single Sign-On Plug-in auf einem XenApp-Server.
2. Navigieren Sie zur Datei AccAssoc.exe auf dem XenApp-Server.
3. Veröffentlichen Sie die Datei AccAssoc.exe und stellen sie den Benutzern zur Verfügung.
4. Informieren Sie die Benutzer, wie sie auf die Kontozuordnung-Tool zugreifen und es verwenden.

Hinweis: Benutzer, die Single Sign-On Plug-in Version 4.8 und früher ausführen, können die Kontozuordnung über eine Menüoption im Plug-In aktivieren. Diese Benutzer müssen auf das Kontozuordnung-Tool nicht als veröffentlichte Anwendung zugreifen.

Aktivieren der Kontozuordnung im Single Sign-On Plug-in

Oct 05, 2015

Bei der Anmeldung an der Domäne, die das Modul "Synchronisierung der Anmeldeinformationen" hostet, müssen Benutzer nichts für die Aktivierung der Kontozuordnung tun. Diese Konten agieren als zentrales Repository für die Anmeldeinformationen jedes Benutzers.

Wenn sich Benutzer an anderen Domänen anmelden, können Sie die Kontozuordnung mit zwei Methoden aktivieren; dies hängt von der verwendeten Version des Single Sign-On Plug-ins ab:

- Benutzer, die diese Version des Single Sign-On Plug-ins verwenden, greifen auf die Kontozuordnung als veröffentlichte Anwendung zu. Sie veröffentlichen die Kontozuordnung und informieren die Benutzer, wie sie darauf zugreifen und das Programm verwenden.
- Benutzern, die das Single Sign-On Plug-in Version 4.8 und früher verwenden, wird jetzt eine Option Kontozuordnung unter Extras im Anmeldungsmanager der Plug-In-Software angezeigt. Benutzer müssen mit dieser Option die Kontozuordnung aktivieren.

1. Abhängig von der verwendeten Plug-in-Version greifen Benutzer auf die Kontozuordnung als veröffentlichte Anwendung zu oder wählen Extras > Kontozuordnung im Anmeldungsmanager. Das Dialogfeld Kontozuordnung wird angezeigt.
2. Benutzer wählen Kontozuordnung aktivieren.
   Hinweis: Wenn Sie die Dienstadresse für das Modul "Synchronisierung der Anmeldeinformationen" nicht angegeben haben, müssen die Benutzer die Adresse im Textfeld eingeben. Wenn das Feld nicht verfügbar ist, haben Sie diese Dienstadresse bereits bereitgestellt und die Benutzer können keinen Text in dieses Feld eingeben.
3. Benutzer klicken auf OK. Das Dialogfeld Für die Kontozuordnung authentifizieren wird angezeigt.
4. Benutzer geben den Benutzernamen und das Kennwort für das dem Benutzer zugeordnete Windows-Konto ein. Wenn die Domäne, in der das Modul zur Synchronisierung der Anmeldeinformationen installiert ist, nicht angezeigt wird, geben Sie den Wert in das Feld Domäne ein.
   Hinweis: Wenn Sie den Domänennamen eingegeben haben, können die Benutzer keinen Text in dieses Feld eingeben.
5. Benutzer klicken auf OK. Die Kontozuordnung ist jetzt aktiviert. Die Anmeldeinformationen des Benutzers werden bei der Synchronisierung der Plug-in-Software synchronisiert.

Verwalten von Benutzerkonfigurationen

Oct 05, 2015

Single Sign-On ermöglicht das Verwalten von Benutzerkonfigurationen. Sie haben folgende Möglichkeiten:

- Benutzerdaten zurücksetzen
- Benutzerdaten löschen
- Benutzer zum erneuten Registrieren auffordern
- Priorität einer Benutzerkonfiguration festlegen
- Benutzerkonfiguration verschiedenen Benutzern zuweisen
- Benutzerkonfiguration für vorhandene Benutzer aktualisieren

Zurücksetzen von Benutzerdaten

Für die Aufgabe Benutzerdaten zurücksetzen muss das Provisioningmodul installiert und konfiguriert sein.

Mit der Aufgabe Benutzerdaten zurücksetzen können Sie Benutzerdaten im zentralen Speicher zurücksetzen, wodurch der ausgewählte Benutzer auf den Originalzustand zurückgesetzt wird.

- In zentralen Speichern unter Active Directory werden die Benutzerdaten (Anmeldeinformationen, Sicherheitsfragen und Antworten usw.) gelöscht, und der Benutzer wird als zurückgesetzt gekennzeichnet.
- In zentralen Speichern auf einer NTFS-Netzwerkfreigabe werden alle Benutzerdaten gelöscht, und der Benutzer wird als zurückgesetzt gekennzeichnet.

Sie können Benutzerdaten zurücksetzen verwenden, wenn ein Benutzer die Antworten auf seine Sicherheitsfragen vergisst oder die Anmeldeinformationen eines Benutzers zurückgesetzt werden müssen, weil die Daten des Benutzers beschädigt wurden. Wenn sich der Benutzer später an der Plug-in-Software anmeldet, um eine Verbindung zum zentralen Speicher herzustellen, sind im lokalen Speicher der Anmeldeinformationen des Benutzers keine Daten mehr enthalten und der Benutzer muss sich erneut registrieren.

Diese Aufgabe kann auch verwendet werden, wenn sich ein Benutzer nicht an der Plug-in-Software anmelden kann.

Wichtig: Der Kennwortverlauf wird pro Benutzer gespeichert. Wenn Sie die Benutzerdaten für einen Benutzer zurücksetzen, wird der Kennwortverlauf entfernt, und der Kennwortverlauf kann nicht für die gelöschten Kennwörter erzwungen werden.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie im Menü "Aktion" auf Andere AufgabenBenutzerdaten zurücksetzen. Das Dialogfeld Benutzer auswählen wird angezeigt.
4. Geben Sie einen Benutzernamen in das Textfeld ein und klicken Sie auf Namen überprüfen.
5. Klicken Sie auf OK, wenn der Name bestätigt wird.
6. Wählen Sie einen Benutzer im zentralen Speicher aus und klicken Sie auf Zurücksetzen.
7. Klicken Sie auf OK. Eine Warnmeldung wird angezeigt.
8. Stellen Sie sicher, dass alle Benutzer, die Single Sign-On als eine von Citrix XenApp gehostete Anwendung ausführen, abgemeldet sind, und klicken Sie auf Weiter, um die Daten des Benutzers für das Zurücksetzen zu markieren.
   Hinweis: Sollten Benutzer nicht abgemeldet sein, klicken Sie auf Abbrechen, setzen Sie die ICA-Sitzung zurück und wiederholen Sie den Schritt.
9. Klicken Sie im Dialogfeld Benutzerdaten zurücksetzen auf OK, wenn die Informationen des Benutzers geprüft und zurückgesetzt wurden. Die Daten des Benutzers werden zurückgesetzt, wenn er sich das nächste Mal mit der Plug-in-Software an Single Sign-On anmeldet.

Löschen von Benutzerdaten

Mit der Aufgabe Benutzerdaten aus dem zentralen Speicher löschen werden alle Benutzerdaten aus dem zentralen Speicher gelöscht. Sie können die Aufgabe Benutzerdaten aus dem zentralen Speicher löschen zum Beispiel verwenden, wenn ein Benutzer das Unternehmen endgültig verlässt.

Der lokale Speicher der Anmeldeinformationen auf dem Computer des Benutzers bleibt bestehen, bis er von einem Administrator oder Operator gelöscht wird.

Wenn der gelöschte Benutzer die Plug-in-Software ausführt, wird der lokale Speicher der Anmeldeinformationen der Plug-in-Software mit dem zentralen Speicher synchronisiert, es sei denn, der lokale Speicher der Anmeldeinformationen wurde von einem Administrator oder Operator gelöscht. Und dies zu verhindern, sollten Sie den Benutzer aus dem Unternehmen löschen (z. B. aus Active Directory löschen oder deaktivieren).

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie im Menü "Aktion" auf Andere Aufgaben > Benutzerdaten aus dem zentralen Speicher löschen. Das Dialogfeld Benutzer auswählen wird angezeigt.
4. Geben Sie einen Benutzernamen in das Textfeld ein und klicken Sie auf Namen überprüfen.
5. Klicken Sie auf OK, wenn der Name bestätigt wird. Klicken Sie zur Bestätigung auf Ja. Eine Bestätigungsmeldung wird angezeigt.
6. Klicken Sie auf OK. Der Benutzer wird aus dem zentralen Speicher gelöscht.

Auffordern der Benutzer zur Neuregistrierung

Sie können einstellen, dass ein bestimmter Benutzer oder alle Benutzer die Antworten auf die Sicherheitsfragen neu registrieren müssen. Diese Features werden aus Sicherheitsgründen oder bei beschädigten Benutzerdaten verwendet.

- Sicherheitsfragenregistrierung für einen Benutzer aufheben
  Aktivieren Sie diese Option, um die Daten zu den Sicherheitsfragen eines Benutzers zu löschen. Die fragenbasierte Authentifizierung steht danach erst wieder zur Verfügung, wenn der Benutzer eine Neuregistrierung vorgenommen hat.

- Alle Benutzer zur Neuregistrierung der Sicherheitsfragen auffordern
  Aktivieren Sie diese Option, um alle Benutzer beim Start der Plug-in-Software aufzufordern, die Sicherheitsfragen und Antworten neu zu registrieren. Die Daten zu den Sicherheitsfragen bleiben erhalten und die Benutzer können mit den aktuellen Antworten noch auf die Features zugreifen, die eine fragenbasierte Authentifizierung erfordern. Die Benutzer werden wiederholt zur Neuregistrierung aufgefordert, bis sie diese Aktion ausführen.

Wenn sich ein Benutzer gegen die Neuregistrierung der Antworten entscheidet, indem er im Dialogfeld Citrix Single Sign-On-Registrierung auf "Abbrechen" klickt, kann er bis zur Neuregistrierung seiner Antworten keine Features verwenden, die eine fragenbasierte Authentifizierung erfordern, wie z. B. Konto-Self-Service.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie im Menü Aktion auf Andere Aufgaben und dann auf Folgendes:
   - Sicherheitsfragenregistrierung für einen Benutzer aufheben
     Das Dialogfeld Benutzer auswählen wird angezeigt. Geben Sie einen Benutzer ein oder wählen Sie ihn aus. Bestätigen Sie, dass Sie die Registrierung der Sicherheitsfragen für diesen Benutzer zurücksetzen möchten.

   - Alle Benutzer zur Neuregistrierung der Sicherheitsfragen auffordern

Klicken Sie auf Ja, um alle Benutzer aufzufordern, und klicken Sie dann auf OK.

Festlegen der Priorität einer Benutzerkonfiguration

Beim Erstellen oder Bearbeiten einer Benutzerkonfiguration können Sie Benutzer, die zu Active Directory-Gruppen gehören, Benutzerkonfigurationen zuordnen. Ein Benutzer in einer Gruppe kann mehreren Benutzerkonfigurationen zugeordnet sein. In einem solchen Fall können Sie festlegen, welche Benutzerkonfiguration die höchste Priorität hat.

Wichtig: Die Organisation der Single Sign-On-Benutzerumgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Das heißt, dass Benutzerkonfigurationen in der Single Sign-On-Umgebung einer Active Directory-Hierarchie (OU oder Benutzer) oder einer Active Directory-Gruppe zugeordnet werden. Wenn Sie sowohl Hierarchien als auch Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Klicken Sie im Menü Aktion auf Andere Aufgaben > Priorität für Benutzerkonfiguration festlegen. Das Dialogfeld Priorität der Benutzerkonfiguration festlegen wird angezeigt.
4. Wählen Sie eine Benutzerkonfiguration aus und verschieben Sie diese nach Wunsch mit Auf oder Ab.

Zuweisen einer Benutzerkonfiguration zu verschiedenen Benutzern

Beachten Sie, dass Sie beim Bearbeiten einer vorhandenen Benutzerkonfiguration nicht den Speicherort der Benutzerkonfiguration verändern können. Sie können einen der folgenden Vorgänge ausführen:

- Anwenden einer Benutzerkonfiguration auf zusätzliche Benutzer durch Duplizierung der Benutzerkonfiguration
- Anwenden einer Benutzerkonfiguration auf andere Benutzer durch Verschieben der Benutzerkonfiguration

Duplizieren einer Benutzerkonfiguration

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie die Benutzerkonfiguration aus.
4. Klicken Sie im Menü Aktion auf Benutzerkonfiguration duplizieren.
5. Geben Sie einen Namen für die duplizierte Konfiguration ein.
6. Geben Sie die OU, den Benutzer oder die Gruppe an, zu der/dem die Benutzer gehören, für die die Benutzerkonfiguration gelten soll.

Verschieben einer Benutzerkonfiguration zu anderen Benutzern

Eine Benutzerkonfiguration, die einer Active Directory-Gruppe zugeordnet ist, kann nicht verschoben werden. Zum Zuordnen der Benutzerkonfiguration zu einer Active Directory-Hierarchie (OU oder Benutzer) duplizieren Sie die Benutzerkonfiguration und geben Sie die gewünschte Zuordnung an.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie die Benutzerkonfiguration aus.
4. Klicken Sie im Menü Aktion auf Benutzerkonfiguration verschieben.
5. Geben Sie die OU, den Benutzer oder die Gruppe an, zu der/dem die Benutzer gehören, für die die Benutzerkonfiguration gelten soll.

Aktualisieren vorhandener Benutzerkonfigurationen

In den Versionen 4.0 und 4.1 von Password Manager wurden die Benutzer über eine Active Directory-Hierarchie (OU oder Benutzer) einer Benutzerkonfiguration zugeordnet. In Password Manager 4.5 und 4.6 sowie Single Sign-On 4.8 und 5.0 können Sie Benutzer einer Active Directory-Gruppe zuordnen.

- Wenn Sie eine vorhandene Benutzerkonfiguration verwenden, die nach Hierarchie organisiert ist, und nun Benutzerkonfigurationen erstellen, die Gruppen zugeordnet sind, und ein Benutzer beiden zugeordnet ist, hat die der Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung. In dieser Situation stellen die Benutzer ggf. ein unerwartetes Verhalten der Plug-in-Software fest. Das heißt, sie können auf Ressourcen zugreifen, die der hierarchiebasierten Benutzerkonfiguration zugeordnet sind, statt auf Ressourcen, die der gruppenbasierten Benutzerkonfiguration zugeordnet sind.
- Wenn Sie die Einstellungen in den vorhandenen hierarchiebasierten Benutzerkonfigurationen beibehalten, jedoch die Zuordnung ändern möchten, verschieben Sie die Benutzerkonfiguration zu einem anderen Benutzer. Diese Schritte gelten für hierarchiebasierte Benutzerkonfigurationen der Versionen 4.1, 4.5, 4.6, 4.8 und 5.0.

Beachten Sie die folgenden Punkte, wenn Sie vorhandene Benutzerkonfigurationen aktualisieren möchten, deren Benutzer einer Active Directory-Hierarchie zugeordnet sind:

Wenn Sie den Single Sign-On-Dienst und die Single Sign-On Console, jedoch nicht die Plug-in-Software aktualisieren, können Benutzer, deren Benutzerkonfigurationen mit Active Directory-Hierarchien (Organisationseinheiten oder Benutzer) verknüpft sind, dennoch die grundlegenden Funktionen der Plug-in-Software verwenden. Die Benutzer haben jedoch dann keinen Zugriff auf die aktuellen Single Sign-On-Features. Sie sollten die Plug-in-Software möglichst aktualisieren, damit sie mit den Versionen des Dienstes und der Konsole übereinstimmt.

Benutzerauthentifizierung und Identitätsprüfung

Oct 05, 2015

Single Sign-On hat zwei Typen der Authentifizierung:

- Primäre Authentifizierung erfolgt, wenn die Benutzer die Benutzernamen, Kennwörter und optional den Domänenname) bei der Windows-Anmeldung eingeben, um auf das Unternehmensnetz zuzugreifen. Das vorhandene Windows-Sicherheitsteilsystem ist für die Verwaltung der Netzwerkauthentifizierung zuständig.
- Die sekundäre Authentifizierung erfolgt, wenn Sie Single Sign-On zum Senden von Anmeldeinformationen konfigurieren, mit denen die Benutzer auf geschützte Ressourcen zugreifen können, für die das Single Sign-On-Feature aktiviert ist. Diese Ressourcen sind beispielsweise Unternehmensanwendungen, Webanwendungen, geschützte Felder innerhalb von Anwendungen, IP-Adressen, URLs usw.

Nach der erfolgreichen Authentifizierung am Netzwerk bezieht Single Sign-On das primäre Kennwort und weitere Variablen über die Windows-Anmeldung und erstellt mit diesen Informationen den Verschlüsselungsschlüssel, der die Anmeldeinformationen geschützt. Die Plug-in-Software ruft mit diesem Schlüssel die Anmeldeinformationen ab und entschlüsselt sie, wenn die Anmeldeinformationen von Anwendungen oder Ressourcen angefordert werden.

Wichtig: Wenn das Kennwort eines Benutzers kompromittiert ist, setzen Sie das Kennwort des Benutzers nicht nur einmal, sondern zweimal zurück, um sicherzustellen, dass das kompromittierte Kennwort nicht als altes Kennwort zur Identitätsprüfung verwendet wird. Benutzer müssen sich mit jedem der neuen Kennwörter anmelden, damit die Plug-in-Software die Änderungen aufzeichnen kann.

Bestätigen der Benutzeridentität

Wenn sich Benutzer an der Umgebung anmelden, bestätigen sie die Identität durch die Eingabe des Benutzernamens und des Kennworts oder verwenden eine Smartcard oder ein anderes Authentifizierungsgerät zur eindeutigen Prüfung der Authentizität.

In verschiedenen Fällen wird jedoch eine zweite Stufe der Authentifizierung benötigt, um zu prüfen, dass der Benutzer, der die Änderung vornimmt, auch die entsprechenden Berechtigungen hat:

Event	Beschreibung
Der Administrator ändert das Hauptkennwort eines Benutzers.	Wenn ein Administrator das primäre Kennwort eines Benutzers ändert, muss der Benutzer seine Identität bestätigen, um sicherzustellen, dass ein autorisierter Benutzer angemeldet ist.
Benutzer setzen das primäre Kennwort mit dem Konto-Self-Service zurück.	Wenn Benutzer das primäre Kennwort mit dem Konto-Self-Service zurücksetzen, müssen sie auch die Identität bestätigen. Verwenden Sie nicht die Authentifizierungsoption Benutzer zur Eingabe des alten Kennworts auffordern, wenn Sie die Self-Service-Features aktivieren.
Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.	Wenn Benutzer die Sperrung des Kontos mit dem Konto-Self-Service aufheben, müssen sie die Identität erneut bestätigen.
Benutzer ändern den Authentifizierungstyp.	Wenn Benutzer beispielsweise von der Smartcard-Authentifizierung zur kennwortbasierten Authentifizierung wechseln, müssen sie ihre Identität erneut bestätigen.

Event	Beschreibung
Das Kennwort wird auf einem Benutzergerät ohne Single Sign-On geändert.	Benutzer, die das primäre Kennwort auf einem Clientgerät ändern, auf dem die Plug-in-Software nicht ausgeführt wird, werden bei der nächsten Anmeldung an einem Clientgerät, auf dem die Plug-in-Software ausgeführt wird, zum Bestätigen der Identität aufgefordert.

Benutzer können die Identität mit den von Ihnen angegebenen Optionen (abhängig von den Unternehmensanforderungen) ändern.

Identitätsprüfung im Überblick

Single Sign-On hat zwei Methoden für die Identitätsprüfung, um sicherzustellen, dass der Benutzer autorisiert ist, Single Sign-On zu verwenden:

- Altes Kennwort
- Sicherheitsfragen

Wenn die Prüfung der Identität ausgelassen werden soll, können Sie das Feature zur automatischen Schlüsselverwaltung verwenden.

Sie können die Benutzer frei zwischen den Methoden für die Authentifizierung wählen lassen (altes Kennwort oder Sicherheitsfragen). Diese Option steht unter der Eigenschaft "Sekundäre Datenschutzmethode" in der Benutzerkonfiguration zur Verfügung.

Altes Kennwort

Bei Verwendung dieser Methode wird die Identität des Benutzers mit dem eingegebenen alten Kennwort geprüft.

Achtung: Wenn als Authentifizierungsmethode nur die Identitätsprüfung mit dem altem Kennwort zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, vom System ausgesperrt. Die Daten der Benutzer müssen aus dem zentralen Speicher und von allen Clientgeräten gelöscht werden, auf denen sie gespeichert sind. Die Benutzer müssen die Anmeldeinformationen für alle Anwendungen neu eingeben.

Sicherheitsfragen

Wenn ein Benutzer sein primäres Kennwort ändert, können Sie die Identität des Benutzers bestätigen, indem der Benutzer die Sicherheitsfragen im Fragenkatalog beantwortet, den Sie erstellen. Dieser Fragenkatalog wird beim ersten Starten der Plug-in-Software angezeigt. Benutzer beantworten die erforderliche Anzahl der Sicherheitsfragen und müssen diese Informationen bei bestimmten Kennwortänderungsereignissen erneut eingeben.

Die im Fragenkatalog enthaltenen Fragen sollten so abgefasst sein, dass nur die Person, die die Frage beantwortet, die Antwort kennt oder leicht erraten kann. Sie können die von Single Sign-On bereitgestellten Standardfragen verwenden oder eigene Fragen erstellen.

Auslassen der Identitätsprüfung

Wichtig: Die automatische Schlüsselverwaltung ist nicht so sicher wie andere Methoden zur Schlüsselwiederherstellung, z. B. Sicherheitsfragen und altes Kennwort.
Wenn Single Sign-On die Prüfung der Identität auslassen und die Verschlüsselungsschlüssel der Benutzer automatisch abrufen soll, aktivieren Sie unter "Sekundäre Datenschutzmethode" die Option Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul).

Diese Methode, die automatische Schlüsselverwaltung, steht zur Verfügung, wenn Sie das Modul "Schlüsselverwaltung" installieren und eine Benutzerkonfiguration erstellen, bei der diese Option aktiviert ist.

Bei dieser Methode melden sich die Benutzer am Netzwerk an und können sofort auf Anwendungen zugreifen, die von Single Sign-On verwaltet werden. Es müssen keine Fragen beantwortet werden. Wenn Benutzer das primäre Kennwort ändern, erkennt die Plug-in-Software die Kennwortänderungen und stellt die Schlüssel der Benutzer mit dem Single Sign-On-Dienst wieder her.

Die automatische Schlüsselverwaltung ist für die Benutzer die einfachste und schnellste Methode zum Zugreifen auf die von ihnen genutzten Anwendungen. Allerdings schützt sie nicht vor unbefugtem Zugriff, da es kein nur dem Benutzer bekanntes "Geheimnis" gibt, mit dem das Netzwerkkennwort des Benutzers geschützt wird. Um dieses potenzielle Problem zu verhindern, sollten Sie die automatische Schlüsselverwaltung zusammen mit dem Self-Service-Modul implementieren. Bei diesem Modul müssen die Benutzer die Identität mit einer fragenbasierten Authentifizierung bestätigen, wenn sie ihre primären Kennwörter zurücksetzen oder die Sperrung ihres Domänenkontos aufheben.

Benutzerseitiges Wechseln zwischen Authentifizierungsmethoden

In Single Sign-On können die Benutzer zwischen den verschiedenen primären Authentifizierungsmethoden wechseln. Single Sign-On schützt die Benutzerkennwörter mit einer eindeutigen Kopie des Sicherheitsschlüssels als Methode zur Neuauthentifizierung. Damit werden die Benutzerdaten jedes Mal, wenn der Benutzer zwischen den Authentifizierungsmethoden wechselt, freigegeben, ohne dass der Benutzer seine Identität bestätigen muss.

Die Option zur Auswahl verschiedener Authentifizierungsmethoden steht auf der Seite Datenschutzmethoden in der Benutzerkonfiguration zur Verfügung.

Beispiel:

- Ein Callcenter-Supervisor meldet sich mit den primären Anmeldeinformationen (Windows-Benutzername und -Kennwort) am Computer an. Auf dem Computer ist die Single Sign-On Plug-in-Software installiert, d. h. der Benutzer kann die Anwendungen verwenden, für die Single Sign-On aktiviert ist.
- Der Supervisor meldet sich gelegentlich mit einer Smartcard und PIN an einem gemeinsam genutzten Computer im Callcenter an und startet eine weitere veröffentlichte Anwendung über XenApp. Dieser Computer verwendet Hotdesktop, um ein schnelles Wechseln zwischen verschiedenen Benutzern mit unterschiedlichen Konten zu ermöglichen.

In Version 4.0 und 4.1 von Citrix Password Manager muss der Callcenter-Supervisor vor der Verwendung von Single Sign-On-aktivierten Anwendungen seine Identität bei jedem Wechsel der primären Authentifizierungsmethoden bestätigen. In diesem Beispiel wurden zwei primäre Authentifizierungsmethoden verwendet: zuerst ein Benutzername und ein Kennwort und dann eine Smartcard und eine PIN-Nummer. In Version 4.0 und 4.1 von Password Manager ist beim Wechsel der Authentifizierungsmethode die Wiederherstellung des Sicherheitsschlüssels und möglicherweise die Bestätigung der Identität erforderlich.

Wenn ein Benutzer zum ersten Mal eine neue Authentifizierungsmethode verwendet oder zu einer neuen wechselt, muss diese Methode zuerst registriert werden. Wird diese neue Methode jedoch später wieder verwendet, muss sie nicht erneut registriert werden (d. h. danach ist keine Schlüsselwiederherstellung mehr notwendig).

Verwalten der fragenbasierten Authentifizierung

Oct 05, 2015

Die fragenbasierte Authentifizierung bietet eine sichere Authentifizierung für Benutzer, die das primäre Kennwort in bestimmten Situationen bzw. die Authentifizierungsmethode ändern oder deren Konto gesperrt ist.

Die Verwendung von Sicherheitsfragen und fragenbasierter Authentifizierung kann den Zugriff nicht berechtigter Benutzer verhindern, da Informationen verlangt werden, die nur der Benutzer kennt. Sie sollten bei der Erstellung der Fragen darauf achten, dass nur Informationen abgefragt werden, die nicht öffentlich zugänglich sind und die nur der zu authentifizierende Benutzer wissen oder herausfinden kann. Auf diese Weise werden das Erraten der Antworten, Wörterbuchangriffe u. ä. die Sicherheit bedrohende Angriffe erschwert.

Wichtig: Wenn Sie die im Modul "Schlüsselverwaltung" von Single Sign-On enthaltenen Self-Service-Funktionen zum Zurücksetzen des Kennworts bzw. zum Entsperren des Domänenkontos verwenden möchten, müssen Benutzer die Identität beim Zurücksetzen des primären Kennworts oder beim Entsperren Domänenkontos mit der fragenbasierten Authentifizierung bestätigen.

Bestätigen der Benutzeridentität durch die fragenbasierte Authentifizierung

Verwenden Sie die fragenbasierte Authentifizierung zur Prüfung der Benutzeridentität, wenn Sie die im Modul "Schlüsselverwaltung" von Single Sign-On verfügbaren Self-Service-Funktionen zur Kennwortzurücksetzung bzw. zum Aufheben der Sperrung des Domänenkontos implementieren. Sie können die fragenbasierte Authentifizierung auch als sekundären Datenschutz wählen, wenn sich die primäre Authentifizierung für einen Benutzer ändert.

Je nach den Einstellungen in der Benutzerkonfiguration der Konsole kann es in folgenden Fällen erforderlich sein, die Identität der Benutzer zu prüfen:

- Der Benutzer ändert den Authentifizierungstyp, z. B. wenn zwischen der Authentifizierung mit Smartcard und mit Kennwort gewechselt wird.
- Der Administrator ändert das primäre Kennwort eines Benutzers.
- Benutzer setzen das primäre Kennwort mit dem Konto-Self-Service zurück.
- Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.
- Benutzer ändern das primäre Kennwort auf einem Computer, auf dem die Plug-in-Software nicht installiert ist, und melden sich dann an einem Gerät an, auf dem die Plug-in-Software installiert ist.

Hinweis: Sie können auch eine Benutzerkonfiguration erstellen, für die keine weitere Authentifizierung erforderlich ist, wenn zwischen Authentifizierungstypen gewechselt wird, weitere Informationen finden Sie unter *— Benutzerseitiges Wechseln zwischen Authentifizierungsmethoden*
.

Abhängig von der Konfiguration wird der Benutzer bei der Erstverwendung der Single Sign-On Plug-in-Software zur Beantwortung der Sicherheitsfragen aufgefordert. Wenn ein Ereignis eintritt, für das eine Prüfung der Benutzeridentität erforderlich ist, startet die Plug-in-Software den von Ihnen erstellten Fragenkatalog. Ein Fragenkatalog ist eine vorkonfigurierte Liste von Fragen, die Sie erstellen.

Jede Frage im Fragenkatalog wird auf einer einzelnen Seite angezeigt. Beispiel: Wenn der Fragenkatalog fünf Fragen enthält, werden den Benutzern fünf Seiten angezeigt, eine für jede Frage. Benutzer müssen jede Frage richtig beantworten. Abhängig von den Administratoreinstellungen müssen die Antworten genau mit den Antworten übereinstimmen (einschließlich der Groß- und Kleinschreibung und Punktierung), die Benutzer bei der Erstverwendung von Single Sign-On eingegeben haben.

Die richtige Kombination aus Fragen und Antworten bestätigt die Identität des Benutzers. Sobald eine Bestätigung erfolgt, verschlüsselt die Plug-in-Software die Schlüssel mit dem neuen primären Kennwort und speichert die sekundären Anmeldeinformationen des Benutzers.

Überlegungen

- Wenn Sie keine Antworten auf Sicherheitsfragen konfigurieren, werden Benutzer zur Eingabe des primären Kennworts aufgefordert, wenn sie das primäre Kennwort ändern und eine Anmeldung mit dem neuen Kennwort versuchen. Sie können die Benutzer frei zwischen den Methoden für die Authentifizierung der Identität wählen lassen. Diese Option ist als Teil der Eigenschaften Sekundäre Datenschutzmethode in der Benutzerkonfiguration verfügbar.
- Kombinieren Sie nicht die benutzerseitige Kennwortzurücksetzung mit der Option Benutzer zur Eingabe des alten Kennworts auffordern, sonst könnten Benutzer vom System ausgesperrt werden. Benutzer, die das Kennwort zurücksetzen, können sich in der Regel nicht an das alte primäre Kennwort erinnern und sind damit nicht in der Lage, ihre sekundären Anmeldeinformationen abzurufen.
- Mehrere Fragen geben den besten Datenschutz.
- In der Standardeinstellung werden für die fragenbasierte Authentifizierung vier Sicherheitsfragen verwendet. Sie können sich zwar auf diese vier Fragen beschränken, es wird jedoch empfohlen, eigene Sicherheitsfragen und Fragengruppen hinzuzufügen.

Wichtig: Abhängig von den Einstellungen des Administrators sind die Groß- und Kleinschreibung, Satzzeichen und Leerzeichen in der Antwort des Benutzers enthalten und müssen genau übereinstimmen, wenn der Benutzer später zur Beantwortung der ausgewählten Sicherheitsfrage aufgefordert wird.

Arbeitsablauf für die fragenbasierte Authentifizierung

Erstellen Sie die Sicherheitsfragen und machen Sie die Fragen verfügbar, bevor Sie die Plug-in-Software bereitstellen. Wenn ein Benutzer eine Frage ausgewählt hat, muss diese jederzeit zur Verfügung stehen. Wenn Sie eine Frage, die verwendet wird, ändern oder entfernen, können die Benutzer die sekundären Anmeldeinformationen erst mit der Sicherheitsfrage wiederherstellen, wenn sie sich erneut registriert haben.

1. Erstellen Sie die Sicherheitsfragen, legen Sie die Mindestlänge und die Erkennung der Groß- und Kleinschreibung fest. Diese Fragen können in den Sprachen zur Verfügung gestellt werden, die Single Sign-On unterstützt.
2. Sie können diese Fragen auch in Sicherheitsfragengruppen gruppieren. Sie können mehrere Fragen erstellen, unter denen die Benutzer auswählen können. Dies ermöglicht den Benutzern eine Frage auszuwählen, deren Antwort sie leichter behalten können. Sie können dann festlegen, wie viele Fragen von jeder Gruppe die Benutzer beantworten müssen.
3. Fügen Sie die Fragen oder Fragengruppen dem Fragenkatalog hinzu.
4. Wählen Sie maximal zwei Fragen aus, die für die Schlüsselwiederherstellung verwendet werden. Mit diesen Fragen werden die Daten für die Schlüsselwiederherstellung verschlüsselt. Die Benutzer müssen jedoch weiterhin die Fragen beantworten, die sie bei der Registrierung ausgewählt haben.
5. Sie können auch das Maskieren der Sicherheitsfragen aktivieren. Mit dieser Funktion können Sie die Benutzerantworten auf Sicherheitsfragen der fragenbasierten Authentifizierung maskieren. Wenn die Option aktiviert ist, sind die Antworten der Benutzer bei der Registrierung der Antworten und der Identitätsprüfung geschützt.
   Das Maskieren der Antworten auf Sicherheitsfragen ist nur in der Konsolen- und Plug-in-Software verfügbar, wenn Password Manager 4.6 und 4.6 mit Service Pack 1 und Single Sign-On 4.8 und 5.0 ausgeführt wird.

Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit

Single Sign-On bietet vier Standardfragen, die Sie für die Benutzerregistrierung verwenden können. Diese Fragen stehen in allen unterstützten Sprachen (Deutsch, Englisch, Französisch, Japanisch, Chinesisch (vereinfacht) und Spanisch) zur Verfügung. Citrix empfiehlt, dass Sie eigene Sicherheitsfragen erstellen und sie in jeder Sprache zur Verfügung stellen, die in

der Umgebung unterstützt wird.

Ein Unbefugter, der versucht, das Kennwort eines Benutzers zu erfahren, muss die Antworten auf alle Fragen kennen, die der Benutzer anfänglich beantwortet hat. Berücksichtigen Sie jedoch, dass es für Benutzer sehr schwierig werden könnte, die Identitäten zu bestätigen, wenn sie zu viele Fragen beantworten müssen.

Sicherheitsfragen sollten nur Informationen abfragen, die nicht öffentlich zugänglich sind und die nur der autorisierte Benutzer wissen kann. Dies erschwert das Erraten der Antworten oder Wörterbuchangriffe. Der wichtigste Faktor bei der Ermittlung der Sicherheit einer Frage ist, wie schwierig es für andere Personen ist, die Antwort zu erraten.

Gute Fragen haben ein hohes Maß für den Informationsgehalt, also Fragen, für die Folgendes gilt:

- Die Anzahl der eindeutigen Antworten ist möglicherweise sehr hoch.
- Die Wahrscheinlichkeit, eine bestimmte Antwort zu raten, ist sehr niedrig.

Aus Verwendungsgründen sollte sich der Benutzer die Frage leicht merken können, die Frage sollte aber für einen Unbefugten schwer zu erraten sein. Beispiel:

- Wie lautet der Name Ihres Lieblingsprofessors oder Lieblingslehrers?
- Wo würden Sie für den ultimativen Traumurlaub hinfahren? (Stadt, Land)
- Wie lautet der Titel Ihres Lieblingsschlagers, oder wie heißt der Künstler?
- Wie lautet der Titel Ihres Lieblingsbuchs, wie heißt der Autor?
- Wie lautet der Name Ihres Lieblingskunstwerks, des Künstlers, wo ist das Kunstwerk ausgestellt?

Bei diesen weiteren Beispielen kann es jedoch passieren, dass Benutzer mit demselben sozialen Hintergrund identische Antworten auf diese Fragen geben, auch wenn sie ihre Antworten gar nicht weitergegeben haben. Dies erhöht das Risiko von Insiderangriffen.

Vermeiden Sie das Erstellen von Fragen, die folgende Merkmale aufweisen:

- Einfache Antworten, z. B. Lieblingsfarbe
- Bekannte oder sich ändernde Informationen, z. B. Adresse

Benutzerseitiges Ändern der Antworten auf die Sicherheitsfragen

Mit Single Sign-On können Benutzer Antworten auf die Sicherheitsfragen jederzeit und ohne Hilfe des Administrators ändern.

Wenn Sie Sicherheitsfragen oder die Konto-Self-Service-Features in der Umgebung verwenden, können Benutzer, die Sicherheitsfragen und Antworten registrieren, mit der Plug-in-Software neue Antworten auf die verfügbaren Sicherheitsfragen eingeben.

Nach der erfolgreichen Eingabe der Antworten werden die Benutzer informiert, dass die neuen Antworten im zentralen Speicher gespeichert sind. Die alten Antworten sind nicht mehr gültig.

Benutzer ändern die Antworten auf die Sicherheitsfragen mit dem Assistenten für die Registrierung der Sicherheitsfragen.

Sie geben den Benutzern Zugriff auf den Assistenten für die Registrierung der Sicherheitsfragen als veröffentlichte Anwendung:

1. Installieren Sie das Single Sign-On Plug-in auf einem XenApp-Server.
2. Navigieren Sie zur Datei QBAEnroll.exe auf dem XenApp-Server.
3. Veröffentlichen Sie die Datei QBAEnroll.exe und stellen sie den Benutzern zur Verfügung.

4. Informieren Sie die Benutzer, wie sie auf den Assistenten für die Registrierung der Sicherheitsfragen zugreifen und ihn verwenden.

Hinweis: Benutzer, die das Single Sign-On Plug-In Version 4.8 ausführen, können den Assistenten für die Registrierung der Sicherheitsfragen über Extras > Sicherheitsfragenregistrierung im Anmeldungsmanager starten. Diese Benutzer müssen auf den Assistenten für die Registrierung der Sicherheitsfragen nicht als veröffentlichte Anwendung zugreifen. Benutzer, die das Single Sign-on Plug-in Version 4.6 Service Pack 1 oder früher ausführen, können auf den Assistenten für die Registrierung der Sicherheitsfragen nicht als veröffentlichte Anwendung zugreifen.

Verwalten der Fragen

Oct 05, 2015

Der Knoten "Fragenbasierte Authentifizierung" in der Single Sign-On-Komponente von Citrix AppCenter bietet einen zentralen Speicherort für die Verwaltung aller Sicherheitsfragen, die mit der Identitätsprüfung, dem benutzerseitigen Zurücksetzen des Kennworts und dem Entsperren des Kontos verbunden sind. Sie können der Liste der Standardfragen eigene Sicherheitsfragen hinzufügen sowie Fragengruppen erstellen und diese für bestimmte Benutzer verwenden.

- Wenn Sie die bestehenden Standardfragen ändern, nachdem Benutzer die Antworten gespeichert haben, sollten Sie die Bedeutung der bearbeiteten Fragen berücksichtigen. Wenn Sie eine Frage bearbeiten, müssen sich die Benutzer nicht neu registrieren. Wenn Sie jedoch die Bedeutung der Frage ändern, könnten Benutzer, die diese Frage beantwortet haben, möglicherweise nicht die richtige Antwort eingeben.
- Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Plug-in-Software starten.
- Einzelne Sicherheitsfragen können zu mehreren Sicherheitsfragengruppen gehören. Wenn Sie Sicherheitsfragengruppen erstellen, können alle erstellten Fragen in jeder Sicherheitsfragengruppe verwendet werden.

Mit diesen Schritten greifen Sie auf die Einstellungen zu, die nachfolgend beschrieben werden:

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie die Knoten Single Sign-On und Identitätsprüfung und wählen Sie den Knoten Fragenbasierte Authentifizierung.
3. Klicken Sie im Menü Aktion auf Fragen verwalten.

Erstellen neuer Sicherheitsfragen

Sie können beliebig viele Fragen erstellen und jeder Frage eine Sprache zuweisen. Sie können auch mehrere Übersetzungen einer Frage bereitstellen. Die Plug-in-Software zeigt dem Benutzer den Fragenkatalog in der Sprache an, die den Spracheinstellungen des Benutzerprofils entspricht. Wenn die Sprache nicht zur Verfügung steht, zeigt Single Sign-On die Fragen in der Standardsprache an.

Hinweis: Wenn Sie die Sprache für eine Sicherheitsfrage angeben, wird die Frage den Benutzern angezeigt, deren Betriebssystemeinstellungen für diese Sprache konfiguriert sind. Wenn die ausgewählten Einstellungen des Betriebssystems nicht mit den verfügbaren Fragen übereinstimmt, wird den Benutzern die ausgewählte Standardsprache angezeigt.

1. Wählen Sie Sicherheitsfragen.
2. Wählen Sie aus der Dropdownliste Sprache eine Sprache aus und klicken Sie auf Frage hinzufügen. Das Dialogfeld Sicherheitsfrage wird angezeigt.
3. Erstellen Sie die neue Frage im Dialogfeld Sicherheitsfrage.

Wichtig: Sie müssen mit dem Befehl Bearbeiten den übersetzten Text bestehender Fragen einschließen. Wenn Sie Frage hinzufügen auswählen, erstellen Sie eine neue Frage, die nicht mit der Originalfrage verknüpft ist.

Einstellen der Standardsprache

Den Benutzern werden die Sicherheitsfragen meistens in der Sprache angezeigt, die dem aktuellen Benutzerprofil zugeordnet ist. Wenn die Sprache nicht zur Verfügung steht, zeigt Single Sign-On die Fragen in der von Ihnen gewählten Standardsprache an.

1. Wählen Sie Fragenbasierte Authentifizierung.
2. Wählen Sie aus der Dropdownliste Standardsprache die Standardsprache aus.

Hinweis: Wenn in diesem Dialogfeld die Option "Prüfung auf Rückwärtskompatibilität durchführen" ausgewählt ist, wird sichergestellt, dass die Fragen zur Identitätsprüfung in der Plug-In-Software von Password Manager Version 4.0 und Password Manager 4.1 weiterhin angezeigt werden können.

Hinzufügen von Text für bestehende Fragen oder Bearbeiten von Text

Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Plug-in-Software starten. Wenn Sie eine Frage bearbeiten, müssen sich die Benutzer nicht neu registrieren. Wenn Sie jedoch die Bedeutung der Frage ändern, können Benutzer, die diese Frage beantwortet haben, möglicherweise nicht die richtige Antwort eingeben.
Wichtig: Passen Sie beim Bearbeiten einer vorhandenen Frage auf, dass Sie nicht die Bedeutung einer Frage ändern. Sonst können die Antworten der Benutzer bei der erneuten Authentifizierung nicht stimmen. Ein Benutzer könnte also eine andere Antwort eingeben, die nicht mit der gespeicherten Antwort übereinstimmt.

1. Wählen Sie Sicherheitsfragen.
2. Wählen Sie aus der Dropdownliste Sprache eine Sprache aus.
3. Wählen Sie die Frage aus und klicken Sie auf Bearbeiten. Das Dialogfeld Sicherheitsfrage wird angezeigt.
4. Bearbeiten Sie die Frage im Dialogfeld Sicherheitsfrage.

Erstellen einer Sicherheitsfragengruppe

Sie können mehrere Sicherheitsfragen erstellen, die Benutzer beantworten, um die Identität zu bestätigen. Jede Frage, die Sie dem Fragenkatalog hinzufügen, muss von den Benutzern beantwortet werden. Sie können diese Fragen auch in einer Sicherheitsfragengruppe zusammenfassen.

Wenn Sie beispielsweise die Fragen in einer Gruppe zusammenfassen, können Sie dem Fragenkatalog sechs Fragen hinzufügen und Benutzer können z. B. drei der sechs Fragen im Fragenkatalog beantworten. Benutzer haben dann die Flexibilität, Fragen auszuwählen und die Antworten einzugeben, die für die Prüfung der Identität verwendet werden.

1. Wählen Sie Sicherheitsfragen.
2. Klicken Sie auf Gruppe hinzufügen.
3. Geben Sie im Dialogfeld Sicherheitsfragengruppe den Namen der Gruppe ein, wählen Sie die Fragen und legen Sie die Zahl der Antworten fest, die der Benutzer beantworten muss.

Bearbeiten einer Sicherheitsfragengruppe

1. Wählen Sie Sicherheitsfragen.
2. Wählen Sie die Sicherheitsgruppe, die Sie bearbeiten möchten, und klicken Sie auf Bearbeiten. Das Dialogfeld Sicherheitsfragengruppe wird mit einer Liste von verfügbaren Sicherheitsfragen für die Gruppe angezeigt. Die Fragen, die bereits in der Gruppe eingeschlossen sind, haben ein Häkchen. In diesem Dialogfeld können Sie den Namen der Gruppe bearbeiten, der Gruppe Fragen hinzufügen und die Anzahl der Fragen von dieser Gruppe auswählen, die der Benutzer beantworten muss.

Auswählen von Fragen für die Schlüsselwiederherstellung

Sie müssen eine Frage oder zwei der Fragen auswählen, die Benutzer beantworten, um die Daten für die Schlüsselwiederherstellung zu verschlüsseln. Die Benutzer müssen die Antworten für alle Fragen eingeben, die sie bei der Registrierung beantwortet haben, mit den von Ihnen ausgewählten Fragen werden Daten bereitgestellt, die bei der Verschlüsselung und der Schlüsselwiederherstellung eingeschlossen werden.

1. Wählen Sie Schlüsselwiederherstellung.
2. Aktivieren Sie das Optionsfeld neben jeder Frage oder Fragengruppe, die Sie bei der Identitätsprüfung für die

Schlüsselwiederherstellung verwenden möchten.
3. Klicken Sie auf OK, um die Frage und die Einstellungen zu speichern. Möglicherweise werden Sie in einer Meldung aufgefordert festzulegen, ob Benutzer ihre Antworten stets neu registrieren sollen. Klicken Sie auf Ja, um eine Neuregistrierung zu erzwingen.

Aktivieren des Maskierens der Antworten auf Sicherheitsfragen

Das Maskieren der Sicherheitsfragen steht nur in den Password Manager-Versionen 4.6 und 4.6 mit Service Pack 1 und Single Sign-On 4.8 und 5.0 zur Verfügung.

Das Maskieren der Antworten auf die Sicherheitsfragen gibt ein zusätzliches Sicherheitsniveau für die Benutzer, wenn sie die Antworten auf die Sicherheitsfragen registrieren oder die Antworten bei der Identitätsprüfung eingeben. Wenn dieses Feature aktiviert ist, werden die Antworten der Benutzer, die Password Manager 4.6, Password Manager 4.6 mit Service Pack 1, Single Sign-On 4.8 oder Single Sign-On 5.0 ausführen, nicht angezeigt. Bei der Registrierung der Antworten werden die Benutzer aufgefordert, die Antworten zweimal einzugeben, um Schreib- oder Rechtschreibefehler zu vermeiden. Benutzer müssen die Antworten bei der Identitätsprüfung nur einmal eingeben, da sie zur erneuten Eingabe aufgefordert werden, wenn Fehler bestehen.

Hinweis: Antworten auf Sicherheitsfragen, die in der Agentsoftware von Password Manager 4.5 registriert wurden, können maskiert werden, wenn Sie die Software auf Single Sign-On-Version 5.0 aktualisieren. Antworten auf Sicherheitsfragen für Benutzer, die die Agentsoftware für Password Manager 4.5, 4.1 oder 4.0 verwenden, werden unabhängig von der Konsoleneinstellung immer angezeigt.

1. Wählen Sie Antworten auf Sicherheitsfragen maskieren.
2. Wählen Sie Antworten auf Sicherheitsfragen maskieren.

Aktivieren der Rückwärtskompatibilität für den Fragenkatalog

Mit dem Rückwärtskompatibilitätsmodus kann die Plug-in-Software Benutzern Fragen zur Identitätsprüfung anzeigen, die Sie in den Pasword Manager-Versionen 4.0 und 4.1 verwendet haben. Im Rückwärtskompatibilitätsmodus können Sie auch weiterhin die Standardfrage "Wie lautet Ihr Satz zur Identitätsprüfung?" verwenden. Wenn Sie ein Upgrade von Version 4.1 durchführen, werden die Fragen zur Identitätsprüfung und die Fragen, die Sie für die benutzerseitige Kennwortzurücksetzung verwendet haben, als Fragenkatalog im Dialogfeld "Fragen verwalten" angezeigt.

Wichtig: Wenn Sie Benutzerkonfigurationen erstellen und bearbeiten, sollten Sie die Rückwärtskompatibilität nicht aktivieren, wenn Sie eine neue Installation von Single Sign-On verwenden, da die Funktionalität der Plug-In-Software auf die der Produktversion 4.0 und 4.1 eingeschränkt wird. Auch sollten Sie die Rückwärtskompatibilität nicht deaktivieren, wenn Sie die Agentsoftware von Version 4.0 oder 4.1 ausführen, da Sie dann die Schlüsselwiederherstellung und Registrierungen für die benutzerseitige Kennwortzurücksetzung verhindern.
Aktivieren Sie die Rückwärtskompatibilität nicht, wenn Sie die automatische Schlüsselverwaltung verwenden. Für die automatische Schlüsselwiederherstellung müssen Benutzer keine Fragen zur Identitätsprüfung beantworten.

Für die Rückwärtskompatibilität für Version 4.0 und 4.1 muss der Fragenkatalog mindestens eine Sicherheitsfrage enthalten, die der Funktion zur benutzerseitigen Kennwortzurücksetzung zugeordnet ist.

Jede Sicherheitsfrage muss die folgenden Einstellungen enthalten:
- Deaktivierte Erkennung der Groß- und Kleinschreibung.
- Mindestlänge der Antwort ist 1.
- Fragen können nicht für die Schlüsselwiederherstellung aktiviert sein.

Prüfen auf Rückwärtskompatibilität

Sie können die Rückwärtskompatibilität prüfen, wenn Sie von einer vorherigen Version von Single Sign-On bzw. Password Manager aktualisieren:

1. Wählen Sie Fragenbasierte Authentifizierung.
2. Wählen Sie Prüfung auf Rückwärtskompatibilität durchführen und klicken Sie dann auf OK.

Single Sign-On führt die Prüfung auf Rückwärtskompatibilität aus und zeigt Fehler in einem Dialogfeld an.

Benutzerseitiges Verwalten der primären Anmeldeinformationen mit dem Konto-Self-Service

Oct 05, 2015

Sie können in den Self-Service-Features von Single Sign-On konfigurieren, dass Benutzer ohne Beteiligung des Administrators oder des Helpdeskpersonals das primäre Kennwort zurücksetzen oder die Windows-Domänenkonten entsperren können. Je nach Bedarf können Sie eine oder beide Konto-Self-Service-Features (Kennwort zurücksetzen und Entsperren des Kontos) sicher in der Single Sign-On-Umgebung implementieren.

Hinweis: Weitere Informationen zur Implementierung des Konto-Self-Service mit dem Citrix Webinterface finden Sie unter *— Webinterface*

.

Die Features des Moduls "Self-Service" werden durch die fragenbasierte Authentifizierung geschützt, die sicherstellt, dass Benutzer berechtigt sind, die Kennwörter zurückzusetzen oder das Konto zu entsperren. Bei der Erstverwendung der Single Sign-On Plug-in-Software oder der ersten Verwendung nach der Konfiguration des Konto-Self-Services müssen Benutzer von Ihnen erstellte und bei der Einrichtung von Single Sign-On ausgewählte Fragen beantworten.

Diese Sicherheitsfragen werden den Benutzern angezeigt, wenn sie das Kennwort zurücksetzen oder das Konto entsperren möchten. Nach dem richtigen Beantworten der Fragen können Benutzer das Kennwort zurücksetzen oder das Konto entsperren und müssen sich nicht an den Helpdesk oder den Administrator wenden.

Wichtig: Für das benutzerseitige Zurücksetzen des Kennworts oder dem Entsperren des Kontos müssen Sie die fragenbasierte Authentifizierung implementieren. Benutzer können diese Features nur verwenden, wenn sie Antworten auf Sicherheitsfragen registrieren. Wenn Sie die fragenbasierte Authentifizierung nicht in der Single Sign-On-Umgebung verwenden, steht das benutzerseitige Zurücksetzen des Kennworts oder das Entsperren des Kontos nicht zur Verfügung. Beachten Sie folgende Faktoren:

- Sie können die Features des Self-Service-Moduls implementieren, damit Benutzer nur in einer Active Directory-Umgebung das primäre Kennwort (Domänenkonto) zurücksetzen oder das Windows-Domänenkonto entsperren können.
- Wenn Benutzer das Anwendungskennwort mit der Single Sign-On Plug-in-Software oder das primäre Kennwort mit der Tastenkombination STRG+ALT+ENTF auf einem Computer ändern, auf dem die Plug-in-Software installiert ist, erfasst Single Sign-On die Kennwortänderung automatisch.
- Für die Bestätigung der Benutzeridentität sollten Sie nicht ausschließlich die benutzerseitige Kennwortzurücksetzung mit der Option Benutzer zur Eingabe des alten Kennworts auffordern kombinieren, sonst könnten Benutzer vom System ausgesperrt werden. Wenn als Authentifizierungsmethode nur die Identitätsprüfung mit dem altem Kennwort zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, vom System ausgesperrt. Die Daten der Benutzer müssen im zentralen Speicher und auf allen Benutzergeräten, auf denen sie gespeichert sind, gelöscht bzw. zurückgesetzt werden. Die Benutzer müssen die Anmeldeinformationen für alle Anwendungen neu eingeben.

Zusammenfassung der Self-Service-Implementierungsaufgaben

Führen Sie die folgenden Schritte aus, um den Konto-Self-Service zu verwenden:

1. Installieren das Self-Service-Modul und die Schlüsselverwaltung.
2. Konfigurieren Sie die fragenbasierte Authentifizierung.
3. Erstellen Sie eine Benutzerkonfiguration, in der das benutzerseitige Zurücksetzen des Kennworts oder das Entsperren des Kontos (oder beide Features) aktiviert sind.
4. Installieren und konfigurieren Sie die Plug-in-Software.

Verwenden der automatischen Schlüsselverwaltung mit dem Self-Service

Eine Kombination der automatischen Schlüsselverwaltung mit dem Self-Service vereinfacht die Verwendung für Benutzer, die auf kennwortgeschützte Anwendungen zugreifen müssen, die von der Single Sign-On Plug-in-Software gehandhabt werden. Beispiel: Wenn Benutzer die primären Kennwörter zurücksetzen, müssen sie nach dem erfolgreichen Zurücksetzen der Kennwörter keine Sicherheitsfragen beantworten. (Sie müssen jedoch Sicherheitsfragen beim benutzerseitigen Zurücksetzen des Kennworts beantworten.)

Bei der automatischen Schlüsselverwaltung müssen die Benutzer nach dem Entsperren des Kontos oder dem Zurücksetzen der Domänenkennwörter nicht die Identität bestätigen.

Zurücksetzen der Self-Service-Registrierung der Benutzer

Wenn die Windows-Konten der Benutzer gesperrt sind, und sie die Antworten auf die Sicherheitsfragen vergessen haben, müssen Sie die Self-Service-Registrierung für die Benutzer mit der Single Sign-On-Komponente im Citrix AppCenter zurücksetzen. Nach dem Zurücksetzen wird der Assistent für die Self-Service-Registrierung angezeigt, wenn die Benutzer die Plug-in-Software öffnen. Die Benutzer können dann Antworten auf Sicherheitsfragen registrieren.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie die Knoten Single Sign-On und Identitätsprüfung und wählen Sie den Knoten Fragenbasierte Authentifizierung.
3. Klicken Sie im Menü "Aktion" auf Andere AufgabenSicherheitsfragenregistrierung für einen Benutzer aufheben.
4. Geben Sie im Dialogfeld Benutzer auswählen den Namen des Benutzers oder der Benutzergruppe ein.

Benutzererfahrung

Nach der Installation und Konfiguration des Dienstes und der Plug-in-Software ändert das Self-Service-Modul das Dialogfeld des Benutzers für die Windows-Anmeldung und das Dialogfeld für das Entsperren des Computers oder auf Willkommenseite unter Windows Vista. Benutzern von Windows 7, Windows Server 2008 und Windows Server 2008 R2 wird eine Schaltfläche Konto-Self-Service angezeigt (verfügbar, wenn Benutzer den Computer mit Strg-Alt-Entf sperren).

Benutzer können die Self-Service-Features erst verwenden, wenn sie sich am primären Domänenkonto angemeldet und Antworten auf Sicherheitsfragen registriert haben. Nach der erfolgreichen Registrierung können sie die benutzerseitige Zurücksetzung des Kennworts und das Entsperren des Kontos verwenden.

Bei der automatischen Schlüsselverwaltung müssen die Benutzer nach dem Entsperren des Kontos oder dem Zurücksetzen der Domänenkennwörter nicht die Identität bestätigen.

Konto-Self-Service

Oct 05, 2015

Single Sign-on-Kunden können die Features des "Konto-Self-Service" (benutzerseitiges Zurücksetzen des Kennworts und Entsperren des Kontos) ohne andere Single Sign-On-Features den Benutzern bereitstellen.

Die Konto-Self-Service-Features von Single Sign-On reduzieren die Anrufe beim Helpdesk, da Benutzer die folgenden Aufgaben selbst durchführen können:

- Ändern des Microsoft Windows-Domänenkennworts
- Aufheben der Sperrung des Windows-Domänenkontos

Mit dem Feature "Konto-Self-Service" können Sie eine Gruppe von Sicherheitsfragen für die Identitätsprüfung erstellen. Nach dem Aktivieren der fragenbasierten Authentifizierung und dem Bereitstellen der Features "Konto-Self-Service" registrieren sich die Benutzer durch Beantworten von mehreren Sicherheitsfragen beim Dienst. Nach der Registrierung klicken die Benutzer auf Konto-Self-Service (A) im Dialogfeld Anmelden an Windows oder unter Microsoft Windows Vista auf der Willkommenseite (B).

Administratoren können eine Neuregistrierung der Benutzer folgendermaßen erzwingen:

- Löschen der Fragen eines Benutzers
- Neuregistrierung aller Benutzer
- Ändern des vorhandenen Fragenkatalogs

Registrierte Benutzer können auch die Neuregistrierung starten, wenn sie die Antworten auf die Sicherheitsfragen ändern möchten.

In diesem Dokument wird beschrieben, wie Sie Single Sign-On installieren und konfigurieren, um den Benutzern nur die Features "Konto-Self-Service" bereitzustellen.

Hinweis: Für den Konto-Self-Service werden keine UPN-Anmeldungen (User Principal Name) unterstützt, z. B. Benutzername@Domäne.com.

Verwenden von Lizenzen

Eine Single Sign-On-Lizenz wird bei der Neuregistrierung verbraucht, wenn Benutzer neue Antworten für die fragenbasierte Authentifizierung eingeben. Die Verwendung von CCU-Lizenzen garantiert, dass die Höchstzahl der Lizenzen im Unternehmen zur Verfügung stehen. Eine CCU-Lizenz wird an den Lizenzpool zurückgegeben, wenn der Benutzer die Neuregistrierung abgeschlossen hat. Eine Benannte Benutzerlizenz bleibt in derselben Situation mindestens 2 Tage dem Benutzer zugewiesen, selbst wenn sie nicht verwendet wird.

Mit Verhältnissen wird pro Single Sign-On-Lizenz eine größere Anzahl von Lizenzen nur für den Konto-Self-Service bereitgestellt. CCU-Benutzerlizenzen verwenden ein Verhältnis von 10:1, d. h. 100 CCU-Benutzerlizenzen werden in 1000 Konto-Self-Service-Lizenzen umgesetzt. Benannte Benutzerlizenzen verwenden ein Verhältnis von 5:1 ratio, wobei 100 Lizenzen in 500 Konto-Self-Service-Lizenzen umgesetzt werden.

Verwenden von verfügbaren CCU-Lizenzen offline

1. Erstellen Sie eine Benutzerkonfiguration.
2. Wählen Sie auf der Seite Lizenzierung konfigurieren des Assistenten für Benutzerkonfigurationen die Option CCU-Lizenz (nur Enterprise und Platinum Edition).
3. Wählen Sie Lizenzverbrauch für Offlineverwendung zulassen aus und legen Sie fest, wie lange die Lizenz beim Lizenzserver ausgecheckt sein kann.
4. Schließen Sie die Benutzerkonfiguration ab.

Für Benutzer, die dieser Benutzerkonfiguration zugeordnet sind, ist das Lizenzierungsmodell dasselbe wie eine benannte Benutzerlizenz: Die Lizenz kann von Benutzern verwendet werden, die gelegentlich remote arbeiten und über längere Zeiträume hinweg offline sind. CCU-Lizenzen werden dann pro Benutzer verbraucht.

Wichtig: Für lokal installierte Instanzen des Single Sign-On Plug-Ins wird keine separate Lizenz für Benutzer benötigt, die auf gehostete Anwendungen in einer Umgebung mit Citrix XenApp, Platinum Edition, zugreifen können.

Erstellen einer Benutzerkonfiguration ausschließlich für den Konto-Self-Service

Mit den folgenden Schritten erstellen Sie eine Benutzerkonfiguration, die Konto-Self-Service-Funktionalität ohne Aktivieren von Single Sign-On ermöglicht.

Hinweis: Anwendungsdefinitionen sind in dieser Benutzerkonfiguration nicht enthalten, da das Feature keine Single Sign-On-Funktionalität enthält. Wenn Benutzer Single Sign-On-Funktionalität benötigen, schließen Sie sie in einer Benutzerkonfiguration ein, die keine speziellen Änderungen für den Konto-Self-Service enthält.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen und wählen Sie Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und klicken Sie auf Benutzerkonfigurationen, um den Assistenten zu starten. Klicken Sie im Bereich Aktionen auf Benutzerkonfiguration hinzufügen, um den Assistenten für Benutzerkonfigurationen zu öffnen.
3. Seite Benutzerkonfiguration benennen:
   1. Geben Sie im Feld Name den Namen der Benutzerkonfiguration ein.
   2. Wählen Sie im Bereich Benutzerkonfigurationszuordnung aus, wie die Benutzerkonfiguration den Benutzern zugeordnet ist; geben Sie die Active Directory-Hierarchie (Organisationseinheit oder Benutzer) oder die Active Directory-Gruppe an.
4. Wählen Sie auf der Seite Produktedition auswählen den Eintrag Single Sign-on Enterprise.
5. Klicken Sie auf der Seite Anwendungen auswählen auf Weiter.
6. Deaktivieren Sie auf der Seite Konfigurieren des Plug-In-Verhaltens die folgenden Kontrollkästchen:
   - Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern
   - Definierte Formulare automatisch verarbeiten, wenn das Single Sign-On sie erkennt

   Klicken Sie auf Erweiterte Einstellungen.
7. Unter Erweiterte Single Sign-On Plug-In-Einstellungen:
   - Wählen Sie Anwendungsunterstützung und deaktivieren Sie das Kontrollkästchen Clientseitige Anwendungsdefinitionen erkennen.

   Klicken Sie auf OK, um Erweiterte Einstellungen zu schließen, und klicken Sie dann auf Weiter.
8. Geben Sie auf der Seite Lizenzierung konfigurieren im Bereich Lizenzserveradresse den Namen und die Portnummer für den Lizenzserver ein.
   Klicken Sie im Bereich Lizenzierungsmodell auf Benannte Benutzerlizenzierung oder CCU-Lizenzierung.

   Hinweis: Die Verwendung von CCU-Lizenzen garantiert, dass die Höchstzahl der Lizenzen im Unternehmen zur Verfügung stehen. Eine CCU-Lizenz wird an den Lizenzpool zurückgegeben, wenn der Benutzer die erneute Registrierung abschließt. Eine Benannte Benutzerlizenz bleibt in derselben Situation mindestens 2 Tage dem Benutzer zugewiesen, selbst wenn sie nicht verwendet wird.

9. Geben Sie auf der Seite Datenschutzmethoden auswählen die benötigten Informationen ein.
10. Klicken Sie auf der Seite Sekundären Datenschutz auswählen auf Benutzerseitige Auswahl der Methode: Altes Kennwort oder Sicherheitsfragen.
11. Wählen Sie auf der Seite Self-Service-Features aktivieren eine oder beide der folgenden Optionen aus:
    - Benutzerseitiges Zurücksetzen des primären Domänenkennworts
    - Benutzerseitiges Entsperren des Domänenkontos
12. Geben Sie auf der Seite Dienstmodule suchen > Schlüsselverwaltungsmodul die Dienstadresse ein.
13. Beenden Sie den Assistenten ohne weitere Änderungen.

Vorbereiten des Computers mit der Plug-in-Software

Hinweis: Sie sollten die folgenden Schritte mit Skripten automatisieren, um Leistungsfähigkeit und Genauigkeit zu erhöhen. Nach der Installation der Single Sign-On Plug-In-Software auf den Computern der Benutzer müssen Sie die Verknüpfung ssoShell.exe und das Menü Start bearbeiten, um den ausschließlichen Benutzerzugriff auf die Konto-Self-Service-Features zu ermöglichen.

Bei der normalen Installation der Single Sign-On Plug-in-Software enthält die Verknüpfung ssoShell.exe die folgende Befehlszeilenoption:

/background

Ändern Sie diese Option zu:

/qbaenroll /noforceqbaenroll

Mit dieser Änderung synchronisiert die Single Sign-On Plug-in-Software auf dem Computer des Benutzers bei der Benutzeranmeldung mit dem zentralen Speicher und ermittelt den Status der fragenbasierten Authentifizierungsregistrierung des Benutzers. Wenn die Registrierung abgeschlossen und aktuell ist, wird der Benutzer nicht aufgefordert, sich zu registrieren. Der Benutzer wird zur Registrierung aufgefordert, wenn eine der folgenden Bedingungen bei der Synchronisierung erkannt wird:

- Der Benutzer hat die fragenbasierte Authentifizierungsregistrierung nicht abgeschlossen.
- Der Administrator hat die Fragen der fragenbasierten Authentifizierung des Benutzers zurückgesetzt.
- Der Administrator hat den Fragenkatalog der fragenbasierten Authentifizierung geändert.

Nach dem Abschluss der Synchronisierung und ggf. dem Start der Registrierung wird ssoShell automatisch beendet.

Aktualisieren der Single Sign-On ssoShell.exe-Verknüpfung

Desktopinstallation:

1. Computer mit Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\ProgramData\Microsoft\Windows\Startmenü\Programme\Start.
   Computer ohne Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\Dokumente und Einstellungen\All Users\Startmenü\Programme\Start.
2. Klicken Sie im Ordner Start auf Single Sign-on Background Process und wählen Sie Datei > Eigenschaften.
3. Klicken Sie im Dialogfeld Single Sign-on Background Process Properties auf das Feld Ziel, gehen Sie an das Ende des Texts in diesem Feld und löschen Sie /background.
4. Geben Sie im Feld Ziel nach dem restlichen Text /qbaenroll /noforceqbaenrollein.

Serverinstallation:
Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

1. Öffnen Sie die Registrierung und navigieren Sie zu HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows NT\CurrentVersion\Winlogon\AppSetup.
2. Doppelklicken Sie in diesem Unterschlüssel auf den Standardeintrag, um das Dialogfeld Zeichenfolge bearbeiten zu öffnen.
3. Feld Wert:
   Ändern Sie: %SystemDrive%\Citrix\Metaframe Password Manager\WTS\SSOlauncher.exe /no ssoshutdown

   in %SystemDrive%\Citrix\Metaframe Password Manager\ssoshell.exe /qbaenroll /noforceqbaenroll.

Die Datei ssoShell.exe ist ausschließlich für die Konto-Self-Service-Funktionalität geändert.

Hinzufügen einer Self-Service-Registrierung-Verknüpfung zum Startmenü

Fügen Sie dem Menü Start eine Verknüpfung hinzu, damit Benutzer die Registrierung eigenständig beginnen können. Dies reduziert Supportanrufe, wenn Benutzer bei der Erstanmeldung keine Antworten eingeben oder die Antworten ändern möchten.

1. Computer mit Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\ProgramData\Microsoft\Windows\Startmenü\Programme\Citrix\.
   Computer ohne Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\Dokumente und Einstellungen\All Users\Startmenü\Programme\Citrix\.

2. Klicken Sie im Menü Datei auf Neu > Verknüpfung. Der Assistent zum Erstellen einer Verknüpfung wird angezeigt.
3. Klicken Sie auf Durchsuchen.
4. Navigieren Sie zu %InstallationDirectory%\Programme\Citrix\Metaframe Password Manager\, wählen Sie ssoShell.exe und klicken Sie auf OK. Das Dialogfeld Ordner suchen wird geschlossen und der Pfad zu ssoShell.exe wird im Feld Geben Sie den Ort des Objekts ein angezeigt.
5. Platzieren Sie den Einfügepunkt im Feld Geben Sie den Ort des Objekts ein hinter ssoShell.exe und geben Sie eine Leerstelle und dann /qbaenroll (J) ein.

6. Klicken Sie auf Weiter.
7. Geben Sie Citrix Account Self-Service Registration Klicken Sie dann auf Fertig stellen.

Die Verknüpfung wird unter Start > Alle Programme > Citrix angezeigt.

Entfernen der Single Sign-on-Verknüpfung

Währen der Installation der Single Sign-On Plug-In-Software wird eine Verknüpfung dem Menü Start hinzugefügt. Wenn ein Benutzer, der nur die Konto-Self-Service-Features verwenden kann, diesen Befehl auswählt, wird ssoShell.exe gestartet und bei unveränderter fragenbasierten Authentifizierung des Benutzers beendet. Dies kann den Benutzer verwirren und zu Supportanrufen führen. Entfernen Sie die Verknüpfung aus dem Menü Start, um dies zu vermeiden.

1. Computer mit Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\ProgramData\Microsoft\Windows\Startmenü\Programme\Citrix\.
   Computer ohne Windows Vista: Navigieren Sie in Windows-Explorer zu %SystemDrive%\Dokumente und Einstellungen\All Users\Startmenü\Programme\Citrix\.

2. Löschen Sie die Single Sign-On-Verknüpfung.

Die Single Sign-On-Verknüpfung wird aus dem Menü Start entfernt.

Entfernen der Single Sign-On Plug-in-Verknüpfung vom Startordner

Entfernen Sie die Single Sign-On Plug-in-Verknüpfung auf dem Benutzergerät, um den Start der Plug-in-Software bei jeder Anmeldung des Benutzers am Computer zu verhindern. Diese Aufgabe verhindert, dass der Benutzer eine Lizenz unnötig verbraucht.

1. Navigieren Sie mit Windows Explorer zu %SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startup.
2. Löschen Sie Single Sign-On Plug-In Background Process im Startordner.
   Hinweis: Wenn die Plug-In-Software in einer Umgebung mit Citrix Presentation Server oder Terminalserver installiert ist, müssen Sie den AppSetup-Registrierungsunterschlüssel unter HKLM\SOFTWARE\microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup bearbeiten und den Verweis auf Password Manager oder Single Sign-On entfernen.

Die Single Sign-On Plug-in-Verknüpfung wird bei der Benutzeranmeldung nicht mehr automatisch gestartet.

Automatisieren der Eingabe der Anmeldeinformationen mit dem Provisioning

Oct 05, 2015

Mit dem Provisioningmodul (auch als Provisioning der Anmeldeinformationen bezeichnet) manipulieren Sie Anmeldeinformationen des Benutzers, die Anwendungen zugeordnet sind, die in einer Benutzerkonfiguration festgelegt sind. Mit dem Provisioning können Sie diese Aufgaben automatisieren und sie auf mehrere Benutzer anwenden. Wenn Sie den Benutzern neue Software bereitstellen, erstellen Sie eine Anwendungsdefinition für die Anwendung und fügen mit dem Provisioning die Anmeldeinformationen aller Benutzer hinzu, die diese Anwendung verwenden.

Zusammenfassung der Provisioningaufgaben

Wenn Sie die Anmeldeinformationen manipulieren möchten, die im zentralen Speicher für Single Sign-On-aktivierte Anmeldungen gespeichert sind, die in Benutzerkonfigurationen enthalten sind, müssen Sie die folgenden Aufgaben ausführen:

1. Installieren des Moduls "Provisioning" des Single Sign-On-Dienstes.
2. Erstellen einer Benutzerkonfiguration, die den Provisioningdienst verwendet.
3. Erstellen einer Provisioningvorlage.
4. Importieren der Anmeldeinformationen des Benutzers in die Vorlage und Auswählen eines auszuführenden Befehls.
5. Verarbeiten der Provisioningdaten.

Wichtig: Die XML-Datei, mit der Sie das Provisioning der Anmeldeinformationen durchführen, enthält sehr vertrauliche Benutzerdaten. Ziehen Sie die Löschung der Datei oder die Verlagerung auf einen sicheren Speicherort in Erwägung, wenn das Provisioning der Anmeldeinformationen abgeschlossen ist.
Wenn Sie die Anmeldeinformationen im zentralen Speicher hinzugefügt, entfernt oder bearbeitet haben, können diese Angaben in der Umgebung verwendet werden. Wenn Benutzer die Plug-in-Software starten, werden die in der Plug-in-Software aktualisierten Anmeldeinformationen und die Anwendungen den Benutzern zur Verfügung gestellt.

Das Hinzufügen, Bearbeiten oder Löschen von Anmeldeinformationen im zentralen Speicher kann viele Systemressourcen verbrauchen. Soweit wie möglich, sollte das Provisioning in Zeiten geringer Systemauslastung durchgeführt werden.

Das Credential Provisioning SDK

Wenn Sie die Anmeldeinformationen vieler Benutzer manipulieren müssen, sollten Sie die Verwendung des Credential Provisioning-SDKs in Erwägung ziehen. Das SDK enthält eine Beschreibung aller APIs, die verfügbar sind, wenn Sie das Provisioning-Modul des Single Sign-On-Dienstes installieren. Mit diesem SDK und dem darin enthaltenen Beispielscode können Sie eigene Provisioningclients erstellen und mit Single Sign-On verwenden.

Erstellen einer Provisioningvorlage

In den folgenden Schritten wird davon ausgegangen, dass Sie eine Benutzerkonfiguration erstellt haben, die mindestens eine Anwendungsdefinition, eine Anwendungsgruppe und eine Kennwortrichtlinie (vielleicht optional eine Kennwortgruppe) enthält, und dass das Provisioning für die Benutzerkonfiguration aktiviert ist.

Eine Provisioningvorlage ist eine XML-Datei, die Informationen zu den Anwendungen enthält, die in dieser Benutzerkonfiguration enthalten sind:

- Anwendungsgruppe
- Name der Anwendungsdefinition und GUID
- Benutzerinformationen, wie z. B. Benutzername und Kennwort

Sie enthält auch Befehle zum Hinzufügen, Entfernen und Bearbeiten, die Sie verwenden, wenn Sie das Provisioning mit der bearbeiteten Vorlage ausführen.

Diese Vorlage enthält Beispiele von Befehlen und Informationen zu der ausgewählten Benutzerkonfiguration.

Erstellen einer Provisioningvorlage

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und wählen Sie Benutzerkonfigurationen.
3. Wählen Sie eine Benutzerkonfiguration aus.
4. Klicken Sie im Menü Aktion auf Provisioningvorlage erstellen.
5. Geben Sie im Dialogfeld Provisioningvorlage erstellen einen Namen für die Vorlage ein.

Verarbeiten der Provisioningvorlage

Die in der XML-Datei enthaltenen Provisioningaufgaben werden mit der Single Sign-On-Komponente im Citrix AppCenter durchgeführt. Single Sign-On prüft die Syntax jedes Befehls, führt die Befehle aus und fügt die Daten dem zentralen Speicher hinzu oder bearbeitet die Daten im zentralen Speicher.

Achtung: Schließen Sie das Dialogfeld für das Verarbeiten des Provisioning erst, wenn das Provisioning ganz angehalten oder abgeschlossen ist. Das Schließen des Dialogfelds hält die Verarbeitung des Provisioning nicht an. Wenn Sie das Dialogfeld während der Verarbeitung des Provisioning schließen, können Sie keine Informationen erfassen oder den Prozess vor dem Abschluss anhalten.

1. Klicken Sie auf Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter.
2. Erweitern Sie den Knoten Single Sign-On und erweitern Sie Benutzerkonfigurationen.
3. Wählen Sie eine Benutzerkonfiguration oder eine Anwendungsgruppe einer Benutzerkonfiguration aus.
4. Klicken Sie im Menü Aktion auf Provisioning ausführen. Der Assistent für das Provisioning wird angezeigt.
5. Klicken Sie auf Next.
6. Geben Sie den Namen der XML-Datei für das Provisioning ein oder klicken Sie auf Durchsuchen, um die Datei zu suchen, klicken Sie dann auf Weiter. Single Sign-On prüft die XML-Datei.
   - Wenn keine Syntaxfehler bestehen, wird eine Zusammenfassung der Änderungen angezeigt, die Sie machen können. Sie können die Zusammenfassung speichern.
   - Wenn Syntax- oder andere Fehler bestehen, wird ein Fehlerprotokoll erstellt. Sie können das Fehlerprotokoll speichern und dann auf Abbrechen klicken, um den Assistenten zu schließen.
7. Klicken Sie auf Weiter, um die Befehle in der Datei auszuführen, wenn keine Fehler festgestellt wurden. Wenn die Informationen im zentralen Speicher geändert werden, werden Fehler angezeigt, die aufgrund des Provisioning aufgetreten sind. Klicken Sie auf Abbrechen, um das Provisioning abzubrechen. Wenn Single Sign-On das Ende des aktuellen Abschnitts der verarbeiteten Daten erreicht (in der Standardeinstellung werden Daten in Gruppen von 50 Codezeilen verarbeitet), wird das Provisioning beendet.

Wenn Sie den Assistenten beenden, können Sie die Provisioningergebnisse speichern.

Feinabstimmen des Provisioning der Anmeldeinformationen

Achtung: Im Rahmen dieses Verfahrens müssen Sie die Registrierung bearbeiten. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch Neuinstallation des

Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Legen Sie stets eine Sicherungskopie der Systemregistrierung an, bevor Sie fortfahren.
Wenn Sie Single Sign-On für das Provisioning der Anmeldeinformationen verwenden, werden die Informationen in der Standardeinstellung in Serien von 50 Befehlen mit einem Timeout von 100.000 Millisekunden verarbeitet. Sie können die folgenden Registrierungsschlüssel bearbeiten, um diese Standardwerte zu ändern:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\BatchSize

Typ: DWORD

Standardwert bei keiner Eingabe: 50

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\ServiceTimeout

Typ: DWORD

Standardwert in Millisekunden bei keiner Eingabe: 100000

Bearbeiten der Provisioningvorlage

Oct 05, 2015

Bearbeiten Sie die erstellte Vorlage in einem Texteditor oder einem XML-Dateieditor. In der Provisioningvorlage wird SPML (Service Provisioning Markup Language), ein XML-basierter Standard für den Datenaustausch, verwendet. Wie bei XML müssen Sie sicherstellen, dass alle SPML-Tags oder -Elemente (z. B.) richtig strukturiert sind und die XML-Syntaxregeln einhalten. Stellen Sie beispielsweise beim Entfernen von Kommentarzeichen wie !-- und -- sicher, dass Sie überflüssige spitze Klammern (< oder >) entfernen, da sonst Fehler bei der Verarbeitung der Provisioningvorlage auftreten können. Weitere Informationen zu XML finden Sie auf der Website von W3C unter http://www.w3.org/. Stellen Sie sicher, dass Sie die entsprechenden Kommentarzeichen (!-- und --) entfernen.

Beispielsausgabe

Die erstellte Vorlage enthält Folgendes:

- Informationen zum Benutzer, der die Vorlage erstellt hat
- Befehl für den Anwendungsnamen in der Benutzerkonfiguration
- Befehl mit dem Namen der Anwendungsdefinition

Am Ende der XML-Datei finden Sie Informationen zu der ausgewählten Benutzerkonfiguration, die Sie kopieren und in der Vorlage verwenden können. Beispiel:

Sie können beispielsweise die Benutzerinformationen zwischen den Tags und kopieren, das Kommentarzeichen entfernen und sie für jeden Benutzer bearbeiten, für den Sie Anmeldeinformationen hinzufügen möchten.

Hinweis: Im obigen Beispiel ist die Domäne und der Benutzername des Benutzers, der die Vorlage erstellt hat. Sie können diese Informationen als Kommentar markieren oder löschen, wenn Sie diese Angaben nicht in der Vorlage speichern möchten.

Das Tag "cpm-provision"

Hinweis: Sie müssen die gewünschten Tags und Befehle im Provisioningtag einschließen (ungefähr auf Zeile 70 in der erstellten XML-Datei):

Fügen Sie an dieser Stelle das Tag und Befehle ein

Das Tag "user"

Mit dem Tag fügen Sie die Domäne und den Benutzernamen für jeden Benutzer hinzu, für dessen Anmeldeinformationen für die Anwendung Sie das Provisioning verwenden möchten. Sie müssen für jeden Benutzer, für den Sie das Provisioning verwenden, ein -Tag bereitstellen. Jedes -Tag enthält auch die Befehle, die für das Konto ausgeführt werden.

Die Befehle haben die folgende Syntax:

DieDomäne\Benutzer-ID"> <Befehl>
Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an, der hinzugefügt wird.
Benutzer-ID	Gibt den Benutzernamen des Benutzers an, der hinzugefügt wird.
command	Gibt die Befehle an, die für diesen Benutzer ausgeführt werden können: • • • • • •

Der Befehl "add"

Mit dem Befehl fügen Sie einen Benutzernamen und ein Kennwort hinzu, die für Anwendungen benötigt werden, die in der Benutzerkonfiguration enthalten sind.

Die Befehle haben die folgende Syntax:

%ANWENDUNGSNAME%">%ANWENDUNGS-GUID% lange Beschreibung%ANMELDEINFORMATIONEN% AusführlicheBeschreibung %ANWENDUNGSNAME% ausgeblendete Beschreibung Be
Wobei Folgendes gilt:

	Pflichteingabe. Das Element und die Attribute werden normalerweise automatisch beim Erstellen einer Vorlage erstellt. Das Attribut name= ist optional. • %ANWENDUNGSNAME% ist der Name der Anwendungsdefinition in der ausgewählten Benutzerkonfiguration. • %ANWENDUNGS-GUID% ist die GUID der Anwendung, die übereinstimmen muss
	Pflichteingabe. Das Element und die Attribute werden normalerweise automatisch erstellt. • %ANMELDEINFORMATIONEN% ist der Name der Anwendung in der Anwendungsdefinition.
	Optional. Geben Sie eine Beschreibung für die Benutzerkonfiguration ein.
	Optional. Geben Sie Text ein.
	Pflichteingabe. Benutzer-ID ist der Name des Benutzers, der hinzugefügt wird.

	Pflichteingabe. Kennwort ist das Kennwort des Benutzers, der hinzugefügt wird.
	Pflichteingabe, wenn ein weiteres Feld für die Authentifizierung benötigt wird (z. B. für ein Feld, in dem der Benutzer die Domäne eingeben muss). Sie können beliebig viele benutzerdefinierte Felder für die Anwendung angeben.

Der Befehl "modify"

Mit dem Befehl ändern Sie einen Benutzernamen und ein Kennwort, die für Anwendungen benötigt werden, die in der Benutzerkonfiguration enthalten sind.

Wichtig: Für diesen Befehl müssen die Anmeldeinformationen des Benutzers eingegeben werden. Sie können die Anmeldeinformationen des Benutzers abrufen, wenn Sie den Befehl vor dem Befehl verwenden.
Schließen Sie nur die Elemente ein, die Sie bearbeiten möchten:

- Löschen Sie die Zeile, wenn ein Wert nicht geändert wird. Beispiel: Löschen Sie das Element , um den Namen der Anwendung unverändert zu lassen.
- Wenn Sie einen Wert ändern möchten, geben Sie den Wert in der Vorlage an. Beispiel: Schließen Sie das Element ein, um einen neuen Anwendungsnamen anzugeben.
- Ein Wert wird entfernt, wenn Sie das Element ohne einen Wert einschließen. Beispiel: Verwenden Sie , um die aktuelle Beschreibung zu löschen.

Die Befehle haben die folgende Syntax:

%ANMELDEINFORMATIONEN-ID% %ANMELDEINFORMATIONEN% ausführlicheBeschreibung %ANWENDUNGSNAME% ausgeblendete Beschreibung Benutzer-ID Kennwort %LABELTEXT%"> E
Wobei Folgendes gilt:

	Pflichteingabe. Der GUID-Wert für die Anmeldeinformationen %ANMELDEINFORMATIONEN-ID% des Benutzers muss mit dem Wert übereinstimmen, der mit dem Befehl zurückgegeben wird.
	Optional. Das Element und die Attribute werden normalerweise automatisch erstellt. • %ANMELDEINFORMATIONEN% ist der Name der Anwendung in der Anwendungsdefinition.
	Optional. Geben Sie eine Beschreibung für die Benutzerkonfiguration ein.
	Optional. Geben Sie Text ein.
	Pflichteingabe. Benutzer-ID gibt den Namen des Benutzers an, der geändert wird.
	Pflichteingabe. Kennwort gibt das Kennwort des Benutzers an, der geändert wird.
	Pflichteingabe, wenn ein weiteres Feld für die Authentifizierung benötigt wird (z. B. für ein Feld, in dem der Benutzer die Domäne eingeben muss). Sie können beliebig viele benutzerdefinierte Felder für die Anwendung angeben.

Der Befehl "delete"

Mit dem Befehl löschen Sie die Anmeldeinformationen eines Benutzers für eine Single Sign-On-aktivierte Anwendung.

Wichtig: Für diesen Befehl müssen die Anmeldeinformationen des Benutzers eingegeben werden. Sie können die Anmeldeinformationen des Benutzers abrufen, wenn Sie den Befehl vor dem Befehl verwenden.
Die Befehle haben die folgende Syntax:

DieDomäne\Benutzer-ID"> %ANMELDEINFORMATIONEN-ID%
Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.
	Pflichteingabe. Der GUID-Wert für die Anmeldeinformationen %ANMELDEINFORMATIONEN-ID% des Benutzers muss mit dem Wert übereinstimmen, der mit dem Befehl zurückgegeben wird.

Der Befehl "remove"

Mit dem Befehl entfernen Sie Benutzerdaten und -informationen aus dem zentralen Speicher. Verwenden Sie den Befehl, wenn ein Benutzer nicht mehr im Unternehmen arbeitet. Der lokale Speicher der Anmeldeinformationen auf dem Benutzergerät bleibt bestehen, bis er von einem Administrator oder Operator gelöscht wird.

Die Befehle haben die folgende Syntax:

DieDomäne\Benutzer-ID">
Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.

Hinweis: Dieser Befehl ähnelt der Single Sign-On-Aufgabe Benutzerdaten aus dem zentralen Speicher löschen, die im Citrix AppCenter ausgeführt wird.

Der Befehl "reset"

Mit dem Befehl setzen Sie Anmeldeinformationen des Benutzers im zentralen Speicher zurück, wodurch dieser Benutzer auf den Originalzustand zurückgesetzt wird. Bei zentralen Speichern, die nicht in Active Directory erstellt sind, bleiben die Benutzerordner gespeichert, aber alle Benutzerdaten (Anmeldeinformationen, Sicherheitsfragen und Antworten usw.) werden gelöscht. In zentralen Speichern, die unter Active Directory erstellt sind, werden die Benutzerdaten gelöscht, und der Benutzer wird markiert, dass die Daten zurückgesetzt wurden.

Die Befehle haben die folgende Syntax:

DieDomäne\Benutzer-ID">
Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.

Hinweis: Dieser Befehl ähnelt der Single Sign-On-Aufgabe Benutzerdaten zurücksetzen, die im Citrix AppCenter ausgeführt wird.

Der Befehl "list-credentials"

Mit dem Befehl rufen Sie die Anmeldeinformationen des Benutzers für jede Anwendung ab, die in der zugeordneten Anwendungsdefinition enthalten ist. Für die Befehle und müssen Sie den abgerufene Anmeldeinformationen-GUID als Wert für den Parameter %ANMELDEINFORMATIONEN-ID% verwenden.

Die Identnummer, die von diesem Befehl abgerufen wird, ist eine Anmeldeinformationen-GUID, z. B. 634EE015-10C2-4ed2-80F5-75CCA9AA5C11.

Die Befehle haben die folgende Syntax:

DieDomäne\Benutzer-ID">
Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.

Hotdesktop: Desktopfreigabeumgebung für Benutzer

Oct 05, 2015

Hotdesktop verbindet die Flexibilität eines schnellen Benutzerwechsels mit der Sicherheit von Single Sign-On. Die Hotdesktop-Funktion wird nicht standardmäßig installiert. Sie können die Funktion bei der Erstinstallation des Single Sign-On Plug-ins auswählen. Vorhandene Bereitstellungen des Single Sign-On Plug-ins können auch für die Hotdesktopverwendung aktualisiert werden. Vor der Implementierung von Hotdesktop müssen Sie die Anwendung entsprechend den vorliegenden Umgebungs- und Unternehmensanforderungen konfigurieren.

Hotdesktop wird nur unter den folgenden Betriebssystemen unterstützt:

- Microsoft Windows XP Professional, Service Pack 2 (32 Bit)
- Microsoft Windows XP Embedded

Hotdesktop wird nicht unter 64-Bit-Betriebssystemen oder Serverbetriebssystemen unterstützt.

Hotdesktop ist nicht verfügbar, wenn Sie Single Sign-On mit Citrix Receiver Updater bereitstellen.

Mit dem Hotdesktop-Feature von Single Sign-On können Benutzer effizient und sicher Arbeitsstationen gemeinsam verwenden. Hotdesktop erweitert die Windows-Standardumgebung und ermöglicht Benutzern Folgendes:

- Schnelle Windows-Authentifizierung mit dem interaktiven GINA-Standarddialogfeld für die Anmeldung
- Ausführen von Single Sign-On-aktivierten Anwendungen in der interaktiven Benutzer-Shell mit Anmeldeinformationen des Benutzers für Single Sign-On
- Abmelden von der Hotdesktop-Arbeitsstation, damit andere Benutzer Anwendungen ausführen können

Zusammenfassung der Hotdesktop-Aufgaben

Vor der Implementierung von Hotdesktop müssen Sie Folgendes ausführen:

- Erstellen eines Hotdesktop-Kontos
- Erstellen von Benutzerkonfigurationen mit speziellen Hotdesktop-bezogenen Einstellungen zum Anpassen der Hotdesktop-Benutzererfahrung
- Definieren des Hotdesktop-Verhaltens beim Starten und Beenden, einschließlich:
  - Festlegen der Anwendungen, die beim Starten geöffnet werden bzw. von denen Hotdesktop-Anmeldeinformationen und -Berechtigungen (Benutzer- bzw. Hotdesktop-Konto) verwendet werden
  - Festlegen der Anwendungen, die für schnelle Benutzerwechsel dauerhaft (d. h. auch nach dem Abmelden von Benutzern) ausgeführt werden bzw. nach dem Abmelden von Benutzern beendet werden, einschließlich persönlicher optionaler Bereinigungsskripte oder Anwendungen zum Löschen von Benutzerinformationen zwischen Sitzungen

Führen Sie die folgenden Aufgaben aus, um Hotdesktop zu konfigurieren und zu aktivieren:

1. Erstellen Sie ein Hotdesktop-Konto, das für jede Arbeitsstation bzw. jedes Benutzergerät, auf dem Hotdesktop ausgeführt wird, verfügbar ist.
2. Legen Sie fest, welche Single Sign-On-aktivierten Anwendungen in der Hotdesktop-Umgebung ausgeführt werden.
3. Legen Sie fest, wie Anwendungen unter Hotdesktop ausgeführt werden und konfigurieren Sie die Hotdesktop-Benutzerumgebung.
4. Erstellen oder ändern Sie eine Benutzerkonfiguration für die Auswahl von Hotdesktop-Optionen.
5. Installieren Sie die Plug-in-Software mit dem ausgewählten Hotdesktop-Feature.

6. Deinstallieren Sie Hotdesktop bei Bedarf.

Prozessablauf beim Starten und Beenden von Hotdesktop

Im Folgenden werden die Ereignisse beschrieben, die im Zusammenhang mit dem Starten und Beenden von Hotdesktop auftreten. Wenn die Arbeitsstation bzw. das Clientgerät gestartet wird, wird es automatisch am Hotdesktop-Konto angemeldet, sodass das Gerät im Desktopfreigabemodus ausgeführt werden kann.

Hinweis: Das Hotdesktop-Konto bleibt durchgehend aktiviert. Benutzer sind nicht berechtigt, das Hotdesktop-Konto zu beenden.

1. Ein Hotdesktop-Benutzer meldet sich an der Arbeitsstation an und gibt einen Benutzernamen und ein Kennwort ein bzw. verwendet eine starke Authentifizierungsmethode, wie z. B. eine Smartcard.
2. Wenn der Benutzer authentifiziert wurde, beginnt die Hotdesktop-Sitzung.
3. Single Sign-On wird gestartet. Die Plug-in-Software synchronisiert die Daten mit dem zentralen Speicher. Dies stellt sicher, dass der Benutzer die aktuellen Anwendungsdefinitionen, Kennwortrichtlinien und anderen Einstellungen für die Plug-in-Software besitzt.
4. Die Datei session.xml wird gelesen und alle Anwendungen, für die Sie festgelegt haben, dass sie unter dem Hotdesktop-Konto oder dem Hotdesktop-Benutzerkonto ausgeführt werden, werden gestartet. Bei diesen Anwendungen kann es sich um lokale oder mit XenApp veröffentlichte Remoteanwendungen handeln. Der Benutzer greift auf die Anwendungen zu, um die ihm übertragenen Aufgaben auszuführen.
5. Der Hotdesktop-Benutzer meldet sich ab.
   Hinweis: Wenn Benutzer eine Arbeitsstation im Leerlauf lassen, initiiert Hotdesktop ein Sitzungstimeout. In der Access Management Console legen Sie fest, wie lange eine Arbeitsstation inaktiv bleiben kann. Wenn das Intervall überschritten wird, sperrt Hotdesktop die Arbeitsstation. Wenn noch weitere Zeit vergangen ist, und der Benutzer nicht zurückkehrt, beendet Hotdesktop die Sitzung.
6. Hotdesktop führt die Anwendungen weiterhin aus oder beendet sie, abhängig von den Einstellungen in der Datei process.xml.
7. Single Sign-On wird beendet.
8. In der Datei session.xml angegebene Skripte zum Beenden werden ausgeführt.
9. Die Hotdesktop-Sitzung wird beendet.

Problembehandlung beim benutzerseitigen Start von Hotdesktop

Wenn sich ein Benutzer an einem Computer mit Single Sign-On anmeldet, der mit Hotdesktop konfiguriert ist, werden die in der Datei session.xml angegebenen Startskripte möglicherweise ausgeführt, bevor der Start der Single Sign-On Plug-in-Software abgeschlossen ist.

Hotdesktop wartet beim Start 30 Sekunden auf den Start der Plug-in-Software, bevor die Startskripte ausgeführt werden. Nach 30 Sekunden werden die Startskripte ausgeführt, selbst wenn die Plug-in-Software noch nicht vollständig funktionsbereit ist.

Diese Situation tritt am wahrscheinlichsten bei der Erstanmeldung des Benutzers auf (d. h. bei der Erstverwendung der Software durch den Benutzer), wenn der Single Sign-On-Administrator eine Liste von Anwendungen festgelegt hat, für die eine Registrierung von Anmeldeinformationen oder ein Beantworten von Sicherheitsfragen erforderlich ist. In diesem Fall gilt folgender Handlungsablauf:

1. Der Benutzer meldet sich am Computer oder Clientgerät mit der Plug-in-Software an und wird in einer Meldung aufgefordert, die Anmeldeinformationen für die aufgelisteten Anwendungen oder Antworten auf Sicherheitsfragen einzugeben.

2. Während er diese Aufgaben ausführt, vergehen 30 Sekunden und die Hotdesktop-Startskripte werden ausgeführt. Je nach den Anwendungen, die in den Startskripten von session.xml angegeben sind, können verschiedene Fenster geöffnet und geschlossen werden.
3. Wenn die Startskript-Fenster vom Computer wiederholt aufgerufen werden, kann dies bei Benutzern zu Frustrationen führen.
4. Wenn die Startskripte abgeschlossen sind, wird eine Fehlermeldung angezeigt. Sie lautet in etwa: "Ein oder mehrere Fehler sind aufgetreten. Weitere Informationen finden Sie im Ereignisprotokoll."

Auch wenn Benutzer dieses Verhalten unter Umständen als frustrierend empfinden, werden dadurch weder die Benutzerdaten noch die Arbeitsumgebung oder Single Sign-On beschädigt.

Empfehlen Sie den Benutzern daher, die Anmeldeinformationen und Antworten auf Sicherheitsfragen erst nach der Anzeige dieser Fehlermeldung zu registrieren. Sie können die Fehlermeldung dann schließen und die Anmeldung und Registrierung abschließen.

Wenn nach der Fehlermeldung und Registrierung eine Anwendung aus der Datei session.xml nicht geöffnet wird, sollten sich Benutzer abmelden und erneut am Konto anmelden. Die Startskripte für Hotdesktop werden erneut gestartet, die ohne Störung ausgeführt werden, da die Registrierung abgeschlossen ist und den Prozess nicht weiter verzögert.

Erstellen des Hotdesktop-Kontos

Sie müssen für Clientgeräte oder Arbeitsstationen, auf denen Hotdesktop ausgeführt wird, ein Hotdesktop-Konto erstellen. Dieses Hotdesktop-Konto kann ein Domänenkonto oder ein lokales Konto auf dem Gerät sein. Bei der Installation von Hotdesktop auf dem Clientgerät geben Sie Anmeldeinformationen für das Hotdesktop-Konto ein. Beim Start wird das Clientgerät bzw. die Arbeitsstation automatisch am Hotdesktop-Konto angemeldet und kann im Hotdesktop-Freigabemodus für Arbeitsstationen ausgeführt werden.

Benutzersitzungen werden "über" der Windows-Sitzung des Hotdesktop-Kontos ausgeführt (Benutzer können das Hotdesktop-Konto nur ändern, wenn Sie es Ihnen ausdrücklich gestattet haben). Benutzer starten eine Hotdesktop-Sitzung durch Eingabe der Windows-Domänenanmeldeinformationen. In einer Hotdesktop-Umgebung wird das Windows-Konto eines Benutzers als Hotdesktop-Benutzer bezeichnet.

Organisieren von Hotdesktop-Benutzern

Wenn Sie beabsichtigen, Hotdesktop bereitzustellen, sollten Sie zunächst die Benutzerumgebung einrichten. Sie können Hotdesktop-Benutzer zum Beispiel in Active Directory in mehreren Organisationseinheiten oder Gruppen zusammenfassen. Außerdem können Sie Benutzer, die Hotdesktop-Benutzer sind und auch eigene Arbeitsstation verwenden, in mehrere Gruppen unterteilen (und diesen Gruppen Prioritäten zuweisen).

Sie können dann Hotdesktop-Einstellungen, Anwendungsdefinitionen, Kennwortrichtlinien und andere Konfigurationsangaben auf mehrere Hotdesktop-Benutzer in diesen Organisationseinheiten anwenden.

Einschränken von Benutzerrechten

Da das Hotdesktop-Gerät von allen Hotdesktop-Benutzern gemeinsam verwendet wird, müssen Sie ggf. Berechtigungen auf ein Minimum beschränken, damit Benutzer die ihnen zugeordneten Anwendungen verwenden können. So sollten Hotdesktop-Benutzer nicht berechtigt sein, das Gerät herunterzufahren. Nur Mitglieder der Administratorgruppe sollten über diese Berechtigung verfügen.

Hotdesktop, Smartcards und Schlüsselwiederherstellung

Hinweis: Wählen Sie die Datenschutzoption Smartcardzertifikat der Benutzerkonfiguration, wenn Benutzer Smartcards in der Hotdesktop-Umgebung verwenden.
Wenn Sie Hotdesktop in einer Umgebung bereitstellen, in der sich Benutzer über Smartcards anmelden, wählen Sie für diese Benutzer nicht die Option Benutzer zur Eingabe des alten Kennworts auffordern als einzige Schlüsselwiederherstellungs- und Datenschutzmethode. Benutzer in diesen Umgebungen können das alte Kennwort nicht korrekt eingeben und hätten daher keinen Zugriff auf das System. Sie vermeiden dieses Problem, indem Sie zur Schlüsselwiederherstellung die Option "Automatische Schlüsselwiederherstellung" wählen oder eine fragenbasierte Authentifizierung als Option anbieten.

Richtlinien für das Hotdesktop-Konto

Beachten Sie beim Erstellen eines Hotdesktop-Kontos die folgenden Richtlinien:

- Stellen Sie sicher, dass das Konto nicht zur Gruppe der lokalen oder Domänenadministratoren gehört.
- Das Hotdesktop-Konto kann ein lokales oder ein Domänenkonto sein. Alle Berechtigungen, die für das Hotdesktop-Konto gelten, sind für den Hotdesktop-Benutzer nur für die von Ihnen angegebenen Anwendungen verfügbar. Sie können also angeben, welche Anwendungen mit Anmeldeinformationen für das Hotdesktop-Konto und welche mit den Windows-Domänenanmeldeinformationen des Benutzers gestartet werden.
- Bei der Installation von Hotdesktop werden der Anmeldename und die Domäne des Hotdesktop-Kontos geprüft. Stellen Sie beim Erstellen dieses Kontos sicher, dass die Option Kennwort läuft nie ab aktiviert ist. Verwenden Sie keine abgelaufenen Anmeldeinformationen.
- Stellen Sie sicher, dass dem Konto nur eingeschränkte Privilegien gewährt werden. Schränken Sie die Berechtigungen nur auf die Hotdesktop-Verwendung ein.
- Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen. Wenn Sie ein lokales Konto verwenden, geben Sie den Hostnamen des Gerätes an.
- Sie sollten das Hotdesktop-Konto "Hotdesktop" nennen. Dies stellt sicher, dass den Benutzern beim Abmelden angezeigt wird, dass sie sich von Hotdesktop abmelden sollen Wenn Sie statt "Hotdesktop" einen weniger aussagekräftigen Namen verwenden, kann die angezeigte Meldung für die Benutzer beim Abmelden verwirrend sein. Bei mehreren Gruppen von Hotdesktop-Benutzern können Sie für jedes Hotdesktop-Konto einen entsprechenden Namen wählen, z. B. "Hotdesktop Marketing", "Hotdesktop Buchhaltung" usw.

Anforderungen für Anwendungen, die mit Hotdesktop verwendet werden

Anwendungen, die in einer Hotdesktop-Umgebung verwendet werden, müssen die folgenden Voraussetzungen erfüllen:

- Anwendungen, für die Anmeldeinformationen des Benutzers benötigt werden, müssen in Anwendungsdefinitionen und Benutzerkonfigurationen für Single Sign-On eingerichtet sein.
- Anwendungen, die vom Hotdesktop-Konto gestartet werden, müssen in der interaktiven Windows-Umgebung ausführbar sein. Bei diesem Szenario benötigen die Anwendungen (und die Hotdesktop-Benutzer) Zugriff auf die Benutzerprofile, Netzwerkfreigaben und auf andere Ressourcen, die dem Hotdesktop-Konto zugeordnet sind.
- Die Anwendungen müssen in der Lage sein, sich ordnungsgemäß zu beenden, wenn sie dazu aufgefordert werden. Hotdesktop beendet Anwendungen mit ähnlichen Verfahren wie bei der Abmeldung von einer interaktiven Windows-Sitzung. Das ordnungsgemäße Beenden von Anwendungen ist in einer Hotdesktop-Umgebung besonders wichtig, da die Anwendung unter Umständen viele Male verwendet wird, bevor die Arbeitsstation oder das Clientgerät heruntergefahren wird.
- Alle Anwendungen, die im Profil des Benutzers vertrauliche Daten speichern oder zum Ändern von Einstellungen auf das Profil des Benutzers zugreifen müssen, sollten als Hotdesktop-Benutzerkonto ausgeführt werden. Anwendungen, die "gemeinschaftliche" Konfigurationsinformationen gemeinsam nutzen können, können als Hotdesktop-Konto ausgeführt

werden. Mit dem in der Datei session.xml definierten Skript zum Beenden können Administratoren sicherstellen, dass benutzerspezifische Dateien am Ende jeder Sitzung entfernt werden.

Wichtig: Wenn Single Sign-On Anmeldeinformationen in einer Hotdesktop-Umgebung für Terminalemulatoren senden soll, die Informationen in der Registrierungsstruktur HKEY_CURRENT_USER speichern, müssen Sie diese Anwendungen als Hotdesktop-Benutzerkonto ausführen. Sie können im Abschnitt "ShellExecute" der Datei process.xml festlegen, welche Terminalemulatoren als Hotdesktop-Benutzerkonto ausgeführt werden. Wenn ein Terminalemulator bei Sitzungsbeginn ausgeführt wird, legen Sie dies im entsprechenden Startskriptabschnitt in der Datei session.xml fest. Terminalemulatoren müssen im Startskript als Hotdesktop-Benutzerkonto ausgeführt werden.

Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer

Single Sign-On stellt zwei Dateien zur Verfügung, mit denen das Anwendungsverhalten in Hotdesktop-Umgebungen gesteuert werden: session.xml und process.xml.

Wichtig: Sie können für einen Prozess nicht festlegen, dass er in der Datei session.xml als Hotdesktop-Konto ausgeführt wird und ihn anschließend in der Datei process.xml als Hotdesktop-Benutzer definieren. Einträge in der Datei session.xml haben Vorrang vor den Einträgen, die Sie in der Datei process.xml unter dem Element vornehmen.
Einführung:

- Um sich an der Arbeitsstation oder am Benutzergerät für Verwaltungszwecke anzumelden (z. B. zum Bearbeiten der Datei process.xml), halten Sie während des Windows-Startvorganges die Umschalttaste gedrückt. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.
- Wenn Sie innerhalb einer Hotdesktop-Benutzersitzung die Hotdesktop-Datei session.xml, Kennwortablaufskripte oder andere Skripte sowie ausführbare Dateien oder Batchdateien ausführen, werden folgende Umgebungsvariablen nicht unterstützt: APPDATA, HOMEDRIVE, HOMEPATH, HOMESHARE und LOGONSERVER. Wenn eine dieser nicht unterstützten Variablen verwendet wird, kann das Skript, die Anwendung oder die ausführbare Datei unter Umständen nicht ausgeführt werden. Um dieses Problem zu vermeiden, sollten Anwendungen in einer Hotdesktop-Benutzersitzung nicht auf Umgebungsvariablen zugreifen, die nicht unterstützt werden.
- Sie müssen die Benutzer anweisen, die Anwendungen zu beenden, die als permanente Prozesse festgelegt sind. Wenn z. B. ein Benutzer einen permanenten Prozess startet, eine Datei erstellt und die Datei beim Beenden der Hotdesktop-Sitzung offen lässt, kann der nächste Benutzer, der sich anmeldet, den Inhalt dieser Datei sehen.
  Wichtig: Weisen Sie daher die Benutzer an, grundsätzlich alle sicherheitsrelevanten Anwendungen, die als permanente Prozesse festgelegt sind, zu schließen, bevor sie ihre Hotdesktop-Sitzungen beenden.
  Wenn Sie eine Anwendung in der Datei process.xml als permanent definieren und die Anwendung in einem Startskript in session.xml angeben, kann sich die Anzahl der Anwendungsinstanzen erhöhen, wenn die Benutzer neue Anwendungsinstanzen während einer Hotdesktop-Sitzung nicht beenden. Um dies zu verhindern, sollten Sie die Anzahl der Instanzen begrenzen, indem Sie ein Skript oder eine "Wrapper"-Anwendung erstellen, das bzw. die die Anwendung startet. Sie können auch die Anwendung selbst bearbeiten, um sicherzustellen, dass immer nur eine Instanz auf einmal ausgeführt wird.

- Anwendungen, die an der Eingabeaufforderung gestartet werden, werden als Hotdesktop-Konto ausgeführt, selbst wenn sie für die Ausführung als Hotdesktop-Benutzerkonto festgelegt worden sind. Um Anwendungen an der Eingabeaufforderung als Hotdesktop-Benutzerkonto zu starten, müssen Sie die Eingabeaufforderung im Abschnitt der Datei process.xml angeben. Wenn die Eingabeaufforderung als Hotdesktop-Konto ausgeführt wird, und die Dateitypzuordnung (z. B. *.txt) im Abschnitt der Datei process.xml definiert ist, wird die Anwendung als Hotdesktop-Benutzerkonto gestartet, wenn der Benutzer eine Datei mit der Dateierweiterung .txt startet.
- Bei permanenten Anwendungen, die das 8.3-Dateiformat verwenden, muss bei der Angabe in process.xml im Pfad der ausführbaren Datei ebenfalls das 8.3-Format verwendet werden.
- Während bei den XML-Tags und den Formatierungen in der Datei process.xml die Groß- bzw. Kleinschreibung

berücksichtigt wird, spielt sie bei den Pfadangaben und den Namen der ausführbaren Dateien keine Rolle.

- Wenn Benutzer SAP Logon for Windows (saplogon.exe) ausführen, muss sie als Hotdesktop-Benutzer ausgeführt werden. Geben Sie in der Datei process.xml unter dem Tag den Eintrag saplogon.exe ein.

Benutzerkonfigurationseinstellungen für Hotdesktop

Oct 05, 2015

Mit den folgenden Einstellungen der Benutzerkonfiguration können Sie die Benutzererfahrung von Hotdesktop anpassen.

Achtung: Für dieses Release müssen Sie eventuell die Registrierung bearbeiten. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Legen Sie stets eine Sicherungskopie der Systemregistrierung an, bevor Sie fortfahren.

Skriptpfad für Sitzungseinstellungen

Speicherort von Hotdesktop-Einstellungen in einer Benutzerkonfiguration

- Beim Erstellen einer neuen Benutzerkonfiguration stehen diese Einstellungen unter Erweiterte Einstellungen im Dialogfeld Plug-In-Verhalten konfigurieren zur Verfügung
- Beim Bearbeiten einer bestehenden Benutzerkonfiguration stehen diese Einstellungen im Bereich Hotdesktop im Dialogfeld Benutzerkonfiguration bearbeiten zur Verfügung.
  Weitere Informationen zu den Einstellungen finden Sie in den Abschnitten
  — Single Sign-On - Einstellungsreferenz > Benutzerkonfigurationen
  .

Konfigurieren des Skriptpfads für die Sitzungseinstellungen

1. Geben Sie auf der Seite Hotdesktop im Dialogfeld Benutzerkonfiguration bearbeiten im Textfeld Skriptpfad für Sitzungseinstellungen den Speicherort der Datei "session.xml" ein. Dies kann auch ein Netzwerkfreigabeordner ein. Wenn Sie die Datei session.xml zum Beispiel auf einer Netzwerkfreigabe wie \\Citrix\MPM\Share\ speichern, geben Sie hier den zugehörigen Pfad ein.
2. Starten Sie die Hotdesktop-Arbeitsstation nach dem Speichern der Benutzerkonfiguration und Installieren der Datei session.xml neu.

Verhalten mit der automatischen Schlüsselwiederherstellung

Wenn Hotdesktop in der Single Sign-On-Umgebung gemeinsam mit der Funktion zur automatischen Schlüsselwiederherstellung verwendet wird, werden Kennwortänderungen, die vom Administrator vorgenommen wurden, nicht an die Plug-in-Software der betroffenen Benutzer mit aktiven Hotdesktop-Sitzungen weitergegeben. Wenn diese Benutzer die aktiven Sitzungen sperren und dann versuchen, die Sperrung aufzuheben, werden sie unter Umständen unerwartet zur Eingabe des alten Kennworts aufgefordert. Benutzer sollten das Dialogfeld "Altes Kennwort" schließen und die Hotdesktop-Sitzung durch Abmelden beenden und neu starten, um die Plug-in-Software weiterzuverwenden.

Hotdesktop-Bildschirmschoner

Damit die Benutzer einfacher feststellen können, auf welchen Arbeitsstationen Hotdesktop ausgeführt wird, enthält die Hotdesktop-Installation einen individuell anpassbaren Bildschirmschoner. Der Bildschirmschoner wird erst gestartet, wenn die Arbeitsstation 10 Minuten lang inaktiv war.

Hinweis: Eine gesperrte Sitzung wird als aktive Sitzung betrachtet. Der Bildschirmschoner wird erst gestartet, wenn das

Gerät 10 Minuten lang im Leerlauf ist, oder sich alle Benutzer von der Arbeitsstation abgemeldet haben.

Installieren von Hotdesktop

Hotdesktop kann über eine neue oder bestehende Installation des Single Sign-On Plug-ins installiert werden.

1. Melden Sie sich am Benutzergerät als lokaler Administrator an.
2. Klicken Sie in der Systemsteuerung auf Programme und Funktionen.
3. Wählen Sie Single Sign-On Plug-In und klicken Sie auf Ändern.
4. Wählen Sie Ändern und klicken Sie auf Weiter.
5. Wählen Sie Hotdesktop und klicken Sie auf Weiter.
6. Bestätigen Sie die Meldung mit Ja, um die Terminaldienste und Remotedesktop zu deaktivieren.
7. Geben Sie den Speicherort des zentralen Speichers an und klicken Sie auf Weiter.
8. Geben Sie die Adresse des Dienstservers an und klicken Sie auf Weiter.
9. Geben Sie die Anmeldeinformationen des Benutzers für das Hotdesktop-Konto ein und klicken Sie auf Weiter. Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen.
10. Klicken Sie auf Installieren. Greifen Sie auf das Installationsmedium zu, damit das Installationsprogramm die MSI-Datei für das Single Sign-On Plug-in finden kann.

Starten Sie nach dem Abschluss der Installation das Benutzergerät neu.

Deinstallieren von Hotdesktop

Wenn Sie das Hotdesktop-Feature von einer Arbeitsstation entfernen, müssen Sie ggf. diese Schritte nach der Deinstallation des Hotdesktop-Features ausführen:

- Wiederherstellen von Terminaldiensten nach dem Deinstallieren von Hotdesktop
- Aktivieren mehrerer Sitzungen nach dem Deinstallieren von Hotdesktop

1. Halten Sie während des Windows-Startvorgangs die Umschalttaste gedrückt, um sich an der freigegebenen Arbeitsstation oder dem Clientgerät anzumelden und Administratoraufgaben auszuführen.
   Damit verhindern Sie, dass das Hotdesktop-Konto angemeldet wird und die Hotdesktop-Umgebung startet. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.

   Melden Sie sich als Administrator an.

2. Klicken Sie in der Systemsteuerung auf Programme und Funktionen.
3. Wählen Sie Single Sign-On Plug-In.
4. Klicken Sie auf Ändern, damit Sie nur das Hotdesktop-Feature entfernen.
5. Klicken Sie auf der Seite Anwendungswartung auf Ändern.
6. Klicken Sie auf der Seite Featureauswahl auf Hotdesktop und machen Sie das Feature nicht verfügbar.
7. Wählen Sie den Typ des zentralen Speichers und bestätigen Sie die Änderungen an der Plug-in-Software.
8. Starten Sie die Arbeitsstation neu.

Hotdesktop ist erst nach dem Neustart der Arbeitsstation komplett entfernt.
Wichtig: Beim Deinstallieren von Software, die die GINA-Kette unterbrochen haben könnte, ist es wichtig, die Software auf dem Clientgerät in der umgekehrten Reihenfolge zur Installation zu deinstallieren. Sonst kann es passieren, dass der Computer nicht mehr funktionsfähig ist. Bearbeiten Sie nicht die Registrierung.

Aktivieren der Terminaldienste nach der Deinstallation von Hotdesktop

Der Hotdesktop-Installationsprozess deaktiviert die Terminaldienste. Führen Sie die folgenden Schritte aus, um die

Terminaldienste zu aktivieren.

1. Melden Sie sich an der Arbeitsstation als Administrator an.
2. Klicken Sie auf Start > Ausführen und geben Sie regedit ein.
3. Ändern Sie den Wert des Registrierungsschlüssels in 1: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]TSEnabled=dword:00000001

Aktivieren mehrerer Sitzungen

Während der Hotdesktop-Installation setzt das Installationsprogramm diesen Registrierungsschlüssel auf 0 zurück. Führen Sie folgende Schritte aus, um mehrere Sitzungen zu aktivieren.

1. Melden Sie sich an der Arbeitsstation als Administrator an.
2. Klicken Sie auf Start > Ausführen und geben Sie regedit ein.
3. Ändern Sie den Wert des Registrierungsschlüssels in 1: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon] AllowMultipleSessions =dword:00000001

Anzeigen von Hotdesktop-Profilen

In einer Hotdesktop-Umgebung wird die Shell (explorer.exe) als Hotdesktop-Konto ausgeführt. Das bedeutet, dass die Shell keine Zugriffsrechte für das Navigieren zum Hotdesktop-Benutzerprofilordner hat.

1. Nehmen Sie in der Datei process.xml unter Internet Explorer (iexplore.exe) auf, damit diese Anwendung als Hotdesktop-Benutzer ausgeführt wird.
2. Melden Sie sich als Hotdesktop-Benutzer an und starten Sie Internet Explorer.
3. Geben Sie zum Anzeigen der Profile in der Adressleiste den vollständigen Pfad zum Hotdesktop-Benutzerprofilverzeichnis ein. Beispiel: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Citrix\MetaFrame Password Manager

Deaktivieren von AutoAdminLogon-Support

Wenn AutoAdminLogon aktiviert ist, kann es passieren, dass die Authentifizierung mit Drittanbieterprodukten nicht funktioniert. Einige Drittanbieteranwendungen deaktivieren oder entfernen den AutoAdminLogon-Wert während der Installation. In dieser Situation müssen Sie Hotdesktop-AutoAdminLogon deaktivieren.

1. Starten Sie die freigegebene Arbeitsstation oder das Benutzergerät neu und halten Sie während des Windows-Startvorgangs die Umschalttaste gedrückt. Damit verhindern Sie, dass das Hotdesktop-Konto angemeldet wird und die Hotdesktop-Umgebung startet. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.
2. Melden Sie sich als Administrator an.
3. Bearbeiten Sie die Registrierung und legen Sie unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\HotDesktop die folgenden Werte fest:

Wertname	Geben Sie	Wert
AutoAdminLogon	REG_SZ	0 zum Deaktivieren

4. Starten Sie nach dem Festlegen des Wertes die Arbeitsstation neu und melden Sie sich manuell mit den Anmeldeinformationen für das Hotdesktop-Konto an. Die Hotdesktop-Anmeldeseite wird angezeigt, von der aus die Benutzer eine Authentifizierung mit einer Drittanbieteranwendung durchführen können.

Ändern des Kennworts für das Hotdesktop-Konto

Unter Umständen müssen Sie das Kennwort für das Hotdesktop-Konto ändern. Sie haben die Anmeldeinformationen des Kontos bei der Plug-In-Installation eingegeben. Mit den folgenden Schritten ändern Sie das Kennwort.

1. Melden Sie sich an einer Arbeitsstation an, auf der Hotdesktop installiert ist.
   Wichtig: Verwenden Sie für Schritt 1 weder ein Administratorkonto noch die Anmeldeinformationen für das Hotdesktop-Konto.
2. Drücken Sie die Tastenkombination STRL+ALT+ENTF. Das Dialogfeld Windows-Sicherheit wird angezeigt.
3. Klicken Sie auf Kennwort ändern.
4. Geben Sie Folgendes ein oder wählen Sie einen Eintrag aus:
   - Benutzername für das Hotdesktop-Konto
   - Domänenname oder Name des lokalen Computers
   - Altes Kennwort
   - Neues Kennwort
5. Klicken Sie auf OK.
6. Klicken Sie im Dialogfeld Windows-Sicherheit auf Herunterfahren und dann auf Neu starten, um den Computer neu zu starten.

Herunterfahren einer Hotdesktop-Arbeitsstation

Da nur Administratoren Hotdesktop-Arbeitsstationen herunterfahren dürfen, enthält das Startmenü von Hotdesktop-Arbeitsstationen keine Option "Beenden".

Drücken Sie STRG+ALT+ENTF, um eine Hotdesktop-Arbeitsstation für eine administrative Verwendung herunterzufahren. Klicken Sie im angezeigten Dialogfeld Windows-Sicherheit auf Herunterfahren.

Dialog mit anderen Citrix Produkten

Single Sign-On unterstützt die Verwendung von Citrix Plug-ins mit Hotdesktop. Verwenden Sie die allgemeinen Richtlinien, die Sie berücksichtigen sollten, wenn Sie Hotdesktop mit diesen Plug-ins und dem Webinterface verwenden möchten:

- Bearbeiten Sie die Datei process.xml, um sicherzustellen, dass Citrix Receiver und das Citrix Offline Plug-In temporäre Prozesse sind (wenn das Plug-In vom Windows-Startprogramm gestartet wird und nach dem Start der ersten Hotdesktop-Sitzung weiter ausgeführt wird).
- Wenn Sie Security Service Provider Interface verwenden, müssen Sie das Plug-In als Hotdesktop-Benutzer ausführen. Sie können das Plug-In auch als Hotdesktop-Benutzer ausführen, wenn Sie Sicherheitsbedenken haben. Die ICA-Dateien werden im Profil gespeichert.
  - Bearbeiten Sie den Abschnitt der Datei process.xml so, dass Citrix Receiver und das Citrix Offline Plug-In als Hotdesktop-Benutzerkonten ausgeführt werden, wenn sie von der Windows-Shell aus gestartet werden.
  - Bearbeiten Sie die Datei session.xml, um ein Startskript oder eine ausführbare Datei festzulegen, das bzw. die beim Start der ersten Hotdesktop-Sitzung auch Citrix Receiver und das Citrix Offline Plug-In startet.

Citrix Receiver

Sie können Citrix Receiver für SSPI (Security Service Provider Interface) konfigurieren. Mit Security Service Provider Interface kann sich Citrix Receiver mit den Anmeldeinformationen des Hotdesktop-Benutzers beim XenApp-Server authentifizieren. Stellen Sie sicher, dass XenApp der Windows-Sicherheitsautorität vertraut, die für die Authentifizierung des Hotdesktop-Benutzers verwendet wird. Weitere Informationen zur Konfiguration von Security Service Provider Interface für Receiver finden Sie in den Abschnitten

— XenApp-Administration

.

Webinterface

Das Hot Desktop-Plug-In kann Anmeldeinformationen über das Webinterface an einen XenApp-Server senden. Weitere Informationen zur Konfiguration finden Sie in Abschnitten

— Webinterface

.

Die Datei "Session.xml"

Oct 05, 2015

Mit der Datei session.xml können Sie die Anwendungen festlegen, die beim Starten einer Hotdesktop-Sitzung gestartet werden (Startskript) und Dateien und andere Informationen entfernen, die nach einer Benutzersitzung noch vorhanden sind (Skript zum Beenden). Bearbeiten Sie die Datei nach Bedarf und speichern Sie sie auf einer Netzwerkfreigabe oder an einem anderen zentralen Speicherort, damit die Hotdesktop-Arbeitsstationen darauf zugreifen können. Sie geben diesen Speicherort der Datei "session.xml" in der Benutzerkonfiguration an.

Die gewünschten Tags müssen sich zwischen den Tags und in der Datei befinden.

Hinweis: Eine Beispieldatei für session.xml finden Sie im Ordner \Support auf dem Installationsmedium.

Beispiel: Bereinigen einer Sitzung mit einem Skript

Verwenden Sie ein mit Visual Basic erstelltes Skript zum Beenden, um alle Benutzerdaten zu bereinigen, die am Ende einer Sitzung noch vorhanden sind. Das Skript session_cleanup.vbs wird als Hotdesktop-Konto (mit der Bezeichnung HDSA) gestartet und befindet sich unter C:\.

Beispiel: Starten von Internet Explorer

Starten Sie Internet Explorer mit der URL des firmeninternen Intranets (mycompany.com). In diesem Fall wird Internet Explorer als Prozess ausgeführt, der dem Hotdesktop-Benutzer zugeordnet ist.

Hinweis: Die gewünschten Tags müssen sich zwischen den Tags und in der Datei befinden.

startup_scripts

In diesem Dateiabschnitt werden alle Anwendungen angegeben, die unter dem Hotdesktop-Konto und dem Windows-Konto für den Hotdesktop-Benutzer gestartet werden.

Wobei Folgendes gilt:

Konto	Gibt das Konto an, unter dem die Anwendung ausgeführt wird. Zur Verfügung stehen Hotdesktop-Benutzer oder der Benutzername für das Hotdesktop-Konto.
Arbeitsverzeichnis	Gibt das Arbeitsverzeichnis der Anwendung an.
Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen Computer an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: %ProgramFiles%\Internet Explorer\iexplore.exe. http://www.yahoo.com

shutdown_scripts

Bearbeiten Sie in der Datei session.xml die Anwendungen zum Beenden von Hotdesktop, damit alle nicht verwendeten Daten aus der vorherigen Benutzersitzung entfernt werden. In der Regel werden von diesen Anwendungen die

Konfigurationsdateien entfernt, die den nächsten Benutzer am Arbeiten hindern könnten, sowie sicherheitsrelevante Dateien, wie z. B. Protokolle, und im System gespeicherte Dokumente. Diese Anwendungen sollten sicherstellen, dass die Hotdesktop-Umgebung für die nächste Benutzersitzung bereinigt ist. Dieser Teil der Datei ist speziell für die Datensicherheit wichtig.

Hinweis: Bei Bedarf können Sie Administratorprogramme oder Skripte initiieren, mit denen die Benutzerumgebung nach dem Abmelden bereinigt wird. So können Sie z. B. mit der Drittanbieteranwendung ein Visual Basic-Skript schreiben, mit dem benutzerspezifische INI-Dateien gelöscht werden.

Wobei Folgendes gilt:

Konto	Gibt das Konto an, unter dem die Anwendung zum Beenden ausgeführt werden soll. Zur Verfügung stehenHotdesktop-Benutzer oder der Benutzername für das Hotdesktop-Konto.
Arbeitsverzeichnis	Gibt das Arbeitsverzeichnis der Anwendung an.
Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen Computer an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: c:\cleanup.vbs

Starten von Anwendungen mit Session.xml

Beachten Sie Folgendes:

- Die Anwendungen, die Sie in der Datei session.xml angeben, müssen bereits auf der Arbeitsstation installiert sein.
- Da Hotdesktop Teil der Single Sign-On Plug-in-Software ist, startet die Plug-in-Software automatisch und muss nicht in dieser Datei angegeben werden.

Andere Anwendungen, die in der Datei session.xml angegeben sind, können unter der Shell des Hotdesktop-Kontos gestartet werden; die Benutzer müssen möglicherweise Anmeldeinformationen eingeben. Die Plug-in-Software wird dann gemäß den Einstellungen in den Benutzerkonfigurationen ausgeführt.

Wichtig: Speichern Sie die Datei session.xml im UTF-8-Format. ANSI-Kodierung ist zulässig, wenn alle Zeichen sich im Bereich von 0 bis 127 (Standardzeichensatz für Englisch) befinden. Wenn die Datei session.xml Sonderzeichen oder Zeichen aus anderen Schriftsystemen enthält, wie z. B. asiatische Schriftzeichen, müssen Sie sie im UTF-8-Format speichern.

Die Datei "Process.xml"

Oct 05, 2015

Hinweis: Die Datei process.xml wird auf allen Arbeitsstationen oder Geräten erstellt, auf denen Hotdesktop im Verzeichnis %ProgramFiles%\Citrix\MetaFrame Password Manager\HotDesktop installiert ist. Eine Beispieldatei für process.xml finden Sie im Ordner \Support auf dem Installationsmedium. Änderungen an dieser Datei müssen daher auf jedem einzelnen Gerät vorgenommen werden. Sie können jedoch über Active Directory jede Datei process.xml für die einzelnen Benutzer über eine Computer-Gruppenrichtlinie ersetzen. Weitere Informationen finden Sie im Citrix Support-Artikel http://support.citrix.com/article/CTX110394.

Legen Sie mit der Datei process.xml fest, welche Anwendungen weiter ausgeführt werden sollen, nachdem sich ein Hotdesktop-Benutzer abgemeldet hat. Diese Anwendungen werden permanente Anwendungen oder permanente Prozesse genannt.

Sie können über die Datei process.xml auch alle Anwendungen festlegen, die nach dem Abmelden eines Hotdesktop-Benutzers beendet werden. Diese Anwendungen werden temporäre Anwendungen oder temporäre Prozesse genannt.

Die gewünschten Tags müssen sich zwischen den Tags und in der Datei befinden.

Wichtig: Speichern Sie die Datei process.xml im UTF-8-Format. ANSI-Kodierung ist zulässig, wenn alle Zeichen sich im Bereich von 0 bis 127 (Standardzeichensatz für Englisch) befinden. Wenn die Datei process.xml Sonderzeichen oder Zeichen aus anderen Schriftsystemen enthält, wie z. B. asiatische Schriftzeichen, müssen Sie sie im UTF-8-Format speichern.

shellexecute_processes

In diesem Dateiabschnitt können Sie alle Anwendungen oder Dateitypen angeben, die als Hotdesktop-Benutzer ausgeführt werden. Diese Einstellung gewährleistet die Sicherheit der Anwendungen, die mit den Anmeldeinformationen der aktuell angemeldeten Benutzer ausgeführt werden.

Hinweis: Nach der Installation gibt die Plug-In-Software automatisch eine ausführbare Shell-Anwendung, ssoshell.exe, (die Single Sign-On Plug-In-Software) in der Datei process.xml an. Standardmäßig ist dies der Prozess, der als Hotdesktop-Benutzer ausgeführt wird.

Während im Startskript in der Datei session.xml die Anwendungen festgelegt sind, die beim Starten einer Hotdesktop-Sitzung gestartet werden, werden in die Anwendungen aufgelistet, die Benutzer im Rahmen einer Hotdesktop-Sitzung starten können.

Anwendungsname

Wobei Folgendes gilt:

Anwendung	Gibt nur den Anwendungsnamen des Prozesses oder der Anwendung an, der bzw. die ausgeführt wird. Der vollständige Pfad ist nicht erforderlich. Beispiel: pnagent.exe.

Hinweis: In der Datei process.xml können außer statischen Dateinamen, z. B. Notepad.exe, auch Platzhalterzeichen (*) verwendet werden. Platzhalterzeichen können allein oder mit Dateinamen verwendet werden. Beispielsweise sind *.txt, pnagent.exe und *.doc gültige Anwendungsnamen.

persistent_processes

In diesem Dateiabschnitt können Sie alle Anwendungen angeben, die weiter ausgeführt werden, nachdem sich der Hotdesktop-Benutzer abgemeldet hat. Angegebene Anwendungen werden nach dem Beenden (Abmelden) der

Hotdesktop-Sitzungen nicht geschlossen, selbst wenn sie während einer Sitzung gestartet wurden. Geben Sie den vollständigen Pfad des permanenten Prozesses an, um sicherzustellen, dass nur die gewünschten Prozesse nach jeder Sitzung weiter ausgeführt werden.

Pfadoptionen

Wobei Folgendes gilt:

Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen Computer an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: %ProgramFiles%\Internet Explorer\iexplore.exe. http://www.yahoo.com

Hinweis: Nach der Installation erstellt die Plug-In-Software in der Datei process.xml automatisch einen Eintrag für eine permanente Anwendung namens activator.exe. Die Anwendung activator.exe ruft die Hotdesktop-Sitzungsanzeige für Benutzer auf. Die Sitzungsanzeige ist ein transparentes verschiebbares Fenster, das die Benutzer beim Anmelden sehen. Es enthält vom Administrator definierte Informationen zu Benutzern und ihren Sitzungen. Activator.exe gehört standardmäßig zu den permanenten Prozessen, d. h., die Anwendung wird nicht neu gestartet, wenn sich einer der Hotdesktop-Benutzer an- oder abmeldet.

transient_processes

In diesem Dateiabschnitt geben Sie alle Anwendungen an, die beendet werden, nachdem sich der Hotdesktop-Benutzer abgemeldet hat.

Hinweis: Nach der Installation wird von der Plug-In-Software in der Datei process.xml automatisch eine temporäre Anwendung namens shellexecute.exe festgelegt. Die Anwendung ist standardmäßig als temporärer Prozess definiert und wird beendet, wenn sich einer der Hotdesktop-Benutzer abmeldet.

Anwendungsname

Wobei Folgendes gilt:

Anwendung	Gibt nur den Anwendungsnamen des Prozesses oder der Anwendung an, der bzw. die beendet wird. Der vollständige Pfad ist nicht erforderlich. Beispiel: pnagent.exe.

Referenz

Oct 05, 2015

In dieser Referenz werden die Einstellungen und die Standardwerte beschrieben, die im Knoten "Single Sign-On" im Citrix AppCenter zur Verfügung stehen. Die Einträge sind gemäß der Position der Konsole geordnet.

Benutzerkonfigurationen

In diesem Abschnitt werden die Einstellungen und Steuerelemente von Benutzerkonfigurationen beschrieben. Alle Hinweise zur Navigation in diesem Abschnitt beziehen sich auf das Bearbeiten einer vorhandenen Benutzerkonfiguration. Zum Dialogfeld Benutzerkonfiguration bearbeiten gelangen Sie folgendermaßen:

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten

Grundlegendes Plug-In-Verhalten

Mit diesen Steuerelementen passen Sie an, wie das Single Sign-On Plug-In für diese Benutzerkonfiguration funktioniert. Die Einstellungen für die Benutzeroberfläche werden hier festgelegt.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Grundlegendes Plug-in-Verhalten

Benutzerseitiges Anzeigen des Kennworts für Anwendungen

Diese Einstellung steuert, ob Benutzer Kennwörter im Fenster "Kennwörter verwalten" anzeigen können. Wenn die Einstellung deaktiviert ist, ist die Schaltfläche "Anzeigen" deaktiviert. Wenn Sie die Kennwortanzeige auf bestimmte Anwendungen beschränken möchten, aktivieren Sie diese Einstellung und steuern Sie dann mit der entsprechenden Einstellung für die Kennwortrichtlinie, ob Benutzer die Kennwörter für Anwendungen anzeigen können, die von dieser Richtlinie verwaltet werden.

Standardeinstellung: Aktiviert

Neuauthentifizierung vor dem Anzeigen der Benutzerkennwörter erzwingen

Diese Einstellung steuert, ob sich Benutzer erneut an Single Sign-On authentifizieren müssen, bevor die Kennwörter angezeigt werden.

Standardeinstellung: Aktiviert

Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern

Diese Einstellung steuert, ob die Plug-In-Software den Benutzer auffordert, Anmeldeinformationen für neu erkannte Anwendungen hinzuzufügen.

Deaktivieren Sie diese Option, wenn die Single Sign-On Plug-In-Software keine Anwendungen erkennen soll, die nicht dieser Benutzerkonfiguration zugeordnet sind. Wenn diese Option deaktiviert ist, müssen die Benutzer ihre Anmeldeinformationen für diese Anwendungen manuell eingeben. Verwenden Sie diese Einstellung, um zu verhindern, dass Benutzer Anwendungen,

die aktuell nicht zu ihrer zugewiesenen Benutzerkonfiguration gehören, den Single Sign-On-Anwendungen hinzufügen.

Wenn diese Option deaktiviert ist, überschreibt sie die Option Benutzer können das Speichern der Anmeldeinfo bei Erkennung einer neuen Anwendung abbrechen auf der Seite Erweiterte Einstellungen > Clientseitiges Verhalten. Sollten Sie die Verwendung des Provisioning planen, verhindert ein Deaktivieren dieser Option auch, dass Benutzer zur Eingabe der Anmeldeinformationen aufgefordert werden.

Standardeinstellung: Aktiviert

Definierte Formulare automatisch verarbeiten, wenn das Single Sign-On sie erkennt

Aktivieren Sie diese Option, damit die Plug-In-Software gespeicherte Anmeldeinformationen automatisch ohne Eingriff des Benutzers senden kann. Wenn die dazugehörige Einstellung Dieses Formular automatisch senden in der Anwendungsdefinition aktiviert ist, die dieser Benutzerkonfiguration zugeordnet ist, werden die Felder zur Eingabe der Anmeldeinformationen in der Anwendung automatisch ausgefüllt.

Standardeinstellung: Aktiviert

Zeitraum zwischen Neuauthentifizierungsanfragen

Mit dieser Einstellung legen Sie den Zeitraum zwischen Plug-In-Anfragen zur Neuauthentifizierung fest. Wenn der angegebene Zeitraum abläuft, wird das Benutzergerät gesperrt und Benutzer müssen die primären Anmeldeinformationen eingeben, um sich neu zu authentifizieren. Der Mindestwert ist 1 Minute.

Standardeinstellung: 8 Stunden

Plug-In-Benutzeroberfläche

Mit diesen Steuerelementen legen Sie die Verzögerung für das Senden der Anmeldeinformationen und die Spalten im Fenster "Kennwörter verwalten" fest.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Plug-In-Benutzeroberfläche

Gibt die Dauer an, für die das Plug-In das Senden der Anmeldeinformationen verzögert

Aktivieren Sie diese Einstellung, um anzugeben, wie lange die Plug-In-Software nach dem Erkennen einer zulässigen Anwendung das Senden der Anmeldeinformationen verzögert. Wenn diese Einstellung aktiviert ist, können Sie angeben, um wie viele Sekunden das Senden der Anmeldeinformationen verzögert werden soll. Stellen Sie mit dieser Einstellung sicher, dass die Anwendung zum Empfang der Anmeldeinformationen bereit ist. In diesem Zeitraum zeigt die Plug-In-Software ein animiertes Symbol an, das angibt, dass die Plug-In-Software einen Vorgang ausführt.

Standardeinstellung: Nicht aktiviert (0 Sekunden)

Standardspalten und Standardspaltenreihenfolge Im Anmeldungsmanager festlegen

Mit dieser Einstellung steuert Sie, welche Spalten in der Detailansicht im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) angezeigt werden. Mit dieser Einstellung steuern Sie auch die Reihenfolge der Spalten.

Die Standardeinstellungen lauten:

- Anwendungsname
- Beschreibung
- Gruppe
- Letzte Verwendung
- Geändert

Clientseitiges Verhalten

Mit diesen Einstellungen werden die Ereignisprotokollierung in der Plug-In-Software, die Speicherung der Registrierungsschlüssel beim Beenden und die Speicherung von Anmeldeinformationen bei neu erkannten Anwendungen konfiguriert.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Clientseitiges Verhalten

Single Sign-On Plug-in-Ereignisse mit der Windows-Ereignisprotokollierung protokollieren

Aktivieren Sie dieses Steuerelement, um informative Ereignisse der Plug-In-Software mit der Windows-Ereignisprotokollierung aufzuzeichnen. Warnungen und Fehlerereignisse werden immer (unabhängig von dieser Einstellung) aufgezeichnet.

Standardeinstellung: Nicht aktiviert

Datenordner und Registrierungsschlüssel des Benutzers beim Beenden des Single Sign-On Plug-ins löschen

Aktivieren Sie dieses Steuerelement, wenn die Registrierungsschlüssel und Datenordner des Benutzers (einschließlich der verschlüsselten Anmeldeinformationen) beim Beenden der Plug-In-Software gelöscht werden sollen.

Standardeinstellung: Nicht aktiviert

Benutzer können das Speichern der Anmeldeinfo bei Erkennung einer neuen Anwendung abbrechen

Mit dieser Einstellung steuern Sie, ob Benutzer zum Speichern der Anmeldeinformationen aufgefordert werden, wenn die Plug-In-Software eine Anwendung erkennt, für die keine Anmeldeinformationen gespeichert sind. Wenn die Einstellung aktiviert ist, können die Benutzer wählen, ob sie die Anmeldeinformationen im Fenster "Kennwörter verwalten" (Anmeldungsmanager) jetzt, später oder nie speichern möchten. Wenn die Einstellung Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern auf der Seite Plug-In-Verhalten konfigurieren nicht aktiviert ist, fordert die Plug-In-Software die Benutzer nicht zum Speichern der Anmeldeinformationen auf.

Standardeinstellung: Aktiviert

Anzahl der Tage einschränken, für die gelöschte Anmeldeinformationen verfolgt werden

Mit diesen Steuerelementen geben Sie an, wie lange der zentrale Speicher Anmeldeinformationen verfolgt, die im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) gelöscht wurden. Wenn Anmeldeinformationen des Benutzers auf mehreren Clientgeräten gespeichert werden, löscht das Plug-In die Anmeldeinformationen, wenn in diesem Zeitraum eine Synchronisierung mit dem zentralen Speicher erfolgt. Wenn die Anmeldeinformationen beim Ablauf des Zeitraums immer noch auf dem Clientgerät gespeichert sind, werden sie wiederhergestellt, wenn das Plug-In mit dem zentralen Speicher synchronisiert wird.

Standardeinstellung: Aktiviert/180 Tage

Synchronisierung

Mit diesen Steuerelementen werden die folgenden Optionen eingestellt: benutzerseitiges Aktualisieren der Plug-In-Einstellungen, Synchronisieren der Konfigurationsinformationen des Benutzers, Ausführen des Plug-Ins, wenn die Verbindung mit dem zentralen Speicher nicht mehr möglich ist sowie Angeben des Zeitraums zwischen automatischen Synchronisierungsintervalls.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Synchronisierung

Benutzer können die Einstellungen für das Single Sign-On Plug-In aktualisieren

Aktivieren Sie diese Einstellung, um den Benutzern das Aktualisieren der Einstellungen in der Plug-In-Software im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) zu ermöglichen. Wenn die Einstellung deaktiviert ist, ist die Schaltfläche Aktualisieren im Fenster "Kennwörter verwalten" deaktiviert.

Standardeinstellung: Aktiviert

Beim Start erkannter Anwendungen/des Anmeldungsmanagers synchronisieren

Aktivieren Sie diese Einstellung, wenn die Plug-In-Software die Informationen zur Benutzerkonfiguration immer synchronisieren soll, wenn ein Benutzer eine erkannte Anwendung oder den Anmeldungsmanager startet. Häufiges Synchronisieren kann die Leistung auf dem Client und Server beeinträchtigen und den Netzwerkdatenverkehr erhöhen.

Standardeinstellung: Nicht aktiviert

Single Sign-On Plug-In funktioniert ohne Wiederverbindung zum zentralen Speicher

Diese Einstellung steuert, ob Single Sign-On ausgeführt wird, wenn für die Synchronisierung keine Verbindung zum zentralen Speicher hergestellt werden kann. Bei Aktivierung dieser Option wird eine lizenzierte Instanz des Single Sign-On Plug-Ins weiter ausgeführt, selbst wenn die Verbindung fehlschlägt. Bei Deaktivierung der Einstellung wird die Plug-In-Software nur ausgeführt, wenn eine Verbindung zum zentralen Speicher besteht.

Standardeinstellung: Aktiviert

Zeitraum zwischen automatischen Synchronisierungsanfragen

Mit diesem Steuerelement geben Sie den Zeitraum zwischen automatischen Synchronisierungsversuchen an. Die automatische Synchronisierung hängt nicht von der Benutzeraktivität ab und wird zusätzlich zu anderen Ereignissen ausgeführt, die eine Synchronisierung auslösen.

Standardeinstellung: Nicht aktiviert/0 Minuten

Zugriff auf Anmeldeinfo über das Modul 'Synchronisierung der Anmeldeinformationen' zulassen

Aktivieren Sie diese Einstellung, um Remoteclients zu erlauben, über den Dienst auf die Anmeldeinformationen der Benutzer zuzugreifen. Diese Option wird zusammen mit der Kontozuordnung verwendet. Mit dieser Option kann sich ein Benutzer einer Plug-In-Software mit einem oder mehreren Windows-Konten an jeder Anwendung anmelden.

Standardeinstellung: Nicht aktiviert

Kontozuordnung

Da Unternehmen über mehrere Windows-Domänen verfügen können, können Benutzer auch mehrere Windows-Konten haben. Mit der Kontozuordnung kann sich ein Benutzer der Agentsoftware mit jedem Windows-Konto des Benutzers an jeder Anwendung anmelden. Mit dieser Steuerelementen können die Benutzer die Anmeldeinformationen mehrerer Windows-Konten zuordnen.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Kontozuordnung

Benutzer können Konten zuordnen

Aktivieren Sie diese Einstellung, um den Benutzern zu erlauben, mehrere Windows-Konten zuzuordnen und die URL sowie den Port anzugeben, an dem das Modul "Synchronisierung der Anmeldeinformationen" installiert ist. Bei der Erstkonfiguration einer Benutzerkonfiguration kann diese Option nicht eingestellt werden. Sie kann nur beim Bearbeiten einer vorhandenen Konfiguration definiert werden.

Standardeinstellung: Nicht aktiviert

Standarddienstadresse angeben

Aktivieren Sie diese Einstellung, wenn die Standarddienstadresse und der Dienstport des Moduls "Synchronisierung der Anmeldeinformationen" definiert werden sollen. Nach der Definition der Einstellungen können Sie die Option "Wird überprüft" auswählen, um den Adresspfad und den Dienstport zu überprüfen.

Standardeinstellung: /MPMService/

Dienstport: 443

Benutzer können Dienstadresse bearbeiten

Wenn eine Dienstadresse definiert wurde, können Sie durch Aktivierung dieser Einstellung festlegen, dass die Benutzer die Einstellungen über die Plug-In-Benutzeroberfläche bearbeiten können. Aktivieren Sie diese Option, wenn die Anmeldeinformationen an mehreren Stellen synchronisiert werden, und die Benutzer die Möglichkeit zum Wechseln haben müssen.

Standardeinstellung: Nicht aktiviert

Standarddomäne angeben

Aktivieren Sie diese Einstellung, um die Standarddomäne anzugeben, die für die Authentifizierung verwendet wird, wenn die Plug-In-Software mit dem zugeordneten Windows-Konto synchronisiert wird. Wenn diese Einstellung aktiviert ist, können Sie den Standarddomänennamen im entsprechenden Feld eingeben. Wenn Sie die Domäne nicht angeben, wissen die Benutzer möglicherweise nicht, welche Anmeldeinformationen eingegeben werden sollen.

Standardeinstellung: Nicht aktiviert

Benutzer können Domäne bearbeiten

Aktivieren Sie diese Einstellung, um den Benutzern zu ermöglichen, die Standarddomäne zu bearbeiten, die für die Authentifizierung verwendet wird, wenn die Plug-In-Software mit dem zugeordneten Windows-Konto synchronisiert wird.

Standardeinstellung: Nicht aktiviert

Benutzer können Kennwort speichern

Aktivieren Sie diese Einstellung, um den Benutzern zu ermöglichen, das Kennwort des zugewiesenen Windows-Kontos in der Plug-In-Software zu speichern.

Standardeinstellung: Nicht aktiviert

Anwendungsunterstützung

Mit diesen Steuerelementen kann die Plug-In-Software bestimmte clientseitige Anwendungsdefinitionen erkennen, die Unterstützung für den Terminalemulator aktivieren und die Mindestanzahl der Domänennamenstufen für die Zuordnung für Webanwendungen definieren.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Anwendungsunterstützung

Clientseitige Anwendungsdefinitionen erkennen

Aktivieren Sie diese Einstellung, damit Single Sign-On Anwendungen mit einer der folgenden Methoden erkennen kann.

- Alle Anwendungen
  Die Software erkennt und reagiert auf Anwendungen, die von einem Administrator oder einem Benutzer (im Fenster "Kennwörter verwalten", früher Anmeldungsmanager) und bei der Installation in den Standardeinstellungen definiert wurden.
- Nur Anwendungen, die von Benutzern im Anmeldungsmanager definiert sind
  Die Software erkennt und reagiert auf Anwendungen, die von einem Administrator und einem Benutzer im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) festgelegt sind. Die Plug-In-Software erkennt keine Anwendungen und reagiert nicht auf Anwendungen, die bei der Installation in den Standardeinstellungen definiert wurden.
- Nur Anwendungen, die mit dem Single Sign-On Plug-In eingeschlossen sind
  Die Software erkennt und reagiert auf Anwendungen, die von einem Administrator und in den Standardeinstellungen bei der Installation definiert sind. Benutzer können keine eigenen Anwendungsdefinitionen im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) erstellen.

Standardeinstellung: Alle Anwendungen

Support für Terminalemulatoren aktivieren

Diese Einstellung steuert die Unterstützung von Terminalemulationsprogrammen. Wenn diese Einstellung aktiviert ist, führt die Plug-In-Software einen Prozess aus, der Terminalemulatoren und terminalemulator-basierte Anwendungen erkennt.

Standardeinstellung: Nicht aktiviert

Zeitintervall, in dem das Plug-In den Terminalemulator auf Änderungen prüft

Mit dieser Einstellung geben Sie an, nach welcher Dauer (in Millisekunden) die Plug-In-Software prüft, ob beim Terminalemulator Bildschirmänderungen aufgetreten sind. Niedrigere Werte können mehr CPU-Zeit auf dem Client belegen und den Netzwerkdatenverkehr erhöhen.

Standardeinstellung: 3000 Millisekunden

Anzahl der Domänennamenstufen für Zuordnung

Mit dieser Einstellung wird die Mindestanzahl der Domänennamenstufen für die Zuordnung für zulässige Webanwendungen angegeben. Bei einem Wert von zwei oder kleiner wird *.domäne1.obersteDomäne zugeordnet; bei einem Wert von drei wird *.domäne2.domäne1.obersteDomäne zugeordnet. Domänennamenstufen, die über dem angegebenen Wert liegen, werden als Platzhalter behandelt. Wenn Sie die URL-Zuordnung für Webanwendungen stark steuern möchten, legen Sie die strenge URL-Zuordnung in den Anwendungsdefinitionen fest.

Standardeinstellung: 99

Hotdesktop

Diese Steuerelemente legen die Handhabung von Hotdesktop-Sitzungen fest.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Hotdesktop

Skriptpfad für Sitzungseinstellungen

Dieses Steuerelement gibt den Pfad der Datei mit den Sitzungseinstellungen an, in der die Skripts definiert sind, die am Anfang und Ende einer Hotdesktop-Sitzung ausgeführt werden. Sie können mit dem Startskript Anwendungen starten. Mit dem Skript zum Beenden können Aufräumarbeiten, wie z. B. das Entfernen von Dateien, ausgeführt werden. Alle Benutzer müssen auf die Datei zugreifen können.

Standardeinstellung: [leer]

Sperrtimeout

Mit diesem Steuerelement wird angegeben, wie viele Minuten eine Hotdesktop-Sitzung aktiv ist, wenn die Arbeitsstation im Leerlauf ist. Nach dem Ablauf des Intervalls wird der Desktop gesperrt.

Standardeinstellung: 10 Minuten

Sitzungstimeout

Mit diesem Steuerelement wird angegeben, wie viele Minuten eine Hotdesktop-Sitzung ausgeführt wird, wenn der Desktop

gesperrt ist. Nach Ablauf des Zeitraums wird die Sitzung beendet, und eine neue Sitzung wird gestartet, wenn der Desktop entsperrt wird.

Standardeinstellung: 5 Minuten

Sitzungsanzeige aktivieren

Diese Einstellung steuert, ob ein Fenster aktiviert ist, das die Hotdesktop-Sitzung kennzeichnet. Bei Aktivierung dieser Einstellung wird in Hotdesktop-Sitzungen ein transparentes, verschiebbares Fenster auf dem Desktop angezeigt. Das Fenster zeigt den Namen des Benutzers und die Dauer der aktiven Sitzung an.

Standardeinstellung: Aktiviert

Grafik aktivieren

Mit diesem Steuerelement wird der Pfad der Grafikdatei angegeben, die in der Anzeige der Hotdesktop-Sitzung angezeigt wird. Die angegebene Datei muss im Windows-Bitmap-Dateiformat (.bmp) in einem Verzeichnis gespeichert sein, auf das alle Benutzer zugreifen können.

Im Ordner %ProgrammFiles%\Citrix\MetaFrame Password Manager\Hot Desktop steht hierfür auf den einzelnen Hotdesktop-Arbeitsstationen die Standardgrafik Citrix.bmp bereit.

Standardeinstellung: [Keine]

Lizenzierung

Mit diesen Steuerelementen geben Sie den Lizenzserver und das Lizenzierungsmodell an.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Lizenzierung

Wichtig: Für lokal installierte Instanzen des Single Sign-On Plug-Ins wird keine separate Lizenz für Benutzer benötigt, die auf gehostete Anwendungen in einer Umgebung mit Citrix XenApp, Platinum Edition, zugreifen können.

Name des Lizenzservers

Geben Sie den vollqualifizierten Domänennamen (Hostname.Domäne.tld) an, der dem Lizenzserver zugeordnet ist.

Standardeinstellung: [leer]

Standard verwenden (für Portnummer des Lizenzservers)

Aktivieren Sie diese Einstellung, um den Standardwert für den Zugangsport auf dem Lizenzserver zu verwenden. Wenn der Lizenzserver einen anderen Port als den Standardport abhört, deaktivieren Sie diese Einstellung und geben Sie den Zugangsport im entsprechenden Feld ein.

Standardeinstellung: Aktiviert

Standardport: 27000

Lizenzierung benannter Benutzer

Diese Option ist aktiviert, wenn Sie als Produktedition Single Sign-On Advanced ausgewählt haben. Sie können diese Option

auch auswählen, wenn Sie als Produktedition Single Sign-On Enterprise einstellen. Mit diesem Lizenztyp kann Single Sign-On nur von bestimmten, benannten Benutzern verwendet werden. Wenn diese Option aktiviert ist, müssen Sie angeben, wie lange (in Tagen, Stunden und Minuten) die Lizenz dem benannten Benutzer zugeordnet ist, bevor die Lizenz abläuft und die Plug-In-Software eine neue Verbindung zum Lizenzserver herstellt. Während des angegebenen Zeitraums wird die Lizenzverwaltung vom Benutzer gesteuert, auch wenn der Computer heruntergefahren wird.

Standardeinstellung: Aktiviert für Single Sign-On Advanced Edition; nicht verfügbar für XenApp Platinum Edition

Standardeinstellung für Trennung: 21 Tage

CCU-Lizenzierung (nur Enterprise und Platinum Edition)

Diese Option ist aktiviert, wenn Sie als Produktedition Single Sign-On Enterprise oder XenApp Platinum auswählen. Sie ist nicht verfügbar, wenn Sie als Produktedition Advanced Edition ausgewählt haben.
Hinweis: Dieses Lizenzierungsmodell ist aktiviert, wenn Sie von den Password Manager Version 4.1 aktualisiert haben. In Bezug auf die Lizenzierung betrachtet Citrix Systems beim Upgrade diese frühere Version als gleichwertig zu Single Sign On 5.0 Enterprise Edition.
Mit diesem Lizenztyp kann eine einzelne Single Sign-On-Lizenz von mehreren Benutzern gemeinsam verwendet werden (jedoch nicht gleichzeitig). Dieser Lizenztyp wird auch als Lizenzierungsmodell Gleichzeitige Benutzer) bezeichnet.

Standardeinstellung: Aktiviert für Single Sign-On Enterprise oder XenApp Platinum Edition; nicht verfügbar für Single Sign-On Advanced Edition

Standardeinstellung für Trennung: 1 Stunde, 30 Minuten, wenn Lizenzverbrauch für Offlineverwendung zulassen deaktiviert ist, 21 Tage, wenn Lizenzverbrauch für Offlineverwendung zulassen aktiviert ist

Lizenzverbrauch für Offlineverwendung zulassen

Diese Option steht nur zur Verfügung, wenn die Option CCU-Lizenzierung aktiviert ist. Aktivieren Sie diese Einstellung, um anzugeben, wie lange ein Benutzer im getrennten Modus (offline) sein darf, bevor die Lizenz abläuft und in den Pool der verfügbaren Lizenzen zurückgeführt wird. Bei Aktivierung behält der Benutzer die Kontrolle über die Lizenz für den angegebenen Zeitraum, selbst wenn der Computer heruntergefahren wird. Standardmäßig ist ein Zeitraum von 1 Stunde und 30 Minuten eingestellt. Es sollte ein Wert zwischen 2 und 365 Tagen definiert werden.

Standardeinstellung: Nicht aktiviert

Fortfahren ohne Prüfung der Lizenzierungsinformationen

Mit dieser Einstellung kann die Bearbeitung ohne gültigen Namen eines Lizenzservers und Ports fortgesetzt werden.

Standardeinstellung: Nicht aktiviert

Datenschutzmethoden

Jul 22, 2016

Mit diesen Einstellungen werden die primären Datenschutzmethoden ausgewählt, die für den Schutz der Anmeldeinformationen der Benutzer verwendet werden. In einigen Umgebungen können die Benutzer mehrere Methoden verwenden.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Datenschutzmethoden

Administratorkontozugriff auf Benutzerdaten steuern

Wählen Sie Ja aus, wenn Administratoren nicht auf die Anmeldeinformationen der Benutzer zugreifen dürfen. Wenn Sie diese Option aktivieren, werden die Optionen unter "Microsoft Data Protection API" (einschließlich der Option DPAPI mit Profil im Auswahlfeld Smartcardschlüsselquelle sowie die Option Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul) unter Sekundäre Datenschutzmethode deaktiviert. Mit dieser Konfiguration haben Administratoren, wie z. B. der Kontoadministrator, keinen Zugriff auf die Benutzerkennwörter oder die Benutzerdaten. Damit wird verhindert, dass ein Administrator die Identität eines Benutzers annimmt. Mit dieser Standardeinstellung kann der Administrator sich nicht als Benutzer anmelden und möglicherweise auf Daten zugreifen, die im lokalen Speicher der Anmeldeinformationen des Benutzers gespeichert sind.

Wählen Sie Nein, wenn Sie die Verwendung aller Features für die mehrfache Authentifizierung auf dieser Seite und in den Konfigurationseinstellungen Sekundäre Datenschutzmethode zulassen möchten.

Standardeinstellung: Ja

Wählen Sie alle in Frage kommenden Datenschutzmethoden aus, um dem Benutzer die Anmeldung zu erleichtern.

Aktivieren Sie diese Option, um die primären Authentifizierungsfunktionen zu verwenden, die in den Einstellungen aktiviert werden, die in der nachfolgenden Tabelle beschrieben werden.

Standardeinstellung: Aktiviert

Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden

Option	Beschreibung
Authentifizierungsdaten der Benutzer	Zum Zugreifen auf die Benutzerdaten und den Datenschutz wird ein "Geheimnis" verwendet. Bei diesem Geheimnis zur Authentifizierung kann es sich um ein Benutzerkennwort oder ein PIN-basiertes Gerät in der Umgebung handeln. Standardeinstellung: Aktiviert Außerdem stehen die folgenden Optionen zum Datenschutz zur Verfügung: Smartcard-PINs zulassen Aktivieren Sie diese Option, um die Verwendung von Smartcard-PINs als Geheimnis zum Datenschutz zu ermöglichen. Verwenden Sie diese Option nur, wenn das Unternehmen oder die Umgebung eine "starke PIN-Richtlinie" hat.

Option	Beschreibung
	Standardeinstellung: Nicht aktiviert Schutz mit leeren Kennwörtern zulassen Aktivieren Sie diese Option nur, wenn die Sicherheitsanforderungen in der Domäne gering sind und die Benutzer leere Domänenkennwörter verwenden dürfen. Wenn diese Option aktiviert ist und die Plug-in-Software erkennt, dass der Benutzer ein leeres Kennwort hat, wird aus der Benutzerkennung ein Geheimnis abgeleitet. Wenn Sie diese Option nicht aktivieren, leitet die Plug-in-Software kein Geheimnis ab und führt auch keine anderen Datenschutzmaßnahmen mit dem leeren Kennwort aus. Wenn Sie die Option Authentifizierungsdaten der Benutzer aktivieren, die Optionen Smartcard-PINs zulassen und Schutz mit leeren Kennwörtern zulassen jedoch nicht, wird eine Fehlermeldung angezeigt, wenn sich der Benutzer zur Erstregistrierung mit einem leeren Kennwort anmeldet, und die Plug-in-Software wird deaktiviert. Standardeinstellung: Nicht aktiviert
Microsoft Data Protection API	Aktivieren Sie diese Option, wenn Sie servergespeicherte Profile mit einem Kerberos-Netzwerkauthentifizierungsprotokoll für die Benutzer verwenden. Diese Option funktioniert nur, wenn servergespeicherte Profile verfügbar sind. Sie würden die Option Authentifizierungsdaten der Benutzer sowie diese Option zum Beispiel dann aktivieren, wenn die Benutzer mit Kennwörtern auf die Computer und mit einem Kerberos-Netzwerkauthentifizierungsprotokoll auf Computer mit einer Citrix XenApp-Farm zugreifen. Mit dieser Methode können Benutzer sich auch mit Anmeldeinformationen und Smartcards anmelden. Standardeinstellung: Nicht aktiviert
Smartcardzertifikat	Aktivieren Sie diese Option, um den Benutzern die Verwendung von kryptographischen Karten zu erlauben, mit denen Authentifizierungsdaten verschlüsselt und entschlüsselt werden. Citrix empfiehlt, diese Option möglichst bei Verwendung von Hotdesktop in der Umgebung zu aktivieren. Standardeinstellung: Nicht aktiviert

Aktivieren Sie diese Option und wählen Sie eine Methode aus dem Listenfeld Smartcardschlüsselquelle aus, wenn die Benutzer eine primäre Authentifizierungsmethode verwenden können bzw. Sie Version 4.0 oder 4.1 der Plug-In-Software verwenden. Wenn Sie den zentralen Speicher von Version 4.1 auf Version 5.0 aktualisiert haben, ist diese Option automatisch aktiviert.

Diese Option ist nur mit der Triple DES-Verschlüsselungsmethode verfügbar.

Mögliche Smartcardschlüsselquellen sind:

- PIN-Nummer als Kennwort

- Smartcard-Datenschutz
- "DPAPI mit Profil" (nicht verfügbar, wenn Sie Möchten Sie den Administratorkontozugriff auf Benutzerdaten beschränken? ausgewählt haben

Standardeinstellung: Nicht aktiviert

Sekundäre Datenschutzmethode

Mit diesen Optionen können Sie die Optionen für den Datenschutz mit sekundären Anmeldeinformationen festlegen, die verwendet werden, bevor die Sperre der Anmeldeinformationen des Benutzers aufgehoben wird, wenn ein Benutzer seine primäre Authentifizierung ändert (z. B. beim Ändern des Domänenkennworts oder Austauschen der Smartcard). Alternativ können Sie einstellen, dass Anmeldeinformationen automatisch wiederhergestellt werden, wenn das Modul "Schlüsselverwaltung" implementiert ist.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Sekundäre Datenschutzmethode

Benutzeridentität prüfen

Standardeinstellung: Aktiviert

Aktivieren Sie dieses Optionsfeld, um eine der folgenden Methoden zur Neuauthentifizierung der Benutzer auszuwählen:

Option	Beschreibung
Benutzer zur Eingabe des alten Kennworts auffordern	Beachten Sie, dass Benutzer, die ihr Kennwort vergessen, ausgesperrt werden und sich mit den sekundären Anmeldeinformationen neu registrieren müssen, wenn Sie diese Option aktivieren. Aktivieren Sie diese Option nicht, wenn die Benutzer Smartcards für die primäre Authentifizierung einsetzen. Standardeinstellung: Aktiviert
Benutzerseitige Auswahl der Methode: Altes Kennwort oder Sicherheitsfragen	Wenn Sie diese Option aktivieren, werden die Benutzer aufgefordert, sich mit der von ihnen ausgewählten Methode zu authentifizieren. Diese Option enthält diese Unteroption: Identitätsprüfung wie in vorherigen Password Manager-Versionen Aktivieren Sie diese Option, wenn Sie von Password Manager Version 4.0 oder 4.1 aktualisiert und die fragenbasierte Authentifizierung oder Fragen zur Identitätsprüfung aktiviert haben. In diesem Fall müssen die Versionen 4.0 und 4.1 der Plug-in-Software nicht auf den Dienst zugreifen. Standardeinstellung: Nicht aktiviert

Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul)

Aktivieren Sie diese Option, wenn Sie das Schlüsselverwaltungsmodul zum Auslassen der Identitätsprüfung und zum automatischen Aufheben der Sperrung der Anmeldeinformationen der Benutzer implementieren. Diese Methode ist nicht so sicher wie andere Datenschutzmethoden, jedoch benutzerfreundlicher, da die Anmeldeinformationen automatisch abgerufen werden.

Standardeinstellung: Nicht aktiviert

Features von Self-Service

Für die in diesem Bereich zur Verfügung stehenden Optionen muss das Dienstmodul "Schlüsselverwaltung" installiert werden. Dieses Modul erweitert das Windows-Anmeldedialogfeld um eine Schaltfläche, mit der die Benutzer ihre Kennwörter zurücksetzen können.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Self-Service-Features

Benutzerseitiges Zurücksetzen des primären Domänenkennworts

Aktivieren Sie diese Einstellung, um das benutzerseitige Zurücksetzen des Kennworts ohne Intervention des Administrators zu ermöglichen.

Standardeinstellung: Nicht aktiviert

Benutzerseitiges Entsperren des Domänenkontos

Aktivieren Sie diese Einstellung, um den Benutzern zu ermöglichen, das Domänenkonto zu entsperren.

Standardeinstellung: Nicht aktiviert

Schlüsselverwaltungsmodul

Mit diesen Steuerelementen werden der Dienstspeicherort und der Dienstport für das Schlüsselverwaltungsmodul definiert.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Schlüsselverwaltungsmodul

Dienstspeicherort (Schlüsselverwaltungsmodul)

Mit dieser Einstellung geben Sie die Dienstadresse und den Dienstport für das Schlüsselverwaltungsmodul an. Prüfen Sie mit der Schaltfläche "Wird geprüft", ob die Einstellungen gültig sind.

Standardeinstellung: [leer]

Dienstport: 443

Provisioningmodul

Mit dem Provisioningmodul können die Anmeldeinformationen der Benutzer in dieser Benutzerkonfiguration importiert, geändert und gelöscht werden. Auf dieser Seite müssen Sie den Speicherort und den Dienstport des Provisioningmoduls angeben.

Start > Alle Programme > Managementkonsolen > Citrix AppCenter > Single Sign-On > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Provisioningmodul

Provisioning verwenden

Aktivieren Sie diese Einstellung, um das Provisioning zu verwenden.

Standardeinstellung: Nicht aktiviert

Dienstspeicherort (Provisioningmodul)

Mit dieser Einstellung werden die Dienstadresse und der Dienstport für das Provisioningmodul definiert. Prüfen Sie mit der Schaltfläche "Wird geprüft", ob die Einstellungen gültig sind.

Standardeinstellung: [leer]

Dienstport: 443

Anwendungsdefinitionen

Jul 22, 2016

In diesem Thema werden die Einstellungen und Steuerelemente zu Anwendungsdefinitionen beschrieben. Alle Hinweise zur Navigation in diesem Thema beziehen sich auf das Bearbeiten einer Anwendungsdefinition.

Anwendungsformulare

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Kennwortlänge und die Zeichenwiederholung gesteuert werden.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungsformulare > [Definiertes Formular] > Bearbeiten > Sonstige Einstellungen

Dieses Formular automatisch senden

Mit dieser Einstellung geben Sie an, ob das Plug-in automatisch auf die Schaltfläche "Senden" klickt oder der Benutzer manuell auf die Schaltfläche "Senden" klicken muss. Wählen Sie Dieses Formular automatisch senden, um das Formular ohne Benutzereingriff zu senden.

Standardeinstellung: Aktiviert

Anwendungssymbol

Mit diesem Steuerelement geben Sie das Symbol an, das neben der Anwendung im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) angezeigt wird.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungssymbol

Anwendungssymbol

Mit dieser Einstellung steuern Sie das Anwendungssymbol, das neben dem Anwendungsnamen im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) angezeigt wird. Zwei Optionen sind verfügbar:

- Standardsymbol verwenden
- Benutzerdefiniertes Symbol verwenden (Pfad eingeben).

Wenn Sie ein benutzerdefiniertes Symbol verwenden, können Sie den Pfad zur Symboldatei über die Schaltfläche "Durchsuchen" angeben. Jede standardmäßige Windows-Symboldatei kann verwendet werden. Microsoft Windows-Umgebungsvariablen werden unterstützt.

Standardeinstellung: Standardsymbol verwenden

Erweiterte Erkennung

Mit diesen Steuerelementen wird die Plug-in-Software gezwungen, nachfolgende Formulare für die Anmeldung oder die Kennwortänderung in einer Anwendungssitzung zu ignorieren, wenn eine Anmeldung oder Kennwortänderung bereits verarbeitet wurde.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungserkennung

Nur die erste Anmeldung für diese Anwendung verarbeiten

Aktivieren Sie dieses Steuerelement, wenn nur die erste Anmeldung für diese Anwendung verarbeitet werden soll und nachfolgende Anmeldeanfragen ignoriert werden sollen.

Standardeinstellung: Nicht aktiviert

Nur die erste Kennwortänderung für diese Anwendung verarbeiten

Aktivieren Sie dieses Steuerelement, wenn nur die erste Kennwortänderungsanfrage für diese Anwendung verarbeitet werden soll und nachfolgende Kennwortänderungsanfragen ignoriert werden sollen.

Standardeinstellung: Nicht aktiviert

Kennwortablauf

Mit diesen Steuerelementen werden die Einstellungen zum Kennwortablauf für diese Anwendung festgelegt. Das Einhalten der Ablaufrichtlinie von Single Sign-On wird nur erzwungen, wenn sie in der Kennwortrichtlinie aktiviert ist, die dieser Anwendung zugeordnet ist.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Kennwortablauf

Bei Kennwortablauf Skript ausführen

Aktivieren Sie diese Einstellung und geben Sie ein Skript und dessen absoluten Pfad an, wenn beim Ablauf des Kennworts eine bestimmte Skriptdatei ausgeführt werden soll. Verwenden Sie keinen UNC-Pfad.

Standardeinstellung: Nicht aktiviert

Citrix Single Sign-On-Ablaufwarnung verwenden

Aktivieren Sie diese Einstellung, um die Single Sign-On-Ablaufwarnung zu verwenden, wenn ein Kennwort abläuft.

Standardeinstellung: Nicht aktiviert

Kennwortrichtlinien

Jul 22, 2016

In diesem Abschnitt werden die Einstellungen und Steuerelemente zu Kennwortrichtlinien beschrieben. Alle Hinweise zur Navigation in diesem Abschnitt beziehen sich auf das Bearbeiten einer vorhandenen Kennwortrichtlinie. Zum Dialogfeld Kennwortrichtlinie bearbeiten gelangen Sie folgendermaßen:

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten

Grundlegende Kennwortregeln

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Kennwortlänge und die Zeichenwiederholung gesteuert werden.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Grundlegende Kennwortregeln

Mindestlänge für Kennwort

Gibt die Mindestanzahl der Zeichen für ein Kennwort an. Mindestwert = 0. Höchstwert = 128.

Standardeinstellung: 8

Höchstlänge für Kennwort

Gibt das Maximum der Zeichen für ein Kennwort an. Mindestwert = 1. Höchstwert = 128.

Standardeinstellung: 20

Höchstanzahl wiederholter Zeichen

Gibt an, wie oft ein Zeichen in einem Kennwort wiederholt werden kann. Mindestwert = 1. Höchstwert = 128.

Standardeinstellung: 6

Höchstanzahl aufeinanderfolgender gleicher Zeichen

Gibt die Höchstanzahl aufeinanderfolgender gleicher Zeichen an. Mindestwert = 1. Höchstwert = 128.

Standardeinstellung: 4

Regeln für Buchstaben

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Buchstaben in Kennwörtern gesteuert wird.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Buchstaben

Kleinbuchstaben zulassen

Steuert, ob Kleinbuchstaben in Kennwörtern zulässig sind.

Standardeinstellung: Kleinbuchstaben zulassen

Erstes Zeichen im Kennwort kann Kleinbuchstabe sein

Steuert, ob Kennwörter mit einem Kleinbuchstaben beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Kleinbuchstabe sein

Letztes Zeichen im Kennwort kann Kleinbuchstabe sein

Steuert, ob Kennwörter mit einem Kleinbuchstaben enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Kleinbuchstabe sein

Mindestanzahl der Kleinbuchstaben

Gibt die Mindestanzahl der Kleinbuchstaben in einem Kennwort an. Mindestwert = 0. Höchstwert = 128.

Standardeinstellung: 0

Großbuchstaben zulassen

Steuert, ob Großbuchstaben in Kennwörtern zulässig sind.

Standardeinstellung: Großbuchstaben zulassen

Erstes Zeichen im Kennwort kann Großbuchstabe sein

Steuert, ob Kennwörter mit einem Großbuchstaben beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Großbuchstabe sein

Letztes Zeichen im Kennwort kann Großbuchstabe sein

Steuert, ob Kennwörter mit einem Großbuchstaben enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Großbuchstabe sein

Mindestanzahl der Großbuchstaben

Gibt die Mindestanzahl der Großbuchstaben in einem Kennwort an. Mindestwert = 0. Höchstwert = 128.

Standardeinstellung: 0

Regeln für Ziffern

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Ziffern (0 bis 9) in Kennwörtern gesteuert wird.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Ziffern

Ziffern zulassen

Steuert, ob Ziffern in Kennwörtern zulässig sind.

Standardeinstellung: Sonderzeichen zulassen

Erstes Zeichen im Kennwort kann Ziffer sein

Steuert, ob Kennwörter mit einer Ziffer beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Ziffer sein

Letztes Zeichen im Kennwort kann Ziffer sein

Steuert, ob Kennwörter mit einer Ziffer enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Ziffer sein

Mindestanzahl der Ziffern

Gibt die Mindestanzahl der Ziffern in einem Kennwort an. Mindestwert = 0. Höchstwert = 128.

Standardeinstellung: 0

Höchstanzahl der Ziffern

Gibt die Höchstanzahl der Ziffern in einem Kennwort an. Mindestwert = 1. Höchstwert = 128.

Standardeinstellung: 20

Regeln für Sonderzeichen

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Sonderzeichen (keine Buchstaben und Ziffern) in Kennwörtern festgelegt wird.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Sonderzeichen

Sonderzeichen zulassen

Steuert, ob Sonderzeichen (keine Buchstaben und Ziffern) in Kennwörtern zulässig sind.

Standardeinstellung: Sonderzeichen zulassen

Erstes Zeichen im Kennwort kann Sonderzeichen sein

Steuert, ob Kennwörter mit einem Sonderzeichen beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Sonderzeichen sein

Letztes Zeichen im Kennwort kann Sonderzeichen sein

Steuert, ob Kennwörter mit einem Sonderzeichen enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Sonderzeichen sein

Mindestanzahl der Sonderzeichen

Gibt die Mindestanzahl der Sonderzeichen in einem Kennwort an. Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 0

Höchstanzahl der Sonderzeichen

Gibt die Höchstzahl der Sonderzeichen in einem Kennwort an. Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 20

Liste zulässiger Sonderzeichen

Gibt die für Kennwörter zulässigen Sonderzeichen an.

Standardeinstellung: !@#$^&*()_-+=[]\|,?

Ausschlussregeln

Mit diesen Steuerelementen werden die Zeichen und Zeichenfolgen angegeben, die für Kennwörter nicht zulässig sind.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Ausschlussregeln

Folgende Liste der Zeichen oder Zeichengruppen von Kennwörtern ausschließen

Wählen Sie die Option Liste bearbeiten aus, um das Dialogfeld Ausschlussliste bearbeiten zu öffnen. Dort können Sie bis zu 256 Zeichen oder Zeichengruppen angeben, die für Kennwörter nicht zulässig sind. Geben Sie ein Zeichen oder eine Zeichengruppe pro Zeile ein. Jede Gruppe kann maximal 32 Zeichen enthalten. Bei Zeichen und Zeichengruppen wird die Groß- und Kleinschreibung nicht beachtet.

Standardeinstellung: [leer]

Anwendungsbenutzername im Kennwort nicht zulassen

Steuert, ob der Anwendungsbenutzername im Kennwort zulässig ist. Aktivieren Sie dieses Kontrollkästchen, wenn der Anwendungsbenutzername im Kennwort nicht zulässig ist.

Standardeinstellung: Nicht aktiviert

Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen

Steuert, ob Teile des Anwendungsbenutzernamens im Kennwort zulässig sind. Dies umfasst alle Zeichengruppen, die vom Benutzernamen verwendet werden können. Diese Einstellung ist mit der Einstellung Zeichenanzahl in Teilen gekoppelt. Beispiel: Wenn diese Einstellung aktiviert ist und Zeichenanzahl in Teilen auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen "citrix" kein Kennwort mit den Zeichenfolgen "citr", "itri" oder "trix" verwenden

Standardeinstellung: Nicht aktiviert

Windows-Benutzername im Kennwort nicht zulassen

Steuert, ob der Anwendungsbenutzername im Kennwort zulässig ist. Wenn diese Option deaktiviert ist, kann der Windows-Benutzername im Kennwort verwendet werden. Diese Einstellung hängt eng mit der Einstellung Zeichenanzahl in Teilen zusammen. Beispiel: Wenn diese Einstellung aktiviert ist und Zeichenanzahl in Teilen auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen "citrix" kein Kennwort mit den Zeichenfolgen "citr", "itri" oder "trix" verwenden

Standardeinstellung: Nicht aktiviert

Kennwortverlauf und -ablauf

Diese Steuerelemente legen fest, ob ein neues Kennwort mit einem alten Kennwort identisch sein darf. Außerdem legen sie die Einstellungen zum Kennwortablauf fest.

Der Kennwortverlauf wird pro Benutzer gespeichert. Wenn Sie die Benutzerdaten für einen Benutzer zurücksetzen, wird der Kennwortverlauf entfernt, und der Kennwortverlauf kann nicht für die gelöschten Kennwörter erzwungen werden.

Die Option für den Kennwortablauf weist Benutzer darauf hin, dass ein Kennwort bald abläuft oder bereits abgelaufen ist. Die Benutzer können abgelaufene Anmeldeinformationen verwenden. Es werden jedoch Erinnerungen für das Ändern des Kennworts oder Aufforderungen zum Ändern des Kennworts angezeigt, bis das Kennwort im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) geändert wird.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Kennwortverlauf und -ablauf

Neues Kennwort darf nicht mit den alten Kennwörtern identisch sein

Steuert, ob das neue Kennwort mit einem der alten Kennwörter identisch sein darf. Die alten Kennwörter werden im Kennwortverlauf gespeichert.

Standardeinstellung: Neues Kennwort darf mit altem Kennwort identisch sein (Kontrollkästchen nicht aktiviert)

Anzahl der gespeicherten alten Kennwörter

Gibt die Anzahl alter Kennwörter an, die im Kennwortverlauf gespeichert sind. Der zulässige Mindestwert ist 1. Der zulässige Höchstwert ist 24.

Standardeinstellung: 1

Den Anwendungsdefinitionen zugeordnete Einstellungen für Kennwortablauf verwenden

Wenn diese Einstellung aktiviert ist, werden die definierten Einstellungen (Anzahl der Tage bis zum Ablauf des Kennworts und Anzahl der Tage für Hinweis der Benutzer auf Kennwortablauf) auf die Anwendungsdefinitionen angewendet, denen diese Richtlinie zugeordnet ist. Die Richtlinie von Single Sign-On funktioniert unabhängig von vorhandenen Kennwortablaufrichtlinien, die in die Anwendung integriert sind.

Standardeinstellung: Kennwortablauf nicht festgelegt (Kontrollkästchen nicht aktiviert)

Anzahl der Tage bis zum Kennwortablauf

Gibt die maximale Anzahl der Tage an, für die ein Kennwort nicht geändert werden muss. Der zulässige Mindestwert ist 1. Der zulässige Höchstwert ist 99999.

Standardeinstellung: 42

Anzahl der Tage für Hinweis der Benutzer auf Kennwortablauf

Gibt die Anzahl der Tage vor dem Ablauf eines Kennworts an, wenn der Benutzer Hinweise auf den Kennwortablauf erhält. Der zulässige Mindestwert ist 0. Der zulässige Höchstwert ist 99998.

Standardeinstellung: 14

Kennwortrichtlinie testen

Mit diesen Steuerelementen kann ein manuell generiertes Kennwort auf die Kompatibilität mit der definierten Richtlinie überprüft werden, automatisch ein mit der Richtlinie kompatibles Kennwort generiert werden und geprüft werden, ob mit den festgelegten Einschränkungen genügend Kennwörter für das Unternehmen generiert werden können.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Kennwortrichtlinie testen

Regeleinhaltung eines manuell erstellten Kennworts testen

Mit diesem Feld kann die Regeleinhaltung eines manuell erstellten Kennworts getestet werden. Geben Sie das manuell erstellte Kennwort ein und klicken Sie auf Testen. Das eingegebene Kennwort wird anhand aller definierten Kriterien überprüft.

Standardeinstellung: Keine

Regelkompatibles, willkürliches Kennwort erstellen

Mit diesem Steuerelement wird ein Kennwort generiert, das die aktuell definierten Kennwortkriterien erfüllt. Klicken Sie auf Erstellen, um ein regelkompatibles Kennwort zu generieren, das aus dem Feld kopiert werden kann (Strg+C).

Standardeinstellung: Keine

Mehrere eindeutige, regelkompatible Kennwörter erstellen und testen

Es kann vorkommen, dass die festgelegten Einschränkungen für Kennwörter dazu führen, dass nicht mehr genügend Kennwörter möglich sind. Mit diesem Steuerelement wird eine benutzerdefinierte Anzahl von regelkompatiblen Kennwörtern generiert, um zu ermitteln, ob die definierte Richtlinie flexibel genug ist, um den Anforderungen des Unternehmens in Bezug auf Kennwörter gerecht werden zu können. Klicken Sie auf Mehrere Kennwörter erstellen, um ein Dialogfeld zu öffnen, in dem Sie eine benutzerdefinierte Anzahl von Kennwörtern generieren können.

Standardeinstellung: Keine

Anmeldeeinstellungen

Mit diesen Steuerelementen wird definiert, ob die Option Anzeigen für Anwendungsdefinitionen verfügbar ist, die diese

Richtlinie verwenden, ob sich die Benutzer vor dem Senden der Anwendungsanmeldeinformationen neu authentifizieren müssen, und wie lange ein Benutzer nach einer fehlgeschlagenen Authentifizierung erneut versuchen darf, sich zu authentifizieren.

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Anmeldeeinstellungen

Benutzerseitiges Anzeigen des Kennworts für Anwendungen

Mit diesem Steuerelement legen Sie fest, ob die Schaltfläche Anzeigen für die Anwendungen, die von dieser Richtlinie verwaltet werden, im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) zur Verfügung steht. Wenn Benutzer im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) auf die Schaltfläche Anzeigen klicken, wird das Kennwort in Klartext angezeigt. Wenn diese Einstellung nicht aktiviert ist, können die Benutzer die Kennwörter nicht anzeigen.

Standardeinstellung: Die Schaltfläche Anzeigen wird nicht angezeigt (Kontrollkästchen ist nicht aktiviert)

Neue Benutzerauthentifizierung vor dem Senden der Anwendungsanmeldeinformationen erzwingen

Mit diesem Steuerelement legen Sie fest, ob die Benutzer ihre primären Anmeldeinformationen eingeben müssen, bevor das Plug-in die Anmeldeinformationen an die Anwendung sendet. Wenn diese Einstellung aktiviert ist, sperrt das Single Sign-On Plug-in die Arbeitsstation sofort, wenn es eine Anwendung erkennt, die von dieser Einstellung verwaltet wird. Benutzer müssen die primären Anmeldeinformationen eingeben, um die Arbeitsstation zu entsperren. Wenn die Arbeitsstation mit den richtigen Anmeldeinformationen entsperrt wurde, sendet das Plug-in die Anmeldeinformationen des Benutzers an die Anwendung. Diese Einstellung ist für Anwendungen nützlich, die auf vertrauliche Informationen zugreifen, da die Prüfung der Benutzeridentität erzwungen wird, bevor das Plug-in die Anmeldeinformationen an die Anwendung sendet.

Standardeinstellung: Benutzer müssen sich nicht neu authentifizieren (Kontrollkästchen ist nicht aktiviert)

Anzahl der Anmeldeversuche

Mit diesem Steuerelement legen Sie fest, wie oft das Plug-in die Anmeldeinformationen eines Benutzers in der angegebenen Zeitspanne erneut an dieselbe Anwendung senden kann. Wenn diese Einstellung auf den Mindestwert von 0 eingestellt ist, erhalten Benutzer sofort beim zweiten versuchten Senden der Anmeldeinformationen an die Anwendung eine Fehlermeldung.

Standardeinstellung: 0

Zeitlimit für Wiederholungsversuche

Mit diesem Steuerelement legen Sie fest, über welchen Zeitraum (in Sekunden) ein Benutzer seine Anmeldeinformationen erneut an dieselbe Anwendung senden kann, wenn das erste Senden der Anmeldeinformationen fehlgeschlagen ist.

Standardeinstellung: 30 Sekunden

Assistent für Kennwortänderungen

Mit diesem Steuerelement wird festgelegt, wie der Assistent für Kennwortänderungen auf Kennwortänderungsformulare antwortet. Eine der vier zur Auswahl stehenden Optionen muss aktiviert werden.

- Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen
- Benutzer können nur ein eigenes Kennwort erstellen
- Benutzer können nur ein systemgeneriertes Kennwort auswählen
- Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden

Start > Alle Programme > Citrix > Managementkonsolen > Citrix AppCenter > Single Sign-On > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Assistent für Kennwortänderungen

Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen

Aktivieren Sie diese Option, wenn die Benutzer im Assistenten für Kennwortänderungen zwischen einem systemgenerierten Kennwort und dem Erstellen eines eigenen wählen können.

Standardeinstellung: Aktiviert

Benutzer können nur ein eigenes Kennwort erstellen

Aktivieren Sie diese Option, wenn die Benutzer im Assistenten für Kennwortänderungen kein systemgeneriertes Kennwort auswählen können und ein eigenes erstellen müssen.

Standardeinstellung: Nicht aktiviert

Benutzer können nur ein systemgeneriertes Kennwort auswählen

Aktivieren Sie diese Option, wenn der Assistent für Kennwortänderungen automatisch ein systemgeneriertes Kennwort verwendet und die Benutzer keine eigenen Kennwörter erstellen können.

Standardeinstellung: Nicht aktiviert

Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden

Bei Aktivierung sendet das Single Sign-On Plug-in automatisch ein systemgeneriertes Kennwort und den Benutzern wird der Assistent für Kennwortänderungen nicht angezeigt. Der Benutzer sieht möglicherweise im Dialogfeld für die Kennwortänderung, dass die Felder eingegeben werden. Die Anwendung zeigt dann an, ob die Kennwortänderung erfolgreich war.

Standardeinstellung: Nicht aktiviert

Abläufe

Jul 22, 2016

Single Sign-On zeichnet vom Plug-in oder dem Benutzer generierte Ereignisse im Windows-Ereignisprotokoll der Anwendung auf dem Hostcomputer auf. Die Ereignisse werden dabei als Informationen, Warnung oder Fehler klassifiziert. Warnungen und Fehlerereignisse werden immer aufgezeichnet. Das Protokollieren von Informationsereignissen ist standardmäßig deaktiviert; Sie können die Protokollierung jedoch nach dem Erstellen der Benutzerkonfiguration in der Konsole aktivieren.

Single Sign-On protokolliert Ereignisse für Features, u. a. Hotdesktop, Smartcards, Lizenzierung und den Single Sign-On-Dienst. Im Ereignisprotokoll werden sicherheitsrelevante Ereignisse erfasst und verifiziert, die u. U. aufgrund gesetzlicher oder regulatorischer Auflagen aufgezeichnet und aufbewahrt werden müssen. Mit der Ereignisprotokollierung in Single Sign-On können Sie auch die IT-Sicherheit erhöhen.

Wenn Sie Single Sign-On in einer XenApp-Umgebung verwenden, enthält das Ereignisprotokoll sowohl Benutzer- als auch Sitzungsinformationen. Es werden sämtliche fehlgeschlagenen Anmeldeversuche erfasst.

Aktivieren der Protokollierung von Informationsereignissen

1. Navigieren Sie in der Konsole auf die Benutzerkonfiguration und klicken Sie im Menü Aktion auf Benutzerkonfiguration bearbeiten.
2. Wählen Sie im Eigenschaften-Dialogfeld der Benutzerkonfiguration Clientseitiges Verhalten.
3. Klicken Sie auf Single Sign-On Plug-in-Ereignisse mit der Windows-Ereignisprotokollierung protokollieren.

In der folgenden Tabelle finden Sie eine Übersicht über einige der Standardereignisse, die von Single Sign-On aufgezeichnet werden:

Standardereignistypen
Anmeldeversuch fehlgeschlagen (Plug-in-Software-Authentifizierung)
Wird aufgezeichnet, wenn ein Benutzer sich nicht erfolgreich an Single Sign-On authentifizieren kann. Fehler beim Öffnen des Speichers für Anmeldeinformationen.
Anmeldeversuch erfolgreich (Plug-in-Software-Authentifizierung)
Wird aufgezeichnet, wenn ein Benutzer sich erfolgreich authentifiziert und den zentralen Speicher öffnen kann.
Anmeldeversuch (Senden von Anmeldeinformationen)
Wird aufgezeichnet, wenn versucht wird, Anmeldeinformationen an eine externe Anwendung zu senden.
Vorgänge mit Anmeldeinformationen
Wird bei Vorgängen mit Kennwörtern, wie Kennwortänderung, Kennwortanzeige und Identitätsprüfung, aufgezeichnet.
Synchronisierung fehlgeschlagen (Kommunikation)
Wird aufgezeichnet, wenn das Synchronisieren mit dem zentralen Speicher aufgrund von Kommunikationsproblemen fehlschlägt.

Standardereignistypen
Synchronisierung fehlgeschlagen (Berechtigungen)
Wird aufgezeichnet, wenn das Synchronisieren mit dem zentralen Speicher aufgrund falscher Benutzeranmeldeinformationen fehlschlägt.
Fehler bei Smartcard-DataProtect-Verschlüsselung/-Entschlüsselung
Wird aufgezeichnet, wenn es beim Verschlüsseln oder Entschlüsseln von Smartcard-Daten zu einem allgemeinen Fehler kommt.
Fehler bei Smartcard-DataProtect-Verschlüsselung/-Entschlüsselung (Karte fehlt)
Wird aufgezeichnet, wenn die Smartcard nicht verfügbar ist.
Starten und Herunterfahren der Plug-in-Software
Wird aufgezeichnet, wenn die Smartcard nicht verfügbar ist.
Fehlende oder beschädigte DLL-Dateien
Wird aufgezeichnet, wenn eine DLL-Datei nicht korrekt geladen werden kann.

In der folgenden Tabelle finden Sie einige der Hotdesktop-Ereignisse, die von Single Sign-On aufgezeichnet werden.

Hotdesktop-Ereignistypen
Fehler bei der Anmeldung an der Hotdesktop-Sitzung
Wird aufgezeichnet, wenn es beim Sitzungsstart zu einem schwerwiegenden Fehler kommt.
Anmeldung an der Hotdesktop-Sitzung erfolgreich
Wird aufgezeichnet, wenn Hotdesktop nach erfolgreicher Benutzerauthentifizierung eine Sitzung startet.
Abmelden von Hotdesktop-Sitzung fehlgeschlagen
Wird nur aufgezeichnet, wenn es beim Beenden der Sitzung zu einem schwerwiegenden Fehler kommt.
Abmelden von Hotdesktop erfolgreich
Wird aufgezeichnet, wenn eine Sitzung infolge einer Benutzereingabe oder eines Sitzungstimeouts erfolgreich beendet wird.

Datei "Mfrmlist.ini"

Jul 22, 2016

Die Datei "Mfrmlist.ini" enthält eine Liste der Terminalemulatoren und Speicherorte der HLLAPI-DLL, die von der Single Sign-On Plug-in-Software überwacht werden. Die Datei ist im folgenden Verzeichnis gespeichert:

%ProgramFiles%\Citrix\MetaFrame Password Manager\Helper\MFEmu

Single Sign-On Plug-in sendet keine Anmeldeinformationen

Jul 22, 2016

Manchmal sendet das Single Sign-On-Plug-in nicht die Anmeldeinformationen eines Benutzers an eine konfigurierte Anwendung. Dieses Problem kann mehrere Ursachen haben, u. a.:

- Änderungen an der Webanwendung führten zu einer veralteten Anwendungsdefinition.
- Eine Einstellung, die versehentlich beim Erstellen der Anwendungsdefinition konfiguriert wurde.

Führen Sie zunächst die folgenden Schritte aus, um die Ursache für das fehlgeschlagene Senden der Anmeldeinformationen zu ermitteln:

- Suchen Sie nach potenziellen Konflikten in den Einstellungen.
- Prüfen Sie, ob das Plug-in so konfiguriert ist, dass Anwendungen erkannt werden.
- Vergleichen Sie die Definitionen des Plug-ins und in der Single Sign-On Console.
- Entfernen Sie nicht übereinstimmende Kriterien und Sendefelder, bis das Plug-in die Anmeldeinformationen sendet.

Wichtig: Single Sign-On enthält viele Einstellungen, die das Erstellen von Anwendungsdefinitionen, Kennwortrichtlinien, Benutzerkonfigurationen und Methoden zur Identitätsprüfung erleichtern. Es ist möglich, widersprüchliche Einstellungen festzulegen, die u. a. dazu führen können, dass Anmeldeinformationen nicht an eine Anwendung gesendet werden.
Wenn das Single Sign-On Plug-in auch nach dem Ausführen dieser Schritte die Anmeldeinformationen des Benutzers nicht sendet, probieren Sie die nachstehenden Methoden zur Problembehandlung bei Web- und Terminalemulatoranwendungen aus.

Webanwendungen

- Vergewissern Sie sich, dass die Einstellung "Strenge URL-Zuordnung" korrekt verwendet wird.
  1. Wählen Sie die relevante Webanwendung in der Single Sign-On-Komponente im Citrix AppCenter.
  2. Klicken Sie im Menü Aktion auf Anwendungsdefinition bearbeiten.
  3. Klicken Sie auf Anwendungsformulare, wählen Sie ein Anwendungsformular aus und klicken Sie auf Bearbeiten.
  4. Klicken Sie auf Formularidentität. Hier können Sie die strenge URL-Zuordnung sowie die Beachtung der Groß-und Kleinschreibung bei URLs aktivieren.
  5. Vergewissern Sie sich, dass die Seiten HTML-kompatible Feldtypen verwenden. Webanwendungsdefinitionen müssen HTML-kompatible Feldtypen enthalten. Nicht definierte oder benutzerdefinierte Feldtypen werden nicht erkannt.

- Wenn Sie InPrivate-Browsen in Internet Explorer 8 verwenden, stellen Sie sicher, dass Symbolleisten und Erweiterungen beim Starten des InPrivate-Browsens deaktivieren nicht aktiviert ist. Weitere Informationen über die Sicherheitsfeatures von Internet Explorer finden Sie auf der Microsoft Website.

Terminalemulatoranwendungen

Erstellen Sie Terminalemulator-Anwendungsdefinitionen mit dem Assistenten für Anwendungsdefinitionen und dem Assistenten für Formulardefinitionen. Wenn Sie einer Benutzerkonfiguration eine Anwendungsdefinition hinzufügen, stellen Sie sicher, dass die Unterstützung für Terminalemulatoren aktiviert ist.

- Vergewissern Sie sich, dass der Terminalemulator in der Datei Mfrmlist.ini konfiguriert ist.
  Der Prozess Ssomho.exe, der das Single Sign-On-Verhalten mit Terminalemulatoren steuert, erkennt nur Emulatoren, die in der Datei Mfrmlist.ini definiert sind. Wenn der Terminalemulator nicht in dieser Datei definiert ist, unternimmt der Prozess Ssomho.exe nicht den Versuch, mit dem Terminalemulator zu kommunizieren.

- Vergewissern Sie sich, dass ein Kurzname für die Sitzung festgelegt ist.
  Der Prozess Ssomho.exe verwendet diesen Kurznamen der Sitzung für die Kommunikation mit der HLLAPI-DLL. Ist kein Kurzname der Sitzung vorhanden, wird Ssomho.exe zwar geladen, die Bildschirmaktivität kann jedoch nicht überwacht werden. Konfigurieren Sie den Kurznamen der Sitzung auf dem Terminalemulator auf dem Clientgerät.

- Vergewissern Sie sich, dass der Prozess Ssomho.exe ausgeführt wird.
  Gehen Sie zur Überprüfung, ob Ssomho.exe ausgeführt wird, wie folgt vor:
  1. Öffnen Sie auf dem Computer mit der Single Sign-On Plug-in-Software den Task-Manager und klicken Sie auf die Registerkarte Prozesse.
  2. Klicken Sie auf die Überschrift Abbildname, um die Prozesse nach dem Namen anzuzeigen.
  3. Prüfen Sie, ob Ssomho.exe in der Liste aufgeführt ist.

  Wenn der Prozess Ssomho.exe nicht in der Liste aufgeführt ist, könnte es sein, dass der Prozess keine HLLAPI-DLLs gefunden hat oder dass er aufgrund von Problemen mit Terminalemulatoren von Drittanbietern beendet wurde.

  Hinweis: Auch wenn der Prozess Ssomho.exe in der Liste aufgeführt wird, ist es möglich, dass er nicht erfolgreich mit der HLLAPI.dll kommuniziert. Vergewissern Sie sich, dass der Kurzname für die Sitzung korrekt ist, bevor Sie nach anderen Gründen für das Problem suchen.
- Testen Sie jeden Terminalemulator einzeln.
  Wenn Sie mehrere unterstützte Emulatoren auf demselben System installiert haben, versucht Ssomho.exe, mit allen diesen Emulatoren zu kommunizieren. Es kann passieren, dass eine der HLLAPI-DLL-Implementierungen zur Instabilität von Ssomho.exe führt. Testen Sie daher jeden Terminalemulator einzeln, indem Sie die anderen Hostemulatoren entfernen oder die Einträge in der Datei Mfrmlist.ini auskommentieren und neu anordnen.

  Auf diese Weise können Sie gut überprüfen, ob der Prozess Ssomho.exe nicht versehentlich eine Verbindung mit einem anderen Emulator als dem herstellt, den Sie gerade auf Fehler untersuchen.

Unterstützen von Terminalemulatoren

Jul 22, 2016

Zum Aktivieren der HLLAPI-Unterstützung für alle Terminalemulatoren in Single Sign-On müssen Sie die Unterstützung für Terminalemulatoren in der Konsole aktivieren.

Wenn die Unterstützung für Terminalemulatoren aktiviert ist, startet SSOShell den Prozess Ssomho.exe. Dieser Prozess liest zuerst die in %ProgramFiles%\Citrix\MetaFrame Password Manager\Helper\MFEmu befindliche Datei Mfrmlist.ini, sucht dann nach allen konfigurierten Emulatoren und versucht anschließend, die in der Datei zugeordnete HLLAPI-kompatible DLL-Datei zu laden.

Die Datei Mfrmlist.ini kann zur Aufnahme zusätzlicher HLLAPI-kompatibler Emulatoren erweitert werden.

Der Prozess Ssomho.exe sucht in der Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE nach dem Speicherort der HLLAPI-kompatiblen DLL-Datei, sofern in der Datei Mfrmlist.ini nichts anderes festgelegt ist.

Einige Terminalemulatoren platzieren den Speicherort unter HKEY_CURRENT_USER. Bei diesen Emulatoren müssen Sie den Speicherort der DLL-Datei mit der expliziten Pfadeinstellung in der Datei Mfrmlist.ini manuell angeben.

Konfigurieren der Emulatorunterstützung

Die Konfiguration von Single Sign-On für das Arbeiten mit getesteten Emulatorprogrammen umfasst mehrere Schritte. Hierfür muss die Emulatorsoftware installiert, eine mit Single Sign-On zu verwendende Emulatorsitzung erstellt und Single Sign-On mit einer Terminalemulator-Anwendungsdefinition konfiguriert werden, die durch Textabgleich eine bestimmte Emulatorsitzung erkennt.

1. Installieren Sie die Terminalemulatorsoftware und starten Sie den Computer neu.
2. Starten Sie die Terminalemulatorsoftware und erstellen Sie eine neue Sitzung. Definieren Sie dabei die Anzeige und die Verbindung.
3. Legen Sie einen Kurznamen für die Sitzung fest.
4. Aktivieren Sie die HLLAPI-API-Unterstützung.
   Hinweis: Für jede einzelne Sitzung, die mit Single Sign-On verwendet wird, wird eine separate Terminalemulator-Anwendungsdefinition benötigt. Die Plug-in-Software erkennt Sitzungen, indem sie Text auf dem Bildschirm der Terminalemulatoranwendung Text in einer bestimmten, von der Anwendungsdefinition vorgegebenen Zeile und Spalte zuordnet. Single Sign-On sendet dann die in der vorgegebenen Zeile und Spalte der Anwendungsdefinition gefundenen Anmeldeinformationen. Deshalb benötigt jede einzelne Sitzung eine eigene Hostanwendungsdefinition.
5. Speichern und schließen Sie die Sitzung.
6. Beenden Sie den Terminalemulator.
7. Erstellen Sie eine Anwendungsdefinition für die Hostanwendung.
8. Öffnen Sie die Konsole und vergewissern Sie sich, dass die Unterstützung in den entsprechenden Benutzerkonfigurationen aktiviert ist.
9. Führen Sie den Emulator aus und öffnen Sie die Sitzung.
10. Starten oder aktualisieren Sie die Single Sign-On Plug-in-Software.

Die Plug-in-Software erkennt dann den Verbindungsbildschirm und zeigt ein Formular für die Anmeldeinformationen an, die eingegeben und gespeichert werden müssen.

Kein Starten der Single Sign-On Plug-in-Software

Jul 22, 2016

Die Single Sign-On Plug-in-Software sollte auf den Benutzergeräten, die nicht unter Windows Server 2008, Windows Server 2008 R2, Windows Vista oder Windows 7 ausgeführt werden, immer als letzte Software, die die GINA ändert, installiert werden. Wenn die Single Sign-On Plug-in-Software zwar installiert ist, jedoch nicht wie erwartet startet, liegt dies möglicherweise an einer unterbrochenen GINA-Kette. Zu einer solchen Unterbrechung kommt es, wenn Software installiert bzw. aktualisiert wird, nachdem die Single Sign-On Plug-in-Software die Windows-GINA-Kette ändert. Von Softwarepaketen, die die Smartcard-Authentifizierung unterstützen, Symantec und XenApp ist bekannt, dass sie die Windows-GINA-Kette ändern.

Wenn Single Sign-On bereits installiert ist und Sie Software installieren oder aktualisieren möchten, die die Windows-GINA-Kette ändert, sollten Sie die Single Sign-On Plug-in-Software zuerst deinstallieren. Nach der Deinstallation der Single Sign-On Plug-in-Software können Sie die neue Software installieren (oder aktualisieren); installieren Sie dann die Single Sign-On Plug-in-Software erneut. So stellen Sie sicher, dass die richtige DLL-Datei installiert und für die Verwendung mit Single Sign-On registriert ist.

Empfohlene Schritte zur Neuinstallation

1. Deinstallieren Sie sämtliche Software von Drittanbietern, die die GINA-Kette ändert.
2. Deinstallieren Sie die Plug-in-Software.
3. Installieren Sie die Drittanbietersoftware.
4. Installieren Sie die Plug-in-Software.

Wenn Sie vor kurzem Drittanbietersoftware aktualisiert oder installiert haben und davon ausgehen, dass diese Software die Windows-GINA-Kette geändert hat, überprüfen Sie den Windows-Registrierungseintrag und das Clientgerät, um festzustellen, ob die DLL-Dateien der GINA-Kette vorhanden sind und sich am korrekten Speicherort befinden. Wenn sich die Dateien nicht auf dem Computer befinden, deinstallieren Sie die Single Sign-On Plug-in-Software und installieren Sie die Software anschließend neu.

Wichtig: Beim Deinstallieren von Software, die die GINA-Kette unterbrochen haben könnte, ist es wichtig, die Software auf dem Benutzergerät in umgekehrter Reihenfolge zur Installation zu deinstallieren. Sonst kann es passieren, dass der Computer nicht mehr funktionsfähig ist. Bearbeiten Sie nicht die Registrierung.

Erstellen eines neuen Signaturzertifikats

Jul 22, 2016

Der Single Sign-On-Dienst generiert sowohl unmittelbar vor dem Ablauf des Signaturzertifikates als auch bei dessen Ablauf Ereignisprotokollwarnungen. Erstellen Sie ein neues Zertifikat, um die Ausgabe der Ereignisprotokollwarnungen zu beenden. Verwenden Sie zum Erstellen eines neuen Zertifikates CtxCreateSigningCert.exe. Signieren Sie mit dem Datensignierungstool, CtxSignData.exe, (mit den vom neuen Zertifikat bereitgestellten Schlüsseln) die Daten im zentralen Speicher.

Ein neues Signaturzertifikat muss nach der Erstkonfiguration des Single Sign-On-Dienstes nur erstellt werden, wenn eine der folgenden Bedingungen eintritt:

- Das Signaturzertifikat läuft demnächst ab oder ist bereits abgelaufen.
- Sie denken, dass die Sicherheit des Signaturzertifikates nicht mehr gegeben ist.

Zum Erstellen eines neuen Zertifikates müssen Sie CtxCreateSigningCert.exe ausführen. Diese Datei befindet sich im Ordner %ProgramFiles%\Citrix\MetaFrame Single Sign-On\Service. Geben Sie auf dem Computer mit dem Single Sign-On-Dienst an einer Eingabeaufforderung CtxCreateSigningCert.exeein.

Geben Sie den Namen der öffentlichen Schlüsseldatei, den Namen der privaten Schlüsseldatei und den Zeitraum (in Monaten) ein, der bis zum Ablauf des Signaturzertifikates vergeht. Damit ist das neue Zertifikat erstellt.

CtxCreateSigningCert	
Syntax:	CtxCreateSigningCert
Wobei Folgendes gilt:	= Dateiname des öffentlichen Zertifikats = Dateiname des privaten Zertifikats = Anzahl der Monate bis zum Ablauf des Zertifikates
Beispiel:	ctxcreatesigningcert "C:\PublicKeyCert.cert" "C:\PrivateKeyCert.cert" "12"

Signieren, Aufheben der Signatur, Neusignieren und Prüfen von Daten

Jul 22, 2016

Mit dem Datensignierungstool, CtxSignData.exe, können Sie Daten im zentralen Speicher signieren, die Signatur aufheben, Daten neu signieren und Daten prüfen. Es handelt sich dabei um ein Befehlszeilentool, das auf dem Installationsmedium im Ordner \Service zur Verfügung steht. CtxSignData.exe ist ferner unter %ProgramFiles%\Citrix\MetaFrame Password Manager\Service\SigningTool\CtxSignData.exe auf dem Server installiert, auf dem der Dienst ausgeführt wird.

Hinweis: Das Datensignierungstool wird mit dem Modul "Datenintegrität" des Single Sign-On-Dienstes installiert. Falls dieses Modul bei der Erstinstallation von Single Sign-On nicht installiert wurde, kann es zu einem späteren Zeitpunkt installiert werden.
Zum Starten des Datensignierungstools geben Sie auf dem Computer mit dem Single Sign-On-Dienst an einer Befehlszeile CtxSignData.exe mit den relevanten Befehlszeilenparameter (-s, -r, -u, -v) ein.

Signieren von Daten (-s)

Verwenden Sie den Befehlszeilenparameter zum Signieren von Daten (-s), um in Umgebungen mit unsignierten Daten die Datenintegrität zu aktivieren.

Hinweis: Wenn in Ihrer Single Sign-On-Umgebung die Datenintegrität nicht ausgeführt wird, und Sie später beschließen, die Datenintegrität zu implementieren, müssen Sie die Daten im vorhandenen zentralen Speicher mit dem Datensignierungstool signieren. Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Single Sign-On-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe oder Active Directory) angeben. Sämtliche Daten werden gelesen und mit dem neuen Zertifikat signiert.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -s lautet:

```
CtxSignData [-r Dienstpfad Zertifikatdatei Speicherort_zentraler_Speicher NTFS|AD]
```

Wobei Folgendes gilt:

-s	Signieren der Datendateien im zentralen Speicher
Dienstpfad	Der Pfad für den Single Sign-On-Dienst im URI-Format
Zertifikatdatei	Dateiname des Zertifikats, das zum Signieren und Neusignieren von Daten verwendet wird
Speicherort_zentraler_Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|AD	NTFS|AD = Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -s:

```
ctxsigndata -s "mpmserver.meineFirma.com/MPMService" "C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -s mpmserver.meineFirma.com/MPMService "C:\priv12mos.cert" DC1.meineFirma.com AD
```

Neusignieren von Daten (-r)

Verwenden Sie den Befehlszeilenparameter für das Neusignieren, wenn das vorhandene Signaturzertifikat demnächst abläuft, bereits abgelaufen ist oder seine Sicherheit nicht mehr gewährleistet ist. Sie müssen den neuen Namen der Signaturzertifikatdatei, den URI für den Single Sign-On-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe oder Active Directory)

angeben. Sämtliche Daten werden gelesen und geprüft und anschließend mit dem neuen Zertifikat signiert. Änderungen an den Einstellungen in der Konsole bzw. der Plug-in-Software sind nicht nötig, da für diese Komponenten die Datenintegrität bereits aktiviert ist.

Mit den folgenden Schritten signieren Sie unlesbare Daten neu:

1. Öffnen Sie die Single Sign-On-Komponente im Citrix AppCenter und navigieren Sie zur relevanten Benutzerkonfiguration.
2. Öffnen Sie die Benutzerkonfiguration, um sicherzustellen, dass die Daten aus dem zentralen Speicher lesbar sind.
3. Schließen Sie die Benutzerkonfiguration, um neue lesbare Daten im zentralen Speicher zu speichern.
4. Signieren Sie die Daten im zentralen Speicher mit dem Signierungstool (ctxsigndata) neu.

Hinweis: Falls die Daten aufgrund eines Sicherheitsbruchs zerstört wurden, führen Sie diese Schritte für alle Benutzerkonfigurationen aus, bevor Sie die Daten neu signieren, um nicht aus Versehen nicht gesicherte Daten zu signieren.
Die Syntax für den CtxSignData-Befehl mit dem Parameter -r lautet:

```
CtxSignData [-s Dienstpfad Zertifikatdatei Speicherort_zentraler_Speicher NTFS|AD]
```

Wobei Folgendes gilt:

-r	Neusignieren der Datendateien im zentralen Speicher (einschließlich -v)
Dienstpfad	Der Pfad für den Single Sign-On-Dienst im URI-Format
Zertifikatdatei	Dateiname des Zertifikates, das zum Signieren und Neusignieren von Daten verwendet wird
Speicherort_zentraler_Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|AD	NTFS|AD = Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -r:

```
ctxsigndata -r "mpmserver.meineFirma.com/MPMService" "C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -r "mpmserver.meineFirma.com/MPMService" "C:\priv3mos.cert" "DC1.meineFirma.com AD
```

Aufheben der Signatur von Daten (-u)

Verwenden Sie den Befehlszeilenparameter für das Aufheben der Signatur von Daten, wenn Sie die Datenintegrität deaktivieren. Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Single Sign-On-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe oder Active Directory) angeben. Sämtliche Daten werden ohne Prüfung gelesen und die Signaturen werden entfernt.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -u lautet:

```
CtxSignData [-u Speicherort_zentraler_Speicher NTFS|AD]
```

Wobei Folgendes gilt:

-u	Aufheben der Signatur aller Datendateien im zentralen Speicher
Speicherort_zentraler_Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|AD	NTFS|AD = Typ des zentralen Speichers für den Verzeichnisdienst, wobei:

	• NTFS = Microsoft NTFS-Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -u:

```
ctxsigndata -u "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -u DC1.meineFirma.com AD
```

Prüfen von Daten (-v)

Verwenden Sie den Befehlszeilenparameter für das Prüfen von Daten, um zu überprüfen, ob alle Daten im zentralen Speicher signiert und geprüft sind. Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Single Sign-On-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe oder Active Directory) angeben. Sämtliche Daten werden gelesen, geprüft und signiert.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -v lautet:

```
CtxSignData [-v Dienstpfad Speicherort_zentraler_Speicher NTFS|AD]
```

Wobei Folgendes gilt:

-v	Prüfen der Signaturen der Datendateien im zentralen Speicher
Dienstpfad	Der Pfad für den Single Sign-On-Dienst im URI-Format
Speicherort_zentraler_Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|AD	NTFS|AD = Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -v:

```
ctxsigndata -v "mpmserver.meineFirma.com/MPMService" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -v "mpmserver.meineFirma.com/MPMService" "https://mpmserver.meineFirma.com/MPMService" DC1.meineFirma.com AD
```

Anzeigen der Hilfe (-h)

Verwenden Sie den Befehlszeichenparameter -h, um die Hilfe für den CtxSignData-Befehl anzuzeigen.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -h lautet:

```
CtxSignData [-h]
```

Wobei Folgendes gilt:

-h	Anzeigen der Hilfe

Im Anschluss finden Sie ein Beispiel des CtxSignData-Befehls mit dem Parameter -h:

```
ctxsigndata -h
```

Aktivieren oder Deaktivieren des Dienstes "Datenintegrität" in der Single Sign-On Plug-in-Software

Jul 22, 2016

Sie können den folgenden Registrierungsschlüssel bearbeiten, um den Dienst "Datenintegrität" für die Single Sign-On Plug-in-Software zu aktivieren oder zu deaktivieren.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\PerformIntegrityCheck

Typ: DWORD

Werte:

0 = Prüfung der Datenintegrität deaktiviert

1 = Prüfung der Datenintegrität aktiviert

Verschieben von Daten in einen anderen zentralen Speicher

Jul 22, 2016

Es kann aus verschiedenen Gründen sinnvoll sein, Kennwortrichtlinien, Anwendungsvorlagen, Anwendungsdefinitionen, Sicherheitsfragen und andere Typen administrativer Daten in Single Sign-On zu migrieren.

- Der Benutzer verwendet eine neue Domäne.
- Ein neuer Server wird der Single Sign-On-Umgebung hinzugefügt
- Eine neue Domäne wird hinzugefügt, sodass Benutzer die Kontozuordnungsfunktion von Single Sign-On verwenden können.
- Die Benutzer verwenden die Kontozuordnung domänenübergreifend.
- Single Sign-On wird von einer Testumgebung in eine Produktionsumgebung verschoben.

Die Migration umfasst zwei Schritte, die mit der Single Sign-On-Komponente im Citrix AppCenter ausgeführt werden: Schritt 1. Exportieren der vorhandenen administrativen Daten. Schritt 2. Importieren der administrativen Daten in die neue Umgebung. Meistens müssen Sie auch die Benutzer auf den neuen zentralen Speicher umleiten.

In der folgenden Tabelle finden Sie die Daten, die mit dem Befehl "Exportieren" migriert bzw. nicht migriert werden können:

Migrierbar	**Nicht migrierbar**
Kennwortrichtlinien (außer für die Standard- und Domänenrichtlinie)	Benutzerkonfigurationen
Anwendungsvorlagen	People-Ordner
Anwendungsdefinitionen	Anwendungsgruppen
Für die fragenbasierte Authentifizierung verwendete Sicherheitsfragen und Sicherheitsfragengruppen	Benutzerinformationen für die Anmeldung
	Fragenkataloge
	Single Sign-On-Dienstdaten

Der Single Sign-On-Dienst kann nicht von einem zentralen Speicher auf einen anderen migriert werden. Wenn Sie einen Dienst verwenden, müssen Sie für eine erfolgreiche Migration den Single Sign-On-Dienst an einem neuen Speicherort installieren und der bestehende und der neue Dienst müssen vorübergehend nach der Migration verfügbar sein.

Achtung: Für eine erfolgreiche Migration sind weitere Schritte erforderlich, wenn die Dienstmodule "Konto-Self-Service" oder "Datenintegrität" installiert sind oder Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen in einer Benutzerkonfiguration aktiviert ist. Benutzerkonfigurationen werden nicht automatisch von einem zentralen Speicher auf einen anderen zentralen Speicher migriert. Sie müssen die Benutzerkonfigurationen stattdessen neu erstellen und die Benutzer auf den neuen zentralen Speicher umleiten. Wenn das Single Sign-On Plug-in die Daten mit Daten im ursprünglichen zentralen Speicher synchronisiert, wird erkannt, dass sich die Werte geändert haben; das Plug-in kopiert dann die Anmeldeinformationen zum neuen zentralen Speicher.

Migrieren von Daten auf einen neuen zentralen Speicher

Mit dem Assistenten für den Export administrativer Daten können Sie alle Anwendungsdefinitionen, Anwendungsvorlagen, Kennwortrichtlinien und Sicherheitsfragen und Sicherheitsfragengruppen im zentralen Speicher exportieren. Sie können ganze Typen von Daten entweder exportieren oder zurücklassen; der Assistent lässt nicht zu, dass Sie mit einem Untersatz der Daten arbeiten. Zum Beispiel müssen Sie entweder alle Kennwortrichtlinien exportieren oder sie im zentralen Speicher zurücklassen.

Im Gegensatz zu den anderen Typen der administrativen Daten können Sie mit dem Befehl zum Exportieren der Anwendungsdefinitionen entscheiden, welche Anwendungsdefinitionen exportiert werden.

Achtung: Für eine erfolgreiche Migration sind manuelle Schritte erforderlich, wenn die Dienstmodule "Konto-Self-Service" oder "Datenintegrität" installiert sind oder Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen in einer Benutzerkonfiguration aktiviert ist.

Exportieren administrativer Daten

1. Klicken Sie im Citrix AppCenter auf den Knoten "Single Sign-On", während Sie mit dem ursprünglichen zentralen Speicher verbunden sind, und klicken Sie dann im Menü Aktion auf Administrative Daten exportieren.
2. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen für den Assistenten für den Export administrativer Daten.

Importieren administrativer Daten

1. Installieren und starten Sie die Single Sign-On-Konsolenkomponente auf der neuen Maschine und schließen Sie Discovery konfigurieren und durchführen ab. Hinweis: Während Discovery konfigurieren und durchführen können Sie den zentralen Speicher angeben, mit dem Sie eine Verbindung herstellen möchten.
2. Klicken Sie im Citrix AppCenter auf den Knoten "Single Sign-On", während Sie mit dem neuen zentralen Speicher verbunden sind, und klicken Sie dann im Menü Aktion auf Administrative Daten importieren.

3. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen für den Assistenten für den Import administrativer Daten.
4. Erstellen Sie neue Benutzerkonfigurationen.
5. Wählen Sie im Citrix AppCenter, während Sie mit dem ursprünglichen zentralen Speicher verbunden sind, eine migrierte Benutzerkonfiguration aus, klicken Sie im Menü Aktion auf Benutzer umleiten und geben Sie den Speicherort des neuen zentralen Speichers an. Wiederholen Sie dies ggf.
6. Stellen Sie sicher, dass sich alle Benutzer mindestens einmal an Single Sign-On anmelden. Jetzt können Sie gefahrlos den ursprünglichen zentralen Speicher und Dienst herunterfahren.

Migrieren auf einen neuen zentralen Speicher bei Aktivierung von Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen

Wenn in Ihrem Unternehmen die Option Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen in Benutzerkonfigurationen aktiviert ist, müssen Sie die folgenden Schritte ausführen, um die administrativen Daten der Benutzer auf einen neuen zentralen Speicher zu migrieren. Sonst zwingen Sie die migrierten Benutzer bei jeder Anmeldung am Computer zur erneuten Registrierung entweder durch die fragenbasierte Authentifizierung oder die automatische Schlüsselwiederherstellung. Dies geschieht, da die administrativen Daten der Benutzer gelöscht werden, wenn sich die Benutzer vom Single Sign-On Plug-In abmelden oder es beenden.

1. Migrieren Sie die administrativen Daten auf einen neuen zentralen Speicher.
2. Erstellen Sie im Citrix AppCenter, während Sie mit dem neuen zentralen Speicher verbunden sind, neue Benutzerkonfigurationen. Aktivieren Sie nicht die Option Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen.
3. Wählen Sie im Citrix AppCenter, während Sie mit dem ursprünglichen zentralen Speicher verbunden sind, eine migrierte Benutzerkonfiguration aus, klicken Sie im Menü Aktion auf Benutzer umleiten und geben Sie den Speicherort des neuen zentralen Speichers an. Wiederholen Sie dies ggf.
4. Stellen Sie sicher, dass sich alle Benutzer mindestens einmal an Single Sign-On anmelden.
5. Erstellen und führen Sie ein Skript aus, um den Typ und den Speicherort des zentralen Speichers in der Registrierung der Benutzercomputer zu aktualisieren. In der folgenden Tabelle finden Sie die Registrierungseinstellungen für den Typ des zentralen Speichers.

Typen des zentralen Speichers	**Alte Einstellungen**	**Neue Einstellungen**
NTFS zu NTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =
NTFS zu Active Directory	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath
Active Directory zu NTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =

Achtung: Eine unsachgemäße Bearbeitung der Registrierung kann schwerwiegende Probleme verursachen und eine Neuinstallation des Betriebssystems erforderlich machen. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Die Verwendung des Registrierungs-Editors geschieht daher auf eigene Gefahr. Sichern Sie die Registrierung auf jeden Fall vor dem Bearbeiten ab.

6. Wählen Sie im Citrix AppCenter, während Sie mit dem neuen zentralen Speicher verbunden sind, die neuen Benutzerkonfigurationen aus und aktivieren Sie Datenordner und Registrierungsschlüssel des Benutzers beim Beenden von Single Sign-On Plug-In löschen. Jetzt können Sie gefahrlos den ursprünglichen zentralen Speicher und Dienst herunterfahren.

Exportieren von Anwendungsdefinitionen

Sie können eine Anwendungsdefinition oder mehrere in eine XML-Datei exportieren.

Exportieren einer Anwendungsdefinition

1. Erweitern Sie im Citrix AppCenter, während Sie mit dem ursprünglichen zentralen Speicher verbunden sind, den Konten "Single Sign-On" und erweitern Sie dann Anwendungsdefinitionen.
2. Wählen Sie die Anwendungsdefinition, die Sie exportieren möchten, und klicken Sie im Menü Aktion auf Anwendungsdefinition exportieren.
3. Speichern Sie die Anwendungsdefinition im Dialogfeld Anwendungsdefinition exportieren an dem Speicherort, auf den Sie von der Konsole auf dem neuen Computer zugreifen können.

Exportieren von mehreren Anwendungsdefinitionen

1. Erweitern Sie im Citrix AppCenter, während Sie mit dem ursprünglichen zentralen Speicher verbunden sind, den Konten "Single Sign-On" und erweitern Sie dann Anwendungsdefinitionen.
2. Klicken Sie auf dem Menü Aktion auf Anwendungsdefinitionen exportieren.
3. Folgen Sie den auf dem Bildschirm angezeigten Anweisungen des Assistenten für das Exportieren von Anwendungsdefinitionen.

Absichern des Dienstes

Stellen Sie beim Absichern wichtiger Dateien sicher, dass Backupmaßnahmen im Unternehmen auch regelmäßig Sicherungskopien des zentralen Speichers mit dem Inhalt, den Zertifikaten und den persönlichen und privaten Schlüsseln angefertigt werden.

Wichtig: Wenn Sie als zentralen Speicher eine NTFS-Netzwerkfreigabe verwenden, müssen Sie die Berechtigungen für diese Dateien in Windows ändern, sodass das Backupprogramm darauf zugreifen kann.

1. Notieren Sie sich die Einstellungen, die Sie vornehmen, wenn Sie das Dienstkonfigurationstool zum Einrichten des Dienstes ausführen.
2. Exportieren Sie den Dienst unter Verwendung von CtxMoveServiceData.exe auf eine sichere Dateifreigabe bzw. ein sicheres Speichermedium:
   1. Öffnen Sie eine Eingabeaufforderung und gehen Sie zu %ProgramFiles%\Citrix\Metaframe Password Manager\Service\Tools.
   2. Geben SieCtxMoveServiceData.exe –export \\server\share\backupfileein.
      Hinweis: Verwenden Sie bei der Pfadangabe keine Umgebungsvariablen.
   3. Geben Sie ein beliebiges Kennwort ein, wenn Sie dazu aufgefordert werden. Notieren Sie sich das Kennwort.
      Wichtig: Die Dienstdaten, die Sie in der Sicherungskopie speichern, werden mit diesem Kennwort verschlüsselt. Bewahren Sie das Kennwort an einem sicheren Ort auf.
   4. Geben Sie das Kennwort erneut ein, wenn Sie dazu aufgefordert werden.
   5. Überprüfen Sie, ob die Sicherungskopie erstellt wurde.

Wiederherstellen des Diensts

1. Installieren Sie den Dienst von den Installationsmedien.
2. Konfigurieren Sie den Dienst mit den richtigen Einstellungen. Nutzen Sie dafür die Notizen, die Sie sich vor der Sicherung gemacht haben.
   Hinweis: Wenn Sie die Datenintegrität implementiert haben, müssen Sie den Serverstandort für die Datenintegrität korrekt konfigurieren, d. h. Sie müssen angeben, ob sich der Serverstandort für die Datenintegrität geändert hat oder gleich geblieben ist.
3. Schließen Sie die Konfiguration ab und starten Sie den Dienst neu. Falls erwünscht, kann der Dienst sofort nach dem Starten wieder beendet werden.
4. Importieren Sie den Dienst unter Verwendung von CtxMoveServiceData.exe von einer sicheren Dateifreigabe bzw. einem sicheren Speichermedium:
   1. Öffnen Sie eine Eingabeaufforderung und gehen Sie zu %ProgramFiles%\Citrix\Metaframe Password Manager\Service\Tools.
   2. Geben SieCtxMoveServiceData.exe –import <\\server\share\backupfile>ein.
   3. Wenn Sie dazu aufgefordert werden, geben Sie das korrekte Kennwort ein.
   4. Wenn Sie gefragt werden, ob Sie AKR.DAT überschreiben möchten, klicken Sie auf Ja.
5. Starten Sie den Dienst. Der Dienst kann nun verwendet werden.

Entfernen gelöschter Objekte im zentralen Speicher

Mit dem Tool CtxFileSyncClean löschen Sie verwaiste Konfigurationsdaten aus dem zentralen Speicher auf einer NTFS-Freigabe. Diese Dateien verwaisten, als die Objekte, auf die sie verwiesen, gelöscht wurden. Das Tool CtxFileSyncClean löscht keine Benutzerdatendateien, selbst wenn der Benutzer gelöscht wurde. Führen Sie die Datei CtxFileSyncClean.exe vom Verzeichnis \Tools auf dem Installationsmedium aus.

Erweiterungen von Anwendungsdefinitionen

Jul 22, 2016

Single Sign-On-Administratoren können im Allgemeinen Anwendungsdefinitionen mit der Single Sign-On-Komponente im Citrix AppCenter und dem Anwendungsdefinitionstool erstellen. Für einige Anwendungen müssen jedoch besondere Anforderungen berücksichtigt werden, für die ein externer Prozess ermitteln muss, ob eine Anwendung gestartet wurde oder Anmeldeinformationen des Benutzers mit dem Single Sign-On Plug-in gesendet wurden.

Implementierer von Drittanbietern, die für diese Anwendungen entsprechende externe Prozesse erstellen, können dabei mit den Erweiterungen von Anwendungsdefinitionen in der Single Sign-On-Komponente im Citrix AppCenter und dem Anwendungsdefinitionstool festlegen, wann und wie diese Prozesse initiiert werden.

Verwenden der Single Sign-On Plug-in-Software

Es gibt zwei verschiedene Typen der Erweiterungen von Anwendungsdefinitionen:

- Identifizierungserweiterungen
  Verwenden von externen Prozessen zum Prüfen, ob es sich bei der Zielanwendung um ein Formular handelt, für das Aktionen zum Verwalten von Anmeldeinformationen von Benutzern erforderlich sind. Diese externen Prozesse können statt oder zusammen mit anderen Fenstererkennungsalgorithmen verwendet werden, die in der Formulardefinition festgelegt sind.

- Aktionserweiterungen
  Verwenden von externen Prozessen zum Ausführen der erforderlichen Aktionen zum Verwalten von Anmeldeinformationen des Benutzers. Diese externen Prozesse können statt oder zusammen mit anderen Fensteraktionsalgorithmen verwendet werden, die in der Formulardefinition festgelegt sind.

Eine Formulardefinition kann so konfiguriert werden, dass Erweiterungen von Anwendungsdefinitionen verwendet werden, um jeweils einen oder beide Vorgänge damit durchzuführen.

Identifizierungserweiterungen

Das Single Sign-On Plug-in ermittelt mit Listenerhooks Ereignisse auf dem Desktop, z. B. Anwendungsinstanziierung, Laden von URLs, Hinweise zur Vollständigkeit von Dokumenten bei HTML-Seiten und andere ähnliche Ereignisse.

Wenn diese Ereignisse auftreten, prüft das Plug-in, ob für die Zielanwendung eine Aktion zum Verwalten von Anmeldeinformationen des Benutzers (z. B. Ignorieren, Anmelden, Kennwort ändern usw.) erforderlich ist. Dafür werden die Merkmale einer Anwendung mit den definierten Merkmalen verglichen, die ein Formular eindeutig identifizieren. Dazu gehören (als Mindestangaben) der Windows-Titel und der Name der ausführbaren Datei sowie bei Bedarf andere erweiterte Zuordnungsmerkmale, z. B. das Verwenden eines externen Prozesses zur Formularidentifizierung (Identifizierungserweiterung).

Bei einer erforderlichen externen Identifizierung werden der oder die zugehörigen Prozesse in der Formulardefinition angegeben. Die Formulardefinition enthält Angaben zur Identifizierungserweiterung und zu allen zugehörigen Parametern. Diese beziehen sich direkt auf eine Einstellung in der Registrierung.

Nach dem Verarbeiten der Mindest- und der erweiterten Zuordnungsalgorithmen durch das Plug-in werden Identifizierungserweiterungen geprüft, die einen externen Prozess erfordern.

Wenn mehrere Identifizierungserweiterungen für das Prüfen eines Formulars definiert sind, werden die Erweiterungen in der

Reihenfolge ausgeführt, in der sie auf der Seite der Identifizierungserweiterungen angezeigt sind (von oben nach unten).

Für jede Identifizierungserweiterung bleibt das Plug-in die festgelegte Zeitdauer inaktiv (definiert in der Registrierungseinstellung), um auf das Beenden des externen Prozesses zu warten und im Anschluss den Prozessbeendigungscode zu analysieren.

Wenn die Prozesse für Mindestzuordnung, erweiterte Zuordnung und externe Zuordnung mit einem Rückgabecode von null abgeschlossen werden, wird die Zielanwendung als Übereinstimmung angesehen. Wenn ein Zuordnungsprozess mit einem anderen Wert beendet wird, wird der Auswertungsprozess beendet, und die Anwendung wird nicht als Übereinstimmung angesehen.

Bei einem negativen Rückgabewert wird in der Windows-Ereignisanzeige ein Fehler protokolliert. Positive Werte werden in eine Protokolldatei geschrieben (falls aktiviert).

Die folgende Aktion zum Verwalten von Anmeldeinformationen des Benutzers kann über eine beliebige Kombination von standardmäßigen Windows-Formularaktionen, Aktionsfolgen oder Aktionserweiterungen durchgeführt werden.

Definieren einer Identifizierungserweiterung

Sie konfigurieren Identifizierungserweiterungen im Assistenten für Formulardefinitionen beim Erstellen der Anwendungsdefinition.

1. Erweitern Sie im AppCenter den Knoten Single Sign-On, wählen Sie Anwendungsdefinitionen und klicken Sie im Menü Aktion auf Anwendungsdefinition erstellen.
2. Navigieren Sie im Assistenten für Anwendungsdefinitionen auf die Seite Formulare verwalten und klicken Sie auf Formular hinzufügen, um den Assistenten für Formulardefinitionen zu starten.
3. Erstellen Sie die Definition, bis die Seite Formular identifizieren angezeigt wird.
4. Klicken Sie auf der Seite Formular identifizieren auf Erweiterte Zuordnung. Ein Dialogfeld wird angezeigt.
5. Klicken Sie im Dialogfeld Erweiterte Zuordnung auf Identifizierungserweiterungen.
6. Klicken Sie auf der Seite Identifizierungserweiterungen auf Hinzufügen, um das Dialogfeld Identifizierungserweiterung hinzufügen zu öffnen. Im Dialogfeld Identifizierungserweiterungen hinzufügen definieren Sie Folgendes:

Erweiterungs-ID	Die Erweiterungs-ID kennzeichnet den ExtensionName nach dem in den Registrierungseinstellungen gesucht wird.
Beschreibung	Eine benutzerdefinierte Beschreibung der zu definierenden Identifizierungserweiterung.
Parameter	Ein beliebiges Name/Wert-Paar (Parametername/Parameterwert), mit dem vom Implementierer definierte Parameter an den externen Prozess gesendet werden, der von dieser Erweiterung gestartet wird.

Der ExtensionName gibt den Namen eines Registrierungsschlüssels an. Der Schlüsselname und die ihm zugeordneten Schlüsselwerte definieren die ausführbare Datei für den externen Identifizierungsprozess und die zugehörigen Verwendungsmerkmale. Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Wobei der Wert für ExtensionName mit der Erweiterungs-ID im Dialogfeld Identifizierungserweiterungen hinzufügen angegeben wird.

Auf 64-Bit-Plattformen befinden sich der Name des Registrierungsschlüssels und die zugeordneten Schlüssel unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Taste	Geben Sie	Wert
Geben Sie	REG_SZ	Muss EXECUTABLE sein.
Timeout	REG_DWORD	0, um ohne Timeout auf das Beenden der Anwendung zu warten. Jeder andere Wert gibt die Wartezeit in Millisekunden an.
TerminateProcess	BOOL implementiert als REG_DWORD	(optional) Prozess bei Timeout beenden. TRUE: (Standard) Prozess beenden. FALSE: (0) Prozess nicht beenden.
Ausführbare Datei	REG_EXPAND_SZ	Der ausführbare Prozess und der vollqualifizierte Pfad.
Argumente	REG_SZ	Parameter für die ausführbare Datei.

Der Wert für Executable gibt den vollständigen Pfad zur ausführbaren Datei an. Umgebungsvariablen sind zulässig. Wenn die Erweiterung als Skript implementiert wird, muss ein Skriptinterpreter für Executable und der Skriptname als Teil von Arguments verwendet werden. Externe Prozesse können mit Editoren/Sprachen oder IDEs Ihrer Wahl entwickelt werden.

Der Wert für "Arguments" unterstützt Parameter, die von der Plug-In-Software durch Echtzeitparameter oder durch die Parametername/Wert-Paare, die im Dialogfeld Identifizierungserweiterungen hinzufügen festgelegt wurden, ersetzt werden können. Jeder zu ersetzende Parameter benötigt als Trennzeichen ein $ (Dollarzeichen) als Präfix und Suffix. Beispielsweise die folgenden Befehlszeilenargumente:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

Diese Befehlszeilenargumente werden von der ausführbaren Datei folgendermaßen interpretiert:

```
/h 1275366 /s "Houston, TX" /t 43
```

Der der Anwendung zugeordnete Handle von Microsoft Windows ist ein unterstützter interner Parameter, der als $_HANDLE$ definiert ist.

Alle internen Parameter verwenden $_ als Präfix, um Benennungskonflikte zu vermeiden. Implementiererparameter dürfen keine Unterstreichungszeichen in Schlüsselnamen haben.

Die Ersetzungspriorität ist festgelegt, damit die Parameterwerte nach dem Schreiben erhalten bleiben. Die Priorität ist definiert als interne Parameter (z. B. $_HANDLE$), gefolgt von Implementiererparametern, gefolgt von Umgebungsvariablen.

Für alle Implementiererparameter können Groß- und Kleinbuchstaben und Ziffern in Schlüsselnamen verwendet werden. Bei den Schlüsselnamen braucht nicht auf die Groß- bzw. Kleinschreibung geachtet zu werden.

Wenn durch die ausführbare Datei der Erweiterungsidentifizierung festgelegt ist, dass Parameter in einer bestimmten Reihenfolge aufgerufen werden müssen, muss Argument die erforderliche Reihenfolge unterstützen. Die Parameternamen/Wert-Paare im Dialogfeld Identifizierungserweiterungen hinzufügen können in einer beliebigen Reihenfolge definiert sein.

Aktionserweiterungen

Aktionserweiterungen verwalten Aktionen zur Verwaltung von Anmeldeinformationen des Benutzers mit einem externen Prozess. Mit dem Erweiterungsdefinitionsprozess können Anmeldeinformationen des Benutzers an die externe Anwendung übertragen werden.

Nachdem ein Formular zum Verwalten von Anmeldeinformationen des Benutzers erfolgreich identifiziert wurde (siehe *— Identifizierungserweiterungen*), kann die folgende Aktion zum Verwalten von Anmeldeinformationen des Benutzers über eine beliebige Kombination von standardmäßigen Windows-Formularaktionen, Aktionsfolgen oder Aktionserweiterungen durchgeführt werden.

Das Single Sign-On Plug-In unterstützt dieselben Features wie unter *— Identifizierungserweiterungen* beschrieben.

Das Plug-In führt den externen Prozess aus und bleibt dann für den festgelegten Zeitraum inaktiv (wenn für WaitForCompletion der Wert TRUE festgelegt ist), um auf das Ende des externen Prozesses zu warten und im Anschluss den Prozessbeendigungscode zu analysieren. Wenn der Prozess mit einem Rückgabewert von null beendet wird, wurde die Erweiterung erfolgreich ausgeführt. Ein Rückgabewert ungleich null verweist auf einen Fehler.

Bei einem negativen Wert wird der Fehler in der Windows-Ereignisanzeige protokolliert. Positive Werte werden in eine Protokolldatei geschrieben (falls aktiviert) (weitere Informationen finden Sie unter *— Aktivieren der Protokollierung*).

Definieren einer Aktionserweiterung

Sie konfigurieren Aktionserweiterungen im Assistenten für Formulardefinitionen beim Erstellen der Anwendungsdefinition.

1. Erweitern Sie im Citrix AppCenter den Knoten Single Sign-On, wählen Sie Anwendungsdefinitionen und klicken Sie im Menü Aktion auf Anwendungsdefinition erstellen.
2. Navigieren Sie im Assistenten für Anwendungsdefinitionen auf die Seite Formulare verwalten und klicken Sie auf Formular hinzufügen, um den Assistenten für Formulardefinitionen zu starten.
3. Erstellen Sie die Definition, bis die Seite Formular identifizieren angezeigt wird.
4. Klicken Sie auf der Seite Formularaktionen definieren auf Aktionseditor.
5. Wählen Sie im Dialogfeld Aktionseditor die Option Aktionserweiterung starten. Der Bereich Aktionen konfigurieren wird angezeigt. In diesem Bereich können Sie Aktionsfolgeeinträge für Aktionserweiterung starten anzeigen, bearbeiten oder hinzufügen.
6. Geben Sie die folgenden Informationen ein und klicken Sie auf Einfügen, um einer Aktionsfolge eine Aktionserweiterung hinzuzufügen:

ID	Die ID kennzeichnet den ExtensionName, nach dem in den Registrierungseinstellungen gesucht wird.
Beschreibung	Eine benutzerdefinierte Beschreibung der zu definierenden Aktionserweiterung.

Parameter	Ein beliebiges Name/Wert-Paar (Parametername/Parameterwert), mit dem vom Implementierer definierte Parameter an den externen Prozess gesendet werden, der von dieser Erweiterung gestartet wird.

Wie bei den Identifizierungserweiterungen kennzeichnet ExtensionName den Namen eines Registrierungsschlüssels. Der Schlüsselname und die ihm zugeordneten Schlüsselwerte definieren die ausführbare Datei für den externen Identifizierungsprozess und die zugehörigen Verwendungsmerkmale. Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Wobei der Wert für ExtensionName mit dem ID-Wert im Bereich Aktionskonfiguration angegeben wird.

Auf 64-Bit-Plattformen befinden sich der Name des Registrierungsschlüssels und die zugeordneten Schlüssel unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Taste	**Geben Sie**	**Wert**
Geben Sie	REG_SZ	Muss EXECUTABLE sein.
Timeout	REG_DWORD	0, um ohne Timeout auf das Beenden der Anwendung zu warten. Jeder andere Wert gibt die Wartezeit in Millisekunden an.
TerminateProcess	BOOL implementiert als REG_DWORD	(optional) Prozess bei Timeout beenden. TRUE: (Standard) Prozess beenden. FALSE: (0) Prozess nicht beenden.
WaitForCompletion	BOOL implementiert als REG_DWORD	(optional) Plug-in wartet auf Beenden des Prozesses. TRUE: (Standard) Warten. FALSE: (0) Nicht warten.
Ausführbare Datei	REG_EXPAND_SZ	Der ausführbare Prozess und der vollqualifizierte Pfad.
Argumente	REG_SZ	Parameter für die ausführbare Datei.

Für den Wert Executable gelten dieselben Konventionen wie für die Identifizierungserweiterungen.

Der Wert für "Arguments" unterstützt Parameter, die vom Plug-in durch Echtzeitparameter oder durch die Parametername/Wert-Paare ersetzt werden können, die in der Ansicht Identifizierungserweiterung starten im Aktionseditor festgelegt wurden. Jeder zu ersetzende Parameter benötigt als Trennzeichen ein $ (Dollarzeichen) als Präfix

und Suffix. Beispielsweise die folgenden Befehlszeilenargumente:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

Diese Befehlszeilenargumente werden von der ausführbaren Datei folgendermaßen interpretiert:

```
/h 1275366 /s "Houston, TX" /t 43
```

Der der Anwendung zugeordnete Handle von Microsoft Windows ist ein unterstützter interner Parameter, der als $_HANDLE$ definiert ist.

Alle internen Parameter verwenden $_ als Präfix, um Benennungskonflikte zu vermeiden. Implementiererparameter dürfen keine Unterstreichungszeichen in Schlüsselnamen haben.

Zusätzlich zum Windows-Handle werden die folgenden internen Parameter zum Verwalten von Anmeldeinformationen unterstützt:

- Benutzername: $_USERNAME$
- Kennwort: $_PASSWORD$
- Benutzerdefiniert 1: $_CUSTOM1$
- Benutzerdefiniert 2: $_CUSTOM2$
- Altes Kennwort: $_OLDPASSWORD$

Die Ersetzungspriorität ist festgelegt, damit die Parameterwerte nach dem Schreiben erhalten bleiben. Die Priorität ist definiert als interne Parameter, gefolgt von Implementiererparametern, gefolgt von Umgebungsvariablen.

Für alle Implementiererparameter können Groß- und Kleinbuchstaben und Ziffern in Schlüsselnamen verwendet werden. Bei den Schlüsselnamen braucht nicht auf die Groß- bzw. Kleinschreibung geachtet zu werden.

Wenn durch die ausführbare Datei der Erweiterungsidentifizierung festgelegt ist, dass Parameter in einer bestimmten Reihenfolge aufgerufen werden müssen, muss Argument die erforderliche Reihenfolge unterstützen. Die Parameternamen/Wert-Paare auf der Seite Aktionskonfiguration können in beliebiger Reihenfolge definiert sein.

Anforderungen an Implementierer

Die externen Prozesse, die für die Aktionen zur erweiterten Zuordnung oder zum Verwalten von Anmeldeinformationen verwendet werden, sind als beliebige Prozesse bzw. Anwendungen definiert, die über eine Befehlszeilenschnittstelle initiiert werden können. Alle erforderlichen oder optionalen Argumente für die Identifizierungserweiterungen oder Aktionserweiterungen müssen auch mit einer Befehlszeilenschnittstelle angegeben werden können.

Für Aktionserweiterungen müssen die Implementierer dieselben Features wie in der oben beschriebenen Windows-Erkennungsimplementierung unterstützen. Benutzername, Kennwort, Benutzerdefiniert 1, Benutzerdefiniert 2 und Altes Kennwort können an die ausführbare Datei übergeben werden.

Bei Identifizierungserweiterungen und Aktionserweiterungen ist der Implementierer für Folgendes verantwortlich:

- Bereitstellen aller ausführbaren Dateien, Supportmodule und Dateien zur Unterstützung der Erweiterung im Single Sign-On Plug-in
- Verwalten aller bereitgestellten Module
- Hinzufügen aller festgelegten Registrierungseinträge auf dem Computer mit dem Plug-in
- Sicherstellen der Eindeutigkeit von Erweiterungsnamen in ihren Domänen

Das empfohlene Benennungsschema für Erweiterungen ist ein umgekehrtes Domänenbenennungsschema (z. B. com.citrix.cpm.ext4).

Aktivieren der Protokollierung

Sie müssen die Registrierung ändern, um das Debugtracing für das Single Sign-On Plug-in zu aktivieren.

Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Log]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Taste	Eingabe	Wert
Aktiviert	REG_DWORD	Der Standardwert ist 0. 0: deaktiviert 1: aktiviert
Filter	REG_DWORD	Bitmaske, die festlegt, welche Protokolleinträge erstellt werden. 0x00000001: Windows-Anwendungsflag zum Protokollieren von Identifizierungserweiterungsfehlern. 0x00000004: Windows-Kennworteintrag zum Protokollieren von Aktionserweiterungsfehlern.
MaxSizeInBytes	REG_DWORD	Maximale Größe der Protokolldatei in Bytes. Der theoretische Höchstwert kann 4 GB (2^32) sein. Standardwert: 819200

Die Protokolldateidaten werden in einer Datei "sso_" im folgendem Verzeichnis gespeichert:

%LocalAppData%\Citrix\MetaFrame Password Manager

Virtuelle Tastencodes für Windows-, Web- und terminalemulator-basierte Anwendungen

Jul 22, 2016

Single Sign-On unterstützt virtuelle Tastencodes für Windows-, Web- und terminalemulatorbasierte Anwendungen. Mit diesen Codes werden bestimmte Tastatureingaben an Felder in Anmelde- oder Kennwortänderungsformularen gesendet.

Codes für VTabKeyN (Windows und Web)

Erstellen Sie mit den folgenden Kennungen eine Tastencodefolge für Windows- und webbasierte Anwendungen.

Code	Beschreibung
'DELAY=N'	N ist die Anzahl der Millisekunden für die Verzögerung.
'VKEY=N'	N ist der virtuelle Tastencode, der gesendet wird.

Beispiel: Senden von Tabulatortaste, Ende-Taste, Leertaste, einer Verzögerung von 1,5 Sekunden, Benutzername für Anmeldung, Leertaste, Benutzername/ID, Pos1, Verzögerung von 0,35 Sekunden, Tabulatortaste und Kennwort:

VTabKey1= 'VKEY=9"VKEY=35' 'DELAY=1500 'Logon username'VKEY=32' VTabKey2='VKEY=36"DELAY=350"VKEY=9'

Codes für VirtualKeyCode und VKEY (Windows und Web)

Taste	Code	Taste	Code	Taste	Code	Taste	Code
Pause	3	5	53	V	86	F5	116
Rücktaste	8	6	54	W	87	F6	117
Registerkarte	9	7	55	X	88	F7	118
Entf	12	8	56	J	89	F8	119
Eingabe	13	9	57	Z	90	F9	120
Umschalt	16	A	65	Links (Fenster)	91	F10	121
Strg	17	B	66	Rechts (Fenster)	92	F11	122
Alt	18	C	67	Num 0	96	F12	123
Feststelltaste	20	D	68	Num 1	97	F13	124
Esc	27	E	69	Num 2	98	F14	125
Leertaste	32	F	70	Num 3	99	F15	126
Bild-Auf	33	G	71	Num 4	100	F16	127

Taste	Code	Taste	Code	Taste	Code	Taste	Code
Bild-Ab	34	H	72	Num 5	101	F17	128
Ende	35	I	73	Num 6	102	F18	129
Pos1	36	J	74	Num 7	103	F19	130
Links	37	K	75	Num 8	104	F20	131
Auf	38	L	76	Num 9	105	F21	132
Recht	39	M	77	Sternchen (*)	106	F22	133
Nach unten	40	N	78	Plus (+)	107	F23	134
Druck	44	O	79	Minus (-)	109	F24	135
Help	47	Z	80	Punkt (.)	110	Num	144
0	48	Q	81	Strich (/)	111	Rollen	145
1	49	R	82	F1	112	Linke Umschalttaste	160
2	50	S	83	F2	113	Rechte Umschalttaste	161
3	51	T	84	F3	114	Linke Strg-Taste	162
4	52	U	85	F4	115	Rechte Strg-Taste	163

Virtuelle Tastencodes für HLLAPI-kompatible Terminalemulatoren

Zeichen/Befehl	Code	Zeichen/Befehl	Code	Zeichen/Befehl	Code
Alt Cursor	@$	Lokaler Druck	@P	PF12/F12	@c
Rücktaste	@<	Reset	@R	PF13/F13	@d
@	@@	Umschalt	@S	PF14/F14	@e
Alt	@A	Dup	@S@x	PF15/F15	@f
Feld -	@A@-	Feldmarkierung	@S@y	PF16/F16	@g
Feld +	@A@+	Tabulatortaste (rechte Tabulaturtaste)	@T	PF17/F17	@h
Feld beenden	@A@E	Cursor auf	@U	PF18/F18	@i
Alt Cursor	@$	Cursor ab	@V	PF19F19	@j
Eingabe entfernen	@A@F	Cursor links	@L	PF20/F20	@k

Zeichen/Befehl	Code	Zeichen/Befehl	Code	Zeichen/Befehl	Code
Systemabfrage	@A@H	Cursor rechts	@2	PF21/F21	@L
Einfügen umschalten	@A@I	Bild-Auf	@U	PF22/F22	@m
Cursorauswahl	@A@J	Bild-Ab	@V	PF23/F23	@n
Achtung	@A@Q	Ende	@q	PF24/F24	@o
Druck	@A@T	Pos1	@0	PA1	@x
Hexadezimal	@A@X	PF1/F1	@1	PA2	@y
Befehl/Funktionstaste	@A@Y	PF2/F2	@2	PA3	@z
Druck (PC)	@A@t	PF3/F3	@3	PA4	@+
Rücktaste/Linke Tabulatortaste	@B	PF4/F4	@4	PA5	@%
Entf	@C	PF5/F5	@5	PA6	@&
Löschen	@D	PF6/F6	@6	PA7	@’
Eingabe	@E	PF7/F7	@7	PA8	@(
EOF löschen	@F	PF8/F8	@8	PA9	@)
Help	@H	PF9/F9	@9	PA10	@*
Einfügen	@I	PF10/F10	@a		
Neue Zeile	@N	PF11/F11	@b		

Single Sign-On Provisioning Software Development Kit (SDK)

Jul 22, 2016

Mit dem Single Sign-On Provisioning Software Development Kit (SDK) können Sie die sekundären Anmeldeinformationen der Benutzer verwalten. Sekundäre Anmeldeinformationen sind anwendungsspezifische Anmeldeinformationen, die Single Sign-On für den Benutzer nach der primären Domänenauthentifizierung sendet.

Mit dem Provisioning der Anmeldeinformationen können Sie viele Aufgaben automatisieren, die bei der Verwaltung der Anmeldeinformationen der Benutzer anfallen. Mit dem Provisioning der Anmeldeinformationen können Sie bei der Bereitstellung einer neuen Single Sign-On-Installation, beim Hinzufügen von neuen Benutzern oder neuen Anwendungen und dem Löschen von überflüssigen Informationen diese Aufgaben schnell abwickeln.

In dieser Onlinehilfe, die nur in Englisch verfügbar ist, wird das Design der Single Sign-On-Funktion "Provisioning der Anmeldeinformationen" skizziert; außerdem finden einen Überblick der API-Funktionen, mit denen Sie Aktionen in der Provisioning-XML-Datei definieren können.

Das Provisioningmodul

Das Provisioningmodul ist Teil des Single Sign-On-Dienstes und ist ein Standardwebdienst, der eine SOAP/SPML-Schnittstelle (Simple Object Access Protocol und Service Provisioning Markup Language) zum Empfang von Provisioningbefehlen freilegt. Die Kommunikation zwischen dem Client und dem Provisioningmodul erfolgt über einen TLS-Kanal (Transport Layer Security).

Stellen Sie sicher, wenn Sie Provisioningbefehle an die Warteschlange senden, dass die Daten sicher gespeichert sind und nicht über eine nicht gesicherte Netzwerkverbindung gesendet werden.

Das Provisioningmodul muss Lese- und Schreibrechte für den zentralen Speicher von Single Sign-On haben, um die eingehenden Provisioningbefehle in die Warteschlange zu setzen, bis das Single Sign-On Plug-in die Befehle ausführt.

Befehle, die an das Provisioningmodul gesendet werden, können nicht rückgängig gemacht werden. Nach dem Senden bleiben Befehle in der Warteschlange, bis sie vom SIngle Sign-On Plug-in ausgeführt werden. Wenn Sie einen Befehl aus der Warteschlange entfernen müssen, senden Sie den gegenteiligen Befehl für jeden Benutzer, jede Anwendung und jedes Anmeldeinformationenobjekt, das aus der Warteschlange entfernt werden muss.

Hinweis: Das Provisioningmodul verwendet eine Schnittstelle, die mit SPML 2.0 konform ist. Nur die Kernvorgänge, die für die Konformität benötigt werden, werden unterstützt.

Das SPML 2.0-Modell

Die Provisioning-XML-Datei und Komponenten von Drittparteien, die SPML-Anfragen ausstellen, werden Requesting Authorities (RA) genannt.

Das Provisioningmodul ist ein Provisioning Service Provider (PSP). Dieser PSP unterstützt ein Provisioning Service-Ziel (PST), Single Sign-On-Provisioningbefehle pro Benutzer in die Warteschlange setzt.

Das Bereitstellen von sekundären Anmeldeinformationen für die Benutzer ist die Aktion, die beim Ausführen des Provisioning durchgeführt wird. Das heißt, dass die Endbenutzer und sekundären Anmeldeinformationen die Provisioning Service-Objekte (PSO) des Provisioning Service-Ziels sind. Die eindeutige Kennung (PSO-ID) für jeden Benutzer ist ein vollqualifizierter

Domänenname (FQDN). Die eindeutige Kennung (PSO-ID) für die sekundären Anmeldeinformationen ist die GUID, die den Anmeldeinformationen beim Erstellung zugewiesen wird. Da die sekundären Anmeldeinformationen einem bestimmten Benutzer zugewiesen sind, fungiert das Benutzer-PSO als Container für die Anmeldeinformationen-PSOs. Dies wird mit dem Element "containerID" in einer SPML-Anfrage ausgedrückt.

Genau genommen fügt Single Sign-On keine Benutzer hinzu, ändert oder löscht sie; Single Sign-On fügt jedoch Daten hinzu, ändert und löscht Daten, die einem Benutzer zugeordnet sind.

Provisioning und das Single Sign-On Plug-in

Da das Single Sign-On Plug-in letztendlich für den Schutz der sekundären Anmeldeinformationen des Benutzers mit benutzerspezifischen Verschlüsselungsschlüsseln verantwortlich ist, umfasst das Provisioning zwei Schritte. Zuerst erteilen Sie den Provisioningbefehl an das Provisioningmodul. Dann wendet das Single Sign-On Plug-in im Namen des Benutzers alle in der Warteschlange vorhandenen Provisioningbefehle auf den Datenspeicher mit den sekundären Anmeldeinformationen des Benutzers an.

Das Single Sign-On Plug-in erkennt in der Warteschlange vorhandene Provisioningvorgänge bei der normalen Synchronisierung, die beim Start erfolgt. Das Plug-in für in der Warteschlange vorhandene Provisioningbefehle aus und setzt dann die normale Aktivität fort. Dies stellt sicher, dass das Plug-in bei der Erstverwendung zuerst die Provisioningaktionen ausführt; dies verringert die Konfigurationsaufgaben, die der Endbenutzer bei der Erstverwendung ausführen muss.

Die Kommunikation zwischen dem Single Sign-on Plug-in und dem Provisioningmodul erfolgt über eine mit TLS gesicherte Verbindung.

Die Provisioninganwendung auf dem Client muss die Zuordnung zwischen den Anwendungen festlegen, die für das Provisioning verfügbar sind, und der clientseitigen Darstellung der Anwendung.

Provisioning von sekundären Anmeldeinformationen

Sekundäre Anmeldeinformationen sind einer bestimmten Anwendungsdefinition zugeordnet, die mit der Single Sign-On-Komponente im AppCenter erstellt wurde; der addRequest-Vorgang muss daher Daten enthalten, die Benutzerdetails in der Anfrage mit einer bestimmten Anwendungsdefinition verbinden. Das heißt, dass die anfordernde Autorität pro Benutzer die Liste der Anwendungen ermitteln muss, die für das Provisioning zur Verfügung stehen, und eine ID einer Anwendungsdefinition im Rahmen des addRequest-Vorgangs bereitstellen muss. Dies belastet die anfordernde Autorität mit der Ermittlung der Zuordnung zwischen den Single Sign-On-Anwendungsdefinitionen und der externen Identifizierung (z. B. dem Anwendungsnamen) der Anwendungen, für die das Provisioning ausgeführt wird.

Da die Person, die Single Sign-On verwaltet, und die Person, die Provisioningaufgaben ausführt, nicht unbedingt identisch sind, besteht das Potenzial von Missverständnissen und Verwirrung. Beispiel: Ein Single Sign-On-Administrator definiert die Anwendung Microsoft Outlook und ein Provisioningadministrator erstellt Microsoft Exchange-Konten. Single Sign-On lässt mehrere sekundäre Anmeldeinformationen für eine bestimmte Anwendungsdefinition zu. Beispiel: Ein Benutzer kann mehrere MSN-Hotmail-Konten haben, für die Single Sign-On Anmeldeinformationen gespeichert hat. Dies bedeutet, dass ein Administrator mehrere addRequests mit identischen Parametern ausgeben kann. In dieser Situation werden mehrere sekundäre Anmeldeinformationen erstellt. Der Administrator kann auch ggf. ein Provisioning mehrerer unterschiedlicher Anmeldeinformationen für dieselbe Anwendung durchführen; die Geheimnisse der Anmeldeinformationen (Benutzer-ID, Kennwort und benutzerdefinierte Felder) werden jedoch vom Single Sign-On Plug-in verschlüsselt und können nicht vom Provisioningmodul wiederhergestellt werden, um es der anfordernden Autorität zu erleichtern, die Anmeldeinformationen später zu unterscheiden.

Als Lösungsansatz für dieses Problem steht ein optionales privates Datenfeld, Provisioningbeschreibung, der anfordernden

Autorität in den Vorgängen addRequest und modifyRequest zur Verfügung. Damit kann die anfordernde Autorität eine ID oder beschreibende Daten hinzufügen, um die Anmeldeinformationen zu unterscheiden. Dieses Feld wird nicht vom Single Sign-On Plug-in oder dem Provisioningmodul geändert oder angezeigt. Es wird gespeichert und an die anfordernde Autorität zurückgegeben, wenn eine Liste der Anmeldeinformationen über lookupRequest angefordert wird.

Das Single Sign-On Plug-in hat vollständigen Bearbeitungszugriff auf alle sekundären Anmeldeinformationen. Hierzu gehört u. a. Duplizieren, Löschen und Ändern der Anmeldeinformationen. Dies bedeutet, dass Benutzer die Daten ändern können, sodass sie nicht mehr dem Zustand entsprechen, der von Provisioningvorgängen erstellt wurde.

Benutzer können Anwendungen auch willkürlich erstellen, d. h. sie können Anmeldeinformationen für Anwendungen hinzufügen, die nicht in der Single Sign-on Console definiert sind. Dies kann zu Eigentümerproblemen führen, beispielsweise ob ein Administrator sekundäre Anmeldeinformationen löschen oder ändern kann, oder ob diese Anmeldeinformationen in lookupResponse aufgelistet werden. Dieses Release des Single Sign-Ons unterstützt keine Eigentümerbeschränkungen; alle Anmeldeinformationen können entweder vom Administrator oder dem Endbenutzer geändert werden.

Anwendungsgruppen

Single Sign-On ermöglicht das Gruppieren von Anwendungen. Ein Attribut dieser Gruppierung ist die Verwendung desselben Kennworts für alle Anmeldeinformationen, die für Anwendungen in der Gruppe festgelegt sind. Wenn ein Benutzer Anmeldeinformationen ändert, die einer Gruppe zugeordnet sind, wird die Änderung auf alle Anmeldeinformationen aller Anwendungen in der Gruppe angewendet.

Dieses Verhalten gilt auch, wenn die Änderungen über die Provisioning-API ausgeführt werden Das heißt, wenn Anmeldeinformationen einer Anwendungsgruppe hinzugefügt werden, wird das neue Kennwort, das als Parameter dem Befehl "add" bereitgestellt wird, das Kennwort für jede Anwendung in der Gruppe. Der Befehl "add" hat dann den Nettoeffekt von "add" und mehrerer Befehle zum Ändern. Genauso ändert ein Befehl "modify" alle Anwendungen in einer Gruppe und hat daher den Nettoeffekt von mehreren Befehlen zum Ändern.

Fehlercodes

Code	Beschreibung
101	Mindestens eines der benötigten Anmeldeinformationenfelder fehlt in der Provisioninganfrage
102	Der angegebene Benutzername ist ungültig; der Benutzername fehlt oder das Format ist falsch
103	Angegebener Benutzer konnte nicht gefunden werden
104	Ungültige Anwendungsdefinition; die Anwendungsdefinition fehlt oder hat eine ungültige Struktur
105	Die Anmeldeinformationen-ID hat ein ungültiges Format.
106	Angegebenen Anmeldeinformationen können nicht gefunden werden.
107	Ungültiges Authentifizierungssicherheitstoken.
108	Nicht autorisiertes Zugriffstoken. Das angegebene Token ist nicht berechtigt, den gewünschten Vorgang auszuführen.
109	Ein anderer Prozess greift auf den Speichermechanismus zu. Versuchen Sie es später erneut.

Code	Beschreibung
110	Ein Fehler trat beim Verbrauch der Provisioningbefehle auf.
111	Benutzer ist nicht berechtigt, auf die Provisioningbefehlswarteschlange zuzugreifen.
112	Ein Fehler trat beim Abruf des geheimen Provisioningschlüssels auf.
113	Speicher für Verschlüsselung kann nicht zugewiesen werden.
114	Entropiedatenpuffer kann nicht zugewiesen werden.
115	Fehler bei der Verschlüsselung.
116	Verschlüsselungstextpuffer kann nicht zugewiesen werden.
117	Fehler bei der Entschlüsselung.
118	Fehler beim Formatieren des Windows-Fehlercodes für die Fehlermeldung.
119	PSO-ID fehlt oder hat falsches Format.
120	Anwendung, auf die verwiesen wird, konnte nicht gefunden werden.
121	Benutzerkonfiguration für diesen Benutzer konnte nicht gefunden werden.
122	Attribut "join" fehlt für Anmeldeinformationen in Kennwortgruppe.
123	Attribut "use-new-password" fehlt für Anmeldeinformationen in Kennwortgruppe.
124	Kennwort fehlt für Anmeldeinformationen in Kennwortgruppe.
125	Name der Anmeldeinformationen ist ungültig oder fehlt. Geben Sie einen gültigen Namen für die Anmeldeinformationen ein.
126	Ungültige Anwendungs-ID.
127	Anmeldeinformationen können Kennwortgruppe nicht erneut beitreten.
128	Provisioning ist für dieses Benutzerkonto nicht aktiviert

Zusammenfassung der API-Funktionen

Jul 22, 2016

Mit den API-Funktionen können Sie Aktionen in der Provisioning-XML-Datei definieren. Zusätzlich zu den Codebeispielen in diesen Themen finden Sie weitere Codebeispiele auf dem Installationsmedium des Produkts.

Alle für Single Sign-On spezifischen Elemente und Attribute haben als Präfix die Namespacekennung "ctxs". Der XML-Teil in jedem Textfeld listet eine Anfrage und eine entsprechende Antwort auf.

Nur der synchrone Ausführungsmodus wird unterstützt. Alle Anfragen zur Verwendung der asynchronen Ausführung führen zu unsupportedExecutionMode-Fehlern.

Aus Übersichtsgründen werden die folgenden beschreibenden Platzhalter statt Beispielwerte verwendet:

Platzhaltertext	**Bedeutung**
FQDN	Der vollqualifizierte Domänenname des Benutzers
application-GUID	Die GUID, die einer Anwendungsdefinition zugewiesen wird, wenn sie mit der Single Sign-On-Komponente der Delivery Service Console erstellt wird
credential-GUID	Die GUID, die den sekundären Anmeldeinformationen vom Provisioning Service nach Abschluss von addRequest zugewiesen ist.
RA-generated-ID	Eine eindeutige ID für eine Anfrage, die von der anfordernden Autorität erstellt wurde. Sie wird im optionalen Attribut requestID der Anfrageelemente verwendet. Sie ist nur relevant, wenn die Unterstützung für die asynchrone Ausführung hinzugefügt wird.
AuthToken	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.

Provisioning einer einzelnen Anwendung - addRequest

Jul 22, 2016

Fügen Sie mit addRequest einer Anwendung Anmeldeinformationen des Benutzers hinzu.

Ein Befehl "addRequest" fordert an, dass ein neues Objekt (die Anmeldeinformationen) dem angegebenen Containerobjekt (Datenspeicher des Benutzers) hinzugefügt wird. Eine Container-ID (der vollqualifizierte Domänenname (FQDN) des Benutzers) muss angegeben werden, und die psoID (Anmeldeinformationen-GUID) für das neu erstellte Objekt wird zurückgegeben. Die Daten der Anfrage sind die zu erstellenden Anmeldeinformationen.

Wenn die Anwendungsdefinition, die den neuen Anmeldeinformationen zugeordnet ist, ein Mitglied einer Kennwortgruppe ist, werden alle Anmeldungsinformationen, die den Mitgliedern dieser Gruppe zugewiesen sind, mit dem neuen Kennwort aktualisiert.

Syntax

AuthToken Credential name Admin Text Credential description appdefGuid Domain salima pass123 domain database

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
targetID (Pflichteingabe)	Die ID des Provisioningmoduls, die durch die targetID 'CPM Provisioning 1.0' identifiziert wird.
returnData (Pflichteingabe)	Data: Details der sekundären Anmeldeinformationen Identifier: Liste der Anmeldeinformationen des Benutzers Name: Wird nicht in Single Sign-On unterstützt Everything: Für diesen Benutzer verfügbare Anwendungsdefinitionen
executionMode (Pflichteingabe)	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token (Pflichteingabe)	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet. .
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.
data (Pflichteingabe)	"Data" ist die Beschreibung der Daten, die geändert werden. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.

ctxs:credential (Pflichteingabe)	Mit dem Credential-Element werden sekundäre Anmeldeinformationen beschrieben. Der Name und die Beschreibung des Credential-Elements sind optional. Wenn sie nicht eingegeben werden, verwendet das Plug-in den Namen und die Beschreibung aus der Anwendungsdefinition.
ctxs:application (Pflichteingabe)	Mit dem Application-Element werden eine Anwendungsdefinition und Details von Anmeldeinformationen beschrieben. Das Application-Element muss dem vorher mit einem lookupApplicationsRequest-Vorgang abgerufenen Element entsprechen.

Syntax für Rückgabewerte (addResponse)

Parameter für Rückgabewerte (addResponse)

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.
pso (Pflichteingabe)	Die Daten von "pso" sind Anmeldeinformationen, wie unter ctxs:credential beschrieben.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist die Anmeldeinformationen-GUID, die von lookupResponse zurückgegeben wird.
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.
data (Pflichteingabe)	"Data" ist die Beschreibung der Daten, die geändert werden. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.

Gruppenelementattribute

Die Attribute join und use-new-password des Gruppenelements steuern, wie sich die neuen Anmeldeinformationen auf die bestehenden Gruppenmitglieder auswirkt. Wenn die Anwendungsgruppe nicht für die gemeinsame Verwendung von Kennwörtern konfiguriert ist, wird das Gruppenelement ignoriert.

Join-Wert	**Use-new-password-Wert**	**Auswirkung**
False	False	Die Zuordnung zwischen den neuen Anmeldeinformationen und den bestehenden Anmeldeinformationen in der Gruppe wird aufgehoben. Es besteht keine Auswirkung auf die bestehende Gruppe.
False	True	Die Zuordnung zwischen den neuen Anmeldeinformationen und den bestehenden Anmeldeinformationen in der Gruppe wird aufgehoben. Es besteht keine Auswirkung auf die bestehende Gruppe.

Join-Wert	Use-new-password-Wert	Auswirkung
True	False	Die neuen Anmeldeinformationen werden der bestehenden Gruppe hinzugefügt. Das Kennwort der neuen Anmeldeinformationen wird auf das Kennwort gesetzt, dass die vorhandenen Gruppenmitglieder gemeinsam verwenden. Wenn es keine vorhandenen Gruppenmitglieder gibt, wird der Wert des Kennworts verwendet.
True	True	Die neuen Anmeldeinformationen werden der bestehenden Gruppe hinzugefügt. Das im Befehl enthaltene Kennwort wird für die neuen Anmeldeinformationen verwendet und allen vorhandenen Gruppenmitgliedern zugeordnet.

Die Anmeldeinformationen-GUID, die als psoID in der Antwort zurückgegeben wird, ist identisch mit der im lookupResponse-Vorgang aufgeführten und kann diese sekundären Anmeldeinformationen auch in den modifyRequest- oder deleteRequest-Vorgängen identifizieren.

batchRequest - Ausführen von einem Batch

Jul 22, 2016

Der batchRequest-Vorgang dient als Container für eine Liste mit anderen Vorgängen (requestnameRequest). Single Sign-On unterstützt nur den sequenziellen Verarbeitungsmodus. Ein batchRequest, der eine parallele Verarbeitung angibt, ergibt keinen Fehler, wird jedoch sequenziell verarbeitet.

Syntax

```
AuthToken
Credential name appdefGuid janed pwd123
AuthToken
Credential name appdefGuid2 salima pass123
```

Parameter

processing (Pflichteingabe)	Der Verarbeitungsmodus. Gültige Werte sind "sequential" und "parallel"; das Single Sign-On unterstützt jedoch nur den sequenziellen Modus. Bei Angabe der parallelen Verarbeitung wird die Anfrage von Single Sign-On sequenziell verarbeitet.
onError	Dies ist die Aktion, die Single Sign-On ausführen soll, wenn ein Fehler bei der Verarbeitung auftritt. Gültige Werte sind "resume" und "exit".
requestnameRequest (Pflichteingabe, Variable)	Listet jede Anfrage auf, die Sie in diesem Batch verarbeiten möchten; es werden die Syntax und die Parameter verwendet, die für diese Anfrage angegeben sind.

Syntax für Rückgabewerte (batchResponse)

Parameter für Rückgabewerte (batchResponse)

requestnameResponse (Variable)	Der Name jeder Anfrage, die in dieser Batchanfrage verarbeitet werden soll. Weitere Informationen zur Syntax der Rückgabewerte, die jeder Anfrage zugeordnet ist, finden Sie in der Dokumentation für diese Anfrage.

Löschen von Anmeldeinformationen - deleteRequest

Jul 22, 2016

Mit dem deleteRequest-Vorgang löschen Sie Anmeldeinformationen. Die Anmeldeinformationen-GUID gibt die Anmeldeinformationen an, die gelöscht werden.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
executionMode (Pflichteingabe)	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token (Pflichteingabe)	Das auth-token-Element ist Pflichteingabe, wird jedoch zurzeit nicht verwendet.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist die Anmeldeinformationen-GUID, die von lookupResponse zurückgegeben wird.
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.

Syntax für Rückgabewerte

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.

Löschen eines Benutzers - deleteRequest

Jul 22, 2016

Mit dem deleteRequest-Vorgang entfernen Sie alle Daten aus dem zentralen Speicher, die einem Benutzer zugeordnet sind.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
executionMode	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist die Anmeldeinformationen-GUID, die von lookupResponse zurückgegeben wird.

Syntax für Rückgabewerte (deleteResponse)

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.

Hinweise

Sie können Daten, die einem Benutzer zugeordnet sind, vollständig entfernen, wenn er das Unternehmen verlässt. Wenn Benutzer wichtige Informationen vergessen und nicht auf ihre Anmeldeinformationen zugreifen können, kann der Zustand von Single Sign-On zurückgesetzt werden, sodass sie erneut anfangen können (siehe resetRequest).

Diese zwei Szenarios, komplettes Entfernen der Daten und das Zurücksetzen der Daten, müssen unterschieden werden, da das Verhalten von Sign-On Plug-In anders ist. Abhängig von den Administratoreinstellungen kann eine lokale Kopie der Single Sign-On-Daten des Benutzers im Benutzerprofil gespeichert sein. Wenn der zentrale Speicher keine Daten des Benutzers enthält, führt das Plug-In einen Registrierungsassistenten aus und kopiert die lokalen Daten des Benutzers zum zentralen Speicher.

Beim Zurücksetzen der Benutzerdaten verwirft die Plug-In-Software die lokalen Daten und führt den Registrierungsassistenten aus.

Abfragen nach Zielen - listTargetsRequest

Jul 22, 2016

Mit dem listTargetsRequest-Vorgang werden im System konfigurierte Ziele abgefragt. Der Single Sign-On-Dienst unterstützt ein Ziel, das Provisioningmodul, das durch die targetID "CPM Provisioning 1.0" identifiziert ist.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
executionMode (Pflichteingabe)	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token (Pflichteingabe)	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.

Syntax für Rückgabewerte

Parameter für Rückgabewerte

requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.
Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
targetID (Pflichteingabe)	De ID des Provisioningmoduls: targetID='CPM Provisioning 1.0'.
schema (Pflichteingabe)	Die Antwort auf diesen Vorgang enthält eine eindeutige ID des Moduls und eines Schemas, die die Objekte beschreibt, die vom Provisioningmodul verwaltet werden, z. B. Benutzer und deren sekundäre Anmeldeinformationen.

Abrufen einer Liste der für einen Benutzer verfügbaren Anwendungen - lookupApplicationRequest

Jul 22, 2016

Mit dem Vorgang lookupApplicationRequest erhalten Sie eine Liste der Anwendungen, einschließlich der Anwendungs-IDs), die für einen bestimmten Benutzer zur Verfügung stehen. In Single Sign-On wird die Gruppe der Anwendungsdefinitionen, die für einen Benutzer verfügbar sind, in der Benutzerkonfiguration festgelegt, die dem Benutzer in der Konsole zugeordnet ist. Diese Anwendungsdefinitionen gehören nicht dem Benutzer und können nicht außerhalb der Konsole bearbeitet werden.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
authentication-token (Pflichteingabe)	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers.

Syntax für Rückgabewerte - lookupApplicationResponse

```
app-GUID1 Outlook Outlook 2003 Domain app-GUID2 Vantive Bug Database SAP
```

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers.
data (Pflichteingabe)	"Data" ist die Beschreibung der Daten, die geändert werden. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.
ctxs:application (Pflichteingabe)	Mit dem Application-Element werden eine Anwendungsdefinition und Details von Anmeldeinformationen beschrieben. Das Application-Element muss dem vorher mit einem lookupApplicationRequest-Vorgang abgerufenen entsprechen. Es gibt genau ein

	Anwendungselement für jede Anwendungsdefinition in der Benutzerkonfiguration des Benutzers. Weitere Informationen finden Sie unter ctxs:application.

Hinweise

Eine Suche nach diesem Typ der Daten ist eine Anomalie, die nicht von der SPML-Standardsemantik abgedeckt wird. Die Liste der für einen Benutzer verfügbaren Anwendungsdefinitionen wird mit einer spezifischen Funktion erhalten.

Abrufen einer Liste der gespeicherten Anmeldeinformationen - lookupRequest

Jul 22, 2016

Mit dem Vorgang lookupRequest erhalten Sie eine Liste der Anwendungen, für die ein Benutzer Anmeldeinformationen gespeichert hat. Der Wert des returnData-Attributs legt die zurückgegebenen Details fest.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
returnData (Pflichteingabe)	Data: Details der sekundären Anmeldeinformationen Identifier: Liste der Anmeldeinformationen des Benutzers Name: Wird nicht in Single Sign-On unterstützt Everything: Für diesen Benutzer verfügbare Anwendungsdefinitionen
executionMode (Pflichteingabe)	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token (Pflichteingabe)	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist die Anmeldeinformationen-GUID, die von lookupResponse zurückgegeben wird.

Syntax für Rückgabewerte - lookupResponse

```
credential-GUID1 Aviva Aviva 5250 Demo Aviva 5250 app-GUID1 Aviva 5250 Demo AppGroup credential-GUID2 Dynamic App1
```

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.
pso (Pflichteingabe)	Die Daten von "pso" sind Anmeldeinformationen, wie unter ctxs:credential beschrieben.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers. Nach dem SPML-Modell von Single Sign-On sind die Daten von pso ein Satz von Anmeldeinformationen, wie unter ctxs:credential beschrieben. Dies wird zurückgegeben, wenn das returnData-Attribut auf "Data" oder "Everything" gesetzt ist. Es gibt ein pso-Element für jede sekundären Anmeldeinformationen. Das ID-Attribut von psoID stellt die Anmeldeinformationen-GUID bereit.
data (Pflichteingabe)	Data ist die Beschreibung der gesuchten Daten. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.

ctxs:credential (Pflichteingabe)	Mit dem Credential-Element werden sekundäre Anmeldeinformationen beschrieben. Der Name und die Beschreibung des Credential-Elements sind optional. Wenn sie nicht eingegeben werden, verwendet das Plug-in den Namen und die Beschreibung aus der Anwendungsdefinition. Weitere Informationen finden Sie unter ctxs:credential.
ctxs:application (Pflichteingabe)	Mit dem Application-Element werden eine Anwendungsdefinition und Details von Anmeldeinformationen beschrieben. Das Application-Element muss dem vorher mit einem lookupApplicationRequest-Vorgang abgerufenen entsprechen. Es gibt genau ein Anwendungselement für jede Anwendungsdefinition in der Benutzerkonfiguration des Benutzers. Weitere Informationen finden Sie unter ctxs:application.

Hinweise

Wenn ein lookupRequest-Vorgang Anmeldeinformationen angibt, enthält die Antwort die Details der Anmeldeinformationen. Im Allgemeinen werden die Geheimnisse der Anmeldeinformationen von der Plug-in-Software verschlüsselt, und das Provisioningmodul kann nicht auf sie zugreifen. Das bedeutet, dass die Zeichendaten der bestimmten Feldelemente für Anmeldeinformationen, die bereits von der Plug-in-Software verwaltet werden, keine Eingabe enthalten.

Provisioning umfasst zwei Schritte. Das Provisioningmodul setzt die Provisioningbefehle zuerst in die Warteschlange. Dann führt die Plug-in-Software die in die Warteschlange gesetzten Befehle aus. Damit Sie eine gerade ausgeführte Aktion prüfen können, muss die zurückgegebene Anmeldeinformationenliste die in die Warteschlange gesetzten Befehle ausweisen. Da die in die Warteschlange gesetzten Befehle vom Provisioningmodul und nicht von der Plug-in-Software geschützt werden, kann das Provisioningmodul die Befehlsparameter entschlüsseln. Für die Anmeldeinformationen, für die Add- oder Modifybefehle in die Warteschlange gesetzt sind, werden auch die zugänglichen Befehlsparameter im lookupResponse-Vorgang aufgelistet. Hinweis: Die Befehlsparameter können die Benutzer-ID, das Kennwort und Werte für benutzerdefinierte Felder enthalten.

Abrufen sekundärer Anmeldeinformationen - lookupRequest

Jul 22, 2016

Mit diesem Vorgang rufen Sie Details von sekundären Anmeldeinformationen ab.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
returnData (Pflichteingabe)	Data: Details der sekundären Anmeldeinformationen Identifier: Liste der Anmeldeinformationen des Benutzers Name: Wird nicht in Single Sign-On unterstützt Everything: Für diesen Benutzer verfügbare Anwendungsdefinitionen
executionMode (Pflichteingabe)	Nur der synchrone Ausführungsmodus wird unterstützt. Alle Anfragen zur Verwendung der asynchronen Ausführung führen zu unsupportedExecutionMode-Fehlern.
authentication-token (Pflichteingabe)	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers.
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.

Syntax für Rückgabewerte - lookupResponse

```
Credential-name Admin text Credential description  app-GUID Outlook description from app-def Domain
```

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.
psoID (Pflichteingabe)	psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers. Nach dem SPML-Modell von Single Sign-On sind die Daten von pso ein Satz von Anmeldeinformationen,

	wie unter ctxs:credential Element beschrieben. Dies wird zurückgegeben, wenn das returnData-Attribut auf "Data" oder "Everything" gesetzt ist. Es gibt ein pso-Element für jede sekundären Anmeldeinformationen. Das ID-Attribut von psoID stellt die Anmeldeinformationen-GUID bereit.
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.
data (Pflichteingabe)	Data ist die Beschreibung der gesuchten Daten. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.
ctxs:credential (Pflichteingabe)	Mit dem Credential-Element werden sekundäre Anmeldeinformationen beschrieben. Der Name und die Beschreibung des Credential-Elements sind optional. Wenn sie nicht eingegeben werden, verwendet das Plug-in den Namen und die Beschreibung aus der Anwendungsdefinition. Weitere Informationen finden Sie unter ctxs:credential Element.
ctxs:application (Pflichteingabe)	Mit dem Application-Element werden eine Anwendungsdefinition und Details von Anmeldeinformationen beschrieben. Das Application-Element muss dem vorher mit einem lookupApplicationRequest-Vorgang abgerufenen entsprechen. Es gibt genau ein Anwendungselement für jede Anwendungsdefinition in der Benutzerkonfiguration des Benutzers. Weitere Informationen finden Sie unter ctxs:credential Element.

Ändern von Anmeldeinformationen - modifyRequest

Jul 22, 2016

Mit dem modifyRequest-Vorgang ändern Sie Anmeldeinformationen, die bereits mit dem Provisioning bereitgestellt wurden. Wenn die Anwendungsdefinition, die den geänderten Anmeldeinformationen zugeordnet ist, ein Mitglied einer Kennwortgruppe ist, werden alle Anmeldungsinformationen, die den Mitgliedern dieser Gruppe zugewiesen sind, mit dem neuen Kennwort aktualisiert.

Syntax

```
AuthToken      New Credential Name   username
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
ctxs:authentication-token	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	Die "credential ID" ist eine GUID (vom Single Sign-On-System erstellt und im zentralen Speicher abgelegt). Sie muss dem Wert entsprechen, der von lookupRequest zurückgegeben wird, und wird für die Suche nach den Anmeldeinformationen verwendet, die geändert werden.
containerID (Pflichteingabe)	Die containerID stellt den FQDN des Benutzers bereit, dem die Anmeldeinformationen gehören.
modification (Pflichteingabe)	modificationMode (optional) add: Hinzufügen von Anmeldeinformationen. Dies ergibt dasselbe Ergebnis wie ein addRequest-Vorgang. Wenn "modificationMode" auf "add" gesetzt ist, gelten dieselben Beschränkungen für psoID und Datenelemente wie beim addRequest-Vorgang. Die psoID darf nur einen Container angeben (wie bei deleteRequest) und die Daten müssen ein Credential-Element enthalten (wie bei addRequest). replace: Ersetzen eines Feldwerts; setzen Sie den neuen Wert in ein Tag. delete: Entfernen eines Feldwerts. Der Inhalt eines Datenelements wird ignoriert.
data (Pflichteingabe)	"Data" ist die Beschreibung der Daten, die geändert werden. Dies ist das Anmeldeinformationen-Element und kann untergeordnete Elemente der Anmeldeinformationen- und Anwendungselemente enthalten.
credential (Pflichteingabe)	Mit dem Credential-Element werden sekundäre Anmeldeinformationen beschrieben. Der Name und die Beschreibung des Credential-Elements sind optional. Wenn sie nicht eingegeben werden, verwendet das Plug-In den Namen und die Beschreibung aus der Anwendungsdefinition. Weitere Informationen finden Sie unter ctx:credential.
name	Der Name ist der Name der Anwendungsdefinition, wie er in der Single Sign-On-Komponente im AppCenter angezeigt wird.

application (Pflichteingabe)	Mit dem Application-Element werden eine Anwendungsdefinition und Details von Anmeldeinformationen beschrieben. Das Application-Element muss dem vorher mit einem lookupApplicationsRequest-Vorgang abgerufenen Element entsprechen. Weitere Informationen finden Sie unter ctxs:application. Wenn eine untergeordnete ID einer Anwendung angegeben wird, muss sie dem Wert entsprechen, der in den Anmeldeinformationen gespeichert ist.
group	Standardwerte werden bereitgestellt, wenn das Group-Element nicht Teil von add request ist. Mit diesem Element wird die Beziehung zwischen den neuen Anmeldeinformationen und den vorhandenen Anmeldeinformationen beschrieben, die der Gruppe zugeordnet sind. Weitere Informationen finden Sie unter Attribute für Group-Element.
fields (Pflichteingabe)	Jedes untergeordnete Element von Feldern, das im lookupResponse-Vorgang aufgelistet ist, muss im addRequest-Vorgang eingeschlossen sein, sonst wird ein Fehler zurückgegeben.
userID (Pflichteingabe)	userID ist das Konto des Benutzers für diese Anmeldeinformationen.
password (Pflichteingabe)	Password ist das Kennwort des Benutzers, das diesen Anmeldeinformationen zugeordnet ist.
Benutzerdefiniertes Feld	"Benutzerdefinierte Felder" enthalten die benutzerdefinierten Werte für diese Anmeldeinformationen. Single Sign-On unterstützt zusätzlich zu den Feldern "Benutzername" und "Kennwort" zwei benutzerdefinierte Felder.
psoID (Pflichteingabe)	Die psoID ist eine eindeutige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers und gibt den Container für die Anmeldeinformationen an, die geändert werden.

Syntax für Rückgabewerte - modifyResponse

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.

Hinweise

Mit modifyRequest können Sie nicht zugeordnete Anmeldeinformationen einer Gruppe hinzufügen, wenn Sie das Attribut join auf 'true' setzen (siehe addRequest). Das Gruppenelement unterliegt denselben Beschränkungen und hat dieselbe Auswirkung, wie unter addRequest beschrieben.

Hinweis: Alle untergeordneten ctxs:fields-Elemente, die für die Anwendung definiert sind, können in einem modifyRequest-Vorgang eingeschlossen werden. Die verfügbaren Felder werden unter
— lookupResponse
aufgelistet.

Gruppenelementattribute

Join-Wert	Use-new-password-Wert	Auswirkung
False	True	Die Zuordnung zwischen den neuen Anmeldeinformationen und den bestehenden Anmeldeinformationen in der Gruppe wird aufgehoben. Es besteht keine Auswirkung auf die bestehende Gruppe.
True	False	Die neuen Anmeldeinformationen werden der bestehenden Gruppe hinzugefügt. Das Kennwort der neuen Anmeldeinformationen wird auf das Kennwort gesetzt, dass die vorhandenen Gruppenmitglieder gemeinsam verwenden. Wenn es keine vorhandenen Gruppenmitglieder gibt, wird der Wert des Kennworts verwendet.
True	True	Die neuen Anmeldeinformationen werden der bestehenden Gruppe hinzugefügt. Das im Befehl enthaltene Kennwort wird für die neuen Anmeldeinformationen verwendet und allen vorhandenen Gruppenmitgliedern zugeordnet.

Die Anmeldeinformationen-GUID, die als psoID in der Antwort zurückgegeben wird, ist identisch mit der im lookupResponse-Vorgang aufgeführten und kann diese sekundären Anmeldeinformationen auch in den modifyRequest- oder deleteRequest-Vorgängen identifizieren.

Zurücksetzen eines Benutzers - resetRequest

Jul 22, 2016

Mit dem resetRequest-Vorgang setzen Sie den Single Sign-On-Status der Benutzer zurück, wenn sie nicht auf die Anmeldeinformationen zugreifen können.

Syntax

```
AuthToken
```

Parameter

requestID (Pflichteingabe)	Die vom Client generierte ID, mit denen die Rückgabewerte dieser Anfrage zugeordnet werden.
executionMode	Single Sign-On unterstützt den synchronen Ausführungsmodus.
authentication-token	Das Element "authentication-token" ist eine Pflichteingabe, wird jedoch zu diesem Zeitpunkt nicht verwendet.
psoID (Pflichteingabe)	Die psoID ist eine einmalige Kennung für jeden Endbenutzer; PSOID ist der FQDN des Benutzers.

Syntax für Rückgabewerte - resetResponse

Parameter für Rückgabewerte

Status (Pflichteingabe)	Mögliche Werte: Success, Failure, Pending
requestID (Pflichteingabe)	Die vom Client erstellte ID, mit denen diese Rückgabewerte dieser Abfrage zugeordnet werden.

Namespace-Elemente

Jul 22, 2016

Alle benutzerdefinierten Single Sign-On-Elemente, die in SPML-Befehlen verwendet werden, sind Mitglied des Namespace http://citrix.com/Provision. Dieser Namespace wird auch als CTXS-Präfix bezeichnet. Dieser Namespace hat drei Elemente auf der obersten Ebene, die in SPML-Befehlen, Authentifizierungstoken, Anwendung Anmeldeinformationen enthalten sind.

Element "Authentication-Token" - ctxs:authentication-token

Das Element "authentication-token" wird als Container für das Authentifizierungstoken (AuthToken) verwendet. Dieses Element ist Pflicht, wird jedoch nicht verwendet. Das Element "authentication-token" hat keine untergeordneten Elemente.

Syntax

```
AuthToken
```

Element "Application" - ctxs:application

Das Element application kann als Element auf der obersten Ebene oder als ein untergeordnetes Element des Elements "credential" auftreten.

Mit dem Element "application" wird sowohl eine Anwendungsdefinition (siehe lookupApplicationRequest) als auch die Details von "credential" beschrieben (siehe addRequest).

Syntax

```
app-GUID Outlook description from app-def  Domain
```

Hinweis: Keines der untergeordneten Elemente des Elements "fields" enthalten Zeichendaten in diesem Beispiel.

Parameter

ctxs-ID (Pflichteingabe)	Die GUID, die der Anwendungsdefinition zugeordnet wird, wenn sie in der Konsole erstellt wird
name	Der vom Administrator festgelegte Name der Anwendungsdefinition
description	Die vom Administrator festgelegte Beschreibung für die Anwendungsdefinition
Gruppe (Pflichteingaben bei Verwendung der gemeinsamen Kennwortverwendung)	Die Anwendungsgruppe, der diese Definition in der Konsole zugeordnet ist. Das Attribut "password-sharing" ist ein boolescher Wert, mit dem angegeben wird, ob diese Gruppe für die gemeinsame Kennwortverwendung konfiguriert ist. Weitere Informationen finden Sie unter addRequest.
fields (Pflichteingabe)	Listet die Datenfelder auf, die in dieser Anwendungsdefinition für Anmeldeinformationen konfiguriert sind. Jeder Untersatz der aufgelisteten Felder kann für eine beliebige Anwendungsdefinition definiert werden. Untergeordnete Elemente des Elements "fields": • userID entspricht der Benutzer-ID • password entspricht dem Kennwort des Benutzers • custom-field entspricht den benutzerdefinierten Feldern, die in einer Definition enthalten

	sein können; das Attribut "index" gibt das bestimmte Feld an (entweder '1' oder '2'), und das Attribut "label" enthält den optionalen Text.

Ein Beispiel eines Elements "application" als untergeordnetes Element des Elements "credential" finden Sie unter ctxs:credential.

Element "Credential" - ctxs:credential

Mit dem Credential-Element werden sekundäre Anmeldeinformationen beschrieben. Die meisten Anmeldeinformationen sind einer bestimmten Anwendungsdefinition zugeordnet; dies wird durch ein untergeordnetes Element "Anwendung" ausgedrückt. Anmeldeinformationen, die Benutzer manuell eingeben, enthalten kein Element "application".

Syntax

```
Credential Name user visible description  optional-RA provided-description   appdefGuid  johnd pass123 mydomain
```

Parameter

Status (Pflichteingabe)	Das Attribut "status" des Elements "credential" gibt den Status dieser Anmeldeinformationen aus Sicht des Single Sign-On Plug-ins an. Werte für Status sind "active (aktiv)" oder "queued (in Warteschlange)". Ein Wert von "active" bedeutet, dass die Anmeldeinformationen aktuell vom Single Sign-On Plug-in verwendet werden können. Ein Wert von "queued" bedeutet, dass ein Befehl zum Hinzufügen der Anmeldeinformationen in die Warteschlange gesetzt wurde, das Single Sign-On Plug-in diesen Befehl jedoch noch nicht verarbeitet hat.
pendingAction	Das Attribut "pendingAction" des Elements "credential" gibt an, ob in die Warteschlange gesetzte Befehle vorhanden sind, die sich auf diese Anmeldeinformationen auswirken. Werte für "pendingAction" sind "add (Hinzufügen)", "modify (Bearbeiten)" und "delete (Löschen)". Ein Wert von "delete" gibt an, dass ein Delete-Befehl für diese Anmeldeinformationen in die Warteschlange gesetzt wurde. Ein Wert von "modify" gibt an, dass ein Modify-Befehl für diese Anmeldeinformationen in die Warteschlange gesetzt wurde. Dieses Attribut ist optional und wird ausgelassen, wenn keine Befehle für die Anmeldeinformationen in die Warteschlange gesetzt wurden.
name	Das Attribut "name" des Elements "credential" ist der Wert, der vom Single Sign-On Plug-in im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) angezeigt wird. Der Benutzer kann diesen Wert im Eigenschaften-Dialogfeld der Anmeldeinformationen bearbeiten.
description	Der Wert "description" des Elements "credential" ist der Wert, der vom Single Sign-On Plug-in im Fenster "Kennwörter verwalten" (früher Anmeldungsmanager) angezeigt wird. Der Benutzer kann diesen Wert im Eigenschaften-Dialogfeld der Anmeldeinformationen bearbeiten.
provision-description	"provision-description" sind Administratordaten, die vom Single Sign-On Plug-in nicht angezeigt oder bearbeitet werden können. Sie werden ausschließlich zur Unterstützung des Provisioning-Administrators bereitgestellt.
application	Das Element "application" gibt die ID der Anwendungsdefinition und die Zeichen für die Benutzer-ID, das Kennwort und die Elemente "benutzerdefinierte Felder" an und enthält die Benutzerangaben für diese Anmeldeinformationen.