

# Info zum Citrix Usage Collector (Version 1.0 und 1.0.1)

Apr 03, 2015

Der Citrix Usage Collector sammelt Informationen zur gebührenpflichtigen Lizenzverwendung durch Citrix Service Provider und erstellt entsprechende Berichte direkt für Citrix.

Sie haben folgende Möglichkeiten:

- Festlegen der Lizenzserver (Sammelpunkte), von denen Nutzungsdaten abgerufen werden.
- Auflisten der Benutzer, die von der Berechnung ausgeschlossen sind.
- Festlegen der Benutzer und Gruppen, die Leseberechtigungen zum Anzeigen von Berichten oder Administratorrechte zum Ändern von Konfigurationen haben.
- Ändern des Anzeigenamens.
- Anzeigen von aktuellen oder vergangenen Berichten.
- Anzeigen von Warnungen.
- Ändern des Ports.

## Überlegungen

Sie können Ihre My Account-Anmeldeinformationen über die Benutzeroberfläche des Usage Collector neu registrieren, jedoch nur, wenn sich Ihre Kunden-ID geändert hat. Wenn Sie Ihre My Account-Anmeldeinformationen ändern und Ihre Kunden-ID sich nicht geändert hat, ist die Übertragung Ihrer Daten gefährdet.

## Behobene Probleme

- Dieser Fix behebt das Sicherheitsrisiko CVE-2014-0160 (Heartbleed). Weitere Informationen finden Sie im Knowledge Center-Artikel [CTX140605](#). [#0479792] (Version 1.0.1)
- Nutzungsdaten werden möglicherweise nicht angezeigt, wenn der Lizenzserver gemäß einem dieser Szenarien konfiguriert ist [#0460627] (Version 1.0.1):
  - Mehrere Lizenztypen (z. B. XDT\_PLT und XDT\_ENT) und ein Typ hat nur ein Subscription Advantage-Datum.
  - Nur ein Lizenztyp (z. B. XDT\_PLT) mit mehreren Subscription Advantage-Daten.
- Der Lizenzserver kann nicht mit dem Usage Collector kommunizieren, wenn ein Proxy konfiguriert ist. [#0460624] (Version 1.0.1)

## Bekannte Probleme

- Wenn Sie eine VM klonen, bei der sich Daten im Postausgangsordner befinden, können diese Daten auf den geklonten Server übernommen werden. Workaround: Leeren Sie den Postausgangsordner, bevor Sie den Server klonen. [#0426508]
- Beim Konfigurieren von Benutzern und Gruppen fügen Sie möglicherweise einen ungültigen oder falsch geschriebenen Benutzer- oder Gruppennamen hinzu, ohne dass eine Fehlermeldung angezeigt wird. Wenn ein Benutzer sich nicht beim System anmelden kann, stellen Sie sicher, dass Benutzername und Gruppenname gültig sind und dass der Benutzer ein Mitglied von Active Directory auf dem Citrix Usage Collector-Server ist. [#0416751]

# Systemanforderungen für Citrix Usage Collector

Apr 03, 2015

Citrix Usage Collector ist kompatibel mit derselben Hardware, die zur Unterstützung der kompatiblen Betriebssysteme erforderlich ist. Keine zusätzliche Hardware ist erforderlich.

## Anforderungen

- Ein oder mehrere Citrix Lizenzserver, Version 11.9 bis 11.12.
- Eine vorhandene Installation von Citrix Service Provider-fähigen Benutzer-/Gerätelizenzen auf einem oder mehreren Lizenzservern.
- Anmeldeinformationen für My Account unter citrix.com.
- Eine eindeutige Kunden-ID mit Anmeldeinformationen, die für die Berichterstellung zur Lizenznutzung für jeden Usage Collector-Server registriert sind. Verwenden Sie My Account, um diese Anmeldeinformationen zu erhalten.

Betriebssysteme	Sie können den Usage Collector auf Servern mit den folgenden Microsoft-Betriebssystemen installieren: <ul style="list-style-type: none"><li>• Windows Server 2008 R2</li><li>• Windows Server 2012</li></ul>
Erforderlicher Speicherplatz:	<ul style="list-style-type: none"><li>• 37 bis 40 MB</li></ul>
Browser	<ul style="list-style-type: none"><li>• Internet Explorer Version 9 und 10</li><li>• Mozilla Firefox Version 14.0 und 15.0</li><li>• Chrome Version 14.0 und 15.0</li></ul>

# Schnelleinstieg für den Citrix Usage Collector

Apr 03, 2015

Vor der Verwendung des Citrix Usage Collector:

1. Verwenden Sie Ihre My Account-Anmeldeinformationen unter [citrix.com](http://citrix.com), um eine eindeutige Kunden-ID mit Anmeldeinformationen zu erhalten, die für die Berichterstellung zur Lizenznutzung für jeden Usage Collector-Server registriert sind.
2. Überprüfen Sie die Anforderungen.
3. Laden Sie den Usage Collector herunter und installieren Sie ihn.
4. Konfigurieren Sie den Usage Collector.
5. Installieren Sie ein Zertifikat manuell (optional).

# Installieren

Apr 02, 2014

So installieren Sie den Citrix Usage Collector mit dem Assistenten

1. Melden Sie sich bei My Account unter [citrix.com](http://citrix.com) an und laden Sie die Datei Ctx\_UsageCollector.msi hier herunter:  
<https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Starten Sie "Ctx\_UsageCollector.msi".
3. Übernehmen Sie den Standardport (8084) oder konfigurieren Sie einen Port manuell.
4. Klicken Sie auf Citrix Usage Collector starten. Der Bildschirm wird geschlossen und eine webbasierte Benutzeroberfläche wird geöffnet. Sie können nun die Erstkonfiguration und anschließend weitere Konfigurationen durchführen.

So installieren Sie den Citrix Usage Collector ohne Benutzereingriff über die Befehlszeile

1. Melden Sie sich bei My Account unter [citrix.com](http://citrix.com) an und laden Sie die Datei Ctx\_UsageCollector.msi hier herunter:  
<https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Führen Sie das Installationsprogramm ohne Benutzereingriff über die Befehlszeile mit dem folgenden Befehl aus:  
msiexec /i Ctx\_UsageReportingTool.msi /quiet parameters

In der folgenden Tabelle werden die Befehlsparameter beschrieben.

Option	Beschreibung
INSTALLDIR =	Vorhandenes leeres Verzeichnis, in dem die Komponenten installiert werden. Überschreibt das Standardinstallationsverzeichnis \Citrix\Licensing\UsageCollector.
CTX_UC_PORT=	Überschreibt die Standardportnummer. Der Standardport ist 8084.
CTX_UC_PORT_AUTO_CONFIG=	Legt die automatische Portkonfiguration (Firewall) fest. 1 = ein (Standardeinstellung), 0 = aus.

Starten Sie die Benutzeroberfläche für die Konfiguration nach der Installation des Usage Collector über Start > Alle Programme > Citrix > Citrix UsageCollector.

# Konfigurieren des Citrix Usage Collector

Jan 10, 2017

So konfigurieren Sie den Citrix Usage Collector nach dem Abschluss der Installation

Verwenden Sie nach der Installation des Usage Collector die Benutzeroberfläche für die Erstkonfiguration.

Wenn Sie zum Beenden des Installationsassistenten auf Citrix Usage Collector starten geklickt haben, wird die Benutzeroberfläche für die Konfiguration angezeigt. Sie können die Erstkonfiguration auch über Start > Alle Programme > Citrix > Citrix UsageCollector starten.

1. Geben Sie Ihre My Account-Anmeldeinformationen ein.
2. Geben Sie einen Lizenzservernamen als Sammelpunkt und einen Webport ein. Lizenzserver, deren Version niedriger als 11.9 ist, können nicht als Sammelpunkte hinzugefügt werden.

So deaktivieren Sie das Abschneiden von Domänennamen

Wenn Sie mehrere Mandanten auf demselben Lizenzserver hosten, darf @domain.com nicht vom Lizenzserver abgeschnitten werden.

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. Navigieren Sie zum Registrierungsschlüssel:

Für 32-Bit-Maschinen: HKLM\Software\citrix\licenseserver

Für 64-Bit-Maschinen: HKLM\Software\Wow6432Node\citrix\licenseserver

Name: UDUseDomain

2. Setzen Sie den Registrierungsschlüssel auf 1.

Daten	Beschreibung
0	Das Domänenfeld wird abgeschnitten. (Standard)
1	Das Domänenfeld wird nicht abgeschnitten.

So nehmen Sie Konfigurationsänderungen vor

Nach der Installation und Erstkonfiguration von Usage Collector können Sie folgende Konfigurationen und Änderungen vornehmen:

- Sammelpunkte: Lizenzserver zum Abfragen von Nutzungsdaten
- Benutzer, die Konfigurationsänderungen vornehmen können
- Benutzer mit der Berechtigung "Nur Bericht"
- Gruppen mit Administratorrechten oder der Berechtigung "Nur Bericht"

1. Wenn Sie eine Verbindung zur Usage Collector-Benutzeroberfläche herstellen möchten, klicken Sie auf Start > Alle Programme > Citrix > Citrix UsageCollector.
2. Klicken Sie auf die Registerkarte Konfiguration und wählen Sie eine der Funktionen im Dropdownmenü aus.

Aufgabe	Anweisungen
<p>Ändern der allgemeinen Konfiguration:</p> <ul style="list-style-type: none"> <li>• Anzeigename</li> <li>• Citrix Service Provider (CSP)-Informationen: Kundenname und ID</li> <li>• Webport</li> </ul> <p>My Account-Anmeldeinformationen neu registrieren: Nur ausführen, wenn sich Ihre Kunden-ID geändert hat. Andernfalls ist die Datenübertragung gefährdet.</p>	Klicken Sie auf der Registerkarte Konfiguration auf Allgemein.
<p>Konfigurieren von Sammelpunkten, von denen der Usage Collector die Lizenznutzungsdaten abrufen. Sie können Sammelpunkte hinzufügen bzw. löschen.</p> <p>Es muss mindestens ein Sammelpunkt konfiguriert sein.</p>	<p>Klicken Sie auf der Registerkarte Konfiguration auf Sammelpunkte.</p> <ul style="list-style-type: none"> <li>• Mit der Schaltfläche Konfiguration testen wird eine Verbindungsanfrage an den Lizenzserver gesendet und es wird überprüft, ob der Citrix Lizenzierungsdienst ausgeführt und mindestens Version 11.9 verwendet wird.</li> <li>• Das Feld <u>Status</u> gibt an, ob ein Lizenzserver ausgeführt wird oder nicht.</li> </ul>
<p>Hinzufügen, Bearbeiten oder Löschen von Einzelpersonen und Gruppen sowie Festlegen von Rollen für Einzelpersonen und Gruppen.</p>	Klicken Sie auf der Registerkarte Konfiguration auf Benutzer.
<p>Hinzufügen und Löschen von Ausnahmen. Ausnahmen sind Benutzer, die vom Zähler des Usage Collector ausgenommen sind.</p> <p>Standardmäßig sind Ausnahmen Benutzer, die eine Lizenz auf einem bestimmten Lizenzserver ausgecheckt haben. Wenn Sie mehrere Clients auf einem einzelnen Lizenzserver hosten, verwenden Sie das Format user@domain.com und stellen Sie sicher, dass der Lizenzserver nicht @domain.com abschneidet.</p> <p>Da Ausnahmennamen aufgrund von Lizenzservereinstellungen und Längenbeschränkungen abgeschnitten werden können, empfiehlt Citrix, dass Sie Ausnahmen basierend auf den Benutzernamen erstellen, die von udamin.exe zurückgegeben werden.</p> <p>Wenden Sie sich an Citrix, um eine Liste von Ausnahmen zu vereinbaren.</p>	Klicken Sie auf der Registerkarte Konfiguration auf Ausnahmen.

Aufgabe	Anweisungen
---------	-------------

Deaktivieren des Abschneidens von Domännennamen unter Citrix Lizenzserver VPX

1. Gehen Sie in der Befehlszeile zur Datei `/opt/citrix/licensing/LS/conf/ud_settings.conf`.
2. Legen Sie mit dem `vi`-Editor `CTX_UD_USERDOMAIN=1` fest.
3. Starten Sie Lizenzserver VPX oder den Citrix Licensing Daemon neu.

Einstellung	Beschreibung
CTX_UD_USERDOMAIN=1	Verwenden Sie die Benutzerdomäne des Benutzerprofils. Deaktiviert das Abschneiden von Domännennamen.
CTX_UD_USERDOMAIN=0	Verwenden Sie nicht die Benutzerdomäne des Benutzerprofils. (Standard)

Daten	Be
0	Da
1	Da

Daten	Be
0	Da
1	Da

# Manuelle Installation eines Zertifikats eines zu einer Domäne gehörenden Usage Collector

Nov 06, 2013

So installieren Sie ein Zertifikat manuell

Sie können ein Zertifikat, das von einem zu einer Domäne gehörenden Usage Collector verwendet wird, manuell auf einem Lizenzserver installieren, der zu einer Domäne gehört.

## Teil 1: Microsoft Management Console (MMC)

Melden Sie sich beim Citrix Usage Collector-Server an, öffnen Sie die MMC und führen Sie die folgenden Schritte aus.

1. Fügen Sie das Zertifikat-Snap-In hinzu, indem Sie Datei > Snap-In hinzufügen/entfernen > Zertifikate > Computerkonto > Lokaler Computer wählen.
2. Klicken Sie im linken Bereich unter Zertifikate mit der rechten Maustaste auf Eigene Zertifikate, wählen Sie Alle Aufgaben > Neues Zertifikat anfordern und klicken Sie auf Weiter.
3. Wählen Sie unter "Zertifikatregistrierungsrichtlinie auswählen" die Option Active Directory-Registrierungsrichtlinie, klicken Sie auf Weiter, aktivieren Sie das Kontrollkästchen neben Computer und klicken Sie rechts auf Details.
4. Klicken Sie im angezeigten Feld auf Eigenschaften, geben Sie auf der Registerkarte "Allgemein" einen Anzeigenamen und eine Beschreibung in die Textfelder ein und klicken Sie auf Übernehmen.
5. Wählen Sie die Registerkarte Antragsteller aus, wählen Sie im Bereich Antragstellernamen im Dropdownmenü Typ die Option Allgemeiner Name aus, geben Sie den Anzeigenamen in das Textfeld Wert ein und klicken Sie auf Hinzufügen und auf Übernehmen.
6. Wählen Sie die Registerkarte Erweiterungen aus und fügen Sie aus dem Dropdownmenü Schlüsselerweiterung die Optionen Digitale Signatur und Schlüsselschlüssel zum Feld "Ausgewählte Optionen" hinzu.
7. Fügen Sie aus dem Dropdownmenü Erweiterte Schlüsselerweiterung (Anwendungsrichtlinien) die Optionen Serverauthentifizierung und Clientauthentifizierung zum Feld "Ausgewählte Optionen" hinzu und klicken Sie auf Übernehmen.
8. Wählen Sie die Registerkarte Privater Schlüssel aus und stellen Sie sicher, dass im Dropdownmenü "Schlüsseloptionen" die Schlüsselgröße 2048 und das Kontrollkästchen Privaten Schlüssel exportierbar machen ausgewählt sind. Klicken Sie dann auf Übernehmen.
9. Wählen Sie die Registerkarte Zertifizierungsstelle aus, stellen Sie sicher, dass das CA-Kontrollkästchen aktiviert ist und klicken Sie auf OK > Registrieren > Fertig stellen.
10. Wählen Sie in der Zertifikatkonsole Eigene Zertifikate > Zertifikate, klicken Sie auf das von Ihnen erstellte Zertifikat, wählen Sie Alle Aufgaben > Exportieren > Weiter, aktivieren Sie das Optionsfeld Ja, privaten Schlüssel exportieren und klicken Sie auf Weiter.
11. Wählen Sie unter Privater Informationsaustausch – PKCS #12 (.PFX) das Kontrollkästchen zum Einbeziehen aller Zertifikate aus, klicken Sie auf Weiter, erstellen Sie ein Kennwort und klicken Sie auf Weiter.
12. Klicken Sie auf "Durchsuchen" und navigieren Sie zu C:\Programme (x86)\Citrix\Licensing\UsageCollector\Apache\conf\, geben Sie Dateiname.PFX ein und folgen Sie den Anweisungen des Assistenten bis zum Fertigstellen.

## Teil 2: Befehlszeile

Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten und führen Sie die folgenden Schritte aus.

1. `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\`

2. `..\bin\openssl pkcs12 -in server.pfx -out server.crt -nokeys`
3. Geben Sie das Kennwort ein, das während des Exportvorgangs erstellt wurde (password).
4. `..\bin\openssl pkcs12 -in server.pfx -out server.key -nocerts -nodes`
5. Geben Sie das Kennwort ein, das während des Exportvorgangs erstellt wurde (password).
6. Starten Sie den Usage Collector neu.



# Manuelle Installation eines Zertifikats für den Usage Collector

Sep 02, 2014

## Erstellen eines Zertifikats

Zum Installieren eines Zertifikats sind drei Schritte erforderlich:

1. Rufen Sie eine .PFX-Datei ab, die das Zertifikat und einen privaten Schlüssel enthält. Sie können dazu eine von zwei Methoden anwenden.
2. Extrahieren Sie das Zertifikat und den privaten Schlüssel aus der .PFX-Datei.
3. Installieren Sie das Zertifikat und den privaten Schlüssel auf dem Usage Collector.

### Schritt 1, Methode 1: Abrufen der .PFX-Datei mit einem Domänenzertifikat

Melden Sie sich bei einem Server in der Domäne an, öffnen Sie die MMC und führen Sie die folgenden Schritte aus:

1. Erstellen Sie das Verzeichnis C:\uc\_cert für die exportierte .PFX-Datei.
2. Fügen Sie das Zertifikat-Snap-In hinzu, indem Sie Datei > Snap-In hinzufügen/entfernen > Zertifikate > Computerkonto > Lokaler Computer wählen.
3. Klicken Sie im linken Bereich unter Zertifikate mit der rechten Maustaste auf Eigene Zertifikate, wählen Sie Alle Aufgaben > Neues Zertifikat anfordern und klicken Sie anschließend auf Weiter.
4. Wählen Sie im Assistenten Zertifikatregistrierungsrichtlinie auswählen die Option Active Directory-Registrierungsrichtlinie, klicken Sie auf Weiter und aktivieren Sie anschließend das Kontrollkästchen neben Computer und klicken Sie rechts auf Details.
5. Wählen Sie Eigenschaften und geben Sie auf der Registerkarte Allgemein einen Anzeigenamen und eine Beschreibung ein.
6. Wählen Sie auf der Registerkarte Antragsteller unter Typ des Antragstellers aus dem Dropdownmenü Typ die Option Allgemeiner Name, geben Sie einen Anzeigenamen in das Textfeld ein, klicken Sie auf Hinzufügen und klicken Sie anschließend auf Anwenden.
7. Wählen Sie auf der Registerkarte Erweiterungen aus dem Dropdownmenü Schlüsselverwendung und fügen Sie Digitale Signatur und Schlüsselverschlüsselung dem Feld "Ausgewählte Optionen" hinzu.
8. Fügen Sie im Dropdownmenü Erweiterte Schlüsselverwendung die Optionen Serverauthentifizierung und Clientauthentifizierung dem Feld "Ausgewählte Optionen" hinzu. .
9. Vergewissern Sie sich auf der Registerkarte Privater Schlüssel unter dem Dropdownmenü Schlüsseloptionen, dass die Schlüsselgröße 2048 ist, aktivieren Sie das Kontrollkästchen Schlüssel ist exportierbar und klicken Sie anschließend auf Übernehmen.
10. Vergewissern Sie sich auf der Registerkarte Zertifizierungsstelle, dass das CA-Kontrollkästchen aktiviert ist, und klicken Sie auf OK > Registrieren > Fertig stellen.
11. Wählen Sie in der Zertifikatkonsole Eigene Zertifikate > Zertifikate, klicken Sie auf das von Ihnen erstellte Zertifikat, wählen Sie Alle Aufgaben > Exportieren > Weiter, aktivieren Sie das Optionsfeld Ja, privaten Schlüssel exportieren und klicken Sie auf Weiter.
12. Wählen Sie unter Privater Informationsaustausch – PKCS #12 (.PFX) das Kontrollkästchen zum Einbeziehen aller Zertifikate aus, klicken Sie auf Weiter, erstellen Sie ein Kennwort und klicken Sie auf Weiter.
13. Klicken Sie auf Durchsuchen, navigieren Sie zu C:\uc\_cert, geben Sie server.PFX ein und folgen Sie anschließend den Anweisungen des Assistenten, um den Vorgang abzuschließen.

## Schritt 1, Methode 2: Abrufen der .PFX-Datei zum Senden einer Anforderung an eine Zertifizierungsstelle (CA)

Diese Schritte hängen von der jeweiligen Zertifizierungsstelle ab.

1. Melden Sie sich beim Usage Collector an, öffnen Sie die MMC und führen Sie die folgenden Schritte aus:
  1. Fügen Sie das Zertifikat-Snap-In hinzu, indem Sie Datei > Snap-In hinzufügen/entfernen > Zertifikate > Computerkonto > Lokaler Computer wählen.
  2. Klicken Sie im linken Bereich unter Zertifikate mit der rechten Maustaste auf Eigene Zertifikate, wählen Sie Alle Aufgaben > Erweiterte Vorgänge > Benutzerdefinierte Anforderung erstellen und klicken Sie auf Weiter.
  3. Wählen Sie auf dem Bildschirm Benutzerdefinierte Anforderung die Option (Keine Vorlage) CNG-Schlüssel aus dem Dropdownmenü und PKCS#10 als Anforderungsformat und klicken Sie auf Weiter.
  4. Klicken Sie im Bildschirm Zertifikatinformationen auf Details und dann auf Eigenschaften.
  5. Geben Sie auf der Registerkarte Allgemein einen Anzeigenamen und eine Beschreibung ein.
  6. Wählen Sie auf der Registerkarte Antragsteller unter Antragstellernamen die Option Allgemeiner Name und geben Sie einen Wert in das Textfeld.
  7. Wählen Sie auf der Registerkarte Erweiterungen die Option Schlüsselverwendung aus dem Dropdownmenü und fügen Sie Digitale Signatur und Schlüsselverschlüsselung hinzu.
  8. Wählen Sie auf der Registerkarte Erweiterungen die Option Erweiterte Schlüsselverwendung aus dem Dropdownmenü und fügen Sie Serverauthentifizierung und Clientauthentifizierung hinzu.
  9. Wählen Sie auf der Registerkarte Privater Schlüssel als Kryptografiedienstanbieter RSA, Microsoft Software Key Storage Provider (Standard) aus dem Dropdownmenü, wählen Sie unter Schlüsseloptionen die Schlüsselgröße 2048 und aktivieren Sie Privaten Schlüssel exportierbar machen.
10. Speichern Sie die Datei als .REQ-Datei, reichen Sie die .REQ-Datei bei einer Zertifizierungsstelle (CA) ein und speichern Sie die .CER-Datei.
2. Wählen Sie in der MMC Zertifikate > Eigene Zertifikate > Zertifikate und klicken Sie mit der rechten Maustaste auf Alle Aufgaben > Importieren. Wählen Sie im Importassistenten die .CER-Datei.
3. Erstellen Sie das Verzeichnis C:\uc\_cert für die exportierte .PFX-Datei.
4. Wählen Sie in der Zertifikatkonsole Eigene Zertifikate > Zertifikate, klicken Sie auf das importierte Zertifikat, wählen Sie Alle Aufgaben > Exportieren > Weiter, aktivieren Sie das Optionsfeld Ja, privaten Schlüssel exportieren und klicken Sie auf Weiter.
5. Aktivieren Sie unter Privater Informationsaustausch – PKCS #12(.PFX) das Kontrollkästchen zum Einbeziehen aller Zertifikate, klicken Sie auf Weiter, erstellen Sie ein Kennwort und klicken Sie anschließend auf Weiter.
6. Klicken Sie auf "Durchsuchen", navigieren Sie zu C:\uc\_cert, geben Sie server.PFX ein und folgen Sie anschließend den Anweisungen des Assistenten, um den Vorgang abzuschließen.

## Schritt 2: Extrahieren des Zertifikats und des privaten Schlüssels

Dieser Schritt erfordert OpenSSL oder ein anderes Tool zum Extrahieren des Zertifikats und eines privaten Schlüssels aus einer .PFX-Datei.

Wichtig: Die im Lieferumfang des Usage Collectors enthaltene Version von OpenSSL unterstützt nicht die Extrahierung von Zertifikaten und privaten Schlüsseln. Sie können OpenSSL for Windows unter <https://www.openssl.org/related/binaries.html> herunterladen. Citrix empfiehlt die Installation von OpenSSL auf einer separaten Arbeitsstation, um diese Schritte auszuführen:

1. Navigieren Sie zum Ordner <openssl-Verzeichnis>\bin.
2. Führen Sie folgenden Befehl aus: `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.crt -nokeys`  
Hinweis: Der Usage Collector verwendet nur das Zertifikatsformat .CRT.

3. Geben Sie das Kennwort ein, das während des Exportvorgangs erstellt wurde (password).
4. Führen Sie folgenden Befehl aus: `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.key -nocerts -nodes`
5. Geben Sie das Kennwort ein, das während des Exportvorgangs erstellt wurde (password).

### Schritt 3: Installieren Sie die .CRT- und .KEY-Dateien auf dem Usage Collector


1. Kopieren Sie die oben erstellten Dateien `server.crt` und `server.key` nach `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\`
2. Starten Sie den Usage Collector neu.


# Berichte

Apr 03, 2015

Auf der Homepage von Citrix Usage Collector werden die vom Usage Collector kompilierten Ergebnisse aufgeführt. Die Ergebnisse umfassen Folgendes:

- Product name:
- Anzahl der verwendeten Lizenzen.
- Anzahl der Ausnahmen: Ausnahmen sind Benutzer, die vom Zähler des Usage Collector ausgenommen sind. Sie legen Ausnahmen auf der Registerkarte Konfiguration im Bildschirm Ausnahmen fest. Weitere Informationen zu Ausnahmen finden Sie unter [Konfigurieren des Citrix Usage Collector](#).
- Es gelten monatliche Abrechnungszeiträume. Sie können Berichte für den aktuellen Monat und für vergangene Monate anzeigen.
- Benachrichtigungen: Anzeige von Informations-, Warn- und Fehlermeldungen. Sie können einzelne oder alle Meldungen löschen.

 Informationsmeldung

 Warnmeldung

 Fehlermeldung

## Exportieren von Berichten

Die Homepage des Usage Collector enthält eine Option zum Exportieren und Speichern von Abrechnungsberichten.

Wenn Sie auf Bericht exportieren klicken, können Sie die CSV-Datei öffnen oder speichern und die Schaltfläche wird zu Bericht speichern, sodass Sie dieselbe Berichtdatei wieder öffnen oder speichern können. Zum Exportieren eines neuen Berichts aktualisieren Sie den Bildschirm des Browsers und die Schaltfläche Bericht exportieren wird erneut angezeigt.

Bei knappem Speicherplatz empfiehlt Citrix das regelmäßige Löschen der Berichte.

Citrix speichert tägliche Nutzungsberichte für den aktuellen Abrechnungszeitraum. Nachdem der letzte Bericht für den Monat übertragen wurde, löscht Citrix die täglichen Berichte und behält nur die monatlichen Abrechnungsberichte auf unbegrenzte Zeit.