

About the Citrix Usage Collector (versions 1.0 and 1.0.1)

Apr 03, 2015

The Citrix Usage Collector collects and reports billable license consumption for Citrix Service Providers directly to Citrix.

You can:

- Specify the license servers (collection points) to poll for usage data.
- List the users who are exempt from billing.
- Specify the users and groups who have read-only permission to view reports or who have administrator permission to modify configurations.
- Change the friendly name.
- View current or past reports.
- View alerts.
- Change the port.

Considerations

You can re-register your My Account credentials in the Usage Collector UI, but do not do so unless you are sure your customer ID has changed. Changing your My Account credentials when your customer ID has not changed jeopardizes your data transmission.

Fixed issues

- This fix addresses the security vulnerability CVE-2014-0160 (Heartbleed). For more information, see Knowledge Center article [CTX140605](#). [#0479792] (Version 1.0.1)
- Usage data might not be displayed when the License Server is configured in either of these scenarios [#0460627] (Version 1.0.1):
 - Multiple license types (for example, XDT_PLT and XDT_ENT) and one type has only one Subscription Advantage date.
 - Only one license type (for example, XDT_PLT) with multiple Subscription Advantage dates.
- The License Server cannot communicate with the Usage Collector when a proxy is configured. [#0460624] (Version 1.0.1)

Known issues

- When you clone a VM that has data in the outbox folder, that data might appear on the cloned server. Workaround: Empty the outbox folder before cloning the server. [#0426508]
- When configuring users and groups, you might be able to add an invalid or mistyped user name or group name without receiving an error message. If a new user is unable to log on to the system, verify that the user and group names are valid and that the user is a member of Active Directory on the Citrix Usage Collector server. [#0416751]

System requirements for Citrix Usage Collector

Apr 03, 2015

Citrix Usage Collector is compatible with the same hardware required to support the compatible operating systems. No additional hardware is required.

Requirements

- One or more Citrix license servers, version 11.9 through 11.12.
- An existing installation of Citrix Service Provider-enabled User/Device licenses on one or more license servers.
- My Account credentials at citrix.com.
- A unique customer ID with credentials registered for reporting usage for each Usage Collector server. Use My Account to acquire the credentials.

Operating Systems	<p>You can install the Usage Collector on servers running the following Microsoft operating systems.</p> <ul style="list-style-type: none">• Windows Server 2008 R2• Windows Server 2012
Disk Space Requirements	<ul style="list-style-type: none">• 37-40 MB
Browsers	<ul style="list-style-type: none">• Internet Explorer Version 9 and 10• Mozilla Firefox Version 14.0 and 15.0• Chrome Version 14.0 and 15.0

Get started with Citrix Usage Collector

Apr 03, 2015

Before using the Citrix Usage Collector:

1. Use your My Account credentials at citrix.com to acquire a unique customer ID with credentials registered for reporting usage for each Usage Collector server.
2. Verify requirements.
3. Download and install the Usage Collector.
4. Configure the Usage Collector.
5. Manually install a certificate (optional).

Install

Apr 02, 2014

1. Log on to My Account at citrix.com and download the Ctx_UsageCollector.msi from <https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Start the Ctx_UsageCollector.msi.
3. You can accept the default port (8084) or choose to manually configure a port.
4. Click Launch Citrix Usage Collector. This screen closes and a web-based UI opens. You can now do the initial configuration and then more advanced configuration.

1. Log on to My Account at citrix.com and download the Ctx_UsageCollector.msi at <https://www.citrix.com/downloads/licensing/components/citrix-usage-collector.html>.
2. Run the installer silently from the command line using:
msiexec /i Ctx_UsageReportingTool.msi /quiet parameters

The following table describes the command parameters.

Option	Description
INSTALLDIR =	Existing empty directory where components will be installed. Overrides the default installation directory <Program Files>\Citrix\Licensing\UsageCollector.
CTX_UC_PORT=	Overrides the default port number. The default port is 8084.
CTX_UC_PORT_AUTO_CONFIG=	Sets automatic port (firewall) configuration. 1 = on (default), 0 = off.

After you install the Usage Collector, start the configuration UI at Start > All Programs > Citrix > Citrix UsageCollector.

Configure the Citrix Usage Collector

Mar 10, 2016

Use the Initial Configuration UI after installing the Usage Collector.

If you clicked on Launch Citrix Usage Collector at the end of the wizard installation, the configuration UI displays. You can also start the initial configuration from Start > All Programs > Citrix > Citrix UsageCollector.

1. Enter your My Account credentials.
2. Enter a license server name as a collection point and a web port. A pre-11.9 license server cannot be added as a collection point.

If you are hosting multiple tenants on the same License Server, ensure that the License Server does not truncate @domain.com.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Locate the registry key:

For 32-bit machines: HKLM\Software\citrix\licenseserver

For 64-bit machines: HKLM\Software\Wow6432Node\citrix\licenseserver

Name: UDUseDomain

2. Set the registry key to 1.

Data	Description
0	The domain field is truncated. (default)
1	The domain field is not truncated.

After you install the Usage Collector and do the initial configuration, you can configure and make changes to:

- Collection points - license servers to poll for usage data
- Users who can make configuration changes
- Users with report-only permission
- Groups with administrator or report-only permission

1. If you need to connect to the Usage Collector UI, click Start > All Programs > Citrix > Citrix UsageCollector.
2. Click the Configuration tab and choose any of the functions in the drop-down menu.

Task	Instructions
<p>Edit the general configuration:</p> <ul style="list-style-type: none">• Friendly name• Citrix Service Provider (CSP) information - Customer name and ID• Web port <p>Re-register My Account credentials - Do not do this unless you are sure that your customer ID has changed; otherwise, your data transmission might be jeopardized.</p>	<p>On the Configuration tab, click General.</p>
<p>Configure the collection points from which the Usage Collector gets the license usage data. You can add or delete collection points.</p> <p>There must be at least one collection point configured.</p>	<p>On the Configuration tab, click Collection Points.</p> <ul style="list-style-type: none">• The Test Configuration button sends a connection request to the license server and verifies that the Citrix Licensing service is running and is at least version 11.9• The <u>Status</u> field specifies whether a license server is running or not.
<p>Add, edit, or delete individuals and groups and to specify the individual and group roles.</p>	<p>On the Configuration tab, click Users.</p>
<p>Add and delete exceptions. Exceptions are users who are exempt from being counted by the Usage Collector.</p> <p>By default, exceptions are users who checked out a license on a specific License Server. If you are hosting multiple clients on a single License Server, use the format user@domain.com and ensure that the License Server will not truncate @domain.com.</p> <p>Because exception names might be truncated based on License Server settings and string lengths, Citrix recommends that you create exceptions based on the usernames returned by uadmin.exe.</p> <p>Contact Citrix to agree on a list of exceptions.</p>	<p>On the Configuration tab, click Exceptions.</p>

1. On the command line, go to the `/opt/citrix/licensing/LS/conf/ud_settings.conf` file.
2. Using the `vi` editor, set `CTX_UD_USERDOMAIN=1`.
3. Restart the License Server VPX or the Citrix Licensing daemon.

Setting	Description
CTX_UD_USERDOMAIN=1	Use user domain from user profile. Disables domain name truncation.
CTX_UD_USERDOMAIN=0	Do not use user domain from user profile. (default)

Data
0
1

Data
0
1

Manually install a certificate used by the Usage Collector joined to a domain

Nov 06, 2013

You can manually install a certificate used by the Usage Collector that is joined to a domain to a license server that is joined to a domain.

Log on to the Citrix Usage Collector Server, open the MMC, and follow these steps.

1. Add the Certificate snap-in by selecting File > Add/Remove Snap-in > Certificates > Computer account > Local computer.
2. In the left pane under Certificates, right-click Personal and choose All Tasks > Request New Certificate, and click Next.
3. In the Certificate Enrollment Policy wizard, choose Active Directory Enrollment Policy, click Next, and select the check box next to Computer, and select Details to the right.
4. In the box that displays, select Properties and type a friendly name and description in the text boxes under the General tab and click Apply.
5. Select the Subject tab and in the Subject Type area, choose Common Name from the Type drop-down menu, type the Friendly Name into the Value text box, and click Add and then Apply.
6. Select the Extensions tab and from the Key usage drop-down menu, add Digital signature and Key encipherment to the Selected options box.
7. From the Extended Key Usage (application policies) drop-down menu, add Server Authentication and Client Authentication to the Selected options box, and click Apply.
8. Select the Private Key tab and under the Key options drop-down menu, ensure that the Key size is 2048 and the Key Exportable check box is selected, and click Apply.
9. Select the Certification Authority tab and ensure the CA check box is selected, and click OK > Enroll > Finish.
10. In the Certificates console, select Personal > Certificates, click the certificate you built, select All Tasks > Export > Next, and select the Yes, Export the Private Key radio button and Next.
11. Under Personal Information Exchange – PKCS #12(.PFX), select the check box to include all certificates, click Next, create a password, and click Next.
12. Click Browse and navigate to C:\program files (x86)\citrix\licensing\UsageCollector\Apache\conf\, type filename.PFX, and follow the wizard to finish.

Open an elevated command prompt and follow these steps.

1. `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf\`
2. `..\bin\openssl pkcs12 -in server.pfx -out server.crt -nokeys`
3. Type the password created during the export process (password).
4. `..\bin\openssl pkcs12 -in server.pfx -out server.key -nocerts -nodes`
5. Type the password created during the export process (password).
6. Restart the Usage Collector.

Manually install a certificate used by the Usage Collector

Sep 02, 2014

To install a certificate, there are three steps:

1. Obtain a .pfx file, which contains the certificate and private key. You can use one of two methods to do this.
2. Extract the certificate and private key from the .pfx file.
3. Install the certificate and private key on to the Usage Collector.

Log on to a server in the domain, open the MMC, and follow these steps:

1. Create a directory c:\uc_cert to hold the exported .pfx file.
2. Add the Certificate snap-in by selecting File > Add/Remove Snap-in > Certificates > Computer account > Local computer.
3. In the left pane under Certificates, right-click Personal and choose All Tasks > Request New Certificate, and then click Next.
4. In the Certificate Enrollment Policy wizard, choose Active Directory Enrollment Policy, click Next, and then select the check box next to Computer, and select Details to the right.
5. Select Properties and on the General tab, type a friendly name and description.
6. On the Subject tab, under Subject Type, choose Common name from the Type drop-down menu, type a friendly name in the text box, click Add, and then click Apply.
7. On the Extensions tab, choose Key usage from the drop-down menu, add Digital signature and Key encipherment to the Selected options box.
8. On the Extended Key Usage drop-down menu, add Server Authentication and Client Authentication to the Selected options box.
9. On the Private Key tab and under the Key options drop-down menu, ensure that the Key size is 2048 and select the Key Exportable check box, and then click Apply.
10. On the Certification Authority tab, ensure the CA check box is selected, and click OK > Enroll > Finish.
11. In the Certificates console, select Personal > Certificates, click the certificate you built, select All Tasks > Export > Next, and select the Yes, Export the Private Key radio button and Next.
12. Under Personal Information Exchange – PKCS #12(.PFX), select the check box to include all certificates, click Next, create a password, and click Next.
13. Click Browse, navigate to C:\uc_cert and type server.PFX, and then follow the wizard to finish.

These steps might vary based on your Certificate Authority.

1. Log on to the Usage Collector, open the MMC, and follow these steps:
 1. Add the Certificate snap-in by selecting File > Add/Remove Snap-in > Certificates > Computer account > Local computer.
 2. In the left pane under Certificates, right-click Personal and choose All Tasks > Advance Operations > Create Custom Request, and click Next.

3. On the Custom request screen, choose (No template) CNG key from the drop-down menu and PKCS#10 for the Request format, and click Next.
 4. On the Certificate Information screen, choose Details and click Properties.
 5. On the General tab, type a friendly name and description.
 6. On the Subject tab, under Subject name, choose Common name and type a value in the text box.
 7. On the Extensions tab, choose Key usage from the drop-down menu, add Digital signature and Key encipherment.
 8. On the Extensions tab, choose Enhanced Key usage from the drop-down menu, add Server Authentication and Client Authentication.
 9. On the Private Key tab, choose RSA, Microsoft Software Key Storage Provider (the default) and from the drop-down menu choose Key options and 2048 for the Key size and Make private key exportable.
 10. Save the file to a .req file, submit the .req file to a Certificate Authority (CA), and save the .cer file.
2. In the MMC, select Certificates > Personal > Certificates and right-click All Tasks > Import. In the Import wizard, select the .cer file.
 3. Create a directory c:\uc_cert to hold the exported .pfx file.
 4. In the Certificates console, select Personal > Certificates, click the certificate you just imported, select All Tasks > Export > Next, and select the Yes, Export the Private Key radio button and Next.
 5. Under Personal Information Exchange – PKCS #12(.PFX), select the check box to include all certificates, click Next, create a password, and then click Next.
 6. Click Browse, navigate to C:\uc_cert and type server.PFX, and then follow the wizard to finish.

This step requires OpenSSL or another tool that allows you to extract the certificate and private key from a .pfx file.

Important: The version of OpenSSL shipped with the Usage Collector does not support extracting certificates and private keys. You can download OpenSSL for Windows at <https://www.openssl.org/related/binaries.html>. Citrix recommends installing OpenSSL on a separate workstation to perform these steps:

1. Navigate to the <openssl directory>\bin folder.
2. Run `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.crt -nokeys`
Note: The Usage Collector uses only the .crt certificate format.
3. Type the password created during the export process (password).
4. Run `openssl pkcs12 -in C:\uc_cert\server.pfx -out server.key -nocerts -nodes`
5. Type the password created during the export process (password).


1. Copy the server.crt and server.key created above to `cd \program files (x86)\citrix\licensing\UsageCollector\Apache\conf`
2. Restart the Usage Collector.


Reports


Apr 03, 2015

The Citrix Usage Collector home page lists the results compiled by the Usage Collector. The results include:

- Product name.
- How many in-use licenses.
- Number of exceptions — Exceptions are users who are exempt from being counted by the Usage Collector. You specify them on the Exceptions screen under the Configuration tab. For more information about exceptions, see [Configure the Citrix Usage Collector](#).
- Billing periods are monthly — You can view reports for the current month, as well as past months.
- Notifications — Display informational, warning, and error messages. You can delete individual messages or all messages.

 Informational message

 Warning message

 Error message

Export reports

The Usage Collector home page contains an option to export and save billing reports.

When you click Export report, you have the option of opening or saving the .csv file and the button changes to Save report enabling you to open or save that same report file again. To export a new report, refresh the browser screen and the Export report button displays again.

Citrix recommends deleting reports periodically if disk space is an issue.

Citrix maintains daily usage reports for the current billing period. After the last report for the month is transmitted, Citrix deletes the daily reports and retains forever only the monthly billing reports.