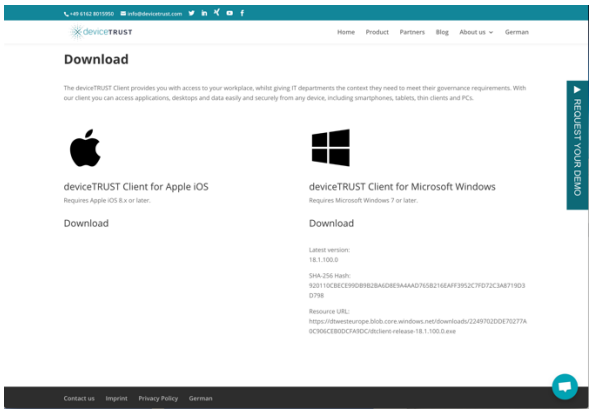
deviceTRUST 18.1.100 for Windows

Welcome to the 18.1 release of deviceTRUST. This release includes a new auto-update feature which can be used to automatically update your deviceTRUST Windows Clients, support for the PCoIP protocol with Amazon WorkSpaces and a new Application Level encryption between the deviceTRUST Host and Client.

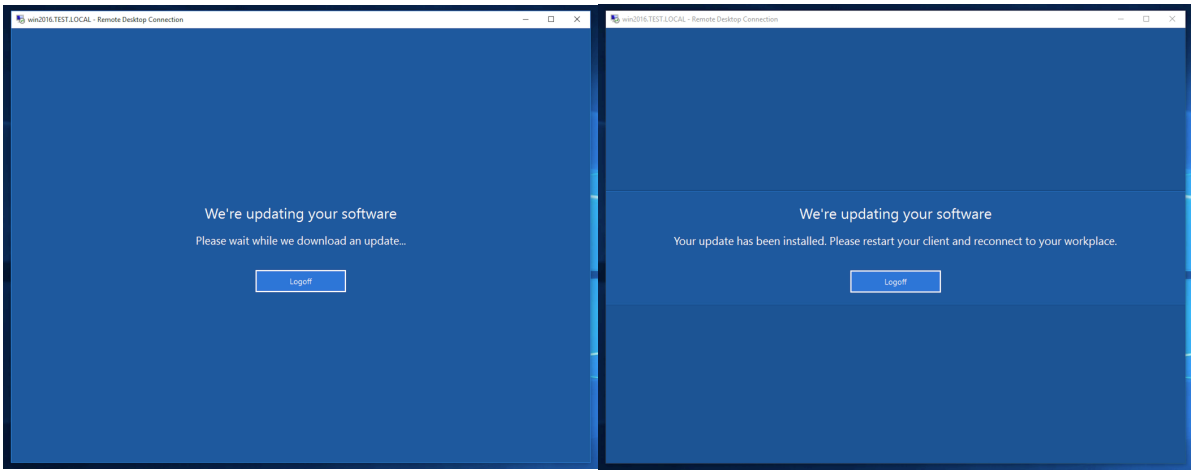
Simplified end user installer for Windows available on deviceTRUST.com

We've replaced our previous Windows Client installers with a single, all users executable, and we've made this installer available to download at https://devicetrust.com/download. This facilitates moving the responsibility of the client installer away from your administrators, and into the hands of your users.



Auto-update support for Windows Client

We've added the ability to seamlessly update our Windows Client, with almost no interaction from the remote user. Firstly, you can now enforce a minimum version of the Windows Client, prompting the user to download the latest client from our website. Secondly, you can choose to perform the upgrade automatically for all compatible clients that don't meet the minimum version policy. When users connect, they will see a message that their deviceTRUST Client is being upgraded.



Release Notes

Support for PCoIP protocol with Amazon WorkSpaces

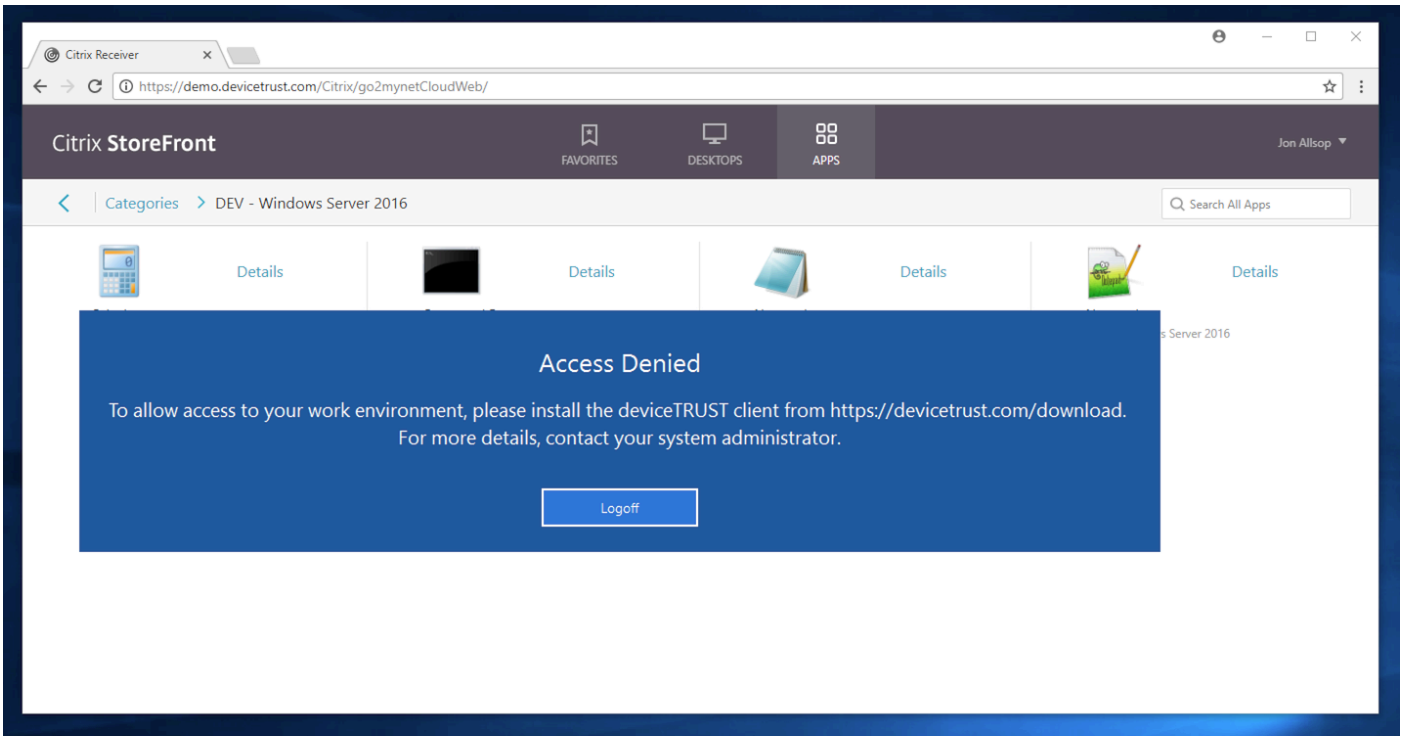
We're very excited to introduce Amazon WorkSpaces support for the PCoIP protocol, bringing the same set of features that are available with RDP and ICA to the PCoIP protocol. The additional context provided by deviceTRUST is more important than ever when hosting your desktops outside of your data center.

Additional level of encryption across virtual channel

The communication between the remote client and the host has always been encrypted by the underlying Virtual Channel protocol, however we've introduced our own application level encryption layer on top for increased security. Our application level encryption involves a key exchange using an automatically generated 2048-bit RSA key pair, followed by encrypting all communication using a 256-bit AES-GCM stream cipher.

Conditional Access now compatible with Citrix and Microsoft published applications.

The conditional access feature previously available to remote desktops, is now also available to remote published applications when using RDP or ICA protocols. The control of conditional access remains with the 'dtcmd ACCESS' command, however for the remote user their applications will be hidden from view whilst a suitable message is shown to the user.



Improved Integration with UEM vendor products

Integration with UEM vendors is of critical importance to us and responding to property changes within these products can be a challenge. To simplify this, we've introduced a new command line tool 'dtnotify.exe', which can be invoked at any time, and with any arguments, to initiate process trigger workflows within UEM vendor products.

Version: 09.05.2018 10:46:03

New VBScript trigger types

We've added support for calling VBScript's from within any of our triggers. VBScript brings comparable power as is provided by PowerShell, but with a performance that's even faster than Batch files, ensuring your Logon and Reconnect times are kept to a minimum.

New auditing policy

All of our auditing events can now be selectively enabled or disabled from within the policy. Combined with the existing policy to whitelist properties, this gives you full control of the information that is written to the Windows Event Log.

New process name option in app termination

In previous releases we've been able to gracefully terminate applications that do not meet the AppLocker policy, or any arbitrary process identified by its process id. In 18.1, we've extended this functionality with the ability to match a process using the process name or process path, optionally using wildcards. Hence the following command will gracefully terminate all running instances of notepad within the current session:

dtcmd.exe APPKILL /message:"Notepad will be closed" /process:notepad.exe

WHOIS properties now support ARIN and LACNIC internet numbers

We've enhanced our WHOIS properties to introduce global support for all regional internet registry's, bringing support for the American Registry for Internet Numbers (ARIN) and Internet Addresses Registry for Latin America and Caribbean (LACNIC).

New properties – Screen Saver

We've introduced Screen Saver properties into both the host and the remote device. These new properties allow new use cases, such as ensuring that remote sessions are only secured by a screen saver and password, if not similarly configured on the remote device. The new properties include:

- DEVICE_SCREENSAVER_ENABLED – Set to true when a screen saver is enabled, false otherwise.
- DEVICE_SCREENSAVER_SECURE – Set to true whenever a password must be entered on resume, false otherwise.
- DEVICE_SCREENSAVER_TIMEOUT – Set to the timeout period in seconds before displaying the screen saver.
- DEVICE_SCREENSAVER_FILENAME – Set to the filename of the configured screen saver.

New properties – Smart Card Reader

Smart card reader properties are new in 18.1 and bring consistency to the same properties that appeared in our 17.2 IGEL client. The new properties include:

- DEVICE_SMARTCARDREADER_COUNT – The number of smart card readers available.
- DEVICE_SMARTCARDREADER_X_NAME – The name of the smart card reader.

New properties – Domain

We've moved some domain properties into a new domain category of properties, whilst adding a few new properties too. These new properties give an additional guarantee that the domain is the one that it claims to be, beyond that of the domain name. The new domain properties include:

- DEVICE_DOMAIN – The name of the domain (previously DEVICE_NAME_DOMAIN).
- DEVICE_DOMAIN_DNS – The DNS name of the domain (previously DEVICE_NAME_DOMAIN_DNS).
- DEVICE_DOMAIN_SID – The security identifier (SID) of the domain.
- DEVICE_DOMAIN_JOINED – Set to true whenever the local machine is domain joined, false otherwise (previously DEVICE_OS_DOMAINJOINED).

New properties – Certificate

Our certificate properties identify certificates which include a private key, are in date, and have a chain of trust to a certificate within the root certificate store. In 18.1, these have been extended with additional information about that trusted root certificate with the following properties:

- DEVICE_CERTIFICATE_ROOT_NAME – The name of the trusted root certificate.
- DEVICE_CERTIFICATE_ROOT_THUMBPRINT_SHA1 – The SHA1 hash of the trusted root certificate.

New properties – Hardware

Our hardware properties have been extended with the following new properties:

- DEVICE_HARDWARE_ROLE – Identifies the role of the local machine and can be set to one of Desktop, Mobile, Workstation, EnterpriseServer, SOHOServer, AppliancePC, PerformanceServer or Slate.
- DEVICE_HARDWARE_LID – On a mobile (i.e. Laptop) role, set to Open whenever the lid of the device is open, otherwise set to Closed.

New properties – OS

We've added one new property to our OS category.

- DEVICE_OS_ID – An arbitrary string which uniquely identifies the installation of the OS. If the OS was reinstalled (or sysprep'd), this identifier would change. If the OS image was transported to another device, this value would stay the same.

Breaking changes

Whilst every effort is made to minimize breaking changes, sometimes this is unavoidable. It is therefore important to review these changes to determine whether an upgrade to 18.1 could impact your current implementation.

- A Microsoft Update to Windows 10 and Windows Server 2016, when using the OS provided firewall, resulted in the DEVICE_ACTIONCENTER_FIREWALL_NAME (and HOST_ACTIONCENTER_FIREWALL_NAME) changing name to "Windows-Firewall" (previously "Windows Firewall" without the "-"). For consistency with all

previous releases of Microsoft Windows, we now look for this value and change it back to “Windows Firewall”.

- On Windows 7, the following properties were previously set to “Unavailable”. In 18.1, we no longer set these properties.
    - DEVICE_ACTIONCENTER_FIREWALL_NAME (and HOST_ACTIONCENTER_FIREWALL_NAME).
    - DEVICE_ACTIONCENTER_ANTIVIRUS_NAME (and HOST_ACTIONCENTER_ANTIVIRUS_NAME).
    - DEVICE_ACTIONCENTER_ANTIVIRUS_TIMESTAMP (and HOST_ACTIONCENTER_ANTIVIRUS_TIMESTAMP).
    - DEVICE_ACTIONCENTER_ANTIVIRUS_UPTODATE (and HOST_ACTIONCENTER_ANTIVIRUS_UPTODATE).
    - DEVICE_ACTIONCENTER_ANTISPYWARE_NAME (and HOST_ACTIONCENTER_ANTISPYWARE_NAME).
    - DEVICE_ACTIONCENTER_ANTISPYWARE_TIMESTAMP (and HOST_ACTIONCENTER_ANTISPYWARE_TIMESTAMP).
    - DEVICE_ACTIONCENTER_ANTISPYWARE_UPTODATE (and HOST_ACTIONCENTER_ANTISPYWARE_UPTODATE).
- The following properties have been removed and are now available in the new Domain category of properties.
    - DEVICE_NAME_DOMAIN (and HOST_NAME_DOMAIN).
    - DEVICE_NAME_DOMAIN_DNS (and HOST_NAME_DOMAIN_DNS).
    - DEVICE_OS_DOMAINJOINED (and HOST_OS_DOMAINJOINED).
- With the addition of the new process name option in app termination, we no longer default to applying ‘dtcmd APPKILL’ against the AppLocker policy whenever the /pid argument was not supplied. Instead, we now require the /policy argument to ensure processes are checked against the AppLocker policy.
- With the new feature to support conditional access to published applications, we’ve changed the following:
    - We’ve renamed our DesktopReady and DesktopStarting triggers to ShellReady and ShellStarting, thus the TRIGGER_NAME property within these triggers will have changed to these new values.
    - We’ve renamed ‘dtcmd DESKTOP’ to ‘dtcmd ACCESS’.
- The timing of ShellStarting has changed when running on a Terminal Server, ensuring that the trigger is now as late as possible before the shell is actually started.
- With the introduction of the new Auditing policy, we’ve deprecated the previous ‘Track Usage’ policy. To disable the tracking of users in 18.1, simply disable ‘Event ID 21: Usage’ from within the auditing policy.

Bugs addressed in 18.1

- We’ve addressed a bug where international characters would not be shown when calling ‘dtcmd GET’.
- We’ve fixed an issue with a black screen after pressing Ctrl+Alt+Del and attempting to run Task Manager from within a restricted desktop.
- An issue with the OS version number has been fixed on Windows 10.
- When using Citrix ICA protocol, we’ve fixed an issue where the HOST_SESSION_CLIENT_IP address displayed the address of the gateway when using IGEL clients.
- When deviceTRUST Client is installed on the same machine as Citrix Receiver, fixed an issue where it is not possible to uninstall deviceTRUST Client after uninstalling Citrix Receiver.
- Various performance improvements.

Known Issues

- The Microsoft Remote Desktop Virtual Channel requires a per-user edit to HKCU, which is automatically registered for the user installing the deviceTRUST Client, but other users with existing logon sessions do not receive this registration until next time they login. This is particularly apparent when a non-administrative user installs the deviceTRUST Client and enters the credentials of an administrative user. In this scenario, the virtual channel is only registered for the administrative user. The user that launched the deviceTRUST Client must logoff and back in again to receive the registration. This issue only impacts users of the Microsoft RDP protocol, and does not impact Citrix ICA or Amazon Workspace clients.

Installation Media

The installation media includes the following components:

- *dthost-x86-release-18.1.100.0.msi* – The 32-bit host installer
- *dthost-x64-release-18.1.100.0.msi* – The 64-bit host installer
- *dtclient-x86-release-18.1.100.0.msi* – The 32-bit all users client installer
- *dtclient-x64-release-18.1.100.0.msi* – The 64-bit all users client installer
- *dtclient-release-18.1.100.0.exe* – 32-bit and 64-bit all users client installer
- *dtpolicydefinitions-18.1.100.0.zip* – The ADMX policy definitions for configuring the software

All of the installation files within the installation media require administrative privileges.

Please note that the Citrix Receiver and Amazon WorkSpaces on a 64-bit operating system contains 32-bit components, therefore ensure the 32-bit client is installed when using ICA or PCoIP on a 64-bit operating system.

Compatibility

Please consult the product data sheet for a list of supported platforms and technologies.