deviceTRUST 17.1.100

Welcome to the 17.1 release of deviceTRUST. This release is packed full of features, including support for Multi-Hop, App Locker integration, App Kill, Popup message, plus new triggers and properties! We've also simplified our iOS client, and published it to the App Store. New triggers include desktop starting and desktop ready. New properties include Windows Update, Windows Defender, Windows Firewall, Logical Disks, Mapped Drives, amongst others. Check out the full list below!

iOS Client

We added a new QR code registration system to our iOS client, allowing simple pairing of the iOS client with your deviceTRUST tenant. Our iOS client has also been published to the Apple App Store.

Multi Hop Support

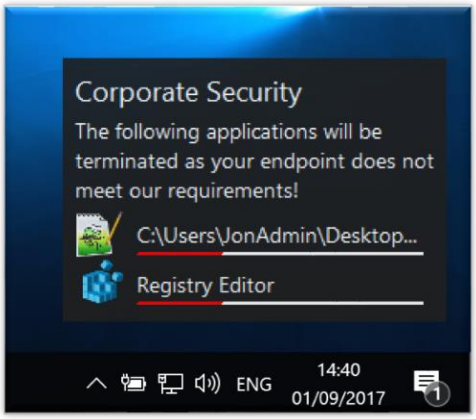
We now support Multi Hop, allowing properties to propagate from the most remote client, across one or more hosts. This behavior is enabled by default, but can be disabled by policy. Additional host properties can be obtained from intermediate hops providing, among other possibilities, the visibility of the route taken from the most remote device to their desktop or application.

AppLocker Integration

We've added integration with Microsoft's AppLocker, allowing individual applications to be allowed or denied based upon the context of the remote device. Using the deviceTRUST Command Processor (dtcmd.exe APPLOCKER), Microsoft AppLocker rules can be changed at any time during the session, even in response to the dynamic change of a property.

App Kill Support

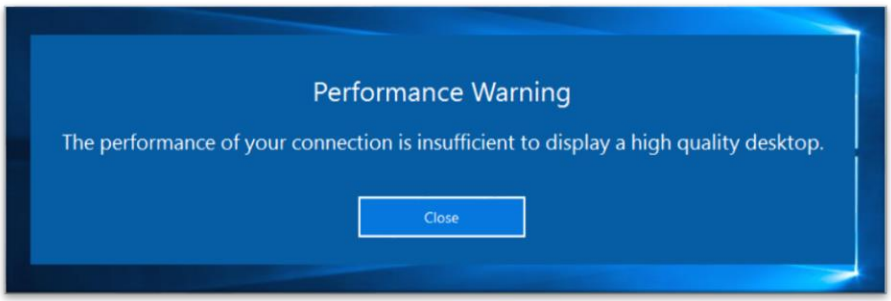
We've added support for the controlled termination of running applications. Using the deviceTRUST Command Processor (dtcmd.exe APPKILL), applications to terminate can either be identified by the PID of a process, or automatically identified by the current AppLocker rules. Applications can optionally be given a title, message and timeout period, during which a top-most popup dialog can inform the user of the pending application termination:



Version: 04.09.2017 11:29:32

Popup's and Toast Message Support

We've added the ability to display popup messages to the user using the deviceTRUST Command Processor (dtcmd.exe POPUP). Popups are displayed with a title and message, and can be a modal dialog as shown below.



Alternatively, on supported platforms popups can be displayed as a non-modal OS notification with an optional image:

User Message Translations

All of the user messages available within the deviceTRUST Configuration can now be translated. Translations can either be targeted at a language (e.g. 'en' or 'de') or a region (e.g. 'en-US' or 'de-DE').

New Trigger – Desktop Starting

We've added a new 'DESKTOP STARTING' trigger which is generated as the shell (explorer.exe) process is first run. This ensures that the OS has finished initializing the session. A new policy allows the host properties to be refreshed before the trigger is executed.

New Trigger – Desktop Ready

We've added a new 'DESKTOP READY' trigger which is generated as soon as the shell (explorer.exe) process has finished initializing. This is useful if you depend upon properties which are only successfully initialized by the shell itself, such as the Mapped Drives. A new policy allows the host properties to be refreshed before the trigger is executed.

Proxy Server Support

Both the host and client now use the Internet Explorer proxy settings of the logged in user for any HTTP requests.

New Properties – Windows Update

We've added support for Windows Update properties, both on the remote Windows devices and the local host. These create interesting security use cases, enabling simple control depending on the local or remote devices Windows Update health.

- DEVICE_WINDOWSUPDATE_ENABLED – Set to true whenever the Windows Update service is enabled.
- DEVICE_WINDOWSUPDATE_VERSION – Set to the version number of Windows Update.
- DEVICE_WINDOWSUPDATE_REBOOTREQUIRED – Set to true whenever Windows Update is awaiting a reboot to finish updating.
- DEVICE_WINDOWSUPDATE_NOTIFICATIONLEVEL – Represents how Windows Update is configured to notify the user, with values NotConfigured, Disabled, NotifyBeforeDownload, NotifyBeforeInstall or ScheduledInstall.
- DEVICE_WINDOWSUPDATE_LASTSEARCH – Set to the time that Windows Update last checked for updates.
- DEVICE_WINDOWSUPDATE_LASTINSTALL – Set to the time that Windows Update last installed updates.
- DEVICE_WINDOWSUPDATE_PENDING_DEFINITION – A list of all pending Windows Defender updates.
- DEVICE_WINDOWSUPDATE_PENDING_CRITICAL – A list of all pending OS critical updates.
- DEVICE_WINDOWSUPDATE_PENDING_SECURITY – A list of all pending OS security updates.
- DEVICE_WINDOWSUPDATE_PENDING_ROLLUP – A list of all pending OS rollups.
- DEVICE_WINDOWSUPDATE_PENDING_SERVICEPACK – A list of all pending OS service packs.
- DEVICE_WINDOWSUPDATE_PENDING_UPDATE – A list of all pending OS updates.

New Properties – Windows Defender

We've added support for Windows Defender properties, on remote Windows devices and the local host. Windows Defender properties are real-time, allowing triggers to quickly respond to changes to threats.

- DEVICE_WINDOWSDEFENDER_STATUS – The status of Windows Defender, which can be one or more of None, ServiceUnavailable, EngineUnavailable, FullScanRequired, RebootRequired, ThreatManualStepsRequired, DueAntivirusSignature, DueAntispywareSignature, DueQuickScan, DueFullScan, InprogressSystemScan, InprogressRoutineCleaning, DueSamples, EvaluationMode, ProductExpired, ThreatCallistoRequired, ServiceOnSystemShutdown, ServiceCriticalFailure, ServiceNonCriticalFailure, Initialised, DuePlatformUpdate, InprogressPlatformUpdate, PlatformAboutToBeOutdated, EndOfLife.
- DEVICE_WINDOWSDEFENDER_LASTQUICKSCAN – The time of the last quick scan.
- DEVICE_WINDOWSDEFENDER_LASTFULLSCAN – The time of the last full scan.
- DEVICE_WINDOWSDEFENDER_SIGNATURETHREATS – The number of threats identified due to the file signature.
- DEVICE_WINDOWSDEFENDER_BEHAVIORTHREATS – The number of threats identified due to the behaviour of the process.
- DEVICE_WINDOWSDEFENDER_VERSION_ENGINE – The version of the engine.
- DEVICE_WINDOWSDEFENDER_VERSION_ANTIMALWARE – The version of the anti-malware component.
- DEVICE_WINDOWSDEFENDER_VERSION_ANTIVIRUS – The version of the anti-virus component.

- DEVICE_WINDOWSDEFENDER_VERSION_ANTISPYWARE – The version of the anti-spyware component.
- DEVICE_WINDOWSDEFENDER_VERSION_NETWORKENGINE – The version of the network engine.
- DEVICE_WINDOWSDEFENDER_VERSION_NETWORKDEFINITION – The version of the network definitions.

New Properties – Windows Firewall

deviceTRUST 17.1 now includes detail information about the state of the Windows Firewall, for both remote devices and the local host. Queries can be defined by policy against both inbound and outbound rules which reduce the reported rules to those of interest.

- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_NAME – The names of all active network profiles.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLED – The active network profiles which have a disabled firewall.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_BLOCKALLINBOUND – The active network profiles which are blocking all inbound traffic.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_INBOUNDALLOWED – The active network profiles that by default allow inbound traffic unless overridden by an inbound rule.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_OUTBOUNDALLOWED – The active network profiles that by default allow outbound traffic unless overridden by an outbound rule.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_DISABLEDNOTIFICATIONS – The active network profiles that do not display a notification to the user when a process is blocked from receiving inbound connections.
- DEVICE_WINDOWSFIREWALL_ACTIVEPROFILES_RESPONDTOMULTICAST – The active network profiles that are permitted to send a unicast response to multicast or broadcast network traffic.
- DEVICE_WINDOWSFIREWALL_INBOUNDRULES_PROGRAMS – A list of all programs and their ports permitted to accept incoming connections.
- DEVICE_WINDOWSFIREWALL_INBOUNDRULES_PACKAGES – A list of all packages and their ports permitted to accept incoming connections.
- DEVICE_WINDOWSFIREWALL_INBOUNDRULES_SERVICES – A list of all services and their ports permitted to accept incoming connections.
- DEVICE_WINDOWSFIREWALL_INBOUNDRULES_SYSTEM – A list of all ports permitted to accept incoming connections by the system.
- DEVICE_WINDOWSFIREWALL_INBOUNDRULES_ANY – A list of all ports permitted to accept incoming connections by any process.
- DEVICE_WINDOWSFIREWALL_OUTBOUNDRULES_PROGRAMS – A list of all programs and their ports permitted to make outbound connections.
- DEVICE_WINDOWSFIREWALL_OUTBOUNDRULES_PACKAGES – A list of all packages and their ports permitted to make outbound connections.
- DEVICE_WINDOWSFIREWALL_OUTBOUNDRULES_SERVICES – A list of all services and their ports permitted to make outbound connections.
- DEVICE_WINDOWSFIREWALL_OUTBOUNDRULES_SYSTEM – A list of all ports permitted to establish outbound connections by the system.
- DEVICE_WINDOWSFIREWALL_OUTBOUNDRULES_ANY – A list of all ports permitted to establish outbound connections by any process.

New Properties – Logical Disk

An array of all logical disks, either on the remote Windows device, or on the local host has been added. By default, all logical disks are returned, however these can be filtered by supplying a custom query within the policy.

- DEVICE_LOGICALDISK_COUNT – The number of logical disks.
- DEVICE_LOGICALDISK_X_TYPE – The type of logical disk, set to one of *Removable, Fixed, Remote, Cdrom or Ramdisk.*
- DEVICE_LOGICALDISK_X_LABEL – The volume label associated with the logical disk.
- DEVICE_LOGICALDISK_X_FLAGS – Flags associated with the logical disk, which can be one or more of *PreservedNames, CaseSensitiveSearch, DaxVolume, SupportsCompression, NamedStreams, PersistentAcls, ReadOnly, SequentialWriteOnce, SupportsEncryption, ExtendedAttributes, HardLinks, ObjectIds, OpenByFileId, ReparsePoints, SparseFiles, Transactions, UsnJournal, UnicodeFileNames, IsCompressed, SupportsQuotas*.
- DEVICE_LOGICALDISK_X_HIDDEN – Set to true if the logical disk is hidden, false otherwise.
- DEVICE_LOGICALDISK_X_FILESYSTEM – The file system of the logical disk, e.g. NTFS.
- DEVICE_LOGICALDISK_X_DRIVE – The drive where the logical disk is mounted.
- DEVICE_LOGICALDISK_X_PATH – The path to the logical disk.
- DEVICE_LOGICALDISK_X_TOTALMB – The total capacity of the logical disk in megabytes.
- DEVICE_LOGICALDISK_X_FREEMB – The number of free megabytes remaining.

New Properties – Mapped Drive

An array of all mapped drives, either on the remote Windows device, or on the local host has been added. By default, all mapped drives are returned, however these can be filtered by supplying a custom query within the policy.

- DEVICE_MAPPEDDRIVE_COUNT – The number of mapped drives.
- DEVICE_MAPPEDDRIVE_X_DRIVE – The drive where the mapped drive is mounted.
- DEVICE_MAPPEDDRIVE_X_SERVER – The name of the remote server.
- DEVICE_MAPPEDDRIVE_X_SHARE – The name of the share on the remote server.
- DEVICE_MAPPEDDRIVE_X_HIDDEN – Set to true if the mapped drive is hidden, false otherwise.
- DEVICE_MAPPEDDRIVE_X_USER – The name of the user authenticating the connection to the remote server.
- DEVICE_MAPPEDDRIVE_X_PROVIDER – The provider of the mapped drive.

New Properties – Carrier

For our mobile devices, defines the carrier that the mobile phone SIM is registered to.

- DEVICE_CARRIER_NAME – The name of the user's cellular service provider.
- DEVICE_CARRIER_COUNTRY_NAME – The country name of the user's cellular service provider.
- DEVICE_CARRIER_COUNTRY_CODE – The ISO country code for the user's cellular service provider.
- DEVICE_CARRIER_NETWORK_NAME – The network name of the user's cellular service provider.
- DEVICE_CARRIER_NETWORK_CODE – The mobile network code (MNC) for the user's cellular service provider.

New Properties – Action Center

Our existing action center properties have been extended with additional information on Windows 8 or later remote Windows devices or the local host.

- DEVICE_ACTIONCENTER_ANTIVIRUS_NAME – The name of the anti-virus product.
- DEVICE_ACTIONCENTER_ANTIVIRUS_TIMESTAMP – The timestamp of the anti-virus product.
- DEVICE_ACTIONCENTER_ANTIVIRUS_UPTODATE – Set to true if the anti-virus product is up to date, false otherwise.
- DEVICE_ACTIONCENTER_ANTISPYWARE_NAME – The name of the anti-spyware product.
- DEVICE_ACTIONCENTER_ANTISPYWARE_TIMESTAMP - The timestamp of the anti-spyware product.
- DEVICE_ACTIONCENTER_ANTISPYWARE_UPTODATE – Set to true of the anti-spyware product is up to date, false otherwise.
- DEVICE_ACTIONCENTER_FIREWALL_NAME – The name of the firewall product.

New Properties – Remoting Client

We've added additional information about the outbound connection to the remote device.

- DEVICE_REMOTINGCLIENT_OUTBOUND_ADDRESS – The IP address of the outbound connection established by the remoting client.
- DEVICE_REMOTINGCLIENT_OUTBOUND_DNS – The DNS name established from a reverse DNS lookup, of the outbound connection of the remoting client.

New Properties – Session

Our session properties have been extended with additional properties on the local host which describe the delivery of the session. These properties are currently only supported on Citrix ICA sessions.

- HOST_SESSION_DELIVERY_TYPE – Set to *Application* when the session contains one or more published application, or *Desktop* when the session is a published desktop.
- HOST_SESSION_DELIVERY_NAME – Set to a semi-colon separated list of published applications when the delivery type is Application, or the name of the published desktop when delivery type is Desktop.

New Properties - Region

We've added additional information about the keyboard to our region properties for the remote device and local host.

- DEVICE_REGION_KEYBOARD_LANGUAGE – The language that the keyboard is currently set to, e.g. 'English (United States)' or 'Germany (Germany)'.
- DEVICE_REGION_KEYBOARD_LOCALE – The locale that the keyboard is currently set to, e.g. en-US or de-DE.

Limitations

We've found that when using the ICA protocol, that our per-user client installer does not always establish the virtual channel, resulting in the properties being unavailable. We've working with Citrix to address this issue; however, we recommend that you use our all-users client installers until this issue is resolved.

Installation Media

The installation media includes the following components:

- *dthost-x86-release-17.1.100.0.msi* – The 32-bit host installer
- *dthost-x64-release-17.1.100.0.msi* – The 64-bit host installer
- *dtclient-x86-release-17.1.100.0.msi* – The 32-bit all users client installer
- *dtclient-x64-release-17.1.100.0.msi* – The 64-bit all users client installer
- *dtclient-user-release-17.1.100.0.exe* – 32-bit and 64-bit per user client installer
- *dtpolicydefinitions-17.1.100.0.zip* – The ADMX policy definitions for configuring the software

All of the MSI files within the installation media require administrative privileges. The per user client installer can be installed without administrative privileges.

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

Compatibility

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