


NativeServices.RegistryGetUserValues

Method	RegistryGetUserValues
Module	NativeServices
Library	Core
Action	Fetch a registry value for every user under HKU.
Parameters	<p>Subkey (string): The registry key to look for.</p> <p>Name (string): The name of the registry value for which to fetch its value. Use an empty string to get the (default) value.</p> <p>UsersOnly (bool, optional, default false): Get values only for keys representing "real" users (and not for keys representing system pseudo-users or groups).</p>
Return values	<p>Name (string): Full location of the value being retrieved.</p> <p>ValueType (string): "REG_DWORD" etc. as appropriate.</p> <p>Value (string): The actual value of an appropriate type, converted to a string if not one already.</p> <p>Sid (string): SID the value was found under.</p> <p>Username (string): Domain\Username of the aforementioned SID.</p>
Example	<pre>NativeServices.RegistryGetUserValues(Subkey: "Console", Name: "FaceName");</pre>
Platforms	<ul style="list-style-type: none">Windows
Notes	<p>REG_NONE keys are not supported.</p> <p>From v4.1, REG_MULTI_SZ values are displayed with a ' ' between each string; up to v4.0 only the first string was displayed.</p> <p>There is a limit of 8192 values being returned. This limit applies to all users in total, <i>not</i> per user. This is currently not changeable.</p> <p>If the subkey or registry value name does not exist, then the method will return Success (no content).</p> <p>If searching for the (default) value and it is 'not set', then the method will return Success (no content).</p> <p>Empty values are returned; empty values are not the same as 'not set'.</p> <p>If information is retrieved from the .DEFAULT key or a _Classes key, the Username will be reported as "Unknown". It is possible to determine the owner of a _Classes key from the SID that precedes it (which will have a correct Username).</p> <p>Registry values of type REG_EXPAND_SZ are not expanded, so for example the variable with Name "TEMP" in the subkey "ENVIRONMENT" usually has a value of "%USERPROFILE%\AppData\Local\Temp". This is because the Tachyon Agent does not have sufficient privilege to impersonate user accounts for security reasons.</p> <div style="border: 1px solid red; padding: 10px;"><p> Warning</p><p>This method may attempt to call AD to translate a SID to a username.</p></div>