**SERVER CONNECTION PROPERTIES**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| XA_SRV | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\Servers\INDY<br>0000: reg_sz | Valid Server NETBIOS or FQDN Name or IP address | Primary XA (SSO) server name |
| XA_AUDIT_SRV | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>0000: reg_sz | Valid Server NETBIOS or FQDN Name or IP address | auditSERVER name |
| XA_PRX_SRV | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\Indy<br>0000: reg_sz | Valid Server NETBIOS or FQDN Name or IP address | Prox Card Server Name |
| X_D_SRV | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>0000: reg_sz | Valid Server NETBIOS or FQDN Name or IP address | HCIDeploy server name |
| X_RA_SRV | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory\INDY<br>0000: reg_sz | Valid Server NETBIOS or FQDN Name or IP address | Remote Authentication Server name |
| X_PREF_IPV4 | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>PreferIPv4: reg_dword<br>HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>PreferIPv4: reg_dword<br>HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient<br>PreferIPv4: reg_dword<br>HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory<br>PreferIPv4: reg_dword<br>HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient<br>PreferIPv4: reg_dword | 1 | Indicates that any TCP/IP communication prefers to use IPv4 when IPv6 is installed and available<br>This setting will be ignored if the *_SRV setting(s) listed above contain a direct IPv6 address. |

**SSO CLIENT SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| X_SP | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\Servers\INDY<br>Port: reg_dword | 15001 | Communications port for XA (SSO) server |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\Servers\INDY<br>EnabledServerIDs: reg_sz | 0 | Enabled Servers List. Comma delimited list of server identifiers 0000,0001,0002, etc. |
| XA_EC | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\SocketTransport\Indy<br>Encryption: reg_sz | RIJNDAEL | Encryption Class:<br>RIJNDAEL, RIJNDAEL128, RIJNDAEL256, BLOWFISH, BLOWFISH256, TWOFISH, SERPENT |
| XA_CC | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\SocketTransport\Indy<br>Compression: reg_sz | VCLZIP | Compression Class:<br>NONE, VCLZIP |

**PROXCARD CLIENT SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| XA_PRX_SRV_PRT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\Indy<br>Port: reg_dword | 30000 | Communications port for Proxcard Server |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\Indy<br>EnabledServerIDs: reg_sz | 0 | Enabled Servers List. Comma delimited list of server identifiers 0000,0001,0002, etc. |
| | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\SocketTransport\Indy<br>Encryption: reg_sz | RIJNDAEL | Encryption Class:<br>RIJNDAEL, RIJNDAEL128, RIJNDAEL256, BLOWFISH, BLOWFISH256, TWOFISH, SERPENT |
| | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\SocketTransport\Indy<br>Compression: reg_sz | VCLZIP | Compression Class:<br>NONE, VCLZIP |

| | | | | |
|---|---|---|---|---|
| X_PROX_RT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ReaderType: reg_sz | USB | ProxCard ReaderType<br>USB - RFIdeas USB device support<br>RFVC - RFIdeas Linux -> Citrix session support<br>RFSerial - RFIdeas Reader Serial device support<br>SCARD - OMNIKEY Reader support |
| X_PSE | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\PIN<br>PinPromptInMinutes: red_dword | 4294967295 | Specify enabling PIN Support. Users will be prompted to validate with pin:<br>Set this to enabled (4294967295) or disabled (0) |
| X_PIN_LEN | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\PIN<br>MinPinLength: reg_dword | 4 | Specify the minimum PIN length a user must use when enrolling a PIN:<br>4, 5, or 6 |
| X_ALLOW_PIN | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient\PIN<br>AllowPinEnrollment: reg_dword | 1 | Set this to enable (1) or disable (0) PIN Self enrollment. |
| X_PSCL | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ParityStripCountLeading: reg_dword | 0 | Parity Strip Count Leading bits |
| X_PSCT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ParityStripCountTrailing: reg_dword | 0 | Parity Strip Count Trailing bits |
| X_BBS | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BlankBadgeScan: reg_dword | 1 | Blank Badge Scanning allowed - if this setting is disabled, enrollment of unassigned cards is disabled. |
| X_HPI | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>HardwarePollInterval: reg_dword | 500 | Hardware polling interval in milliseconds |
| X_TOUT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>SupportTapoutUpdateTime: reg_dword | 1 | Rolling password save enabled |
| X_PSWT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ServiceStartupConnectionWaitTimeout: reg_dword | 30 | Service Startup Connection Wait Timeout in seconds |
| X_VBC | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ValidBitCount: reg_sz | | Valid Bit Count comma delimited list |
| X_PIBCM | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>InvalidBitCountMessage: reg_sz | | Message to display to user when their card has an invalid bit count |
| X_PIFM | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>InvalidFacilityMessage: reg_sz | | Message to display to user when their card has an invalid facility code |
| X_PIPM | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>InvalidParityMessage: reg_sz | | Message to display to user when their card has an invalid parity calculation |
| X_PIRM | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>InvalidRangeMessage: reg_sz | | Message to display to user when their card has an ID that is not in a valid range |
| X_PSEDM | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>SelfEnrollmentDisabledMessage: reg_sz | | Message to display to user when prox card self enrollment has been disabled |
| X_PSDM | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ServerDownMessage: reg_sz | | Message to display to the user when the server cannot be contacted |
| X_PIN_AT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>PIN_Auth_Title: reg_sz | AUTHENTICATION | Title of message to prompt user for PIN Authentication |
| X_PIN_ET | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>PIN_Enroll_Title: reg_sz | ENROLLMENT | Title of message to prompt user for PIN Enrollment |
| X_CPT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>PIN_Change_Message: reg_sz | Change my PIN | Message to prompt user for manually changing their PIN |
| X_BMML | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BadgeMsg_ManualLogin: reg_sz | Enter username and password | Message to prompt user for manual login when prox reader is not attached |
| X_BMUA | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BadgeMsg_UnAuthenticated: reg_sz | Enter your password | Message to prompt user their badge is not authenticated and a password is required |
| X_BMUR | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BadgeMsg_Unregistered: reg_sz | Enter username and password to register badge. | Message to prompt the user for badge enrollment (the card is not registered) |
| X_PX_RB | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>CardRequiredForLogin: reg_dword | 0 | Require Proxcard for Login enabled(1) or disabled(0) |

| | | | | |
|---|---|---|---|---|
| | | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>HWGConfig: reg_sz | | The full path and filename to an HWG+ formatted configuration file that will be used to configure the proximity card reader device.<br><br>Warning: Setting this file path overrides all other prox card device configuration settings as specified in the registry, as well as those that are built into the product. This includes Parity Strip count, Reader Beep, MessageValidForMS, and potentially ValidBitCount settings. Use caution when using this method to configure devices, and ensure proper operation before distribution. |
| X_PSWT | | HKEY_LOCAL_MACHINE\Software\HealthCast\ProxCardClient<br>ServcieStartupConnectionWaitTimeout: reg_dword | 30 | This setting indicates how long to wait during a startup phase to ignore server/network availability errors before reporting a problem to the HealthCast client. |
| | | HKEY_LOCAL_MACHINE\Software\HealthCast\ProxCardClient<br>ReaderBeepEnabled: reg_dword | | Indicates if using a RFIdeas reader model that includes an internal speaker, that tapping a badge the reader will beep indicating the badge was read. |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>ConnectionTimeout: reg_dword | 1 | The time in seconds that the client will attempt to connect to the all of the configured servers before returning an error to the client for a connection failure. |
| | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BeepSoundFile: reg_sz | <install folder path>\beep2.wav | The default WAV file that will play when a card is tapped, and the setting to play beep sound is enabled |
| X_BEEP | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ProxCardClient<br>BeepSoundPlayOnBadgeTap: reg_dword | 0 | Beep sound is enabled to play when set to 1, disabled when set to 0 |

**REMOTE AUTHENTICATION SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| X_RA_PORT | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>SocketPort: reg_dword | 20000 | Communications port for Remote Authentication |
| | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory\INDY<br>EnabledServerIDs: reg_sz | | Enabled Servers List. Comma delimited list of server identifiers 0000,0001,0002, etc. |
| X_RAEC | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory<br>Encryption: reg_sz | NONE | Encryption Class: (Only if communicating with a server Advanced Communications port: 20001)<br>RIJNDAEL, RIJNDAEL128, RIJNDAEL256, BLOWFISH, BLOWFISH256, TWOFISH, SERPENT<br>If communicating with the Compatibility communication port: 20000, this setting MUST match the configuration on the server:<br>RIJNDAEL, BLOWFISH |
| X_RACC | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory<br>Compression: reg_sz | VCLZIP | Compression Class:<br>NONE, VCLZIP<br>If communicating with the Compatibility communication port: 20000, this setting MUST match the configuration on the server:<br>NONE, VCLZIP |
| X_RARL | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory<br>RemoteLogon: reg_dword | 1 | Remote Authentication Enabled (1) or Disabled (0) |
| X_RAID | KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCCitrixSessionDirectory<br>ID: reg_sz | EA12G54 | Remote Authentication Shared Key for legacy communications<br>If communicating with the Compatibility communication port: 20000, this setting MUST match the configuration on the server |

**AUDIT CLIENT SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>SocketPort: reg_dword | 25000 | Communications port for Proxcard Server |

| | | | | |
|---|---|---|---|---|
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>EnabledServerIDs: reg_sz | 0 | Enabled Servers List. Comma delimited list of server identifiers 0000,0001,0002, etc. |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>EncryptionClass: reg_sz | NONE | Encryption Class:<br>RIJNDAEL, RIJNDAEL128, RIJNDAEL256, BLOWFISH, BLOWFISH256, TWOFISH, SERPENT |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\AuditServerClient\Connection\INDY<br>CompressionClass: reg_sz | VCLZIP | Compression Class:<br>NONE, VCLZIP |

**HCIDeploy CLIENT SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| X_D_PORT | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>Port: reg_dword | 26000 | Communications port for HCIDeploy |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>EnabledServerIDs: reg_sz | | Enabled Servers List. Comma delimited list of server identifiers 0000,0001,0002, etc. |
| X_D_EC | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>EncryptionClass: reg_sz | RIJNDAEL | Encryption Class:<br>RIJNDAEL, RIJNDAEL128, RIJNDAEL256, BLOWFISH, BLOWFISH256, TWOFISH, SERPENT |
| X_D_CC | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>CompressionClass: reg_sz | VCLZIP | Compression Class:<br>NONE, VCLZIP |
| X_D_PORT_CRM | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>ClientPort: reg_dword | 26100 | Communications port for HCIDeploy remote management |
| X_D_GRPS | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient<br>DefaultGroups: reg_sz | | Default Locations the workstation should be registered in. (When the service starts, it will register these location names, then remove the setting) |
| X_D_RM | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>EnableRemoteManagement: reg_dword | 1 | Enable(1) or Disabled(0) management port. If this setting is disabled, the HCIDeploy Console will not be able to display the deployed package state on the workstation |
| X_D_HID | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>ConfiguredHashID: reg_sz | {A439AF92-98CD-4C20-83AC-5FD12308F51A} | Indicates the communications hash ID the remote management listening port requires for encryption handshake:<br>MD5 (128 bit) GUID: {A439AF92-98CD-4C20-83AC-5FD12308F51A}<br>WHIRLPOOL (512 bit) GUID: {C86DDD9B-09B2-4360-878B-F5D3B6997CDE} |
| X_D_SCH | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Schedule<br>Schedule: reg_sz | | Schedule information string indicates how often the client will check in with the server to determine if a package update or uninstall is needed on the workstation |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\HCIDeployClient\Indy<br>ConnectionTimeout: reg_dword | 1 | The time in seconds that the client will attempt to connect to the all of the configured servers before returning an error to the client for a connection failure. |

**MISCELLANEOUS SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| XA_N_BREQ | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\Identity Automation\XANotification<br><br>BindingRequest: reg_sz | tcp://127.0.0.1:6226 | The port specified 6226 can be adjusted if necessary.<br><br>NOTE: The Windows (or other) Firewall may also need to be adjusted to allow network communication on this port for proper communication on the local machine between the XA client and the Browser Plug-in. The port must match what is used in XA_N_BRESP. |

| | | | | |
|---|---|---|---|---|
| XA_N_BRESP | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\Identity Automation\XANotification<br><br>BindingResponse: reg_sz | tcp://localhost:6226 | The port specified 6226 can be adjusted if necessary.<br><br>NOTE: The Windows (or other) firewall may also need to be adjusted to allow network communication on this port for proper communication on the local machine between the XA client and the Browser Plug-in. The port must match what is used in XA_N_BREQ. |
| XA_ALE | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>AutoLogoffEnabled: reg_dword | 1 | Enables (1) or Disables (0) idle session logoff. Logoff only occurs after the session has locked. |
| X_KM_AL_TIME | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>LogoffTimeLimit: reg_dword | 600 | The number of seconds the session can be idle (locked) before the session will be logged off. |
| X_KM_LTL | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>LockTimeLimit: reg_dword | 300 | The number of seconds a session can be idle before the session is automatically locked |
| X_PRA | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\PasswordReset<br>URL: reg_sz | | Password Reset URL to a web site than allows a user to reset their domain password (such as ADPWR) |
| X_ACT | SUM,KM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\PasswordReset<br>AutoCancelTime: reg_dword | 120 | The auto cancel time for inactivity of the password reset web display in seconds. |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>ShowXAStatusMessages: reg_dword | 1 | When Enabled (1) Allows XAUCM to display the status message during startup, show desktop, and shutdown. These status messages will not be shown when Disabled (0) |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>SkipLoadingAppList: reg_dword | | When Enabled (1) Indicates that XA should not load the application list during login to improve performance. When Disabled (0), XA will load the users application list from the server.<br><br>This setting is required to be Disabled (0) if the user will launch SnapApp enabled applications (either Windows or Web) on the system where the setting is set.<br><br>Also, if the ExactAccess Desktop will be displaying applications on the workstation, this setting must be Disabled (0) so the users authorized applications will be loaded for presentation.<br><br>Not all workstations require this setting to be disabled - for instance, in a Published Application scenario, this setting can be enabled on the RSM server if the user will launch WebSSO or Windows SnapAPP applications on their local workstation and use published connectors for applications on the RSM server.<br><br>This setting can also be Enabled (1) when using the Kiosk Mode Passthrough configuration, as the desktop presentation will be handled by an RSM or VDI desktop (remote session), so the local workstation does not need to retrieve the application list. |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>BeepBeforeLockEnabled: reg_dword | 32 | Enables (1) or Disables (0) a system beep during the about to lock countdown |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>LockBeepIntervalInSeconds: reg_dword | | This value is how many seconds occur between each beep during the countdown before lock. |
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>LockBeepStartTimeInSeconds: reg_dword | | This value is how many seconds before lock does the beep notice start to occur. It also indicates when the visual status will indicate the system is about to lock. |

| | | | | |
|---|---|---|---|---|
| | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>LockBeepIndex: reg_dword | 32 | May be one of the following values<br><br>0 - play sound associated with Default Beep sound in the Sound Scheme 16 - play sound associated with Critical Stop sound in the Sound Scheme<br><br>32 - play sound associated with Question sound in the Sound Scheme<br><br>48 - play sound associated with Exclamation sound in the Sound Scheme<br><br>64 - play sound associated with Asterisk sound in the Sound Scheme<br><br>4294967295 - use PC Speaker beep instead of scheme sound<br><br>Note that the user may not have a .WAV file associated with the Sound Scheme values listed. Verify with the Sound Scheme that each of the items identified is associated with a .WAV file.<br><br>These values can be found under:<br>HKEY_CURRENT_USER \AppEvents \Schemes \Apps \<Type> \.Current -- (Default)<br><br>Where <Type> is one of the following values:<br>.Default, SystemHand, SystemQuestion, SystemExclamation, SystemAsterisk |
| X_LDM | ALL | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>KMLockDisplayMode: reg_dword | 5 | Change how the user name is displayed in the Active User List, Privacy Shield, and the XA Desktop<br><br>0 - Full Name*<br>1 - Last Name only<br>2 - First Name Only<br>3 - Directory Service Name **<br>4 - Initials Only<br>5 - First Name, Last Initial<br>6 - First Initial, Last Name<br>7 - "In use" only **<br>8 - No user name display **<br><br>Warning<br>* Full Name is the First + Last, or Display Name field, depending on how the server is configured.<br><br>Warning<br>** In Passthrough configuration, only values 3,7,8 are valid.<br>** Optionally, in Kiosk Mode, The user name can be removed from the privacy shield with the PSLoginNameVisible setting (allowing the name to remain showing on the XA Desktop) |
| | ALL | HKLM\Software\HealthCast\ExactAccess\Override<br>LogoffOnDesktopClose: reg_dword | | Enables (1) or Disables (0) initiating logoff if the user closes the Application Desktop (not valid for Toolbar Desktop) |
| | ALL | HKLM\Software\HealthCast\ExactAccess\Override<br>ShowDesktopOnLogoffCancel: reg_dword | | Enables (1) or Disables (0) initiating re-launching the XA Application Desktop (not valid for Toolbar Desktop) if the user cancels logoff |
| | ALL | HKLM\Software\HealthCast\ExactAccess\Display<br>DesktopStyle: reg_sz | hcgreen.vsf | The visual style file applied to change the look and feel of the XA Toolbar Desktop (not valid for Application Desktop). |

| | | | | |
|---|---|---|---|---|
| XA_DSK_CLASS | ALL | HKLM\Software\HealthCast\ExactAccess\XAServerManager<br>Desktop: reg_sz | AppDesktop.clsAppDesktop | AppDesktop.clsAppDesktop: also referred to as Application Desktop, launches an application window similar to a web page that lists the user's SSO enabled applications as well as "lock" and "logoff" buttons.<br><br>**NoDesk.clsNoDesk**: also referred to a No Desktop, does not launch an XA Desktop when XA is started.<br><br>**xatbdesk.clsxatbdesk**: also referred to as Toolbar Desktop allows for the XA Menu to appear as a popup/context menu from the XA Taskbar icon. Additionally, a secondary application can be launched that looks and acts like the standard Windows task/start bar in that it will display favorite applications and has a start button to display a popup menu of applications with a work space similar to Windows 10.<br><br>**HCCitrixDesk.clsDesktop** is a specialized desktop presentation used when the same Citrix server publishes a full Windows desktop and the user should see an XA menu of SSO enabled applications. The same Citrix server may also be used to publish xa directly but have the nodesktop option so an xa desktop does not appear.<br><br>**Required**: When using the XATBDesk.clsXATBDesk class, it is necessary that the DESKTOP_SERVER.XML be registered with the XA server before it will function.<br><br>See **Registering application XML files** in the **ExactAccess Administrator**. |
| | All | HKLM\Software\HealthCast\ExactAccess\XAServerManager<br>ClientDSProgID | Note<br>This setting must be manually updated after an installation on RSM to use the virtual channel class to retrieve the current XA user from the end point device. Using the Client Configuration tool may reset this value when saving settings.<br><br>Warning<br>This setting may not be set during the install or with a transform. | Class that determines where the user identification is retrieved from.<br>NTClientDSUser.clsNTClientDSUser (SUM,RSM,VDI)<br>hciVCCred.clshciVCCred (RSM ONLY)<br>NTKMDSUser.clsNTKMDSUser (KIOSK ONLY) |
| X_ALA_CHK | ALL | HKLM\Software\HealthCast\ExactAccess\AutoLaunch<br>CheckAccess: reg_dword | 0 | This setting determines whether an access check should be performed before the application is auto-launched. If the value is set to zero (0), the application will be launched and is not required to be registered in XA. The user logging in does not have to be granted access to launch the application. If the value is set to one (1), the application must be registered in XA and the user must belong to a role that has been granted access to the application. |
| X_ALA_PATH | ALL | HKLM\Software\HealthCast\ExactAccess\AutoLaunch<br>Launch: reg_sz | | |

**STANDARD-MODE SPECIFIC MISCELLANEOUS SETTINGS**

| Parameter Name | Applicable Modes | Registry Keys Affected | Value | Setting Description |
|---|---|---|---|---|
| X_AULV | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings<br>ActiveUserListVisible: reg_dword | 0 | Enables (1) or Disables (0) the Standard Mode Active User List display that shows the active ExactAccess Sessions/Users on the workstation |

| | | | | |
|---|---|---|---|---|
| X_LS | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings LimitSessions: reg_dword | 1 | Limit sessions to a single session with tap-over supported<br>0=session limit disabled (unlimited number allowed)<br>1 or more=session limit enabled with define number allowed |
| X_DTO | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings SingleUserOnly: reg_dword | 0 | Enalbles (1) or Diables (0) Single User only operation. Tap-Over is disabled when this setting is enabled. The session locks rather than disconnecting when this setting is enabled. |
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.PasswordResetEnabled: reg_dword | | Enables (1) or Disables (0) Password reset link on the login tile. Requires the password reset URL also be configured. |
| X_QSA | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.STATUS_ALIGNMENT: reg_dword | 1 | Proximity card dialog alignment<br>0=Left<br>1=Center<br>2=Right<br>3=Absolute Position (use X_QSX, X_QSY to specify position) |
| X_QSBC | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.STATUS_BACK_COLOR: reg_dword | 11430670 (AE6B0E) — blue | Credential Provider Dialog Background Color<br>Color is specified in the following format: NBGR (none,blue, green,red values from left to right 00, BB, GG, RR) |
| X_QSFC | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.STATUS_FONT_COLOR: reg_dword | 16777215 (FFFFFF) — white | Credential Provider Dialog Font Color<br>Color is specified in the following format: NBGR (none,blue, green,red values from left to right 00, BB, GG, RR) |
| X_QSX | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.STATUS_XPOS: reg_dword | 0 | Status Dialog Absolute X (horizontal) position |
| X_QSY | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.STATUS_YPOS: reg_dword | 0 | Status Dialog Absolute Y (vertical) position |
| X_QULF | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USER_LIST_FONT_NAME: reg_sz | Tahoma | Active User List Font Name |
| X_QULA | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USERLIST_ALIGNMENT: reg_dword | 1 | Active User List Dialog Alignment<br>0=Top<br>1=Center<br>2=Bottom<br>3=Absolute Position (use X_QULX, X_QULY to specify position) |
| X_QULFC | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USERLIST_FONT_COLOR: reg_sz | 16094997 (F59715) — blue | Active User List Item Font Color<br>Color is specified in the following format: NBGR (none,blue, green,red values from left to right 00, BB, GG, RR) |
| X_QULFS | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USERLIST_FONT_SIZE: reg_sz | 28 (1C) | Active User List Item Font Size |
| X_QULX | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USERLIST_XPOS: reg_sz | 0 | Active User List Dialog Absolute X (horizontal) position |
| X_QULY | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.USERLIST_YPOS: reg_sz | 0 | Active User List Dialog Absolute Y (verticle) position |
| X_QASE | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.MSG.SELFENROLLDISABLED: reg_dword | 0 | Disables (1) or Enables (0) Prox Card Self Enrollment for Standard Mode |
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess\QAW\Settings QAW.TRANSPARENT_BACKGROUND: reg_dword | 1 | Enables (1) or Disables (0) transparency effects for the Status Dialog |
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess BeepBeforeAutoLogoffEnabled: reg_dword | | |
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess AutoLogoffBeepIntervalInSeconds: reg_dword | | |
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess AutoLogoffBeepStartTimeInSeconds: reg_dword | | |

| | | | | |
|---|---|---|---|---|
| | SUM | HKEY_LOCAL_MACHINE\SOFTWARE\HealthCast\ExactAccess<br>AutoLogoffBeepIndex: reg_dword | 32 | May be one of the following values:<br><br>0 - play sound associated with Default Beep sound in the Sound Scheme 16 - play sound associated with Critical Stop sound in the Sound Scheme<br>32 - play sound associated with Question sound in the Sound Scheme<br>48 - play sound associated with Exclamation sound in the Sound Scheme<br>64 - play sound associated with Asterisk sound in the Sound Scheme<br>4294967295 - use PC Speaker beep instead of scheme sound<br><br>Note that the user may not have a .WAV file associated with the Sound Scheme values listed. Verify with the Sound Scheme that each of the items identified is associated with a .WAV file.<br><br>These values can be found under:<br>HKEY_CURRENT_USER \AppEvents \Schemes \Apps \<Type> \.Current -- (Default)<br><br>Where <Type> is one of the following values:<br>.Default, SystemHand, SystemQuestion, SystemExclamation, SystemAsterisk |
| | SUM | HKEY_LOCAL_MACHINE\Software\HealthCast\ExactAccess\cache<br>isCacheEnabled: reg_dword | 0 | Enables (1) or Disables (0) local credential caching |