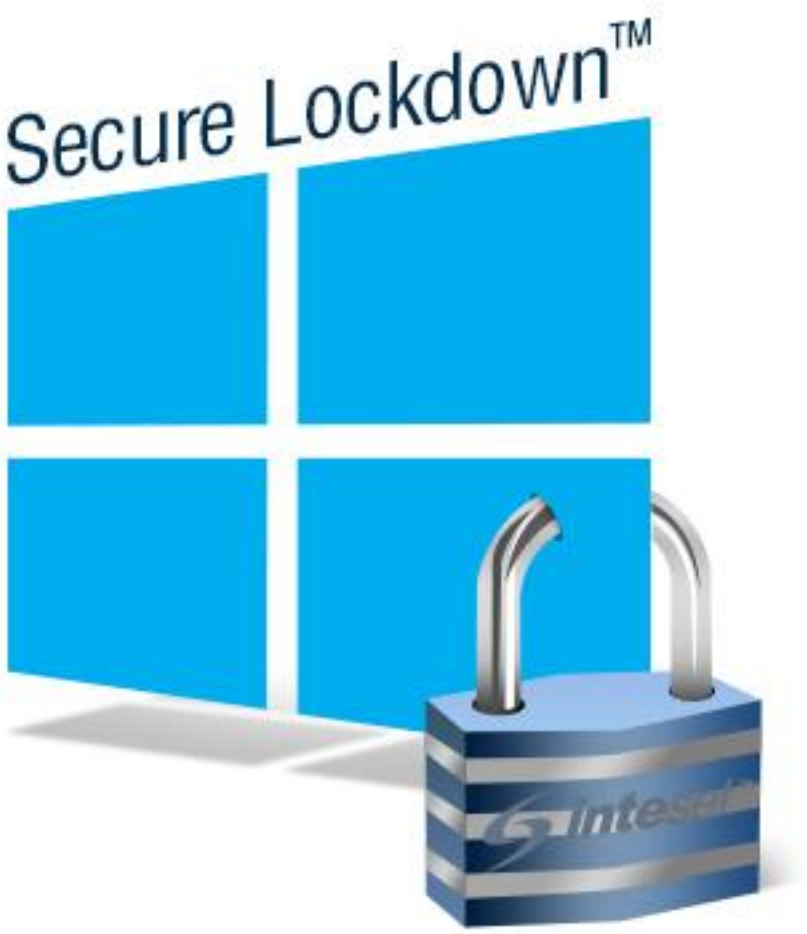
Inteset Secure Lockdown™ ver. 2.0

for

Windows 7, 8, 10



Administrator Guide

Table of Contents

Thank You!

As a bulk purchaser of Secure Lockdown v2, Inteset thanks you for your extremely valued business! Along with your bulk purchase, you will receive premium support. We will assist you in your Secure Lockdown unattended or OS image installation setup via phone or email support and provide you with the tools necessary allowing a smooth and successful installation.

Administrative Tools and Procedures

Below describes the tools and procedures available and how to use them. This includes:

- an automatic password generation utility
- the ability to copy Secure Lockdown configuration settings from one system to another
- the ability to temporarily disable the application installation lockdown feature
- hidden administrative Secure Lockdown features
- command-line abilities to export/import settings and enable/disable Secure Lockdown
- a procedure to build an OS image integrating Secure Lockdown

Note: This document corresponds with Secure Lockdown version **2.00.203** or greater. Please be sure that you are running this version before proceeding. The version information of Secure Lockdown can be found in the *Help* > *About* tab of the Secure Lockdown configuration utility.

Automatic Password Generation

Secure Lockdown should be set up to require a password in order to access its configuration screens. In unattended or OS Image installations, it may be necessary to generate passwords based on an algorithm that can be determined by the administrator. Inteset has created a password generation tool for this purpose. This utility is a command line executable file called "SLPasswordGenerator.exe" and is useful for creating passwords based on a defined prefix and the system's serial number. If you would like to obtain this tool, contact Inteset Technical Support via email @ techsupport@inteset.com.

Application Installation Guard Utility

When enabled, Secure Lockdown can be set to block application installation. The setting ("No App Install") to do this is found under the System Lockdown/Machine Level tab. In some cases, it may be necessary to periodically make automated, scheduled updates to the system. For example, you may want to run Windows Updates or antivirus definition updates. If the "No App Install" option is enabled, these updates will not be possible. To facilitate automated and scheduled updates while Secure Lockdown is enabled and while the "No App Install" option is enabled, Inteset has created a simple command line utility called "AppInstGrd.exe" that will allow you to temporarily disable the app installation lock, then enable it again once the updates are completed. This utility can be found in the program folder of Secure Lockdown. It is typically run using the Windows Task Scheduler along with the "Run with highest privileges…" and the "Run only when user is logged on" settings. The task is typically scheduled to run (with the *allow* parameter) just previous to performing updates, then run again (with the *disallow* parameter) just after the updates are installed successfully.

Below is the syntax used in the command line:

Usage:
AppInstGrd <installState>

Parameters:
If no parameter is specified, when run, the App Installation Guard utility (AppInstGrd.exe) by default will set Secure Lockdown to *allow* installations.

<*InstallState*> - The desired lock state of application installations. Valid entries for this parameter are none (allow) “allow” or “disallow”.

Examples:
1. “C:\Program Files\Inteset\Secure Lockdown\ AppInstGrd.exe” allow

Note: If there are any errors, they will be reported within the Windows Application Event Log under the "Secure Lockdown" source.

Keep Application On Top Utility

In some cases, Secure Lockdown implementations may require ancillary applications such a calculator, virtual keyboard, power meter, or other programs to always be available and visible to the user. The *Keep Application On Top* utility provides the ability to ensure an application is always started and on top of all other windows. This command line utility is included with Secure Lockdown and is found in the Secure Lockdown program folder (ie: “KeepAppOnTop.exe”). It can be started via the Secure Lockdown Background Apps feature, the Windows Task Scheduler, a script, or manually.

Below is the syntax used in the command line:

Usage:
KeepAppOnTop <ProcessName> <IntervalSeconds>

Parameters:
<*ProcessName*> (required) - The name of the process that is to be monitored. Process names can be found in the Windows Task Manager under the Processes tab and are typically the name of the application’s executable file (without the extension).

<*IntervalSeconds*> (optional) - The amount of time that passes where the Keep App On Top utility checks that the specified process is started and on top of all other windows.

Example:
1. “C:\Program Files\Inteset\Secure Lockdown\KeepAppOnTop.exe” calc 3

The above example command line will monitor the Windows Calculator process every 3 seconds.

Note: The application (process) must be started before it can be monitored.

Note: This utility will not work properly with applications that spawn multiple processes such as the Internet Explorer or Chrome browsers.

Note: This utility will not work properly if the same process is running under a different user account than the current one (it is not user aware).

Hidden Secure Lockdown Features

Based on requests from users, several hidden features are available to implement when Secure Lockdown is enabled. The hidden features can be activated by creating Windows Registry entries under the "HKEY_CURRENT_USER\Software\Inteset\SecureLockdown_v2" key. Options available are:

Master Process Exit Delay (applies to *Secure Lockdown – Standard Edition* only) – Typically, a "Master Application" remains open (ie: a kiosk application) indefinitely, or until the user closes it. Secure Lockdown immediately monitors if the application exits once it is started. If the application exits as soon or shortly after it starts, this indicates that the specified master application is likely an application launching program (ie: a batch file or script) that is run for a very short period and not the program that is intended to be monitored by Secure Lockdown. If the Master Application tab/*Keep Running* feature of Secure Lockdown is enabled, by default, Secure Lockdown will disable it automatically because it cannot monitor a program that exits immediately. However, sometimes it is necessary to use a "launching program" (script) as the master application. If this is the case, after Secure Lockdown starts the launching program, it is necessary to indicate how long Secure Lockdown should wait before it considers it to be a launching mechanism and not the monitored process.

The "Master Process Exit Delay" setting should be used if the launching program takes longer than 200 milliseconds (default) to run, then exit. The specified delay time should be somewhat longer than the launching program takes to run, then exit. Also, if the specified master application is a launching program, and you want to monitor a process that is launched by the launching program, you will need to specify that process in the Master Application tab/*Process Name* field. This process will be monitored if the *Keep Running* feature is enabled.

To change the time interval to a value other than 200 milliseconds, add the registry DWORD key value "MasterProcessExitDelay= <milliseconds>". Note that the data value is in milliseconds (ie: 1 second = 1000 milliseconds.)

Keep Running Start Interval – If the Master Application/*Keep Running* option is enabled, Secure Lockdown will automatically restart the Master Application when it is closed. There is a time interval as to how often Secure Lockdown checks if the master application is running. By default, it checks every 10 seconds. To change the time interval to a value other than 10 seconds, add the registry DWORD key value "KeepRunningStartInterval= <milliseconds>". Note that the data value is in milliseconds (ie: 1 second = 1000 milliseconds.) The minimum value is 2000 milliseconds.

Note: this feature does not apply to *Secure Lockdown – Multi-application Edition*

Lock Workstation – To enable the "Lock Workstation" feature of Windows which is disabled by Secure Lockdown by default, add the registry DWORD key value "DisableLockWorkstation = 1".

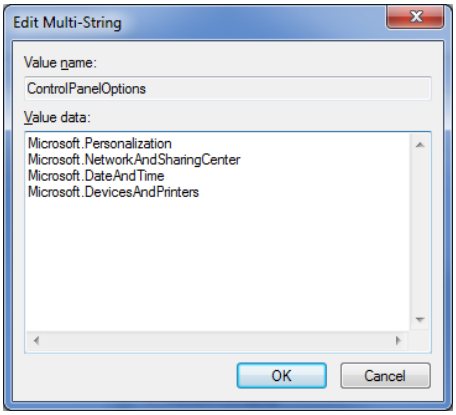
Enable Change Password – To enable the "Change a password" feature of the Windows CTRL-ALT-DELETE screen, add the registry DWORD key value "EnableChangePassword = 1".

Enable Task Manager – By default, Secure Lockdown prevents access to the Windows Task Manager. To allow access to the Task Manager and its accompanying applications, add the registry DWORD key value

"EnableTaskManager = 1". The Task Manager ("C:\Windows\System32\taskmgr.exe") can be started via the Background Apps feature of Secure Lockdown.

Enable Control Panel – By default, Secure Lockdown prevents access to the Windows Control Panel. To allow access to the Control Panel and its accompanying applications, add the registry DWORD key value "EnableControlPanel = 1". Note that many features of the Control Panel will still be disabled by Secure Lockdown. In addition, to allow access to certain Control Panel functions, the options needed must be specified. See the "Control Panel Options" setting below.

Control Panel Options - By default, Secure Lockdown disables access to the Windows Control Panel and all of its features. Using a "hidden" Secure Lockdown setting (see above "Enable Control Panel" option), the Control Panel can be enabled while the system is locked down. While it's enabled and as a security precaution, no options are available to select in the Control Panel screen. In order to enable a specific Control Panel option, it must be specified in a Secure Lockdown specific Windows registry setting. Add the **Multi-String** registry key value name of "ControlPanelOptions". Then add the Control Panel options needed based on the well known "Canonical Names" to the key data. Canonical names are listed and described on the following Microsoft web page: http://msdn.microsoft.com/en-us/library/windows/desktop/ee330741(v=vs.85).aspx



Enable Management Console - By default Secure Lockdown restricts access to Windows Management Console apps. To allow access to any Management Console snap-in (*.msc), add the registry DWORD key value "EnableManagementConsole= 1".

Enable Command Prompt - By default Secure Lockdown restricts access to the Windows Command Prompt. To allow access to the Command Prompt, add the registry DWORD key value "EnableCommandPrompt= 1".

Enable Registry Editor - By default Secure Lockdown restricts access to Windows Registry Editor. To allow access to the Windows Registry Editor, add the registry DWORD key value "EnableRegEdit= 1".

Enable Explorer Command Bar - By default Secure Lockdown removes the Explorer Command Bar (menu bar) that appears at the top of Windows Explorer. To display the Explorer Command Bar, add the registry DWORD key value "EnableExplorerCommandBar= 1".

Enable Explorer Navigation Pane - By default Secure Lockdown removes the Explorer Navigation Pane that appears at the left side of the Explorer Window and displays Library folders and Network locations. To display the Explorer Navigation Pane, add the registry DWORD key value "EnableExplorerNavigationPane= 1".

Ignore Physical Keyboard Check – To prevent Secure Lockdown from doing a physical keyboard scan, add the registry DWORD key value "IgnorePhysicalKeyboardCheck= 1". This may be desirable if you're using a tablet or touch device, but do not want to display the "No physical keyboard…" warning message when enabling Secure Lockdown.

Master App Pause - To pause (temporarily close) your Master Application, add the registry DWORD key value "MasterAppPause= 1". To restart the Master Application, delete this key name, or set the value equal to “0”. This feature can be useful if you have a process that updates your Master Application software and requires that the app be closed for the update to occur. This feature is most commonly used with *Secure Lockdown - Standard Edition*.

Disable Block System Keys – To prevent Secure Lockdown from blocking Windows system and various Internet Explorer key sequences, add the registry DWORD key value "DisableBlockKeys= 1". This may be desirable if you’re using a tablet or touch device, where the system’s touch functionality does not work properly. This is the case due to driver conflicts with this Secure Lockdown functionality. Inteset has found that some Windows 7 touch devices have this issue.

Disable Password Attempts – If you’d like to disable password attempts after a certain number of tries, add the registry DWORD key name "PasswordDisableMinutes". Set the value (Decimal) to the number of minutes you’d like to delay the ability to enter passwords. This feature will disable the *Password* field and *Unlock* button for the specified minutes before allowing passwords to be entered again. To increase or decrease the default number of allowed password entry attempts (3), add the registry DWORD key name "PasswordAttemptAllowances". Set the value (Decimal) to the number of attempts you’d like to allow. This feature works only when Secure Lockdown is enabled.

Disable Secure Lockdown Hotkey – In some cases, when Secure Lockdown is enabled, it may be desired to prevent the *Alt+Shift+S* hotkey from invoking the Secure Lockdown utility. If so, you can remove the feature by add the registry DWORD key value "DisableSLHotkey= 1". Note that if this feature is enabled, you will not be able to disable Secure Lockdown unless you have either set up a second Windows administrator account on the system, or you have registered the system with the *Inteset Remote Management Services* which has an *Enable/*D*isable Secure Lockdown* feature. If you choose to use the 2nd administrator account as the method to disable Secure Lockdown (see *Disable Secure Lockdown from 2nd Admin Account* feature below), be sure that the 2nd admin account is accessible when Secure Lockdown is enabled by ensuring the following:

- The *Windows Auto Login* feature, if used, can be interrupted so that you can gain access to the second admin account (the method to do this differs between Windows OSs). Or…
- The Secure Lockdown > System Lockdown > Machine Level > No User Switching option is disabled. And…
- The Secure Lockdown > System Lockdown > Machine Level > No Ctrl+Alt+Del option is disabled

Before enabling this feature, be sure to test the above setup.

Disable Secure Lockdown from 2nd Admin Account – If you want to disable Secure Lockdown from a 2nd Windows Administrator account on the locked down system, add the “HKEY_LOCAL_MACHINE \Software\Inteset\SecureLockdown_v2” Windows Registry String Value (REG_SZ) of "SLCommandVerb=disable_secure_lockdown”. Once added, the next time a user logs into the locked down account. Secure Lockdown will disable itself and reboot the computer.

Chrome Custom Command Line Switch – Chrome accommodates many command line switches that are responsible for an array of functionality. Secure Lockdown – Chrome Edition allows you to add any

custom switch which will be applied when Secure Lockdown runs Chrome. Add the "CustomSwitches" Windows Registry String Value (REG_SZ) key name, to the "HKEY_CURRENT_USER\Software\Inteset\SecureLockdown_v2_CM\ChromeLockdownOpts" key, then enter a Chrome command line switch(es) into the Value Data field.

Note: this feature applies to *Secure Lockdown – Chrome Edition* only.

Remove Branding – To remove all Inteset branding and system information found in the *Help > About* dialog, add the registry DWORD key value "RemoveBranding= 1". This feature applies when Secure Lockdown is enabled.

Enable Alternative Hotkey – The Secure Lockdown utility is hidden in the background when it's enabled. To reveal it, an administrator must press the "Alt+Shift+S" keyboard sequence. In some cases is may be necessary to use an alternative hotkey. To use the alternative hotkey, add the one of the following registry DWORD key values:

Option 1: "EnableAlternateHotkey"= 1" (use "Alt+F9" key sequence)
Option 2: "EnableAlternateHotkey"= 2" (use "F9" key)

International Keyboard Support – Many international keyboards possess an "AltGr" key. It is used in combination with other keys to produce special characters. To enable the "AltGr" key, add the registry DWORD key value "InternationalKB= 1".

Enable Modify Printers – To enable the ability to add and remove printers, including network printers, add the registry DWORD key value "EnableModifyPrinters= 1".

Enable Microsoft Edge (applies to *Secure Lockdown – Multi-applicationEdition* only) – To enable the ability to use the Microsoft Edge browser, add the registry DWORD key value "EnableMicrosoftEdge= 1".

Enable User OS Drive Access – To enable the ability for users to access the OS drive (typically "C"), add the registry DWORD key value "EnableUserOSDriveAccess= 1". Note that the "C" drive will not be visible in Windows *Open* and *Save* dialogs, but it will still be accessible by typing the path in the address bar. This feature is not recommended and should be avoided if possible. It can safely be used if users have no interface (ie: Open, Save dialog) to the file system.

Using the Command Line

Secure Lockdown has the ability to be enabled and disabled from a command line. In addition, the settings can be exported and imported from a command line. Common uses for this feature might include enabling or disabling Secure Lockdown or changing its settings through a script or from remote administration. It is also useful during bulk or OS image installations. Below is the syntax used in the command line:

Enable or Disable

Usage:
IntesetSecureLockdownV2 <command> <password> <logoff>

Parameters:
< *command*> (required) – the desired lockdown state of Secure Lockdown (ie: enabled or disabled). Valid entries for this parameter are “enabled” or “disabled”

<*password*> (required) – the password to access Secure Lockdown. If there is no password, use quotes (“”) to specify an empty password

<*logoff*> (optional) – to enable or disable Secure Lockdown completely, you must either log out of Windows or restart the computer. By default, if this parameter is not included, the system will restart. If you wish to log out of Windows instead, specify “logoff” for this parameter. Note, if you specify this parameter, you must specify the password parameter even if there is no password. In this case, use quotes (“”) to specify an empty password.

Examples:
1. “C:\Program Files\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe” enable
2. “C:\Program Files\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe” disable mypassword
3. “C:\Program Files\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe” enable “” logoff

Note: if an error occurs (ie: the password is invalid), Secure Lockdown will launch in normal mode. If another instance of Secure Lockdown is already running, the second instance will terminate. All errors are reported in the Windows Application Event log.

Export or Import

Usage:
IntesetSecureLockdownV2 <command> <file path> <logoff>

Parameters:
< *command*> (required) – enter whether or not to import or export Secure Lockdown settings. Valid entries for this parameter are “export” or “import”.

Note: Performing an import from the command line will either restart the computer, or log out of the Windows account depending on the *Logoff* parameter specified (see below). Performing an export does not require a system restart or log off. Either command can be performed when Secure Lockdown is enabled or disabled.

<*file path*> (required) – the file path and name of the file to export or import Secure Lockdown settings. If the file path has a space, the *file path* parameter must be wrapped in quotes (“”). The file name should have a “.bac” extension.

<*logoff*> (optional) – to import Secure Lockdown settings, you must either log out of Windows or restart the computer. By default, if this parameter is not included, the system will restart. If you wish to log out of Windows instead, specify “logoff” for this parameter.

Examples:
1. “C:\Program Files\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe” export “c:\program files\inteset\secure lockdown\securelockdown_v2_settings.bac”

2. “C:\Program Files\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe” import “c:\program files\inteset\secure lockdown\securelockdown_v2_settings.bac” logoff

Note: All errors are reported in the Windows Application Event log.

Copying Secure Lockdown Configuration Settings to Other Computers

If you’re setting up multiple computers with the same settings, you can accumulate these settings and apply them across the other computers saving time and effort. Below are the different areas of settings related to Secure Lockdown.

Secure Lockdown Settings

Secure Lockdown settings, can be exported and imported via command line. Please see the above section regarding command-line options.

Internet Explorer Settings

If you’re using *Secure Lockdown – Multi Application Edition* or *Internet Explorer Edition*, you may want to copy the following specific Internet Explorer cache, history, favorites, and cookies items that are stored here:

Cache – c:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer
History - c:\Users\<username>\AppData\Local\Microsoft\Windows\History
Favorites - c:\Users\<username>\Favorites
Cookies - c:\Users\<username>\AppData\Roaming\Microsoft\Windows\Cookies

These files can be moved and copied to the matching location on the other computers.

Circle Dock

If you’re using *Secure Lockdown – Multi Application Edition* and the Circle Dock functionality, make the needed adjustments to Circle Dock, then copy the Circle Dock “.ini” files found in the following folder to the other computers:

“C:\Program Files\Inteset\Secure Lockdown\CircleDock\System\Settings\”

Note: The programs and their locations used in Circle Dock must be the same on the other computer(s).

Build an OS Image with Automatic Product Activation

When performing OS image setups, it is necessary to use the automatic product activation featured of Secure Lockdown. Implementing automatic product activation eliminates the need for the initial Secure Lockdown splash screen where user interaction is required and activation is performed.

Note: This OS image setup procedure assumes the Secure Lockdown license will be activated *prior* to end user distribution. If you intend to have the Secure Lockdown license activated *after* distribution to the end user, please contact Inteset Support (techsupport@inteset.com) for instructions on how to do so.

In addition to the system requirements of Secure Lockdown (see the *User Guide*), auto-product activation has separate requirements to operate:

1. You must have a product activation key (provided by Inteset Systems)
2. You must have a Secure Lockdown password
3. An internet connection must be available (unless an Offline License was purchased)

If an Offline License was purchased (100 units or more), additional requirements are:

4. You must have a License Certificate file (provide by Inteset Systems)
5. You must have a License Certificate password (provide by Inteset Systems)
6. The Windows Firewall Service must be installed and running
7. No web traffic on port 80 is allowed on any network interface
8. Offline Licensing is not available on Windows XP

If all of the above requirements have been met, you can begin the OS image build and automatic product activation steps below. It is important to read through all of the following steps before proceeding with them. It is also important to follow the steps in the exact order listed.

Note: In the subsequent steps below, there are several references to the Secure Lockdown root Windows Registry key name: "HKCU/Software/Inteset/SecureLockdown_V2". Depending on what edition of Secure Lockdown you're installing, the root key name may end in "SecureLockdown_V2" (Standard Edition), "SecureLockdown_V2_IE" (Internet Explorer Edition), "SecureLockdown_V2_CM" (Chrome Edition), "SecureLockdown_V2_MA" (Multi Application Edition). Be sure to apply the correct key name based on the product you're installing.

Step 1 – Set up a Unique Secure Lockdown Password Using the Password Generator Tool

If you want to define a unique Secure Lockdown password for each system, use the Secure Lockdown password generator tool. This tool and usage documentation can be obtained by contacting Inteset Support (techsupport@inteset.com). Otherwise, skip to *Step 2*.

1. Install the *SLPasswordGenerator.exe* file in a folder path accessible by the administrator account. For example: "c:\SLPasswordGenerator.exe"
2. Create a task using the *Windows Task Scheduler* to run the *SLPasswordGenerator* command line as defined in the above *Auto Password Generation Setup* section

Step 2 – Install and Configure Secure Lockdown

Install and configure Secure Lockdown by performing the following tasks:

1. Install Secure Lockdown as you would any other Windows application by double-clicking on the installation file. In some cases, you may want to install Secure Lockdown in "Silent" mode. To do so, use the following command line:

   IntesetSecureLockdown_V2.exe /s /v"/qb"

   Note: Secure Lockdown must be installed and configured under a Windows Administrative account (usually a local computer administrator.)

2. Run Secure Lockdown. The initial Splash screen will appear giving you the opportunity to run Secure Lockdown as a Trial. Press the "Get Trial" button. If the trial activation is successful, Secure Lockdown will close. Run Secure Lockdown again and press the "Run Trial" button.

   Note: you will need an Internet connection to proceed with this step (or you can proceed with the "Off-line" trial activation option that you will be presented with if you do not have an Internet connection.)

3. Currently, there should not be a password required to enter the configuration settings because the command line (in *Step 1* above) has not yet been executed. If you are **not** using the auto password generator tool (as defined in *Step 1* above) and you want to have the same password for all installation, define a password by pressing the "Set" button under the "Password" tab.

4. Configure all Secure Lockdown settings to your needs. Note that you'll need to know what the Secure Lockdown configuration settings are at this point. As described in the *Copying Secure Lockdown Configuration Settings to Other Computers* section above, you could obtain these settings from another computer using Secure Lockdown, then import the settings file on the target system.

5. Close Secure Lockdown once you're satisfied with the configuration of Secure Lockdown.

Step 3 – Define the Product Activation Key

Create the following Windows Registry key Name and Data value (String) and populate it with the product activation code provided to you by Inteset Systems when you purchased the bulk license:

Key Name: HKEY_CURRENT_USER\Software\Inteset\SecureLockdown_v2
Value Name: "AutoRegistrationKey" (String Value)
Value Data: <product activation code>

When configuring auto-activation, you should use a license key (product activation code) that will work with the number of installations you plan. For example, if you plan to build 100 systems, you should use a license key that supports 100 units. Note that when you purchase Secure Lockdown in quantity on our web site, you are provided a single key for the number of licenses you purchased. It is this key that should be used in the auto-activation setup and the registry value above.

Note: You can always use the same key even if more licenses are needed/purchased in the future. Inteset has a "Merge License Key" feature available on its website that will allow you to merge a new license key with a previously purchased one. See the *My Account > Manage Licenses* feature on the www.intesetsystems.com website for access to this feature.

Step 4 – Apply the Offline Certificate File and Certificate Password

If you have purchased an Offline License or have received an Offline Trial license, perform the tasks below. Otherwise, skip to *Step 5*.

1. Inteset Systems provided you with a certificate file with a similar name as "<company name>-yyy-mm-dd.SLCert.cer". Rename the file by removing the prefix so that it is named "SLCert.cer" instead.
2. Place the "SLCert.cer" file in the program directory of Secure Lockdown (ie: "C:\Program Files (x86)\Inteset\Secure Lockdown")
3. Inteset Systems provided you with a certificate password. Create the following Windows Registry key name and enter the password exactly as it was provided in the value data field:

   Key Name: HKEY_CURRENT_USER\Software\Inteset\SecureLockdown_v2
   Value Name: "CertPassword" (String Value)
   Value Data: <certificate password>

Note: Once the Secure Lockdown auto-activate process succeeds, the above registry entry will be removed and the "SLCert.cer" file will be deleted automatically.

Step 5 – Set up Secure Lockdown to Run and Enable Itself on Startup

Set up Secure Lockdown to run upon Windows startup and enable itself by creating the following Windows Registry command-line entry:

Key Name: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Value Name: "SecureLockdownAutoRegistration" (String Value)
Value Data: "C:\Program Files (x86)\Inteset\Secure Lockdown\IntesetSecureLockdownV2.exe" enable "<Secure Lockdown password>"

Note: The *Value Data* path above may be different depending on which Windows OS (ie: 32bit vs. 64bit) and version of Secure Lockdown is being used (ie: *Secure Lockdown - Standard*, *Internet Explorer*, or *Multi-application Edition*). In addition, you should enter quotes ("") as the second parameter (password) if you're making use of the SLPasswordGen utility. Otherwise, the second parameter should be the password you set in *Step 2* above wrapped in quotes.

Note: Once the Secure Lockdown auto-activate process succeeds, the above registry entry will be removed.

Step 6 – Generate the Final OS Image

Do NOT log out of the account or restart the computer yet. Now is the time to start the final image burn process. The image burn process may or may not require a system restart once complete. Regardless, upon completion of the image burn process, you can safely restart the system.

Upon logout, then logging back in, or restarting, Secure Lockdown will auto-activate itself, then it will start the Secure Lockdown enable process and complete it by rebooting the system automatically.

If Secure Lockdown is not activated upon reboot, the Secure Lockdown Splash Screen will appear. If this occurs, something went wrong (check for Secure Lockdown errors in the Windows Application Event Log) and you will need to go through the above steps again. You can disable Secure Lockdown by the normal procedure (ie: the Secure Lockdown configuration tool) to regain access to the system if it is enabled.

Note: During testing, you may need to deactivate the license on the system. This can be accomplished by selecting the *Help > Deactivate* tab in the Secure Lockdown configuration screen and pressing the *Deactivate* button. The Deactivate button is only visible if Secure Lockdown is activated.