# Lab #1: Develop System Administration Procedures for Windows 8.1 Security Configuration

## Purpose: Develop systems administration procedures to implement systems security configuration guidance and best practices.

## Objectives

1. Develop a Windows *system restore point* systems administration procedure to implement an industry recognized best practice for maintaining system integrity and availability.
2. Develop a Windows system administration procedure to manage *programs and features*.
3. Develop a *systems administration* procedure to implement configuration rules from *systems security technical* *guidance* issued by a vendor or government organization.

## Overview

In this lab, our focus is upon developing a set of procedures which can be incorporated into an organization’s security implementation guidance and documentation. For each procedure, you will develop, test, and document the steps required to implement the selected best practices and security configuration guidance (as provided in the lab instructions and notes). You will write three separate procedures for this lab:

1. *Creating, Using, Removing System Restore Points for Windows 8.1*
2. *Managing Windows 8.1 Programs and Features*
3. *Implementing Security Configuration Rules for Windows 8.1*

Each procedure will have the following major sections (see Figure 1):

* Title:
* Operating Environment:
* Description:
* Notes, Warnings, & Restrictions:
* Resources (Further Reading):
* Procedures:

Some procedures will contain a large number of steps. To make the procedures easier to read, you should divide your procedures into groups of related steps. Place a group heading (e.g. *Create System Restore Points*) at the beginning of each group. Each group heading should be followed by a brief paragraph that explains the purpose of the group (e.g. This group (or “section”) contains step by step instructions for creating System Restore Points using the “System Restore ” tool….)

|  |
| --- |
| **Title:**  **Operating Environment:**   1. **Hardware** 2. **Software**   **Description:**  **Notes, Warnings, & Restrictions:**  **Resources (Further Reading):**        **Procedures:**  ***[Group Heading]***  *Brief introduction paragraph for this group of steps*       ***[Group Heading]***  *Brief introduction paragraph for this group of steps* |

**Figure 1. Required Outline for System Administration Procedures**

## Instructions

### Part (a): Implementing System Restore Points

1. Investigate the *System Restore* tool (used to manage system restore points). To access the tool, open the *System* tool from Control Panel (Control Panel > System and Security > System). Then, click on System Protection (left menu).
2. Identify appropriate sources of information (e.g. Windows Help, Microsoft Technet, etc.) for instructions for using the Windows 8.1 System Restore Point capability. Using those sources, research the procedures required to perform the following tasks:
   1. Create a system restore point for a Windows 8.1 system
   2. Use a system restore point to roll-back changes made to a Windows 8.1 system
   3. Remove system restore points from a Windows 8.1 system (some and all)

**Note:** you will not be able to do the full rollback (item 2(b)) in the VDA due to security restrictions. Your procedure should contain these steps, however. Use the Microsoft “System Restore” documentation to obtain the required information about what happens after the system restart for the rollback. You do not need to provide an “after” snapshot for this step.

1. Paste the procedure outline (Figure 1) into your Lab #1 file. Make sure that you insert a page break so that the “Title” heading appears at the top of a new page.
2. Using the required outline, develop a systems administration procedure which can be used to perform tasks related to item #1 (management and use of system restore points).
3. Test your draft procedures using the virtual machine provided in the online lab environment (UMUC’s VDA). Do NOT use your personal computer or a work computer.
4. As you run your tests, collect screen snapshots to illustrate key steps in your procedures. (Use the snipping tool on your local PC to snapshot portions of the VDA browser or client window.) Insert these snapshots at the appropriate points in your procedure. The snapshots must show the procedures as run in the VDA environment.

### Part (b): Managing Programs and Features for Windows 8.1

1. Investigate the *Programs and Features* tool (used to manage installed programs and optional features / capabilities). To access the tool, open *Programs and Features* from the Windows Control Panel.
2. Identify appropriate sources of information (e.g. Windows Help, Microsoft Technet, etc.) for instructions for using the *Programs and Features* tool. Using those sources, research the procedures required to perform the following tasks:
   1. Turn Windows Features On or Off
   2. Modify, Repair, or Uninstall a program from a Windows 8.1 system
   3. Select and Install Updates for Windows and Windows Applications, Find an installed Update, Remove an installed update
3. Paste a second blank copy of the procedure outline (from Figure 1) at the end of your Lab #1 file. Make sure that you insert a page break before you paste to ensure the “Title” heading appears at the top of a new page.
4. Using the required outline, develop a systems administration procedure which can be used to perform tasks related to item #2. Provide examples for each of the required tasks. (Select a specific feature, program, or update and use that as an example in your procedure.)
5. As you run your tests, collect screen snapshots to illustrate key steps in your procedures. (Use the snipping tool on your local PC to snapshot portions of the VDA browser or client window.) Insert these snapshots at the appropriate points in your procedure. The snapshots must show the procedures as run in the VDA environment.

### Part (c): Implementing Security Configuration Rules Using the Local Group Policy Editor

**Note:** you are NOT implementing the DISA / DoD STIG in this section. You are implementing a set of security configuration rules that your “company” has selected from *industry accepted sources.*

1. Investigate the *Local Group Policy Editor* tool (Windows Key + R then type gpedit.msc). Pay particular attention to the menu tree in the left hand pane (expand and review the categories of settings which can be changed using this tool).
2. Research the security configuration rules listed in Table 1. These rules were developed from the Department of Defense *Security Technical Implementation Guidance for Windows 8.1*.
3. When you are ready to begin writing your procedure, paste a blank copy of the procedure outline (from Figure 1) at the end of your Lab #1 file. Make sure that you insert a page break before you paste to ensure the “Title” heading appears at the top of a new page.
4. Determine how you will group related security configuration rules. Each group will need a “section heading” (see Figure 1) and introductory paragraph (2 -3 sentences) which explains the purpose of the group.
5. Next, develop a step by step procedure for each group of rules. See the *“Suggested Procedure Group”* column in Table 1 for suggested categories. Your groupings should allow for inclusion of additional, related rules at a later date. (For example, there are two “energy saving” rules in the table; an organization may wish to add additional rules to this category at some point in the future.)
6. For each group of rules, develop step-by-step written procedures for systems administrators. Your written procedures must implement the “remediation” guidance as listed in Table 1[[1]](#endnote-1).
7. Test your procedures by running them in the VDA. As you run your tests, collect screen snapshots to illustrate key steps in your procedures. (Use the snipping tool on your local PC to snapshot portions of the VDA browser or client window.) Insert these snapshots at the appropriate points in your procedure. The snapshots must show the procedures as run in the VDA environment.
8. Incorporate your screen snapshots for key steps into the draft procedures. Each snapshot should be placed UNDER (after) the step to which it applies. Captions are not required.
9. Make any additional changes required to address issues found during testing of the step-by-step procedures.

### Finalize Your Deliverable

1. Using the grading rubric as a guide, refine your step-by-step procedures. Your final products should be suitable for inclusion in an organization’s *Systems Administrator’s Handbook*. Remember that you are preparing multiple system administration procedures which must be presented separately.
2. As appropriate, cite your sources using footnotes or another appropriate citation style.
3. Use the *resources* section to provide information about recommended readings and any sources that you cite. Use a standard bibliographic format (you may wish to use APA since this is required in other CSIA courses). I**nformation about sources and recommended readings, including in-text citations, should be formatted consistently and professionally.**
4. Each procedure document should be placed in the listed order in a SINGLE FILE (see deliverables list above). Each file should start with a title page which lists the following information:

* Lab Title and Number
* Procedure Name
* Date
* Your Name

1. The **CSIA 310 Template for Lab Deliverable.docx** file is set up to provide the required title page and three lab procedure templates.

## Additional Requirements for this Lab

1. Your target audience for these procedures will be Windows 8/8.1 SYSTEM ADMINISTRATORS. Do not write procedures for home users or individuals using their own computers.
2. Your step-by-step procedures should tell the System Administrator where to find and how to launch the systems administration tools used to change security configuration settings for the Windows 8.1 operating system.
3. It is not necessary to specify every step that a system administrator must take to implement the security rules. But, you must address each security configuration rule separately and include enough detail that your reader will understand how to perform the required steps to implement the security configuration changes.
4. Use screen snapshots to cue the reader to important steps or provide information required to complete check points for proper completion of a step or set of steps (e.g. including a snapshot which shows the “after” state for a group of security settings).
5. Make sure that your snapshots will enhance the reader’s understanding of the procedure and required configuration changes. Too many snapshots or illustrations can make a procedure difficult to use.
6. All snapshots must be created by you for this lab using screen captures showing how you personally performed (tested) the systems administration procedure as written by you. You may not copy and paste images from help pages, manuals, or the Internet.
7. Images (screen snapshots) should be cropped and sized appropriately.
8. A screen snapshot belonging to a specific procedure step does not require a caption.
9. Make sure that the sources you cite or recommend (*additional reading*) are authoritative and are the best ones available.
10. Your Operating Environment section should identify the hardware, operating system, and/or software applications to which the procedure applies. For this lab, your procedures will apply to:
    1. Hardware: Laptop or Desktop Computers
    2. Operating System: Windows 8.1 Professional
11. Your Notes, Warnings & Restrictions section should include important information that is not found elsewhere in the procedures document. For example, this section could include information about alternatives to the selected security configuration settings. Or, this section could include information about related security procedures or policies. If this procedure implements controls relevant to an external security requirement, e.g. the HIPAA Security Rule, then that information should be included in the notes section. Consult the *Windows 8.1 STIG* to see what types of information you may need to include in your document. This section should also include important information about harm or risk that could occur if the procedure is not correctly followed or implemented.
12. **The procedures that you write for this lab will become part of the final project for this course (System Administration Manual).**

**Table 1 begins on the next page.**

## Table 1. Required Security Configuration Rules

| **Rule ID** | **Rule** | **Vulnerability Discussion** | **Remediation** | **Suggested Procedure Group** |
| --- | --- | --- | --- | --- |
| SV-48022r1\_rule | The required legal notice must be configured to display before console logon. | Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive Logon: Message text for users attempting to log on" to the [banner text]. Note: see STIG for DoD Warning Notice. In registry, check make sure that you have configured the "LegalNoticeText" value for key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ | Banner |
| SV-48049r1\_rule | The Ctrl+Alt+Del security attention sequence for logons must be enabled. | Disabling the Ctrl+Alt+Del security attention sequence can compromise system security. Because only Windows responds to the Ctrl+Alt+Del security sequence, you can be assured that any passwords you enter following that sequence are sent only to Windows. If you eliminate the sequence requirement, malicious programs can request and receive your Windows password. Disabling this sequence also suppresses a custom logon banner. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive Logon: Do not require CTRL+ALT+DEL" to "Disabled". | Banner |
| SV-48510r1\_rule | The Windows dialog box title for the legal banner must be configured. | Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive Logon: Message title for users attempting to log on" to a site-defined warning. In registry, check make sure that you have configured both the "LegalNoticeCaption" value for key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ | Banner |
| SV-48313r2\_rule | The display must turn off after 20 minutes of inactivity when the system is running on battery. | Turning off an inactive display supports energy saving initiatives. It may also extend availability on systems running on a battery. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Video and Display Settings -> "Turn Off the Display (On Battery)" to "Enabled" with "1200" seconds or less. | Energy Saving |
| SV-48314r2\_rule | The display must turn off after 20 minutes of inactivity when the system is plugged in. | Turning off an inactive display supports energy saving initiatives. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Video and Display Settings -> "Turn Off the Display (Plugged In)" to "Enabled" with "1200" seconds or less. | Energy Saving |
| SV-48051r1\_rule | The Smart Card removal option must be configured to Force Logoff or Lock Workstation. | Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive logon: Smart card removal behavior" to "Lock Workstation" or "Force Logoff". | Lock Screen |
| SV-48310r2\_rule | App notifications on the lock screen must be turned off. | App notifications that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged on user. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Logon -> "Turn off app notifications on the lock screen" to "Enabled". | Lock Screen |
| SV-55990r2\_rule | Camera access from the lock screen must be disabled. (Windows 8.1) | Enabling camera access from the lock screen could allow for unauthorized use. Requiring logon will ensure the device is only used by authorized personnel. | This requirement is NA for the initial release of Windows 8. It is applicable to Windows 8.1. If the device does not have a camera, this is NA.  Configure the policy value for Computer Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Prevent enabling lock screen camera" to "Enabled". | Lock Screen |
| SV-55991r2\_rule | The display of slide shows on the lock screen must be disabled. (Windows 8.1) | Slide shows that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged on user. | Configure the policy value for Computer Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Prevent enabling lock screen slide show" to "Enabled". This requirement is NA for the initial release of Windows 8. It is applicable to Windows 8.1. | Lock Screen |
| SV-48018r1\_rule | The shutdown option must be available from the logon dialog box. | Preventing display of the shutdown button in the logon dialog box may encourage a hard shut down with the power button. (However, displaying the shutdown button may allow individuals to shut down a system anonymously.) | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Shutdown: Allow system to be shutdown without having to log on" to "Enabled". | Logon Screen |
| SV-48164r1\_rule | The system must be configured to prevent the display of the last username on the logon screen. | Displaying the username of the last logged on user provides half of the userid/password equation that an unauthorized person would need to gain access. The username of the last user to log onto a system must not be displayed. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive logon: Do not display last user name" to "Enabled". | Logon Screen |
| SV-48228r2\_rule | The classic logon screen must be required for user logons. | The classic logon screen requires users to enter a logon name and password to access a system. The simple logon screen or Welcome screen displays usernames for selection, providing part of the necessary logon information. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Logon -> "Always use classic logon" to "Enabled". If the system is a member of a domain, this is NA. | Logon Screen |
| SV-48244r2\_rule | Users must be prompted for a password on resume from sleep (on battery). | Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (on battery). | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Sleep Settings -> "Require a password when a computer wakes (on battery)" to "Enabled". | Logon Screen |
| SV-48245r2\_rule | The user must be prompted for a password on resume from sleep (plugged in). | Authentication must always be required when accessing a system. This setting ensures the user is prompted for a password on resume from sleep (plugged in). | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Power Management -> Sleep Settings -> "Require a password when a computer wakes (plugged in)" to "Enabled". | Logon Screen |
| SV-48460r2\_rule | The machine inactivity limit must be set to 15 minutes, locking the system with the screensaver. | Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. | Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Interactive logon: Machine inactivity limit" to "900" seconds". | Logon Screen |
| SV-55993r2\_rule | The network selection user interface (UI) must not be displayed on the logon screen. (Windows 8.1) | Enabling interaction with the network selection UI allows users to change connections to available networks without signing into Windows. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Logon -> "Do not display network selection UI" to "Enabled". | Logon Screen |
| SV-48464r2\_rule | Notifications from Windows Push Network Service must be turned off. | The Windows Push Notification Service (WNS) allows third-party vendors to send updates for toasts, tiles, and badges. | Configure the policy value for User Configuration -> Administrative Templates -> Start Menu and Taskbar -> Notifications -> "Turn off notifications network usage" to "Enabled". | Notifications |
| SV-48465r2\_rule | Toast notifications to the lock screen must be turned off. | Toast notifications that are displayed on the lock screen could display sensitive information to unauthorized personnel. Turning off this feature will limit access to the information to a logged on user. | Configure the policy value for User Configuration -> Administrative Templates -> Start Menu and Taskbar -> Notifications -> "Turn off toast notifications on the lock screen" to "Enabled". | Notifications |
| SV-48240r2\_rule | A system restore point must be created when a new device driver is installed. | A system restore point allows a rollback if an issue is encountered when a new device driver is installed. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation -> "Prevent creation of a system restore point during device activity that would normally prompt creation of a restore point" to "Disabled". | Restore Point |
| SV-48273r2\_rule | A screen saver must be enabled on the system. | Unattended systems are susceptible to unauthorized use and must be locked when unattended. Enabling a password-protected screen saver to engage after a specified period of time helps protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. | Configure the policy value for User Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Enable Screen Saver" to "Enabled". | Screen Saver |
| SV-48274r2\_rule | The screen saver must be password protected. | Unattended systems are susceptible to unauthorized use and must be locked when unattended. Enabling a password-protected screen saver to engage after a specified period of time helps protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. | Configure the policy value for User Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Password protect the screen saver" to "Enabled". | Screen Saver |
| SV-48461r2\_rule | A screen saver must be defined. | Unattended systems are susceptible to unauthorized use and must be locked when unattended. Enabling a password-protected screen saver to engage after a specified period of time helps protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. | Configure the policy value for User Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Force specific screen saver" to "Enabled" with "scrnsave.scr" specified as the Screen saver executable name. | Screen Saver |
| SV-48462r2\_rule | Changing the screen saver must be prevented. | Unattended systems are susceptible to unauthorized use and must be locked. Preventing users from changing the screen saver ensures an approved screen saver is used. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. | Configure the policy value for User Configuration -> Administrative Templates -> Control Panel -> Personalization -> "Prevent changing screen saver" to "Enabled". | Screen Saver |
| SV-48337r2\_rule | The Windows SmartScreen must be turned off. | Some features may send system information to the vendor. Turning off this capability will prevent potentially sensitive information from being sent outside the enterprise. | Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> File Explorer -> "Configure Windows SmartScreen" to "Enabled" with "Turn off SmartScreen" selected. | Smart Screen |
| SV-48119r1\_rule | Media Player must be configured to prevent automatic Codec downloads. | The Windows Media Player uses software components, referred to as Codecs, to play back media files. By default, when an unknown file type is opened with the Media Player, it will search the Internet for the appropriate Codec and automatically download it. To ensure platform consistency and to protect against new vulnerabilities associated with media types, all Codecs must be installed by the System Administrator. | Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Windows Media Player -> Playback -> "Prevent Codec Download" to "Enabled". | System Integrity |
| SV-48218r1\_rule | The system must notify antivirus when file attachments are opened. | Attaching malicious files is a known avenue of attack. This setting configures the system to notify antivirus programs when a user opens a file attachment. | Configure the policy value for User Configuration -> Administrative Templates -> Windows Components -> Attachment Manager -> "Notify antivirus programs when opening attachments" to "Enabled". | System Integrity |
| SV-48300r2\_rule | Access to the Windows Store must be turned off. | Uncontrolled installation of applications can introduce various issues, including system instability and allow access to sensitive information. Installation of applications must be controlled by the enterprise. Turning off access to the Windows Store will limit access to publicly available applications. | Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Internet Communication Management -> Internet Communication settings -> "Turn off access to the Store" to "Enabled". | System Integrity |
| SV-48341r3\_rule | Automatic download of updates from the Windows Store must be turned off. | Uncontrolled system updates can introduce issues to a system. Obtaining update components from an outside source may also potentially allow sensitive information outside of the enterprise. Application updates must be obtained from an internal source. | Windows 8.1 split the original policy that configures this setting into two separate ones. Configuring either one to "Enabled" will update the registry value as identified in the Check section. Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Store -> "Turn off Automatic Download of updates on Win8 machines" or "Turn off Automatic Download and install of updates" to "Enabled".  Windows 8: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Store -> "Turn off Automatic Download of updates" to "Enabled". | System Integrity |
| SV-48344r2\_rule | The Windows Store application must be turned off. | Uncontrolled installation of applications can introduce various issues including system instability, and provide access to sensitive information. Installation of applications must be controlled by the enterprise. Turning off access to the Windows Store will limit access to publicly available applications. | Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Store -> "Turn off the Store application" to "Enabled". | System Integrity |
| SV-55997r2\_rule | The option to update to the latest version of Windows from the Store must be turned off. (Windows 8.1) | Uncontrolled system updates can introduce issues into the environment. Updates to the latest version of Windows must be done through proper change management. This setting will prevent the option to update to the latest version of Windows from being offered through the Store. | Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Store -> "Turn off the offer to update to the latest version of Windows" to "Enabled". This requirement is NA for the initial release of Windows 8. It is applicable to Windows 8.1. | System Integrity |

1. Table 1 was adapted from the Department of Defense *Security Technical Implementation Guidance (STIG) for Windows 8/8.1*. Available from: <http://iasecontent.disa.mil/stigs/zip/Apr2015/U_Windows_8_and_8-1_V1R9_STIG.zip> [↑](#endnote-ref-1)