

# HOW TO CONDUCT SYSTEM HARDENING USING THE DEFENSE INFORMATION SYSTEMS AGENCY'S (DISA) "GOLD DISK"

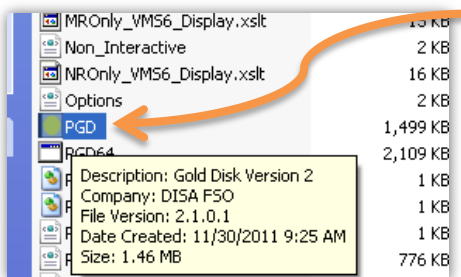
---

Holes in your IT infrastructure can make for some [awkward situations](#). Whether you're dealing with sensitive customer information, upcoming product designs, or simply just don't want people messing with your stuff, maintaining system integrity can be difficult. Symantec is great, but what do you do when the integrity of your system directly relates to national security? Where do you turn when the boss says you gotta [keep those centrifuges spinning](#) or heads will roll?

The DoD has developed a process, called DIACAP, for certifying that an Information System (IS) is compliant with DoD security standards. DIACAP stands for DoD Information Assurance Certification and Accreditation Process and you can find additional information about it [here](#) and [here](#).

The DISA (an agency within the DoD) has developed a tool, called "Gold Disk", to help identify and mitigate security holes according to DIACAP standards. It scans your machine and produces a detailed outline of all the Category 1, 2, and 3 vulnerabilities it finds, depending on the applicable Mission Assurance Level. It even goes as far as to suggest the appropriate means of resolving the issue, point out relevant Microsoft Security Bulletins, and offer to fix things for you.

## HOW TO CONDUCT SYSTEM HARDENING USING THE DEFENSE INFORMATION SYSTEMS AGENCY'S (DISA) "GOLD DISK"



### **STEP 1: LOCATE THE APPLICATION'S .EXE FILE!**

Inside the application's folder, look for an exe file called "PGD". This is the main executable and there should be both a PGD and a PGD64 file. Select the one that is appropriate for the machine being scanned.

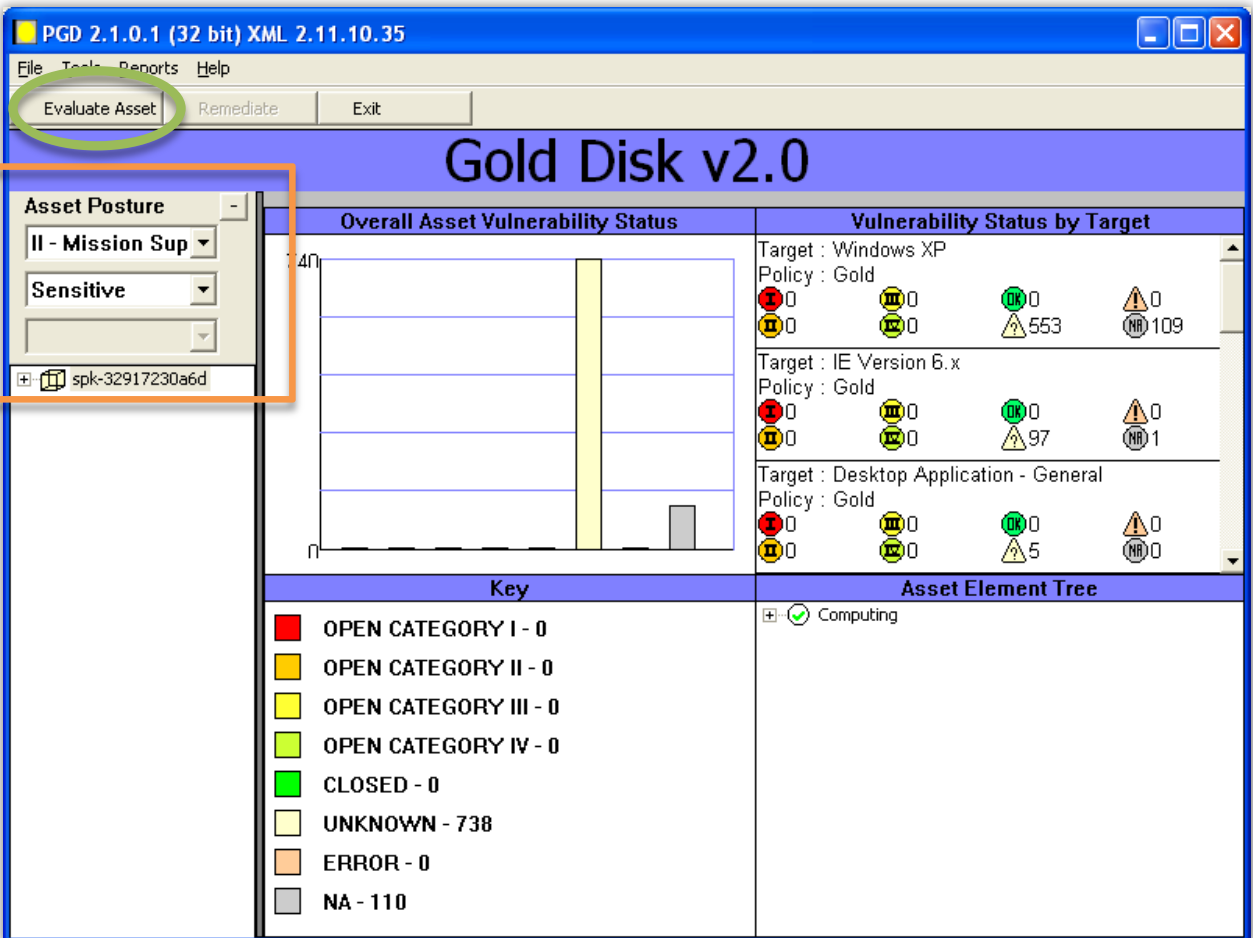
### **STEP 2: SELECT SPECIAL CASES AND BEGIN THE SCAN!**

When the Gold Disk application loads, you should see a list of special cases. If none of these applications are installed, uncheck them to help improve the speed of the scan. When you're ready to begin, press "Continue" to start scanning the machine. You will see two progress bars indicating the state of the current operation and the overall status of the scan.



### STEP 3: EVALUATE THE ASSET!

Once the initial scan is completed, you will see a screen that looks like this:



The screenshot shows the PGD 2.1.0.1 (32 bit) XML 2.11.10.35 application window. The title bar reads "PGD 2.1.0.1 (32 bit) XML 2.11.10.35". The menu bar includes "File", "Tools", "Reports", and "Help". Below the menu bar are three buttons: "Evaluate Asset" (circled in green with a '2'), "Remediate", and "Exit". The main window title is "Gold Disk v2.0".

On the left side, there is a sidebar with "Asset Posture" settings. A green '1' is next to this sidebar. The "Asset Posture" section has a dropdown menu set to "II - Mission Sup" and another dropdown set to "Sensitive". Below this is a field containing "spk-32917230a6d".

The main content area is divided into several sections:

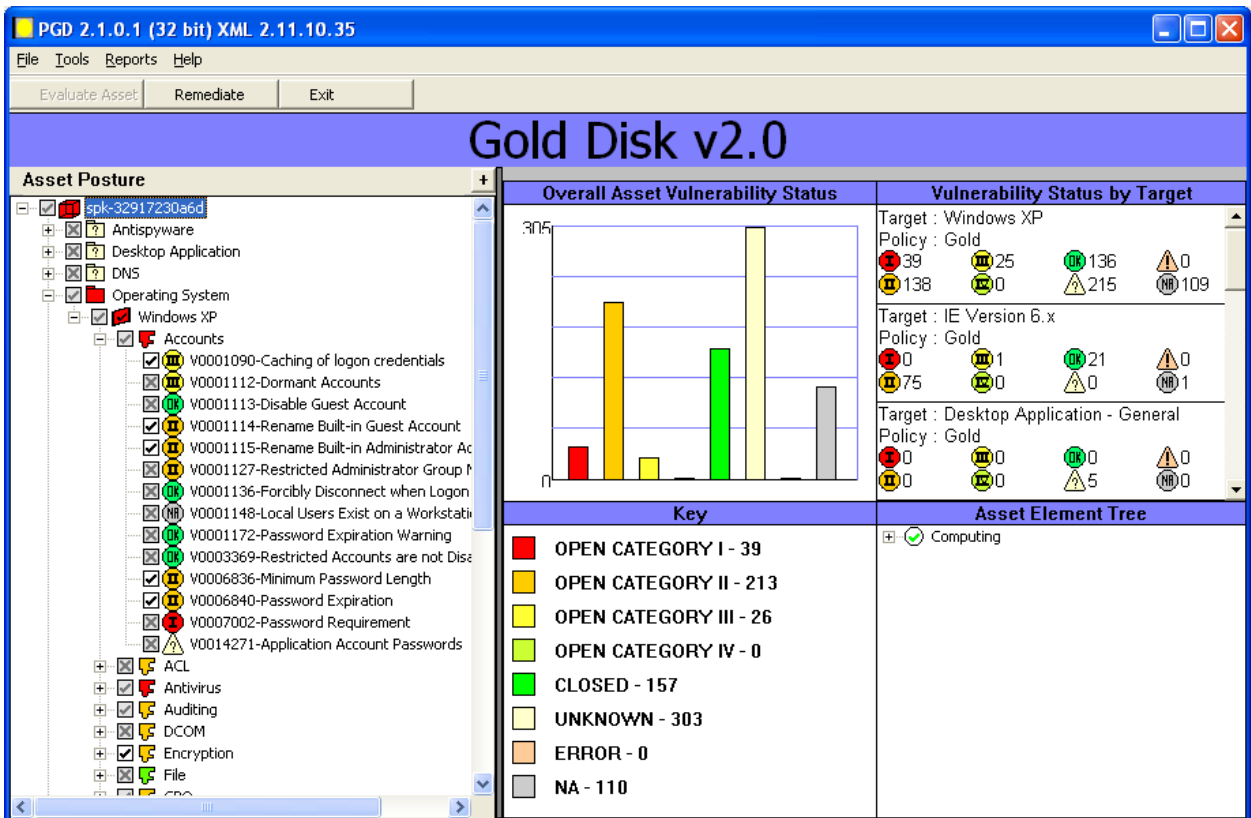
- Overall Asset Vulnerability Status:** A bar chart showing vulnerability counts across categories.
- Vulnerability Status by Target:** A table showing vulnerability counts for different targets:
 

Target	Policy	Category I	Category II	Category III	Category IV	Closed	Unknown	Error	NA
Windows XP	Gold	0	0	0	553	0	109	0	0
IE Version 6.x	Gold	0	0	0	97	0	1	0	0
Desktop Application - General	Gold	0	0	0	5	0	0	0	0
- Key:** A legend for vulnerability categories:
  - OPEN CATEGORY I - 0 (Red)
  - OPEN CATEGORY II - 0 (Orange)
  - OPEN CATEGORY III - 0 (Yellow)
  - OPEN CATEGORY IV - 0 (Light Green)
  - CLOSED - 0 (Green)
  - UNKNOWN - 738 (Light Yellow)
  - ERROR - 0 (Brown)
  - NA - 110 (Grey)
- Asset Element Tree:** Shows a tree view with "Computing" selected.

Notice the drop-down menu on the left side of the screen. 1) Select the "Asset Posture" that best describes your Mission Assurance Level: "I – Mission Critical", "II – Mission Support", or "III – Administrative". 2) Next, press the "Evaluate Asset" button . You will see two progress bars, identical to the ones in the previous step.

**STEP 4: REVIEW THE RESULTS!**

Once the evaluation process is complete you will be presented with a screen, just like the last one, with the number of open Category 1, 2, and 3 findings properly identified. Along the left is a tree structure listing, categorically, all the findings for this machine. Category 1 (CAT1) findings will appear in red, CAT2 findings will be orange, and CAT3 yellow.



The screenshot displays the Gold Disk v2.0 interface. On the left is the 'Asset Posture' tree for asset 'spk-32917230a6d', showing categories like Antispyware, Desktop Application, DNS, Operating System, and Windows XP. The main area is divided into 'Overall Asset Vulnerability Status' (with a bar chart) and 'Vulnerability Status by Target' (with counts for Windows XP, IE Version 6.x, and Desktop Application). A 'Key' section at the bottom defines finding categories: OPEN CATEGORY I (39), OPEN CATEGORY II (213), OPEN CATEGORY III (26), OPEN CATEGORY IV (0), CLOSED (157), UNKNOWN (303), ERROR (0), and NA (110).

Overall Asset Vulnerability Status	Vulnerability Status by Target
<p>Bar Chart Data:</p> <ul style="list-style-type: none"> <li>OPEN CATEGORY I: 39</li> <li>OPEN CATEGORY II: 213</li> <li>OPEN CATEGORY III: 26</li> <li>OPEN CATEGORY IV: 0</li> <li>CLOSED: 157</li> <li>UNKNOWN: 303</li> <li>ERROR: 0</li> <li>NA: 110</li> </ul>	<p>Target : Windows XP Policy : Gold</p> <ul style="list-style-type: none"> <li>OPEN CATEGORY I: 39</li> <li>OPEN CATEGORY II: 25</li> <li>OPEN CATEGORY III: 136</li> <li>OPEN CATEGORY IV: 0</li> <li>CLOSED: 138</li> <li>UNKNOWN: 215</li> <li>ERROR: 0</li> <li>NA: 109</li> </ul> <p>Target : IE Version 6.x Policy : Gold</p> <ul style="list-style-type: none"> <li>OPEN CATEGORY I: 0</li> <li>OPEN CATEGORY II: 1</li> <li>OPEN CATEGORY III: 21</li> <li>OPEN CATEGORY IV: 0</li> <li>CLOSED: 75</li> <li>UNKNOWN: 0</li> <li>ERROR: 0</li> <li>NA: 1</li> </ul> <p>Target : Desktop Application - General Policy : Gold</p> <ul style="list-style-type: none"> <li>OPEN CATEGORY I: 0</li> <li>OPEN CATEGORY II: 0</li> <li>OPEN CATEGORY III: 0</li> <li>OPEN CATEGORY IV: 0</li> <li>CLOSED: 0</li> <li>UNKNOWN: 5</li> <li>ERROR: 0</li> <li>NA: 0</li> </ul>

Selecting a vulnerability allows you to examine its particular details.



**Disallow AutoPlay/Autorun from Autorun.inf**

Status : **Vulnerable** VMS 6 ID : V0017900  
Severity: **Critical (CAT I)** PDI : 2.022

Description	Discussion	Details	Detection	Remediation	Notes	Impact/Mitigation	Misc.
-------------	------------	---------	-----------	-------------	-------	-------------------	-------

This registry key will prevent the autorun.inf from executing commands.

**Disallow AutoPlay/Autorun from Autorun.inf**

Status : **Vulnerable** VMS 6 ID : V0017900  
Severity: **Critical (CAT I)** PDI : 2.022

Description	Discussion	Details	Detection	Remediation	Notes	Impact/Mitigation	Misc.
-------------	------------	---------	-----------	-------------	-------	-------------------	-------

**Finding Details**

The value: SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf(null) does not exist.

**Disallow AutoPlay/Autorun from Autorun.inf**

Status : **Vulnerable** VMS 6 ID : V0017900  
Severity: **Critical (CAT I)** PDI : 2.022

Description	Discussion	Details	Detection	Remediation	Notes	Impact/Mitigation	Misc.
-------------	------------	---------	-----------	-------------	-------	-------------------	-------

**Manual Procedures**

In the Registry Editor, navigate to the following registry key:

Registry Hive: HKEY\_LOCAL\_MACHINE  
Subkey: SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\Autorun.inf  
Value Name: (Default)  
Type: REG\_Sz  
Value: @SYS.DoesNotExist

**Disallow AutoPlay/Autorun from Autorun.inf**

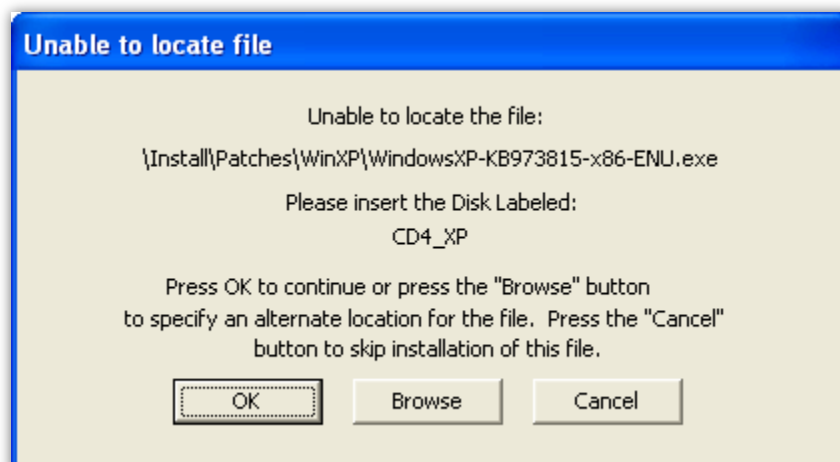
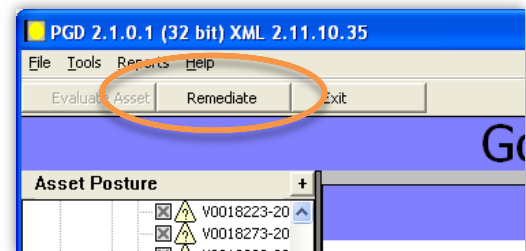
Status : **Vulnerable**      VMS 6 ID : V0017900  
Severity: **Critical (CAT I)**      PDI : 2.022

Description	Discussion	Details	Detection	Remediation	Notes	Impact/Mitigation	Misc.
<p><b>Manual Procedures</b></p> <p>Add the registry value as specified in the manual check.</p> <p><b>Automatic Procedures</b></p>							

Along with a description of the vulnerability and the method used for identifying it, you will also find instructions for resolving the issue.

### STEP 5: MITIGATION!

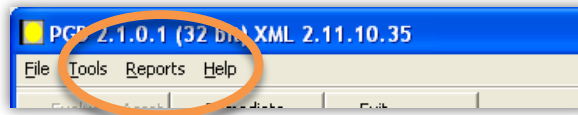
There are two methods for applying the recommended fixes to your machine: Manually or automatically. If you would like to let Gold Disk do all the work for you, then click the "Remediate" button up in the top left of the screen. This can be a potentially hazardous choice as it may apply changes that contradict the intended purpose of for the machine. For instance, you might not want the machine to automatically lockout after an idle period if it's meant to function as kiosk-style system in an operating room. The other thing to note is that automatic remediation will try to apply the appropriate Microsoft security patches, but it will require you to point it to the location of those patches somewhere on the system. If the patch cannot be found, the vulnerability will remain unresolved.



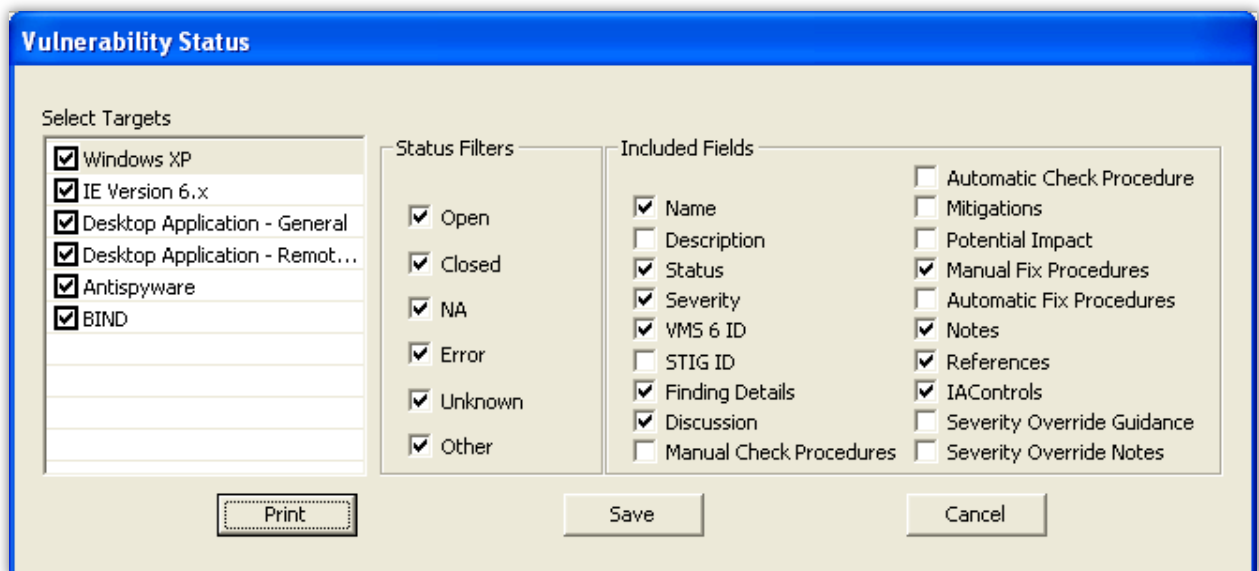
Mitigating the vulnerabilities manually can be a time consuming process, but is a much safer option. The majority of vulnerabilities generally boil down to changing registry values, modifying user accounts, and applying Microsoft patches.

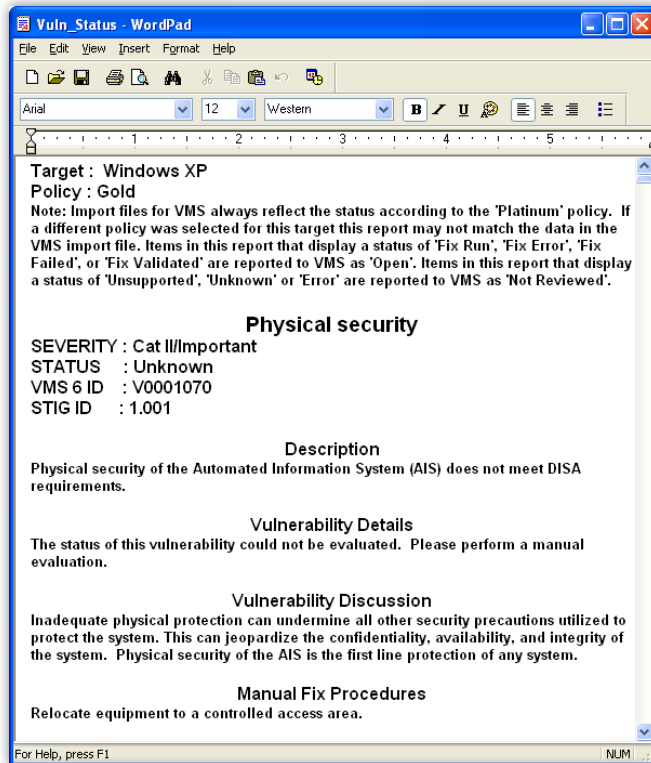
### GENERATING REPORTS

Gold Disk offers two methods for exporting the results of a scan, both of which are found under the “Reports” menu option found along the top of the application.



The “Vulnerability Status” report generates an .rtf file loaded with all the information for each vulnerability the scan produces. Prior to executing the report you have the option of selecting which pieces of information to include.

A screenshot of the 'Vulnerability Status' dialog box. The dialog has a blue title bar and a light beige background. It is divided into three main sections: 'Select Targets', 'Status Filters', and 'Included Fields'.  
**Select Targets:** A list of checkboxes with the following items checked: Windows XP, IE Version 6.x, Desktop Application - General, Desktop Application - Remot..., Antispyware, and BIND.  
**Status Filters:** A list of checkboxes with the following items checked: Open, Closed, NA, Error, Unknown, and Other.  
**Included Fields:** A list of checkboxes with the following items checked: Name, Status, Severity, VMS 6 ID, Finding Details, Discussion, and Manual Check Procedures. Unchecked items include: Description, STIG ID, Automatic Check Procedure, Mitigations, Potential Impact, Manual Fix Procedures, Automatic Fix Procedures, Notes, References, IAControls, Severity Override Guidance, and Severity Override Notes.  
At the bottom of the dialog are three buttons: 'Print', 'Save', and 'Cancel'.



Here is what the resulting file looks like.

The "VMS 6.X" option generates an .xml report similar in format to the Vulnerability Status report. To view this report requires the user to also have 4 supporting files:

- GoldDiskReports.htm
- MROnly\_VMS6\_Display.xslt
- NROnly\_VMS6\_Display.xslt
- VMS6\_Display.xslt

These files are located in the same directory as the PGD.exe file.

David Hubbell  
SPK Software Engineer

