Setting the Security Policies on a Windows 2012 Standard Server

June 13, 2013

Copyright © 2013 by World Class CAD, LLC. All Rights Reserved.

Security for Administrators

While larger companies have their servers secured in secluded and well protected areas, in a small business, servers can be in rooms around other employees. We want to have password security somewhat more complex than what we see on the Internet. We need to set the password policy after loading the computer, the Service Packs and Windows Updates and prior to adding our administrator accounts.



Setup Security Policies

To set the security polices for the Windows 2012 Standard Server, we select the Server Manager button and select Tools. From the list we choose Local Security Policies.



a	Server M	anager		
Set of the set of	bard	• 🗇 🖡	Manage Too	
 ■ Dashboard ■ Local Server ■ All Servers ■ File and Storage Services ▷ 	Roles: 1 Server groups: 1 Servers total: File and Storage 1 O Manageability Events Performance BPA results	_	1 A T Ev Se Pe Bi	Component Services Computer Management Defragment and Optimize Drives Event Viewer iSCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Security Configuration Wizard Services System Configuration Wizard Services System Information Task Scheduler Windows Firewall with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell (x86) Windows PowerShell ISE

Local Security Policies

The Local Security Policies window will open. In the left pane, we select Account Policies and then Password Policies. A list of Password Policies will appear in the right pane.



The Password Policy

There are six polices under the Password Policy heading.

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirement
- Store passwords using reversible encryption

Enforce Password History

Password history is a policy that keeps individuals from toggling with just a handful or two different passwords. Many people juggle between two or three passwords to fool the poorly setup server. For example, the first password can be R1PVanWinkle and the second secret phrase is StOryBOard21. If we do not enforce the password remembered variable, they can just toggle between the two every 30 days.

The default for password history is 0, however we will change the number to the maximum of 24.



Explanation of the Policy

For most policies dialogue boxes in a Windows Server, we can opt to choose the Explain tab and read about the default setting and what the policy will do. For new server managers, it is a good idea to take the time and read about the policy in full and not to just follow a checklist made by others. That way when we need to alter our standard server settings or respond to a security issue, we know where to look on the server and what policy setting can affect the users.



Maximum Password Age

Maximum password age can range between 1 to 999 days. One day is extreme and nearly a thousand days, we might as well keep the password permanent. Many professionals believe that 15 to 30 days range is appropriate.

The system default is 42 days, however, we will require the staff to change their password every 30 days.

Maxin	num pass	word age	Properties	?	x
Local Security Setting	Explain				
Maximum pas	ssword age				
Password will expir					
		ОК	Cancel	Ap	ply

Minimum Password Age

Minimum password age can range between 1 to 998 days. By increasing the number of days, we can help enforce the time until the computer user return to their favorite password. If this is a problem in your department, we can increase the number of days to 29, one below the maximum days we set.

The system default is 1 day, and we will keep the personnel from changing their password for one day.

Minimum p	assword age	Properties	?	x
Local Security Setting Explain				
Minimum password ag	je			
Password can be changed 1 days	after:			
	ОК	Cancel	Ap	ply

Minimum Password Length

Minimum password length is one of the two policies that help us create a smart password criteria. We need at least 6 characters and then we want those symbols to be upper case, lower case letters, numbers and special characters.

We will set the password to 7 characters which also happens to be the default setting for Domain Controllers.

Minimum password length Properties ? ×
Local Security Setting Explain
Minimum password length
Password must be at least: T characters
OK Cancel <u>A</u> pply

Password Must Meet Complexity Requirement

Password must meet complexity requirement is the second of the two policies that help us create a smart password. We need to enable the regulation and then we will have to have three of the four criteria which are upper case, lower case letters, numbers and special characters in the password.

We will enable the rule.



Store Passwords Using Reversible Encryption

Only used in cases where applications need knowledge of user's passwords. We should leave the policy disabled unless required by a server application.

Default setting is disabled and we will keep it that way.

Store passwords using reversible encryption Prope ?	x
Local Security Setting Explain	
Store passwords using reversible encryption	
 <u>E</u>nabled <u>Disabled</u> 	
OK Cancel Apply	

The Local Security Password Settings

1	Local Security Policy	_ D X
Eile Action View Help Security Settings Account Policies Password Policy Account Lockout Policy Local Policies Network List Manager Policies Public Key Policies Software Restriction Policies Software Restriction Policies Mplication Control Policies IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Store passwords using reversible encryption	Security Setting 24 passwords remember 30 days 1 days 7 characters Enabled Disabled
	<u>.</u>	

We can observe all of our password security changes in the right pane.

Export the Local Security Policy Password Settings

Eile Action View elp Image: Security Settings Account Policies Password Policy Account Lockout Policy Account Lockout Policy Account Lockout Policies Windows Firewall with Advanced Sect Network List Manager Policies Public Key Policies Software Restriction Policies IP Security Policies on Local Compute Advanced Audit Policy Configuration		Local Security Policy	_ D X
	 Security Settings Account Policies Password Policy Account Lockout Policy Account Lockout Policy Local Policies Windows Firewall with Advanced Security Network List Manager Policies Public Key Policies Software Restriction Policies Software Restriction Policies IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Enforce password history Maximum password age Minimum password age Minimum password length Password must meet complexity requirements	24 passwords remember 30 days 1 days 7 characters Enabled

To export the settings to a text file, we push the Export icon at the top of the window.

Export List

We save the file to the Server's My Documents folder. We can open the text file and we can put the information in our Disaster Recovery Plan (DRP) folder or procedure file so that we can have the data on hand if we need to setup the server again.

Password polic
<u>F</u> ile <u>E</u> dit F <u>o</u> rmat <u>V</u> iew <u>H</u> elp
Policy Security Setting
Enforce password history 24 passwords re
Maximum password age 30 days
Minimum password age 1 days
Minimum password length 7 characters 📃
Password must meet complexity requirements E
Store passwords using reversible encryption

