

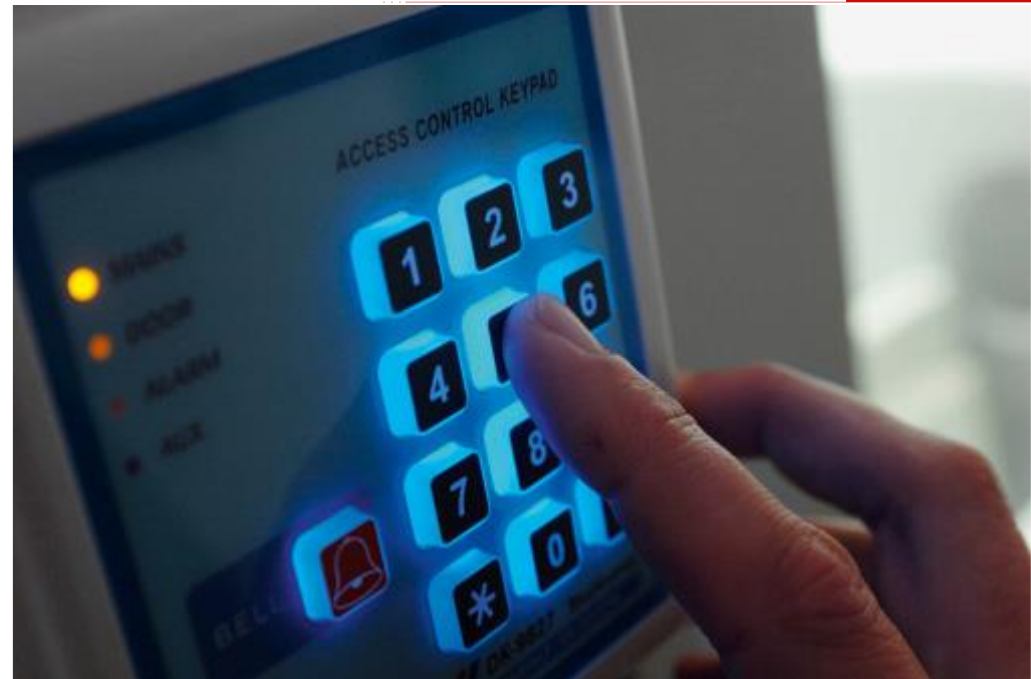


Security Assessment

RSOP Computer Settings Report

Prepared for: My IT Client

Prepared by: YourIT Company

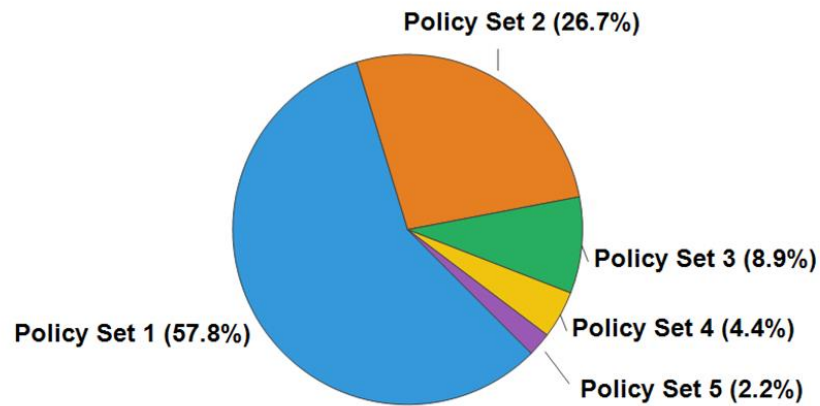


CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Summary

This report analyzes the various Resultant Sets of Policy (RSOP) based on user settings on computers in the environment and helps point out commonalities in the sets and which users / computer combinations have the configurations applied.

Policy Set Utilization



Policy Set Utilization	Total	Percent
Policy Set 1	26	57.8%
Policy Set 2	12	26.7%
Policy Set 3	4	8.9%
Policy Set 4	2	4.4%
Policy Set 5	1	2.2%
Total	45	100%
Overall Total	45	100%

Policy Sets

A policy set represents a common set of policy settings that are shared by multiple users and computer combinations. The color coding in the table below helps you quickly identify similarities between policy sets.

Policy Setting	Policy Sets				
	1	2	3	4	5
ClearTextPassword	Not Enabled	Not Enabled	Not Enabled	Not Enabled	Not Enabled
ForceLogoffWhenHourExpire	Not Enabled	Not Enabled	Not Enabled	Not Enabled	Not Enabled
Groupname	Remote Desktop Users				Remote Desktop Users
InteractiveLogonRight	Administrators Everyone PIT\Domain Admins				Administrators Everyone PIT\Domain Admins
LockoutBadCount	4	4	4	4	4
LockoutDuration	4294967295	4294967295	4294967295	4294967295	4294967295
LSAAnonymousNameLookup	Not Enabled	Not Enabled	Not Enabled	Not Enabled	Not Enabled
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\InactivityTimeoutSecs	500	500	500	500	500
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	1				1
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash	1	1	1	1	1
MaximumPasswordAge	90	90	90	90	90
Members	PIT\Domain Users PIT\Domain Admins				PIT\Domain Users PIT\Domain Admins
MinimumPasswordAge	2	2	2	2	2
MinimumPasswordLength	12	12	12	12	12



Policy Setting	Policy Sets				
	1	2	3	4	5
NetworkLogonRight	Administrators Everyone				Administrators Everyone
PasswordComplexity	Enabled	Enabled	Enabled	Enabled	Enabled
PasswordHistorySize	24	24	24	24	24
RequireLogonToChangePassword	Not Enabled	Not Enabled	Not Enabled	Not Enabled	Not Enabled
ResetLockoutCount	30	30	30	30	30
Software\Policies\Microsoft\Power\PowerSettings\94ac6d29-73ce-41a6-809f-6363ba21b47e\ACSettingIndex	0	0	0	0	0
Software\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab\ACSettingIndex	0	0	0	0	0
Software\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94ea-171b0ed546ab\DCSettingIndex	1	1	1	1	1
Software\Policies\Microsoft\Power\PowerSettings\ActivePowerScheme	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c	8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c
SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\010103000F0000F0010000000F0000F0C967A3643C3AD745950DA7859209176EF5B87C875FA20DF21951640E807D7C24\Category	1	1	1	1	1
Software\Policies\Microsoft\Windows NT\Terminal Services\DenyTSConnections	0			0	0
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\AllowDefaultCredentials			1		
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\AllowDefaultCredentials\HyperVMig			Microsoft Virtual System Migration Service/*		



Policy Setting	Policy Sets				
	1	2	3	4	5
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\AllowDefCredentia			1		
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\AllowDefCredentia			Microsoft Virtual System Migration Service/*		
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\ConcatenateDefaults_AllowDefault			1		
SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation\ConcatenateDefaults_AllowDefNTLMOnly			1		
SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\AllowAutoConfig	1	1	1	1	1
SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\IPv4Filter	*	*	*	*	*
SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\IPv6Filter	*	*	*	*	*
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\DefaultInboundAction					0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\DefaultOutboundAction					0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\EnableFirewall	1	1	1	1	1
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowInboundEchoRequest	1	1	1	1	1
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowInboundMaskRequest	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowInboundRouterRequest	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowInboundTimestampRequest	0	0	0	0	0



Policy Setting	Policy Sets				
	1	2	3	4	5
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowOutboundDestinationUnreachable	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowOutboundPacketTooBig	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowOutboundParameterProblem	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowOutboundSourceQuench	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowOutboundTimeExceeded	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\IcmpSettings\AllowRedirect	0	0	0	0	0
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\RemoteAdminSettings\Enabled	1	1	1	1	1
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\RemoteAdminSettings\RemoteAddresses	10.0.0.0/24	10.0.0.0/24	10.0.0.0/24	10.0.0.0/24	10.0.0.0/24
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint\Enabled	1	1	1	1	1
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\FileAndPrint\RemoteAddresses	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\RemoteDesktop\Enabled	1	1	1	1	1
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\Services\RemoteDesktop\RemoteAddresses	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21	10.0.0.0/21
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\{9A4897C3-82EA-46E6-B6A5-FB7161E0AF39}	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=59	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=59	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=59	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=59	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=59

Policy Setting	Policy Sets				
	1	2	3	4	5
	86 Name=W SMAN	86 Name=W SMAN	86 Name=W SMAN	86 Name=W SMAN	86 Name=W SMAN
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS- NB_Name-In-UDP	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=1 7 LPort=137 App=System Name=@Fir ewallAPI.dll,- 28519 Desc= @FirewallAP I.dll,- 28522 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=1 7 LPort=137 App=System Name=@Fir ewallAPI.dll,- 28519 Desc= @FirewallAP I.dll,- 28522 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=1 7 LPort=137 App=System Name=@Fir ewallAPI.dll,- 28519 Desc= @FirewallAP I.dll,- 28522 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=1 7 LPort=137 App=System Name=@Fir ewallAPI.dll,- 28519 Desc= @FirewallAP I.dll,- 28522 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=1 7 LPort=137 App=System Name=@Fir ewallAPI.dll,- 28519 Desc= @FirewallAP I.dll,- 28522 Embe dCtxt=@Fire wallAPI.dll,- 28502
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS- NB_Session-In-TCP	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 LPort=139 A pp=System Name=@Fir ewallAPI.dll,- 28503 Desc= @FirewallAP I.dll,- 28506 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 LPort=139 A pp=System Name=@Fir ewallAPI.dll,- 28503 Desc= @FirewallAP I.dll,- 28506 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 LPort=139 A pp=System Name=@Fir ewallAPI.dll,- 28503 Desc= @FirewallAP I.dll,- 28506 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 LPort=139 A pp=System Name=@Fir ewallAPI.dll,- 28503 Desc= @FirewallAP I.dll,- 28506 Embe dCtxt=@Fire wallAPI.dll,- 28502	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 LPort=139 A pp=System Name=@Fir ewallAPI.dll,- 28503 Desc= @FirewallAP I.dll,- 28506 Embe dCtxt=@Fire wallAPI.dll,- 28502
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\FPS- SMB-In-TCP	v2.26 Action =Allow Active =TRUE Dir=I	v2.26 Action =Allow Active =TRUE Dir=I	v2.26 Action =Allow Active =TRUE Dir=I	v2.26 Action =Allow Active =TRUE Dir=I	v2.26 Action =Allow Active =TRUE Dir=I



Policy Setting	Policy Sets				
	1	2	3	4	5
	n Protocol=6 LPort=445 App=System Name=@FirewallAPI.dll,-28511 Desc=@FirewallAPI.dll,-28514 EmbedCtxt=@FirewallAPI.dll,-28502	n Protocol=6 LPort=445 App=System Name=@FirewallAPI.dll,-28511 Desc=@FirewallAPI.dll,-28514 EmbedCtxt=@FirewallAPI.dll,-28502	n Protocol=6 LPort=445 App=System Name=@FirewallAPI.dll,-28511 Desc=@FirewallAPI.dll,-28514 EmbedCtxt=@FirewallAPI.dll,-28502	n Protocol=6 LPort=445 App=System Name=@FirewallAPI.dll,-28511 Desc=@FirewallAPI.dll,-28514 EmbedCtxt=@FirewallAPI.dll,-28502	n Protocol=6 LPort=445 App=System Name=@FirewallAPI.dll,-28511 Desc=@FirewallAPI.dll,-28514 EmbedCtxt=@FirewallAPI.dll,-28502
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WINRM-HTTP-In-TCP	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain Profile=Private LPort=5985 App=System Name=@FirewallAPI.dll,-30253 Desc=@FirewallAPI.dll,-30256 EmbedCtxt=@FirewallAPI.dll,-30267	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain Profile=Private LPort=5985 App=System Name=@FirewallAPI.dll,-30253 Desc=@FirewallAPI.dll,-30256 EmbedCtxt=@FirewallAPI.dll,-30267	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain Profile=Private LPort=5985 App=System Name=@FirewallAPI.dll,-30253 Desc=@FirewallAPI.dll,-30256 EmbedCtxt=@FirewallAPI.dll,-30267	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain Profile=Private LPort=5985 App=System Name=@FirewallAPI.dll,-30253 Desc=@FirewallAPI.dll,-30256 EmbedCtxt=@FirewallAPI.dll,-30267	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain Profile=Private LPort=5985 App=System Name=@FirewallAPI.dll,-30253 Desc=@FirewallAPI.dll,-30256 EmbedCtxt=@FirewallAPI.dll,-30267
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-ASYNC-In-TCP-NoScope	v2.20 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Dom	v2.20 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Dom	v2.20 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Dom	v2.20 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Dom	v2.20 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Dom



Policy Setting	Policy Sets				
	1	2	3	4	5
	ain LA4=10.0 .5.126 LA4=1 0.0.6.129 LA 4=10.0.5.48 LA4=10.0.5.3 2 LA4=10.0.5 .34 LA4=10.0 .5.122 LA4=1 0.0.5.123 LA 4=10.0.5.64 LA4=10.0.5.7 0 LA4=10.0.5 .72 RA4=10. 0.5.126 RA4 =10.0.6.129 RA4=10.0.5. 48 RA4=10.0 .5.32 RA4=1 0.0.5.34 RA4 =10.0.5.122 RA4=10.0.5. 123 RA4=10. 0.5.64 RA4= 10.0.5.70 RA 4=10.0.5.72 App=%system root%\system32\wbem\ unsecapp.exe Name=@Fi rewallAPI.dll, - 34256 Desc= @FirewallAP I.dll,- 34257 Embe	ain LA4=10.0 .5.126 LA4=1 0.0.6.129 LA 4=10.0.5.48 LA4=10.0.5.3 2 LA4=10.0.5 .34 LA4=10.0 .5.122 LA4=1 0.0.5.123 LA 4=10.0.5.64 LA4=10.0.5.7 0 LA4=10.0.5 .72 RA4=10. 0.5.126 RA4 =10.0.6.129 RA4=10.0.5. 48 RA4=10.0 .5.32 RA4=1 0.0.5.34 RA4 =10.0.5.122 RA4=10.0.5. 123 RA4=10. 0.5.64 RA4= 10.0.5.70 RA 4=10.0.5.72 App=%system root%\system32\wbem\ unsecapp.exe Name=@Fi rewallAPI.dll, - 34256 Desc= @FirewallAP I.dll,- 34257 Embe	ain LA4=10.0 .5.126 LA4=1 0.0.6.129 LA 4=10.0.5.48 LA4=10.0.5.3 2 LA4=10.0.5 .34 LA4=10.0 .5.122 LA4=1 0.0.5.123 LA 4=10.0.5.64 LA4=10.0.5.7 0 LA4=10.0.5 .72 RA4=10. 0.5.126 RA4 =10.0.6.129 RA4=10.0.5. 48 RA4=10.0 .5.32 RA4=1 0.0.5.34 RA4 =10.0.5.122 RA4=10.0.5. 123 RA4=10. 0.5.64 RA4= 10.0.5.70 RA 4=10.0.5.72 App=%system root%\system32\wbem\ unsecapp.exe Name=@Fi rewallAPI.dll, - 34256 Desc= @FirewallAP I.dll,- 34257 Embe	ain LA4=10.0 .5.126 LA4=1 0.0.6.129 LA 4=10.0.5.48 LA4=10.0.5.3 2 LA4=10.0.5 .34 LA4=10.0 .5.122 LA4=1 0.0.5.123 LA 4=10.0.5.64 LA4=10.0.5.7 0 LA4=10.0.5 .72 RA4=10. 0.5.126 RA4 =10.0.6.129 RA4=10.0.5. 48 RA4=10.0 .5.32 RA4=1 0.0.5.34 RA4 =10.0.5.122 RA4=10.0.5. 123 RA4=10. 0.5.64 RA4= 10.0.5.70 RA 4=10.0.5.72 App=%system root%\system32\wbem\ unsecapp.exe Name=@Fi rewallAPI.dll, - 34256 Desc= @FirewallAP I.dll,- 34257 Embe	ain LA4=10.0 .5.126 LA4=1 0.0.6.129 LA 4=10.0.5.48 LA4=10.0.5.3 2 LA4=10.0.5 .34 LA4=10.0 .5.122 LA4=1 0.0.5.123 LA 4=10.0.5.64 LA4=10.0.5.7 0 LA4=10.0.5 .72 RA4=10. 0.5.126 RA4 =10.0.6.129 RA4=10.0.5. 48 RA4=10.0 .5.32 RA4=1 0.0.5.34 RA4 =10.0.5.122 RA4=10.0.5. 123 RA4=10. 0.5.64 RA4= 10.0.5.70 RA 4=10.0.5.72 App=%system root%\system32\wbem\ unsecapp.exe Name=@Fi rewallAPI.dll, - 34256 Desc= @FirewallAP I.dll,- 34257 Embe

Policy Setting	Policy Sets				
	1	2	3	4	5
	dCtxt=@FirewallAPI.dll,-34251	dCtxt=@FirewallAPI.dll,-34251	dCtxt=@FirewallAPI.dll,-34251	dCtxt=@FirewallAPI.dll,-34251	dCtxt=@FirewallAPI.dll,-34251
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-RPCSS-In-TCP-NoScope	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=135 RA4=10.0.6.129 RA4=10.0.5.126 RA4=10.0.5.105 RA4=10.0.5.172 RA4=10.0.5.72 RA4=10.0.5.39 RA4=10.0.5.34 RA4=10.0.5.118 RA4=10.0.5.89 RA4=10.0.5.48 RA4=10.0.5.64 RA4=10.0.5.19 RA4=10.0.5.102 RA4=10.0.5.42 App=%SystemRoot%\system32\svchost.exe Svc=rpcss Name=@FirewallAPI.dll,-34252 Desc=@FirewallAP	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=135 RA4=10.0.6.129 RA4=10.0.5.126 RA4=10.0.5.105 RA4=10.0.5.172 RA4=10.0.5.72 RA4=10.0.5.39 RA4=10.0.5.34 RA4=10.0.5.118 RA4=10.0.5.89 RA4=10.0.5.48 RA4=10.0.5.64 RA4=10.0.5.19 RA4=10.0.5.102 RA4=10.0.5.42 App=%SystemRoot%\system32\svchost.exe Svc=rpcss Name=@FirewallAPI.dll,-34252 Desc=@FirewallAP	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=135 RA4=10.0.6.129 RA4=10.0.5.126 RA4=10.0.5.105 RA4=10.0.5.172 RA4=10.0.5.72 RA4=10.0.5.39 RA4=10.0.5.34 RA4=10.0.5.118 RA4=10.0.5.89 RA4=10.0.5.48 RA4=10.0.5.64 RA4=10.0.5.19 RA4=10.0.5.102 RA4=10.0.5.42 App=%SystemRoot%\system32\svchost.exe Svc=rpcss Name=@FirewallAPI.dll,-34252 Desc=@FirewallAP	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=135 RA4=10.0.6.129 RA4=10.0.5.126 RA4=10.0.5.105 RA4=10.0.5.172 RA4=10.0.5.72 RA4=10.0.5.39 RA4=10.0.5.34 RA4=10.0.5.118 RA4=10.0.5.89 RA4=10.0.5.48 RA4=10.0.5.64 RA4=10.0.5.19 RA4=10.0.5.102 RA4=10.0.5.42 App=%SystemRoot%\system32\svchost.exe Svc=rpcss Name=@FirewallAPI.dll,-34252 Desc=@FirewallAP	v2.26 Action=Allow Active=TRUE Dir=In Protocol=6 Profile=Domain LPort=135 RA4=10.0.6.129 RA4=10.0.5.126 RA4=10.0.5.105 RA4=10.0.5.172 RA4=10.0.5.72 RA4=10.0.5.39 RA4=10.0.5.34 RA4=10.0.5.118 RA4=10.0.5.89 RA4=10.0.5.48 RA4=10.0.5.64 RA4=10.0.5.19 RA4=10.0.5.102 RA4=10.0.5.42 App=%SystemRoot%\system32\svchost.exe Svc=rpcss Name=@FirewallAPI.dll,-34252 Desc=@FirewallAP

Policy Setting	Policy Sets				
	1	2	3	4	5
	I.dll,- 34253 EmbedCtxt=@Fire wallAPI.dll,- 34251	I.dll,- 34253 EmbedCtxt=@Fire wallAPI.dll,- 34251	I.dll,- 34253 EmbedCtxt=@Fire wallAPI.dll,- 34251	I.dll,- 34253 EmbedCtxt=@Fire wallAPI.dll,- 34251	I.dll,- 34253 EmbedCtxt=@Fire wallAPI.dll,- 34251
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules\WMI-WINMGMT-In-TCP-NoScope	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 Profile=Dom ain RA4=10. 0.6.129 RA4 =10.0.5.126 RA4=10.0.5. 105 RA4=10. 0.5.72 RA4= 10.0.5.172 R A4=10.0.5.39 RA4=10.0.5. 34 RA4=10.0 .5.118 RA4= 10.0.5.89 RA 4=10.0.5.48 RA4=10.0.5. 64 RA4=10.0 .5.19 RA4=1 0.0.5.102 RA 4=10.0.5.42 App=%Syste mRoot%\syst em32\svchos t.exe Svc=wi nmgmt Nam e=@Firewall API.dll,- 34254 Desc=	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 Profile=Dom ain RA4=10. 0.6.129 RA4 =10.0.5.126 RA4=10.0.5. 105 RA4=10. 0.5.72 RA4= 10.0.5.172 R A4=10.0.5.39 RA4=10.0.5. 34 RA4=10.0 .5.118 RA4= 10.0.5.89 RA 4=10.0.5.48 RA4=10.0.5. 64 RA4=10.0 .5.19 RA4=1 0.0.5.102 RA 4=10.0.5.42 App=%Syste mRoot%\syst em32\svchos t.exe Svc=wi nmgmt Nam e=@Firewall API.dll,- 34254 Desc=	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 Profile=Dom ain RA4=10. 0.6.129 RA4 =10.0.5.126 RA4=10.0.5. 105 RA4=10. 0.5.72 RA4= 10.0.5.172 R A4=10.0.5.39 RA4=10.0.5. 34 RA4=10.0 .5.118 RA4= 10.0.5.89 RA 4=10.0.5.48 RA4=10.0.5. 64 RA4=10.0 .5.19 RA4=1 0.0.5.102 RA 4=10.0.5.42 App=%Syste mRoot%\syst em32\svchos t.exe Svc=wi nmgmt Nam e=@Firewall API.dll,- 34254 Desc=	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 Profile=Dom ain RA4=10. 0.6.129 RA4 =10.0.5.126 RA4=10.0.5. 105 RA4=10. 0.5.72 RA4= 10.0.5.172 R A4=10.0.5.39 RA4=10.0.5. 34 RA4=10.0 .5.118 RA4= 10.0.5.89 RA 4=10.0.5.48 RA4=10.0.5. 64 RA4=10.0 .5.19 RA4=1 0.0.5.102 RA 4=10.0.5.42 App=%Syste mRoot%\syst em32\svchos t.exe Svc=wi nmgmt Nam e=@Firewall API.dll,- 34254 Desc=	v2.26 Action =Allow Active =TRUE Dir=I n Protocol=6 Profile=Dom ain RA4=10. 0.6.129 RA4 =10.0.5.126 RA4=10.0.5. 105 RA4=10. 0.5.72 RA4= 10.0.5.172 R A4=10.0.5.39 RA4=10.0.5. 34 RA4=10.0 .5.118 RA4= 10.0.5.89 RA 4=10.0.5.48 RA4=10.0.5. 64 RA4=10.0 .5.19 RA4=1 0.0.5.102 RA 4=10.0.5.42 App=%Syste mRoot%\syst em32\svchos t.exe Svc=wi nmgmt Nam e=@Firewall API.dll,- 34254 Desc=

Policy Setting	Policy Sets				
	1	2	3	4	5
	@ FirewallAPI.dll,-34255 EmbeddedCtxt=@FirewallAPI.dll,-34251	@ FirewallAPI.dll,-34255 EmbeddedCtxt=@FirewallAPI.dll,-34251	@ FirewallAPI.dll,-34255 EmbeddedCtxt=@FirewallAPI.dll,-34251	@ FirewallAPI.dll,-34255 EmbeddedCtxt=@FirewallAPI.dll,-34251	@ FirewallAPI.dll,-34255 EmbeddedCtxt=@FirewallAPI.dll,-34251
SOFTWARE\Policies\Microsoft\WindowsFirewall\PolicyVersion	539	539	539	539	539
Utilization	57.8%	26.7%	8.9%	4.4%	2.2%
Instances	26	12	4	2	1

Policy Set Utilization

The policy set utilization table shows which policy sets are in use by each user and on which corresponding computers. Only computers that a user logs into are shown in policy set utilization table.

User	Policy Sets					Exceptions
	1	2	3	4	5	
DESKTOP-DUJTHSR\USER	DESKTOP-DUJTHSR					
DESKTOP-J8T7SRK\USER	DESKTOP-J8T7SRK					
DESKTOP-JSMM8F4\USER	DESKTOP-JSMM8F4					
DESKTOP-O7URO65\USER	DESKTOP-O7URO65					
DESKTOP-SN53S6E\USER	DESKTOP-SN53S6E					
DESKTOP-V9U4SOT\USER				DESKTOP-V9U4SOT		
PIT\AD.BROWN	DESKTOP-72AR7RV DESKTOP-HPBDIGN DESKTOP-JSMM8F4 SALE-003	RFHVDS2 VPNGW	RFHVDS			
PIT\AD.DOLAN	DESKTOP-72AR7RV	RFHVDS2 VPNGW	RFHVDS			
PIT\AD.SAUNDERS	DESKTOP-SN53S6E					
PIT\ADMINISTRATOR		VPNGW				



User	Policy Sets					
	1	2	3	4	5	Exceptions
PIT\BJONES	DESKTOP-O7URO65					
PIT\BOSIER		VPNGW				
PIT\CHODGE	DESKTOP-DE32156					
PIT\DBROWN	DESKTOP-J8T7SRK DESKTOP-SN53S6E	RFHVDS2 VPNGW	RFHVDS			
PIT\DDEMILLE	DESKTOP-JSMM8F4					
PIT\JBRUMLEVE					JUSTINB-PC	
PIT\JDOLAN	DESKTOP-72AR7RV					
PIT\JPETERS	DESKTOP-C4TVJMF					
PIT\JSTOUDENMIRE	DESKTOP-J8T7SRK					
PIT\JVALDES	SALE-003					
PIT\JWEAKLAND	DESKTOP-6ND4Q8O					
PIT\JWEINER				DESKTOP-V9U4SOT		
PIT\MCOURTNEY	DESKTOP-SN53S6E					
PIT\MGRINBERG	PITSPARE001					
PIT\MITTEL	DESKTOP-RMKC7AF					
PIT\MPORTANKA		VPNGW				



User	Policy Sets					Exceptions
	1	2	3	4	5	
PIT\PMURPHY	DESKTOP-N6S4H9A					
PIT\PSOLER		VPNGW				
RFHVDS\ADMINISTRATOR			RFHVDS			
RFHVDS2\ADMINISTRATOR			RFHVDS2			
SALE-003\USER	SALE-003					
VPNGW\ADMINISTRATOR		VPNGW				



Policy Exceptions

Policy exceptions show variants of the policy sets in use. These are policy sets that are minor variations to the most popular policy sets. When possible, the variants are compared to the closest matching policy set.

No Policy Exceptions Detected.