Security Assessment & System Review

VERTEKS
VOICE & DATA
NETWORKS

For:

Drafted by:
Pete Kamay
Verteks Consulting, Inc.
2102 SW 20th Place, Suite 602
Ocala, FL 34471
352-401-0909

TABLE OF CONTENTS

I. Recommendations

Recommendations Summary

In summary, here are our recommendations for security improvements to your IT infrastructure:

High Priority

- Review failed login attempts on your servers. You have several servers with over 100 failed login attempts in the last 30 days. This volume is attributable to either external penetration attempts or a bad stored password. Invalid stored passwords prevent vital services from operating correctly and affect your productivity.
- Your current Exchange Server certificate configuration is using SSL2, a very outdated encryption methodology that is leaves your network vulnerable to multiple malware attacks including the "Drown Attack." You need to upgrade to a newer certificate that supports TLS encryption that will support newer protocols. This will also block system protocols from being sent outbound and support forwarding secrecy – two vital security components that are not currently supported through your certificate security protocols.
- Update end of life operating systems. You have 15 Server 2003 and two Windows XP active systems on your network. Both operating systems reached end of life several years ago and no longer have security/vulnerability patching available. Many external malware and ransomware attacks are targeting out of date operating systems as the most vulnerable point of egress on a network.
- Update your password policy to meet compliance standards. You have 880 accounts set to "Never Expire" and have a policy in place with no password complexity and a maximum age of 180 days. Microsoft Best Practices dictates that at minimum password complexity should be applied as well as a maximum password age of 90 days. Passwords older than 90 days are more vulnerable to password cracking tools.
- All units on your network need to have up to date managed antivirus installed. 11 workstations currently have no reporting antivirus solution.
- Implement Web Filtering. All of your network workstations have unlimited access to the Internet from simple time wasting game/social media sites to more dangerous warez/pornography sites. We recommend a firewall solution that will allow you to control what your users are allowed to visit as well as to generate reports of current website usage for all users.

- Block insecure listening ports. Ports such as Telnet and FTP that by default are usually blocked/disabled on workstations are open on 27 of your PCs. Commonly used ports are frequently scanned by outside intruders to find an opening into the network. All ports that are not actively being used should by blocked by policy.
- Maintain up to date security patching on all servers and workstations. Your Exchange Server has 77 unapplied critical updates. Critical updates prevent threats from affecting your server. Unapplied updates leave these units vulnerable to thousands of malware incursions.
- Remove inactive users and computers from your Active Directory. You have 815 users and 118 PCs that are part of AD that have not checked into your domain in over 30 days. Inactive accounts are a point of vulnerability for threats, internally and externally.
- RPC is enabled externally. This protocol was used externally with older versions of Exchange for OWA, but has since been made obsolete due to performance and security issues.
- Free up space or increase storage on network resources. The D Drive is reporting 95% full and the [deleted] workstation C Drive is 98% full. This capacity seriously affects the performance of the units and will cause a system failure imminently.

Medium Priority

- Implement a disaster recovery solution with offsite High Availability. Your Acronis solution backs up all of your data, but in the event of an outage in your central facility you cannot maintain server data access to your remote facilities. With offsite server virtualization, you will be able to meet your Recovery Time Objectives (RTO) and keep the other 16 branches running until full core functionality can be restored.
- Demote and remove offline domain controllers from your AD infrastructure. [****] is being seen as a DC, but is not accessible. Offline DCs lead to catalog syncing issues and can cause data loss/corruption.
- Resolve DNS conflicts. You have over 400 listed DNS conflicts listed on your DNS server. Duplicate DNS entries can cause routing problems throughout your network.
- Remove unpopulated Organizational Units (OUs). You have 10 OUs setup with no members. Unused OUs are similar to inactive user accounts that can be used to penetrate your network.

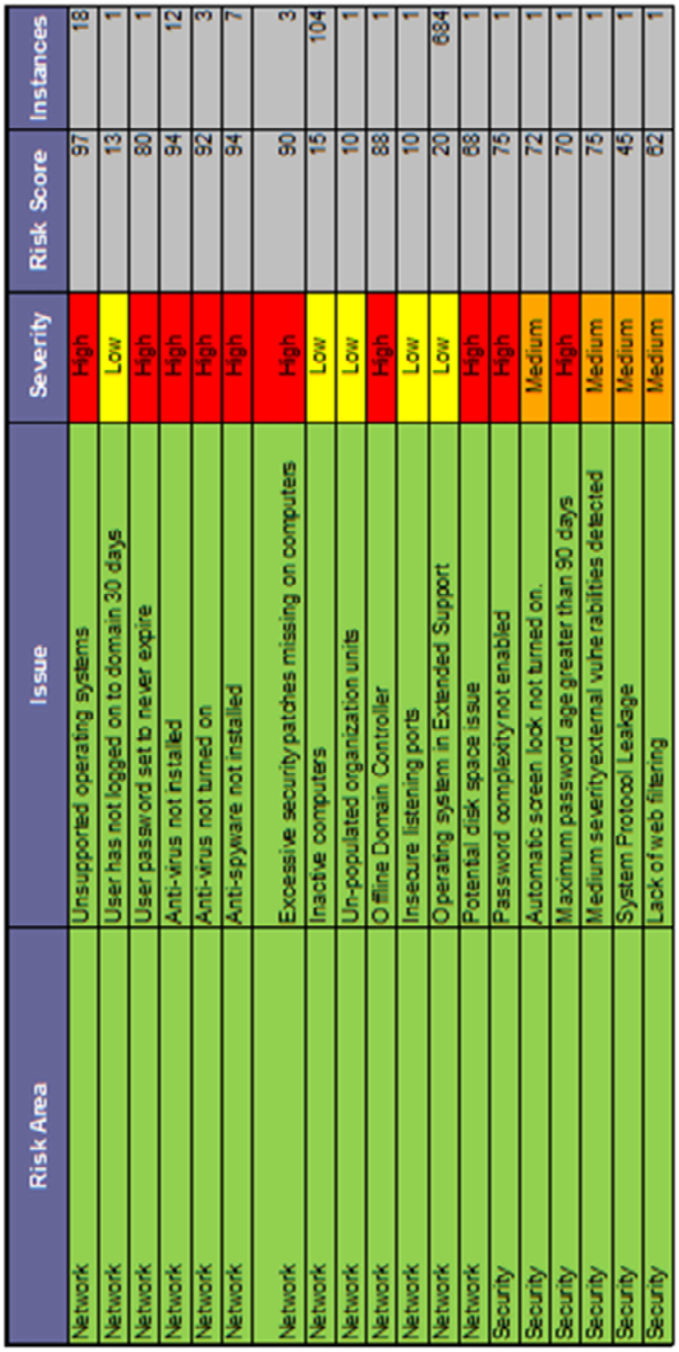
- Implement screen lock timeouts on all of your servers. The [*****] and [*****] servers have no screen lock timeout. Internal network users walking by can have access to private network resources.

Additional Performance Issues

- Disable the autoshrink feature on you SQL servers. Autoshrink has shown that it can caused increased fragmentation on your indexes, causing performance issues on database queries.
- Store your SQL data and log files on different servers to reduce I/O congestion. Database files should also not be stored on the same volume as your OS files. Modifying the location of the data and log files will give you better performance of your SQL data.

II. Consolidated Risk Report

Consolidated Risk Assessment



Risk Area	Issue	Severity	Risk Score	Instances
Network	Unsupported operating systems	High	97	18
Network	User has not logged on to domain 30 days	Low	13	1
Network	User password set to never expire	High	80	1
Network	Anti-virus not installed	High	94	12
Network	Anti-virus not turned on	High	92	3
Network	Anti-spyware not installed	High	94	7
Network	Excessive securitypatches missing on computers	High	90	3
Network	Inactive computers	Low	15	104
Network	Un-populated organization units	Low	10	1
Network	Offline Domain Controller	High	88	1
Network	Insecure listening ports	Low	10	1
Network	Operating system in Extended Support	Low	20	684
Network	Potential disk space issue	High	68	1
Security	Password complexitynot enabled	High	75	1
Security	Automatic screen lock not turned on.	Medium	72	1
Security	Maximum password age greater than 90 days	High	70	1
Security	Medium severityexternal vulnerabilities detected	Medium	75	1
Security	System Protocol Leakage	Medium	45	1
Security	Lack of web filtering	Medium	62	1

III. Network Risk Report

Table of Contents

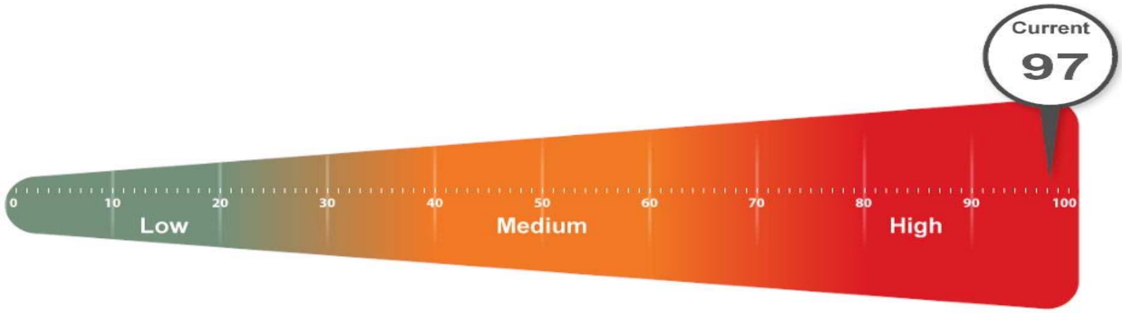
Discovery Tasks

The following discovery tasks were performed:

	Task	Description
✓	Detect Domain Controllers	Identifies domain controllers and online status.
✓	FSMO Role Analysis	Enumerates FSMO roles at the site.
✓	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
✓	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓	Detect Local Mail Servers	Detects mail server(s) on the network.
✓	Detect Time Servers	Detects server(s) on the network.
✓	Discover Network Shares	Discovers the network shares by server.
✓	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓	Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓	Web Server Discovery and Identification	Lists the web servers and type.
✓	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓	Internet Access and Speed Test	Tests the Internet access and performance.
✓	SQL Server Analysis	Lists the SQL Servers and associated database(s).
✗	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓	Password Strength Analysis	Uses MBSA to identify computers with weak passwords that may pose a security risk.
✓	Missing Security Updates	Uses MBSA to identify computers missing security updates.
✓	System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
✓	External Security Vulnerabilities	Lists the security holes and warnings from External Vulnerability Scan.

Risk Score

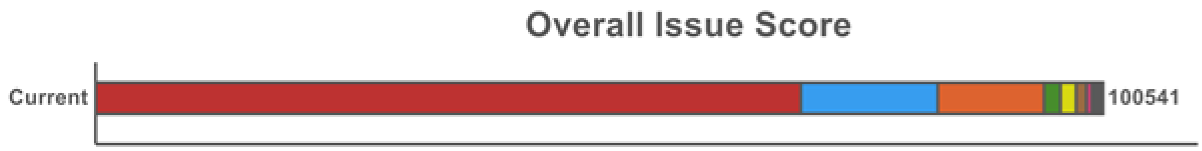
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issues Summary

This section contains a summary of issues detected during the Network Assessment process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Overall Issue Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	User password set to never expire (80 pts each)
70400	***Current Score:*** 80 pts x 880 = 70400: 70.02%
	Issue: User accounts with passwords set to never expire present a risk of use by unauthorized users. They are more easily compromised than passwords that are routinely changed.
	Recommendation: Investigate all accounts with passwords set to never expire and configure them to expire regularly.

	Operating system in Extended Support (20 pts each)
13660	***Current Score:*** 20 pts x 683 = 13660: 13.59%
	Issue: Computers are using an operating system that is in Extended Supported. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.
	Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

	User has not logged on to domain 30 days (13 pts each)
10595	***Current Score:*** 13 pts x 815 = 10595: 10.54%
	Issue: Users that have not logged in in 30 days could be from A user that has not logged in for an extended period of time could be a former employee or vendor.
	Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

	Unsupported operating systems (97 pts each)
1649	***Current Score:*** 97 pts x 17 = 1649: 1.64%

	Issue: Computers found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.
	Recommendation: Upgrade or replace computers with operating systems that are no longer supported.

	Inactive computers (15 pts each)
1545	***Current Score:*** 15 pts x 103 = 1545: 1.54%
	Issue: Computers have not checked in during the past 30 days
	Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, or powered on.

	Anti-virus not installed (94 pts each)
1034	***Current Score:*** 94 pts x 11 = 1034: 1.03%
	Issue: Anti-virus software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: To prevent both security and productivity issues, we strongly recommend ensuring that anti-virus is deployed to all possible endpoints.

	Anti-spyware not installed (94 pts each)
564	***Current Score:*** 94 pts x 6 = 564: 0.56%
	Issue: Anti-spyware software was not detected on some computers. Without adequate anti-virus and anti-spyware protection on all workstations and servers, the risk of acquiring malicious software is significant.
	Recommendation: Assure that anti-spyware is deployed to all possible endpoints in order to prevent both security and productivity issues.

	Potential disk space issue (68 pts each)
272	***Current Score:*** 68 pts x 4 = 272: 0.27%
	Issue: 4 computers were found with significantly low free disk space.
	Recommendation: Free or add additional disk space for the specified drives.

	Insecure listening ports (10 pts each)
270	***Current Score:*** 10 pts x 27 = 270: 0.27%
	Issue: Computers are to be using potentially insecure protocols.
	Recommendation: There may be a legitimate business need, but these risks should be assessed individually. Certain protocols are inherently insecure since they often lack encryption. Inside the network, their use should be minimized as much as possible to prevent the spread of malicious software. Of course, there can be reasons these services are needed

	and other means to protect systems which listen on those ports. We recommend reviewing the programs listening on the network to ensure their necessity and security.

	Anti-virus not turned on (92 pts each)
184	***Current Score:*** 92 pts x 2 = 184: 0.18%
	Issue: We were unable to determine if an anti-virus software is enabled and running on some computers.
	Recommendation: Determine if anti-virus is enabled properly.

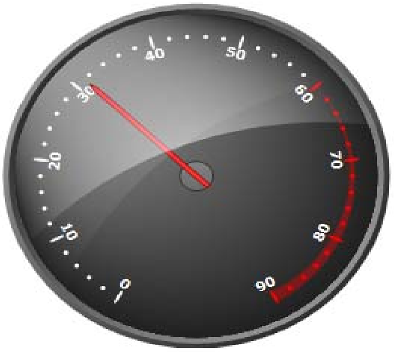
	Excessive security patches missing on computers (90 pts each)
180	***Current Score:*** 90 pts x 2 = 180: 0.18%
	Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Lots is defined as missing three or more patches.
	Recommendation: Address patching on computers with missing security patches.

	Un-populated organization units (10 pts each)
100	***Current Score:*** 10 pts x 10 = 100: 0.1%
	Issue: Empty organizational units (OU) were found in Active Directory. They may not be needed and can lead to misconfiguration.
	Recommendation: Remove or populate empty organizational units.

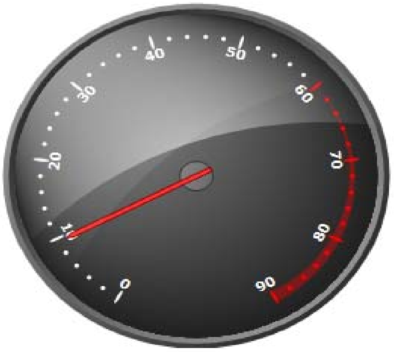
	Offline Domain Controller (88 pts each)
88	***Current Score:*** 88 pts x 1 = 88: 0.09%
	Issue: One or more offline Domain Controller were found. This could either be an indication of an error caused by an improperly de-commissioned Domain Controller or a fail-over condition that should be remediated.
	Recommendation: Investigate all offline Domain Controllers and determine if they need to be properly un-joined from the domain or if they should be brought back online.

Internet Speed Test Results

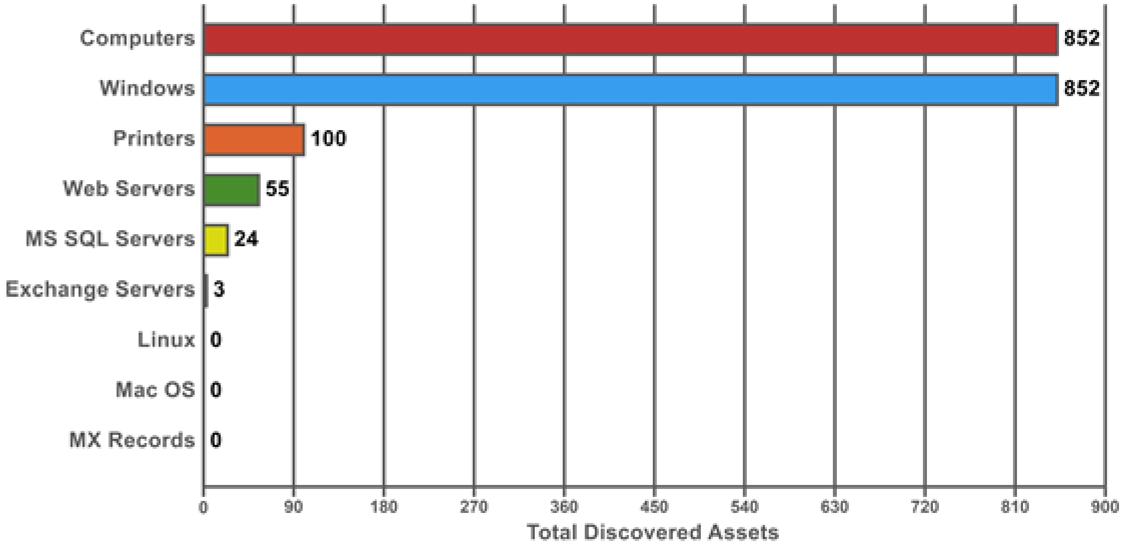
Download Speed: **31.23 Mb/s**



Upload Speed: **9.60 Mb/s**

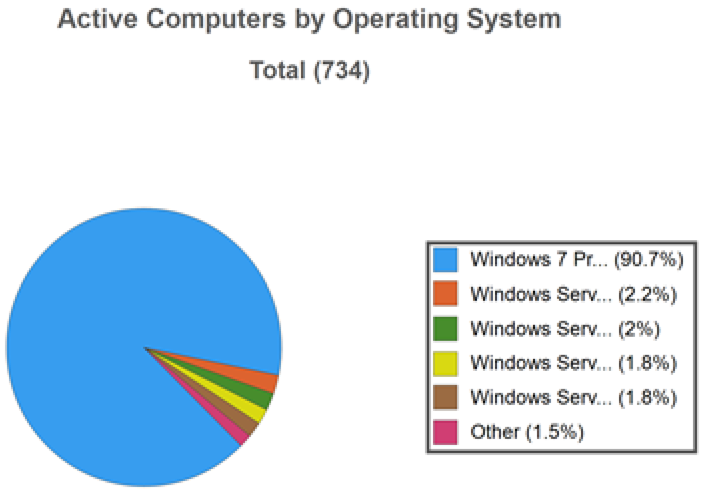


Asset Summary: Total Discovered Assets

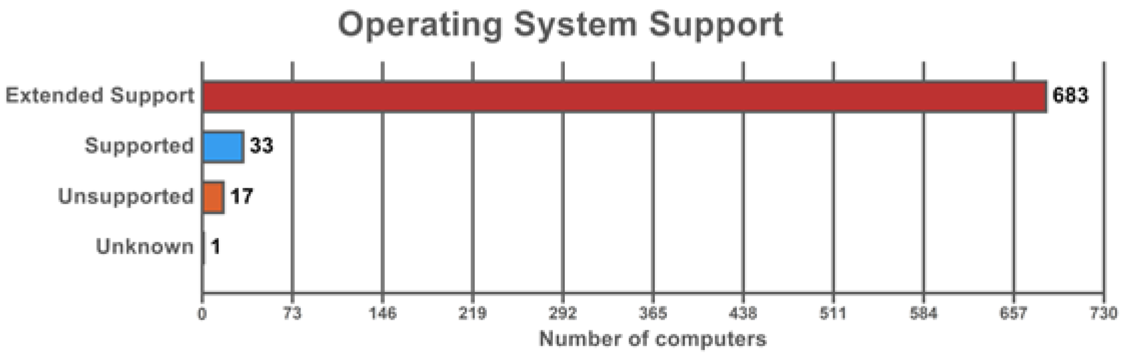


Asset Summary: Active Computers

Active Computers are defined as computers that were either actively responding at the time of the scan or have checked in with Active Directory within the past 30 days.

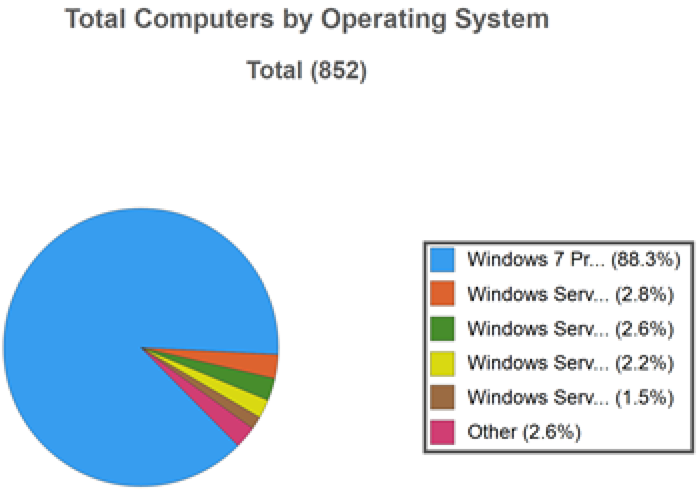


	Operating System	Total	Percent
	Top Five		
🟦	Windows 7 Professional	666	90.7%
🟧	Windows Server 2012 R2 Standard	16	2.2%
🟩	Windows Server 2003	15	2%
🟨	Windows Server 2008 R2 Standard	13	1.8%
🟫	Windows Server 2016 Standard	13	1.8%
	Total - Top Five	**723**	**98.5%**
	Other		
🟥	Windows Server 2008 Standard	5	0.7%
	Windows XP Professional	2	0.3%
	unknown	1	0.1%
	Windows 10 Pro	1	0.1%
	Windows Embedded Standard	1	0.1%
	Windows Server 2012 Standard	1	0.1%
	Total - Other	**11**	**1.5%**
	Overall Total	**734**	**100%**


Operating System Support
Extended Support
Supported
Unsupported
Unknown
683
33
17
1
0
73
146
219
292
365
438
511
584
657
730
Number of computers

Asset Summary: All Computers

The list of all computers includes computers that may no longer be active but have entries in Active Directory (in a domain environment).

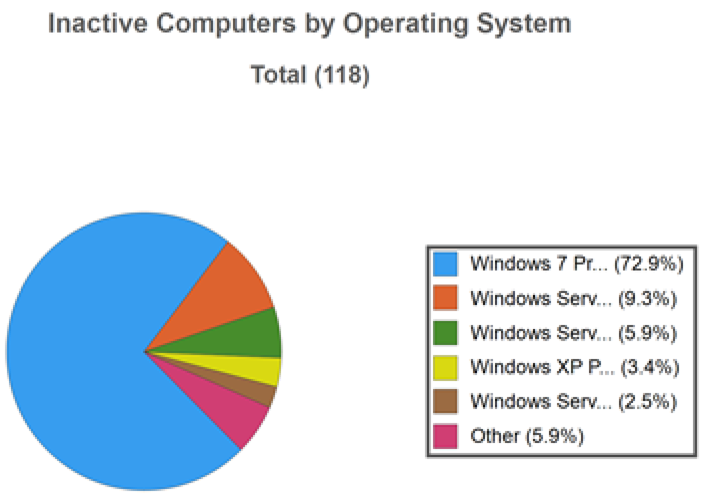


	Operating System	Total	Percent
	Top Five		
🟦	Windows 7 Professional	752	88.3%
🟧	Windows Server 2008 R2 Standard	24	2.8%
🟩	Windows Server 2003	22	2.6%
🟨	Windows Server 2012 R2 Standard	19	2.2%
🟫	Windows Server 2016 Standard	13	1.5%
	Total - Top Five	**830**	**97.4%**
	Other		
🟥	Windows Server 2008 Standard	7	0.8%
	Windows XP Professional	6	0.7%
	Unidentified OS	2	0.2%
	unknown	2	0.2%
	Windows 8.1 Pro	2	0.2%
	Windows 10 Pro	1	0.1%
	Windows Embedded Standard	1	0.1%
	Windows Server 2012 Standard	1	0.1%
	Total - Other	**22**	**2.6%**

Operating System	Total	Percent
Overall Total	**852**	**100%**

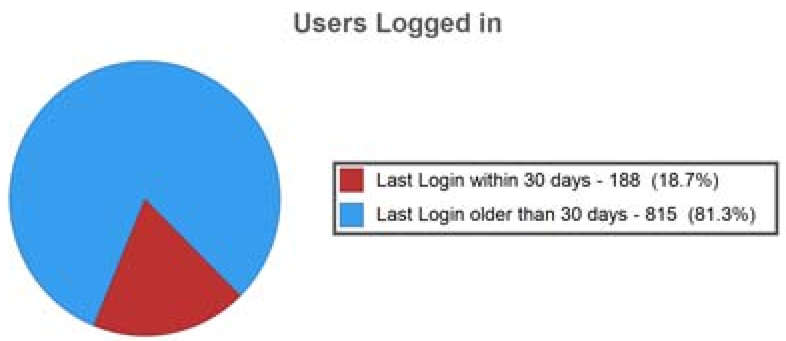
Asset Summary: Inactive Computers

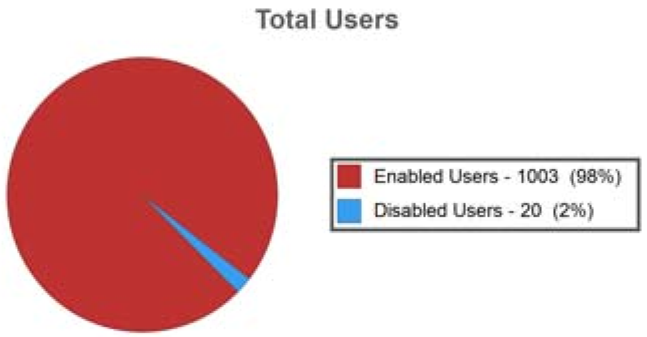
Inactive computers are computers that could not be scanned or have not checked into Active Directory in the past 30 days.

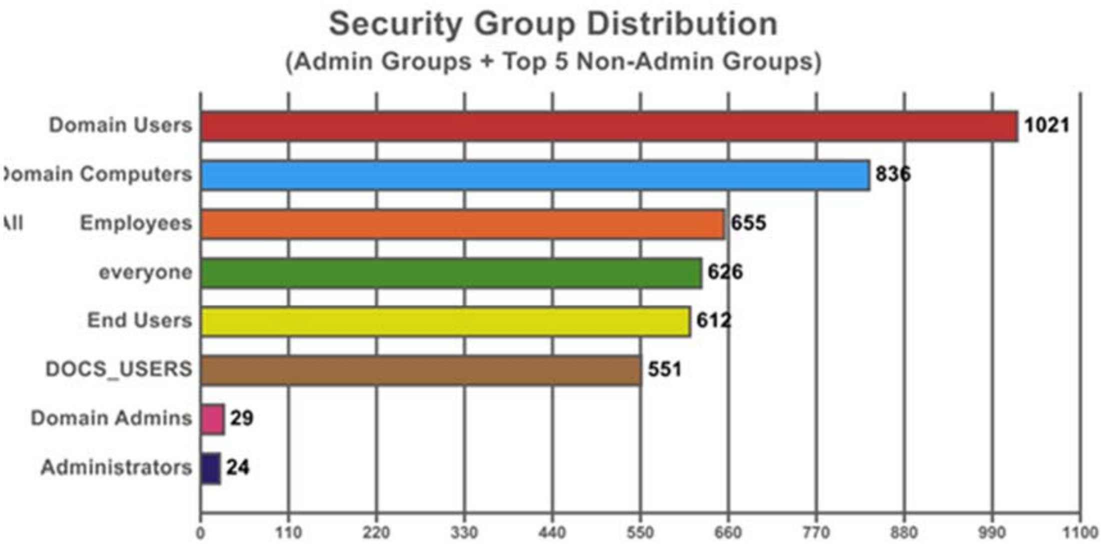


	Operating System	Total	Percent
	Top Five		
🟦	Windows 7 Professional	86	72.9%
🟧	Windows Server 2008 R2 Standard	11	9.3%
🟩	Windows Server 2003	7	5.9%
🟨	Windows XP Professional	4	3.4%
🟫	Windows Server 2012 R2 Standard	3	2.5%
	Total - Top Five	**111**	**94.1%**
	Other		
🟥	Unidentified OS	2	1.7%
🟥	Windows 8.1 Pro	2	1.7%
🟥	Windows Server 2008 Standard	2	1.7%
🟥	unknown	1	0.8%
	Total - Other	**7**	**5.9%**
	Overall Total	**118**	**100%**

Asset Summary: Users

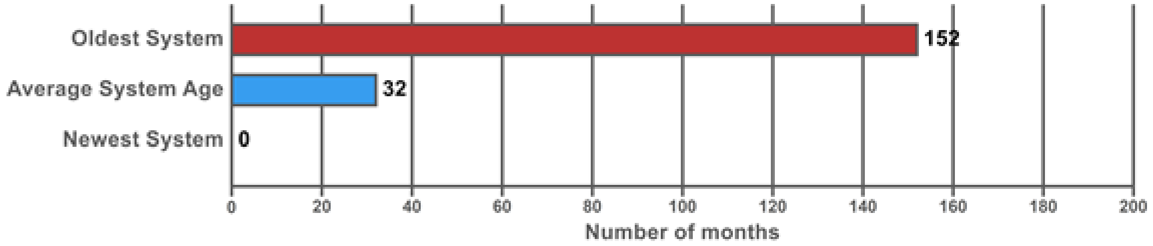




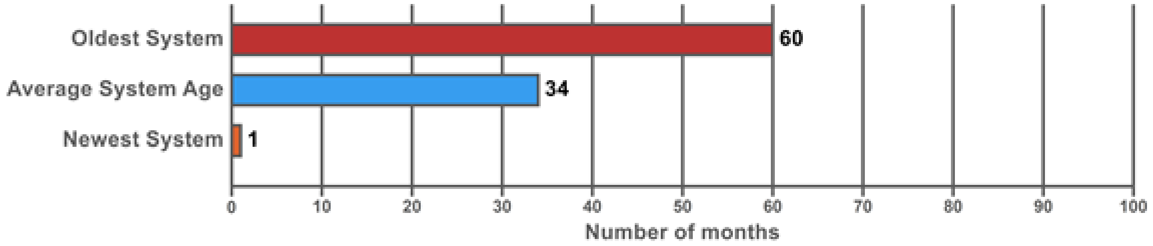


Security Group Distribution
(Admin Groups + Top 5 Non-Admin Groups)

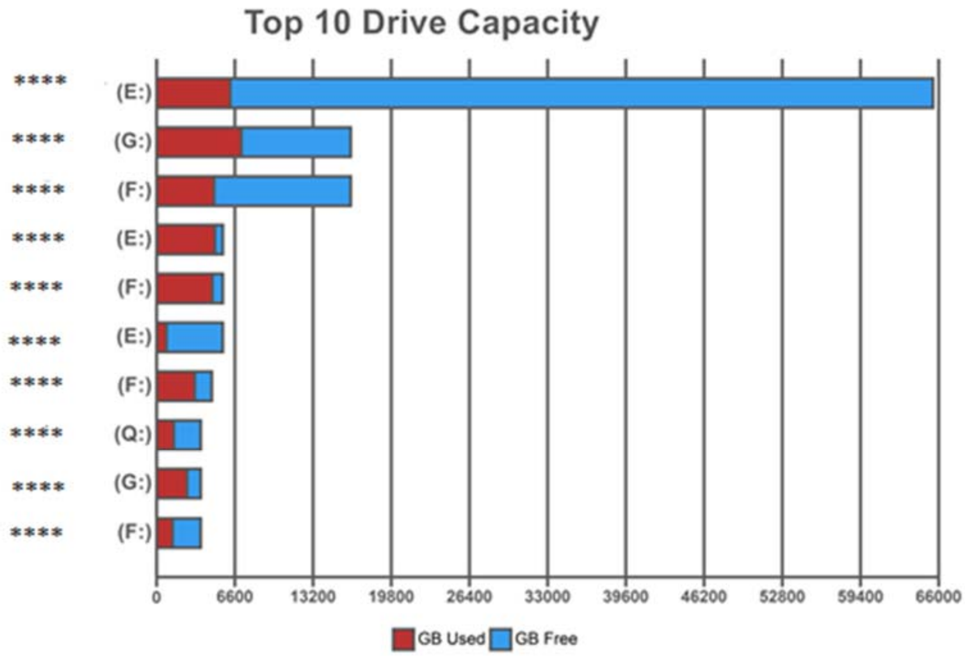
Server Aging

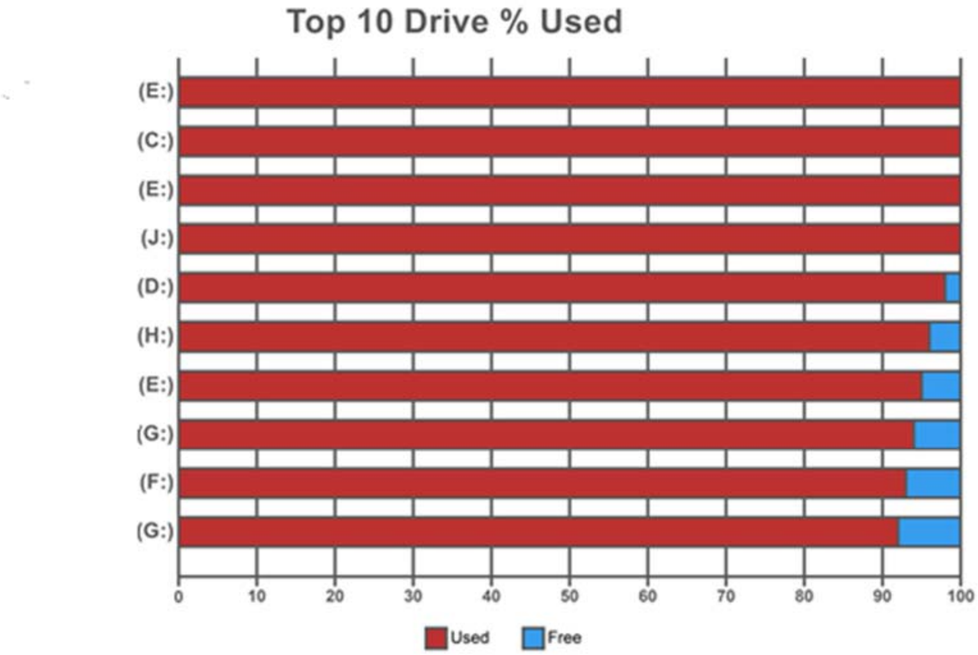


Workstation Aging

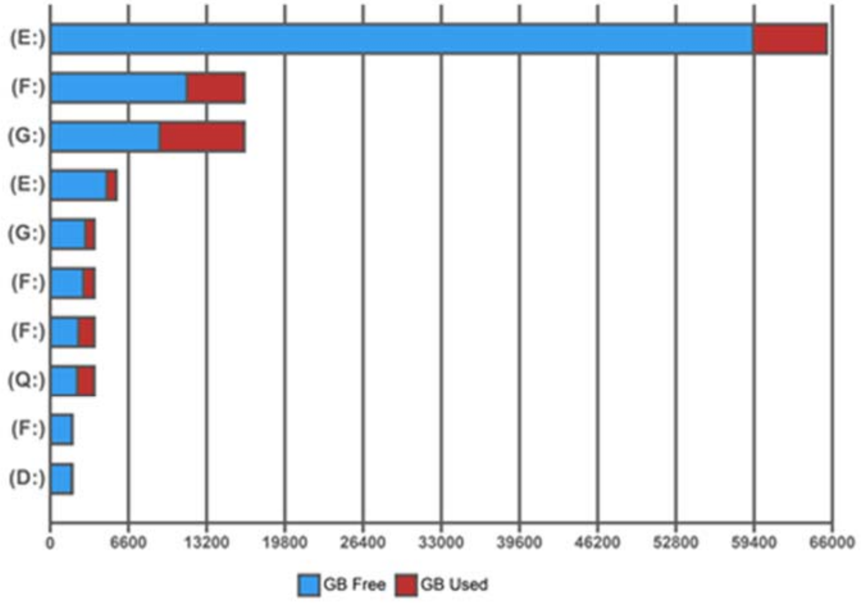


Asset Summary: Storage





Top 10 Drive Free Space



IV. Security Risk Report

Table of Contents

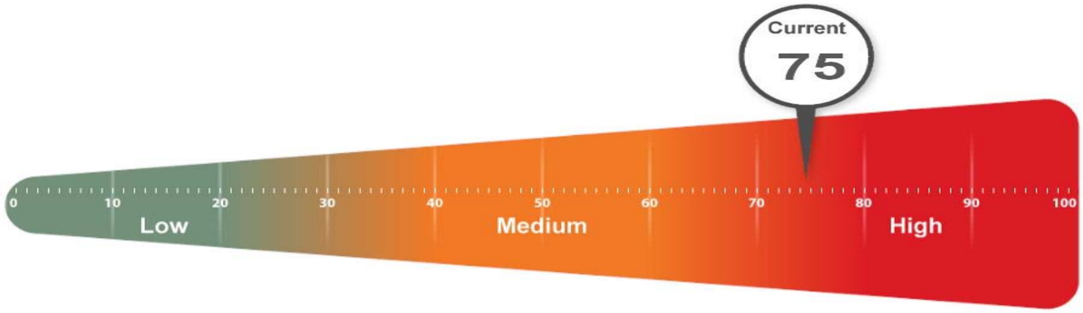
Discovery Tasks

The following discovery tasks were performed:

	Task	Description
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✗	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✓	External Security Vulnerabilities	Performs detailed External Vulnerability Scan. List and categorize external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.

Risk Score

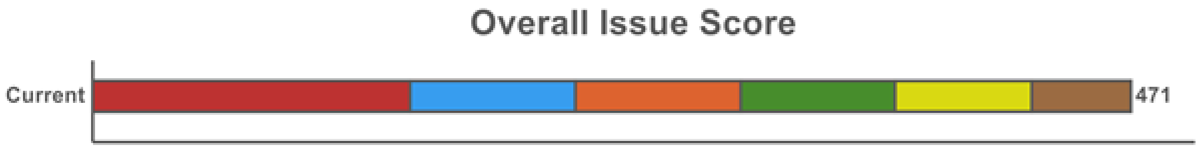
The Risk Score is a value from 1 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.



Several critical issues were identified. Identified issues should be investigated and addressed according to the Management Plan.

Issues Summary

This section contains summary of issues detected during the Security Assessment. It is based on general Industry-wide, and may indicate existing issues or points of interest. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.



Overall Issue Score: Risk Score x Number of Incidents = Total points: Total percent (%)

	Automatic screen lock not turned on. (72 pts each)
144	***Current Score:*** 72 pts x 2 = 144: 30.57%
	Issue: Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enabled allows unauthorized access to network resources.
	Recommendation: Enable automatic screen lock on the specified computers.

	Medium severity external vulnerabilities detected (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 15.92%
	Issue: External vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
	Recommendation: Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.

	Password complexity not enabled (75 pts each)
75	***Current Score:*** 75 pts x 1 = 75: 15.92%
	Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
	Recommendation: Enable password complexity to assure domain account passwords are secure.

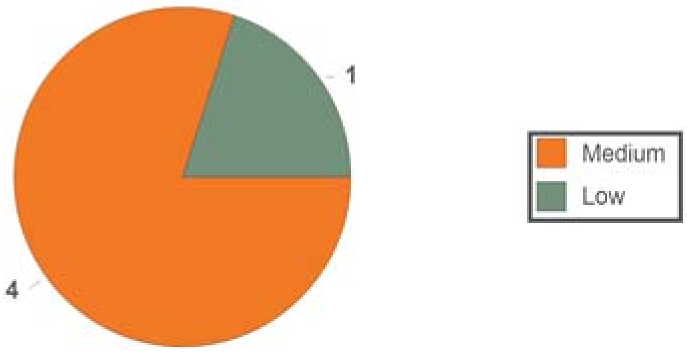
	Maximum password age greater than 90 days (70 pts each)
70	***Current Score:*** 70 pts x 1 = 70: 14.86%
	Issue: Passwords that are not changed regularly are more vulnerable to attack and unauthorized use. Minimizing the allowed password age greatly reduces the window of time that a lost or stolen password poses a threat.

	Recommendation: Modify the maximum password age to be 90 days or less.

	Lack of web filtering (62 pts each)
62	***Current Score:*** 62 pts x 1 = 62: 13.16%
	Issue: Access to all websites appears to be unrestricted. This issue does not imply that any particular user is currently accessing restricted sites, but rather that they can. Controlling access to the Internet and websites may help reduce risks related to security, legal, and productivity concerns. Lack of adequate content management filtering to block restricted sites may lead to increased network risk and business liability.
	Recommendation: Put access controls in place to block websites that violate the company's Internet use policy.

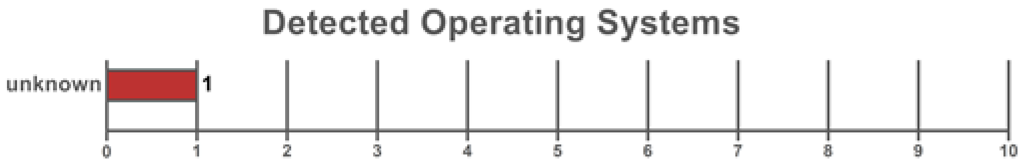
	System Protocol Leakage (45 pts each)
45	***Current Score:*** 45 pts x 1 = 45: 9.55%
	Issue: System protocols were allowed to be sent outbound. To prevent potential loss of data and reduce the risk of malicious behavior by malware, these protocols should be restricted or blocked by external access controls. There are very few instances where system protocols are needed outside of the internal network. Allowing these protocols to \"leak\" does not mean that they are currently posing a threat, but is an indication of a lack of a managed firewall or proper policies to block these protocols.
	Recommendation: We suggest ensuring adequate access controls in place to block these protocols or note them as acceptable risks.

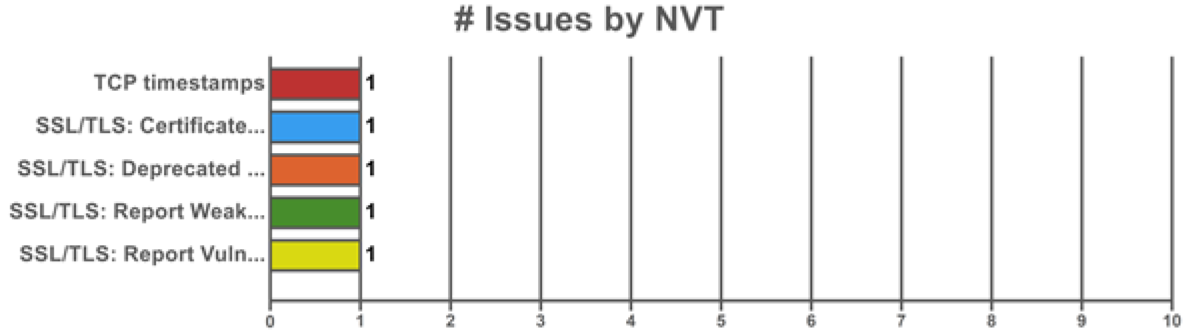
External Vulnerabilities



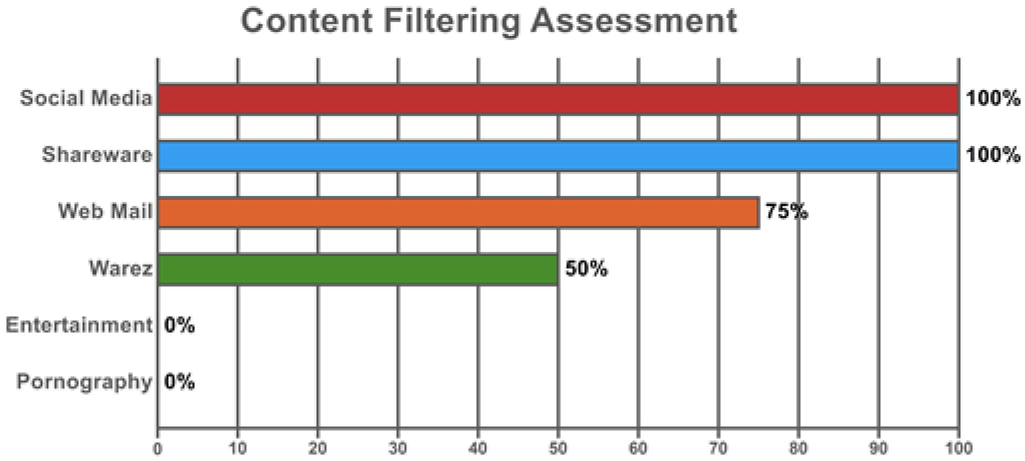
Host Issue Summary

Host	Open Ports	High	Med	Low	False	Highest CVSS
(XXX.XXX.XXX.XXX)	2	0	4	1	0	5.0
Total: 1	2	0	4	1	0	5.0

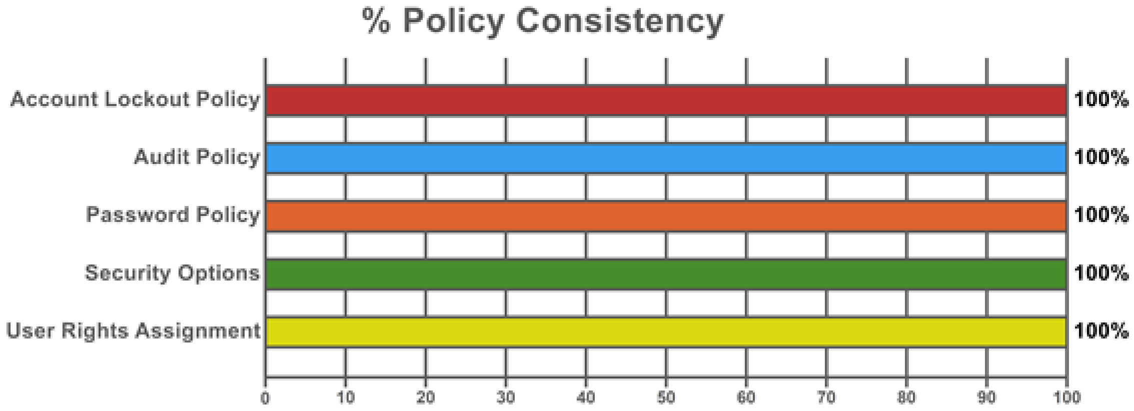



# Issues by NVT
TCP timestamps
SSL/TLS: Certificate...
SSL/TLS: Deprecated ...
SSL/TLS: Report Weak...
SSL/TLS: Report Vuln...
1
1
1
1
1
0
1
2
3
4
5
6
7
8
9
10

Internal Vulnerabilities



Local Security Policy Consistency



V. External Vulnerabilities Summary Report

Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the global Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

Medium Risk

CVSS	Recommendation
5	**SSL/TLS: Report Vulnerable Cipher Suites for HTTPS** **Summary** This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services. **Solution** The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task. **Affected Nodes** 174.141.16.50(174.141.16.50.nw.nuvox.net)
4.3	**SSL/TLS: Report Weak Cipher Suites** **Summary** This routine reports all Weak SSL/TLS cipher suites accepted by a service. NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication. **Solution** The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task. **Affected Nodes** 174.141.16.50(174.141.16.50.nw.nuvox.net)
4.3	**SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection** **Summary** It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

CVSS	Recommendation
	Solution It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. **Affected Nodes** 174.141.16.50(174.141.16.50.nw.nuvox.net)

Low Risk

CVSS	Recommendation
4	**SSL/TLS: Certificate Signed Using A Weak Signature Algorithm** **Summary** The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm. **Solution** Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS certificates to avoid these web browser SSL/TLS certificate warnings. **Affected Nodes** 174.141.16.50(174.141.16.50.nw.nuvox.net)
2.6	**TCP timestamps** **Summary** The remote host implements TCP timestamps and therefore allows to compute the uptime. **Solution** To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152 **Affected Nodes** 174.141.16.50(174.141.16.50.nw.nuvox.net)

VERTEKS
VOICE & DATA
NETWORKS

VI. SQL Server Security/Health Report

Table of Contents

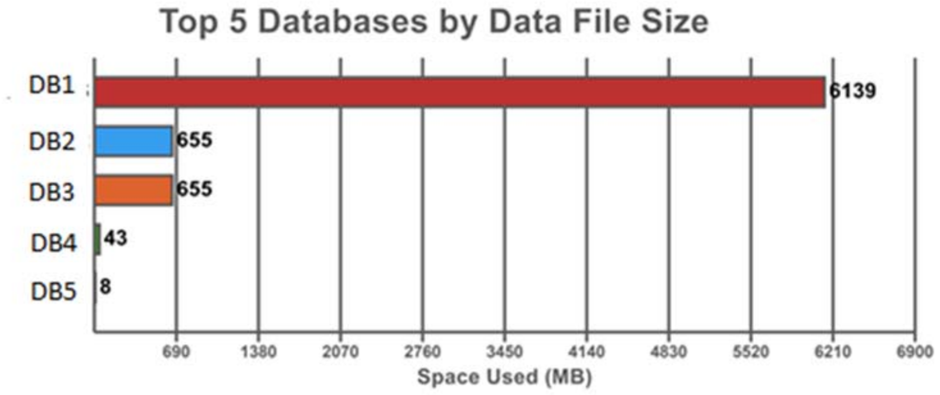
1 - About this Report

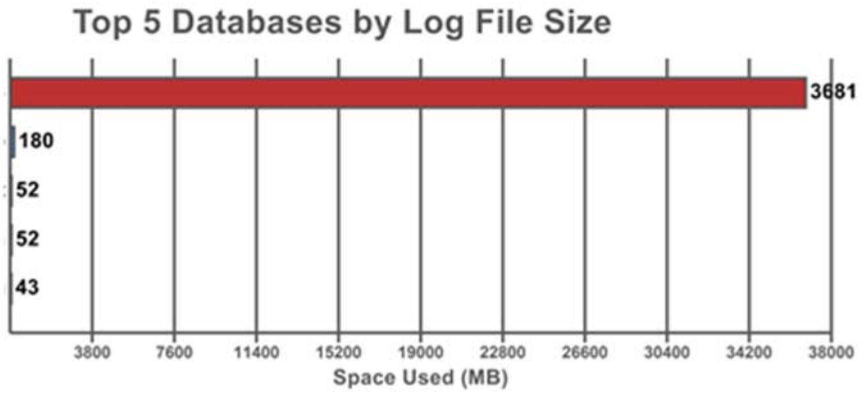
This report assesses the health of the SQL Server using three major categories. These include settings, file, and resources. Setting health looks for configuration issues that may go against prescribed best practices. File health looks at how the database interacts with the file system, looking for adequate space and compares the current configuration versus best practices. Resource health looks to ensure adequate resources are available to operate the SQL Server optimally and looks for indicators pointing to performance issues. Resource health comprises of three sub-categories – wait health, task health, and memory health. Wait health deals with issues with database processing waits and delays. Task health validates that scheduled tasks and jobs are working optimally. Memory health looks to ensure adequate memory is available to run the SQL Server properly.

The assessed health is based on published best practices from Microsoft and other resources. They are only generalizations and there can be instances where violating a best practice may be necessary and even desirable. Please consult a SQL Server DBA for further analysis and evaluation.

2 - SQL Server System Summary

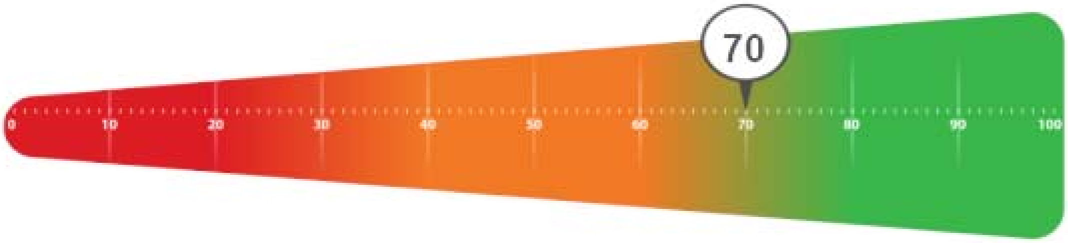
SQL Server: *******	
Version	10.0.5500.0
User Databases	8
System Databases	4
Total Databases	12
Total Jobs	13

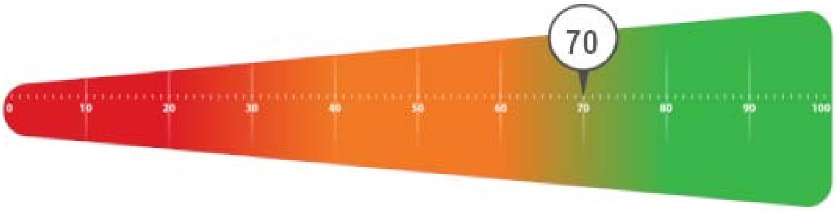
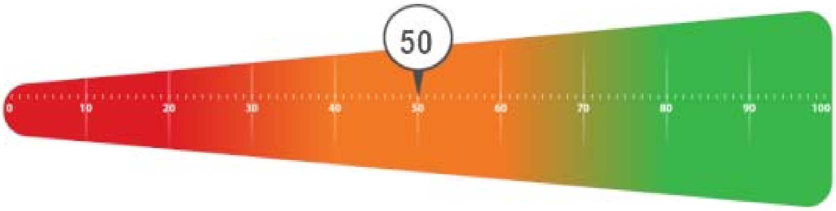
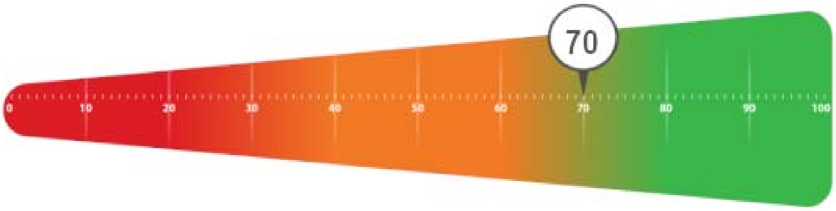


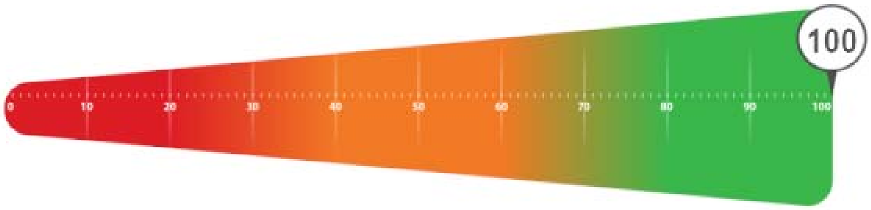


3 - SQL Server Health Summary

Overall Health



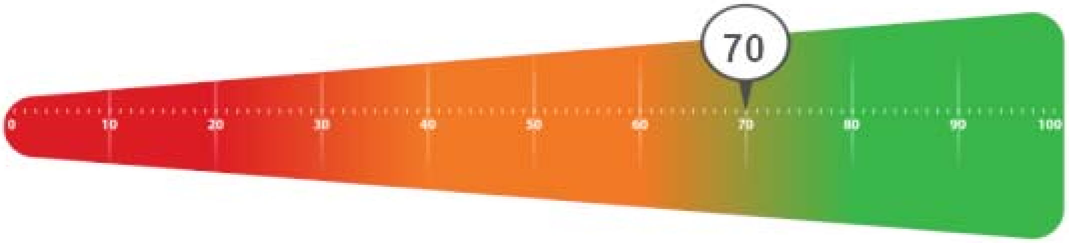
Category	
Settings Health	
File Health	
Resource Health	

Category	
SQL Server Agent Health	

4 - SQL Server Health Detail

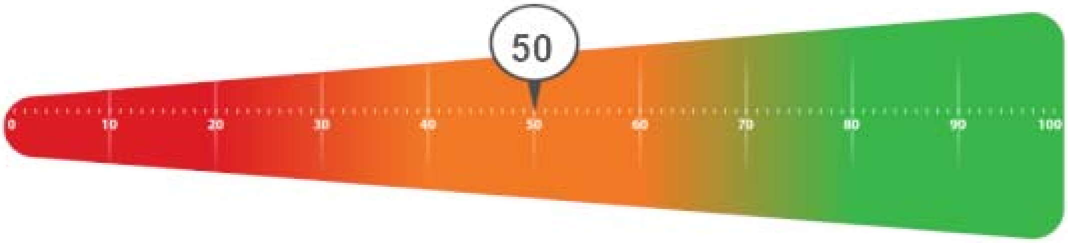
The following sections break down the individual health scores and shows what factors contributed to raising or lowering the health score.

4.1 - Settings Health



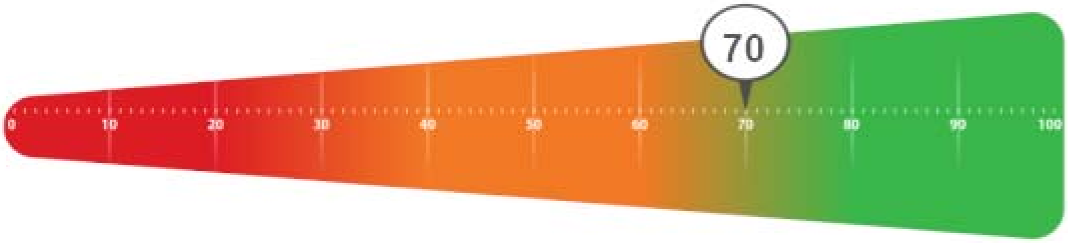
Settings Health Factors			
Backup Compression Default	Not Enabled	⚠	Backup compression helps save size on the target drives by compressing backups and reduces the time of the backup window. In most cases, enabling this feature is desired.
CLR	Not Enabled	👍	
Lightweight Pooling	Not Enabled	👍	
Priority Boost	Not Enabled	👍	
Optimize for Ad-Hoc Workloads	Not Enabled	👍	
Auto Shrink	Enabled	⚠	Auto Shrink can cause fragmentation of indexes. In most cases, disabling this feature is desired.
Auto Close	Not Enabled	👍	

4.2 - File Health



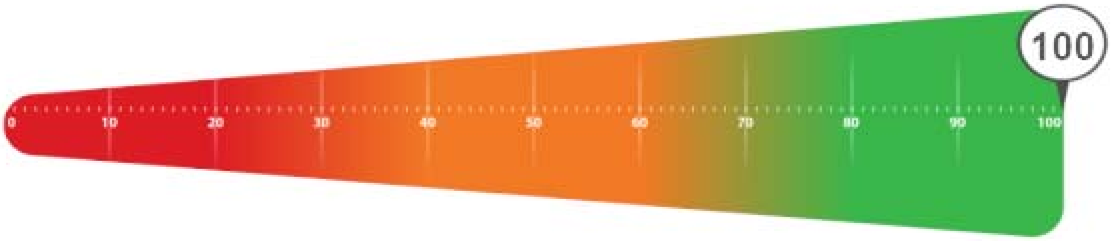
File Health Factors			
Data and Log File Placement	On same drive	⚠	Data and Log files should be placed on separate drives to reduce I/O congestion.
File Placement	On OS Drive	⚠	Database files should not be placed on the Operating System drive in order to reduce the risk of Operating System failure causing database corruption.
TempDb Placement	Not on Isolated Drive	⚠	TempDb should be placed on isolated drive to reduce I/O congestion
Available Disk Space	Unable to determine. Space assumed to be sufficient.	👍	
Available Disk Space Trend (90 Days Projection)	Sufficient(> 10 GB	👍	
I/O Stalls	Acceptable	👍	

4.3 - Resource Health



Resource Health Factors			
Signal Waits	Above 10%	⚠	Signal Waits at a rate above 10% indicate the need for more CPU power.
Average Current Tasks	< 10	👍	
Physical Memory Available	Sufficient	👍	

4.4 - SQL Server Agent Health

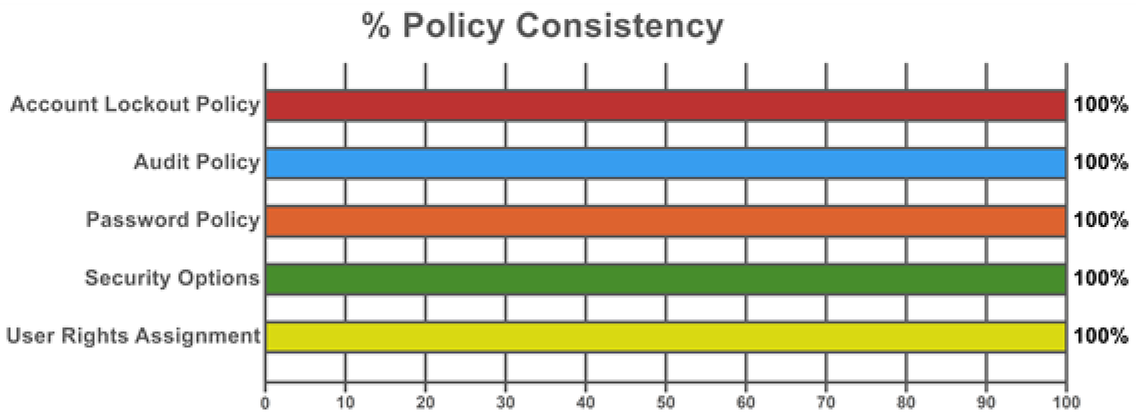


SQL Server Agent Health Factors		
Running	Yes	👍
Failed Jobs (past 30 days)	0	👍

VII. Security Policy Assessment

Table of Contents

1 - Summary



1.1 - Sampled Systems

IP Addresses	Computer Name	Operating System
10.0.0.1	*********	Windows Server 2008 R2 Standard
10.0.0.75	**********	Windows Server 2008 R2 Standard

2 - Domain Policies: ******.com

2.1 - Default Domain Policy: ******.COM

2.1.1 - Account Policies/Password Policy

Policy	Setting
Enforce password history	7 passwords remembered
Maximum password age	180 days
Minimum password age	10 days
Minimum password length	6 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

2.1.2 - Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

2.1.3 - Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

2.1.4 - Local Policies/Security Options

Interactive Logon

Policy	Setting
Interactive logon: Prompt user to change password before expiration	7 days

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Disabled

Network Security

Policy	Setting
Network security: Force logoff when logon hours expire	Enabled

2.1.5 - Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	6/30/2004 2:42:53 AM	File Recovery

2.1.6 - Public Key Policies/Trusted Root Certification Authorities

Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

2.2 - Default Domain Controllers Policy: ******.COM

2.2.1 - Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

2.2.2 - Local Policies/User Rights Assignment

Policy	Setting
Access this computer from the network	
Act as part of the operating system	
Add workstations to domain	NT AUTHORITY\Authenticated Users
Adjust memory quotas for a process	
Allow log on locally	
Back up files and directories	
Bypass traverse checking	
Change the system time	NT AUTHORITY\LOCAL SERVICE, BUILTIN\Administrators
Create a pagefile	BUILTIN\Administrators
Create a token object	
Create permanent shared objects	
Debug programs	BUILTIN\Administrators
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Enable computer and user accounts to be trusted for delegation	BUILTIN\Administrators
Force shutdown from a remote system	BUILTIN\Administrators
Generate security audits	

Policy	Setting
Increase scheduling priority	BUILTIN\Administrators
Load and unload device drivers	BUILTIN\Administrators
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Manage auditing and security log	BUILTIN\Administrators,
Modify firmware environment values	
Profile single process	BUILTIN\Administrators
Profile system performance	BUILTIN\Administrators
Remove computer from docking station	BUILTIN\Administrators
Replace a process level token	$SPAREBRANCH$BKUPEXEC, S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,
Restore files and directories	S-1-5-21-880543812-1657410183-313593124-1227, BUILTIN\Backup Operators, BUILTIN\Administrators, UESORL\Administrator
Shut down the system	BUILTIN\Backup Operators, BUILTIN\Administrators
Synchronize directory service data	
Take ownership of files or other objects	BUILTIN\Administrators

2.2.3 - Local Policies/Security Options

Microsoft Network Server

Policy	Setting
Microsoft network server: Digitally sign communications (always)	Disabled

3 - Local Security Settings (Sampled Systems)

3.1 - Account Policies

3.1.1 - Password Policy

Policy	Setting	Computers
Enforce password history	7 passwords remembered	********
Maximum password age	180 days	********
Minimum password age	10 days	********
Minimum password length	6 characters	********
Password must meet complexity requirements	Disabled	********
Store passwords using reversible encryption	Disabled	********

3.1.2 - Account Lockout Policy

Policy	Setting	Computers
Account lockout duration	30 minutes	********
Account lockout threshold	5 invalid logon attempts	********
Reset account lockout counter after	30 minutes	********

3.2 - Local Policies

3.2.1 - Audit Policy

Policy	Setting	Computers
Audit account logon events	Success, Failure	********
Audit account management	No auditing	********
Audit directory service access	No auditing	********
Audit logon events	No auditing	********
Audit object access	No auditing	********
Audit policy change	No auditing	********
Audit privilege use	No auditing	********
Audit process tracking	No auditing	********
Audit system events	No auditing	********

3.2.2 - User Rights Assignment

Policy	Setting	Computers
Access this computer from the network	Everyone,Administrators,Users,Backup Operators	********
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-21-3844168905-3350625487-1764690772-1001,Acronis Agent User,Administrators,Classic .NET AppPool,DefaultAppPool	********
Allow log on locally	Administrators,Backup Operators	********
Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users	********
Back up files and directories	Administrators,Backup Operators	********
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Backup Operators	*******
Change the system time	LOCAL SERVICE,Administrators	*******
Change the time zone	LOCAL SERVICE,Administrators	*******
Create a pagefile	Administrators	*******
Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	*******
Create symbolic links	Administrators	*******
Debug programs	Administrators	*******
Deny log on locally	*S-1-5-21-3844168905-3350625487-1764690772-1001,Acronis Agent User	*******
Force shutdown from a remote system	Administrators	*******

Policy	Setting	Computers
Generate security audits	LOCAL SERVICE,NETWORK SERVICE,Classic .NET AppPool,DefaultAppPool	*******
Impersonate a client after authentication	LOCAL SERVICE,NETWORK SERVICE,Administrators,IIS_IUSRS,SERVICE	*******
Increase a process working set	Users	*******
Increase scheduling priority	Administrators	*******
Load and unload device drivers	Administrators	*******
Log on as a batch job	Administrators,Backup Operators,Performance Log Users,IIS_IUSRS	*******
Log on as a service	*S-1-5-21-3844168905-3350625487-1764690772-1001,Acronis Agent User, ,NT SERVICE\ALL SERVICES,Classic .NET AppPool,DefaultAppPool	*******
Manage auditing and security log	Administrators	*******
Modify firmware environment values	*S-1-5-21-3844168905-3350625487-1764690772-1001,Acronis Agent User,Administrators	*******
Perform volume maintenance tasks	Administrators	*******
Profile single process	Administrators	*******
Profile system performance	Administrators,NT SERVICE\WdiServiceHost	*******
Remove computer from docking station	Administrators	*******
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE,*S-1-5-21-3844168905-3350625487-1764690772-1001,Acronis Agent User,Classic .NET AppPool,DefaultAppPool	*******
Restore files and directories	Administrators,Backup Operators	*******
Shut down the system	Administrators,Backup Operators	*******
Take ownership of files or other objects	Administrators	*******

3.2.3 - Security Options

Policy	Setting	Computers
Accounts: Administrator account status	Enabled	*******
Accounts: Guest account status	Disabled	*******
Accounts: Limit local account use of blank passwords to console logon only	Enabled	*******

Policy	Setting	Computers
Accounts: Rename administrator account	Administrator	*******
Accounts: Rename guest account	Guest	*******
Audit: Audit the access of global system objects	Disabled	*******
Audit: Audit the use of Backup and Restore privilege	Disabled	*******
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined	*******
Audit: Shut down system immediately if unable to log security audits	Disabled	*******
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	*******
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined	*******
Devices: Allow undock without having to log on	Enabled	*******
Devices: Allowed to format and eject removable media	Not Defined	*******
Devices: Prevent users from installing printer drivers	Enabled	*******
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined	*******
Devices: Restrict floppy access to locally logged-on user only	Not Defined	*******
Domain controller: Allow server operators to schedule tasks	Not Defined	*******
Domain controller: LDAP server signing requirements	None	*******
Domain controller: Refuse machine account password changes	Not Defined	*******
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	*******
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	*******

Policy	Setting	Computers
Domain member: Digitally sign secure channel data (when possible)	Enabled	*******
Domain member: Disable machine account password changes	Disabled	*******
Domain member: Maximum machine account password age	30 days	*******
Domain member: Require strong (Windows 2000 or later) session key	Enabled	*******
Interactive logon: Display user information when the session is locked	Not Defined	*******
Interactive logon: Do not display last user name	Disabled	*******
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	*******
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	*******
Interactive logon: Prompt user to change password before expiration	7 days	*******
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	*******
Interactive logon: Require smart card	Disabled	*******
Interactive logon: Smart card removal behavior	No Action	*******
Microsoft network client: Digitally sign communications (always)	Disabled	*******
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	*******
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	*******
Microsoft network server: Amount of idle time required before suspending session	15 minutes	*******
Microsoft network server: Digitally sign communications (always)	Disabled	*******
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	*******

Policy	Setting	Computers
Microsoft network server: Disconnect clients when logon hours expire	Enabled	*******
Microsoft network server: Server SPN target name validation level	Not Defined	*******
Network access: Allow anonymous SID/Name translation	Disabled	*******
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	*******
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	*******
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled	*******
Network access: Let Everyone permissions apply to anonymous users	Disabled	*******
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions,System\CurrentControlSet\Control\Server Applications,Software\Microsoft\Windows NT\CurrentVersion	*******
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers,System\CurrentControlSet\Services\Eventlog,Software\Microsoft\OLAP Server,Software\Microsoft\Windows NT\CurrentVersion\Print,Software\Microsoft\Windows NT\CurrentVersion\Windows,System\CurrentControlSet\Control\ContentIndex,System\CurrentControlSet\Control\Terminal Server,System\CurrentControlSet\Control\Terminal Server\UserConfig,System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SysmonLog	*******
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	*******
Network access: Shares that can be accessed anonymously	Not Defined	*******
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	*******

Policy	Setting	Computers
Network security: Allow Local System to use computer identity for NTLM	Enabled	*******
Network security: Allow LocalSystem NULL session fallback	Not Defined	*******
Network Security: Allow PKU2U authentication requests to this computer to use online identities	Not Defined	*******
Network security: Configure encryption types allowed for Kerberos	Not Defined	*******
Network security: Do not store LAN Manager hash value on next password change	Enabled	*******
Network security: Force logoff when logon hours expire	Enabled	*******
Network security: LAN Manager authentication level	Not Defined	*******
Network security: LDAP client signing requirements	Negotiate signing	*******
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	*******
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	*******
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined	*******
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined	*******
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined	*******
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined	*******
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined	*******
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined	*******
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined	*******

Policy	Setting	Computers
Recovery console: Allow automatic administrative logon	Disabled	*******
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	*******
Shutdown: Allow system to be shut down without having to log on	Disabled	*******
Shutdown: Clear virtual memory pagefile	Disabled	*******
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	*******
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	*******
System objects: Require case insensitivity for non-Windows subsystems	Enabled	*******
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	*******
System settings: Optional subsystems	Posix	*******
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Disabled	*******
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled	*******
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	*******
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	*******
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	*******
User Account Control: Detect application installations and prompt for elevation	Enabled	*******
User Account Control: Only elevate executables that are signed and validated	Disabled	*******

Policy	Setting	Computers
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	*******
User Account Control: Run all administrators in Admin Approval Mode	Enabled	*******
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled	*******
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	*******

VIII. Security Management Plan

Management Plan

The Management Plan ranks individual issues based upon their potential risk to the network while providing guidance on which issues to address by priority. Fixing issues with lower Risk Scores will not lower the global Risk Score, but will reduce the Overall Issue Score. To mitigate global risk and improve the health of the network, address issues with higher Risk Scores first.

High Risk

Risk Score	Recommendation	Severity	Probability
75	Enable password complexity to assure domain account passwords are secure.	H	H
75	Assess the risk of each vulnerability and remediating all external vulnerabilities as prescribed.	H	H
72	Enable automatic screen lock on the specified computers. □ ******* □ ********	M	M

Medium Risk

Risk Score	Recommendation	Severity	Probability
70	Modify the maximum password age to be 90 days or less.	H	L
62	Put access controls in place to block websites that violate the company's Internet use policy.	M	M

Low Risk

Risk Score	Recommendation	Severity	Probability
45	We suggest ensuring adequate access controls in place to block these protocols or note them as acceptable risks. □ MS RPC	L	L

IX. Assessment Scorecard

Assessment Scorecard - Area 1: Security

Area 1: Security Scorecard Summary	Weight	Score
Data Preservation	40%	3.8
Network Security	30%	4.0
System Security	30%	1.7
Compliance	0%	0.0
Weighted Average Score (0=low to 5=high)	**3.24 /**	**65%**
Overall Security Rating	**C**	

Data Preservation	Pass	Fail
Backup system with offsite data portability functional		X
Adequate, current and supported backup software	X	
Data centralized through roaming profiles/redirected folders		X
Backup software configured properly to backup company data	X	
Backup software configured properly to backup system states	X	
Backup software configured properly for notifications/reporting	X	
Adequate media rotation including archive volumes	X	
Offsite and offline storage of backup volumes		X
Adequate media capacity for data volume	X	
Backup software configured properly to backup OS/Applications	X	
Existing sample restoration routine processes	X	
Availability of installation media	X	
Daily review of backup notifications	X	
Data Preservation Rating (0=low to 5=high)	**3.8**	

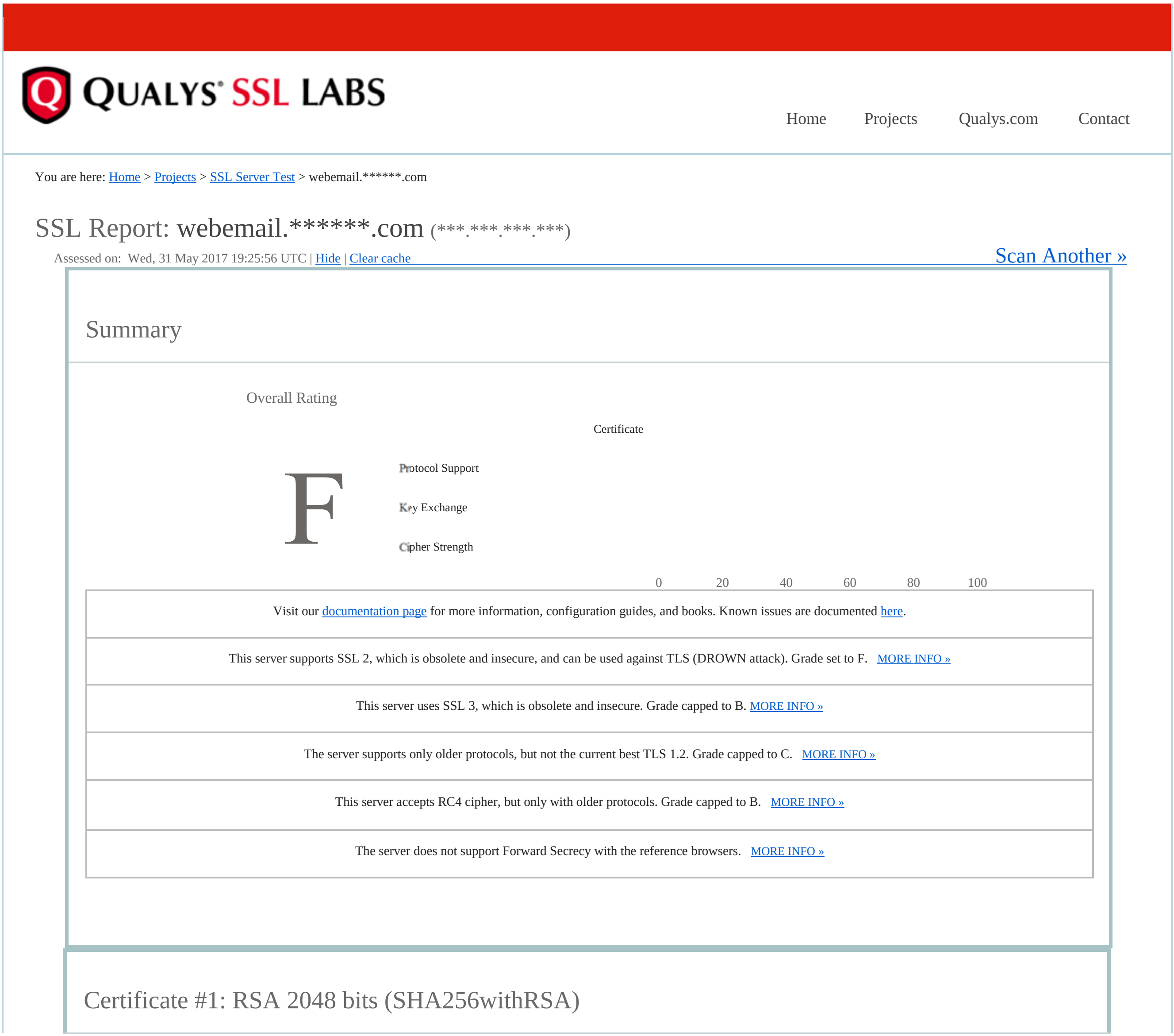
Network Security	Pass	Fail
Firewall hardware functional		
Firewall configured with at least basic protection	X	
Wireless system secured (if applicable)	X	
Centrally managed antispam software available	X	
Centrally managed antivirus software available	X	
Antivirus software thoroughly deployed and updating	X	
Antispam software thoroughly deployed and updating properly		X
Wireless system secured with VPN	X	
Gateway-level antispyware system available, configured and updating	X	
Gateway-level intrusion prevention system online, configured and updating		X
Password policies (complexity, history, expiration)	X	
Network Security Rating (0=low to 5=high)	**4.0**	

System Security	Pass	Fail
File/share permissions for employee access control		
Restrictions on confidential/proprietary data transmission		X
Server and server-based application updates current		X

Workstation OS updates current		X
RAID configured on all mission-critical servers		X
Adequate environmental facilities (AC, Power, etc)	X	
Adequate UPS battery capacity for equipment	X	
UPS Communication system installed	X	
UPS Communication system configured		X
Existing UPS testing routine process		X
System Security Rating (0=low to 5=high)	**1.7**	

Compliance	**Pass**	**Fail**
Meets security compliance requirements (PCI/FINRA/HIPAA) - N/A		X
Compliance Rating (0=low to 5=high)	**0.0**	

X. SSL Health Discovery



You are here: Home > Projects > SSL Server Test > webemail.******.com

SSL Report: webemail.******.com (***.***.***.***)

Assessed on: Wed, 31 May 2017 19:25:56 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

F

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. MORE INFO »

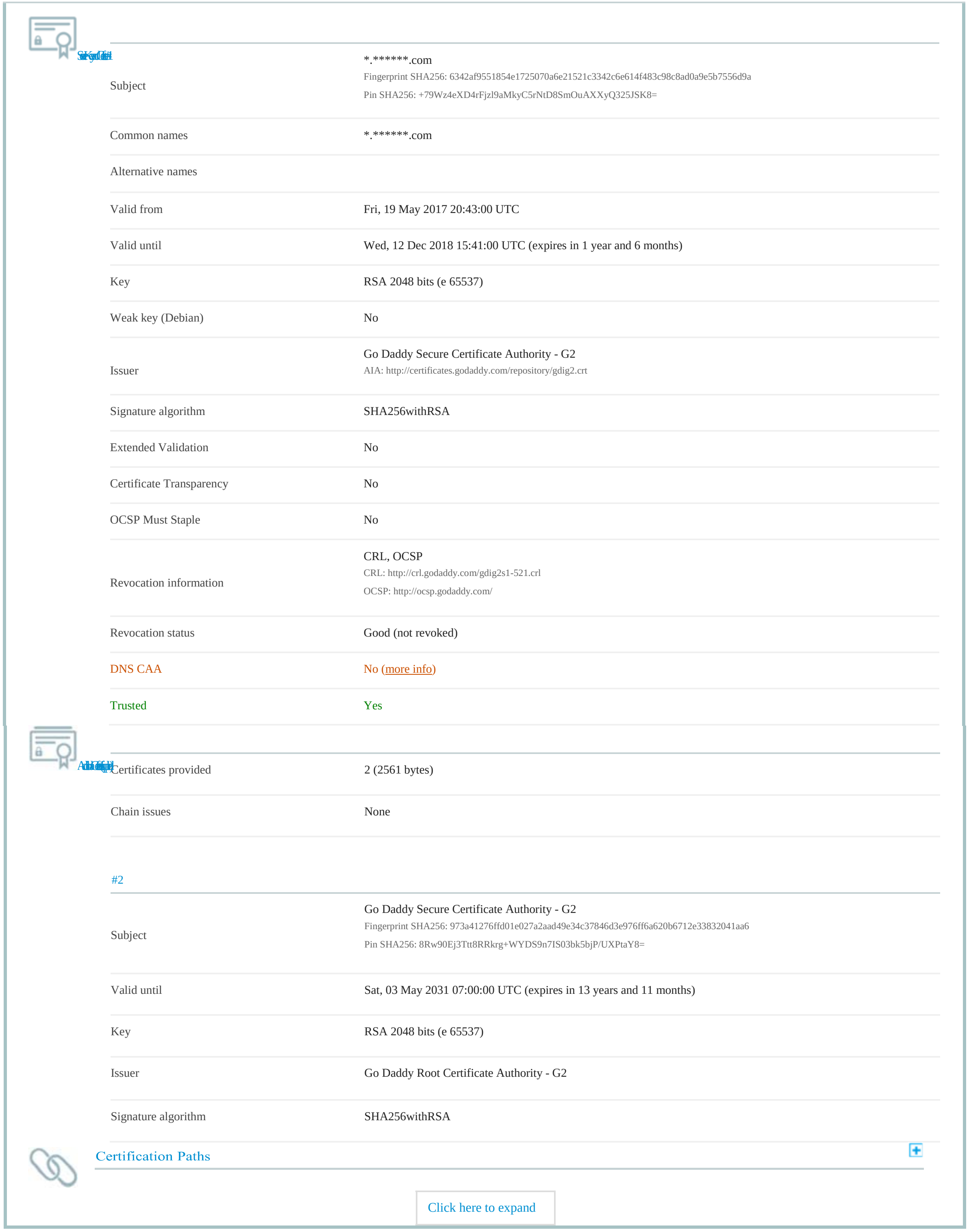
This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)



[illegible]

Subject	*.******.com Fingerprint SHA256: 6342af9551854e1725070a6e21521c3342c6e614f483c98c8ad0a9e5b7556d9a Pin SHA256: +79Wz4eXD4rFjzl9aMkyC5rNtD8SmOuAXXyQ325JSK8=
Common names	*.******.com
Alternative names	
Valid from	Fri, 19 May 2017 20:43:00 UTC
Valid until	Wed, 12 Dec 2018 15:41:00 UTC (expires in 1 year and 6 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Go Daddy Secure Certificate Authority - G2 AIA: http://certificates.godaddy.com/repository/gdig2.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.godaddy.com/gdig2s1-521.crl OCSP: http://ocsp.godaddy.com/
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes

[illegible]

Certificates provided	2 (2561 bytes)
Chain issues	None

#2

Subject	Go Daddy Secure Certificate Authority - G2 Fingerprint SHA256: 973a41276ffd01e027a2aad49e34c37846d3e976ff6a620b6712e33832041aa6 Pin SHA256: 8Rw90Ej3Ttt8RRkrg+WYDS9n7IS03bk5bjP/UXPtaY8=
Valid until	Sat, 03 May 2031 07:00:00 UTC (expires in 13 years and 11 months)
Key	RSA 2048 bits (e 65537)
Issuer	Go Daddy Root Certificate Authority - G2
Signature algorithm	SHA256withRSA

Certification Paths

Configuration

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2 INSECURE	Yes

Cipher Suites

# TLS 1.0 (suites in server-preferred order)

TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256
TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE		128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK		112
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_RC4_128_MD5 (0x4) INSECURE		128

# SSL 3 (suites in server-preferred order)

TLS_RSA_WITH_RC4_128_SHA (0x5) INSECURE	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
TLS_RSA_WITH_RC4_128_MD5 (0x4) INSECURE	128

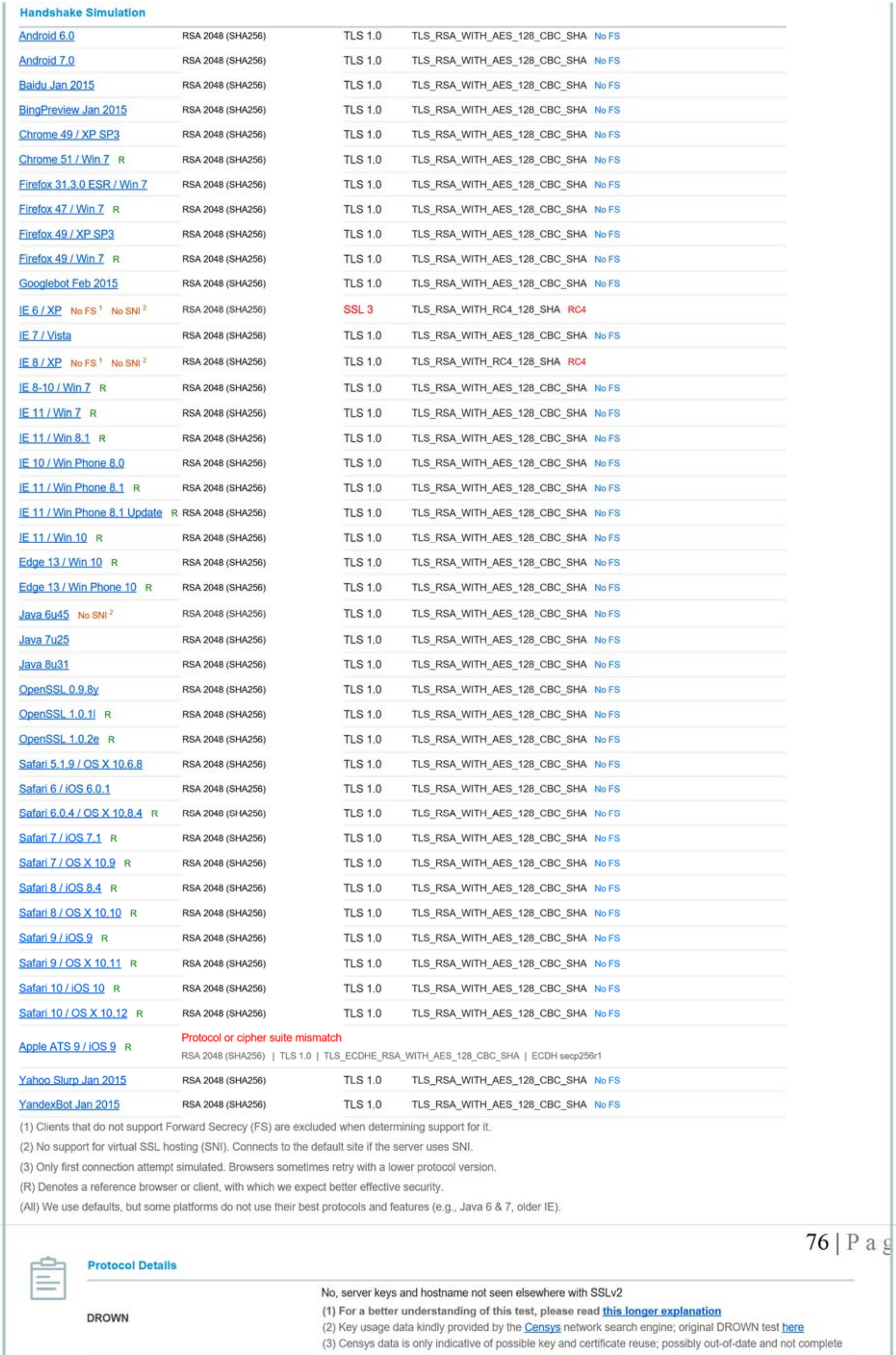
# SSL 2 (client selects suite)

Android 5.0.0 RSA 2048 (SHA256) TLS 1.0 TLS_RSA_WITH_AES_128_CBC_SHA No FS

SSL_CK_RC4_128_WITH_MD5 (0x10080) INSECURE	128
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) INSECURE	112

Handshake Simulation

Androi No SNI [2]	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Androi	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Androi	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Androi	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Androi	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Androi	RSA 2048 (SHA256)	TLS	TLS_RSA_WITH_AES_128_CBC_SHA No FS



Handshake Simulation

Android 6.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Chrome 51 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Firefox 49 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Googlebot Feb 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 6 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	SSL 3	TLS_RSA_WITH_RC4_128_SHA RC4
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 8 / XP No FS [1] No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_RC4_128_SHA RC4
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Edge 13 / Win 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 8u31	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
OpenSSL 1.0.2e R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
Apple ATS 9 / iOS 9 R	Protocol or cipher suite mismatch RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1		
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

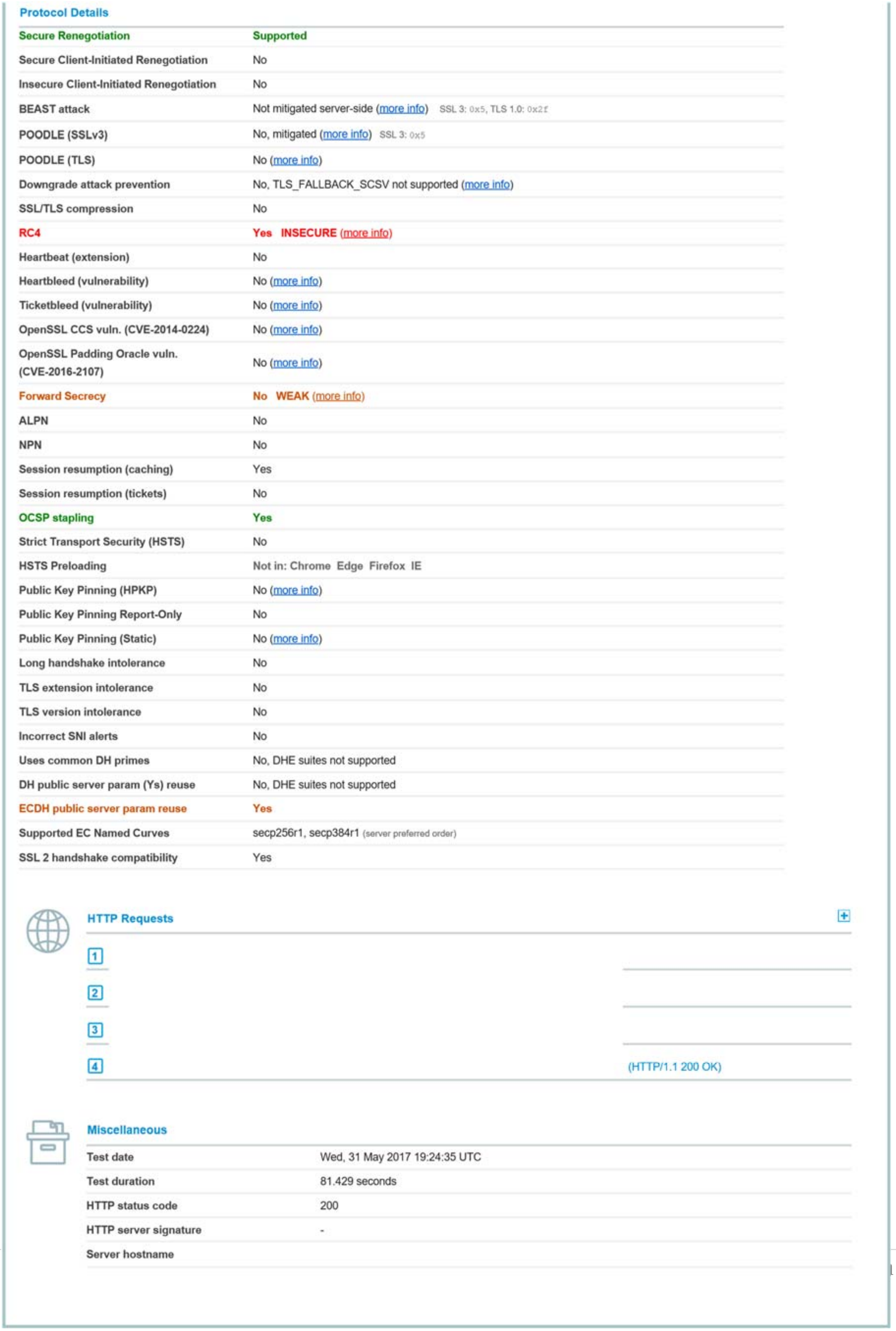
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete



Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x5, TLS 1.0: 0x2f
POODLE (SSLv3)	No, mitigated (more info) SSL 3: 0x5
POODLE (TLS)	No (more info)
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	Yes INSECURE (more info)
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	No WEAK (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	Yes
Supported EC Named Curves	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes

HTTP Requests

1	
2	
3	
4	(HTTP/1.1 200 OK)

Miscellaneous

Test date	Wed, 31 May 2017 19:24:35 UTC
Test duration	81.429 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	

SSL Report v1.28.5

Terms and Conditions

Qualys is the leading provider of integrated asset discovery, network security, threat protection, compliance monitoring and web application security solutions.