

Scores and weightings for .auCheck MAILTEST

Last updated: February 2022

STATUS_FAIL = mandatory test, will impact score	essential or important
STATUS_INFO = informational, no impact on score	recommended
STATUS_NOTICE = optional, no impact on score	suggested

ENCRYPTION AND AUTHENTICITY OF MAIL SERVER

STARTTLS

Can your mail server set up a secure and encrypted connection?	STARTTLS available		Essential
MAIL_TLS_STARTTLS_EXISTS_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_STARTTLS_EXISTS_WORST_STATUS	STATUS_FAIL		
Is your mail server using the latest encryption standards?	TLS version		Essential
MAIL_TLS_PROTOCOLS_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_PROTOCOLS_OK	HALF_WEIGHT_POINTS	9	
MAIL_TLS_PROTOCOLS_BAD	NO_POINTS	0	
Is your mail server using up-to-date methods of encrypting	Cipher suites		Important
MAIL_TLS_SUITES_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_SUITES_OK	HALF_WEIGHT_POINTS	5	
MAIL_TLS_SUITES_BAD	NO_POINTS	0	
Does your mail server enforce the most secure method of encryption?	Cipher order		Important
MAIL_TLS_CIPHER_ORDER_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_CIPHER_ORDER_OK	HALF_WEIGHT_POINTS	5	
MAIL_TLS_CIPHER_ORDER_BAD =	NO_POINTS	0	
key exchange parameters	key exchange parameters		Important
MAIL_TLS_FS_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_FS_OK	HALF_WEIGHT_POINTS	5	
MAIL_TLS_FS_BAD	NO_POINTS	0	
hash function for key exchange	hash function for key exchange		Important
MAIL_TLS_KEX_HASH_FUNC_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_KEX_HASH_FUNC_OK	HALF_WEIGHT_POINTS	5	
MAIL_TLS_KEX_HASH_FUNC_BAD	NO_POINTS	0	
TLS compression	TLS compression		Important
MAIL_TLS_COMPRESSION_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_COMPRESSION_BAD	NO_POINTS	0	

secure renegotiation	secure renegotiation		Important
MAIL_TLS_SECURE_RENEG_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_SECURE_RENEG_BAD	NO_POINTS	0	
Client-initiated renegotiation	Client-initiated renegotiation		Important
MAIL_TLS_CLIENT_RENEG_GOOD	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_CLIENT_RENEG_BAD	NO_POINTS	0	
0-RTT	0-RTT		Suggested
MAIL_TLS_ZERO_RTT_GOOD	FULL_WEIGHT_POINTS	10	STATUS_NOTICE
MAIL_TLS_ZERO_RTT_BAD	NO_POINTS	0	
Certificate			
trust chain of certificate	trust chain of certificate		Essential
MAIL_TLS_TRUSTED_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_TRUSTED_BAD =	NO_POINTS	0	
public key	public key		Essential
MAIL_TLS_PUBKEY_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_PUBKEY_OK =	FULL_WEIGHT_POINTS	10	
MAIL_TLS_PUBKEY_BAD	NO_POINTS	0	
signature of certificate	signature of certificate		Essential
MAIL_TLS_SIGNATURE_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_SIGNATURE_BAD	NO_POINTS	0	
domain name on certificate	domain name on certificate		Essential
MAIL_TLS_HOSTMATCH_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_TLS_HOSTMATCH_BAD =	NO_POINTS	0	
DANE			
Can your visitors use domain name records to check they can trust your website?	DANE existence		Suggested
N/A			STATUS_NOTICE
Are your certificates properly set up in your domain name server?	DANE validity		Suggested
MAIL_TLS_DANE_VALIDATED =	FULL_WEIGHT_POINTS	10	STATUS_NOTICE
MAIL_TLS_DANE_NONE =	NO_POINTS	0	
MAIL_TLS_DANE_NONE_BOGUS =	NO_POINTS	0	
MAIL_TLS_DANE_FAILED =	NO_POINTS	0	
Is your domain certificate set up to handle a smooth transition when a certificate expires?	DANE rollover scheme		Suggested
N/A			STATUS_NOTICE
Security of Domain Name / DNS SECURITY			
Is your website set up to allow a visitor to check it's authentic?	DNSSEC existence		Suggested

N/A			STATUS_NOTICE
Is your website set up correctly so visitor know it's authentic?	DNSSEC validity		Suggested
MAIL_DNSSEC_SECURE =	FULL_WEIGHT_POINTS	10	STATUS_NOTICE
MAIL_DNSSEC_INSECURE =	LESS_WEIGHT_POINTS	2	
MAIL_DNSSEC_BOGUS =	NO_POINTS	0	
MAIL_DNSSEC_ERROR =	NO_POINTS	0	
MAIL AUTHENTICATION			
DMARC			
Is your mail server set up to handle unverified emails from your domain?	DMARC existence		Essential
MAIL_AUTH_DMARC_PASS	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_AUTH_DMARC_FAIL	NO_POINTS	0	
MAIL_AUTH_DMARC_ERROR	NO_POINTS	0	
Does your mail domain have a policy for treating unverified emails and is it strict enough?	DMARC policy		Essential
MAIL_AUTH_DMARC_POLICY_PASS	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_AUTH_DMARC_POLICY_PARTIAL	HALF_WEIGHT_POINTS	5	
MAIL_AUTH_DMARC_POLICY_FAIL	NO_POINTS	0	
DKIM			
Does your mail server have records to verify the authenticity of its domain?	DKIM existence		Essential
MAIL_AUTH_DKIM_PASS	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_AUTH_DKIM_FAIL	NO_POINTS	0	
MAIL_AUTH_DKIM_ERROR	NO_POINTS	0	
SPF			
Does your mail domain have records that tell which servers re authorised to send emails?	SPF existence		Essential
MAIL_AUTH_SPF_PASS	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_AUTH_SPF_FAIL	NO_POINTS	0	
MAIL_AUTH_SPF_ERROR	NO_POINTS	0	
Are the records that are set up for your authorised amil servers secure enough?	SPF policy		Essential
MAIL_AUTH_SPF_POLICY_PASS	FULL_WEIGHT_POINTS	10	STATUS_FAIL
MAIL_AUTH_SPF_POLICY_PARTIAL	HALF_WEIGHT_POINTS	5	
MAIL_AUTH_SPF_POLICY_FAIL	NO_POINTS	0	
IPv6			
Cam the IPv6 address of your name server be reached?	IPv6 address name servers		Suggested
N/A			STATUS_NOTICE
Do the IPv6 address of your name servers work?	IPv6 reachability name servers		Suggested
IPV6_NS_CONN_GOOD =	FULL_WEIGHT_POINTS	10	STATUS_NOTICE

IPV6_NS_CONN_PARTIAL =	LESS_WEIGHT_POINTS	2	
IPV6_NS_CONN_FAIL =	NO_POINTS	0	
Can the IPv6 address of your mail server be reached? N/A	IPv6 address name servers		Suggested STATUS_NOTICE
Do the IPv6 address of your mail servers work?	IPv6 reachability name servers		Suggested
MAIL_IPV6_MX_CONN_GOOD	FULL_WEIGHT_POINTS	10	STATUS_NOTICE
MAIL_IPV6_MX_CONN_PARTIAL	LESS_WEIGHT_POINTS	5	
MAIL_IPV6_MX_CONN_FAIL	NO_POINTS	0	

Max amount of points available **210**