



Your Trusted Security Partner



RSA SECURID HEALTHCHECK



2MN LTD

www.2mn.co.uk

Telephone: +44(0)8709192892

Email: info@2mn.co.uk

The SecurID Healthcheck is designed for IT Security professionals who implement and maintain RSA SecurID solution to help increase operational efficiency, maximize system uptime, and reduce costs.



		Y, N, NA	F, O	Comments
SERVER INSTALL/CONFIG REVIEW				
PRIMARY SERVER INSTALL/CONFIG				
1	Does the Hardware comply with the Install Requirement?			
2	Is the server a single IP or Multi-interfaces server?			
3	Has a FQDN been assigned to the server?			
4	Has the Server been installed successfully			
5	Has the server been configured with its FQDN or short name (hostname)? FQDN recommended			
6	Are all required services present and running?			
7	Is the back-end database recording activities and creating server log?			
8	Is the server Log Monitoring and Auditing recording any activities?			
9	Is Server running in production or debug mode? Are logs rotating daily?			
10	Is the server clock in synch with the system clock?			
11	Is the server' side authentication working? (Remote mode test or sctest)?			
12	Is there an Admin User Account with a token or static password assigned?			
13	Is the server an agent host itself with a node secret set?			
14	Is the server configured as a Radius client* with a shared secret and Radius ports set?			
15	Is the server in a DMZ or a Domain member?			
16	Is there any scanning or monitoring tool installed? If yes, is it excluding the RSA directory during its scan?			



REPLICA SERVER INSTALL/CONFIG				
17	Is Replica Server getting updates from Primary (example, is a new user creation replicated)?			
18	Can users authenticate on Primary and Replica (Failover testing)?			
LDAP USERS SYNCHRONISATION				
19	For LDAP Synch, are users being added or updated from the remote LDAP?			
20	Are LDAP Synch updates showing in the Log Monitor?			
PRIMARY RADIUS SERVER				
21	Radius, Is the Radius Management console accessible?			
22	Is the Replica Server added as a Secondary Radius?			
23	Is Radius Replication up-to-date from the Radius Management?			
24	Are Radius Clients also present as Agent host in the SecurID server?			
25	Is Radius Test from NTRadping working from the RSA server and radius client computer?			
CLIENT INSTALL/CONFIG REVIEW				
1	Is the client defined as an agent host in the server?			
2	Is the client defined with its FQDN?			
3	Can the client resolve the server FQDN (forward/reverse)?			
4	Has the client config file been created and available in the default location /system32/ for windows or /var/ace for UNIX/Linux			
5	Is the client a multi-home workstation?			
6	Has a secondary node entry been added for that multi-home client?			
7	Is the client a DHCP or static IP client? For DHCP client, was the auto-registration tool installed on the client? Is the RSA server configured to allow auto-registration?			



7	Are the agent registry keys set properly HKLM/RSA/STDI/?			
8	Does the client display the server's status as active?			
9	Can the client authenticate against the Primary and Replica server?			
10	Does the Server Log Monitor show the agent activity?			
RADIUS CLIENT				
11	Radius Agent (VPN concentrator) defined as Radius client and RSA agent?			
12	Is the Concentrator an RSA securID "ready" device?			
13	Is the concentrator configured to forward authentication request to the RSA Radius?			
14	Is basic authentication from the concentrator working without RSA integration?			
15	Are Radius profiles being forwarded along with the user credentials?			
UNIX AGENT				
16	Did the PAM agent install ok? (correct PAM version for UNIX/Linux version)			
17	IS PAM /bin/acetatus displaying the server status as active?			
18	Is PAM authentication working (/bin/acetest)?			
19	Are all securID required agent files present with the correct permission? /var/ace 755 sdconf.rec 755 nodeseecret 755 sdstatus.12			
RSA AGENT API				
20	Does the rsa_api.properties point to the default config files location? SDCONF_LOC=/var/ace/sdconf.rec SDSTATUS_LOC=/var/ace/sdstatus.1 SDOPTS_LOC=/var/ace/sdopts.rec SDNDSCRT_LOC=/var/ace/securid			



BACKUP AND RESTORE				
1	Is there a backup strategy in place? How often is the server backup?			
2	Are the backup data, the system files and license file stored in a safe place? <code>sddump</code> , <code>server.cer</code> , <code>server.key</code> , <code>license.rec</code>			
3	Can the system be restored to an operational mode using the recent backup data?			

Y=Yes, N=No, NA=Not Applicable, F=Finding, O=Observation

DO NOT COPY

