PRIXL

PRIXL RESEARCH · FIELD NOTE

Day One

The security settings we found on CA firm servers, and a ten-minute check you can run on yours

Edition 1 · October 2026 · Prixl Technologies

Summary

When Prixl Warden is installed it audits the server's security settings and scores them out of 100. This note looks at the first audit of **three Windows servers at three CA firms in India**, made in March 2026, and at their latest audit in October 2026. Nothing in it identifies a firm or a server. Three servers is a small sample, so read these as observations, not statistics about the profession. They are still worth reading, because every gap below is common, quick to check and quick to fix.

37 / 100
average score at the first audit (41, 41 and 29)

3 of 3
servers had no minimum password length set

3 of 3
did not report Microsoft Defender's real-time protection as on

1 of 3
had all three Windows Firewall profiles switched off

What the first audit found

Passwords. None of the three servers had a minimum password length set, so Windows did not require any particular length. None remembered previous passwords, so a user could set the same password again immediately. One server had no account lockout, so a password could be guessed without limit. That last one matters most: these servers were receiving tens of thousands of password attempts a day (see our paper *Remote Desktop Under Attack*).

Antivirus. On all three servers, Windows did not report Microsoft Defender's antimalware service and real-time protection as both switched on. That can be fine if another antivirus product has taken over, but it is exactly the kind of thing that nobody checks until it matters. If you rely on a third-party product, open its console and confirm it is running and up to date.

Firewall. On one server, all three Windows Firewall profiles (domain, private and public) were switched off. With the firewall off, every service the server runs is reachable by anything that can reach the server.

What was already right. All three had SMBv1 disabled, Network Level Authentication required for Remote Desktop, the Guest account disabled and sign-in auditing turned on. Windows Server 2019 and later ship that way, and nobody had undone it.

Six months later

Setting	First audit (March)	Latest audit (October)
Minimum password length set	0 of 3	1 of 3, below the recommended length
Password history kept	0 of 3	1 of 3, below the recommended number
Account lockout on	2 of 3	3 of 3
Microsoft Defender reported on	0 of 3	1 of 3
All three firewall profiles on	2 of 3	2 of 3; the third server had one profile back on
A Windows update installed in the last 30 days	2 of 3	0 of 3 (each had updates 31 to 90 days old)
Remote Desktop on its default port, 3389	3 of 3	2 of 3

Two patterns stand out.

Where the firm acted, settings improved. The server whose firm worked through the audit went from 41 to 65: lockout on, Defender on, the remote-management service (WinRM) closed, Remote Desktop restricted. The other two moved much less.

On all three, updates drifted. At the first audit two of the servers had installed a Windows update within 30 days. Six months later none had. Monthly updates are easy to forget when nothing appears to be wrong.

Scores are only roughly comparable over time, because the audit gained checks during the period; the table above compares like with like.

What a fresh server looks like

For comparison, two brand-new Windows Server machines that Prixl runs in the cloud scored 57 and 53 at their first audit. They also had no minimum password length. Fresh does not mean hardened: password policy, lockout and Remote Desktop exposure are left to whoever sets the server up.

A ten-minute check for your own server

Run these in an administrator PowerShell window on the server. Each line says what you should see.

Check	Command	You want to see
Password length, history and lockout	`net accounts`	Minimum password length at least 15 (14 on servers older than Windows Server 2022); minimum password age 1 day; maximum password age Unlimited, unless an auditor requires otherwise; history 24; lockout threshold 5 to 10

Check	Command	You want to see
Firewall on, all profiles	`Get-NetFirewallProfile -PolicyStore ActiveStore | Select-Object Name, Enabled`	True for Domain, Private and Public
Defender running	`Get-MpComputerStatus | Select-Object AMServiceEnabled, RealTimeProtectionEnabled`	True and True, or your own antivirus confirmed running
Last Windows update	`Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 1`	A date in the last 30 days
Who is an administrator	`Get-LocalGroupMember Administrators` (if it shows an error, `net localgroup Administrators`)	Only named people who need it
Guest account	`Get-LocalUser Guest | Select-Object Enabled`	False
SMBv1	`Get-SmbServerConfiguration | Select-Object EnableSMB1Protocol`	False
Network Level Authentication	`(Get-CimInstance -Namespace root\cimv2\TerminalServices -ClassName Win32_TSGeneralSetting -Filter "TerminalName='RDP-Tcp'").UserAuthenticationRequired`	1
Remote Desktop reachable from the internet	Ask your IT provider whether port 3389, or whatever port Remote Desktop uses, is forwarded from the router	No. Use a VPN instead
Clock synchronised	`w32tm /query /status`	A recent "Last Successful Sync Time" (CERT-In expects NIC or NPL time servers)

If any line is not what you want to see, the matching control and the reason for it are in Prixl's free *Information Security Policy for CA Firms*.

Method

Audits are Prixl Warden's own checks, run on the server: password settings from `net accounts`, Defender status from `Get-MpComputerStatus`, update age from the newest installed hotfix, firewall profiles from Windows' firewall settings. "First audit" is the first audit after installation, in March 2026; "latest" is the audit in early October 2026. Published under section 8 of the Prixl Warden licence terms; no firm or server is identified.

PRIXL

About Prixl. Prixl Technologies builds Prixl Warden, which audits and hardens the Windows servers of small professional firms, fixes common settings in one click, and alerts the partners when something changes. More at prixl.io. Questions: support@prixl.io.

General information, not legal or professional advice; observations of three servers, not statistics about the profession. © 2026 Prixl Technologies. You may share this note in full, unchanged, with credit to Prixl Technologies.