



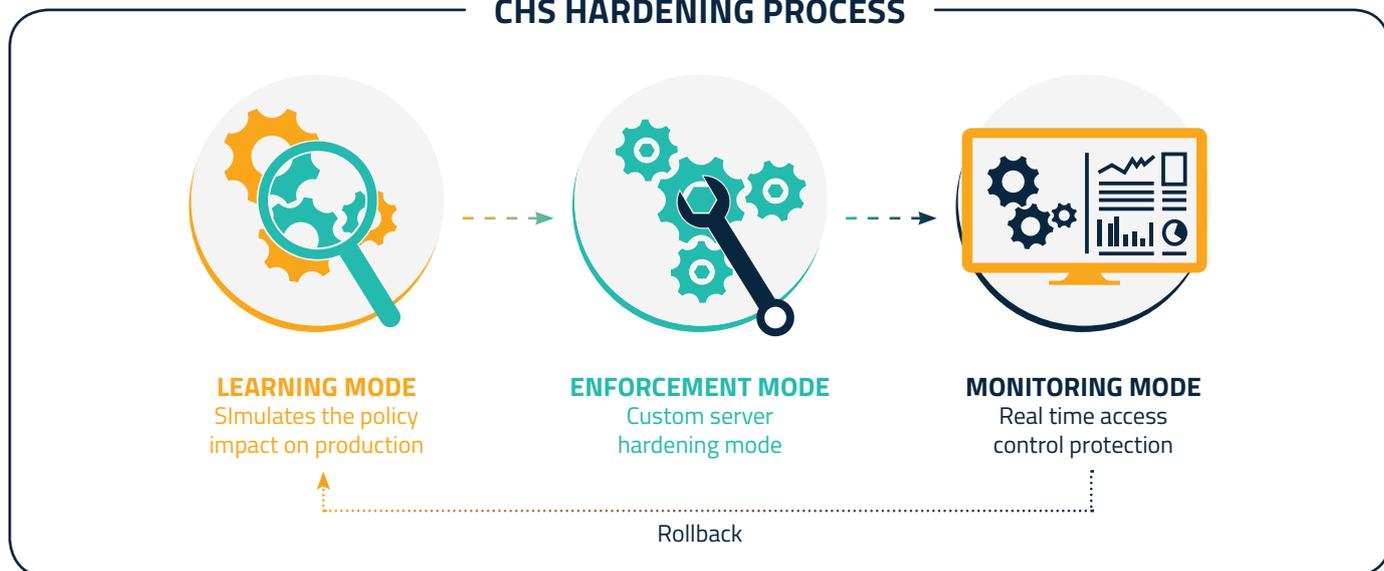
BOOST COMPLIANCE WITH CHS AUTOMATED SERVER HARDENING

CalCom CHS is a solution for automating and managing server configuration hardening. CHS offers the unique ability to 'Learn' where desired hardening changes will adversely impact production activity. CHS determines the impact of baseline changes before they implemented, and in doing so prevents outages. CHS eliminates time consuming testing, dramatically improves compliance posture, and reduces the cost and impact of hardening.

WINDOWS SERVER HARDENING CHALLENGE

Windows server hardening is time consuming, costly and impacts production server activity. Long hours are spent testing target policies in a lab environment before promoting them to production. Unfortunately, even the best lab environments fail to fully simulate production server activity. It is impossible, through testing alone, to ensure that production will not be impacted by hardening efforts. Due to limited testing resource, and out of concern for production stability, organizations rarely harden more than a small subset of recommended configuration settings – this to the detriment of the organization's compliance and security posture. Once implemented, maintaining hardened settings is an upstream battle. Multiple privileged users in an enterprise environment all but guarantee configuration drift, requiring additional work to determine gaps, reestablish baseline standards, and ensure audit readiness.

CHS HARDENING PROCESS



CHS HARDENING SOLUTION FOR WINDOWS®

The CHS Hardening Solution for Windows implements an automated approach that dramatically improves the breadth of baseline coverage with respect to hardening standards, while reducing time and money spent. Only CHS eliminates the need to manually test baseline changes prior to promotion, effectively automating the very expensive and time-consuming test process. How does CHS do this? For each server in your environment, CHS's proprietary 'Learning' mode observes production activity over time with respect to the desired policy. CHS automatically builds an understanding of production activity that will be impacted or broken by a proposed configuration change – without manual testing. From this understanding, CHS builds, deploys and enforces the optimal 'non-impactful' policy for each server in the enterprise!

THE CHS POLICY CENTER

| Description | Expected Value ¹ | Actual Value ² | Match ³ | Mark |
|---|-----------------------------|---------------------------|--------------------|-------------------------------------|
| Section: System Access | | | | |
| Accounts: Guest account status | 0 | 0 | True | <input checked="" type="checkbox"/> |
| Accounts: Administrator account status | 1 | 1 | True | <input checked="" type="checkbox"/> |
| Network access: Allow anonymous SID/name ... | 0 | 0 | True | <input checked="" type="checkbox"/> |
| Store passwords using reversible encryption | 0 | 0 | True | <input checked="" type="checkbox"/> |
| Accounts: Rename guest account | "Adm" | "Guest" | False | <input checked="" type="checkbox"/> |
| Accounts: Rename administrator account | "Dave" | "Administrator" | False | <input type="checkbox"/> |
| Network security: Force logoff when logon ho... | 1 | 0 | False | <input checked="" type="checkbox"/> |
| Account lockout duration | -1 | -1 | True | <input checked="" type="checkbox"/> |
| Reset account lockout counter after | 99999 | 99999 | True | <input checked="" type="checkbox"/> |
| Account lockout threshold | 5 | 0 | False | <input checked="" type="checkbox"/> |
| Enforce password history | 24 | 24 | True | <input checked="" type="checkbox"/> |
| Password must meet complexity requirements | 1 | 1 | True | <input checked="" type="checkbox"/> |
| Minimum Password Length | 14 | 7 | False | <input checked="" type="checkbox"/> |
| Minimum Password Age | 1 | 1 | True | <input checked="" type="checkbox"/> |
| Maximum Password Age | 90 | 42 | False | <input checked="" type="checkbox"/> |
| Section: User Rights Assignment | | | | |
| Deny log on as a batch job | nt authority\anonym... | | False | <input checked="" type="checkbox"/> |
| Deny access to this computer from the network | nt authority\anonym... | | False | <input type="checkbox"/> |
| Debug programs | builtin\administrators | builtin\administra... | True | <input checked="" type="checkbox"/> |
| Create permanent shared objects | | | True | <input checked="" type="checkbox"/> |
| Create a pagefile | builtin\administrators | builtin\administra... | True | <input checked="" type="checkbox"/> |
| Change the time zone | builtin\administrators... | server operators... | False | <input checked="" type="checkbox"/> |
| Change the system time | builtin\administrators... | server operators... | False | <input checked="" type="checkbox"/> |
| Bypass traverse checking | nt authority\network ... | window manager... | False | <input checked="" type="checkbox"/> |
| Back up files and directories | builtin\administrators | builtin\backup op... | False | <input checked="" type="checkbox"/> |
| Allow log on through Remote Desktop Services | builtin\remote deskto... | builtin\administra... | False | <input checked="" type="checkbox"/> |

1 Expected Value
Displays the desired policy value.

2 Actual Value
Determines the object's current status – shows its "actual value".

3 Match / Impact
Indicates the impact of hardening as the following:

False: When yellow, the value will be changed when enforcing the policy - with no impact on server operation.

False: When red, the object is used by the production system and the actual value is valid, therefore, hardening the policy will cause damage to servers in production.

The above Impact Analysis Report is generated by CHS at the end of the learning period. This report projects the impact of the target policy on production activity. The desired value for each object to be hardened is shown in the "Expected Value" column. Actual values observed during Learning Mode are shown in the "Actual Value" column. Finally, the projected impact on production of hardening per the target policy is shown in the "Match" column. From this Gap Analysis report, the optimal "ready-to-go" promotion plan is generated for each server, one that maximizes policy compliance while avoiding impact to production.

THE CHS POLICY ANALYSIS CENTER

The CHS Policy Analysis Center presents each server's compliance and risk posture. The Policy Analysis Center helps IT management prioritize baseline hardening tasks, and assists in documenting and managing unhardened objects as "exceptions" in support of audit requirements.

