



## What is Policy Minder?

**Policy Minder** is about “enforcing” your i5/OS and OS/400 security.

**Policy Minder** is security compliance management tool designed by iSeries expert Carol Woodbury.

By managing your user profile settings, library authorities, file authorities, directory authorities, system values and more; **Policy Minder** enables you to keep to your security implementation at “the way you want it to be.”

## SkyView Policy Minder For i5/OS and OS/400

### Case Study:

#### Managing user profile configuration compliance

One area of compliance that made a lot of extra work for this administrator was user profile configuration management. Here's how Policy Minder made that task bearable.

#### Identifying Inactive Profiles and Documenting the Exceptions

One area that was difficult to manage was inactive profiles. No OS/400 tools are available to list the inactive profiles. Furthermore, some profiles are always inactive – group profiles, profiles that own applications, etc. Sorting these profiles from the “real” inactive profiles was tedious and hard to explain to his auditor. This administrator created a Policy Minder user profile template that included all profiles on his system except for the profiles that are always active and then specified an inactivity period of 60 days. He has scheduled a compliance check for this policy to run nightly. In the morning he reviews the compliance report to see if any profiles have exceeded the allowed 60 days of inactivity.

Explaining to his auditors how he manages this part of his security policy is now very easy. He shows them the Policy Minder template, which documents the profiles that are always inactive and shows how the compliance report is reviewed on a daily basis.

#### Managing the Number of \*ALLOBJ Profiles and How they're Created

This administrator's internal auditors required that he adhere to a policy that allowed only 8 \*ALLOBJ profiles on his production system. In addition to specifying how many profiles with \*ALLOBJ can be on the system, the internal auditors require that the profiles be configured to

- change their passwords more frequently than the rest of the user community (every 30 days rather than every 90 days)
- have command string (\*CMD) auditing turned on (so that every command is logged)
- ensure that the profiles' passwords cannot be a default password.

To monitor this policy he created a user profile template that included all profiles with \*ALLOBJ special authority (you don't need to know who these users are ahead of time – just specify that the template should contain all users with this special authority and Policy Minder determines the rest.) He runs a compliance check on this template once a week to ensure that the allowable number has not been exceeded and that the profiles are configured per his company's policy.

#### An Easy Fix

After reviewing the compliance report, he runs the Policy Minder FixIt function which sets non-compliant profiles to the attributes as defined in the policy.

**For More Information on SkyView Policy Minder:** Contact SkyView Partners or an authorized SkyView Reseller.

