



SkyView Policy Minder for i5/OS and OS/400

FAQs

I do all of this already - why do I need Policy Minder?

System Administrators find themselves taking hours of time and lots of resource just to make sure policies are enforced and implemented properly, ... but how thoroughly?.. and do you check EVERY object in a Library? plus EVERY profile? plus EVERY directory? Policy Minder's tasks range from checking configurations to repairing problems as they arise on everything from library authorities, to directory authorities, to system values, to user profile configurations and more. Rather than spend the hours doing this manually (and not completely), Policy Minder lets you check compliance automatically.

Why should I try Policy Minder, when I haven't fully implemented Risk Assessor?

First, let's make one thing perfectly clear; Risk Assessor and Policy Minder are totally independent products that do two very important, but very different things. Risk Assessor is about "judging" your security. By comparing your security to industry best practices, Risk Assessor gives you documentation of where you may have areas of concern, as well as, what steps are necessary, if you chose to change how you are doing security. Policy Minder is about "enforcing" your security. Policy Minder is designed to automate the process to keep you in compliance with whatever your existing security implementation is. In short, no security implementation will ever be perfect, but whether you have completed all, some, or even none of Risk Assessor's recommendations, you still have the need to be in compliance with your "existing" security implementation.

Can Policy Minder check object ownership so programs are easily maintainable?

Yes! Let's say that John the programmer promotes some source changes into the production application. The ownership of these objects is set to: JOHNV. But, the profile that should own objects in production is: SUPERGROUP. The System Admins dutifully back up all SuperGroup libraries... but don't know about JOHN V. John leaves the company and they delete his libraries. **Oops!** The source for several objects is now gone. If Policy Minder was in place, the System Admins could check to make sure that all objects were owned correctly, so that all libraries can be backed up properly... Without Policy Minder you have to manually check everything.. OR hope that they follow change management procedures.

Can Policy Minder reduce the risk of exposure by making sure that *PUBLIC authorities are set appropriately for files and libraries with sensitive information?

Yes! Let's say that you're a healthcare company, and you (obviously) have files in libraries that contain sensitive patient information. Say all the files are set to PUBLIC *EXCLUDE, but your programmers, etc. are constantly changing programs etc. and in doing so they are "resetting" public authority to *USE or *CHANGE. This violates security policy and creates huge exposures to information. With Policy Minder, you look at the PUBLIC setting comparing it to your policy of *EXCLUDE. For those files that pop up with something other than *EXCLUDE... you use "FixIt" to set them appropriately.

Can Policy Minder help me know a system is "fail over ready" in my HA (High Availability) environment?

Yes! Let's say that you have a high availability system and you need to ensure that the system's security settings match the current production system. User profiles, libraries, and directories with the appropriate authority and ownership need to be configured the same on both systems and system values need to match before you can "fail over" to the target system. Using Policy Minder you can take your policy from the current production system and "import" it to the fail over system. When you run a compliance check, Policy Minder will identify the "mismatches" between the production system and the target system for user profile attributes, object authorities, object ownership and more. To rectify the situation if mismatches are discovered, you can run "FixIt" to configure User Profiles to have the correct special authorities, group profiles, initial menus, etc. You can also run FixIt to correct any libraries' or directories' (or the objects contained in them) ownership or authorities settings as well as use FixIt to set system values to the appropriate value. This way you can ensure the security system values, user profiles and object authority settings on the fail over system match the settings on the production machine.

