NetIQ Universal Policy Administrator

Policy orchestration, consolidation, and normalization. NetIQ Universal Policy Administrator provides an automated, centralized, and consistent policy management solution and enforcement, for a wide variety of endpoints: Windows, Linux, Mac, or Non-Domain Joined Windows devices.

Introduction

Historically, organizations have relied on a siloed and disparate approach of managing security and configuration policies and controls, such as AD, GPOs, Linux, MDM, Mac controls, etc. It also takes many different people with different domain expertise, to agree on and manage the various taxonomies, which makes centralizing management difficult. As a result, organizations experience issues including configuration and security control drift, which can result in breaches and failed audits. In a world of escalating security breaches and expanding compliance regulations, it makes no sense to expose your organization to heightened risk with decentralized and disorganized security policy management.

So centrally managing both Windows and non-Windows resources within a single pane of glass and controlling access with a single identity, or in policy groups, improve efficiency, especially as you move to the cloud (if you haven't started already). This approach enables you to skip the manual, fragmented management processes and scripts by unifying how you manage authorization and authentication across your entire environment. Utilizing a single management platform to access every system simplifies your entire identity and access management strategy. With Universal Policy Administrator (UPA), you can control all your policies from a single cloud-based console using a very familiar tool—your browser!

Product Highlights

Control all your policies from a single console using a modern, cloud-based solution. Most organizations have multiple platforms in their ecosystem. Whether you're using Windows, Linux, Mac, or Non-Domain Joined Windows devices, you can pull all of them into the UPA system and place them under centralized policy management. This will simplify policies by translating various policy mechanisms into a simplified policy language, which can then be applied to the endpoints in the multiple silos, multiple platforms. In fact, these resources can live anywhere—on premises, in any cloud, even in a container.

This means that you can update all of your policies in one place and document what was done when, and by whom. Compliance audits will be much easier, regulators will be impressed with how organized you are, and you'll look like a hero because the auditor didn't need to overstay their welcome. Additionally, UPA identifies policy conflicts and collisions. Or if someone does try to bend the rules or makes a configuration error, you'll catch it before the policy is deployed, helping you to prevent potential security lapses.

Universal Policy Administrator at a Glance:

- **Policy Consolidation:** Improve ROI by centrally managing existing platform investments by extending your privilege, delegation, and policy management toolsets to all managed resources.
- **Device Management:** Increase efficiency by centrally resources within a single pane of glass and a single identity.
- **Compliance Requirements:** reduce risk by implementing consistent security controls and auditing capabilities across your entire environment.

Key Features

We live in a complex IT world of on-premises, cloud, service, and XaaS configurations. Regardless of your deployment, you will have multiple security policies, but using UPA will make managing them infinitely easier. Any conflicting settings or security controls can be quickly and easily resolved, because you're managing them through policy, from a central location. You can resolve any conflict in policies and avoid the hours of writing scripts that are incomprehensible to anyone but the person who created them. Instead, you utilize UPA to manage the rules across your entire IT ecosystem.

With UPA, policy scope goes beyond the mundane. UPA supports policy that helps protect operating systems, COTS and custom applications, remote services, and more. Flexibility is required in today's complex environments. UPA supports a variety of endpoints, regardless of where they "live" or when they come online. You can even cover specific settings in customer application configurations while leaving other configuration settings that are more bespoke up to the individual server or service—by only putting a portion of configuration under policy.

Capabilities

POLICY CONSOLIDATION

- A single pane of glass solution that provides you the ability to perform policy management for devices throughout your complex and hybrid enterprise, including Windows GPOs, Mac, Linux, and non-domain-joined Windows machines.
- Reporting is greatly simplified. Gone are the days of collecting various log files or custom reports and then consolidating them in a spreadsheet.

DEVICE MANAGEMENT

- You and your fellow policy administrators are able to continue managing specific devices without having to hand over policy management to anyone else. You can utilize the policy translation and simplification processes within UPA, without the need to leverage complex or non-intuitive scripting methods.
- Delegation of resources is a key method to let experts manage their specific applications and technology through policy without handing them the keys to the kingdom. With UPA, you can let Linux experts manage Linux resources and Windows admins manage their resources.

COMPLIANCE REQUIREMENTS

You know what a burden compliance requirements are. It's tough to decipher the specific policy settings, and capturing audit logs continues to frustrate auditors and compliance officers. You can make your job easier. With UPA, auditors and compliance teams can easily run policy setting reports, audit history, and conflict analysis details to ensure policy administrators are complying with industry regulations, as well as track who is making changes to security policies throughout the enterprise.

Key Benefits

- Simplify and transforms security and configuration policies into readable and translatable language for systems within the control of UPA.
- Support versioning and rollback if anything goes wrong or some setting isn't working as expected.
- Manage policies from a singular delegated cloud-hosted web console across multiple policy silos.
- Rest easy with an Offline Policy Repository for safe and effective policy management when creating and testing security policies.
- Simplify device security policy by extending policy management control and authority to devices that do not typically live under the control of AD GPOs:
  - Linux
  - MAC
  - Non-domain-joined Windows machines
  - Cloud-based or on-premises resources
- Allow policy administrators to manage their respective devices without having to hand over control to other administrators.
- Extensive out-of-the-box reports for RSOP analysis, conflict analysis to help alleviate the complexities of determining policy order.
- Centralize and simplify policy management across multiple domains, forests, cloud-based VMs, and various workstations.

Key Differentiators

Reduce policy silos. With today's technology, there's no reason to let a mishmash of security policies lead you to a security breach or compliance violation. Control all of your policies from a single console that unifies policies and provides a single pane of glass into your policy environment.

Continue to use what you have. We have extended AD capabilities so that they no longer apply to Microsoft alone. Whether you're using Linux, Mac, or Non-Domain Joined Windows devices, you can pull all of them into the UPA system and place them under centralized policy management.

One policy applies them all! You will still have multiple security policies, but managing them will be much easier. Any conflicting policies can be quickly and easily resolved because you're managing them from a central

Contact us at **CyberRes.com**
Like what you read? Share it.

location. You can resolve any conflict in policies and avoid the hours of writing scripts. Instead, you will utilize UPA to manage the policies across your entire system.

Compliance isn't easy, but it can become easier. Save time and hassle associated with compliance. You can update all of your policies in one place and document what was done when, and by whom. Compliance audits will be much easier, and regulators will be impressed with how organized you are. Additionally, UPA identifies policy conflicts and collisions before a policy is deployed, helping you to prevent potential security lapses.

Set the standard, keep it that way. You can improve security by avoiding the mistakes and loopholes created by fragmentation. With UPA, you can create company-wide management standards. For example, you could institute a workflow that requires a second manager to approve and validate changes to a security policy before they are deployed. This type of policy can stop administrators from skirting the rules and keep your organization safe and compliant. So if someone does try to bend the rules or makes a configuration error, you'll see it on a central dashboard, or the security team can see it from their SIEM dashboard. Then you can quickly contact the admin and fix the problem before it causes any serious damage.

It's part of something bigger. With the Micro Focus portfolio of universal policy management solutions, you can be certain that your security rules are enforced throughout the enterprise at all times. And you can easily make compliance changes or correct any misconfigurations from a single, central console. Instead of having IT technicians who write complex scripts for a multitude of outside applications and having no oversight of their work, you can simply use AD in conjunction with UPA to control your policies—just as you have always done within Microsoft. Every server, app, or device that you move to the cloud is scrutinized in advance to ensure security, compliance, and compatibility. As your company moves more workloads to the cloud, you need a security policy solution that moves with you, not against you. Micro Focus makes the transition easy and gives you the visibility and control that a 21st-century workplace demands.