Virtual Identity Server for Automated Compliance Management™

Providing a codeless solution for performing automated real-time compliance with an AD Environment

The Virtual Identity Server for Automated Compliance Management (VIS for ACM™) provides organizations with a point and click, codeless, automated solution for performing compliance related tasks within the Active Directory (AD) environment in near real-time. This powerful compliance engine is built upon and leverages the virtual directory component of the Virtual Identity Server to provide a complete easy to use compliance tool.

How it works

Step 1—Define Policy Filter

Using a familiar "Office" interface, administrators define policy filters. The policy filter defines what *criteria or condition* they are looking for within their environment. For example, an administrator could set a policy filter to find all users across all domains/forests that have changed their password today.

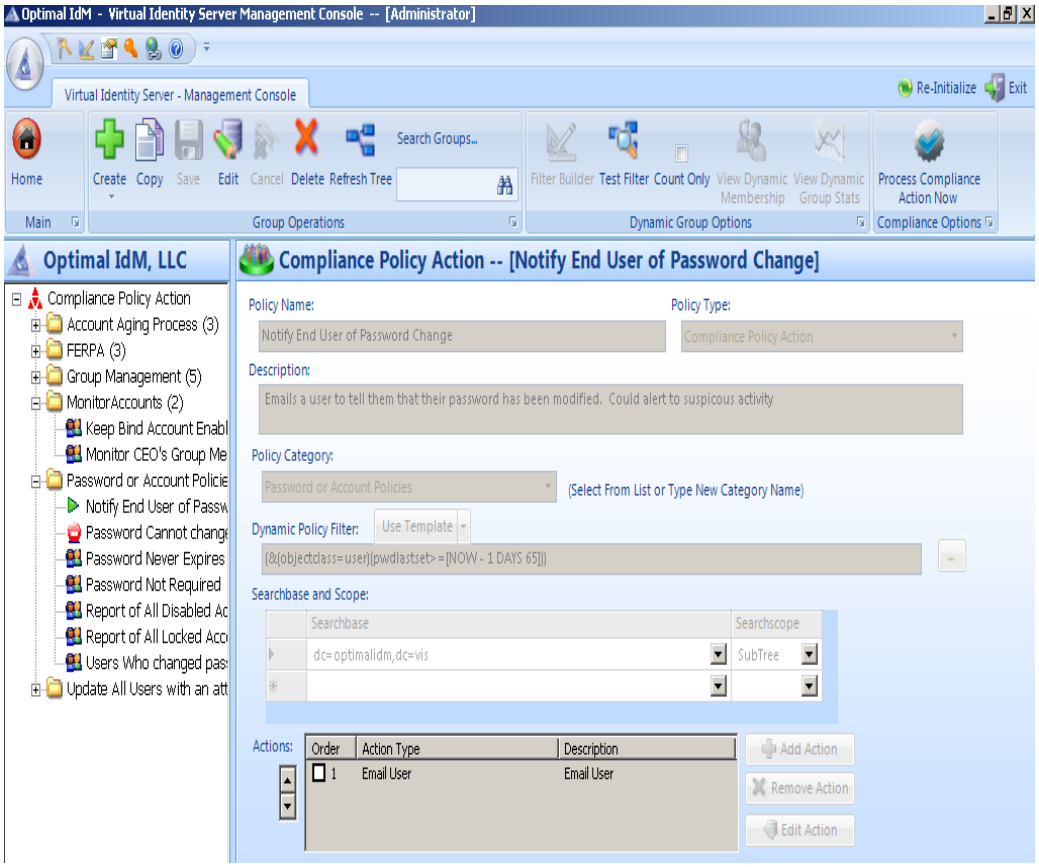
Step 2—Define the action to take

The administrator then defines what *action* to take based on this condition. There are over 20 out of the box actions, ranging from reporting/exporting data, e-mailing end users/managers, to taking corrective action to remediate the situation.

In this example the administrator defines, via the point and click interface, an action to e-mail the end user with a personalized e-mail informing the user their password was changed. This would alert an end user that their account was compromised if they did not initiate the password change.

Step 3—Automate the process

The administrator then defines the processing interval for this policy, such as once a day/hour.
A standard Windows service then monitors and performs this policy on the configured interval.



Point and Click Codeless Solution Achieving Automated Compliance

Over 20 out-of-the-box actions

Installs in under 5 minutes

http://www.optimalidm.com/vis/

Virtual Identity Server for Automated Compliance Management

Example Use Cases

- **Monitor Application Bind Accounts** to ensure that their password has not changed or been disabled. In the event this occurs, multiple actions such as emailing administrators or re-enabling the account can occur.
- **Benefit:** Prevents system outages for key applications.
- **Monitor & Enforce AD Group Membership** Monitor and optionally enforce the membership of Active Directory groups in real-time. Administrators control the criteria and the optional corrective actions (adding/ removing users from the group).
- **Benefit:** Stops a rogue end user or administrator from changing group membership for key groups.
- **Automate Account Aging Process** by emailing end users or managers with accounts that have inactivity over x days. Accounts can then be automatically moved, disabled or deleted after further inactivity.

  Benefit: Reduces user identities no longer in use, lowers risk of systems breach, or audit failure.
- **Separation of Duties (SoD) Compliance** can be achieved by identifying toxic combinations as the policy filter. For example, users that are a member of the Check Writing AD group should not be a member of the Invoice Approval AD group.
- **Benefit:** Event notifications (emails/reports) can instantly alert administrators of the condition, and can also be remediated automatically.
- **Attestation** can now be completely automated to delegated administrators and end users. ***AD Group attestation*** can be achieved by periodically reporting/ notifying AD group owners of the members of the group, or optionally making group owners attest/verify the members of the group. ***Likewise, AD user attestation*** can be achieved by periodically reporting/notifying managers of end users access and optionally having them attest/verify the permissions for their employees.
- **Benefit:** Manual attestation processes (or no process) can be quickly and easily automated to gain compliance and eliminate audit failures.

Key Benefits

Automate manual processes in minutes with easy to use point and click configuration.

Requires no custom coding or skills, using a familiar "Office" look and feel.

Enables administrators to easily monitor and remediate their Active Directory infrastructure.

Lower Total Cost of Ownership (TCO) by installing in minutes and leveraging the Virtual Identity Server platform and the existing investment in the Microsoft platform.

Continuous Return on Investment (ROI) by providing built-in extensibility to develop custom actions.

Single Point of Administration for achieving and maintaining compliance across multiple forests.

Achieve immediate and instant payback Deploys in minutes and comes with over 20 out-of-the-box actions ranging from reporting to email notifications to actions that remediate the situation.

Provides compliance across multiple disparate systems such as extranet LDAP directories.

AD group membership can be monitored and enforced in near real time.

Leverages and extends the existing investment in the Microsoft platform.

Technical Specifications

- **Microsoft .NET 2.0 Framework or Greater**
- **40 MB of Disk Space**

About Optimal IdM, LLC.

Optimal IdM, LLC. is a leading global provider of identity management consulting and software solutions. Headquartered in Land O' Lakes, Florida, Optimal IdM provides sales and services through regional offices across the United States and a growing network of resellers and distributors.

Optimal IdM's customers include Fortune 1000 companies, as well as, Federal, State and Local Government agencies in more than 12 countries on 4 continents. Founded in 2005, Optimal IdM is privately held and has been profitable in every quarter since inception.

For more information on our products and services, please visit our website at http://www.optimalidm.com or call +1.813.425.6351

Optimal IdM, LLC.
2209 Collier Parkway, Suite 140
Land O' Lakes, FL 34639
Email: Sales@optimalidm.com
Phone +1.813.425.6351
Fax +1.813.425.6351