



## ACCOUNT RESET CONSOLE SPOTLIGHT FEATURE: DELEGATION

### ACCESS MANAGED

Account Reset Console (ARC) is a highly configurable web based solution. Already a complete packaged tool, the flexibility of **delegation** is the red bow that ties the tool together and separates it from the competition.

ARC's management settings allow administrators to delegate:

- Who can logon to the web interface.
- Who can reset other users passwords.
- Who can view console logs and task reports.


In addition to delegating who has access, another strong feature of ARC's delegated management is the account reset features. Here, administrators are able to define rules for when accounts are reset.

For example:

- Should disabled accounts be disabled?
- Should locked accounts be unlocked?
- Should it be required that passwords be changed on next login?

For each option, the administrator defines the rule by selecting "Always," "Optional" or "Never."

In delegating who is able to log on and reset passwords, it is critical that the proper hurdles are in place to maintain security. Thus, administrators can rest assured that no matter who is granted access, they will still have to confirm their identity (set in the "Configuration" stage) before making any changes.


**LIEBERMAN SOFTWARE**  
**Account Reset Console**

Logged-in user: DOMAINjoe
[Log Out]

Accounts Scheduling/Reporting Management Configuration Index

**Manage Program Access Permissions**

<p><b>Program Access</b></p> <p>Group Access</p> <p>Account Reset Features</p> <p>Password Change Features</p> <p>Configure Email Settings</p> <p>Appearance</p>	<p><b>Add a New Global Program Access Rule:</b></p> <p><input type="checkbox"/> Allow Web Logon</p> <p><input type="checkbox"/> Allow Reset of Other Users' Accounts</p> <p><input type="checkbox"/> View Console Logs and Task Reports</p> <p><input type="checkbox"/> Manage All Web Access Controls</p>
--	--

**Global Program Access Rules**

Global Access Category	Allowed Windows Groups
Allow Web Logon	domain\domain admins <a href="#">[del]</a> DOMAIN\can reset <a href="#">[del]</a> DOMAIN\Manage All Access Controls <a href="#">[del]</a> DOMAIN\test <a href="#">[del]</a> DOMAIN\self service reset group <a href="#">[del]</a>
Manage All Web Access Controls	domain\domain admins <a href="#">[del]</a> DOMAIN\Manage All Access Controls <a href="#">[del]</a>
Allow Reset of Other Users' Accounts	domain\domain admins <a href="#">[del]</a> DOMAIN\can reset <a href="#">[del]</a> DOMAIN\Manage All Access Controls <a href="#">[del]</a> DOMAIN\test <a href="#">[del]</a>
View Console Logs and Task Reports	domain\domain admins <a href="#">[del]</a> DOMAIN\Manage All Access Controls <a href="#">[del]</a>

**Use this screen to grant access to this system to specified Windows Groups.**

- Allow Web Logon:** This privilege allows users to logon to the Account Reset Console.
- Allow Reset of Other Users' Accounts:** This privilege allows users to reset other users' passwords. Example holders of this permission would be help desk personnel.
- Manage All Web Access Controls:** This privilege allows users to manage program and group access permissions, and to view the system logs.

To add a Program Access Rule, select the appropriate permissions on the left side and a Windows Group from the second menu, and click the Add Global Access Rule button.

Global Program Access Rules can be deleted by clicking the 'Del' link to the right of each rule.

Emergency revocation of privileges should be followed up with a webserver reset.