



Altiris® 6

Local Security Solution™

CENTRALIZED MANAGEMENT OF LOCAL GROUP MEMBERS AND PASSWORDS

BENEFITS

- > Gain visibility and control over local users and groups
- > Enforce consistent local account memberships
- > Randomize passwords based on strong password criteria
- > Cycle passwords on administrator defined schedules
- > Detect and resolve compliance anomalies

Arellia™ Local Security Solution™ provides centralized management that quickly and easily provisions and manages local administrative users and groups within the environment. Local Security Solution's automated policy enforcement of group membership and randomization of administrative passwords across systems secures the corporate network from malicious attacks on an organization's information assets.

PROTECT YOUR ORGANIZATION'S INFORMATION

An organization's sensitive and proprietary corporate information assets must be protected at all costs. Through proper implementation of local security policies, organizations can protect that information from attack. Comprehensive management also prevents employees and outsiders from exploiting weak security to browse confidential files, commit fraud or launch dangerous code. By protecting information through proper security controls, organizations also satisfy the requirements of many regulations by implementing reasonably hard to compromise local logon credentials.

INVENTORY AND PROVISIONING

Without centralized inventory and provisioning of local accounts and memberships, organizations rarely understand the true state of who has access to individual systems and therefore the potential security risks. As a result, the door is open to both malicious individuals and to uninformed users who unintentionally make configuration changes and compromise system security. Local Security Solution reduces 90 percent of the labor and time costs associated with manual configuration changes or scripting of local users and accounts. Centralized maintenance is simplified through policy-based management that remotely inventories and provisions user and group accounts with specified rights. This allows end users who are members of the group to access and use system services based on the rights specified in the account.

GROUP POLICY ENFORCEMENT

Policy-based enforcement of users and groups is important so that unauthorized users are not granted privileges they should not have. IT management increasingly wants to lock down desktops, but technical, political, and resource requirement obstacles have prevented widespread

adoption. As a result, users with administrative privilege may easily create and modify local administrative accounts. Local Security Solution's group provisioning policies help preserve the integrity of your local group accounts with automated group membership enforcement. The solution helps ensure that unauthorized users are not maliciously or mistakenly added to administrative group accounts.

PASSWORD RANDOMIZATION AND CYCLING

Avoid problems with a single password that works on all instances of local administrative accounts in your environment. Local Security Solution significantly tightens security in your environment by automating the cycling of administrative passwords and ensuring that every instance of a managed user or group account in the environment has a randomized password. By instituting automated password cycling and randomization policies, Local Security Solution allows you to limit use of administrative passwords and help prevent unauthorized access to your organization's systems management environment.

COMPLIANCE REPORTING

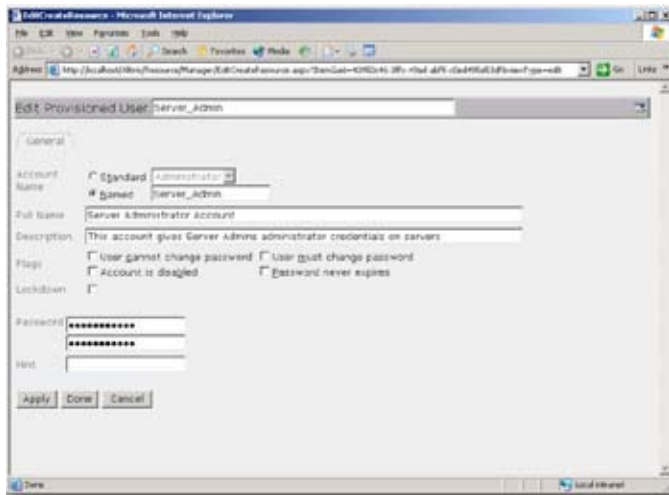
The mandates of numerous regulations, such as Sarbanes-Oxley, HIPAA, and FISMA, require the implementation of reasonably hard-to-compromise local logon credentials. Tightening controls around local account credentials mitigates outside or insider attempts to compromise data covered by the regulations, such as financial data or patient records. Validating compliance of local accounts across similar systems reduces the risk of unauthorized users gaining administrative access. With Local Security Solution you can detect account anomalies in your environment by generating compliance reports that detail all account-related differences between a known secure baseline system and a corresponding collection of systems.

“As any security pro will tell you, the network perimeter is getting harder and harder to define, let alone defend. Moreover, those who have authorized access to internal resources are often far more dangerous than those who need to breach a perimeter firewall to get inside the network.”

—FORRESTER RESEARCH
 “Securing the Network from the Inside Out”
 Paul Stamp & Robert Whiteley
 November 2005



Randomize passwords using strong password criteria, such as specified password length and character complexity.



Create, delete, and/or modify local accounts, including descriptions and user account flags.

SYSTEM REQUIREMENTS

Local Security Solution requires that you install and configure the Altiris Notification Server™ version 6.0 SP3.

Notification Server Minimum Requirements

- > Processor—Pentium® III 800 MHz or faster
- > Memory—1 GB RAM
- > Hard drive—20 GB
- > Operating system—Windows® Server 2003 or Windows 2000 Server
- > Database—Microsoft® SQL Server 2000 SP3
- > Browser—Microsoft Internet Explorer 6 or later

Local Security Solution supports these client operating systems

- > Windows 2003 SP1
- > Windows XP SP1 or higher
- > Windows 2000 SP1 or higher

TRY LOCAL SECURITY SOLUTION FOR FREE!
 Download a free 30-day evaluation version of Application Control Solution at www.arellia.com/eval

Copyright © October 2009, Arellia, Inc. All rights reserved. Except as provided in Arellia's license agreement governing Arellia Application Control Solution, Arellia assumes no liability whatsoever, and disclaims any express or implied warranties relating to the use of this product, including without limitation, warranties of fitness for a particular purpose, merchantability, or infringement of any third-party intellectual property rights. Altiris may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to this product. The furnishing of this document and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any foregoing intellectual property rights. *Other brands and names are the property of their respective owners.