

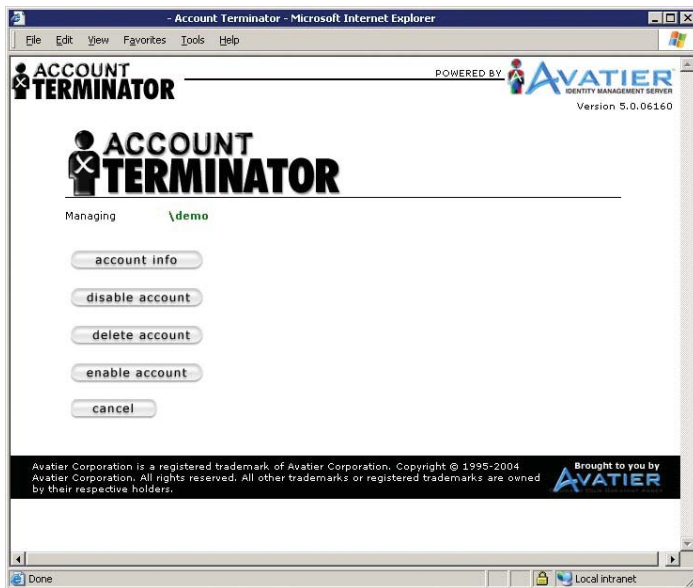
# ACCOUNT TERMINATOR™

## Automated User Deprovisioning

**Joe left the company four months ago but can still logon to all his systems. The auditors are asking for a list of terminated employees to test access. You are paying to license software for departed employees.**

IT organizations are starting to recognize that timely elimination of dormant accounts from their various systems will result in lower software license costs and better protection from security breaches. Account Terminator™ lowers these costs by deactivating all associated accounts for former workers with one simple procedure while properly documenting the process for auditors.

New market and privacy regulations require organizations to implement and audit internal access controls to achieve compliance. With the workforce constantly being redefined by mergers, acquisitions, reorganizations, divestitures, and general staff reductions, the problem and expense of tracking who has access to what systems is becoming a top priority. Account Terminator allows your IT staff to securely disable and/or delete employee user accounts across multiple platforms through an administrative web browser that also provides a complete audit trail.



Avatier's simple and intuitive Account Terminator web interface allows delegated end users to securely automate enabling, disabling, deleting and displaying real-time account status across many platforms at once.

### Instant Identity Management™

Account Terminator is designed to service the needs and scale of large complex enterprises. The solution implements in minutes, not months, and it instantly delivers measurable cost savings with minimal ongoing maintenance.

The Avatier Identity Management Suite™ (AIMS) platform is the foundation for Account Terminator and other modules. AIMS provides centralized alerting, auditing, reporting, and on-demand installation of software updates with Avatier's LiveUpdate service.

### Strategic Benefits

#### Reduce exposure by eliminating overlooked accounts

When dormant accounts and newly departed employee accounts are deactivated in one swift action across all platforms, IT organizations are better able to control access and reduce opportunities for security breaches across the enterprise. Better asset management also reduces software license and maintenance costs.

#### Increase IT efficiency by automating account termination

Through delegated administration and task automation, it is possible to securely offload the administrative burden of account deactivation from central IT groups.

#### Facilitate security compliance

To ensure compliance with regulations stemming from HIPAA, Homeland Security, Gramm-Leach-Bliley, and Sarbanes-Oxley, it is vital that organizations have proper controls to system access that include the necessary levels of auditing and reporting.

### Key Features

#### Delayed Delete™

Now you can flag accounts to be initially disabled and then configure the number of days before they are automatically deleted.

#### Home directory archival

Account Terminator can automate the task of moving or copying files and directories to an alternate location upon an account deletion.

#### Scheduled usage reporting

Summary and detailed usage reports of all account deletions, disables, and enables can be sent hourly, daily, weekly, or monthly to system administrators.

#### Key account and group membership alerting

Security administrators can be automatically emailed when a flagged account is deleted or disabled. Groups can also be flagged as critical containers, such that administrators are automatically emailed any time a critical group member account is deleted.

#### Two Factor Deletion™

Account Terminator can be configured to require manager approval for all user account deletions. The manager can authorize the deletion via email.

#### Disable and delete RSA SecurID tokens

Account Terminator supports de-provisioning RSA SecurID tokens.

AVATIER™

# Platforms Supported

Password synchronization, real-time account status, account termination, and employee provisioning are natively supported on the following platforms

Platforms	Supported Versions
<b>Operating Systems</b>	
	Microsoft Windows NT/AD 4.0, 2000, 2003
	Microsoft Windows Server 4.0, 2000, XP, 2003
	Sun Solaris 2.6 and above
	HP/UX 11 and above
	IBM AIX 4.3 and above
	Redhat Linux 7.1 and above
	z/OS (IBM OS/390) V2R8 and above
	iSeries (IBM AS/400) V4R5 and above
	Digital VMS 7.3-1 and above
	Tru64 5.1 and above
<b>Directories</b>	
	RSA SecurID ACE/Server 5.2 and above
	Sun Java System Directory 4.2 and above
	Novell NDS 4.01 and above
	Novell eDirectory 8.6 and above
	Oracle Internet Directory All Versions
	Microsoft ADAM All Versions
	IBM Directory Server 5.2 and above
<b>Databases</b>	
	Microsoft SQL Server 7.0 and above
	Oracle 8.x and above
	Sybase 12.x and above
	IBM DB2/UDB 6.x, 7.x, and 8.1
	PostgreSQL 6.2 and above
	MySQL 5.x and above
<b>Applications</b>	
	IBM Lotus Notes R4 and above
	Oracle E-Business Suite 8.x and above
	PeopleSoft 8.x and above
	SAP 4.5B and above
	Infinium HCM all versions
	Agilysys LMS/MMS all versions
	Aristocrat all versions
	Infogenesis all versions
	Bally Technologies CMS all versions

## Avatier's Technology Partners



business partner



## Minimum Requirements

### Hardware

#### AIMS Administration Server:

- 400 MHz CPU speed or higher
- 256 MB RAM
- 100 MB for program files and auditing database
- Monitor capable of displaying 16-bit color or greater and a resolution of 1024 x 768 or higher

### Software

#### AIMS Administration Server:

- Microsoft XP Professional, Windows 2000 Server, Windows 2003 Server - Standard Edition. When managing either a Microsoft Windows NT or Active Directory domain, we recommend making the AIMS Administration Server a member in at least one of the managed domains.
- Not intended for Microsoft Windows 2003 - Web Edition or domain controllers
- Microsoft Internet Information Server (IIS) 5.0 or later
- Microsoft SQL Server (optional)
- Microsoft Data Access Control (MDAC) 2.8 or later
- Microsoft .NET Framework 1.1 extensions necessary

### Primary User Directory Store:

- Microsoft Active Directory
- Microsoft Active Directory Application Mode (ADAM)
- Novell eDirectory
- Sun Java System Directory Server (Formerly Sun One Directory Server and iPlanet Directory Server)
- IBM Directory Server
- Oracle Internet Directory
- Any LDAP Server

### Web Clients:

- Microsoft Internet Explorer 5.5 or later
- Firefox 1.0 and later
- Safari 1.0 or later

## Languages Supported

Arabic	Hungarian
Chinese (Simplified)	Italian
Chinese (Traditional)	Japanese
Czech	Korean
Dutch (Netherlands)	Polish
English	Portuguese (Brazil)
French	Portuguese
French (Canadian)	Russian
German	Slovak
Hindi	Spanish

## Contact

### Worldwide Headquarters

Avatier Corporation  
12647 Alcosta Blvd, Suite 140  
San Ramon, CA 94583

925-217-5170 main  
925-275-0853 fax  
800-609-8610 sales

[info@avatier.com](mailto:info@avatier.com)  
[www.avatier.com](http://www.avatier.com)  
[www.passwordstation.net](http://www.passwordstation.net)



Copyright © 1995-2007 Avatier Corporation. All rights reserved. All other trademarks or registered trademarks are owned by their respective holders.