



POSTINI STREAMLINES I.T. PROCESSES AND IMPROVES INTERNAL SECURITY WITH IDSENTRIE

Postini is the leading provider of integrated message management, serving more than 30,000 businesses worldwide and handling 3+ billion emails per week. Postini's managed services reduce the cost, risks and complications of securing and managing IP-based messaging for businesses.

Managing employee accounts is a critical part of maintaining the security and availability of Postini's company data. Maintaining different types of authentication environments has required the use of multiple account data sources. With a mix of Active Directory, LDAP, two-factor, and local machine accounts, managing accounts is burdensome. Brad Robinson, Postini's Information Security Administrator, was looking for a better way to integrate these systems. "We have gone down a long road at trying to make user account administration easy," says Robinson, "Several talented Network and System Engineers had done an admirable job at integrating our account systems, but there were still hurdles that had to be overcome, primarily around auditability." Postini maintains WebTrust, SAS-70, and Safe Harbor certifications which require frequent internal and third-party audits. "Even after our integration efforts, we still have to make periodic sweeps of our user data sources to make sure they are in sync and current. We really needed the 'single source of truth' IDSentrie provides by integrating these various sources," says Robinson.

IDSentrie also came to the rescue on another front: user password maintenance. Postini's security policy mandates employees periodically change their passwords across all account sources. IDSentrie provides a one-stop, self service web interface and seamless synchronization that all users can navigate with ease to accomplish the task.

"We've only begun to tap some of the exceptional capabilities of the IDSentrie appliance," says Robinson, "As we continue to delve into its many features, we're seeing more and more opportunities to make use of its authentication and logging architecture."

Today, Postini is using its IDSentrie system to provide rapid, automated provisioning of employee accounts and RADIUS authentication with full logging.

Robinson stated that the Unified Identity Management (UIM) interface built into IDSentrie has been extremely useful in streamlining his previously manual process and mitigating security risk. He particularly values the IDSentrie system's unique combination of strong RADIUS authentication plus firewall log analysis, and the ability to manage all of these critical functions using the system's centralized interface and its built-in, identity-based reports.

For more information about Postini, visit www.postini.com.

About A10 Networks

A10 Networks was founded in 2004 with a mission to create a new class of affordable, identity-aware network solutions, including the industry's first "Smart" identity management system. A10's solutions help businesses and government increase efficiency and agility, address regulatory compliance and security risks while reducing the complexity and costs of managing global networks. A10's products unify critical identity and access management functions with networking and security to offer network administrators centralized management and unparalleled visibility into network activity. A10 is a well-financed, privately held company headquartered in San Jose, California, with offices in Beijing. For more information, visit www.a10networks.com.

#