

Huntington Bank

Huntington bank needed to consolidate customer data while meeting both regulatory and security mandates. The goal was to safely leverage cloud applications while streamlining the employee and customer login experience. Using NetIQ® Identity Manager and NetIQ Access Manager™, Huntington automated provisioning and simplified employee and customer access to Salesforce.com while safeguarding authentication credentials.



Overview

A full-service bank with over 600 locations, Huntington offers commercial, consumer and mortgage banking services; equipment leasing; investment management, trust and brokerage services; customized insurance services; and other financial products and services.

Challenge

With more than 600 banking offices located in Indiana, Kentucky, Michigan, Ohio, Pennsylvania and West Virginia, Huntington Bank set out to improve customer service by consolidating customer data and presenting a unified customer view to its colleagues. Because regulatory mandates are constantly in flux,

“Colleagues can quickly access all of a customer’s information without having to log into multiple systems. That’s a big plus. We can then spend more of our valuable time addressing our customers’ financial needs.”

MARK EDSON

Manager, Enterprise Desktop and Directory Services
Huntington Bank

Huntington also needed a means to continually interpret them and implement control changes to ensure compliance. Of course, as Mark Edson, manager of Enterprise Desktop and Directory Services for Huntington Bank, acknowledged, “Merely complying with government regulations does not equate to good risk management. We also must be great custodians of our information assets.”

To this end, the bank sought to securely employ cloud applications. “We decided to use Salesforce.com to better serve our customer needs,” said Edson. “We needed to do this in a secure, seamless manner so our colleagues wouldn’t have to log in a second time to access Salesforce.com. To safeguard data, we needed to establish a federated connection to the cloud. This way, our colleagues’ authentication credentials could be securely passed to our cloud provider, but their corporate passwords would never be shared.”

Huntington also wanted to make the login process to its cloud provider faster and more secure. “The most common reason people call our service desk is for password resets,” said Edson. To forestall this problem, Huntington set out to enable web single-sign-on (SSO) capabilities.



At a Glance

- **Industry**
Financial Services
- **Location**
United States
- **Challenge**
To safeguard data, the bank needed to establish a federated connection to a cloud application.
- **Products and Services**
Identity Manager
Access Manager
- **Results**
 - + Improved service experience with single sign-on
 - + Automated user management with an event-based model
 - + Provided the ability to scale as the bank acquires new cloud applications

“Our ability to safeguard our colleagues’ information assets in the cloud is a market differentiator.”

MARK EDSON

Manager, Enterprise Desktop and Directory Services
Huntington Bank

Contact us at:
www.microfocus.com

Like what you read? Share it.



Solution

Huntington had long relied on Identity Manager to manage more than 12,000 identities across the enterprise.

Identity Manager was already connected with the bank’s human resources (HR) system, so as soon as HR created a new colleague record, Identity Manager automatically provisioned the colleague’s access rights to numerous applications. Extending this solution to provision and deprovision identities in the cloud was a natural fit.

Using Identity Manager, Huntington loaded roughly 8,000 accounts into Salesforce.com in just one night. “It could have taken months to get those accounts created and set up,” explained Edson.

Huntington leverages the workflow engine in Identity Manager to grant access privileges to Salesforce.com, significantly reducing administrative overhead. “The same thing occurs with employee termination,” said Edson. “As soon as HR hits the termination button, access is automatically revoked across all connected systems. This event-based processing model is critical.”

Huntington also chose Access Manager as the secure web SSO solution for its cloud-based and enterprise applications. “It provides federated identity management to cloud applications so that we can authenticate our colleagues without ever sharing their passwords with cloud providers,” Edson said.

Professional Services played a key role in meeting Huntington’s aggressive implementation schedule, thus accelerating the new solution’s time to value.

Results

“The incorporation of programmatic events gives us tremendous efficiencies,” said Edson. When colleagues move to new departments or change their phone numbers, addresses, cost centers or access privileges, Identity Manager propagates the changes across all connected systems in a matter of seconds. As Edson said, “It doesn’t get better than that.”

The bank has gained a solution that will scale as it continues to take advantage of new cloud applications. Web SSO capabilities have also helped improve service experiences. “...our colleagues’ main focus is our customer, not our systems,” Edson said. “Colleagues can quickly access all of a customer’s information without having to log into multiple systems. That’s a big plus. We can then spend more of our valuable time addressing our customers’ financial needs.”

Ultimately, protecting information assets was one of the greatest benefits. “Our ability to safeguard our colleague’s information assets in the cloud is a market differentiator,” said Edson. Identity Manager and Access Manager played an integral role in helping Huntington Bank achieve this goal.