

## White Paper

ENTERPRISE

[www.novell.com](http://www.novell.com)

# Enabling Retail Banks to Improve Customer Service, Security and Compliance

Novell® Identity, Security and Compliance Solutions for Retail Banking

**Novell.**

**Table of Contents:**

<b>2</b>	.....	Executive Summary
<b>2</b>	.....	Seeking Advantages in the Midst of Transformation
<b>3</b>	.....	Front-office Inefficiencies
<b>5</b>	.....	Back-office Challenges
<b>6</b>	.....	The Ideal Retail Banking Solution
<b>10</b>	.....	Novell Identity-Driven Solution for Retail Banks
<b>12</b>	.....	Novell ZENworks Patch Management

# Executive Summary

## Key Improvements Needed in Retail Banking

- Simplified and secure access to IT systems
- Improved employee productivity
- Reduced operational costs
- Automated compliance reporting
- Ability to focus on customer service

While struggling to comply with an overwhelming number of regulatory standards, retail banks are undergoing a significant transformation in response to increasing consumer demands and industry consolidation. In the midst of all of this, banks must stay focused on delivering the best customer service possible and that means empowering front-line employees at the retail banking branches to perform their jobs efficiently and effectively. Unfortunately, as today's front- and back-office employees are forced to spend valuable time managing and gaining access to the systems and applications that run the business, they are limited in their ability to focus on strategic activities. Novell® offers an identity-driven solution—designed specifically for retail banks—that provides the foundation needed to securely deliver the right resources to the right people—anytime, anywhere. With this solution, retail banks can enforce security and better address regulatory compliance, improve productivity, satisfy customer demands and increase revenue.

## Seeking Advantages in the Midst of Transformation

As a retail bank, your organization faces a number of challenges that complicate your ability to operate efficiently. For instance, you are likely already addressing consumer fraud and the related security measures. At the same time, many of your internal security measures are under scrutiny from a number of organizations and agencies to ensure compliance with a growing number of regulations. These include the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act, HIPAA, the Patriot Act, Basel II, and multi-factor authentication as recommended as best practice by the FFIEC, to name a few.

To complicate matters, your industry is in the midst of a transformation that is changing the face of retail banks. Your bank may be investing significantly into its branches and offering a diversified set of new products and services to customers, while also opening new banking centers. Increasingly, you are hiring part-time and temporary front-office and back-office employees, while rotating personal bankers and product specialists between your various banking centers.

At the same time, the banking industry is undergoing unprecedented levels of consolidation. The associated challenge of integrating IT systems and organizations from multiple companies is making it difficult to ensure uninterrupted operations in the front office.

In the midst of this transformation, retail banks need to do the following:

- *Ensure simplified and secure access to heterogeneous IT systems*
- *Improve employee productivity and reduce operational costs*
- *Automate compliance reporting*
- *Free up employees to focus on customer service*

## Simplified and Secure Access to Heterogeneous IT Systems

To be successful, your employees need unimpeded and easy access to key business applications, whether they work in, or roam between, your branch offices. Yet today's bank infrastructure often comprises many home-grown applications, as well as a maze of legacy systems and applications inherited through merger and acquisition

activity. And though your bank has probably introduced Web-based applications to both employees and customers, the reality is that the legacy mainframe systems and client/server applications of your IT systems infrastructure are not going away any time soon. This leads to a challenging situation for your front-line employees, as each IT system and the associated business processes in this heterogeneous environment are accessed via separate user IDs and passwords.

### **Improve Employee Productivity and Reduce Operational Costs**

A number of process inefficiencies—such as time-consuming user provisioning, manual data gathering and reporting for compliance and frequent calls to the helpdesk—lead to higher operational costs. For instance, as your employees struggle to remember multiple user IDs and passwords to access the numerous and various applications they need to perform their jobs, they increasingly call the helpdesk. This is not only inconvenient and time-consuming for the front-office employee, but is costly in terms of helpdesk assistance and the associated phone calls. (In fact, analysts estimate that each time end users call the helpdesk, it costs anywhere from \$10 to \$31.)<sup>1</sup> At the same time, these administrative tasks sidetrack your back-office employees from strategic initiatives. By automating and improving processes, you can reduce helpdesk calls, which in turn enables your employees to focus on serving customers instead of on issues related to system access, provisioning and policy and regulatory compliance.

### **Automate Compliance Reporting**

Your security and IT employees often find themselves scrambling to address compliance requirements. Without automated and repeatable processes, they are forced to manually track down and report on the information required by the various standards affecting your institution. Again, these inefficient

processes cost your business significant sums of money. Yet, like most banks, you likely feel you have no choice but to suffer through this repeated fire drill. After all, you can not afford to see your company's name appear on the front page of *The Wall Street Journal* for violation of regulatory compliances since this will significantly affect the reputation of your bank.

### **Free Up Employees to Focus on Customer Service**

Ultimately, you must make it easier for your employees to perform their jobs and serve your customers, as this will engender customer loyalty and afford opportunities to cross- and up-sell additional products and services. What is needed is a robust infrastructure that incorporates automated processes and tools to guarantee that the right people have access to the right information. This not only ensures productivity but safeguards valuable information assets while freeing your front- and back-office employees to focus on strategic activities that ensure customer satisfaction and higher revenues.

### **Front-office Inefficiencies**

Without a doubt, you are seeking ways to make it easier for your employees to do their jobs. After all, an improvement in productivity leads to reduced costs, increased customer satisfaction and additional opportunities to sell more services. Unfortunately, today's retail bank branches and centers are plagued by a number of inefficiencies that make it difficult to achieve this goal. The following key front-office challenges are described in the sections below:

- *Passwords left out in the open*
- *Calling on the helpdesk to access front-office applications*
- *Slow customer service reduces revenue opportunities*
- *Inefficient processes impact productivity*

### **Front-office Inefficiencies**

- **Exposed passwords**
- **Calling on the helpdesk to access applications**
- **Reduced revenue opportunities due to slow customer service**
- **Poor productivity as the result of inefficient processes**

---

<sup>1</sup> Source: Gartner Research—*"Justify Identity Management Investment with Metrics"* by Roberta J. Witty, Kris Brittain and Ant Allan (ID Number: TG-22-1617), February 23, 2004

## The theft of a valid user name and password combination could ultimately lead to the theft of customer information that your institution is legally bound to protect.

The yellow sticky note syndrome is prevalent in many industries, but in a retail bank the potential for misuse is significant.

### ***Passwords Left Out in the Open***

Because they struggle to remember the variety of passwords they need, your front-office employees are likely to resort to such methods as jotting passwords down on paper. The yellow sticky note syndrome is prevalent in many industries, but in a retail bank the potential for misuse is significant. Front-office workers, particularly personal bankers and branch managers who sit out front serving customers, often leave a list of their passwords written on a training manual on their desk, in an unlocked desk drawer, or on notes stuck to their computer monitors. And teller supervisors maintain a list of passwords to multiple systems. This information is often in plain view and easily accessed by anyone who enters the branch office.

The theft of a valid user name and password combination could ultimately lead to the theft of countless other bits of personal data, including customer information that your institution is legally bound to protect. Similarly, many of the applications used by your employees do not automatically log out the user after a given period of time. So when a customer service representative or mortgage officer walks away from his or her desk, anyone could potentially access the system to conduct a transaction or look up customer information. If such activity became public knowledge, it would probably lead to a loss of customers and a damaged reputation that your bank may find difficult to overcome.

### ***Calling on the Helpdesk to Access Front-office Applications***

When tellers, customer service representatives or branch managers forget a password,

they are locked out of their applications and must call the helpdesk for a password reset. In fact, it's not unusual for tellers to get locked out of a system multiple times per month and when they do, they are kept waiting—along with customers—until an IT employee can help them gain access to the required application.

Some of your employees probably give up trying to remember their password because they know they will be locked out of the system after a certain number of attempts. Instead, they automatically call the helpdesk and request a password reset since this will save some time—even if only a few minutes—in gaining access. Not only does this increase the costs of bank operations and impede productivity, it negatively impacts customer service. And ironically, at the end of this inefficient process, the front-office employee has yet another password to remember.

### ***Slow Customer Service Reduces Revenue Opportunities***

The difficulty of remembering passwords can also reduce your bank's revenue opportunities. As your front-office employees take the necessary—and time-consuming steps—to get their passwords reset, the customer may get tired of waiting and simply leave the bank. If your customer service representative was attempting to sell additional services to the customer, the opportunity is lost. This type of situation negatively impacts the customer's perception of your bank, reducing future opportunities to conduct business with, and gain more share of wallet from, that customer.

### ***Inefficient Processes Impact Productivity***

All front-office employees, whether they are tellers, personal bankers or branch managers, are impacted by a lack of automation when it comes to gaining access to the necessary IT systems. For instance, many banks have no standard process for requesting access to

these systems. Instead, employees must submit a paper-based provisioning request, which is both time-consuming to fill out on the front-end and to fulfill in the back office. This inefficient process leaves many front-office employees unable to perform key aspects of their job for some amount of time, ranging from hours to days.

Like many retail banks, your organization is likely implementing an increasing number of computer applications to support the sale of a growing number of products and services. And though each employee requires access to only certain aspects of any given application, most of these applications are not configured to display only the functions and views that are relevant to the employee's role. This problem applies to employees throughout your bank, such as part-time employees who work in shifts, as well as roaming employees who work in multiple banking centers. The result is a work environment that is not personalized to ensure maximum productivity and meet security and compliance requirements.

## Back-office Challenges

One of the biggest challenges facing your IT group is maintaining the balance between keeping systems secure, staying compliant with regulations and enabling user productivity. Your IT director or vice president may have determined that the costs are too high to deploy a solution that resolves this issue. Yet relying upon employees to always take the right action and upon manual, paper-based processes to address compliance requirements is not only inefficient—it's very costly. The following common back-office challenges are discussed in the sections below:

- *Breaching compliance and security policies*
- *Difficult and costly manual provisioning*
- *Rising costs of managing passwords*
- *Struggling to comply with regulations and policies*

### ***Breaching Compliance and Security Policies***

Because many banking applications support only one account ID and password combination, your teller supervisors and branch managers are forced to share passwords with their employees. Without being able to associate each user with a unique ID and password combination, your chief security and compliance officers are unable to determine who accessed which systems and performed certain activities. After all, when two or three tellers are sharing a generic ID and password, how can one determine who last opened the vault or cash drawer or why it is short?

For convenience sake, many of your employees probably violate the corporation's security policies. For instance, mobile and remote users often ask other employees to share their passwords with them so that they can access systems while they are on site. Similarly, head tellers often share their unique log-in credentials with a teller who is serving as a backup. In cases where the system does not allow multiple user names and passwords, the teller has no choice but to share the password to enable the backup to assume her responsibilities. Unfortunately, this workaround complicates your compliance auditing efforts.

At the same time, helpdesk personnel who are called upon to reset forgotten passwords often violate corporate e-mail and security policies during the password reset, in spite of their best intentions. They often e-mail the new password to the teller, personal banker or branch manager, and they may also call employees to confirm that they have received the new password. This inefficient process ends up doubling the workload associated with password resets and transmits the password via insecure communication channels, which leaves your bank vulnerable to potential fraud.

### **Back-office Challenges**

- **Breached compliance and security policies**
- **Difficult and costly manual provisioning**
- **Rising costs of managing passwords**
- **Struggling to comply with regulations and policies**

Without an automated and quick way to de-provision existing rights and provision new sets of rights, your bank is unable to ensure that its systems and information are secure.

---

<sup>2</sup> Bank Systems Technology, *The Automation of IT: Identity Management Suites*, February 1, 2006

<sup>3</sup> NetworkWorld, *Firms Bank on Identity Management*, February 7, 2005

### ***Difficult and Costly Manual Provisioning***

Those banks that are unable to grant system access based on an employee's role struggle to understand, track and manage access rights. This is a painful issue in an industry characterized by high employee turnover, constant mergers and acquisitions and migration of employees (including contractors and temporary employees) between various roles. Whether an employee is transferred, promoted or terminated, your back-office employees must be able to revoke existing rights and grant new ones where applicable. Without an automated and quick way to de-provision existing rights and provision new sets of rights, your bank is unable to ensure that its systems and information are secure. This issue is exacerbated during layoffs that affect hundreds or thousands of employees. How can you be certain that these people no longer have access to core banking applications and sensitive data?

In addition, to accommodate the inordinate number of paper-based provisioning requests received from the front office, your bank may employ a significant number of back-office employees. Not only does this drive up costs, it fails to efficiently address the issue of ensuring productive front-end employees. After all, the process is still manual and tellers, personal bankers and branch managers must wait for someone to process their request.

### ***Rising Costs of Managing Passwords***

The burgeoning number of passwords in today's retail bank environments drives up administration costs as IT personnel have to separately manage passwords for dozens of different systems. Furthermore, password

resets alone are a major burden within large organizations, amounting to \$48.54 per employee per year.<sup>2</sup> According to Gartner, the average password reset call to an organization's helpdesk costs the company between \$10 and \$30.<sup>3</sup>

### ***Struggling to Comply with Regulations and Policies***

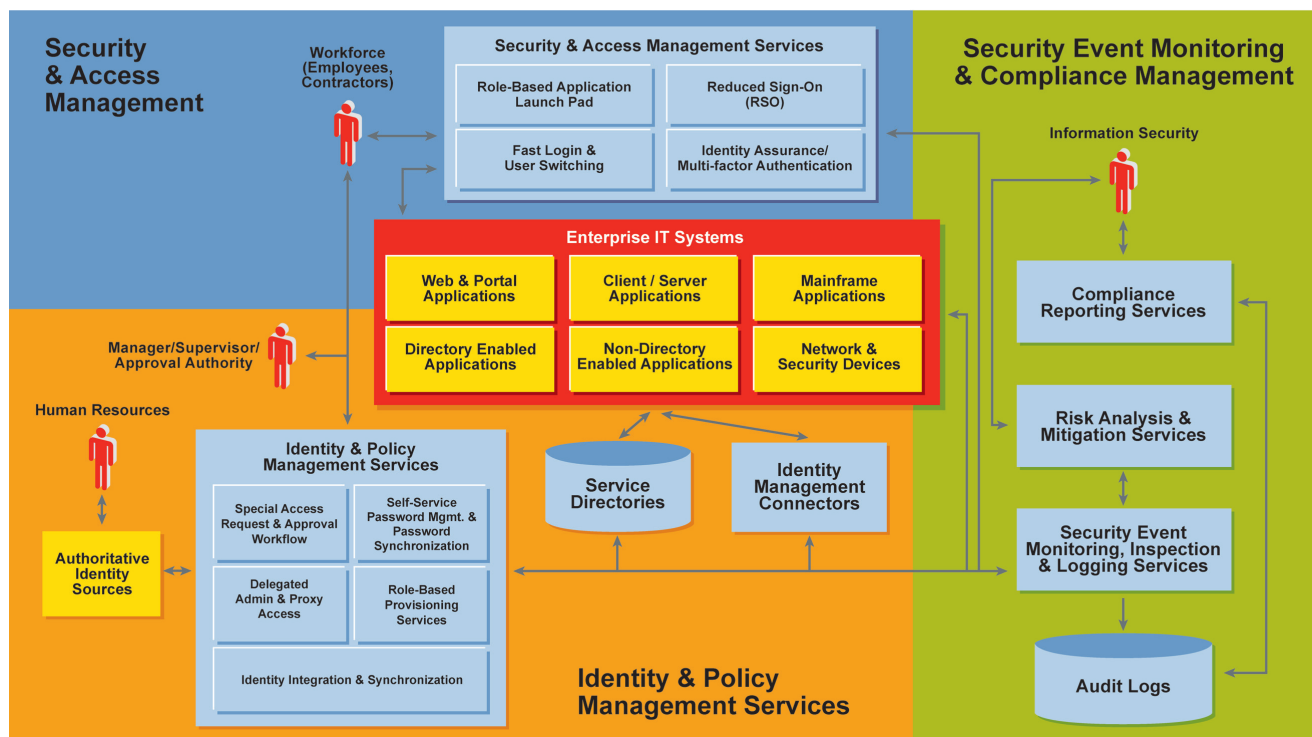
As a retail bank, your organization is subject to multiple compliance audits throughout the year. Yet with no automated way to track and prove compliance with policies and standards, your vice president or director of information security is likely forced to hire temporary employees to manually collect the required information. This time- and cost-intensive process detracts from efforts to ensure that enterprise IT systems are as secure and efficient as possible for your employees.

On top of that, there is no guarantee that the reports generated by these temporary employees are correct. Without an automated attestation process to verify who should have access to what, as well as insight into the necessary data, you are unable to follow an audit trail and trace compliance throughout the organization.

## **The Ideal Retail Banking Solution**

A solid and secure infrastructure is critical to ensuring the necessary agility and streamlined processes that enable competitive advantage. An identity, security, and compliance management solution designed specifically for the banking industry plays a key role in this infrastructure and can help improve your processes within both the front and back offices.

# Retail Banking Identity Solution Architecture



**Figure 1.** The ideal retail banking solution improves front- and back-office processes

To address the common pain points discussed earlier in this paper, organizations should seek a retail banking identity solution that provides the following capabilities:

- *Role-based application launch pad*
- *Reduced sign-on (RSO)*
- *Robust security*
- *Password synchronization*
- *Employee self-service*
- *Temporary access management*
- *Automated and powerful provisioning*
- *Security and compliance management*

## Resolving Front-office Issues

The front office represents the face of your bank and presents multiple opportunities to generate more business and gain more share of wallet from your customers. You need a solution that will help your front-office

employees efficiently and effectively perform their jobs so they can focus on providing customers with the best service possible.

## Role-based Access to IT Systems

The ideal identity management solution should allow your employees to log in to a single workstation and be presented with a launch pad that displays all necessary applications to perform their jobs. By only showing the applications relevant to each employee, the solution eliminates confusion and helps employees be productive immediately. Not only does this enable employees to quickly log in, it makes it easier and faster to switch between users. Such a method allows workers to quickly log in and log out of all applications instantaneously so that multiple employees can easily and securely access the information and resources they need with minimum effort. Furthermore, by employing role-based

By employing additional measures such as strong passwords and multi-factor authentication, your bank can significantly improve its security.

**The ideal identity and security management solution enables password synchronization so that your employees need only a single password for access to all systems.**

access technology, you can easily authenticate roaming and temporary employees and grant access to the necessary applications without violating security policies or best practices.

#### **Reduced Sign-on**

Reduced sign-on simplifies an otherwise time-consuming process and allows your employees to quickly access all necessary applications. By simplifying system access, your organization can increase productivity, reduce the volume of calls to the helpdesk and lower IT staffing requirements.

Typically security officers are hesitant to implement an RSO solution since they think that it will provide a key to the kingdom. An identity assurance solution can support stronger password enforcement, such as through strong / multi-factor authentication techniques, to alleviate these security concerns and ensure the identity of the user accessing the bank's IT systems.

#### **Robust Security**

Today's technology is mature enough that the solution should allow your bank to choose what level and types of security to implement. For instance, to ensure that a single user name and password system does not become a weak point, you should be able to implement policies that encourage stronger passwords. Or you can issue one-time passwords, employ smart cards or fingerprint biometrics or use a combination of authentication methods. By employing additional measures such as strong passwords and multi-factor authentication, your bank can significantly improve its security.

#### **Password Synchronization**

The ideal identity and security management solution enables password synchronization so that your employees need only a single password for access to all systems. Employees can focus on the tasks at hand and are relieved from remembering a password for each application. Password synchronization does not necessarily mean that the same password is used for access to all systems. Through policies, you can randomly generate passwords to ensure strong security. At the same time, this method allows you to enforce access management in a streamlined fashion.

#### **Employee Self-services**

Instead of relying upon the branch manager and the IT group to provide access to the necessary systems and applications, the solution should provide a self-service interface that automatically assigns resources to new, transferred and temporary employees. The ideal solution should also offer a way for your employees to quickly resolve issues. For instance, if they forget or lose their password, they should be able to log into a Web interface to reset it. Self-service password reset allows your front-office employees to easily reset forgotten or expired passwords so that they are quickly back up and running and productive.

#### **Temporary Access Management**

The ideal solution will also allow your authorized employees to delegate temporary access to certain systems and applications. This becomes especially important for times when a supervisor needs to assign a senior teller to act as the supervisor, such as over the weekend or while the supervisor is on vacation. By allowing temporary access delegation, the solution enables an efficient process that allows your supervisor to seamlessly assume responsibility once back in the front office.

### Streamlining Back-end Processes

You rely upon your back-office employees to ensure smoothly functioning operations. But they need to use the right technology and best practices to get the job done. The ideal solution will deliver the necessary tools, freeing your IT and security groups to focus on strategic initiatives.

employee. But in today's retail banking world marked by numerous mergers and acquisitions and the opening of new branches, provisioning pain is greatly magnified. With more systems, applications and employees to manage, it is virtually impossible to satisfy compliance requirements without automating the provisioning process.

With more systems, applications and employees to manage, it is virtually impossible to satisfy compliance requirements without automating the provisioning process.

### Automated and Powerful Provisioning

Perhaps more than any other task, provisioning is the biggest challenge facing your back-office employees. The process is difficult whether the issue is to bring a new employee on board or to de-provision a departing

The ideal identity and security management solution allows your bank to integrate its provisioning system with the system of an acquired company and automatically provision employee access based on roles. This solution should provide full control over and insight into which rights employees are

### Recommended Best Security Practices

Solid security practices improve the overall security of your organization's infrastructure. The following are recommended best practices for implementing a security management framework:

1. **Define Security Policies.** *Establishing security policies is an important first step in the security management lifecycle. Security policies establish clear guidelines about what needs to be protected, who needs access to what systems, and what is considered acceptable behavior throughout the organization, including the use of information technology and considerations around the protection of information assets.*
2. **Security Awareness.** Security policies are meaningless unless employees are aware of them and understand their role in following and enforcing the policies. Employee awareness helps ensure successful policy adoption and execution. Making employees aware of security policies should include training about the appropriate processes to follow for password creation and resets. Temporary, roaming and remote employees may require awareness training tailored to their unique circumstances.
3. **Security Control Points.** A solid security framework is built upon people, processes and technology. Once processes are established and employees understand their role in following and enforcing them, your bank can implement technology to support the policies and people. By automating and standardizing these IT controls, you can realize increased efficiencies while ensuring that employees do not violate important policies.
4. **Monitor Control Points.** Security management is not a one-time event; rather, it is an ongoing process. Once IT controls are in place, they must be monitored to ensure no violations occur. In other words, your IT group must still confirm that employees do not access systems they are not authorized to access.
5. **Remediation Management and Compliance Reporting.** To complete the circle, you must implement processes for identifying and remediating any gaps discovered in your security framework. Using technology to identify and recommend remediation steps can go a long way to ensuring an effective process. Technology can also provide the enhanced visibility that enables your bank to respond in real time to compliance needs, such as by generating compliance reports.

Novell security and identity management solutions enable you to gain control of identities and use identity information to assign access rights for users inside and outside your organization.

entitled to, based upon their roles. It should also allow your IT and security teams to immediately assign and revoke access rights as required, whether to deal with temporary employees or the provisioning of thousands of new employees. This includes the ability to control access to both physical resources and logical information systems with a single authentication measure. With a robust identity management infrastructure in place, your bank can even use the identity management solution to automatically cancel all access to corporate applications on an employee's last day.

### Security and Compliance Management

Just as important, such a solution should support efforts to comply with regulations and allow your organization to respond to compliance and audit needs in real time. The solution should help you streamline the collection of events necessary to respond to

audit and compliance needs. It should also facilitate the attestation process associated with ensuring the right people have access to the right resources. And by helping you distribute access rights' reports to managers on a periodic basis, the solution enables your organization to increase accountability at all levels of the enterprise. With support for ad hoc reporting, the ideal solution also enables your organization to more easily satisfy specific audit or regulatory compliance requirements.

### Novell Identity-Driven Solution for Retail Banks

Novell offers an end-to-end security and compliance management solution that allows you to address the front- and back-office issues discussed in this paper. Created with market-leading technology and drawing upon extensive experience in implementing complex security, identity and compliance management solutions, this solution provides you with a security, identity and compliance management foundation that supports your complex business environment and evolving business practices.

## Best Practice: Security & Compliance Management Framework



**Figure 2.** Recommended best practices for a solid security management framework

### Enhancing Security While Simplifying Access

Novell security and identity management solutions enable you to gain control of identities and use identity information to assign access rights for users inside and outside your organization. These solutions consistently enforce access policies across all resources to ensure that all users—internal and external—gain access to only what they should. And whether people tap into your business resources through the Web, wireless, dial-up, terminal, client, firewall or virtual private network, access is always secure.

This robust security and identity management foundation enables your business systems to identify the user and deliver the right information based on the user's role or

relationship. Users can access multiple resources with a single login, so they do not have to remember multiple usernames and passwords. This eliminates redundant log-in steps that confuse users, hamper productivity and drive up support costs. And once logged into your system, users can even access partner sites seamlessly, saving time and increasing productivity.

### **Enabling Compliance While Controlling Costs**

By helping you streamline compliance and provisioning tasks, Novell identity, security and compliance management solutions make it easier to comply with internal and external regulations—and reduce costs. The solutions simplify the collection and aggregation of events needed to satisfy audit and compliance requirements. For instance, your organization can establish an automated attestation process to verify who should have access to what, allowing you to accurately trace compliance throughout the organization. And with Novell solutions, your organization can easily generate and distribute reports enterprisewide to ensure awareness and accountability. By gaining control of the processes and policies that define how information is shared and how users interact with resources, your organization can more simply monitor and report on enterprisewide activities and data. Self-services and automated provisioning minimize IT administration while also ensuring your employees have access to the right systems. This not only allows you to reduce IT costs but also the costs associated with poor front-office productivity.

### **Building on a Sound Management Foundation**

Novell security, identity and compliance management solutions bring identity under control, giving you a platform for other identity-

**By helping you streamline compliance and provisioning tasks, Novell identity, security and compliance management solutions make it easier to comply with internal and external regulations—and reduce costs.**

based business initiatives that further increase agility and success. For example, you can leverage this management foundation to:

- *Create customized and self-service portals that empower employees, customers and partners to obtain information and perform tasks and transactions on their own.*
- *Build compliance monitoring dashboards that aggregate data across the entire security systems within your network and present it in a clear, concise format to facilitate decision making and regulatory compliance.*
- *Free up and dynamically combine disparate information and capabilities to orchestrate value-added business processes.*

### **Making the Right Choice**

Novell security, identity and compliance solutions are made up of a comprehensive, modular set of products and technologies that connect with any application, data store, directory or security system in your IT environment—without modification to those business resources. The solution components are completely cross-platform, running on Microsoft\* Windows\*, Solaris\*, NetWare® and Linux\*. Best of all, the solution components position you for the future by giving you the security, identity and compliance foundation that supports other security and identity-based business initiatives, such as secure employee and customer portals, business workflows and software as a service.

**Novell security, identity and compliance solutions are made up of a comprehensive, modular set of products and technologies that connect with any application, data store, directory or security system in your IT environment.**

With Novell Identity Manager, you can manage the full user lifecycle, deliver first-day access to essential resources, synchronize multiple passwords into a single login, modify or revoke access rights instantly and even support compliance with internal policies and government regulations.

Novell SecureLogin integrates seamlessly with the other product components in this identity, security and compliance solution to provide the necessary desktop control for simplifying the user's experience.

### **Novell Identity, Security and Compliance Solutions**

Novell Identity Manager helps you securely manage the access needs of your ever-changing user community. With Novell Identity Manager, you can manage the full user lifecycle, deliver first-day access to essential resources, synchronize multiple passwords into a single login, modify or revoke access rights instantly and even support compliance with internal policies and government regulations. Identity Manager also provides self-service features that enable users to maintain their own passwords and profile information. In addition, it offers a simple application launch pad that serves as a basic role-based application launcher for the specific retail-banking applications used by your users. With these capabilities you will realize tangible business benefits: streamlined administration, increased security, reduced costs and a rapid return on investment (ROI).

Novell eDirectory™ is a powerful and proven cross-platform directory service that is commonly deployed for a variety of services implementations. Key implementations are the central identity vault for Novell identity and access management solutions and global authentication points, to name a few. The solution delivers the precise identity control and strong, scalable foundation you need to build a profitable secure identity-management solution. Novell eDirectory also includes an extensible, advanced authentication service—Novell Modular Authentication

Service—that offers you an easy way to centrally manage multiple authentication methods across your network. With Novell Modular Authentication Service you can implement stronger forms of authentication and authorization to secure your critical corporate resources.

Novell Access Manager is a robust security infrastructure that provides extranet access management, Web SSO, identity federation and SSL VPN services. With Novell Access Manager in place, you gain a true business-to-business platform that enables data sharing between separate business entities such as branches, valued partners and customers.

Novell SecureLogin reduces helpdesk costs, simplifies users' access to applications and improves security by delivering scalable and reliable single sign-on and fast user switching. Novell SecureLogin integrates seamlessly with the other product components in this identity, security and compliance solution to provide the necessary desktop control for simplifying the user's experience. Examples of the types of integration supported include common credential sharing with Novell Access Manager, pre-populating the common credential store in eDirectory with the credentials your users need with Identity Manager, multi-factor and advanced authentication support through eDirectory, and desktop monitoring and reporting via Novell Sentinel™.

Novell Sentinel is a comprehensive security event and information management platform that allows you to monitor and control the security of all systems within your network. Novell Sentinel provides a broad range of out-of-the-box collectors, robust event correlation, intuitive remediation tools and easy-to-use, real-time dashboard and report generation tools.

The combined set of products that make up this identity, security and compliance solution enables you to securely deliver the

right resources to the right people—anytime, anywhere. By streamlining approval processes, enabling delegation of authority and providing self-service features, the Novell security, identity, and compliance management solution eases the management burden on your staff—and lowers your costs. It also lets you deliver first-day access to essential resources, synchronize passwords across connected systems, instantly modify or revoke access rights and enforce security and regulatory compliance. By freeing your employees to focus on strategic activities, you can satisfy customer demands and increase revenues.

### **Join Leading Financial Groups in Choosing Novell**

Leading financial groups worldwide have partnered with Novell to gain competitive advantage and grow in a dynamic market. In fact, nine of the top ten banks in North America rely on the high performance, scalability, flexibility, reliability and stability of Novell solutions. Webster Bank, N.A.—a subsidiary of Webster Financial Corporation, the largest independent bank headquartered in New England with more than \$17.8 billion in assets—is one such organization that trusts in Novell to help it securely expand its business.

Webster Bank is growing quickly and, having recently expanded from Connecticut into Massachusetts, Rhode Island and New York, needed to integrate multiple IT environments, simplify user access, create consistency

across an expanding enterprise and ensure regulatory compliance.

The bank selected Novell SecureLogin and Novell ZENworks® to streamline user access and automate desktop management. Working with Novell, Webster Bank increased security, built a foundation for rapid growth and saved significant time and money after reducing the number of passwords by 75 percent and desktop administration time by 40 percent.

Integrating SecureLogin with Novell eDirectory and Microsoft Active Directory\*, Webster Bank provides its 3,300 users with single sign-on access to nearly 25 core applications. The IT staff can now quickly integrate new applications following an acquisition, giving all users access to the right information. Streamlined password management helps Webster Bank enforce tighter security policies, including frequent password changes. With a self-service option, users can reset their own passwords rather than wait for helpdesk support.

To learn more about Novell identity, security and compliance solutions and how they can help your retail bank improve customer service, security and compliance, contact a sales representative or visit: [www.novell.com/identity](http://www.novell.com/identity)

Special thanks to the Novell customers and partners that participated in discussions and interviews about the key challenges their industry faces.



**“We constantly have new applications and ZENworks makes it easy for us to deploy them in days, rather than weeks or months.”**

**John Jahne**

*Vice President of Network Services*  
Webster Bank

[www.novell.com](http://www.novell.com)



Contact your local Novell  
Solutions Provider, or call  
Novell at:

1 888 321 4272 U.S./Canada  
1 801 861 4272 Worldwide  
1 801 861 8473 Facsimile

**Novell, Inc.**  
404 Wyman Street  
Waltham, MA 02451 USA