Solution Brief

CORE SECURITY
A HelpSystems Company

PROVISIONING

Policy-based End-user Provisioning

Benefits

+ Flexible: Fits seamlessly into even the most complex, heterogeneous environments
+ Cost-effective: Doesn't require a substantial investment in prerequisite software or systems
+ Quick time to value: Rapid deployment methodology and modular architecture get you up and running quickly
+ Total cost of ownership: Meeting changing business requirements is easier, requiring fewer resources and delivering lower TCO
+ Business alignment Managers are empowered to enforce security policy based on knowledge of the business
+ Improve compliance: Enforces compliance with corporate security policies, industry standards (e.g., PCI-DSS) and government regulations (HIPM, Sarbanes-Oxley, Data Privacy Act, etc)

Provisioning Features

+ Provisioning is a complete enterprise provisioning system, which enables organizations to manage the provisioning lifecycle, from policy definition, to granting application access, through to end-user termination.

Provisioning is Core Security's user provisioning solution for organizations seeking to improve alignment with business goals; cut costs; enforce compliance with internal security policies, industry standards and government regulations; and reduce the risk of security incidents.

Part of Core Security's Enterprise Suite of products, Core Provisioning delivers these benefits by accelerating the process of provisioning and managing user access to vital corporate resources based on business policy.

Access Request and Provisioning

Access Request is Core Security's unique approach to ensuring only the right individuals have access to the right resources and are doing the right things. Access Request unifies governance, provisioning and Compliance even in the most complex, heterogeneous environments. A core element of Access Request is end-user provisioning.

Provisioning is the process of defining and implementing policies for access to enterprise information and resources. It involves creating, managing and terminating end-user accounts, along with their associated access rights and entitlements, based on those policies. The ability to automate the management of end-user accounts provides many benefits, including: enforcing compliance with internal security policies, industry standards or government regulations; enhancing the end-user experience; streamlining business processes; and reducing overhead expenses.

Provisioning Functions

Core Provisioning performs the following major functions:

+ Provides the flexibility to leverage existing policy information and dynamically generate new policy in accordance with changing business needs.
+ Enables business managers to directly provision new accounts - allowing security policy to be enforced based on operating knowledge of the business.
+ Seamlessly integrates user provisioning with your business workflow for creating, changing and terminating access rights - protecting the organization against the risk of unauthorized access by employees whose roles have either changed or been eliminated.
+ Delivers a secure, reusable audit framework to automate periodic or ad hoc access verification, reporting and attestation.

Self-Service Provisioning

Provisioning Workflows	Enable authenticated users to easily create, enable, disable, or delete accounts and user IDs without manual intervention or fully automated "lights-out" provisioning workflows initiated by a triggering event
Full Spectrum Delegation	Delegate provisioning rights as determined by the security policy

Policy Driven Request/Approve Process Provide advanced requester/approver functionality with expanded automation, including multi-step serial/ parallel, bulk and policy-driven approval workflows.

Dynamic Communities	Enable the component elements of roles and rules to be assembled in real time based on business, security and operational policies
User Modeling	Create new accounts for a user by choosing a "modeled" user with a similar job function or access requirements
ID Generation	Enforce existing corporate account ID rules and eliminate non-compliance
Automatic Account Discovery	Automatically discover accounts created outside of Core Provisioning and link them to users through automated mapping (Identity Mapping) or user self-claiming (Resource Claiming)
Extended Provisioning	Extend provisioning to IT and physical assets, facilities and other business services

Policy Management

Provisioning provides key policy definition capabilities—both to define new policies and to link to existing policies using Core Security's exclusive Policylink™ connection technology. By retrieving policy data from its source within the existing infrastructure at the time a transaction occurs, enterprises are assured that only current, relevant policy data is being utilized. This ensures that provisioning actions which would result in policy infringements, such as segregation of duty violations, are detected and prohibited.

Flexibility and Adaptability

Every business is unique and Provisioning delivers the operational flexibility and adaptability to meet the needs of complex environments. Provisioning quickly connects to your existing heterogeneous IT infrastructure, accessing authoritative sources in real-time, thereby always remaining up to date without requiring any additional data-cleansing, replication or metadirectory initiatives.

Core Security workflows and connectors are easily configured using a graphical drag-and drop editor to design multi-step approval processes using multi-step serial, parallel or bulk workflows, including escalations and alerts. The ability to configure the system, using a graphical editor, rather than requiring expensive programming resources to customize it, significantly reduces the time and effort required to deploy and maintain the system.

Low Total Cost Of Ownership

As a result, Core Security's low license-to-services ratio saves you thousands of dollars in initial deployment and on-going maintenance costs.

IT Compliance Capabilities

Segregation of Duties	Facilitate discovery of SoD policy conflicts.
Automate Policy for Access Rights	Ensure immediate disablement of access rights upon termination for increased security and regulatory compliance
Notifications	Configure e-mail and pager alerts to confirm provisioning actions or warn of suspicious activity
Auto-lockout and Intrusion Alerts	Configure the number of failed authentication attempts before lock out and notification of security staff or system administrators
Automated Ticketing and Audit Trails	Automatically open, populate, and close service tickets for real-time security audit and service level reports

Comprehensive Integration

Core Security's multi-tier Connector Framework links Provisioning to more than 150 different enterprise systems. Provisioning can:

+ Manage access rights to a wide variety of operating systems, mainframes, networks, databases, directories and enterprise applications.
+ It also supports popular access management tools for two-factor authentication, enterprise single sign-on, and privileged password management.
+ Link in real-time to existing service desk systems, enabling you to track user provisioning details.
+ Extend provisioning beyond traditional IT applications to include tangible assets - such as mobile phones, laptops, vehicles, and security badges.
+ Virtualize your policy stores, business rules and processes to dynamically build communities using existing authoritative sources.

Core Security integrates with —and reflects the look and feel of—your company's support portal, Intranet or web site, enabling users to interact with a familiar environment, while Core Security's multilanguage capability enables user interfaces in a variety of languages other than English.

Backed by Industry-Proven Services

Core Security's Enterprise Suite is backed by world-class, expert services delivered directly by Core Security or by our Certified Solution Partners. Core Security's discovery and implementation methodology allows customers to efficiently achieve the desired level of policy automation for their targeted business processes. Core Security's unrivaled access and compliance management expertise delivers the strategic services and support required to achieve timely deployments, a process for capturing and tracking measurable results, substantial cost savings, and notable improvements in your company's security and service quality.

Open Architecture

Provisioning is based on a scalable , service-oriented architecture (SOA) and runs on familiar Microsoft® Windows® technology. The multi-tier design of Core Security's Connector Framework enables organizations to distribute connectors to meet performance or availability requirements, or where it is desirable to isolate a customized connector to a unique system. Support for clustered environments provides enterprise availability and scalability.

Supported industry standards include: Service Provisioning Markup Language (SPML), Business Process Execution Language (BPEL), Lightweight Directory Access Protocol (LDAP), Simple Object Access Protocol (SOAP), .NET Framework, and Health Level Seven (HL7).

Provisioning includes a robust transaction repository containing a record of all transactions, along with a library of pre-defined management reports that can be used for reporting and audit analysis purposes.

Technical Specifications

Windows Server	Microsoft Windows Server® 2003 (Service Pack 1 or higher) OR Microsoft Windows Server® 2008 Microsoft XML 6.0 and Microsoft XML 3.0 Microsoft Message Queuing	Minimum 3 GB of memory (single server installation) Minimum of 2.0 GHz processing speed (multiple CPUs or multicore CPUs recommended) NTFS formatted disk drive, 80 GB minimum
Web Server	Microsoft IIS 6.0 or higher on Windows Server 2003, Microsoft IIS 7.0	