



PasswordCourier®

Automated Password Management

Benefits

- **Secure:** Enforces strong password policies and reduces potential access vulnerabilities.
- **Rapid ROI:** Dramatically reduces costs associated with help desk calls.
- **Flexible:** Multiple password reset user interface options (desktop, web, phone, kiosk, voice.)
- **Convenient:** Improves services delivery and end-user satisfaction through self-service.
- **Investment protection:** Plugs into your existing infrastructure, including robust service desk integration.
- **Enterprise-class:** Enables unlimited simultaneous password resets.
- **Improve compliance:** Ensures password policies comply with corporate security requirements.

PasswordCourier® is Courion's password management solution for enterprises seeking to deploy self-service password reset and synchronization for users, as well as to enforce secure password policies. PasswordCourier is the industry standard for secure, self-service password management. It features multiple access options, robust service desk integration and the ability to enforce consistent password policies for any system, application, or web portal.

Access Assurance and Password Challenges

Access Assurance is Courion's unique approach to ensuring only the right individuals have access to the right resources and are doing the right things. Access Assurance unifies Access Governance, Access Provisioning and Access Compliance even in the most complex, heterogeneous environments. A core element of Access Assurance is delivering robust password management.

Today's business environment is increasingly complex with more pressure than ever to reduce costs and increase user productivity while improving security levels. Password management is unique in its ability to simultaneously achieve all three of these objectives.

Password resets are consistently the number one source of service desk calls. Organizations that implement a strong self-service password management solution achieve rapid ROI that is easily demonstrable by reducing service desk call volume by 80% or more.

Improved service levels increase end user convenience and productivity by reducing time wasted waiting for the help desk to reset an account password.

Regulatory pressures and greater awareness of the need to protect information assets are driving organizations to implement stronger security, including password policies such as longer and more complex passwords and regular password resets. This, coupled with the ever-increasing number of enterprise applications, makes it difficult for end users to remember more and more passwords, which leads to insecure end user practices (e.g., writing passwords down and failing to properly secure the written list.)

PasswordCourier enables organization to enforce secure policies and, at the same time, reduce end user frustration by enabling self-service password reset and allowing a single password to be used by multiple systems through synchronization.

Password Self-Service and Profile Management

PasswordCourier's self-service profile management option enables your employees, business partners and customers to privately and securely register and maintain their authentication questions and answers as well as personal profile information directly within your existing enterprise directories or corporate databases. PasswordCourier's self-service capabilities help your organization reduce support costs, deliver more personalized service, and ensure the privacy and integrity of your users' digital identities.

You ensure that end user accounts are secure, while relieving your support and security organizations of the burden of processing routine, labor-intensive functions. The entire password management process is automatically logged within your help desk application and all user-related information and transaction data is collected and tracked. The end result is better service, stronger privacy, and high-quality data for security and compliance reporting.

Enforcing Strong Policies

Password management solutions must support the ability to enforce strong password policies. PasswordCourier enables organizations to centrally define and consistently enforce strong password policies to ensure compliance with corporate security guidelines and to maximize data security. PasswordCourier's policy engine enables you to apply simple or highly complex rules to target systems and applications. By prechecking the password to ensure that it complies with the policy and then updating the native system's password history with the new password, PasswordCourier enables an unlimited range of password policies to increase security and user adoption.

Flexible Policies

Using PasswordCourier's policy engine, organizations can apply a wide variety of password rules to all systems and applications, selected groups of systems and applications (e.g. all UNIX systems, all z/OS systems, all web portals), or individual systems and applications. Just a few examples of the wide variety of password rules that can be put into effect include minimum/maximum password length, history and dictionary checking, required mixed case, and numeric or special character use.

Administrators also have flexible options for managing password synchronization. **Active Synchronization** enables end users to choose individual accounts and passwords from an eligible list. **Transparent Synchronization** enables password changes made using native tools to be propagated to all systems. It has the intelligence to know which resets have been initiated by PasswordCourier and which came from native tools, which enables PasswordCourier to avoid "double loops" of resets.

Maximizing User Adoption

The success of any self-service password management initiative begins and ends with how many people use the solution. If end users can't or won't access the system, your organization will not see the call reduction, cost savings, productivity increases, and security improvements that are expected.

PasswordCourier's multiple access options provide the ease of use, 24x7x365 availability, and flexibility to accommodate your business needs and end user preferences. The options include Web access, desktop access, telephone, voice recognition, secure kiosk, and service desk access.

Access Options

| | |
|--------------------------|---|
| Web Access | Enables end users to manage passwords through a Web interface. |
| Desktop Access | Enables self-service resets from any Windows® login screen, including Windows Vista®. |
| Telephone | Interactive voice response enables password reset using a telephone touchpad. |
| Voice Recognition | Enables users to reset their password by speaking with an automated telephone system like they would with a live help desk agent. |
| Secure Kiosk | Reset and synchronize passwords through a dedicated, shared network workstation. |
| Service Desk | Enable service desk personnel to manage password resets on behalf of users. |

Easy Administration

PasswordCourier delivers robust integration with all leading service desk applications. PasswordCourier automatically opens and manages service desk tickets, ensuring rapid service delivery and accurate security audit and service level reporting. This makes it easy for your help desk to deal with users who are unable or unwilling to manage their own passwords.

Implementation is simplified because developers have a graphical view of the service desk schema, enabling rapid, point-and-click configuration of ticket fields specifying the information to be captured with each ticket.

Security Capabilities

| | |
|----------------------------------|--|
| Password Policies | Facilitate discovery of SoD policy conflicts. |
| Authentication | Allow end users to create custom challenge/response question and answer pairs to ensure fast, secure self-service authentication. |
| Selective Synchronization | Configure e-mail and pager alerts to confirm provisioning actions or warn of suspicious activity. |
| Audit Trails | Automatically capture the details for every password reset request in service tickets within your existing service desk application or database. |
| Notifications | Automatically open, populate, and close service tickets for real-time security audit and service level reports. |
| Secure Sessions | Transfer data using SSL encryption, and store and compare data in encrypted or hashed formats. |

Optimizing Existing Infrastructure

Courion delivers more than 150 enterprise connectors covering all major operating and network systems, platforms, middleware and applications, that ensure password policies are enforced consistently and use the most appropriate native format for the target system. For platforms or applications not currently supported, Courion provides a Rapid Development Kit (RDK) for connector development.

Infrastructure Integration

| | |
|---|--|
| Database and Directory Integration | Leverage existing sources of employee, business partner, and customer data to quickly create password management workflows. |
| Workflow Flexibility | Dynamic communities provide granular control over password management workflows, including flexibility for bulk actions. |
| Enterprise Level Performance | Multiple password workflows per server and support for multiple servers accommodate unlimited numbers of simultaneous password reset requests. |
| Customizable Web pages | PasswordCourier can be easily adapted to reflect the look and feel of your company's support portal, Intranet, or web site. Multi-language support provides user interfaces in a variety of non-English languages. |

Backed by Industry-Proven Services

Courion's Enterprise Suite is backed by world-class, expert services delivered directly by Courion or by our Certified Solution Partners. Courion's discovery and implementation methodology allows customers to efficiently achieve the desired level of policy automation for their targeted business processes. Courion'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.

Courion Access Assurance Suite Solution

PasswordCourier is part of the Courion Access Assurance Suite, which includes:

| | |
|-------------------------------|--|
| ComplianceCourier | Access certification and remediation – ensure that end user access rights comply with corporate policy, industry standards or government regulations. |
| RoleCourier | Enterprise role management – define and manage end user roles to automate role creation, provide role lifecycle management, and assign users to one or more roles as part of the provisioning process. |
| AccountCourier | End user provisioning – define and implement accounts and access rights to enterprise systems, including operating systems, networks, databases, servers and applications. |
| PasswordCourier | Client-based password management, including end user self-service password and profile management. |
| Sensitive Data Manager | Review sensitive data identified by data loss prevention products and approve or remediate user access rights to reduce risk and ensure compliance. |
| User Activity Manager | Monitor and manage access rights for users who may be engaged in risky or unauthorized activity. |

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 on Windows Server 2008 | |

Other requirements may apply, contact Courion for further information.

About Courion

Courion, the leader in access risk management, helps companies identify, quantify and manage the risks associated with information access. Used by nearly 500 organizations and over 14 million users worldwide to quickly and easily solve their most complex identity and access management (password management, provisioning, and role management), risk and compliance challenges, Courion can help your company win in today's mobile, always-on, cloud-based business environment.

For more information, please visit our website at www.courion.com, our blog at blog.courion.com, or on Twitter at twitter.com/Courion.

