Secure and Efficient Password Administration:

Problem Solved by SplashID™

Managing Passwords and Other Confidential Records in the Secure Enterprise

Find Out How SplashID Offers the Best Solution, Increases Security, Improves Productivity and Decreases IT Costs

SplashData, Inc.
201 Los Gatos-Saratoga Road
Los Gatos, CA 95030

www.splashdata.com/enterprise

Target Audience

- IT architects, engineers, and administrators interested in password security
- Technical evaluators for IT security solutions
- Executives reviewing options for improving password security

Executive Summary

- Password security is critical in the modern enterprise.
- Password policies are necessary for security but create user frustration and increase IT help desk costs.
- For larger enterprises, Single Sign-On (SSO) systems can help alleviate these issues, but SSO systems rarely offer complete coverage of all password needs, leaving security gaps. For smaller organizations, SSO systems are generally cost prohibitive.
- SplashData's SplashID™ Enterprise can augment SSO in larger enterprises and effectively replace SSO in smaller organizations.
- SplashID Enterprise not only helps an organization's admin secure and manage passwords, but also helps departments such as IT, Finance, HR, and Engineering manage and share records, including IP addresses, host names, software registration codes, account numbers, documents, and more
- SplashID Enterprise is cost effective: starting at $5 per user per month, and volume discounts can take the price as low as $1 per user per month
- For more information, go to splashdata.com/enterprise or contact Arjun Thyagarajan at SplashData:

Arjun Thyagarajan

enterprise@splashdata.com

408-335-7363

Introduction

Today nearly all of an organization's critical information is digital, stored in a variety of databases throughout the enterprise. This information can be extremely sensitive: financial records, legal documents, strategic plans, and sensitive personal information.

The cost to the organization when these databases are compromised can be astronomical. A recent study by Poneman Institute, an information management research firm, relating to data security breaches in the United States shows that total per-incident costs in 2009 were $6.75 million. The most expensive data breach in the study cost almost $31 million to resolve.

Since organizations are continuing to digitize an ever-increasing amount of information, there are consequently more and more databases and storage locations. While requiring employees to use a username/password combination to limit access to sensitive data is obviously necessary, the number and types of usernames and passwords that many employees must remember has been steadily growing.

Employees need more secure usernames and passwords, yet this increasing volume of username/password combinations leads to major issues for IT managers.

There is a fundamental dilemma in optimizing access and boosting productivity while maintaining security

- Without the right password and information management solution, it is difficult for enterprises to simultaneously maintain employee productivity and ensure password and information security.

The lack of a password management solution can result in a costly cycle of lost employee productivity

- Employees forget their passwords and have to call the IT department for password help instead of working on the task at hand.
- The IT department becomes tied up with requests to change employees' passwords and is not able to service important requests.

Password and Information Management Problems

While the cost for breaches of security when it comes to passwords, account numbers, PINs, and web logins requires solutions, the solutions themselves raise problems for IT managers.

Problem #1: Lack of Compliance

There are well-known, accepted standards for creating and maintaining secure passwords, including specifying length, type of characters, and frequency of password changes.

Unfortunately, these standards become a hassle for users. The frustration and inconvenience of remembering multiple secure passwords can lead employees to compromise prudent standards. Any of the common actions below make digital identities and sensitive information less secure, creating a serious corporate security risk:

- Forgetting passwords, tying up your IT department with internal calls.
- Writing down passwords or storing them in insecure files on computers.
- Relying on a browser, cookies, or an unsecured web site to remember passwords.
- Using simple, easy to remember passwords that are easily compromised.
- Recycling passwords or using slight variations of the same username/password combination over and over.

Problem #2: Identity Theft

Even if all of your employees adhere to your organization's password policy, outside identity thieves can still pose security threats to your organization. Identity theft is a serious and widespread problem, one that has grown with the proliferation of online services and information. After obtaining a valid username/password combination, identity thieves can access your organization's databases at will and are difficult to detect.

A strong password policy can be an effective deterrent, but it cannot completely stop three common security threats:

- Keylogging uses specialized software to record a user's keystrokes. Usernames, passwords, and the sites on which they are entered can often be determined using keylogging tools.
- Password hacking involves methods ranging from guessing people's passwords based on personal information to using hacking software to steal passwords directly.
- Phishing is a method of piracy. Thieves create fraudulent sites (often made to resemble legitimate sites) that ask for information such as account numbers, passwords, and

Social Security numbers. Thieves then use this information to make financial transactions or steal trade secrets.

Dr. Anita Amico, an information security specialist, delineates two types of costs to an organization from a data security breach:

1) Lost business due to the unavailability of breached information resources
   - Lost business that can be traced directly to accounts fleeing to a "safer" environment
   - Lost productivity of the non-IT staff, who must work in a degraded mode, or not at all, while the IT staff tries to contain and repair the breach
   - Labor and material costs associated with the IT staff's detection, containment, repair and reconstitution of the breached resources
   - Labor costs of the IT staff and legal costs associated with the collection of forensic evidence and the prosecution of an attacker
   - Public relations consulting costs to prepare statements for the press and answer customer questions
   - Increases in insurance premiums
   - Costs of defending the company in any liability suits resulting from the breached company's failure to deliver assured information and services.

2) Intangible costs of security breaches:
   - Customers' loss of trust in the organization
   - Failure to win new accounts due to bad press associated with the breach
   - Competitor's access to confidential or proprietary information.

Parts of the Password Security Solution

Leading technology-oriented enterprises and organizations are seeking to protect data confidentiality by using a combination of the following:

- Strong Password Policies
- Multiple-factor Authentication
- Password Administration System

Part 1: Strong Password Policies

Most companies start to solve their password challenges by adopting and attempting to enforce strict password policies.

- Passwords must be at least six or eight characters long.
- Passwords should never be a common word found in the dictionary and should contain at least one letter and one digit. Even stronger passwords should contain at least one punctuation mark or other special character.
- Passwords should contain a mix of upper-case and lower-case letters.
- Passwords should be changed at least every 30 days.

A password policy is an essential step, but the problem with this solution on its own is that the stronger the password policy, the harder it is for employees to keep track of username/password combinations. This generally leads to employees taking shortcuts that compromise security and can lead to significantly increased calls and costs to the IT department.

Part 2: Multiple-factor Authentication

Multiple-factor authentication means there are at least two different types of credentials that must be submitted in conjunction to be authenticated. There are three categories of authentication factors:

- something you have (a hardware or software token)
- something you know (a password)
- something you are (a thumbprint, retina scan or voice print)

Each factor in the authentication mechanism should be from a different category. By layering on additional factors in your authentication process, you can make it very tough for hackers to force their way into your systems.

Multiple-factor authentication can be an effective addition to security, but it can be cost prohibitive for many organizations and even in larger enterprises it is often used only for the most secure facilities or systems. And even when multiple-factor authentication is in place, one

factor usually is still a password covered by a password policy, which can lead to the same associated risks described above.

Part 3: Password Administration System

The answer to the security issues raised by passwords is a password administration system. To date, most advanced enterprises have used a system called Single Sign-On, or SSO. SSO is an authentication mechanism to gain access to multiple independent software systems, although those systems are often related. With SSO a user logs in once and gains access to multiple systems without being prompted to log in again at each of them. SSO does effectively enhance security, but SSO solutions often take months to deploy across an enterprise, require extensive application integration, and due to high costs typically do not provide immediate ROI.

Even when an SSO system is in place, there are almost always legacy systems in the enterprise that are not covered by the SSO system. Or there are websites outside the SSO system that employees need to regularly access. Or there are client or partner systems not covered by the SSO system. In fact, this situation is so common that there is an acronym for it– RSO for Reduced Sign-On. Most SSO systems are in fact RSO, leaving security gaps.

Now there is an effective alternative or addition to SSO/RSO: SplashID Enterprise.

SplashID Enterprise is the Solution

SplashID Enterprise is designed to quickly and effectively address the most immediate password management concerns of IT. It allows an organization to use stronger password management practices without compromising security or increasing costs.

For almost 10 years, SplashData's SplashID has been the leading application for safely and securely storing sensitive passwords and other records in a secure, encrypted database locally on desktops, notebooks, smartphones and other mobile devices. SplashID organizes and protects user names, passwords, filenames, account information and other critical data. SplashID has over 1 million individual users worldwide and has also been licensed in volume for employees by security conscious organizations such as financial institutions (State Street, Bessemer Trust, America First, NetBank), research facilities (Los Alamos National Labs, Lawrence Livermore National Labs, National Institutes of Health), and universities (University of California, University of Florida, Texas A&M, University of Wisconsin).

Responding to requests from these enterprise users, SplashData now offers a completely new version of SplashID enabling centralized administration by IT management. The new edition is called SplashID Enterprise.

Overview of SplashID Enterprise

SplashID Enterprise provides a complete password management and security solution for organizations using either Windows or Mac OS platforms for end users. SplashID Enterprise offers IT managers powerful control for the centralized administration of password and security policies across various departments and employee groups throughout an enterprise.

Benefits of SplashID Enterprise

- Increase employee productivity: SplashID makes managing and accessing passwords easier and more convenient, giving your employees more time to focus on important tasks. SplashID will decrease forgotten password requests, ridding IT of unnecessary distractions and allowing focus on projects that create real value. In addition, the next update of SplashID Enterprise will optionally give your employees access to records on their smartphones, enabling them to be more productive out of the office as well.
- Decrease potential costs of security threats. As described earlier, the costs of data breaches are astronomical. By implementing SplashID, your organization significantly reduces the risk of information stolen via password exposure, including data loss, legal costs, the loss of customers, and the loss of employee productivity.

Features and Benefits of SplashID Enterprise

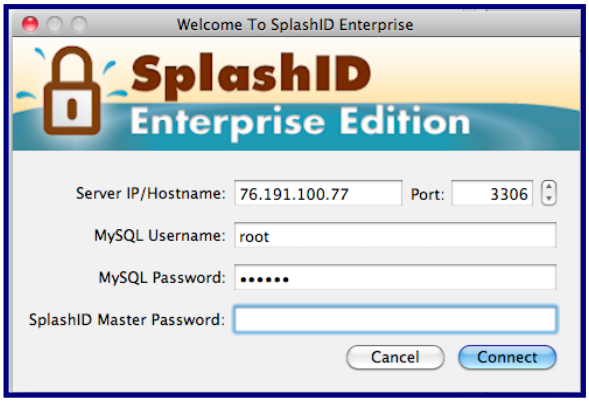
The major features of SplashID Enterprise include:

- Cross-platform Windows and Mac end-user support
- Support of MySQL server on Windows, Mac, or Linux
- Centralized secure database of usernames, passwords, documents, and other records
- Administrative control panel for IT with user management
- Customizable group-level and user-level permissions
- Customizable deployment architecture
- Multi-layer database security
- Optional client applications for smartphones (including iPhone, Android, and BlackBerry), tablets, and browsers

SplashID makes it easier for organizations to protect passwords and other information assets:

Easy to Use for Employees

- Each employee protects his or her important information with one secure master password
- Each employee will also have the option of creating their own 'personal' database which only they have access to.
- SplashID enables users to automatically login to websites (IT can disable this option if desired)
- SplashID offers definable list views, support for custom icons and field labels
- All data is encrypted via multiple layers of encryption, including FIPS-approved 256-bit AES, and is automatically backed up on the central server

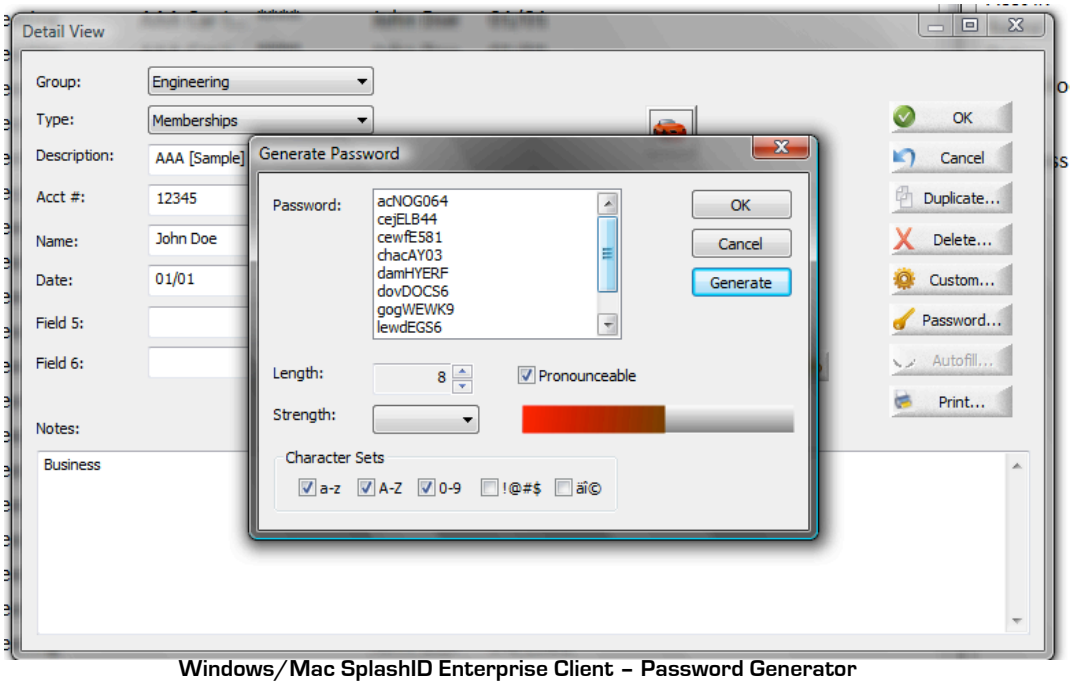


Easy to Manage for IT Administrators

- Centralized control panel makes it easy to create, edit and delete users, assign permissions and quickly employ password policy revisions across the enterprise.
- SplashID supplies a single registration code to the IT department that can be used for an entire deployment so you will not have to bother with individual registration codes for each user.

Secure Your Company Passwords and Information

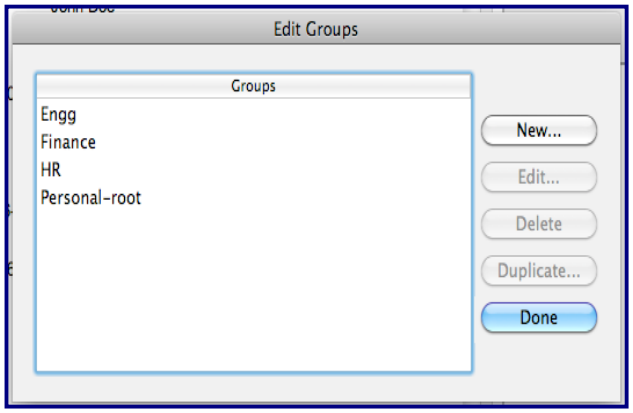
- Stores passwords and other information and protect them with powerful FIPS-approved 256-bit AES encryption plus additional layers of security (see below)
- No records are stored locally on users' hard drives, giving IT complete control over records
- Since SplashID makes it easy to remember passwords, employees are better able to follow recommended procedures for creating strong passwords.
- SplashID includes a password generator capable of creating hard-to-guess random passwords.

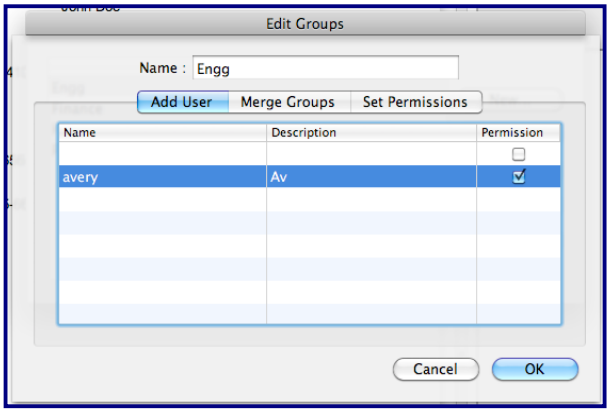


Windows/Mac SplashID Enterprise Client – Password Generator

Secure Groups Creation

A great feature in SplashID Enterprise version is the ability to create Groups. Groups can be created for departments or other types of functional teams within the company. Every Group can have a specific set of records that only members of the Group have access to. A new user





assigned, for example, just to the Finance Group can view only the records specific to Finance.

Groups act as filters for grouping related records. Groups can be created on the Admin application or Client application (provided the employee has the permission to create a Group).

Each user will also have the option of creating a set of Personal records, which only that user will have access to.

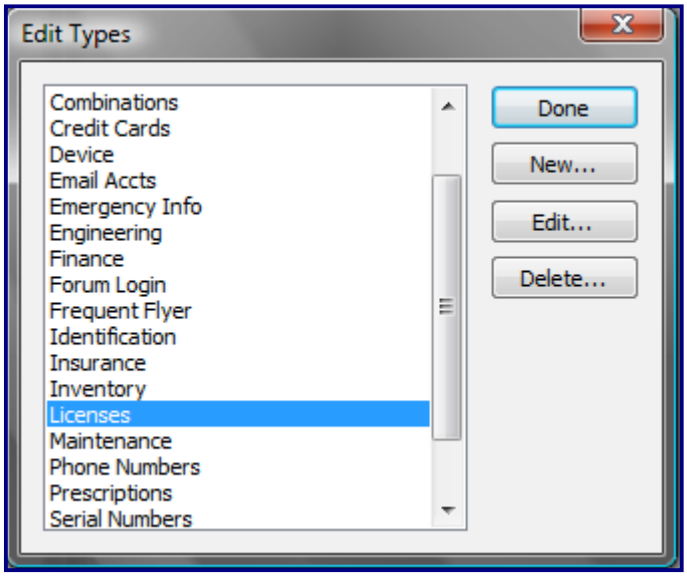
Multiple Record Types

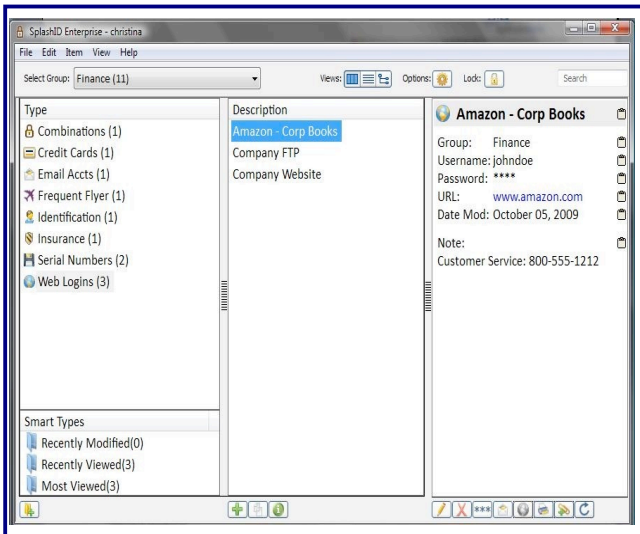
One of the benefits of SplashID Enterprise is that it can be used to manage more than just username/password combinations. In fact, SplashID Enterprise can be considered not just as a password administration tool, but as a solution for secure record management and sharing. SplashID contains forms for storing records for web logins, accounts, codes, contacts, and more. New custom forms can be added, making SplashID's capability for record storage unlimited.

Also, employees may choose to store personal records in addition to enterprise records in SplashID, and the records are kept separate on the server.

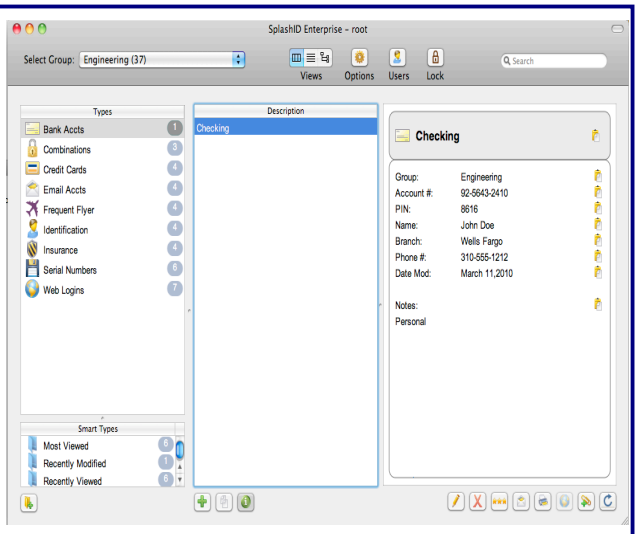
Some examples of the kinds of records companies store in SplashID are:

- IP addresses
- Host names
- Bank account numbers
- Insurance records
- Software registration codes
- Contact information
- Serial numbers
- Vehicle information





Windows SplashID Enterprise Desktop Client



Mac SplashID Enterprise Desktop Admin

Attachment Support

SplashID Enterprise also enables users to add attachments to records.

- Photographs
- Schematics
- Drawings
- User manuals
- Instructions
- PDF's
- Text documents
- Spreadsheets

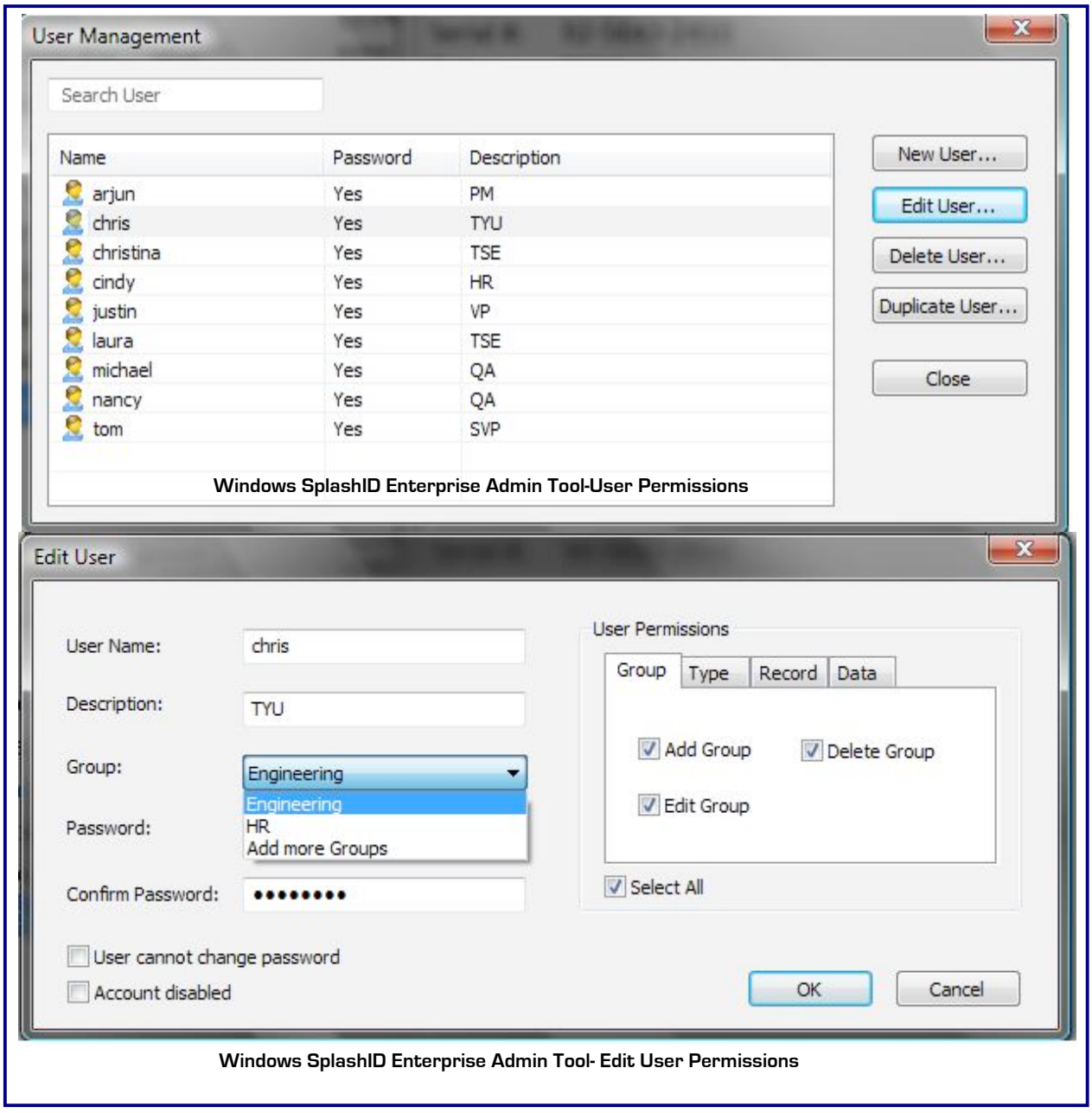
Record Sharing

One of the advantages of SplashID Enterprise is the enabling of sharing and collaboration. In many cases in an enterprise organization, certain logins or other records need to be shared company wide, department wide, or among only a certain group of employees, and SplashID makes this process easy and secure.

This record sharing feature of SplashID Enterprise is customizable by not just the central IT admin but also by individual groups or departments within the enterprise.

Here are some real examples of how SplashID Enterprise's sharing capabilities are being used:

- An IT department shares records containing IP addresses and server information, but only among specific IT personnel within the department
- A Finance department shares bank account records, but only within the department and with the CEO
- An HR department shares contact information for vendors providing payroll, insurance and 401(k) plans, but only within the department and with Finance



Windows SplashID Enterprise Admin Tool-User Permissions

Windows SplashID Enterprise Admin Tool- Edit User Permissions

Security

SplashID Enterprise allows you to securely store company data. Data is encrypted, protected, and locked on a central database, and only users that have access to the system can read or edit data.

Key Security Features of SplashID Enterprise

- **256-bit Blowfish and AES encryption** - Your SplashID data goes through two rounds of encryption - 256-bit AES and 256-bit Blowfish. The password is also encrypted within the MySQL

database. SplashID Enterprise uses approved Blowfish and AES libraries for all of its encryption and key generation. SplashID Enterprise is also compliant with FIPS 140-1 and FIPS 140-2.

- **Secure communication** - Client-server communication of SplashID data occurs only when the data is in an encrypted state. Communication is directly over TCP/IP, where IPsec provides an additional layer of security.

- **Secure MySQL database** - MySQL itself encrypts the data using the in-built MySQL encryption methods. Only the SplashID Enterprise Admin with root access can log in to the database. If the database is running locally or within the company network, TCP networking can be disabled for remote access.

- **User Permissions** - While creating users, the SplashID Enterprise Admin applies access control settings for each user. The Admin assigns Group and record based permissions, and so each employee's access depends on the permissions granted by the Admin.

- **Secure Backups** - SplashID Enterprise Admin can backup the company's SplashID data to a secure password protected SplashID vID file. Also, the entire MySQL database can be backed up, and that backup is also encrypted.

- **Timeout** - SplashID will automatically lock and hide the data after a specified period of time, so the Admin or employee doesn't need to remember to logout of SplashID when leaving a desk.

- **Strong Password Generator** - Admin and users can use the customizable Password Generator in SplashID to create passwords that are complex and unguessable.

Implementation of SplashID Enterprise Edition

SplashID Enterprise offers a simple architecture that works with existing enterprise systems so that SplashID can be up and running on your employees' computers in very little time, under an hour in most cases.

There are three components that comprise the SplashID Enterprise System:

- **MySQL Server** (SplashID database) - SplashID Enterprise records are encrypted and stored in a MySQL database server. MySQL server can run on Windows, Linux or Mac.
- **SplashID Enterprise Admin application** (used by the IT Administrator) – The SplashID Administrative Control Panel application requires root access to the MySQL server. The Administrative Control Panel is used for User Management to create, edit, delete users and assign permissions on the system. The Admin application can run on Windows or Mac.
- **SplashID Enterprise Client application** (used by Employee) - Employees or IT installs the SplashID Enterprise client application on desktop instances (Windows or Mac). The IT administrator provides employees with initial SplashID Enterprise login credentials via an automated system.

SplashID Enterprise Deployment

There are two ways to deploy SplashID Enterprise:

Deployment Option 1: Self Hosted

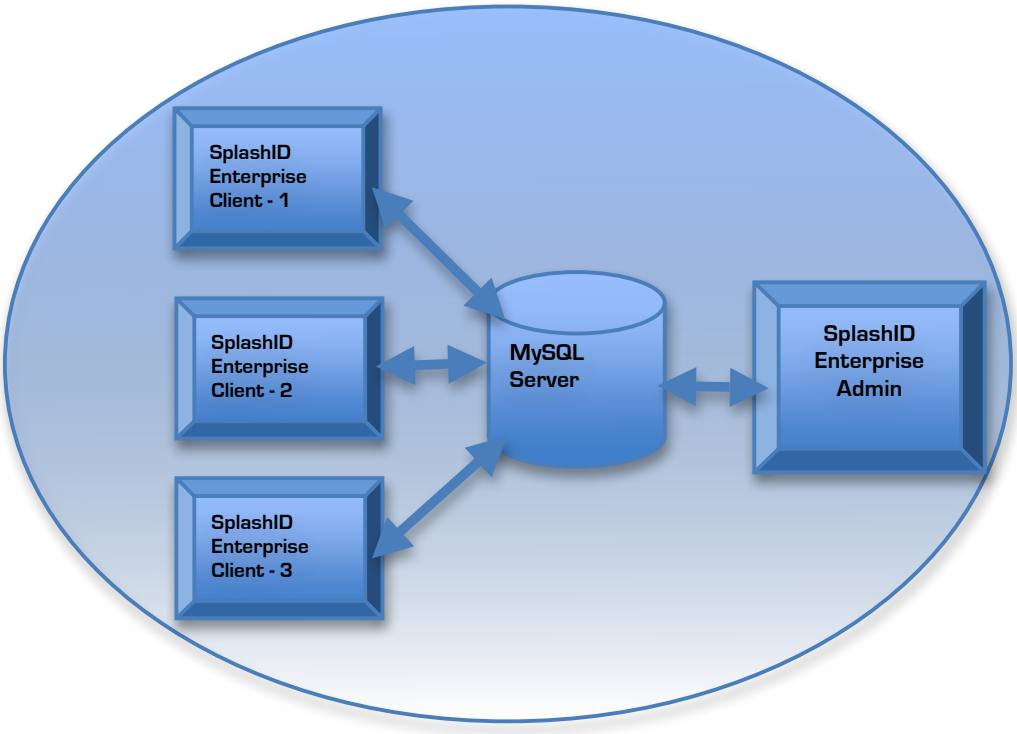
If someone in your organization has experience setting up MySQL servers, you can easily host SplashID Enterprise either in your intranet or in the cloud. Detailed instructions can be found in the SplashID Enterprise Getting Started Guide. The setup will generally take less than one hour. If you prefer a self hosted solution but do not have MySQL expertise in house, SplashData offers consulting services for setting up a self hosted MySQL server. To take advantage of these services, contact Arjun Thyagarajan on SplashData's enterprise team by email: enterprise@splashdata.com.

With either self hosted solution, the steps to deploy SplashID Enterprise are simple:

1. Install MySQL server
2. Launch SplashID Enterprise Admin application
3. Connect Admin application to MySQL server with root access
4. Create users, assign permissions, and create groups as needed
5. Employees launch SplashID Enterprise client applications with login details provided by Admin

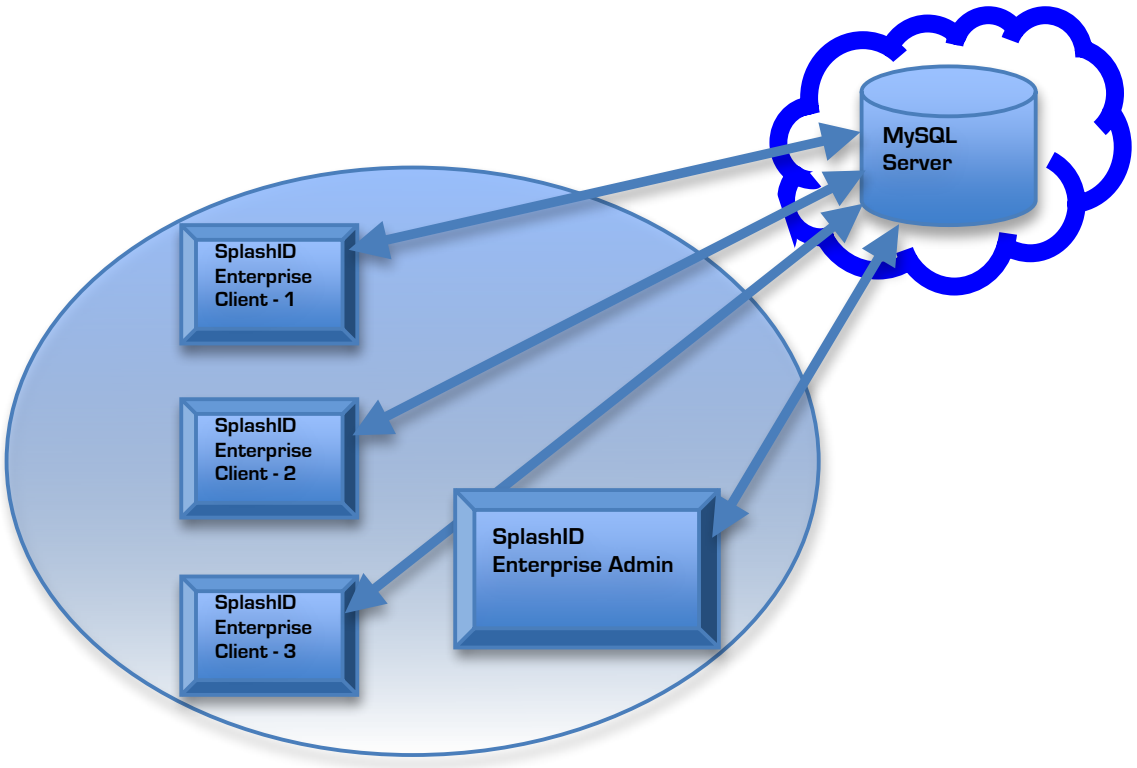
MySQL Server Inside Company Intranet

MySQL server needs to be installed on a system inside the company intranet. Admin and Clients can access the server only while inside the company network or through VPN.



MySQL Server in the Cloud

MySQL server needs to have a globally accessible hostname or IP address, which can be used by the Admin and Client applications to establish connection.



Deployment Option 2: Hosted Solution

SplashData also offers a hosted version of SplashID Enterprise. A hosted solution delivers the benefits of fast and easy implementation, high security, and worry free management. Costs are as low as $100 per month. If you are interested in a hosted solution, please contact Arjun Thyagarajan at SplashData by email: enterprise@splashdata.com.

Costs

SplashID Enterprise is available on a per-seat basis starting at $5 per user per month with significant discounts for volume installations.

How does your organization evaluate SplashID from a cost/benefit standpoint?

To help answer this question, we used a case study of an organization with 1,000 employees and looked at the costs and benefits of a SplashID deployment over two years. Note that the chance of a security breach is variable, since each organization has a different password management system in place and a different value of information at risk.

Explanation of Value Added	Value Added (2 Years)
Increased Employee Productivity: 1000 employees with an average wage of $30 per hour each gain 1 hour of productivity per year	$60,000
20 fewer calls per week to IT about lost or forgotten passwords. Cost of each call including time spent on task after call is assumed to be $5	$10,400
Eliminating the Potential Cost of Security Breach: Without SplashID, assume that there is a 10% chance of a security breach each year that would cost the organization $100,000 (both estimates are conservative).	$20,000
Total Value Added	$90,400

Explanation of Costs	Costs
1000 seats of SplashID at $1 per user per month	$12,000 / year
Service, support, upgrades, hosting, additional mobile and web clients	All included
Total Costs	$24,000

Bottom Line: Net Value Added	**$66,400**
Return on Investment (ROI)	**376%**

SplashData Company Background

SplashData, Inc. (www.splashdata.com) is a leading provider of security and productivity software for Windows and Mac-based computers as well as mobile computing environments, including iPhone, BlackBerry, Android, Windows Mobile, Symbian S60, UIQ, and Palm OS and Palm webOS. Based in Los Gatos, California, SplashData was founded in 2000.

For almost 10 years, SplashData's SplashID product line has been a clear market leader in password management and security, and SplashID now has over 500,000 users worldwide. Many different types of organizations have entrusted SplashID with their critical data by acquiring volume licenses for IT departments or groups of employees. SplashID has been adopted by government agencies, technology companies, investment banks, research labs, and other organizations needing a simple and effective password security solution.

Selected organizations that have deployed SplashID in volume include:

- America First Credit Union
- Bessemer Trust
- Carleton College
- Columbia Forest Products
- Lawrence Livermore National Labs
- Los Alamos National Labs
- Fairfax Water
- Farmers State Bank
- The Getty Foundation
- HealthPlus of Michigan
- HM Land Registry (UK)
- Johns Hopkins University
- National Institutes of Health (NIH)
- National Science Foundation (NSF)
- Montgomery Law Group
- State Street Bank
- Texas A&M
- University of California
- University of Florida
- University of Wisconsin
- US Federal Court System
- US District Court System
- US Bankruptcy Court System
- White Sands Federal Credit Union
- YMCA

Next Steps and Contact Information

- For more information, go to splashdata.com/enterprise
- For specific questions, please contact Arjun Thyagarajan at SplashData:

Arjun Thyagarajan, SplashData Enterprise Team

enterprise@splashdata.com

408-335-7363