SCM Anywhere
TM
Hosted

DynamsoftTM PRESENTS...

Secure Your Source Code and Digital Assets
– World's 1st Hosted SCM Solution

Studies show that companies of all sizes have begun adopting SaaS (Software as a Service) solutions in a faster pace as a way to implement IT services more quickly and to lower IT costs.

SCM Anywhere Hosted is the world's 1st hosted SCM (software configuration management) solution. It is delivered as a SaaS application and comes with **fully integrated version control, issue tracking, build automation and professional service** to manage your whole software development life cycle. SCM Anywhere Hosted is hosted in Primus Data Center to ensure that you have the most reliable access to mission-critical data and uncompromised security.

Dynamsoft has heavily invested in SCM Anywhere Hosted's development, infrastructure, support and maintenance. As a software development company, we fully understand the importance of source code and digital assets security. We designed SCM Anywhere Hosted to operate at a level of security that most in-house operations can't match.

This white paper describes SCM Anywhere Hosted's security features and gives an overview of the data center.

SCM Anywhere Hosted Security Features

SCM Anywhere Hosted incorporates a range of security features that secure your source code and digital assets from accidents and malevolent attacks. Here's how the features break down.

Secure Sockets Layer (SSL) Protocol

Secure Sockets Layer (SSL) is a strong cryptography and security protocol used to safe-guard sensitive data during transmission over open, public networks. Originally developed by Netscape to secure online financial transactions, SSL is now one of the leading security protocols on the web. Today, SSL supports millions of online transactions every day and is the de facto standard for secure online credit card purchases, stock trading and banking.

SCM Anywhere Hosted provides 128-bit SSL encryption to protect your data, including passwords and data files, being transferred across the Internet.
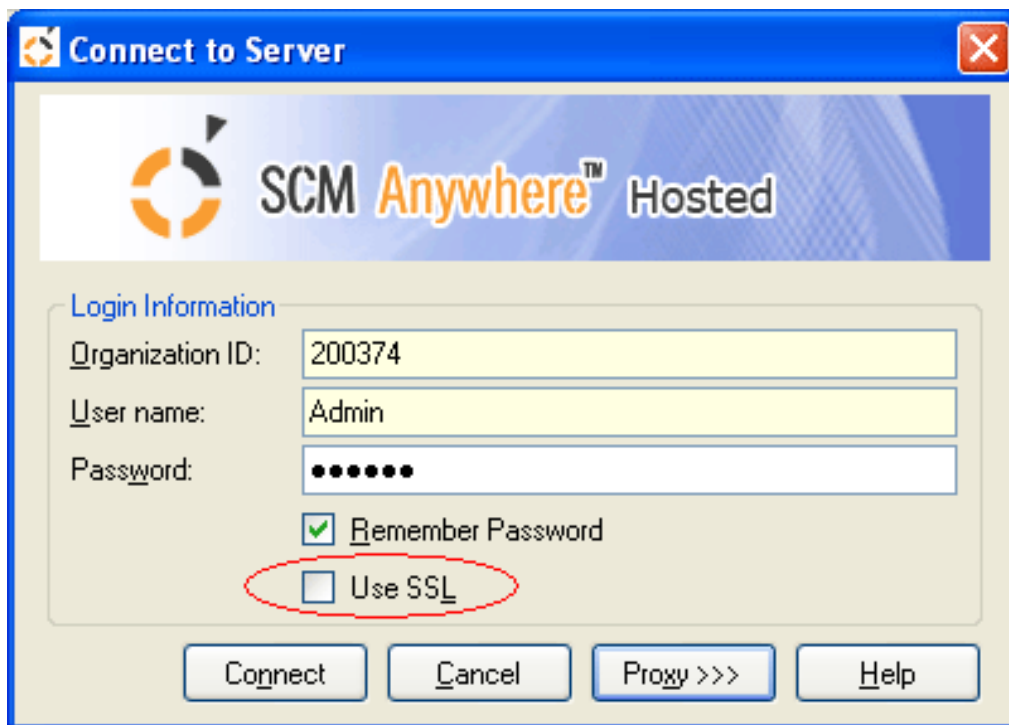

Sophisticated Password Policy

Passwords are the front line of computer security. SCM Anywhere Hosted uses an industry-standard approach to password policy. We enable granular control of password length, memory, complexity and expiration.

The 'Minimum password length' and 'Password must meet complexity requirements' settings can make a password very difficult to hack.

The 'Enforce password history' feature prevents old passwords from being reused again and again.

The 'Maximum password age' feature can force the user to change his/her password after a certain period. And if an attacker cracks the password, he/she only has access to the database until the password expires. Also, since the password must be changed periodically, it is difficult for attackers to crack.

The 'Lock out' option prevents hackers from guessing at passwords. This feature is particularly important for network applications, like SCM Anywhere Hosted. Here's an example. If a server responds to a login request in 100 milliseconds, an attacker can try 36,000 different passwords in 1 hour. By using the 'Lock out' setting, administrators can minimize the number of password attempts within a specified time frame. For example, if an administrator mandates a 10-minute lock out after five incorrect attempts, the attacker can only try 30 passwords within one hour. This obviously makes a password much safer.
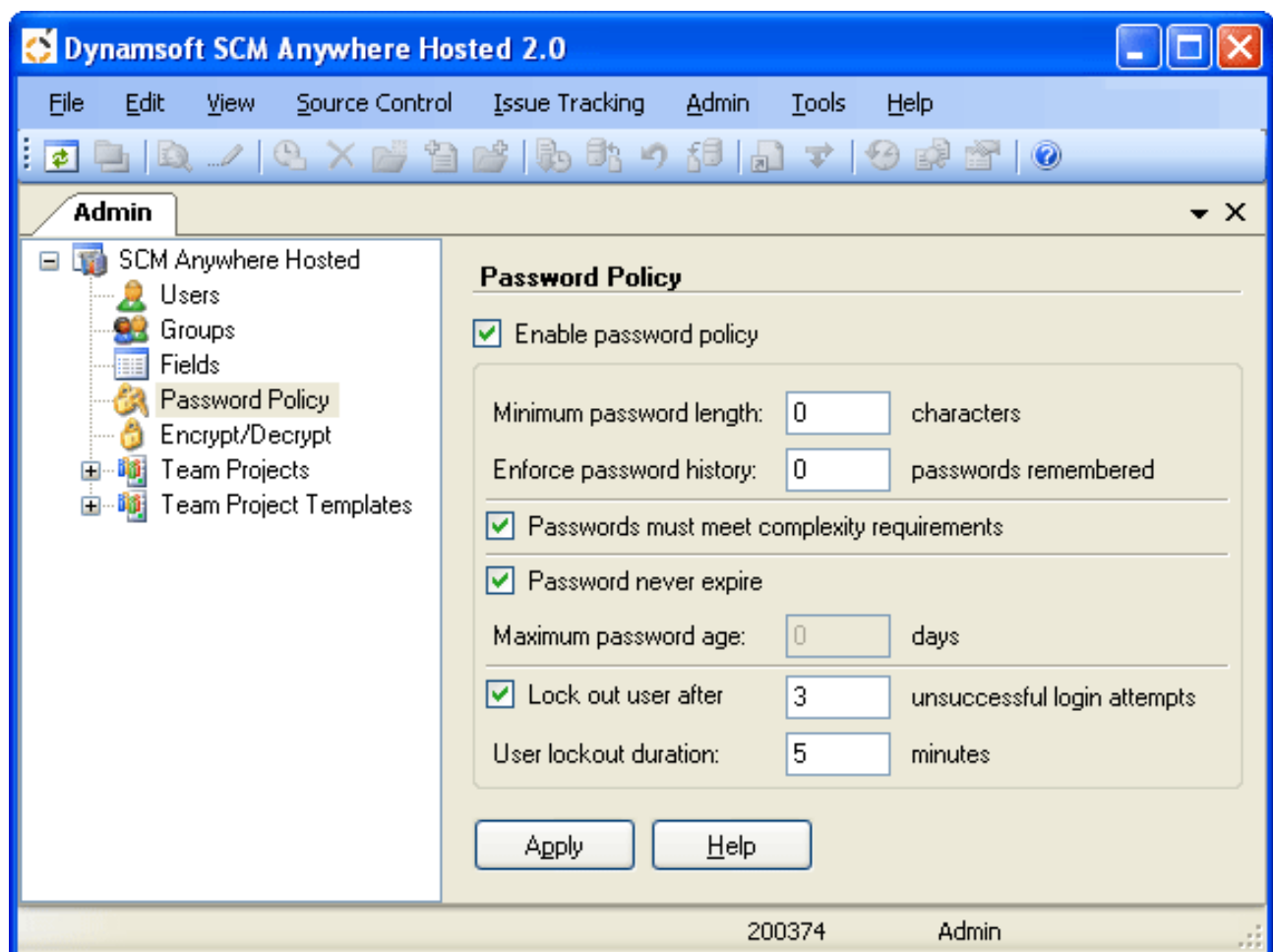
Independent and Isolated Databases for Each Customer

In the SCM Anywhere Hosted server, each customer's data is stored in an independent, dedicated database that's isolated from other customers' data. Customers can only access their specified database, and operations on one database will have no influence on other customers' data.

Database Encryption, the Ultimate Way

SCM Anywhere Hosted provides database encryption, which is an ultimate approach to protect your data. With database encryption, all of your file content stored in SQL Server is encrypted by a passphrase you provide during the encryption process. Under the unlikely worst scenario, even if your database is copied without your permission, no one can read a single file in your repository unless they know your passphrase.
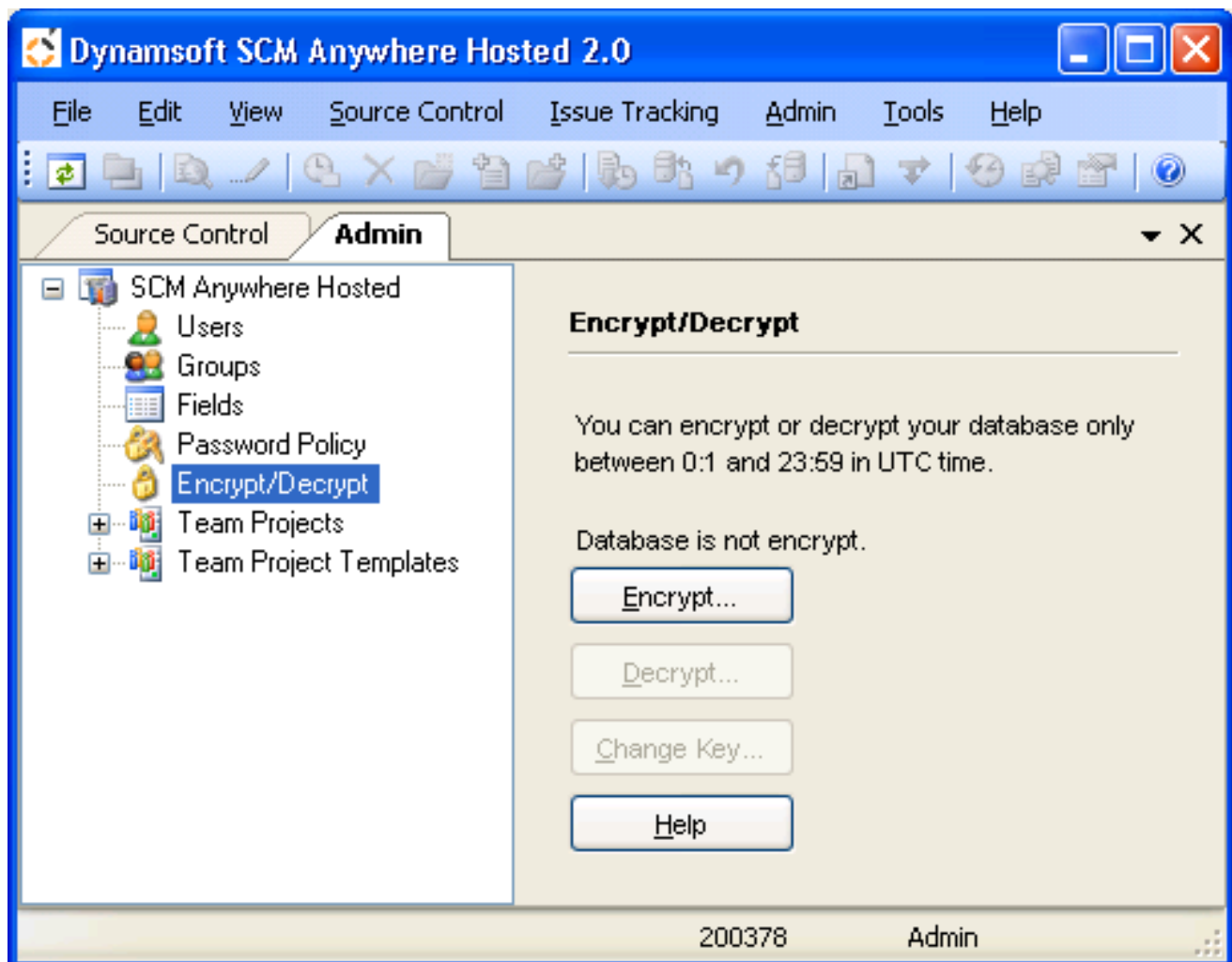
Cache File Encryption for Speed and Security

SCM Anywhere Hosted uses a sophisticated cache mechanism to reduce server workload and improve performance. For the cached files, SCM Anywhere Hosted uses Blowfish encryption to ensure the security of data during the process of caching.

The passphrase is randomly generated by the server when it is started and discarded when the server is down.

Combined with database encryption, cache file encryption guarantees that no file content is written to hard disk without being encrypted.
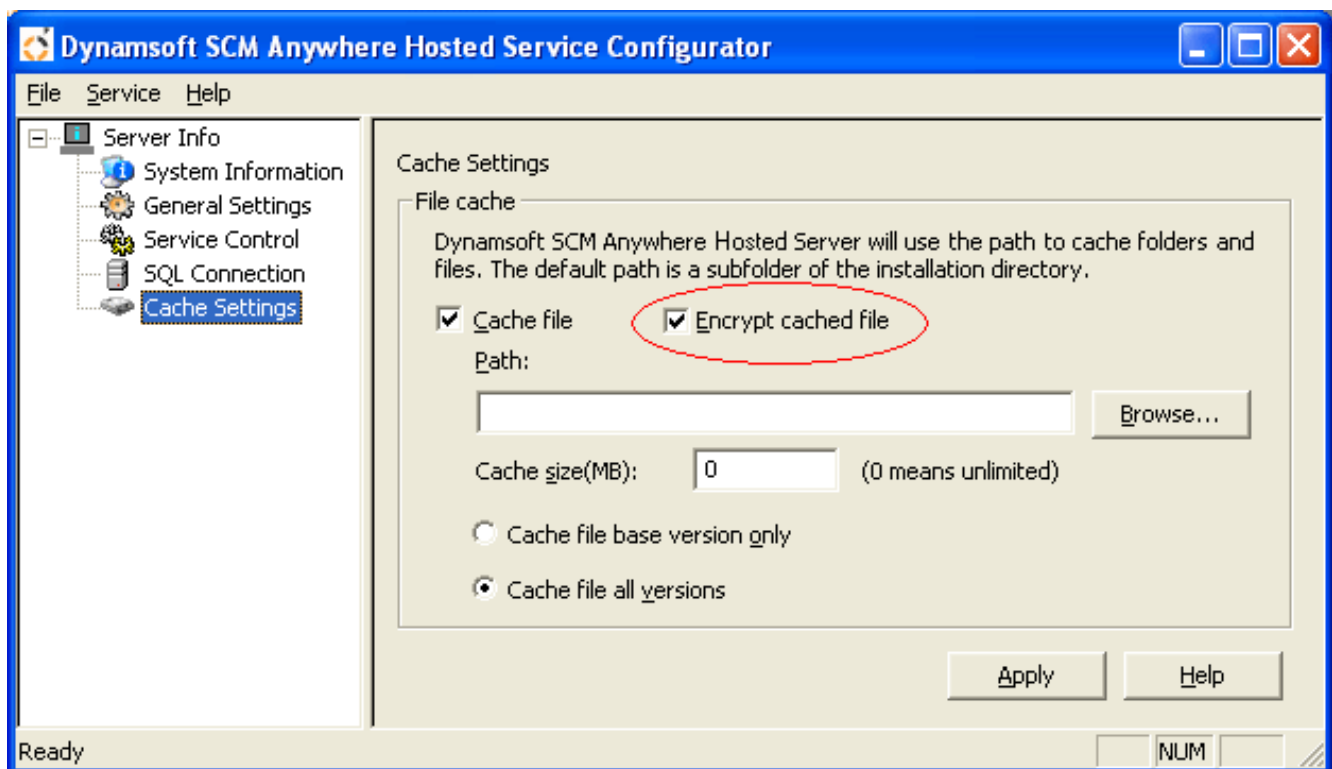
Login Log for Monitoring Suspicious Activity

You can use SCM Anywhere Hosted's *Login Log* to view the 10 latest login attempts to Hosted Server using your organization ID and user name. Using this feature, you can easily identify any suspicious activity in your account. For example, you did not use SCM Anywhere Hosted yesterday, but you see a login log for yesterday or you use SCM Anywhere only from the office but you see an unfamiliar IP in the login log. Once the suspicious activities are identified, proper measurements can be taken to stop the damage.
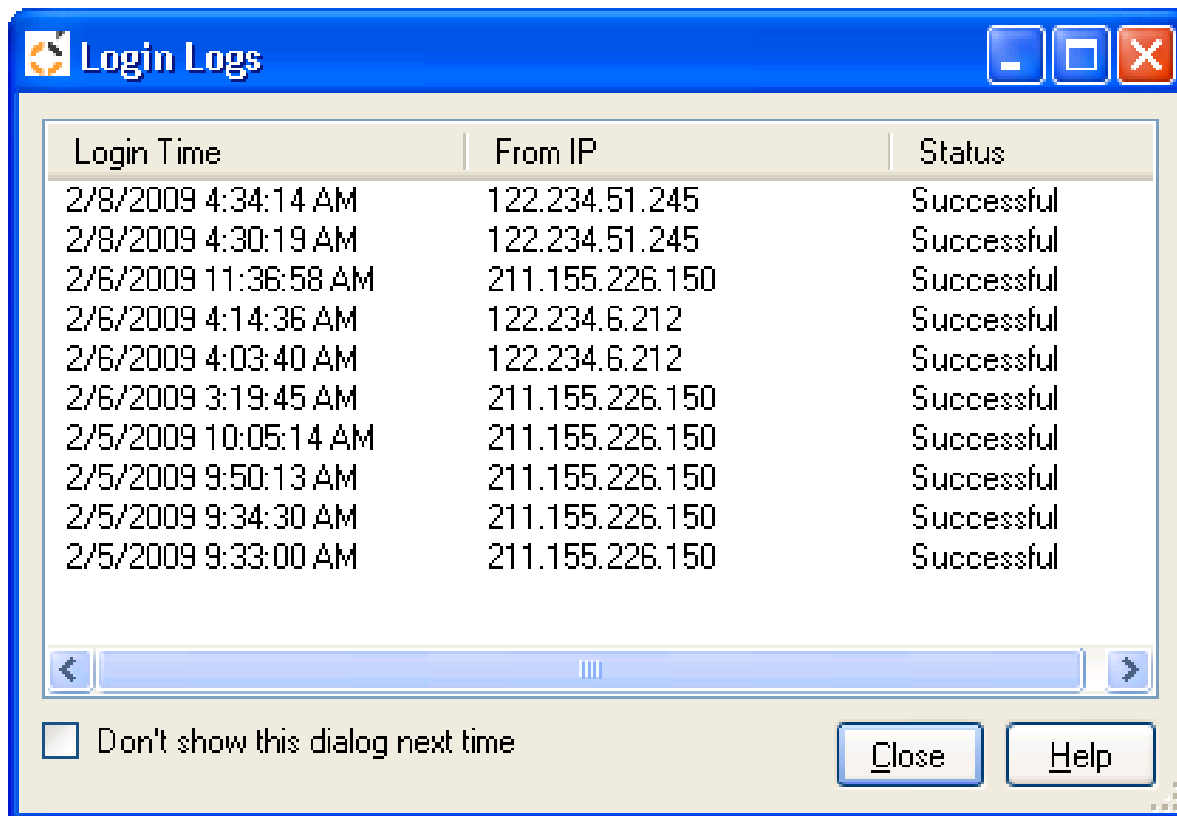
Flexible IP & MAC Filter Rules

You can set up IP & MAC filter rules in SCM Anywhere Hosted. You can create rules for a collection of IP and MAC addresses that allow only specified addresses to access your SCM Anywhere Hosted account. If you choose not to define rules, then all traffic is allowed.

The optional IP filter adds another layer of security. For example, if you only access SCM Anywhere Hosted from your office, you add your office IP address in the filter so your SCM Anywhere Hosted account cannot be accessed from outside of your office. If you also access SCM Anywhere Hosted from home, you can add the IP address of your home in the filter. In the case that your IP address is dynamic (using dial-up), you can simply input your network interface card's MAC address into the filter. Also you can use MAC addresses exclusively to make sure only the specified physical machine can access your SCM Anywhere Hosted account.

Note: IP Filter does not apply to the SCM Anywhere Hosted web portal on the Dynamsoft website.

Add

Type	Address	Modify	Delete
IP	100.100.100.1-100.100.100.255		
IP	192.168.1.12		
MAC	15-16-26-9e-c4-7b		

Total 3 Records

SSL Certificate for Web Site Access

All your account information on our website is encrypted by SSL Certificate.

Secure Backup Encryption

SCM Anywhere Hosted offers onsite and offsite backup. All backups are password encrypted. Plus, the backup folder is also encrypted using Microsoft Windows 2003 Public Key Infrastructure (PKI) file system.

The Primus Data Center

A secure data center is the cornerstone of the SCM Anywhere Hosted SaaS service. Having a secure and resilient data centre ensures high availability and business continuity for our customers, and for us. We offer a secure, state-of-art data center by partnering with Primus. Though hosting with Primus is more costly, we're convinced Primus data center gives our customers the most reliable access to mission-critical data and uncompromised security.

The following are Primus Data Center security features. To learn more about additional features, such as data center redundancy, please visit http://www.scmsoftwareconfigurationmanagement.com/Products/SCMhosted_DataCenter.aspx

- 24x7 monitoring and technical support
- Biometric access control systems and video camera surveillance
- Gas fire suppression system and pre-action sprinkler systems
- Massive power distribution systems with full redundant battery
- UPS backup and diesel generator protection
- Redundant fiber-based multi-homed internet backbone
- Diesel generator power backup system

◇ Summary

SCM Anywhere Hosted offers unrivalled security. It features SSL encryption, password policy, independent and isolated database, database encryption, cache file encryption, login log, IP & MAC filter rule, SSL certificate for web site access and backup encryption.

A world-class Primus data center is used to ensure the physical security of the servers.

For more information about Dynamsoft SCM Anywhere Hosted, please visit:
http://www.scmsoftwareconfigurationmanagement.com/Products/Software-Configuration-Management-SCM-Hosting.aspx