

ControlSphere

Secure Desktop/Laptop Protection System

ControlSphere is a computer security and automation solution designed to protect user data and automate most of authentication tasks for the user at work and home environments.

ControlSphere secures user data, protects privacy and eliminates the need of remembering and typing any passwords. The solution integrates common authentication and data storage procedures on a PC and substitutes them with strong two-factor authentication (with smartcards or USB tokens) making itself a central security and SSO point.

ControlSphere is a modular solution consisting of four general services which can be used separately or in combination. These are:

- **Windows and Network Logon service** allows quick and easy access to multiple computers with multiple Windows accounts by using a single smartcard/token device.
- **Hard disk and file encryption service** allows transparent hard disk and file/folder encryption with variety of options.
- **Password Management service (SSO)** allows password and other secure data storage on a portable secure device. This data will be automatically delivered to requesting Windows programs and WEB forms.
- **Enterprise Token Management System Server** is an enterprise control and configuration module of ControlSphere. It automatically synchronizes and controls secure data on user's smartcard devices.

Windows and Network Logon support service

Besides the standard means of Windows user authentication system, ControlSphere supports strong two and three-factor user authentication to Windows and Active Directory service by leveraging use of smartcard or token devices.



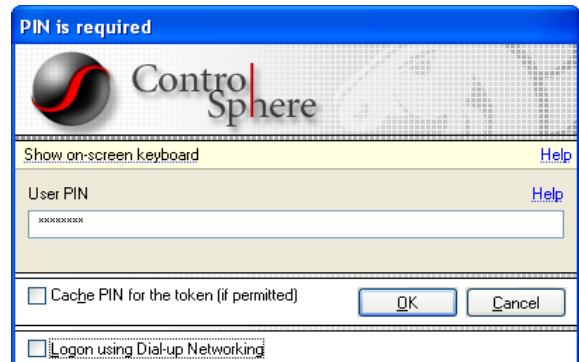
The smartcard (or reader-less USB security smartcard *token* device) can hold a number of user accounts and ControlSphere uses them to logon to Windows on single or multiple computers. At the same time standard Windows authentication means can be enabled or disabled depending on security requirements.

ControlSphere allows users not to remember or even know their password list by keeping and maintaining all secret information on a protected device. All that is required by a user to know is a PIN (personal identification number) or password for the smartcard/token device to logon to Windows and Network.

Once the correct PIN is acquired and the access to secret data is granted, ControlSphere asks user to login using one of the user accounts which match the computer. Same approach is used to unlock a computer.

Once the smartcard/token is removed from the port reader, ControlSphere notifies a user on that and (optionally) gives the user some time to reconnect the device back.

Then program blocks access to the computer or logs the user off depending on the configuration, also performing predefined security actions.



Benefits

- ☑ No manual entry of secure information (user names/passwords)
- ☑ Possibility to use longer and complex passwords
- ☑ Possibility to store and use multiple Windows account credentials on same smartcard/USB token
- ☑ Enable seamless authentication to different user accounts on single or multiple computers with the same smartcard/token
- ☑ Usage of randomly generated passwords unknown to a user
- ☑ Hardware user authentication
- ☑ Two and three-factor authentication
- ☑ Automatic Windows password lifecycle support
- ☑ No need to acquire security certificates or install Certificate server as well as other 3rd party software required for traditional Windows smartcard logon – ControlSphere is self sufficient
- ☑ Product configuration according to individual enterprise security policy
- ☑ Full customization on the authentication methods
- ☑ Automatic blocking of selected programs on smartcard/token removal, session data protection
- ☑ Tight integration with other services of ControlSphere, like for example, automatic encrypted drive mounting on Windows logon.

Hard disk and file encryption service

ControlSphere can store and maintain one or multiple encryption keys (AES256) on a protected device. It is possible to use stacked keys growing the bulk encryption key up to 2048 (8x256) bit. The keys are given names, they can be exported to other secure device or backed up to a Token Image (an encrypted token data clone in a file). The keys can also be centrally maintained by an enterprise security management team. The keys are used in hard disk and file encryption services.

Hard disk encryption support:

This service protects sensitive information from unauthorized access, copying, modifying, and theft on personal computers and removable media devices.

The data is stored on any media in a protected (encrypted) way. Once the encrypted disk is mounted, ControlSphere provides transparent access to the sensitive information. The data is transparently decrypted when it is read from the disk and encrypted before it is written.

A valid encryption key being used by the disk is required to access the encrypted data. The key can be stored on a smartcard/token device (a valid PIN will be required to access it) or in a Token Image (a password-protected file containing cloned ControlSphere token data). The protected information cannot be viewed or copied by other users who do not have an access to the encryption key.

The following operations are supported by ControlSphere on the encrypted drives:

- Manual drive mounting and dismounting, the drive is visible among other hard disks in the operating system;
- Automatic drive mounting and dismounting with a configuration sorted on a smartcard/token;
- Optional automatic dismounting on the key-source device (smartcard/token) removal;
- Disk data backup;
- Disk checking against logical errors with automatic correction;
- Multi-user encrypted drive usage;
- Remote encrypted drive usage from enterprise network on different computers;
- Automatic re-routing of a standard user environment paths (including temporary storage paths) to an encrypted drive (User Home Drive);
- Command-line support for convenient drive administration.

ControlSphere is fully integrated with Windows, which makes encrypted drive management extremely easy of use. Windows Explorer automatically recognizes the encrypted drives and folders, marking them for easier recognition by a user.

Hard disk encryption on Windows boot-up

ControlSphere starts its hard disk encryption service before the main Windows services, allowing encrypted drive usage by Windows services (such as Disk sharing service) and 3rd party services like databases, mail enterprise management systems.

File and Folder Encryption

ControlSphere uses a special technology called "Encrypted Archives" which was exclusively designed by our company. Encrypted Archive file is a file containing compressed and encrypted partition of dynamic size that grows or shrinks as archive files are added or removed to/from the archive.

The archive contents are protected by AES256 encryption key, similarly to encrypted drives of ControlSphere. ControlSphere also provides an ability to use a secure password instead of the encryption key to protect the archive.

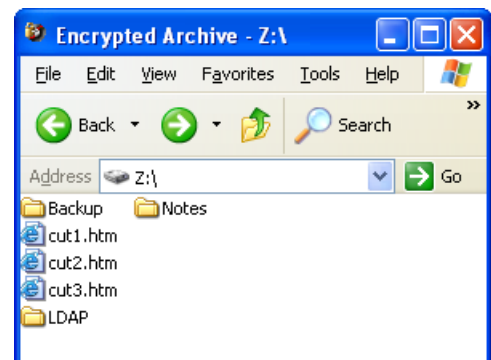
Encrypted Archives are mounted as ordinary drives (drive letters) and act exactly as they would be hard drives themselves. Once the archive is mounted as a drive, its contents (files and directory structures) are available for reading and modification operations for Windows programs just like ordinary files on a hard drive. This approach eliminates the need of copying them to an unsecured location before actual usage.

The file system support in Encrypted Archives is equivalent to traditional file systems, except that files are encrypted and compressed. Once the Encrypted Archive is mounted as a drive, ControlSphere displays corresponding status window describing the archive status. The status area of the window will display corresponding (animated) description every time archive files are being accessed, modified, deleted or the archive space is being compacted.



Similarly to encrypted drives, ControlSphere makes encrypted archive management as convenient as it can be. Windows Explorer recognizes encrypted space and correspondingly marks its folders as secure location.

Since the size of encrypted archives is related only to the amount of data stored, they are usually not taking much space on the computer hard drive or removable media. It is easy to exchange them over un-secure networks without the risk of data exposure or modification.



Encrypted archives are an ultimate help in different sort of data backups, including automated ones. ControlSphere also provides command-line support for encrypted archive maintenance operations, including automated backup procedures.

Password Management service

ControlSphere provides password storage and management service on secure devices (smartcards/tokens). In addition to that ControlSphere can also automate account and password entry to 3rd party Windows and WEB programs when requested.

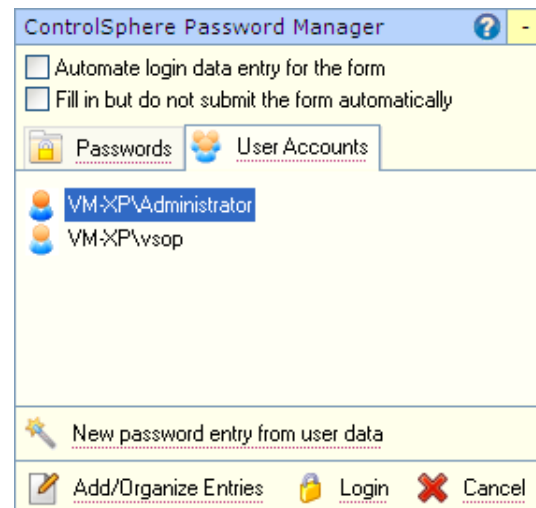
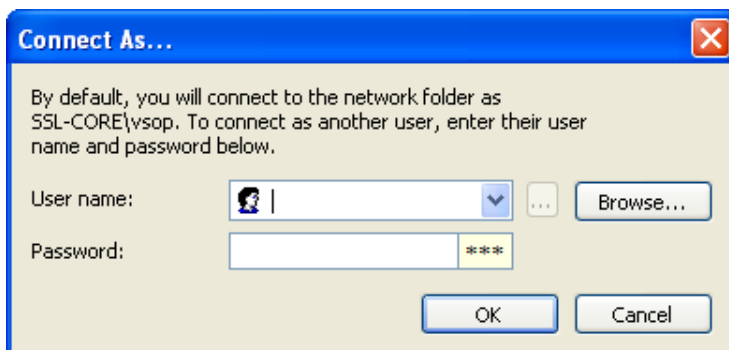
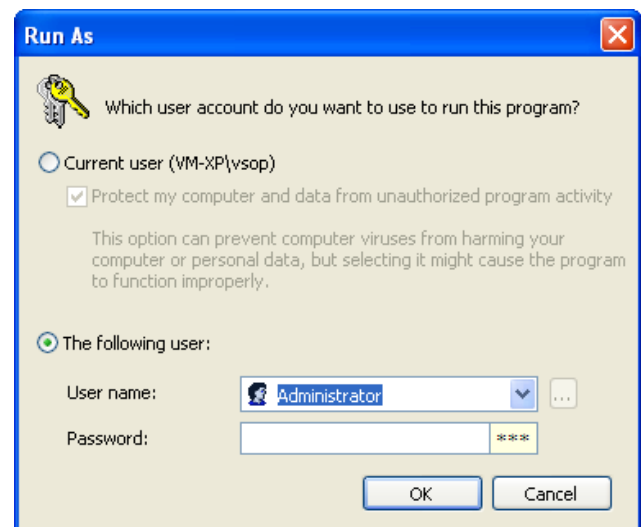
Thanks to heuristic approach, it can automate nearly all credentials/password retrieval actions Windows operating system and other third-party programs can fire. This eliminates the need of remembering user names, passwords and other authentication data. A token device can store all passwords (or password records to be precise) for its holder and pass this information to password-requesting applications in a secure manner.

This credential data is filled in directly into the authenticating application and neither mouse nor keyboard is used. Thus there is no chance for malicious "sniffer" programs (if there any are infecting the system) to capture the sensitive data.

Automating Windows authentication requests

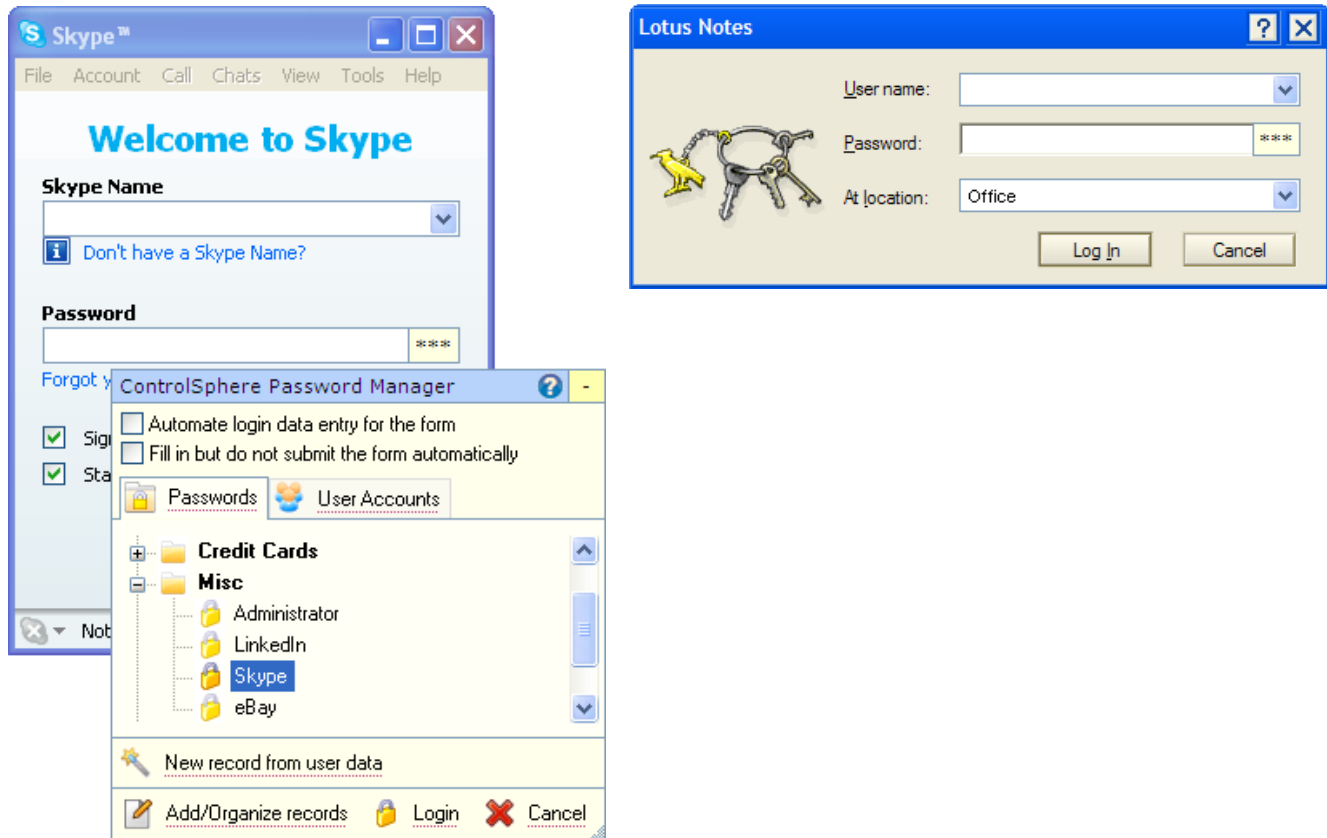
Besides the original Single-Sign-On (SSO) functionality ControlSphere provides further automation called SSO Automation feature. It provides convenient enhancements to standard Windows "Connect As", "Run As" and other credential authentication requests.

It allows the use of existing on-token Windows user accounts in those dialogs/requests and eliminates the need for manual user name/domain/password entries.



Password Automation for Windows programs

ControlSphere provides the ability to automate the account/password entry function for most Windows programs. Password automation allows you to perform a secure login with a password entry stored on a token and additionally create a Login Automation rule for the program. The automation rule will fill the requested user credentials automatically the next time it will require them.



Password Automation for WEB forms

ControlSphere provides the ability to automate login data entry in web-based (HTML) applications similarly to Windows programs.

The feature is available in Microsoft Internet Explorer as well as other Internet browsers which utilize MSIE engine and Mozilla Firefox. Google Chrome support is coming.

Token Management System (TMS)

The Token Management System of ControlSphere is a comprehensive set of tools and functions designed to help companies control the lifecycle of their secure devices (smartcards/tokens) fleet. In addition to that Token Management System (TMS) provides full control over secure data on the ControlSphere-enabled devices.

ControlSphere TMS consists of two general parts: TMS server which is as an ASP extension installed on IIS and a client, which is nothing else but the ControlSphere client program itself.

In general ControlSphere TMS provides the following features:

- ☑ TMS database holds centralized company-wide token, user and security group registry.
- ☑ TMS database holds complete ControlSphere token data contents, including device PINs.
- ☑ All changes on ControlSphere data made by a token holder on a client (ControlSphere program) are automatically replicated to the TMS database, including device PIN changes. The replication is done implicitly and securely.
- ☑ ControlSphere data on a user's tokens can be remotely and securely updated from server using the push technology (pending updates) of TMS. The updates are made implicitly to a user.
- ☑ TMS database maintains token data update history automatically. Token can be restored to its backed-up state remotely using the push technology of TMS.
- ☑ It is possible to distribute ControlSphere data objects (such as encryption keys, password entries, configuration items, etc.) to a group of users/tokens using the push technology of TMS.
- ☑ TMS database can be used to update ControlSphere license information and other configuration items on a token remotely.
- ☑ TMS can be used to remotely reset locked User PIN.
- ☑ TMS can ensure that contents of a lost or stolen token will be remotely wiped should someone try to use it.

Additional features of ControlSphere

ControlSphere provides extra functionality in addition to the main services:

- ☑ Additional token security policies; device PIN entry, change and control policy; extra protection against PIN capture by 3rd party programs.
- ☑ Complete protection over the temporary user session files by redirecting temporary file storage paths (TEMP, TMP and Temporary Internet Files folders) to an encrypted User Home Drive.
- ☑ Additional token holder identification mechanism via public data entries on a token (name, description and holder photo). These publicly accessible data can be retrieved from the device without the need of providing user PIN.
- ☑ Full or partial ControlSphere data backup to another device or encrypted (password-protected) Token Image file; full or partial data restore functionality.
- ☑ In addition to manual token data backup functionality ControlSphere provides fully-automated implicit token data backup function.
- ☑ Besides the data restoration itself, ControlSphere provides an ability of a direct data usage right from the Token Image files as they would be physical hardware devices. This approach simplifies the recovery process should the token be lost, stolen or forgotten at home.