

# ControlSphere

CONVENIENCE AND SECURITY

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.

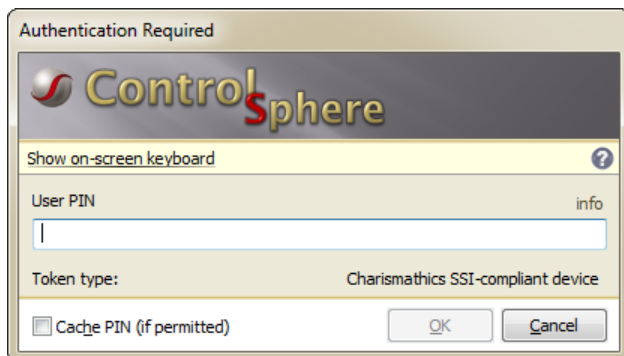
## Smartcard-based Windows and Network Logon

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



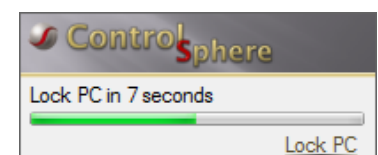
A smartcard (or reader-less USB security smartcard *token* device) can hold a number of Windows user accounts which can be used to log on to Windows or Active Directory services on single or multiple computers. At the same time standard Windows authentication means can be enabled or disabled depending on security requirements.

ControlSphere allows users to even disregard their passwords 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) for the smartcard/token device to logon to Windows and Network.



Once a correct PIN is acquired, ControlSphere asks the user to login using one of the Windows user account records stored on the device. Same approach is used to unlock a computer.

ControlSphere displays optional notification message should the device be disconnected from a port reader and finally performs a pre-configured action (e.g. lock PC).



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 unknown to users
- ☑ Possibility to store and use multiple Windows account credentials on same smartcard/USB token
- ☑ Enable seamless authentication to different user accounts or Active Directory services on single or multiple computers with the same smartcard/token
- ☑ Automatic usage of randomly generated passwords unknown to a user
- ☑ Automatic Windows password lifecycle support
- ☑ No need to acquire security certificates or install Certificate server as well as other 3<sup>rd</sup> 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 and session data protection
- ☑ Tight integration with other services of ControlSphere is provided. No need in secondary authentication for hard disk encryption or password management (SSO) functionality.

## Hard disk and file/folder encryption

ControlSphere uses highly secure AES256 encryption algorithm, approved for use by a number of worldwide authorities. Furthermore it can stack multiple encryption keys in a single "super-key" (up to 8x256 bit) for unbeatable encryption strength.

There can be a number of named encryption keys stored on a single device/token, providing any level of granularity on data access control. Keys can be shared between multiple users, allowing secure data exchange and information sharing.

The encryption keys can be exported to other secure device or backed up to a Token Image - an encrypted token data clone stored in a password-protected file. The keys can also be centrally distributed and maintained by an enterprise security management team. The keys are used in hard disk and file encryption services.

## Hard disk encryption

The disk encryption service of ControlSphere protects sensitive information from unauthorized access, copying, modifying, and theft on personal computers and removable media devices. By leveraging encrypted virtual drive approach ControlSphere can encrypt sensitive data on a local hard drive, removable or network location. Furthermore it can fully secure user profile (Desktop, Favorites, usage history, etc.) and temporary data by automatically redirecting these folders to an encrypted location. Storing encrypted user profiles on a network allows true employee portability and roaming desktop feature on all company computers.

The encrypted containers are visible to a user as ordinary hard drives, allowing transparent access to the sensitive information. The data is transparently decrypted when it is read from the disk or network and encrypted before it is written.

A valid encryption key 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 - an encrypted password-protected file containing cloned ControlSphere token data.

The protected information cannot be viewed or copied by other users not having an access to the encryption key.

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 as "secure" for easier recognition by a user.

Users are given a possibility to mount and dismount their encrypted volumes manually or automatically, e.g. mount upon token-based logon to Windows or dismount upon device disconnection event.

Command-line support is available for convenient encrypted volume management operations.

## **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 3<sup>rd</sup> party services like databases and e-mail enterprise management systems (such as Exchange server).

## **File and Folder Encryption**

ControlSphere uses a special technology called "Encrypted Archives" – encrypted virtual drives behave exactly as physical ones. The file system itself is stored in a compressed and encrypted container file which grows or shrinks as 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 data.

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.

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.

Encrypted archives are usually not occupying much space on computer's hard drive or removable media since their size is related to the amount of data stored only. 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 as well provides command-line support for encrypted archive maintenance operations, including automated backup procedures.

## Password Management / Single-Sign-On

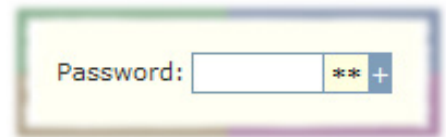
ControlSphere provides password storage and management service on secure devices (smartcards/tokens). In addition to that it can also automate account and password entry to all standard Windows, 3<sup>rd</sup> party and WEB programs when it is requested.

Thanks to heuristic approach, it can automate nearly all credentials/password retrieval actions Windows operating system and other third-party programs can request. This eliminates the need of remembering user names, passwords and other authentication data and thus provides a possibility to make passwords long and truly unbreakable.

A token device can store all password records for its holder and pass this information to password-requesting applications automatically, in a secure manner. This secure data is filled directly into the authenticating application and neither mouse nor keyboard is used.

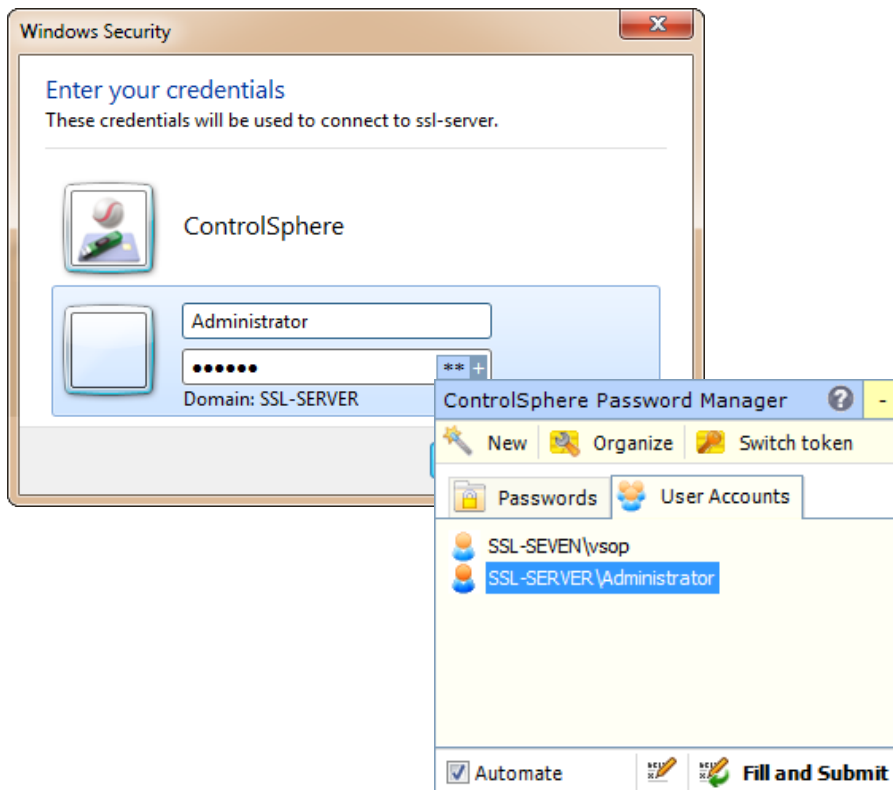
Thus there is no chance for malicious "sniffer" programs (if there any are infecting the system) to capture the sensitive data.

We believe that the password management of ControlSphere is one of the most convenient SSO solutions available, as it visually extends password fields with the automation and interaction area.



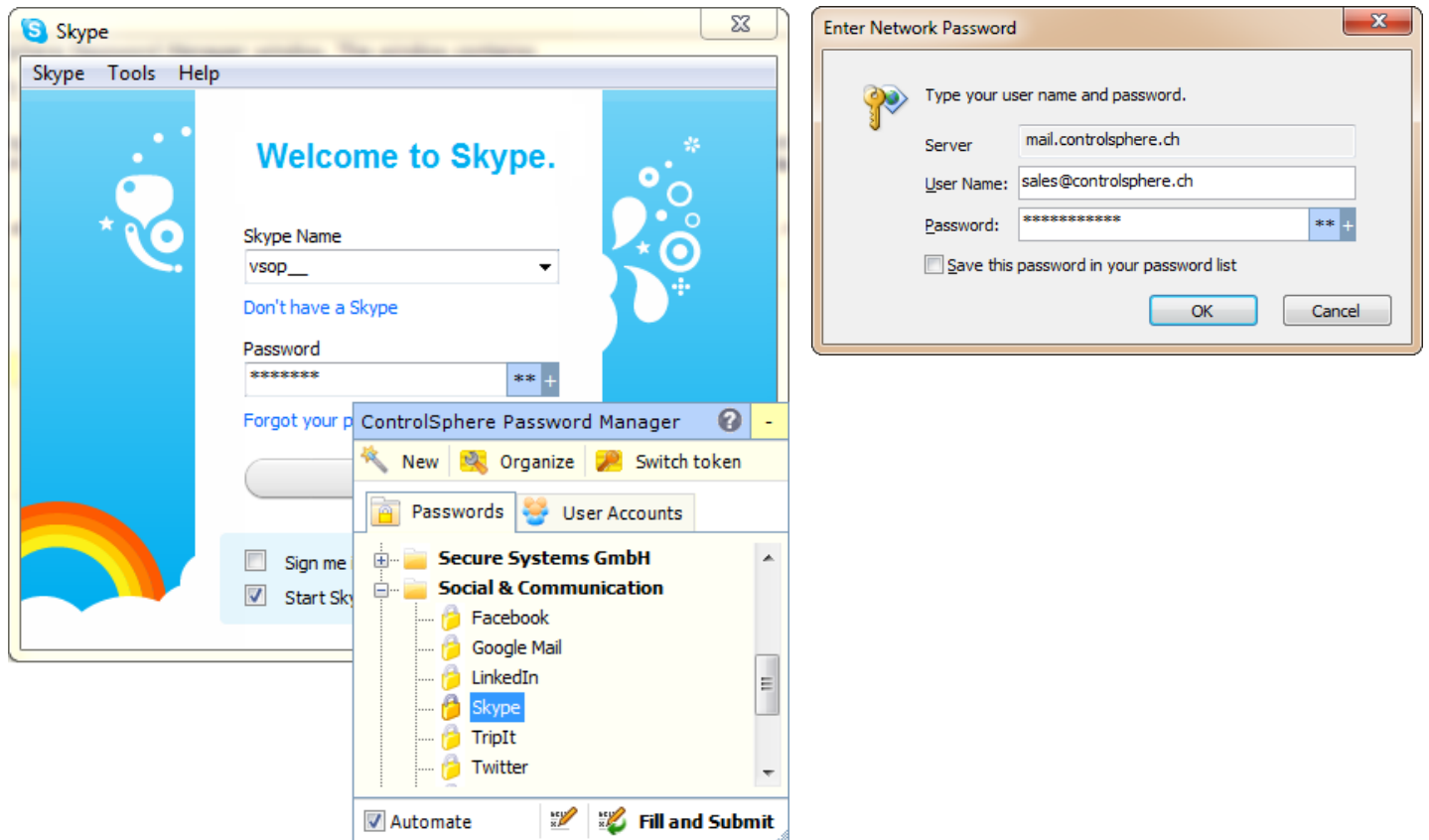
## Automating Windows authentication requests

ControlSphere provides convenient enhancements to standard Windows authentication requests: "Connect As", "Run As", elevation prompt and practically all others.



## Password Automation for Windows programs

ControlSphere provides the ability to automate the account/password entry function for nearly all Windows programs. Password automation allows performing a secure login with a password record stored on a token and optionally to create a Login Automation rule for the request. The automation rule ensures that the requested user credentials are automatically pre-filled and optionally the login action automated the next time the same authentication request reappear.



## 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, Mozilla Firefox and Google Chrome. Support for other browsers is coming.

## Token Management System (TMS)

The Token Management System of ControlSphere is a comprehensive set of tools and functions designed to help companies to 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 software (installed on Microsoft IIS server) and a client software: the ControlSphere client program itself.

The most noticeable features of ControlSphere TMS are:

- ☑ 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

In addition to the main services ControlSphere provides extra security features like:

- ☑ Additional token security policies; device PIN entry, change and control policy; extra protection against PIN capture by malicious programs and “sniffers”.
- ☑ Additional token holder identification mechanism via public data records 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.
- ☑ ControlSphere provides fully-automated implicit token data backup function in addition to manual token data backup functionality.
- ☑ 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.