



Clavister SMS One-Time Password Service

Service Data Sheet

- Supports Clavister Secure Access Gateway
- Multi-Factor Authentication
- Easy-to-use and cost-effective
- World-wide support for more than 200 operators

Clavister SMS One-Time Password Service

Clavister Secure Access Gateway enables organizations to rapidly deploy a powerful and cost-effective solution for secure remote access. Users can access network resources, including corporate data resources, applications and files residing on file shares, using any standard Web browser. In order to access a resource, the user must first authenticate them. It is possible to set up different authentication method for different types of resource. One of the more secure authentication methods is Multi-Factor Authentication (MFA). This is sometimes referred to as strong authentication or two-factor authentication.

Multi-Factor Authentication (MFA)

Clavister Secure Access Gateway offers a multitude of different authentication methods, ranging from single factor authentication methods, such as username/password, Web-based token, to multi-factor authentication methods, such as the use of SMS token with one-time passwords.

The purpose of a one-time password (OTP) is to make it more difficult to gain unauthorized access to restricted resources. Traditionally static passwords can more easily be accessed by an unauthorized intruder given enough attempts and time. By constantly altering the password, as it is done with a one-time password, this risk can be greatly reduced.

Multi-factor authentication combines two or more factors to make it harder to illegally obtain a user's credentials. One factor is something that the user has, for example a mobile phone and something that the user knows, for example a pass phrase. By requiring both these factors when users are asked to authenticate themselves, a high level of security is achieved.

Clavister SMS One-Time Password Service

To expedite the use of SMS-based one-time passwords, Clavister is introducing the Clavister SMS One-Time Password Service. This new online service will make it easier than ever to roll out an organization-wide multi-factor authentication solution using Clavister Secure Access Gateway. This service comes pre-installed on all Clavister Secure Access Gateways which means that your organization can start using Multi-Factor Authentication instantly.

The one-time password is generated by the Clavister Secure Access Gateway and distributed by Clavister Service Provisioning Network (CSPN) to the user's mobile phone as a flash SMS. The one-time password expires once it has been used or its scheduled lifecycle has expired.

Quality of Service

The Clavister SMS One-Time Password Service offers a number of advantages over standard SMS delivery. Clavister can offer connectivity to more than 200 operators around the world and 99.5% of all SMS are delivered within seconds. Since one-time passwords are time-restricted, a timely delivery is of the essence.

Getting Started with Clavister SMS One-Time Password Service

Before you can start to use SMS tokens with your Clavister Secure Access Gateway installation, you need to purchase pre-paid tokens. This process is simple and straightforward.

1. Log on to the Clavister Client Web site and select your registered Clavister Secure Access Gateway license.
2. Select Products and Services in the Web Shop section.
3. Select the amount of SMS credits that you want to purchase.
4. Enter your credit card information and select Pay.
5. Your SMS credits are immediately activated in the Clavister Service Provisioning Network (CSPN).

You are now ready to use the Clavister SMS One-Time Password Service with your Clavister Secure Gateway.

How It Works

A typical scenario is where the user requests access to a resource protected with the SMS token authentication method. The user enters their username and password and a one-time password is generated. The newly generated one-time password is then distributed through the Clavister Service Provisioning Network (CSPN) to the user's mobile phone as a flash SMS. The user can then enter the one-time password when prompted. The whole procedure is fast, trouble-free and reliable.

