Supremo Security Statement

Summary

1. Target Audience

The purpose of this document is to provide detailed information about the security standards of Supremo. The target audience are professional network administrators and IT specialists that have to deal with security concerns of their customers. This document describes all the technical features of Supremo about security with the aim to erase any doubts before reselling and distributing our software.

This Security Statement can also be sent to customers who fear they are not protected enough when connecting remotely via Supremo or who simply desire to know more about the technical aspects of security of our software.

2. Who We Are

For over 30 years, Nanosystems has provided IT consulting services, technical assistance and system integration to help your business grow and improve with powerful, versatile software created by our young development team.

Nowadays the core business is the development of 3 main products: Supremo, Uranium Backup, Supremo Console

Supremo, distributed in 150 countries around the world, is one of the most reliable high performing remote control software on the market. Its mobile version, Supremo Remote Desktop, is available for Android and iOS.

Uranium Backup, with active users in more than 110 countries, is a complete, versatile and valuable backup solution.

In July 2016, Nanosystems created the IT Management Console, which allows users to monitor and manage Uranium Backup clients and simultaneously synchronize, manage, and control Supremo contacts.

3. About Security

Supremo is an easy-to-use and powerful remote desktop solution. In terms of technical assistance or remote working, tools like Supremo are now getting more and more useful to carry out one's work.
Supremo allows an user to remotely control a PC/server without the need to be physically in front of the machine and, if properly configured, to gain administrator rights on that computer/server.

It goes without saying that users are fearful about security aspects and want to be protected against potential Internet attacks in many ways.

The topic of security plays an extremely important role and our company mission is to provide safe software which customers can trust.
A secure remote desktop tool ensures great satisfaction to our users and a long-term success of our product.

4. Encryption Technical Details

The data traffic of Supremo has a double encryption.
The first one by TLS_ECDHE_RSA with AES_256_GCM SHA384, 256 bit keys TLS 1.2 .
Supremo Traffic body is also secured using RSA public/private key exchange and AES (128 bit) session encryption.
There is no way to decipher the traffic by both interconnected computers and Supremo gateways.

5. No Stealth Mode

It is not possible to run Supremo in stealth mode: this means that Supremo is not developed to be launched completely in the background even if installed as a service for unattended access.

Users are always aware when Supremo is running and they can check active remote connections (both incoming and outcoming) at any moment.

First of all, if Supremo is active, users can see its logo icon on the tray bar of their machine. Clicking on it it is possible to open the Session Manager and to check whether a remote connection is operating (the Supremo ID of the remote machine is shown).
Users can disconnect a remote incoming or outgoing session with just a few clicks.

When a user connects remotely to a PC, the PC owner will always get a pop-up alert which warns him/her that an incoming remote connection through Supremo is established.
Please remember that it is possible to gain access to a remote machine only if credentials are known and the password assigned by Supremo is variable.

Supremo generates logs for each incoming and outgoing connection so that each user can check data about connections in real time (for further details please see below).

6. Brute-Force Protection

A brute-force attack is an attempt to decode encrypted data such as passwords, using a trial and error method and hoping, eventually, to guess them correctly. This activity involves repetitive successive attempts of trying various password combinations to break into an account.

A brute-force attack is the simplest method to gain access to a site or an account (or anything that is password protected): usually, every common ID has a password.

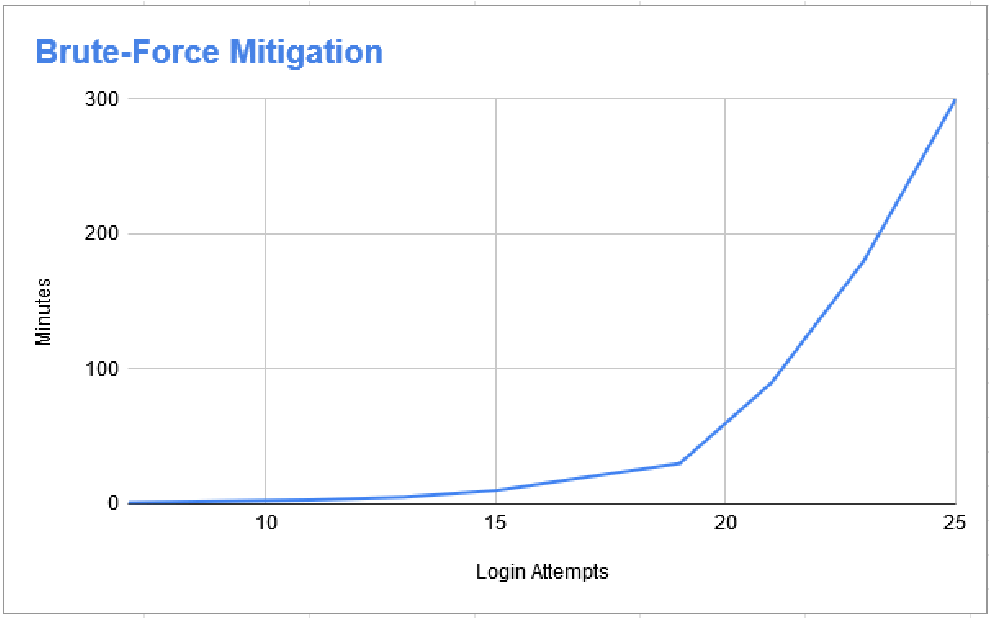
This is an old attack method, but it's still effective and popular with hackers that try to crack passwords proceeding through all possible combinations of characters in sequence until they find the correct input. They often use automated tools.

As a defence against brute-force attacks, Supremo take some preventative measures:

- Password Length and Complexity: Obviously, the longer the password, the more time it will take to find the correct input. Longer passwords increase the number of combinations of characters available and consequently the difficulty in getting the right one. It is possible to enable the 10-character secure random password in the section *Tools – Security.* Supremo passwords will be generated with alphanumeric characters and not only with numeric numbers in order to grow the number of possible combinations.

- Restricted Login Attempts: Limits in login attempts exponentially increases the latency between connection attempts. A wrong password input will lock out a user for a specified amount of time; the more attempts fail the more this time increases before a new password can be entered again.

  The latency time is only reset after successfully entering the correct password.



7. Anti-DDoS Protection

A DDoS attack is a cyberattack that aims to overwhelm a target website with fake traffic: a huge amount of fake requests are sent simultaneously from a multitude of sources around the globe, all targeting one system or network. The intensity of requests make your system unstable or even completely unavailable.
So DDoS assaults don't try to breach the security perimeter but it attempts to make your website and servers unavailable to legitimate users.
Our Provider services include protection against every type of DDoS attack.

8. Infrastructure

Nanosystems pays much attention to customer data and makes use of an infrastructure with the best service quality which is located in data centers compliant with ISO/IEC **27001:2013**, **27017:2015**, **27018:2019**, **27701:2019**, **22301:2019**, **9001:2015**, and **CSA STAR CCM v4.0**.
Nanosystems carefully searches its providers and selects only those who ensure high levels of trust and standards.
All Supremo services are running on servers located in strictly monitored data centers, fenced with barbed wire and video surveillance (motion detection systems are in continuous operation). Surveillance teams work on site **24/7/365**.
The data centres have a high level of security and only authorized personnel can gain entry.
There are strict security procedures to be authorized to access servers rooms such as:

- Monitoring of each staff members access to the data centers
- RFID name badges that allow and restrict access to employees
- Security doors that open only after a RFID name badge verification
- regularly reassessment of staff members rights

9. Password Management

Supremo generates random passwords that change at each restart of the software or of the machine. It allows you to define the random password complex up to 10 characters, furthermore you can disable the random password definitively.
A remote connection is possible only if you know the Supremo ID and the momentaneous valid password of the remote PC; otherwise there is no way to control another machine.
Customers can change their password when they want just relaunching Supremo and you can connect to their devices only if you are invited to do so.
When installing Supremo as a service for unattended remote access (e. g. servers or in the case of smart working), it is possible to configure more than one personal and fixed password, only managed by the user itself.
Supremo supports 2-Factor Authentication for login to the Contacts Address Book.

10. Code Signing

All our software is digitally signed via Digicert Code Signing. A Code Signing Certificate allows end-users to verify that the code they receive has not been altered or compromised by a third party.
Digicert Code Signing is an important additional security feature that guarantees the authenticity of our software. The digital signature automatically becomes invalid if the software is compromised or modified.

11. Supremo Console Account

Supremo Console accounts are hosted on dedicated Supremo servers.
For information on access control, please refer to Infrastructure.

12. Incoming and Outgoing connections monitoring

Security of the tool Supremo is also guaranteed by some features that allow you and your customers to monitor and control any incoming and outgoing connections.You can individually configure some connection settings of Supremo:

- Session Manager: as already said in the "No Stealth Mode" paragraph, Supremo has a Session Manager where users can check whether a remote connection is operating (the Supremo ID of the remote machine is shown). Users can disconnect a remote connection (independently if it's an incoming or an outgoing session) with just a few clicks.
- Connection logs: Supremo creates folders where the connection logs are stored in real time. You can check data about each incoming and outgoing connection at any moment.
- External Connections Authorization: it is possible to set automatic controls on incoming connections on your PC. Enabling the option "Ask authorization", you will receive a connection request from a remote user and you have to grant him/her access to your PC by clicking on a specific pop-up alert (otherwise remote connection is automatically blocked).
- Whitelist Feature Access Control: you can manage a personal "allowed IDs" list of remote Supremo users. This means that only the Supremo IDs saved in that list can gain access to your PC.
  If a computer is configured for unattended remote access (i.e. installation of Supremo as a Windows service), the Whitelist feature is a relevant additional security option to restrict access to this computer to a number of specific remote Supremo clients.
- Password settings: you can set a personal password to the configuration made to your Supremo. Nobody can access your settings panel and nobody can change configurations like allowed IDs, Ask authorizations, etc etc.

13. Security Testing

Supremo infrastructure is subject to security testing on a regular basis.

Infrastructure testing is a penetration test or vulnerability assessment of computer systems, network devices or IP address ranges to identify vulnerabilities that could be exploited. Testing on our infrastructure is performed by independent companies, specialized in security testing. If any vulnerability is identified they immediately report it to us providing recommendations about how to strengthen the infrastructure security. Penetration tests allow us to find vulnerabilities, avoid damages from a security breach and assure our customers and suppliers that their data is secure and their remote connections safe.