

NSN Connect: Security

Introduction

NSN Connect allows its users to remotely access, with maximum security, your irrigation computer that's connected to the Internet in any part of the world. This document describes the principal security measures implemented in the product in order to guarantee the privacy of sensitive data.

Physical Security

Toro NSN guarantees that the servers that host NSN Connect are located in data centers with:

- Environmental security
- Electrical security
- Physical security
- Architectural security

Storage Areas

The storage areas of the data warehouses typically have the following physical characteristics:

- Technical Floor
- Fire Protection
- Racks (Type and Capacity)
- Network Cabling

Incident Management

A monitoring system is automatically feeding information into the Incident Management System using:

- Incident Resolution and Escalation
- Incident Detection

System Backup

To protect its customers and to ensure a rapid recovery in the event of a system failure, Toro NSN regularly backs up its systems and all of its customers' valuable data.

System Architecture

The system architecture of NSN Connect has the following features:

- Flexible bandwidth which expands when reaching 50% of its load.
- Frontal security structure based on redundant firewalls, Failover configured (active-active) to ensure availability without interruptions even in case of a device failure or malfunction.
- Switches and server network-cards, redundant both at the front- and back-ends.
- Cluster-balanced IIS servers to ensure the optimum load-level in each server.
- Redundant remote-control servers, geographically-distributed to ensure the best response time in deployed sessions.
- Replicated database-server and application-servers.

Product

Software Certification

NSN Connect is certified by Thawte. The Thawte certificate guarantees to users that they are using an original copy of NSN Connect – a copy supplied by Toro NSN. Toro NSN guarantees that the software is free of all viruses.

All NSN Connect websites on all connected platforms have their identity verified by SSL certificates provided by companies such as VeriSign or Thawte.

All installers, other executable files and ActiveX controls are certified by VeriSign on all of the platforms connected by NSN Connect.

Secure Connections

NSN Connect uses standard ports to establish connections.

The operator only needs an Internet connection and a browser to connect to NSN Connect.

The design of NSN Connect guarantees that the connection will be made in seconds even when both sides are using NAT or Firewall.

Data Encryption

All of the algorithms used by NSN Connect have been validated by the official tests provided by the creators/owners of that algorithm. All communication passes through the NSN Connect server.

Encrypted Storage

Confidential or sensitive data stored in the database are always encrypted.

NSN Connect uses 2 levels of encryption. The level used depends on whether the data sent or stored compose a message, password or email address.

- Other features, such as, the remote control, file transfer and the 'desktop share mode', always use 256-bit AES encryption.
- Use of SSL is compulsory.

Secure Sessions

NSN Connect uses secure sessions that have been developed in accordance with the recommendations of the OWASP Guide. The session identifiers are non-predictable. Sessions are managed through tokens (sequences of numbers) that give one-time-only access to each requested page. This means that once the owner of the session has viewed a page, nobody else will be able to access it even if they have discovered a session identifier.

Blocking User Access to NSN Connect

Blocking IP Addresses:

NSN Connect offers a sophisticated system for blocking access from specific IP addresses for variable periods of time. This means that as more attacks are received from a given IP address, the address will be blocked for longer.

Blocking User Accounts.

NSN Connect allows the blocking of 'nuisance' users (those with whom they do not wish to communicate).

User-account blocking provides a defense against brute-force attacks and identity theft as user logins are automatically blocked for fifteen minutes after three successive failed logon-attempts.

Attack Detection

Thanks to its sophisticated systems of data validation and attack-pattern detection, the NSN Connect backend can detect attacks against its systems and block each attack in a way appropriate to the type of attack and its frequency.

At the application level the company detects the following types of attack:

- SQL injection
- Cross-site scripting (XSS)
- Buffer overflow
- Hijacking
- Flooding

The strictest type of block is a permanent block, which can only be unblocked by the Toro NSN administrator.

SSL

SSL is a cryptographic protocol that provides a secure connection across the Internet. This enables the client and server applications to communicate in a way that prevents eavesdropping, tampering and message forgery.



NSN Connect users always use a secure (SSL) connection when logging in to NSN Connect. All communications use the SSL protocol in order to provide confidentiality and integrity.

Security Processes

To improve security, NSN Connect prevents the reloading of a webpage and any attempt to do so will produce a security error. For this reason, the 'F5' key and the 'Refresh' browser option are disabled.

Security of NSN Connect tools

Block Remote Computer

Block the remote computer's screen, mouse and keyboard during remote control.

KeyCard Security

Require the user to enter a code from a keycard before performing certain restricted actions.

Computer Password Protection

Require the user to enter a password in order to connect to the remote computer. If no password is entered a default one is generated.

Remote control Invitations

Grant other users temporary permission to remotely control to one of your computers by sending them an invitation that expires within a maximum of 24 hours.

Conclusion

NSN Connect has implemented numerous security measures to protect its users against unauthorized access to their data and systems.