Stratus ActiveService Network: Secure online services delivery

All the benefits of remote 24/7/365 monitoring and management for Stratus systems—with none of the risks

Stratus' ActiveService™ Network provides secure 24/7/365 monitoring and troubleshooting of hardware and software issues—no matter where in the world your Stratus systems are located.

Secure online support environment

Stratus systems, like ftServer, V Series, ztC Edge, and everRun-based solutions, come equipped with something no other vendor offers—Stratus' ActiveService Network (ASN), a secure, private communications channel that delivers 24/7/365 online monitoring and management services.

If you're like most businesses today, security is at the forefront of your concerns. As a Stratus customer, you need not worry. The ASN includes a comprehensive set of built-in features and controls that address data, online connectivity, and human security issues. And, all of these technologies are backed by nearly 40 years of expertise in online services delivery to critical application environments.

The ASN is an encrypted, IP-based worldwide network that enables instantaneous around-the-clock monitoring and troubleshooting and prompt resolution of system incidents. Combining real-time alerts with our Atlas knowledgebase and follow-the-sun technical support services, the ASN ensures your critical servers are up and running all the time.

Key benefits

- **Proactive communications:**
  - Communicates alerts to the Stratus® Atlas database for rapid problem resolution
  - Enables automatic parts replacement
  - Provides notification for known bug avoidance
  - Sends a heartbeat signal to Stratus to ensure around-the-clock communications with Stratus' support infrastructure
- **Real time and over time trending**
  - Data sent to the Atlas knowledgebase over the ASN is used to spot trends in real time, analyze the root cause of issues, and proactively alert you to problems before they affect your business
- **Secure link to on-demand support**
  - Built-in ASN security features and controls protect your systems, data and ASN transactions from unauthorized access
  - Outgoing "call-home" alerts only connect to Stratus and contain no user data. Only Stratus can determine the source of the call or location of the server

Stratus ActiveService™ Network— your secure link to 24/7/365 on-demand services

ActiveService Security Features	
Data Security	
User data	No user data or authentication information (e.g. password) is included in ASN communications
Alert data	Secure web connections via HTTPS using transport layer security (TLS) protocols
Network security	Multi-factor ASN authentication using unique system Site ID
Stratus data center access	Physically secure data center locations protected by extensive firewalls
Stratus database access	Secure Atlas knowledgebase
IP addresses	IP filtering via proxy server in DMZ
Connection Security	
Network access	System management module (SMM) and LAN can be on separate subnets
Heartbeat signals	Stratus recommends configuring systems to generate periodic heartbeat signals over the ActiveService Network to confirm that a good connection exists with the server
Call-home messages generated by error events or threshold triggers	There are multiple ways to communicate server-generated, call-home messages to Stratus customer assistance centers based on your specific security needs: • Encrypted Internet call-home capabilities • Proxy server or modem call-home capabilities if Internet access is prohibited
Authentication control	Multi-factor authentication (MFA)
Credential authentication	Public certificate authority
External connection initiation	Not allowed, all connections are initiated by Stratus systems
Access Security	
Connection logging	Can view comprehensive system connection logs at any time via the ActiveService Manager (ASM) web portal
Authentication control	Limited access with five levels of approval
Remote control access	Access only from secure ASN connection servers inside Stratus premises
Access control	Comprehensive employee background checks
Unique security policy	Can add additional site restrictions based on your specific security policies
Authorization groups	Access is limited to designated connection groups

Call-home message categories

- Diagnostic messages
- Hardware configuration
- Software revisions
- Current system status (duplex or simplex)
- Software revisions
- Log entries

Learn more about Stratus' 24/7/365 ActiveService Network

For more information contact your authorized Stratus representative, or visit **www.stratus.com**.

Stratus

www.stratus.com