

# Features and Benefits

## Dominion<sup>®</sup> SX



Features	Benefits
<b>Flexibility</b>	
<i>Wide variety of supported models</i>	Models available in 4-48 ports. Offering the highest port density (48-ports) in the market in a 1U rack unit. Variety of power options, including dual-feed, load-sharing power supplies with zero failover time. AC and DC power models. Choice of one or two 10/100 Base-T Ethernet ports with intelligent automatic failover. Models are available with or without built-in modem, and with one or two “at the rack” serial ports for local access.
<i>Increased Memory on 8-, 16-, 32- &amp; 48-port models</i>	Port buffer has been increased to 256KB which provides expanded logging of 80 pages of local events and alerts. Users now have expanded event logging and storage.
<i>1U Form Factor</i>	Small form-factor saves rack and/or closet space and makes it perfect for remote offices where space is limited. Rack-mount brackets included for all DSX16-48 port models; optional on all DSX4 and DSX8 port models, except the DSXA-8 dual-power which comes with a rack-mount kit.
<i>International Language Support</i>	The Raritan Serial Console can support four languages: English, Japanese, Korean and Chinese
<b>Reliability</b>	
<i>Intelligent Auto-Failover on Dual-LAN models</i>	On all dual-LAN models, the administrator can enable failover to the second LAN port. One or two IP addresses may be used. Either LAN connection can be used as the access port to the Dominion SX.
<i>Cross-platform and Hardware Independent</i>	Allows the connection of multiple disparate servers running SUN <sup>®</sup> Solaris <sup>™</sup> , HP-UX, AIX, Linux <sup>®</sup> , Windows <sup>®</sup> Server 2003, and UNIX <sup>®</sup> -based servers as well as multiple serial devices to a single Dominion SX – making it perfect for situations where a range of equipment is needed, which is common in remote locations.

# Features and Benefits

Features	Benefits
<i>AC and DC Power Options</i>	<p>Integrated power supply ensures proper power provision and system reliability.</p> <ul style="list-style-type: none"> <li>• AC Power: 100-240VAC auto-switching available on all port models</li> <li>• Auto-Switching DC Power: -36-72V DC, available in 32 and 48 port models</li> </ul>
<i>No moving parts – higher reliability</i>	No fans or other moving parts to fail means higher reliability. Cooler running units mean lower heat dissipation and lower power consumption.
<i>Integrated 56K Modem via RJ11 connection available*</i>	Provides emergency access in the event of a network outage. This capability enables an administrator to access server and network equipment for trouble shooting/disaster recovery. Integrated modem provides a very clean installation and removes the need for an external modem/cabling and power or a separate remote access server, flimsy PCMCIA slot modem cards, local authentication software, and thus minimizing the potential points of failure.
<b>Security</b>	
<i>Fully featured firewall</i>	User selectable and customizable system security levels catering to wide range of user needs for security. Enhancements to the firewall – added pre- and post-routing and Static NAT (SNAT) support.
<i>Man In The Middle (MITM) attack mitigation</i>	Enhanced security of communication channels by using client and server SSL certificates.
<i>Selective Static Routing Support</i>	Supports connections between modem and LAN 1, modem and LAN 2 or LAN 1 and LAN 2. This allows users to utilize two different network (Public and Private) and modem access to KVM or Ethernet controlled devices. When used with the firewall function, secure access will be enabled.
<i>TCP Port Addressing for Telnet and SSHv2</i>	<p>Direct Port Addressing can function with TCP port addressing for both Telnet and SSH. Independent IP addresses or TCP port numbers can be assigned to each port for Direct Port Access.</p> <p>Com Port Redirection can be supported for third-party software redirectors.</p>
<i>Local User Groups</i>	Allows flexibility of assigning user permission per SX with the use of local groups. Now the Authentication server can send back the group after it authenticates and permissions can be determined locally.
<i>Flexible strong password support</i>	Offers user-selectable password parameters to satisfy a wide range of password security levels.
<i>Customizable login &amp; consent banner</i>	Improved security with audit option during identification and authorization.
<i>Rejecting access attempts using SSHv1</i>	Due to the many known security vulnerabilities of the SSHv1 protocol, the Dominion SX will automatically reject SSHv1 connections.

# Features and Benefits

Features	Benefits
<i>Enhanced Encryption Options</i>	Support more encryption options: web-browser security through 128-bit SSL and RC4 encryption; for SSHv2 connections, AES and 3DES are supported (client-dependent).
<i>Authentication and Authorization Support - Kerberos</i>	Support provided for the RADIUS, LDAP, TACACS+, Kerberos V.5 and Active Directory®; Primary and secondary servers are supported.
<i>Login Name and Password never stored in clear text</i>	Sensitive information is MD5 hashed for storage on the unit.
<i>User Defined and Installable Security Certificates</i>	Dominion SX includes user authentication security and user-defined and installable security certificates. Use with Active Directory and LDAPS for secure communication. Both client and server certificates are supported.
<i>SecureID Support</i>	SecureID is supported via RADIUS for added security.
<i>Target server disconnection option</i>	Once a user is timed out for inactivity, a user defined logoff command is sent to the target. Improved security of user sessions results as the next user that connects to the port will need to login to the target with their own credentials. Some users may know this capability as an exit macro.
<i>Modem dial-back Security</i>	For enhanced security, Dominion SX supports modem dial-back with Linux®, and Windows 2000/XP clients.
<i>Disabling Authentication and Authorization</i>	This option saves user time when accessing SX in data center where security is provided through other means. User does not need to type in user name and password.
<i>Disable Local Authentication Option</i>	This option allows for enhanced security where required by security policy, ensuring that a single directory service is used for all users.
<b>End User Experience</b>	
<i>HTML Implementation</i>	Reduces the time to load the Java applet in a browser implementation to less than one minute.
<i>Full Modern CLI – GUI Equivalence</i>	Improved usability, with command completion and history. CLI admin has the same functionality as the GUI, thereby allowing scripting of any command.
<i>Broad Range of Supported Browsers</i>	Offers broad range of browsers – Mozilla Firefox, Internet Explorer 6.0+; ensuring compatibility with the wide variety of operating systems and devices.
<i>Single Appliance – Higher Security and No Additional Software Required</i>	Appliance model offer enhanced security with no user access to underlying Linux OS of the console server. Provides true 'Plug and Play' capability making installation and set-up quick and easy. No additional client/host software or hardware to buy and no special networking equipment or design is necessary. When using a Java-enabled web-browser, there is no need for expensive SSH client software, and it reduces the need to manage additional client software.

# Features and Benefits

Features	Benefits
<b>Manageability</b>	
<i>Easy to Install</i>	Installation in less than 3 minutes, with just a web browser or a VT100 terminal (or equivalent). Some competitive products require burdensome editing of multiple files to complete a basic installation.
<i>IPMI support</i>	Improved system performance monitoring and management. Allows for discovery and management of IPMI enabled servers.
<i>Port Keyword Monitor and Alert</i>	Also sometimes called “port triggers”. Users can define up to 14 keywords per port with up to 40 characters each. The SX will scan the data coming from the port and if a keyword is encountered, it will send alerts via SNMP or e-mail to predefined addresses. This allows monitoring and alerting of problems with the targets even when the user is not attached, thereby reducing Mean Time to Repair (MTTR), and faster notification of a problem than by traditional SNMP monitoring systems.
<i>Access via WebBrowser, SSHv2 &amp; Telnet</i>	Easy point-and-click access via a Java-enabled Web browser, and SSHv2/Telnet client from a desktop, laptop, or handheld device. Direct Port Access via a SSH user string syntax. Customer can upload, view and delete SSH keys for greater security.
<i>VT100/220/320/ANSI support</i>	Increased choice of terminal emulation options, allows support of a broader range of devices. SX 3.1 can support the following code-sets: US-ASCII (ISO 646); ISO 8859-1 (Latin-1); ISO 8859-15 (Latin-9); UTF-8
<i>SecureChat Instant Messaging</i>	Allows encrypted instant messaging for online collaboration with other authorized web-browser users and maximizes the contribution and effectiveness of a distributed workforce. This feature reduces the time to resolve problems, and allows multiple administrators to troubleshoot a problem. This feature can also be used for training purposes.
<i>Comprehensive SNMP Traps</i>	Enhancements in SMTP notifications –persistent attempts (automatic retries) to send SMTP notifications and support for mail server authentication. SNMP v2 and v3.
<i>Syslog</i>	Supports Syslog to multiple servers, allowing administrators to track activity; logs can also be stored locally on the unit.
<i>NFS Logging</i>	Allows logging of all keystrokes and server/device responses to NFS server(s). Primarily used for audit trails. NFS logging can now be stored on the NFS server with user-defined encryption keys for greater security. Thus if there is an intrusion into the file, the data will be useless without the key under which it was encrypted. Keep-alive messages in the NFS log allow easy monitoring if the managed server/device goes down.

# Features and Benefits

Features	Benefits
<i>Integrated 56K Modem via RJ11 connection available for out of band emergency access</i>	Provides emergency access in the event of a network outage. This capability enables an administrator to access server and network equipment for trouble shooting/disaster recovery. Integrated modem provides a clean installation and removes the need for an external modem/cabling and power. Unlike a separate remote access server, flimsy PCMCIA slot modem cards, and software solutions, the integrated modem, available on select models, minimizes potential points of failure.
<i>CLI Power Control Support of Raritan's Rack Power Distribution Units (PDU)</i>	<p>A Raritan power control unit (RPC/Dominion PX/Dominion PX2) can be connected to each serial port on a Dominion SX. Customers can also control RPCU without a GUI, through scripting and the command line interface (CLI).</p> <p>Outlet associations for servers and networking devices with multiple power feeds, from one power distribution unit or multiple power distribution units.</p>

<b>Integration with CommandCenter® Secure Gateway</b>	
<i>Extensible</i>	When deployed with CommandCenter Secure Gateway, hundreds of Dominion SX devices can be managed with centralized authentication and authorization.
<i>Firmware Upgradeable via Network Connection or CommandCenter Secure Gateway</i>	Simplifies the deployment of firmware updates via CommandCenter Secure Gateway. Administrator can schedule firmware upgrades for single or multiple SX devices.
<i>GUI Remote Power Control via CommandCenter Secure Gateway of Raritan's Intelligent Rack PDU's</i>	Raritan rack PDU's can be connected to each serial port on a Dominion SX. For servers/equipment that have multiple power feeds, multiple power outlets can be associated together to switch equipment on or off with a single click of the mouse.
<i>Single IP Address for Administration and target connection</i>	Administrators and users can connect to one IP address with one login via CommandCenter Secure Gateway to manage the SX or connected serial devices. This connection can be via web browser or through SSH. Only Raritan allows direct SSH connection to the aggregator. Option for SX at-the-rack access while under CC-SG management.