System security is a critical concern among healthcare providers and customers. Siemens has integrated advanced and comprehensive security technology, Ultrasound System Security (USS), directly into its ultrasound platforms.

**Key Benefits**
- A comprehensive solution to protect systems against different types of security threats
- Minimal impact on system performance due to USS low overhead software solution
- Lower operational cost without manual effort

**Key Features**
- Effectively prevents execution of all unauthorized software, scripts and dynamic-link libraries (DLLs)
- Automatically accepts new software added through an authorized process
- Alleviates IT overhead with centralized administration

**Comprehensive. Secure. Certain.**
Siemens Ultrasound System Security (USS) is one of the industry's most advanced, automated and proactive security solutions available today. Utilizing the McAfee™ Embedded Control Security solution, USS allows that only trusted applications run on the systems. It blocks unauthorized access, protects against threats from both networks and infected thumb drives and provides control over when, and by whom, changes are allowed. This means you can focus on providing patient care and taking advantage of Siemens pioneering workflow innovations rather than investing additional time and resources on configuring, updating and managing system security.

**Compatible Systems**

<table>
<thead>
<tr>
<th>Ultrasound System</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACUSON S3000™ ultrasound system</td>
<td>R 1.0 (VC20) and above</td>
</tr>
<tr>
<td>ACUSON S2000™ ultrasound system</td>
<td>R 3.0 (VB20) and above</td>
</tr>
<tr>
<td>ACUSON S1000™ ultrasound system</td>
<td>R 1.0 (VC10) and above</td>
</tr>
<tr>
<td>ACUSON SC2000™ ultrasound system</td>
<td>R 1.6 and above</td>
</tr>
<tr>
<td>ACUSON X700™ ultrasound system</td>
<td>R 1.1 and above</td>
</tr>
<tr>
<td>ACUSON X300™ ultrasound system</td>
<td>R 7.5 and above</td>
</tr>
<tr>
<td>ACUSON X300™ ultrasound system, premium edition (PE)</td>
<td>R 2.5 and above</td>
</tr>
<tr>
<td>ACUSON X150™ ultrasound system</td>
<td>R 2.5 and above</td>
</tr>
</tbody>
</table>
**Light Load. Heavy Hitter.**

Siemens USS software blocks unauthorized executable programs and does not require frequent signature or scanner updates. It automatically and seamlessly provides security protection in the background at all times – online and offline. This makes it an especially valuable feature for hospitals, labs or private practices that rely on networked and portable ultrasound systems.

Siemens USS requires much less resource allocation than a typical virus protection solution, providing continuous security without affecting the ultrasound system’s high-performance imaging or workflow applications. In addition, Siemens USS audits and documents all changes to critical system files, aiding in regulatory compliance, patient data privacy and control requirements of the FDA and HIPAA.

**Siemens Remote Service – Better than Ever.**

Siemens USS works together with Siemens Remote Service. This means data transfers between Siemens and customers’ ultrasound systems are secure (and certified by TÜV). You can confidently take advantage of a suite of available cost-effective, interactive service and support capabilities. These range from remote service access, data transfers, auto-reporting, remote software updates, and remote application training.

**Integrating USS with Siemens Remote Service is simple and convenient:**

- The Siemens system is pre-installed with USS – it requires no customer IT support for configuration or updates.
- Siemens’ local service engineer can quickly connect the customer system to Siemens Remote Service with one onsite visit.
- You can begin taking advantage of remote service capabilities available through a secure connection.

For more information on Ultrasound System Security, contact your local Siemens sales representative.

---

**USS is as simple as 1, 2, 3.**

1. **Inventory**
   - A white-list of “known applications”

2. **Update/Upgrade**
   - All changes must be authorized
   - Admin

3. **Change Record**
   - An updated white-list of “known applications”