

## Course Outline

Security Center 5.x: Advanced Troubleshooting	
<b>Code</b>	SC-STC-002 (5.x)
<b>Level</b>	Advanced
<b>Duration</b>	2 days
<b>Target audience</b>	Technicians, Administrators, and IT Professionals
<b>Prerequisites</b>	Security Center Synergis training (SC-STC-001 5.x) or, equivalent practical experience managing a Security Center system
<b>Objectives</b>	<p><u>Upon successful completion of this course the participant will be able to:</u></p> <ul style="list-style-type: none"> <li>• Describe the architecture of a Security Center access control system</li> <li>• Configure secure areas for antipassback, interlock, 1<sup>st</sup> person, visitor escort</li> <li>• Share cardholder and credential information with Global Cardholder Sync</li> <li>• Import cardholders and credentials from Windows Active Directory</li> <li>• Configure threat levels to change access within a system with a single click</li> <li>• Enroll and configure:               <ul style="list-style-type: none"> <li>○ Synergis Cloud Link, HID and Mercury controllers</li> <li>○ Enroll and configure biometric readers</li> <li>○ Update firmware and EEPROM files</li> <li>○ Add OSDP readers</li> </ul> </li> <li>• Troubleshoot a Security Center access control system using Security Center tools, Windows tools and 3<sup>rd</sup> party tools</li> <li>• Use the Server, Cloud Link or Client diagnostic console for troubleshooting</li> <li>• Find, open and read the contents of the various log files</li> </ul>
<b>Certification</b>	An open-book, practical exam will be given at the end of this course.

Topic	Description
<b>Module 1:</b> <i>Introduction &amp; Troubleshooting</i> (1½ hour)	<ul style="list-style-type: none"> <li>• Introduction</li> <li>• Troubleshooting methodology</li> <li>• Where to find information               <ul style="list-style-type: none"> <li>○ <a href="https://portal.genetec.com">https://portal.genetec.com</a></li> </ul> </li> </ul>
<b>Module 2:</b> <i>Architecture review</i> (1½ hour)	<ul style="list-style-type: none"> <li>• High level system architecture</li> <li>• Role based architecture</li> <li>• Services</li> <li>• Processes</li> <li>• Hardware connections</li> <li>• Fail-over Access Manager</li> </ul>
<b>Module 3:</b> <i>Advanced Configurations</i> (4 hours)	<ul style="list-style-type: none"> <li>• Secured areas               <ul style="list-style-type: none"> <li>○ Antipassback</li> <li>○ Interlock</li> <li>○ 1<sup>st</sup> Person in</li> <li>○ Visitor escort</li> </ul> </li> <li>• Global Cardholder Synchronizer</li> <li>• Active Directory integration</li> <li>• Threat Levels and Clearance levels</li> <li>• Occupancy limits on areas</li> <li>• Duress PIN</li> </ul>
<b>Module 4:</b> <i>Advanced Troubleshooting</i> (3 hours)	<ul style="list-style-type: none"> <li>• Synergis Cloud Link</li> <li>• HID</li> <li>• Mercury</li> </ul>
<b>Module 5:</b> <i>More Hardware</i> (2 hours)	<ul style="list-style-type: none"> <li>• Electronic locks               <ul style="list-style-type: none"> <li>○ Assa Abloy</li> <li>○ Allegion Schlage</li> <li>○ Simon Voss</li> <li>○ Salto Sallis</li> </ul> </li> <li>• OSDP               <ul style="list-style-type: none"> <li>○ Adding OSDP readers to: Axis, HID, Mercury</li> </ul> </li> <li>• Biometric integrations               <ul style="list-style-type: none"> <li>○ Bioconnect</li> <li>○ Morpho</li> </ul> </li> </ul>
<b>Module 6:</b> <i>Diagnostic Console &amp; Log files</i> (2 hours)	<ul style="list-style-type: none"> <li>• Access Manager console</li> <li>• Softwire console</li> <li>• Client console</li> <li>• Log files</li> </ul>