

Plan du cours

Security Center : Dépannage avancé	
Code :	SC-STC-002
Niveau :	Avancé
Durée :	2 jours (Formation dirigée par un instructeur)
Public concerné :	Techniciens, administrateurs et informaticiens
Prérequis :	Formation Security Center Synergis (SC-STC-001) ou expérience pratique équivalente en gestion d'un système Security Center
Objectifs :	<p><u>Une fois ce cours terminé avec succès, le participant pourra :</u></p> <ul style="list-style-type: none"> • Décrire l'architecture d'un système de contrôle d'accès Security Center. • Configurer des secteurs sécurisés pour l'antiretour, les sas, superviseur présent, escorte de visiteurs. • Partager des données de titulaires de cartes et d'identifiants avec la Synchronisation des titulaires de cartes globaux. • Importer des titulaires de cartes et identifiants depuis Windows Active Directory. <ul style="list-style-type: none"> ○ Contrôleurs Synergis Cloud Link, HID et Mercury. ○ Inscrire et configurer les lecteurs biométriques. ○ Mettre à jour le micrologiciel et les fichiers EEPROM. • Dépanner un système de contrôle d'accès Security Center à l'aide des outils Security Center, des outils Windows et d'outils tiers. • Utiliser la console de diagnostic Server, Cloud Link ou Client pour le dépannage. • Rechercher, ouvrir et consulter le contenu de différents fichiers journaux.
Certification :	Un examen pratique à livre ouvert est organisé à la fin de cette formation.

Sujet	Description
Module 1 : <i>Introduction</i> (1 heure)	<ul style="list-style-type: none"> • Introduction • Processus de dépannage • Où trouver des informations <ul style="list-style-type: none"> ◦ https://portal.genetec.com
Module 2 : <i>Révision de l'architecture</i> (1h30)	<ul style="list-style-type: none"> • Architecture système de haut niveau • Architecture basée sur les rôles • Services • Processus • Connexions matérielles • Gestionnaire d'accès de basculement
Module 3 : <i>Configurations supplémentaires</i> (3h30)	<ul style="list-style-type: none"> • Secteurs sécurisés <ul style="list-style-type: none"> ◦ Antiretour ◦ Sas ◦ Premier entré ◦ Escorte de visiteur ◦ PIN de contrainte • Synchroniseur des titulaires de carte globaux • Intégration Active Directory • Niveaux de risque et d'habilitation
Module 4 : <i>Configuration matérielle avancée et micrologiciels</i> (3 heures)	<ul style="list-style-type: none"> • Micrologiciel • Personnalisation des entrées • Synergis Cloud Link • HID • Mercury
Module 5 : <i>Matériel supplémentaire</i> (1½ heure)	<ul style="list-style-type: none"> • Verrous électroniques <ul style="list-style-type: none"> ◦ Assa Abloy ◦ Allegion Schlage ◦ Simon Voss ◦ Salto Sallis • OSDP <ul style="list-style-type: none"> ◦ Ajout de lecteurs OSDP à : Axis, HID, Mercury
Module 6 : <i>Méthodologie de dépannage</i> (1½ heure)	<ul style="list-style-type: none"> • Méthodologie de dépannage • Scénarios • Exercices de dépannage
Module 6 : <i>Console et fichiers journaux</i> (2 heures)	<ul style="list-style-type: none"> • Console serveur • Console Softwire • Consoles client • Fichiers journaux