Date de publication : 05/08/2025

Formation : Implementing and Configuring Cisco Identity Services Engine (SISE) v4.0

Cours officiel, préparation à l'examen 300-715 SISE

Formation pratique - 5j - 35h00 - Réf. ERX
Prix : 4350 € H.T.

Avec cette formation, vous déployez et utilisez Cisco Identity Services Engine (ISE) pour appliquer des politiques d'accès sécurisées sur les réseaux filaires, sans fil et VPN. Vous apprenez à gérer les accès invités, le BYOD, la conformité des terminaux, le contrôle via TACACS+, et à renforcer votre posture Zero Trust. Grâce aux labs pratiques, vous gagnez en visibilité sur le réseau et optimisez la gestion des politiques de sécurité.

INFORMATIONS

Pour toute inscription en inter ou en intra-entreprise, chaque participant doit disposer d'un compte Cisco Learning Space associé à l'adresse e-mail utilisée lors de son inscription à la formation. Cette démarche obligatoire permet d'accéder au support de formation officiel Cisco.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Présenter Cisco ISE et ses cas d'usage en sécurité réseau
- Expliquer le déploiement et l'architecture de Cisco ISE
- Décrire les composants d'application des politiques dans Cisco ISE
- Configurer les politiques d'accès dans Cisco ISE
- Diagnostiquer les politiques Cisco ISE et la compatibilité des équipements tiers (NAD)
- Configurer l'accès invité, les hotspots et les portails invités
- Présenter les services de profiling Cisco ISE et les bonnes pratiques associées
- Mettre en place une solution BYOD avec Cisco ISE
- Configurer la conformité des terminaux et les services de posture client
- Configurer l'administration des équipements et TrustSec dans Cisco ISE

PARTICIPANTS

Ingénieurs et architectes sécurité réseau, administrateurs ISE, membres senior du SOC, ainsi qu'aux intégrateurs et partenaires Cisco.

PRÉREQUIS

Connaissance du CLI Cisco IOS, de Cisco AnyConnect, de Windows, du 802.1X et formation de niveau CCNP Security recommandée.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Public concerné

Ingénieurs et architectes sécurité réseau, administrateurs ISE, membres senior du SOC, ainsi qu'aux intégrateurs et partenaires Cisco.

Prérequis

Connaissance du CLI Cisco IOS, de Cisco AnyConnect, de Windows, du 802.1X et formation de niveau CCNP Security recommandée.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français (ou en anglais sur demande). Support de cours officiel en anglais.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Programme officiel

- Introduction à l'architecture Cisco ISE.
- Introduction au déploiement de Cisco ISE.
- Introduction aux composants d'application des politiques dans Cisco ISE.
- Introduction à la configuration des politiques dans Cisco ISE.
- Dépanner les politiques Cisco ISE et la prise en charge des NAD tiers.
- Introduction à l'authentification web et aux services invités.
- Configuration des hotspots et des portails invités.
- Introduction au profiler Cisco ISE.
- Introduction aux bonnes pratiques et aux rapports de profilage.
- Configuration de Cisco ISE pour le BYOD (Bring Your Own Device).
- Introduction aux services de conformité des points d'extrémité dans Cisco ISE.
- Configuration des services de posture client et de conformité.
- Utilisation des dispositifs d'accès réseau (NAD).
- Exploration de Cisco TrustSec.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

2 Travaux pratiques officiels

- Configurer l'initialisation de Cisco ISE et l'utilisation des certificats système.
- Intégrer Cisco ISE avec Active Directory.
- Configurer une politique Cisco ISE pour le contournement d'authentification par adresse MAC (MAB).
- Configurer une politique Cisco ISE pour 802.1X.
- Configurer l'accès invité.
- Configurer un hotspot et l'accès invité en auto-inscription.
- Configurer l'accès invité avec approbation par sponsor et l'accès invité entièrement sponsorisé.
- Créer des rapports invités.
- Configurer le profilage.
- Personnaliser la configuration de profilage de Cisco ISE.
- Créer des rapports de profilage Cisco ISE.
- Configurer le BYOD (Bring Your Own Device).
- Gérer un appareil BYOD perdu ou volé.
- Configurer les services de conformité Cisco ISE.
- Configurer l'approvisionnement client.
- Configurer les politiques de posture.
- Tester et surveiller l'accès basé sur la conformité.
- Configurer Cisco ISE pour l'administration basique des équipements.
- Configurer l'autorisation de commandes Cisco ISE.
- Configurer Cisco TrustSec.

Options

Certification : 340 € H.T.

Pour l'obtention de la certification Cisco Certified Network Professional Security (CCNP Security), la réussite de l'examen 350-701 SCOR est requise ainsi que la réussite de l'un des examens suivants (au choix) : 300-710 SNCF, 300-715 SISE, 300-720 SESA, 300-725 SWSA, 300-730 SVPN, 300-740 SCAZT ou 300-745 SDSI.

Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Ce programme est une création originale, conçu par les équipes pédagogiques d'ORSYS Formation. Toute reproduction, représentation, adaptation ou exploitation, totale ou partielle, sans autorisation préalable écrite d'ORSYS, est strictement interdite. ORSYS se réserve le droit d'engager toute action nécessaire à la protection de ses droits de propriété intellectuelle.

Dates et lieux

CLASSE À DISTANCE
2026 : 23 nov.

2027 : 7 juin, 7 juin