

Engineering Cisco Meraki Solutions Part 2 (ECMS2)

ID ECMS2 Prix CHF 2 980,- (Hors Taxe) Durée 3 jours

A qui s'adresse cette formation

- Professionnels qui déploient ou gèrent régulièrement des réseaux Meraki et qui souhaitent approfondir leur expertise technique et leur compréhension de la suite complète de produits Meraki et de ses fonctionnalités
- Ingénieur-conseil en systèmes
- Ingénieur de déploiement
- Administrateur réseau
- Gestionnaire de réseau
- Ingénieur réseau
- Ingénieur en fiabilité de site
- Ingénieur système
- Architecte de solutions techniques
- Ingénieur conception sans fil
- Ingénieur sans fil

Pré-requis

Avant de vous inscrire au cours ECMS2, il est fortement recommandé d'avoir déjà suivi et terminé le cours ! avant de participer à cette formation.

Vous devez également avoir une compréhension générale du réseau, des compétences spécifiques à Meraki et des connaissances dans les domaines suivants :

Réseau général :

- Être activement engagé dans la conception, le déploiement, la mise à l'échelle et la gestion des réseaux d'entreprise.
- Solide connaissance fondamentale des schémas d'adressage et de sous-réseau IP nécessaires à la construction de réseaux locaux.
- Solide connaissance fondamentale des protocoles de routage dynamique (accent mis sur l'Open Shortest Path First [OSPF] et le Border Gateway Protocol [BGP]).
- Une compréhension fondamentale des mécanismes de qualité de service (QoS) avec et sans fil, des opérations de file d'attente de paquets et des implémentations pratiques.
- Avoir une expérience de la conception et de la configuration de l'IPsec et des technologies de réseau privé virtuel (VPN) associées.

- Une compréhension fondamentale des contrôles/protocoles de sécurité du réseau, des meilleures pratiques de gestion du réseau et de la sécurité des données.
- Une compréhension fondamentale des principes de conception des meilleures pratiques en matière de radiofréquence (RF) et des mises en œuvre pratiques.
- Une connaissance fondamentale des meilleures pratiques en matière de sécurité sans fil, centrées sur le contrôle d'accès (802.1x) et la sécurité du spectre par le biais de systèmes de détection des intrusions sans fil (WIDS) et de systèmes de prévention des intrusions sans fil (WIPS).
- Maîtrise fondamentale des protocoles de journalisation et de surveillance standard (en particulier le protocole de gestion de réseau simple [SNMP], syslog et les webhooks) et des composants ou outils de mise en œuvre connexes.
- Connaître et avoir une connaissance de base des interfaces de programmation d'applications (API) et des langages/formats associés (REST, JavaScript Object Notation [JSON]).

Connaissance de Meraki :

- Être capable de décrire la sécurité, la fiabilité et l'évolutivité de l'architecture cloud de Cisco Meraki dashboard et de son plan de contrôle hors bande.
- Compréhension fondamentale de la structure organisationnelle de Dashboard, de la délimitation des privilèges et des processus administratifs primordiaux.
- Être en mesure d'exposer les principaux composants de la licence Meraki (modèle de co-résilience et période de grâce d'expiration)
- Avoir les connaissances et la capacité de déployer des fonctions de sécurité avancées sur les appareils de sécurité MX (détection/prévention des intrusions, protection avancée contre les logiciels malveillants [AMP], règles de pare-feu des couches 3 et 7).
- Compréhension fondamentale de l'Auto VPN et de son objectif lorsqu'il est utilisé dans un déploiement de réseau étendu défini par logiciel (SD-WAN).
- Être en mesure de décrire les concepts sous-jacents à une solution WLAN basée sur le cloud et les fonctionnalités qui peuvent être fournies, notamment la mise en forme du trafic de couche 7 et les différentes méthodes d'authentification de l'accès des invités.
- Compréhension fondamentale de la conteneurisation des profils de périphériques et des capacités de gestion à

distance, telles que gérées par la plate-forme Systems Manager.

- Compréhension fondamentale de l'architecture périphérique telle qu'elle est mise en œuvre par les caméras de sécurité Meraki MV et de ses implications sur la rétention vidéo grâce à diverses options configurables.

Voici les offres recommandées de Cisco qui peuvent vous aider à remplir ces conditions préalables :

- [Implementing and Administering Cisco Solutions \(CCNA\)](#)
- [Implementing and Operating Cisco Enterprise Network Core Technologies \(ENCOR\)](#)
- !

Objectifs

À l'issue de ce cours, vous serez capable de :

- Planifier de nouvelles architectures Cisco Meraki et étendre les déploiements existants.
- Concevoir le réseau pour une gestion évolutive et une haute disponibilité
- Décrire comment automatiser et faire évoluer les déploiements Meraki avec des outils de tableau de bord.
- Utiliser les protocoles de routage dynamique pour étendre les réseaux et améliorer les performances du réseau étendu.
- Décrire les configurations de routage basées sur la QoS, les politiques et les performances sur un réseau Cisco Meraki et l'optimisation du WAN par la mise en forme du trafic.
- Décrire les topologies de réseau privé virtuel (VPN) et de réseau étendu (WAN) et comment les intégrer.
- Sécuriser, étendre et façonner le réseau
- Mettre en œuvre les concepts et pratiques des réseaux commutés, et configurer les réseaux d'invités
- Mettre en œuvre les concepts et pratiques de configurations sans fil
- Décrire les concepts et pratiques de gestion des terminaux à l'aide de Cisco Meraki Systems Manager.
- Décrire les concepts et pratiques de sécurité physique
- Obtenir un aperçu du réseau en surveillant les applications
- Décrire comment préparer les services de surveillance, de journalisation et d'alerte
- Configurer les capacités de rapport et d'audit dans le tableau de bord Cisco Meraki
- Surveiller et résoudre les problèmes à l'aide des outils Cisco Meraki

- Planification de nouvelles architectures Cisco Meraki et extension des déploiements existants
- Conception d'une gestion évolutive et d'une haute disponibilité
- Automatisation et mise à l'échelle des déploiements Meraki
- Conception du routage et des pratiques sur la plate-forme Meraki
- Décrire la qualité de service (QoS) et la conception de la mise en forme du trafic.
- Création de topologies VPN et WAN
- Sécuriser, étendre et façonner le réseau
- Décrire les concepts et les pratiques du réseau
- Mise en œuvre des pratiques et des concepts de configuration sans fil
- Décrire les concepts et pratiques de gestion des points d'extrémité
- Décrire les concepts et pratiques de sécurité physique
- Obtenir un aperçu du réseau grâce aux applications de surveillance
- Préparation des services de surveillance, de journalisation et d'alerte
- Configuration des capacités de rapport et d'audit dans le tableau de bord Cisco Meraki
- Obtenir une visibilité et résoudre les problèmes à l'aide des fonctions Meraki et des outils de dépannage intégrés

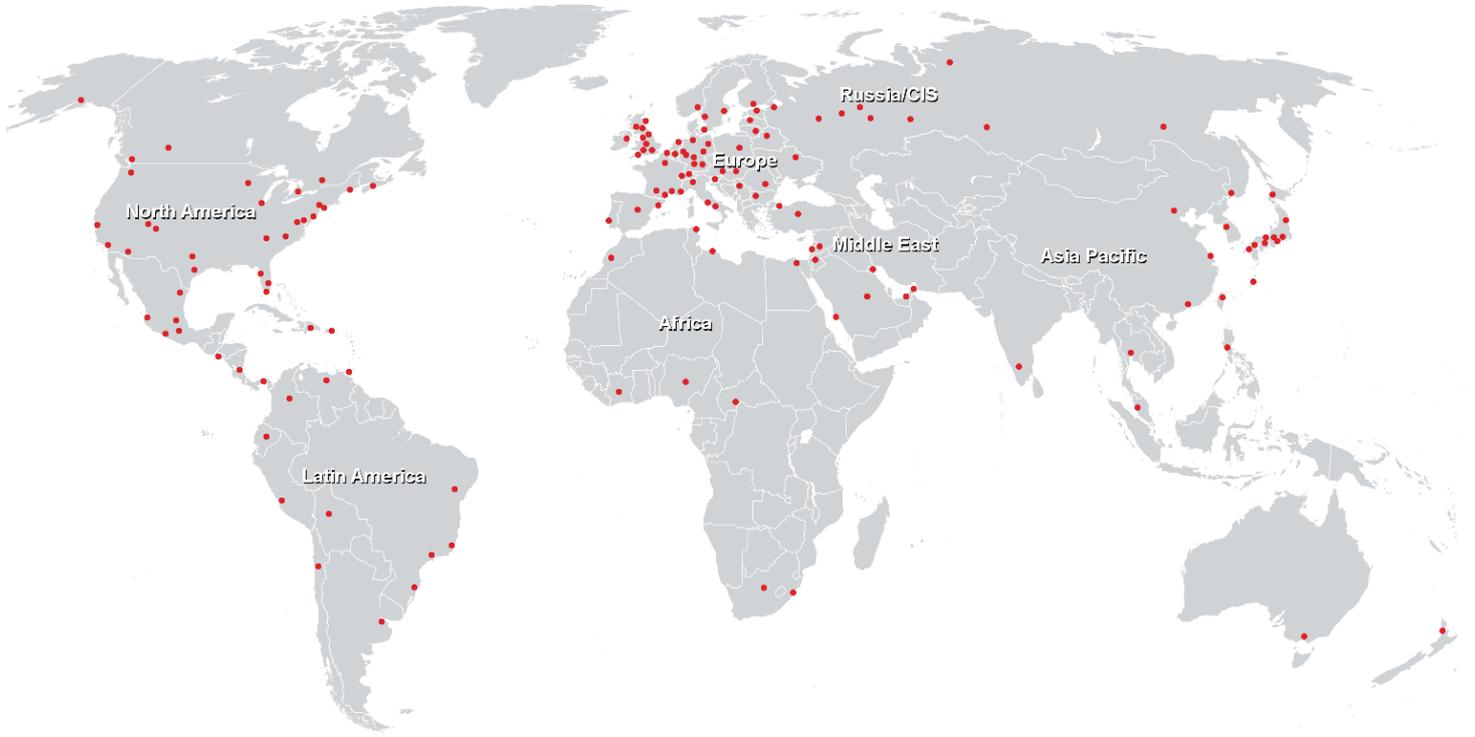
Labs

- Configurer les balises, l'agrégation de liens, la mise en miroir de ports et les SSID haute densité.
- Établissement d'un VPN automatique
- Configuration des interfaces virtuelles et du routage sur les commutateurs Cisco Meraki MS
- Configuration des routes et de la redistribution
- Configuration de la qualité de service
- Configuration de la mise en forme du trafic
- Configuration de l'équilibrage de charge
- Définition des règles de pare-feu
- Activation de la protection avancée contre les logiciels malveillants, de la détection des intrusions et de la prévention des intrusions
- Activation du filtrage de contenu
- Configurer et appliquer des politiques d'accès
- Configurer l'accès invité sans fil
- Configurer les identificateurs d'ensembles de services (SSID)
- Mise en œuvre des profils RF
- Mise en œuvre de l'Air Marshal
- Créer des profils de configuration du gestionnaire de systèmes Cisco Meraki (SM)
- Définir des politiques de sécurité
- Appliquer la sécurité de bout en bout
- Configuration des alertes de mouvement
- Déployer des caméras sans fil

Contenu

- Gestion de la conservation des vidéos
- Activer les alertes
- Ajouter la surveillance et les rapports
- Générer et analyser les rapports de synthèse
- Gestion des micrologiciels
- Générer un rapport de conformité PCI (Peripheral Component Interconnect)
- Dépannage d'un dispositif hors ligne
- Dépannage du filtrage de contenu
- Dépannage de la connectivité des sites distants

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>