+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 14/08/2025

S'inscrire

Formation Outils d'assistance à distance

2 jours (14 heures)

Présentation

Les outils d’assistance à distance permettent de diagnostiquer et résoudre les incidents en temps réel, d’accompagner les utilisateurs et d’opérer des postes en toute sécurité.

De TeamViewer à AnyDesk, en passant par RustDesk et Apache Guacamole, ces solutions allient performance, sécurité et simplicité pour professionnaliser le support.

Notre formation Outils d’assistance à distance vous apprendra à choisir, déployer et administrer ces solutions à l’échelle.

Vous saurez définir une gouvernance d’accès, intégrer l’outillage à votre ITSM, sécuriser les sessions (MFA, rôles, enregistrement), et piloter la qualité de service avec des KPI actionnables.

À l’issue, vous serez en mesure de standardiser vos pratiques (runbooks, modèles), automatiser l’exploitation, et communiquer efficacement côté support et management.

Comme toutes nos formations, celle?ci présente les dernières versions stables des principaux outils comme la v15.68.6 de TeamViewer, la v9.5.11 d'AnyDesk, la v1.4.1 de RustDesk ou encore la v1.6.0 d'Apache Guacamole.

Objectifs

- Comparer les solutions et choisir selon votre contexte
- Déployer, intégrer (annuaire/SSO) et configurer l’accès non assisté
- Sécuriser les sessions : MFA, rôles, traçabilité
- Industrialiser l’exploitation : scripts, MDM, runbooks
- Mesurer et améliorer via KPI et rapports
- Établir PRA/PCA et amélioration continue

Public visé

- Responsables support IT
- Administrateurs systèmes
- Responsables formation
- Consultants support à distance

Pré?requis

- Bases systèmes, réseau et sécurité
- Notions de SSO recommandées

Programme de notre formation Outils d'assistance à distance

Enjeux et panorama des outils d’assistance

- Cas d’usage : support, prise en main à distance, co-browsing, AR
- Comparatif : TeamViewer, AnyDesk, RustDesk, Apache Guacamole
- Architectures : SaaS, on?premises, self?hosted, passerelles RDP/VNC/SSH
- Sécurité de base : chiffrement, MFA, journaux, rôles
- Processus d’assistance : ouverture ? résolution ? clôture
- atelier : parcours d’assistance de bout?en?bout (initiation)

Gouvernance, conformité et gestion des accès

- Politiques : RBAC, SSO, gestion des secrets et appareils
- Conformités : GDPR, traçabilité des sessions
- Bonnes pratiques : moindre privilège, durcissement postes
- Gestion des risques et shadow IT
- Modèle opérationnel : rôles L1/L2/L3, catalogue
- atelier : ACL + MFA + politique de logs

Déploiement et intégration en entreprise

- Pré?requis : ports, proxy, certificats TLS, pare?feu
- Déploiement MSI/PKG, MDM (Intune, Jamf)
- Intégration ITSM (ITIL), annuaire Azure AD/LDAP, SAML/OIDC
- Paramétrages : accès non assisté, codes de session
- Sécurité avancée : black screen, enregistrement, consentement
- atelier : déploiement + SSO/annuaire (PoC)

Opérations quotidiennes et expérience utilisateur

- Files de demandes, SLA, messages et macros
- Multi?OS (Win/macOS/Linux/Mobile) & BYOD
- Qualité de service : latence, bande passante, codecs

- Gestion des incidents récurrents & base de connaissances
- Mesure de la satisfaction (CSAT)
- atelier : runbook + scripts d’automatisation

Supervision, reporting et pilotage

- Tableaux de bord, KPI et exports CSV/JSON
- Supervision centralisée, alertes, intégration SIEM
- Gestion des logs et conservation RGPD
- Capacity planning : licences, canaux, coûts
- Communication & posture de service
- atelier : construire un tableau de bord KPI

Roadmap, bonnes pratiques et continuité

- Choix & évolution outillage : critères, coûts, TCO
- Standardiser : modèles, check?lists, dictionnaire de données
- Continuité : PRA/PCA, mode dégradé, back?up d’outils
- Sécurisation avancée : bastion, segmentation, Zero Trust
- Capitalisation : rétrospectives, coaching, acculturation
- atelier : simulation d’incident & REX

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.