Livre blanc

GoToAssist® CORPORATE

Livre blanc sur la sécurité de Citrix GoToAssist Corporate

GoToAssist Corporate offre des mesures de sécurité robustes de bout en bout qui préviennent à la fois les attaques passives et actives visant la confidentialité, l'intégrité et la disponibilité.

CITRIX® | online

Sommaire

Portée et audience

Ce guide est destiné aux utilisateurs de Citrix® GoToAssist® Corporate et aux autres parties prenantes qui ont besoin de comprendre comment GoToAssist prend en charge le risque de sécurité des informations et l'adéquation à leur environnement.

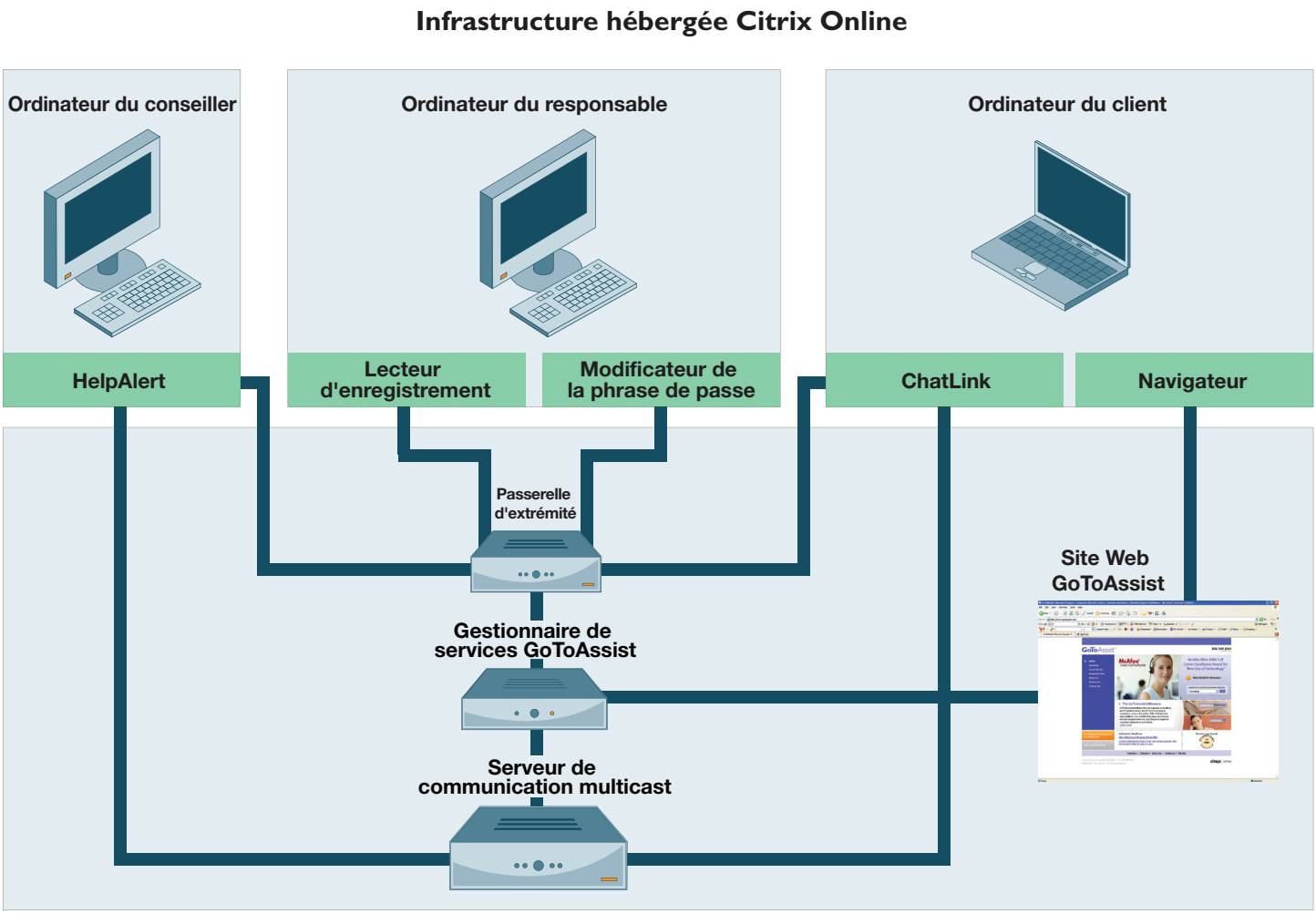
Introduction

GoToAssist Corporate est un service hébergé qui permet de fournir une assistance à distance sur des ordinateurs Windows. Grâce à GoToAssist Corporate, un utilisateur peut demander de l'assistance à un conseiller et ce dernier peut voir et éventuellement contrôler le PC de l'utilisateur final à distance.

Ce document est consacré aux fonctions de GoToAssist Corporate qui ont trait à la sécurité des informations. Le lecteur est supposé posséder une connaissance de base du produit et de ses fonctions. Pour obtenir des documentations supplémentaires sur GoToAssist Corporate, visitez le site Web www.citrixonline.com ou contactez un conseiller Citrix Online.

Architecture de prestation de services GoToAssist Corporate

Le graphique ci-dessous schématise les principaux composants et chemins de communication de la prestation de services avec GoToAssist Corporate.



Définitions

HelpAlert : cet exécutable Win32 réside sur l'ordinateur du conseiller et permet à celui-ci de recevoir les requêtes des clients et d'y répondre.

ChatLink : cette application d'extrémité facilite la communication textuelle entre un client et un conseiller du support technique.

Navigateur : navigateur Internet standard, comme Firefox, Internet Explorer, etc.

Lecteur d'enregistrement : application d'extrémité qui permet aux responsables d'équipe et d'entreprise de réécouter des sessions GoToAssist Corporate enregistrées. Le lecteur d'enregistrement permet de revoir les partages d'écran à distance, les partages d'écran locaux, les conversations et les diagnostics à distance.

Modificateur de la phrase de passe : application d'extrémité qui facilite le changement de la phrase de passe utilisée pour protéger l'accès crypté aux enregistrements de session.

Site Web GoToAssist : application Web qui permet l'accès au site Web GoToAssist et aux portails d'administration externes et internes.

Gestionnaire de services GoToAssist : application Web en charge des fonctions de rapport, de stockage permanent et de gestion des services et des comptes GoToAssist Corporate.

Serveur de communication multicast : serveur faisant partie d'une flotte distribuée dans le monde entier servant à fournir une gamme de services de communication unicast et multicast à haute disponibilité.

Passerelle d'extrémité : passerelle spécifique utilisée par différentes applications d'extrémité pour accéder en toute sécurité au Gestionnaire de services GoToAssist à des fins diverses à l'aide d'appels de procédure distante.

Sécurité de l'application

GoToAssist Corporate permet l'accès à une gamme de ressources et de services en utilisant un système de contrôle d'accès basé sur des rôles qui est mis en œuvre par les différents composants de prestation de services. Les différents rôles et les termes qui leur sont associés sont définis dans le tableau ci-dessous :

Rôles

Administrateur (ou admin)	Employé Citrix Online qui crée des groupes et des portails dans le Management Center GoToAssist Corporate d'une entreprise. Les administrateurs peuvent créer, modifier et effacer des comptes, des portails et des responsables d'entreprise ou d'équipe GoToAssist Corporate, modifier les abonnements et les tarifs et effectuer d'autres tâches administratives.
Entreprise	Client GoToAssist Corporate pour lequel les portails sont configurés.
Responsable d'entreprise	Employé de la société cliente ayant accès au Management Center GoToAssist Corporate. Il est autorisé à modifier les comptes, les portails, les conseillers et les équipes associés à son compte.
Client	Employé de la société cliente qui demande de l'assistance via GoToAssist Corporate.
Groupe / Équipe	Ensemble de conseillers affectés à un portail spécifique. Chaque conseiller appartient à un groupe ou à une équipe unique ; chaque groupe ou équipe est affecté à un portail unique. Les groupes / équipes contiennent certains paramètres par défaut pour les conseillers.
Responsable de groupe / Responsable d'équipe	Un employé du client autorisé par un responsable de l'entreprise à modifier certains aspects d'une équipe et des conseillers et portails qui lui sont associés.
Conseiller	Membre de l'équipe d'assistance qui répond aux questions des clients via HelpAlert.

Authentification

Les administrateurs, les responsables et les conseillers GoToAssist Corporate sont authentifiés à l'aide d'un nom de compte et d'un mot de passe fort.

Les mots de passe sont régis par les règles suivantes :

Mots de passe forts : un mot de passe fort comporte entre 8 et 32 caractères et doit contenir au moins trois des quatre éléments suivants : lettres majuscules [A à Z], lettres minuscules [a à z], chiffres [0 à 9] et caractères spéciaux [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Les mots de passe forts doivent être différents du nom de connexion ou du nom/prénom figurant sur le compte du conseiller. La longueur du mot de passe est vérifiée lors de l'initialisation ou du changement du mot de passe.

Période de validité du mot de passe : la période de validité du mot de passe est configurable. Comprise entre 10 et 120 jours, sa valeur par défaut est de 90 jours. Si le détenteur d'un compte tente de se connecter avec un mot de passe obsolète, il est contraint de changer de mot de passe.

Historique des mots de passe : il existe un historique des mots de passe. Un mot de passe ne peut pas être défini sur une valeur qui a déjà été utilisée. Le nombre de mots de passe mémorisé est configurable. Compris entre 1 et 5, sa valeur par défaut est de 3.

Verrouillage de compte : après 3 échecs de connexion consécutifs, le compte est automatiquement mis en état de verrouillage temporaire. Le détenteur du compte ne pourra alors plus se connecter avant une période de temps comprise entre 5 (valeur par défaut) et 30 minutes. Après expiration de la période de verrouillage, le détenteur du compte peut réessayer de saisir ses informations de connexion.

Une option de verrouillage définitif est également disponible. Après un nombre d'échecs de connexion configurable, le compte est verrouillé de manière définitive. Le détenteur du compte ne pourra alors plus se connecter à son compte tant que son mot de passe n'aura pas été réinitialisé par un autre détenteur de compte disposant de privilèges administratifs. Le verrouillage définitif est activé après un nombre d'échecs de connexion compris entre 10 (valeur par défaut) et 50.

Protection des données et des PC client

Protégeant l'accès au PC du client et aux données qu'il contient, le modèle de contrôle d'accès sur approbation du client constitue un composant essentiel de la sécurité de GoToAssist Corporate.

Chaque session GoToAssist Corporate doit être initiée par le client distant. La solution GoToAssist Corporate n'est pas conçue pour une prestation de services sans surveillance.

D'autre part, le client doit toujours donner son accord avant qu'un partage d'écran, un contrôle à distance ou un transfert de données de diagnostic, de fichiers ou d'autres informations puisse se faire.

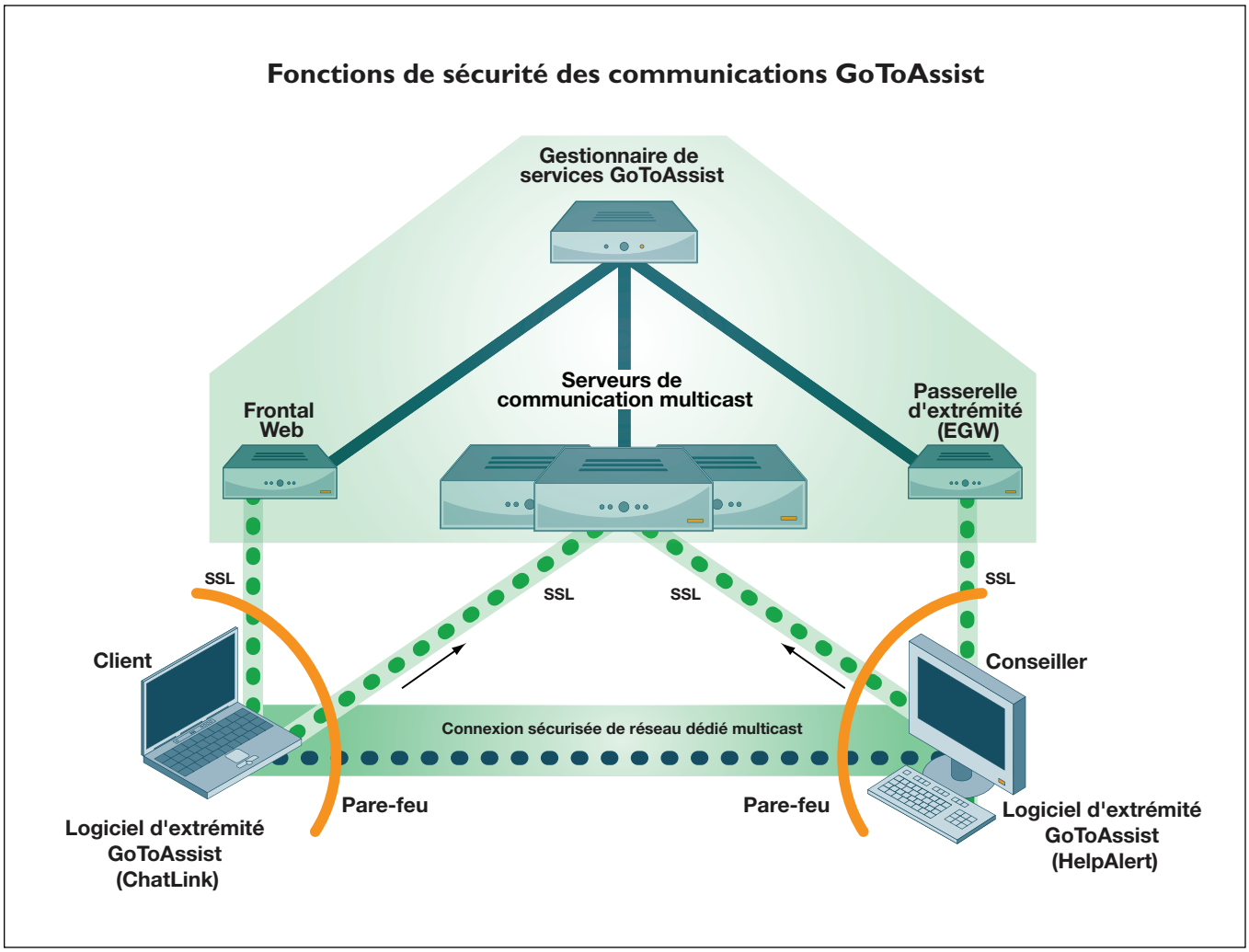
Après autorisation d'un contrôle à distance et d'un partage d'écran, le client peut suivre chaque action du conseiller. Le client peut facilement reprendre le contrôle de son PC ou interrompre la session à tout moment.

Les contrôles de sécurité locaux du PC client ne sont jamais outrepassés. Le client ou le conseiller doit toujours fournir les informations d'authentification Windows ou d'application.

Enfin, toutes les activités de connexion sont consignées et les partages d'écran ou les conversations peuvent être enregistrés et revus ultérieurement.

Fonctions de sécurité des communications

La communication entre les participants d'une session GoToAssist Corporate se fait par le biais d'une pile réseau multicast qui vient se superposer à la pile TCP/IP conventionnelle sur chaque PC utilisateur. Ce réseau est formé à partir d'un ensemble de serveurs de communication multicast (MCS) Citrix Online. L'architecture de communication est résumée par la figure ci-dessous.



Les participants à une session GoToAssist Corporate (« extrémités ») communiquent avec les serveurs et passerelles de l'infrastructure Citrix Online à l'aide de connexions TCP/IP sortantes sur les ports 8200, 443 et 80. GoToAssist Corporate étant un service Web hébergé, les participants peuvent être localisés n'importe où sur Internet, qu'ils soient dans un bureau distant, à domicile, dans un centre d'affaires ou connectés au réseau d'une autre société.

Le service GoToAssist Corporate est accessible en tout lieu et à tout moment, fournissant une connectivité et une flexibilité maximales. Cependant, pour protéger la confidentialité et l'intégrité des communications commerciales privées, GoToAssist Corporate comprend également des fonctions de sécurité renforcée.

Confidentialité et intégrité des communications

GoToAssist Corporate offre des mesures de sécurité renforcée de bout en bout qui préviennent à la fois les attaques passives et actives visant la confidentialité, l'intégrité et la disponibilité. Toutes les connexions GoToAssist Corporate sont cryptées de bout en bout et accessibles uniquement aux participants de session d'assistance autorisés.

Les données de partage d'écran, les données de contrôle de la souris et du clavier et les informations de conversation textuelle ne sont jamais exposées sous forme non cryptée pendant leur passage sur les serveurs de communication Citrix Online ou pendant leur transmission sur des réseaux publics ou privés.

Si l'enregistrement est désactivé, la clé de session GoToAssist Corporate n'est conservée sous aucune forme que ce soit sur les serveurs Citrix Online. Ainsi, l'attaque d'un serveur ne permet pas d'obtenir les clés des flux cryptés.

Si l'enregistrement est activé, les données de conversation, de partage d'écran et de visionnage d'écran sont stockées sous forme cryptée. La clé de session est également enregistrée, mais elle est protégée par un cryptage à clé publique/privée RSA de 1 024 bits. La session est cryptée avant enregistrement à l'aide d'une clé publique spécifique à chaque portail. Pour lire la session, trois éléments sont nécessaires : l'enregistrement de la session, la clé de session cryptée et la clé privée du portail.

Des contrôles de sécurité de communication basés sur un cryptage renforcé sont mis en œuvre à deux niveaux : la « couche TCP » et la « couche MPSL » (Multicast Packet Security Layer ou couche de sécurité des paquets multicast).

Sécurité de la couche TCP

Des protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) de norme IETF sont utilisés pour protéger toutes les communications entre les extrémités. Pour offrir une protection maximale contre l'écoute clandestine, l'altération des données et les attaques par rejeu, la seule suite de chiffrement SSL prise en charge pour les connexions TCP non-Web est la clé RSA de 1 024 bits avec les algorithmes HMAC-SHA1 et AES-CBC de 128 bits. Toutefois, pour assurer une compatibilité avec un maximum de navigateurs Web et de bureaux utilisateur, le site Web GoToAssist prend en charge les connexions entrantes utilisant les suites de chiffrement SSL les plus répandues. Dans leur propre intérêt, Citrix Online recommande aux utilisateurs de configurer leur navigateur afin qu'il utilise un cryptage renforcé par défaut dès que possible et de toujours installer les derniers correctifs de sécurité disponibles pour leur navigateur et leur système d'exploitation.

Lorsque des connexions SSL/TLS sont établies avec le site Web GoToAssist et entre les composants GoToAssist Corporate, les serveurs Citrix Online s'authentifient auprès des clients à l'aide de certificats de clé publique VeriSign/Thawte. Pour une protection renforcée contre les attaques d'infrastructure, une authentification mutuelle basée sur certificat est mise en œuvre pour toutes les liaisons entre serveurs (MCS à MCS, MCS au Gestionnaire, par exemple). Ces mesures d'authentification renforcées empêchent les éventuels fraudeurs de faire passer leur machine pour un serveur d'infrastructure ou de s'immiscer dans des sessions d'assistance.

Couche de sécurité des paquets multicast

Outre la sécurité déjà offerte par les protocoles SSL/TLS, des fonctions de protection supplémentaires viennent sécuriser de bout en bout les données de paquets multicast. Tout particulièrement, les données de session multicast sont protégées par un cryptage de bout en bout et des mécanismes d'intégrité qui empêchent quiconque ayant accès à nos serveurs de communication (que cette personne soit bien intentionnée ou non) d'écouter clandestinement une session GoToAssist Corporate ou de manipuler les données sans être repérée. Seule la solution GoToAssist Corporate offre un tel niveau de confidentialité et d'intégrité en matière de communication. Les communications d'entreprise ne sont jamais visibles par des tiers, qu'il s'agisse d'un utilisateur n'ayant pas été invité à une session d'assistance donnée ou de Citrix Online elle-même.

La clé MPSL est mise en œuvre sur la base d'un accord de clé authentifié SRP-6 basé sur clé publique utilisant un module de 1024 bits pour établir une clé de cryptage principale. (Voir http://srp.stanford.edu/design.html.) Cette clé de cryptage principale est ensuite utilisée pour distribuer la clé symétrique de groupe à l'aide de l'algorithme d'enveloppe de clé AES, IETF RFC 3394. Tous les composants de la clé sont créés à l'aide d'un générateur de nombres pseudo-aléatoires compatible FIPS alimenté à l'aide de données d'entropie recueillies sur la machine hôte à partir de différentes sources pendant l'exécution. Ces méthodes d'échange et de génération de clé dynamiques et robustes offrent une protection renforcée contre le décryptage des clés.

MPSL renforce la protection des données de paquets multicast contre l'écoute clandestine en utilisant un cryptage AES de 128 bits en mode compteur. Les données de texte brut sont comprimées avant cryptage à l'aide de techniques propriétaires hautes performances pour optimiser la bande passante. L'intégrité des données est protégée en incluant une valeur de contrôle d'intégrité générée avec l'algorithme HMAC-SHA-1. GoToAssist Corporate utilise des mesures cryptographiques renforcées qui sont conformes aux normes industrielles ; les clients ont ainsi la garantie que les données de session d'assistance multicast sont protégées contre toute divulgation non autorisée ou toute modification non détectée.

De plus, ces fonctions de sécurité essentielles n'entraînent pas de coûts supplémentaires, de dégradation des performances ni de difficultés d'utilisation. Les données du client sont protégées par des mesures de sécurité normalisées et hautes performances à chaque session GoToAssist Corporate.

Points clés

- Le cryptage AES de 128 bits est utilisé pour la confidentialité des sessions.
- La clé de session initiale est choisie de manière aléatoire par le Gestionnaire, puis transmise aux extrémités par des canaux cryptés et authentifiés.
- Les extrémités négocient alors une clé de session finale entre elles.
- La clé de session finale n'est pas connue du Gestionnaire.
- Les serveurs de communication se contentent d'acheminer les paquets cryptés et ne disposent pas de la clé de cryptage de session.
- L'architecture de GoToAssist Corporate minimise le risque d'exposition des données de session tout en optimisant la mise en relation des agents avec les utilisateurs.

Compatibilité avec les proxy et les pare-feu

À l'instar des autres produits Citrix Online, GoToAssist Corporate inclut une logique de gestion des connexions et de détection des proxy intégrée qui permet d'automatiser l'installation des logiciels, d'éviter les (re)configurations de réseau complexes et de maximiser la productivité des utilisateurs. Les pare-feu et les proxy déjà présents sur votre réseau n'ont généralement pas besoin d'être reconfigurés pour permettre l'utilisation de GoToAssist Corporate.

Au démarrage du logiciel d'extrémité GoToAssist Corporate, l'application tente de contacter le Gestionnaire de services GoToAssist via la passerelle d'extrémité (EGW) en initiant une ou plusieurs connexions TCP sortantes protégées par SSL sur les ports 8200, 443 et/ou 80. La première connexion qui répond est utilisée, les autres sont abandonnées. Cette connexion servira de base à toutes les participations aux sessions d'assistance ultérieures en permettant la communication entre les serveurs hébergés et le bureau de l'utilisateur.

Lorsque l'utilisateur essaie de se connecter à une session d'assistance, le logiciel d'extrémité GoToAssist Corporate établit une ou plusieurs connexions supplémentaires aux serveurs de communication Citrix Online en utilisant là encore les connexions TCP protégés par SSL aux ports 8200, 443 et/ou 80. Ces connexions acheminent les données de session d'assistance durant une session active.

Pour les tâches d'optimisation de la connectivité, le logiciel d'extrémité initie également une ou plusieurs connexions TCP de courte durée sur les ports 8200, 443 et/ou 80 qui ne sont pas protégées par SSL. Ces « sondes » réseau n'acheminent aucune information sensible ou exploitable et ne présentent donc aucun risque en ce qui concerne la divulgation d'informations secrètes.

Pour une liste exhaustive des plages d'adresses IP utilisées par Citrix Online, consultez la page www.citrixonline.com/iprange.

En ajustant automatiquement les conditions du réseau local en utilisant des connexions sortantes uniquement et en sélectionnant un port déjà ouvert sur la majorité des pare-feu et proxy, GoToAssist Corporate fournit un degré élevé de compatibilité avec les mesures de sécurité réseau existantes. Contrairement à d'autres produits, GoToAssist Corporate n'exige pas des entreprises qu'elles désactivent les contrôles de sécurité du périmètre réseau existants pour permettre aux sessions d'assistance en ligne d'avoir lieu. Ces fonctions optimisent la compatibilité et la sécurité réseau globale.

Fonctions de sécurité du système d'extrémité

Le logiciel de session d'assistance en ligne doit être compatible avec une grande variété d'environnements de bureau tout en créant une extrémité sûre sur le bureau de chaque utilisateur. GoToAssist Corporate répond à ses exigences en utilisant des exécutables disponibles sur Internet qui emploient des mesures cryptographiques renforcées.

Logiciel d'extrémité signé

Le logiciel d'extrémité client GoToAssist Corporate est un exécutable Win32 qui est téléchargé sur l'ordinateur des utilisateurs. Une applet Java signée numériquement contrôle le téléchargement et vérifie l'intégrité du logiciel d'extrémité GoToAssist Corporate à partir des serveurs Citrix Online. Cela évite que l'utilisateur installe par inadvertance un cheval de Troie ou un autre logiciel malveillant imitant une application GoToAssist Corporate.

Le logiciel d'extrémité est composé de plusieurs exécutables Win32 et de bibliothèques reliées de manière dynamique. Lors du développement et du déploiement, Citrix Online suit des procédures strictes de gestion de la configuration et de contrôle de la qualité pour assurer la sécurité du logiciel. Le logiciel d'extrémité n'expose aucune interface réseau disponible en externe et ne peut pas être utilisé par des logiciels malveillants ou des virus pour exploiter ou infecter les systèmes distants. Ainsi, les différents bureaux connectés à une session d'assistance ne peuvent pas être infectés par un participant compromis.

Mise en œuvre du sous-système cryptographique

L'ensemble des fonctions cryptographiques et des protocoles de sécurité utilisés par le logiciel d'extrémité client GoToAssist Corporate sont mis en œuvre à l'aide des bibliothèques de pointe Certicom Security Builder® Crypto™ et Certicom Security Builder® SSL™, gage de tranquillité d'esprit et de hautes performances. (Voir www.certicom.com pour plus d'informations.)

L'utilisation des bibliothèques cryptographiques est limitée à l'application d'extrémité GoToAssist Corporate ; les API externes ne sont pas accessibles aux autres logiciels exécutés sur ce bureau. Tous les algorithmes d'intégrité et de cryptage, la taille de clé et les autres paramètres de cryptographie sont codés de manière statique lors de la compilation de l'application. Aucun paramètre cryptographique n'est configurable par l'utilisateur final. Par conséquent, les utilisateurs ne peuvent pas affecter la sécurité des sessions GoToAssist Corporate suite à une erreur de configuration accidentelle ou intentionnelle. Les entreprises qui utilisent GoToAssist Corporate ont la garantie que toutes les extrémités connectées bénéficient du même niveau de sécurité de session d'assistance en ligne, quel que soit le propriétaire ou l'utilisateur du bureau.

Fonctions de sécurité de l'infrastructure hébergée

Citrix Online distribue GoToAssist Corporate en utilisant un modèle de prestation de services d'application (ASP) conçu spécifiquement pour assurer un fonctionnement robuste et sûr tout en s'intégrant de manière transparente à l'infrastructure réseau et de sécurité existante de l'entreprise.

Infrastructure fiable et évolutive

L'architecture de service globale de Citrix Online a été conçue pour offrir des performances, une fiabilité et une évolutivité optimales. Le service GoToAssist Corporate est piloté par des serveurs et des équipements réseau de grande capacité et conformes aux normes industrielles qui sont équipés des tout derniers correctifs de sécurité disponibles. Des routeurs et des commutateurs redondants sont intégrés dans l'architecture pour éliminer tout point de défaillance. Des systèmes de sauvegarde et des serveurs en grappe aident à assurer un flux transparent des processus d'application, même en cas de charge importante ou d'erreur système. Pour des performances optimales, le Gestionnaire GoToAssist répartit la charge des sessions client/serveur entre des serveurs de communication dispersés géographiquement.

Sécurité physique

Tous les serveurs Web, d'application, de communication et de base de données GoToAssist Corporate sont hébergés dans des centres de données sécurisés et colocalisés. L'accès physique aux serveurs est très restreint et contrôlé en permanence. Tous les sites disposent de contrôles de l'environnement et de l'alimentation redondants.

Sécurité réseau

Citrix Online utilise des contrôles d'accès basé sur VPN, routeur et pare-feu pour protéger ses réseaux de service privé et ses serveurs dorsaux. La sécurité de l'infrastructure est constamment contrôlée et des tests de vulnérabilité sont régulièrement effectués par l'équipe interne en charge de la sécurité et par des vérificateurs indépendants.

Respect de la vie privée des clients

Parce que garder la confiance de nos clients est une priorité, Citrix Online s'engage à respecter leur vie privée. Vous trouverez un lien vers la déclaration actuelle de confidentialité de Citrix GoToAssist Corporate sur notre site Web d'assistance, à l'adresse www.citrixonline.com.

Conformité dans des environnements réglementés

Grâce à son ensemble complet de contrôles de sécurité de communication et d'application, y compris son modèle de sécurité basé sur l'autorisation client, GoToAssist Corporate peut être utilisé en toute confiance pour assurer le dépannage d'ordinateurs et d'applications exécutés dans des environnements soumis aux lois HIPAA, Gramm-Leach-Bliley Act ou Sarbanes-Oxley et exigeant des contrôles d'intégrité et de confidentialité des données performants.

Citrix Online recommande aux entreprises de passer soigneusement en revue toutes les fonctions de sécurité standard et configurables de GoToAssist Corporate dans le contexte de leurs environnements, populations d'utilisateurs et cadres réglementaires spécifiques pour déterminer les fonctions à activer et la meilleure configuration à adopter. Dans certains cas, il est conseillé de fournir des instructions d'utilisation supplémentaires aux utilisateurs afin de garantir le respect des objectifs de sécurité de toutes les parties prenantes. L'équipe de service professionnel de Citrix Online peut fournir des documentations complémentaires concernant les meilleures pratiques de déploiement et d'utilisation de GoToAssist Corporate.

Conclusion

La fonctionnalité et l'interface sécurisées et intuitives de GoToAssist Corporate en font la solution de conduite de sessions d'assistance en ligne la plus efficace du marché. Grâce à GoToAssist Corporate, les professionnels de l'informatique, du conseil et de l'assistance peuvent rapidement et facilement offrir un support technique à des clients du monde entier.

En arrière-plan, l'architecture de service hébergée de Citrix Online prend en charge de manière transparente la collaboration multipoint en fournissant un environnement sûr et fiable. Comme ce document le montre, GoToAssist Corporate offre flexibilité et facilité d'utilisation sans compromettre l'intégrité, la confidentialité ni le contrôle administratif des communications professionnelles et des équipements informatiques.

Annexe : Conformité aux normes de sécurité

GoToAssist Corporate est compatible avec les normes industrielles et des États-Unis suivantes en matière d'algorithmes cryptographiques et de protocoles de sécurité :

- Protocole TLS/SSL, version 1.0 IETF RFC 2246
- Norme AES (Advanced Encryption Standard), FIPS 197
- (Mise en œuvre validée par le FIPS, certificat NIST n°175)
- Suites de chiffrement AES pour TLS, IETF RFC 3268
- Algorithme d'enveloppe de clé AES, IETF RFC 3394
- RSA, PKCS n°1
- SHA-1, FIPS 180-1 (mise en œuvre validée par le FIPS, certificat NIST n°89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Génération de nombres pseudo-aléatoires, ANSI X9.62 et FIPS 140-2

Citrix Online

Division Citrix Online

Informations sur le produit :
www.citrixonline.com

Demandes de renseignements :
France@citrixonline.com
Téléphone : +33 (0) 1 73 04 56 50

Presse :
pr@citrixonline.com
Téléphone : +441 49 454 1715

www.citrixonline.com

Pour plus d'informations sur Citrix GoToAssist Corporate, visitez www.citrixonline.com

À propos de Citrix Online

Citrix Online offre des solutions en ligne sûres et faciles à utiliser qui permettent de travailler en tout lieu avec des clients du monde entier. Qu'ils utilisent GoToMyPC® pour travailler sur un PC distant, GoToAssist® pour assister des clients ou GoToMeeting® pour tenir des Webinaires et des réunions en ligne, nos clients (soit plus de 35 000 entreprises et des centaines de milliers d'individus) augmentent leur productivité, réduisent leurs coûts de déplacement et bénéficient d'une amélioration globale des ventes, de la formation et du service. Division de Citrix Systems, Inc. (Nasdaq : CTXS), la société est basée à Santa Barbara, Californie. Pour plus d'informations, visitez www.citrixonline.com ou composez le 805-690-6400.

18191/17.11.08/PDF