

Citrix utredningsrapport om säkerhet för GoToAssist Corporate

GoToAssist Corporate har oavbrutet dataskydd som tar hand om såväl passiva som aktiva attacker mot konfidentialitet, integritet och tillgänglighet.

Innehållsförteckning

Innehåll och målgrupp	3
Inledning	3
GoToAssist hierarki för tjänsteleveranser	4
Definitioner	5
Programsäkerhet	6
Autentisering	7
Skydd för kundens dator och data	7
Säkerhetsfunktioner vid kommunikation	8
Konfidentialitet och integritet vid kommunikation.....	9
Säkerhet i TCP-skiktet	9
Säkerhetsskikt för multisändningar	10
Brandväggs- och proxykompatibilitet.....	11
Säkerhetsfunktioner i klientsystem	12
Signerat klientprogram.....	12
Implementering av kryptografiska subsystem	12
Säkerhetsfunktioner i värdinfrastrukturen	13
Skalbar och tillförlitlig infrastruktur	13
Fysisk säkerhet	13
Nätverkssäkerhet	13
Kundens integritet	13
Efterlevnad i reglerade miljöer	14
Sammanfattning	14
Bilaga: Efterlevnad av säkerhetsstandarder	15

Innehåll och målgrupp

Den här handboken riktar sig till Citrix® GoToAssist® Corporate- kunder och andra intressenter som behöver veta hur GoToAssist påverkar säkerhetsrisker vid informationsspridning och efterlevnad i arbetsmiljön.

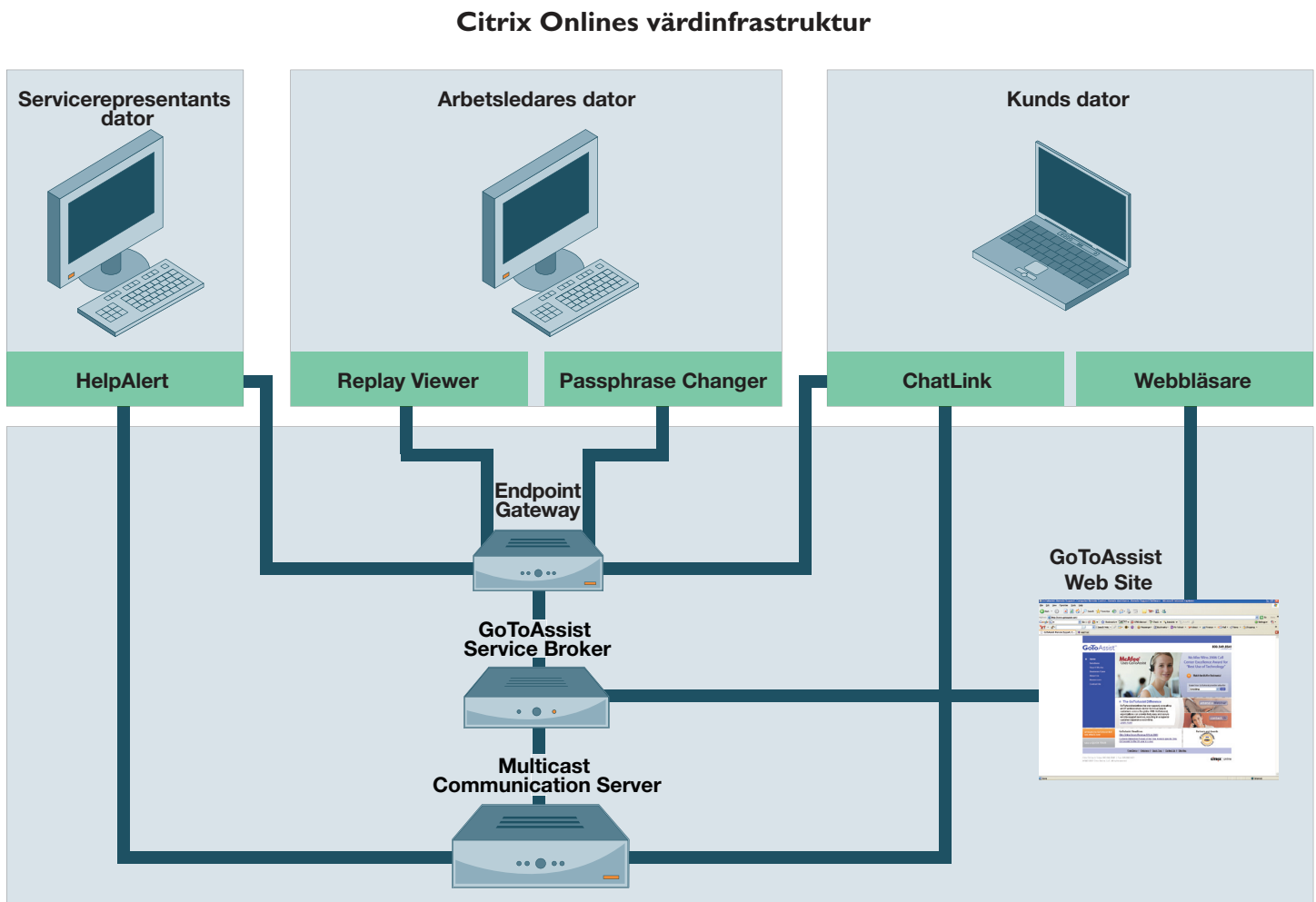
Inledning

GoToAssist Corporate är en värdtjänst med vilken fjärrsupport kan levereras till Windowsbaserade datorer. Via GoToAssist Corporate kan du som användare begära support från en representant varvid han/hon kan granska och vid behov fjärrstyra din dator.

I detta dokument beskrivs funktionerna för informationssäkerhet i GoToAssist Corporate. Du förväntas ha en grundläggande uppfattning om produkten och dess funktioner. Mer information om GoToAssist Corporate finner du online på www.citrixonline.com eller genom att kontakta en representant från Citrix Online.

GoToAssist Corporates hierarki för tjänsteleveranser

I nedanstående schema visas alla viktiga komponenter och kommunikationsvägar i GoToAssist Corporate.



Definitioner

HelpAlert: Körbart Win32-program som finns i tjänsterepresentantens dator och används för att ta emot och svara på inkommande frågor från kunderna.

ChatLink: Klientprogram som används för textbaserad kommunikation mellan en kund och en representant.

Webbläsare: Standardwebbläsare som t.ex. Firefox, Internet Explorer etc.

Replay Viewer: Klientprogram som gör det möjligt för företagsledare, gruppleddare och arbetsledare för representanter att spela upp inspelade GoToAssist Corporate-sessioner. Fjärrskärmsdelning, lokalskrämsdelning, chatt och fjärrdiagnostik kan spelas upp.

Passphrase Changer: Klientprogram för byte av en lösenfras som används för att skydda krypterad åtkomst till inspelade sessioner.

GoToAssist Web Site: Webbprogram som ger åtkomst till GoToAssists webbplats och webbaserade interna och externa administrationsportaler.

GoToAssist Service Broker: Webbprogram för konto- och tjänstehantering, beständig lagring och rapportfunktioner i Go ToAssist Corporate.

Multicast Communication Server: En av många globalt spridda servrar som används för att realisera en mängd olika lättillgängliga kommunikationstjänster med multi- och enkelsändningar.

Endpoint Gateway: En specialanpassad gateway som används i olika klientprogram för säker åtkomst till GoToAssist Service Broker i olika syften med hjälp av fjärrmanövrer.

Programsäkerhet

I GoToAssist Corporate finns åtkomst till en mängd resurser och tjänster via ett rollbaserat styrsystem som aktiveras av olika komponenter i tjänsteleveransen. Rollerna och tillhörande termer definieras i nedanstående tabell:

Roller

Administratör (eller admin)	En anställd hos Citrix Online som skapar Grupper och Portaler i ett företags GoToAssist Corporate Management Center. En administratör kan skapa, modifiera och radera konton, portaler, företags- och gruppleddare, ändra abonnemangs- och prisinformation samt utföra andra administrativa funktioner i GoToAssist Corporate.
Företag	GoToAssist Corporate-kund för vilken portaler sätts upp.
Företagsledare	En anställd i ett klientföretag som har åtkomst till företagets GoToAssist Corporate Management Center. Tillåts modifiera konton, portalgrupper och representanter som tillhör detta konto.
Kund	Den person som begär support från klientföretaget via GoToAssist Corporate.
Grupp/team	Samling av representanter som tilldelas en särskild portal. Varje representant tillhör en grupp eller ett team. Varje grupp eller team tilldelas exakt en portal. Grupper/team innehåller några standardinställningar för representanterna.
Grupp-/teamledare	En anställd som godkänts av företagsledaren att ändra vissa aspekter för ett team och teamets tillhörande portal och representanter.
Representant	En supportperson som svarar på kundfrågor via HelpAlert.

Autentisering

Administratörer, chefer och representanter i GoToAssist Corporate är autentiserade att använda ett kontonamn och ett starkt lösenord.

Lösenord styrs av följande praxis:

Starka lösenord: Ett starkt lösenord är 8-32 tecken långt och måste innehålla minst tre av de fyra följande teckentyperna: stora bokstäver [A-Z], små bokstäver [a-z], siffror [0-9] och specialtecken [-~!@#\$%^&*()_+={}|~\.:;''<>,.?/]. Ett starkt lösenord får inte vara detsamma som inloggningsnamnet eller för- eller efternamn som registrerats för kontot. Lösenorden kontrolleras med avseende på styrka när de initieras eller ändras.

Lösenords giltighetstid: Lösenordets giltighetstid är konfigurerbar (min: 10 dagar, max: 120 dagar, standard: 90 dagar). Om kontoinnehavaren loggar in och lösenordet har gått ut måste han/hon ändra det.

Lösenordshistorik: Historik över lösenord lagras. Ett lösenord kan inte ändras till ett som redan finns i historiken. Historiklängden kan ställas in (min: 1, max: 5, standard: 3).

Kontospärr: Efter tre på varandra följande misslyckade inloggningsförsök spärras kontot. Det innebär att kontoinnehavaren inte kan logga in förrän efter en konfigurerbar tidsperiod (min: 5 minuter, max: 30 minuter, standard: 5 minuter). Efter det att spärrperioden löpt ut, kan kontoinnehavaren försöka logga in på kontot igen.

Ett annat konfigurerbart alternativ är kontospärr som måste återställas manuellt. Efter ett konfigurerbart antal misslyckade inloggningsförsök, spärras kontot. Det innebär att kontoinnehavaren inte kan logga in på sitt konto förrän lösenordet återställts av en annan behörig kontoinnehavare. Kontospärren aktiveras efter ett konfigurerbart antal försök (min: 10, max: 50, standard: 10).

Skydd för kundens dator och data

En viktig del i GoToAssist Corporates säkerhet är den tillståndsbaserade åtkomstkontrollen för skydd av kundens datorer och data som finns i dem.

För det första måste alla GoToAssist Corporate-sessioner initieras av fjärrkunden. GoToAssist Corporate är inte avsedd för oövakade supportaktiviteter.

För det andra uppmanas kunden alltid att i förväg ge sitt tillstånd till skärmdelning, fjärrkontroll eller överföring av diagnosdata, filer eller annan information.

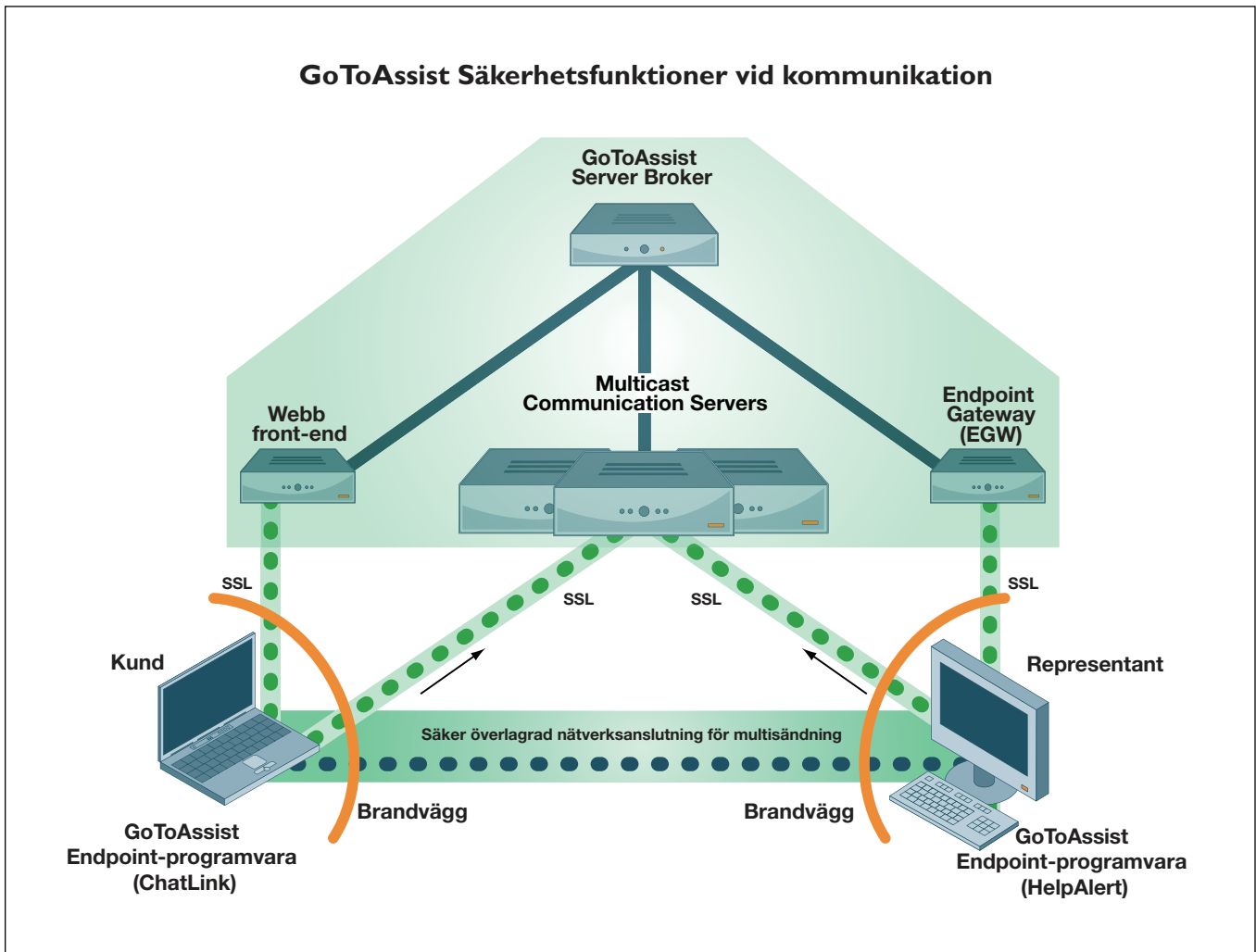
Om fjärrkontroll och skärmdelning auktoriserats, kan kunden vid alla tillfällen se vad representanten gör. Dessutom kan kunden enkelt återta kontrollen eller avsluta sessionen vid valfri tidpunkt.

Lokala säkerhetskontroller på kundens dator åsidosätts aldrig. Kunden eller representanten måste fortfarande ange autentiseringsinformation för Windows eller program.

Slutligen loggas alla anslutningsaktiviteter. Skärmdelning och chattsession kan alternativt spelas in och spelas upp för granskning vid senare tillfälle.

Säkerhetsfunktioner vid kommunikation

Kommunikation mellan deltagare i en GoToAssist Corporate-session sker via en överlagrad nätverksstack för multisändning som logiskt ligger överst på den konventionella TCP/IP-stacken i varje användares dator. Det här nätverket som realiseras via en samling servrar för multisändningskommunikation (MCS) drivs av Citrix Online. Kommunikationsarkitekturen framgår av figuren nedan.



Deltagarna i en GoToAssist Corporate-session ("ändpunkter") kommunicerar med Citrix Onlines servrar och gatewayer för infrastrukturkommunikation med hjälp av utgående TCP/IP-anlutningar på portarna 8200, 443 och 80. Eftersom GoToAssist Corporate är en webbaserad värdtjänst kan deltagarna lokaliseras var som helst på Internet – vid ett fjärrkontor, hemma, vid ett företagscenter eller anslutna till ett annat företags nätverk.

Åtkomst när som helst/var som helst till GoToAssist Corporate-tjänsten medför maximal flexibilitet och anslutningsbarhet. Men för att bevara konfidentialiteten och integriteten vid privat affärskommunikation, innehåller även GoToAssist Corporate robusta säkerhetsfunktioner när du kommunicerar.

Konfidentialitet och integritet vid kommunikation

GoToAssist Corporate har oavbrutet dataskydd som tar hand om såväl passiva som aktiva attacker mot konfidentialitet, integritet och tillgänglighet. Alla GoToAssist Corporate-anslutningar är krypterade hela vägen och enbart åtkomliga av behöriga deltagare i supportsessioner.

Skärmdelningsdata, tangentbords-/musdata och textchattsinformation visas aldrig i okrypterad form under det att de temporärt befinner sig på Citrix Onlines kommunikationsservrar eller under överföring i offentliga eller privata nätverk.

När inspelning är avaktiverat, lagras inte nyckeln till GoToAssist Corporate-sessionen i någon form på Citrix Online-servrarna. På så sätt kan ett intrång i en server inte avslöja nyckeln till en krypterad ström som hackaren kan ha fångat in.

När inspelning aktiverats, lagras chatt, skärmdelning och skärmgranskningsdata i krypterad form. Sessionsnyckeln lagras också men är skyddad av en 1024-bitars RSA offentlig/privat nyckelkryptering. En portalspecifik offentlig nyckel används för att kryptera sessionsnyckeln före lagring. Det behövs tre poster för uppspelning, nämligen sessionsinspelningen, den krypterade sessionsnyckeln och den privata nyckeln till portalen.

Säkerhetskontroller för kommunikation baserade på stark kryptering implementeras i två skikt, nämligen "TCP-skiktet" respektive "MPSL-skiktet" (Multicast Packet Security Layer - säkerhetsskikt för multisändningspaket).

Säkerhet i TCP-skiktet

IETF-standardprotokollen Secure Sockets Layer (SSL) och Transport Layer Security (TLS) används för att skydda all kommunikation mellan ändpunkter. För maximalt skydd mot tjuvlyssning, modifiering eller uppspelningsattacker, är 1024-bitars RSA med 128-bitars AES-CBC och HMAC-SHA1 det enda SSL-chiffreeringspaket som kan hantera icke webbaserade TCP-anslutningar. Men för maximal kompatibilitet med nästan alla webbläsare i olika datorer, kan GoToAssist-webbplatsen hantera ingående anslutningar med hjälp av de flesta SSL-chiffreeringspaketen som stöds. För kundens eget skydd rekommenderar Citrix Online att han/hon konfigurerar sin webbläsare så att stark kryptografi används som standard och alltid installerar de senaste säkerhetsuppdateringarna för operativsystemet och webbläsaren.

När SSL/TLS-anslutningar upprättats till GoToAssists webbplats och mellan komponenterna i GoToAssist Corporate autentiserar Citrix Onlines servrar sig själva till klienter genom att använda VeriSign/Thawte offentliga nyckelcertifikat. För ytterligare skydd mot infrastrukturattacker används ömsesidig certifikatsbaserad autentisering på alla server-till-server-länkar (t.ex. MCS-till-MCS, MCS-till-Broker). Dessa starka autentiseringsåtgärder förhindrar eventuella hackers från att maskera sig som infrastruktursservrar eller för att ta sig in mitt i supportsessionskommunikationer.

Säkerhetsskikt för multisändningar

Ytterligare funktioner ger oavbrutet skydd för multisändningspaketdata, oberoende av de som tillhandahålls av SSL/TLS. Alla sessionsdata för multisändning skyddas av obruten kryptering och integritetsmekanismer som förhindrar någon med åtkomst till våra kommunikationsservrar (såväl vänligt som fientligt inställda) från tjuvlyssning av en GoToAssist Corporate-session eller manipulering av data utan upptäckt. Den här extra kommunikations- och konfidentialitetsnivån är unik för GoToAssist Corporate. Företagskommunikationer är aldrig synliga för utomstående, inklusive de två användarna som inte inbjuds till en given supportsession och i själva Citrix Online.

Etablering av MPSSL-nyckel åstadkoms med hjälp av ett offentlig-nyckel-baserat SRP-6 autentiserat nyckelavtal via en 1024-bitars modul för att etablera en krypteringsnyckel för primär nyckel. (Se <http://srp.stanford.edu/design.html>). Krypteringsnyckeln för primär nyckel används därefter för gruppsymmetrisk nyckeldistribution via AES-nyckelkrypteringsalgoritmen, IETF RFC 3394. Allt nyckelmaterial genereras med hjälp av en FIPS-kompatibel pseudoslumpsiffregenerator matad med entropidata som insamlats vid körtid från flera källor på värddatorn. Den här robusta, dynamiska nyckelgenereringen och utbytesmetoden ger starkt skydd mot nyckelgissning och -knäckning.

MPSSL skyddar dessutom multisändningspaketdata från tjuvlyssning med hjälp av en 128-bitars AES-kryptering i Counter-läge. Oformaterade textdata komprimeras före krypteringen med hjälp av tillverkarspecifika högpresterande tekniker för att optimera bandbredden. Skydd av dataintegritet uppnås genom ett integritetskontrollvärde som genereras via HMAC-SHA-1-algoritmen. Eftersom GoToAssist Corporate använder mycket stark kryptering enligt branschstandard kan kunderna vara helt förvissade om att supportsessionsdata med multisändningar skyddas mot obehörigt avslöjande eller oupptäckt modifiering.

Dessutom förknippas inga extra avgifter, prestandaförsämringar eller användbarhetsbegränsningar med dessa viktiga säkerhetsfunktioner för kommunikation. Höga prestanda och standardbaserad datasäkerhet är "inbyggda" egenskaper i varje GoToAssist Corporate-session.

Nyckelpunkter

- 128-bitars AES-kryptering används för sessionskonfidentialitet.
- Initial sessionsnyckel väljs slumpmässigt av Broker och skickas därefter till ändpunkterna över autentiserade och krypterade kanaler.
- Ändpunkterna tar bland sig själva fram en slutlig sessionsnyckel.
- Den slutliga sessionsnyckeln är inte känd av Broker.
- Kommunikationsservrarna dirigerar bara krypterade paket och har inte sessionens krypteringsnyckel.
- Tack vare hierarkin i GoToAssist Corporate minimeras risken för exponering av sessionsdata medan dess förmåga att länka operatörerna till de som begär hjälp maximeras.

Brandväggs- och proxykompatibilitet

Liksom i andra Citrix Online-produkter finns det inbyggd proxydetektion och anslutningslogik i GoToAssist Corporate. På så sätt kan du automatisera programinstallationen, undvika behovet av (om)konfiguration av komplexa nätverk och maximera användarproduktiviteten. De brandväggar och proxyer som redan finns i ditt nätverk behöver i regel ingen speciell konfiguration för att GoToAssist Corporate ska kunna användas.

När klientprogrammet GoToAssist Corporate startas, försöker det kontakta GoToAssist Service Broker via EGW-gatewayen (Endpoint Gateway) genom att initiera en eller flera utgående SSL-skyddade TCP-anslutningar på portarna 8200, 443 och/eller 80. Den av anslutningarna som svarar först används och de andra släpps. Denna anslutning utgör grunden för deltagande i alla framtida supportsessioner genom att kommunikation mellan värdserverar och användardatorer aktiveras.

När användaren försöker gå med i en supportsession upprättar klientprogrammet GoToAssist Corporate en eller fler ytterligare anslutningar till Citrix Onlines kommunikationsserverar varvid de SSL-skyddade TCP-anslutningarna på portarna 8200, 443 och/eller 80 används. Via dessa anslutningar överförs supportsessionsdata under en aktiv session.

Klientprogrammet initierar dessutom, för optimering av anslutningsbarhet, en eller flera kortlivade TCP-anslutningar på portarna 8200, 443 och/eller 80 som inte är SSL-skyddade. Dessa "nätverkssonder" innehåller ingen känslig eller exploaterbar information och utgör ingen risk att känslig information avslöjas.

En fullständig lista på IP-adresser som används av Citrix Online finns på www.citrixonline.com/iprange.

GoToAssist Corporate är mycket kompatibel med befintliga nätverkssäkerhetsåtgärder genom att tillstånden för det lokala nätverket justeras automatiskt enbart via de utgående anslutningar och en port som redan är öppen i de flesta brandväggar och proxyer väljs. Till skillnad från andra produkter kräver GoToAssist Corporate inte att företag avaktiverar befintliga säkerhetskontroller vid nätverkets yttre gräns för att tillåta supportkommunikation online. De här funktionerna maximerar såväl kompatibilitet som generell nätverkssäkerhet.

Säkerhetsfunktioner i klientsystem

Programvaran för onlinesupport måste vara kompatibel med många olika datormiljöer och ändå skapa en säker ändpunkt på varje användares dator. GoToAssist Corporate uppnår detta genom att hämtbara körbara webbfiler med starka krypteringsåtgärder används.

Signerat klientprogram

Klientprogrammet GoToAssist Corporate är en körbar Win32-fil som hämtas till en användares dator. En digitalt signerad Java-applet används för att medla hämtningen och verifiera integriteten i klientprogrammet GoToAssist Corporates från Citrix Online-servrar. Detta skyddar användaren från att oavsiktligt installera en trojan eller annat skadligt program som ger sig ut för att vara GoToAssist Corporate-programvara.

Klientprogrammet är sammansatt av flera körbara Win32-filer och dynamiskt länkade bibliotek. För att garantera programsäkerhet följer Citrix Online strikta rutiner för kvalitetskontroll och configurationshantering under utveckling och distribution. I klientprogrammet visas inga externt tillgängliga nätverksgränssnitt och det kan inte nyttjas av sabotageprogram eller virus för att exploatera eller infektera fjärrsystem. Detta skyddar andra datorer som deltar i en supportsession från att bli infekterade av en komprometterad värd som nyttjas av en annan deltagare.

Implementering av kryptografiska subsystem

Alla kryptografiska funktioner och säkerhetsprotokoll som används av klientprogrammet GoToAssist Corporate implementeras med hjälp av de toppklassade biblioteken Certicom Security Builder® Crypto™ och Certicom Security Builder® SSL™ för försäkring och höga prestanda. (Mer information finns på www.certicom.com.)

Användningen av de kryptografiska biblioteken begränsas till klientprogrammet GoToAssist Corporate, inga externa API:er visas för åtkomst av andra program som körs på datorn. Alla krypterings- och integritetsalgoritmer, nyckelstorlek och andra kryptografiska parametrar kodas statiskt när programmet kompileras. Det är omöjligt för en användare att försvaga säkerheten i en GoToAssist Corporate-session genom oavsiktlig eller avsiktlig felkonfigurering, eftersom det inte finns några kryptografiska inställningar som slutanvändaren kan konfigurera. Ett företag som använder GoToAssist Corporate kan vara säker på att samma säkerhetsnivå för en supportsession online finns hos alla deltagande ändpunkter oberoende av vem som äger eller använder respektive dator.

Säkerhetsfunktioner i värdinfrastrukturen

Citrix Online levererar GoToAssist Corporate med hjälp av en ASP-modell som uttryckligen utvecklats för att kunna säkerställa robust och säker drift under det att den integreras fullständigt med ett företags befintliga nätverk och säkerhetsstruktur.

Skalbar och tillförlitlig infrastruktur

Citrix Onlines globala tjänstehierarki har utvecklats för maximal prestanda, tillförlitlighet och skalbarhet. GoToAssist Corporate-tjänsten drivs av högeffektiva servrar och nätverksenheter i branschstandard med de senaste säkerhetsuppdateringarna på plats. Redundantswitchar och -routrar är inbyggda i hierarkin för att säkerställa att det aldrig finns en enda felpunkt. Med hjälp av klustrade servrar och backupsystem kan ett oavbrutet flöde av programprocesser garanteras - även vid hög belastning eller systemfel. Optimala prestanda erhålls genom att GoToAssist Broker fördelar belastningen på klient/server-sessionerna över geografiskt spridda kommunikationsservrar.

Fysisk säkerhet

Alla GoToAssist Corporates webb-, program-, kommunikations- och databasservrar befinner sig i säkra datacenterlokaler. Den fysiska åtkomsten till serverna är strängt begränsad och övervakas kontinuerligt. Alla anläggningar har reservkraft och miljökontroller.

Nätverkssäkerhet

Citrix Online använder brandvägg, router och VPN-baserade åtkomstkontroller för att säkra våra privattjänstenätverk och backendservrar. Infrastruktursäkerhet övervakas kontinuerligt och sårbarhetstestning genomförs regelbundet av intern säkerhetspersonal och utomstående kontrollanter.

Kundens integritet

Det är viktigt för oss på Citrix Online att du som användare har ett fortlöpande förtroende och vi respekterar således din integritet. En länk till en kopia av Citrix GoToAssist Corporates gällande sekretesspolicy finns på webbplatsen www.citrixonline.com.

Efterlevnad i reglerade miljöer

GoToAssist Corporate kan, tack vare sina omfattande säkerhetskontroller av program och kommunikationer samt den kundgodkända, behörighetsbaserade säkerhetsmodellen, användas med tillförsikt för att stödja datorer och program i miljöer som lyder under HIPAA, Gramm-Leach-Bliley Act eller Sarbanes-Oxley-bestämmelserna, vari kontroll av datakonfidentialitet och integritet måste göras.

Citrix Online rekommenderar att organisationer noggrant granskar alla GoToAssist Corporates standard- och konfigurerbara säkerhetsfunktioner med avseende på sina specifika miljöer, antal användare och policykrav för att bestämma vilka funktioner som ska aktiveras och hur de bäst ska konfigureras. I vissa fall rekommenderas en fördjupad användarvägledning för att säkerställa att alla intressenters mål uppfylls på ett tillfredsställande sätt. Citrix Onlines professionella team kan tillhandahålla mer material om bästa tillvägagångssätt för distribution och användning av GoToAssist Corporate.

Sammanfattning

GoToAssist Corporates intuitiva och säkra gränssnitt och funktioner gör det till den effektivaste lösningen för supportsessioner online. Supporten, rådgivningen och IT-proffsen för GoToAssist Corporate kan snabbt och enkelt ge teknisk hjälp till kunder över hela världen.

Bakom scenen stödjer Citrix Onlines värdtjänst ett transparent flerpunktssamarbete genom att tillhandahålla en säker, tillförlitlig miljö. Som framgår i detta dokument, främjar GoToAssist Corporate användarvänlighet och flexibilitet utan att göra avkall på integritet, sekretess eller den administrativa kontrollen över företagets kommunikation eller IT-tillgångar.

Bilaga:

Efterlevnad av säkerhetsstandarder

GoToAssist Corporate uppfyller följande bransch- och USA- standarder för kryptografiska algoritmer och säkerhetsprotokoll:

- TLS/SSL-protokollet, version 1.0 IETF RFC 2246
- Avancerad krypteringsstandard (AES), FIPS 197
- (FIPS-validerad implementering, NIST-certifikat nr 175)
- AES-chiffreringspaket för TLS, IETF RFC 3268
- AES-nyckelkrypteringsalgoritm, IETF RFC 3394
- RSA, PKCS nr 1
- SHA-1, FIPS 180-1 (FIPS-validerad implementering, NIST-certifikat nr 89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudoslumpsiffregenerering, ANSI X9.62 och FIPS 140-2

Citrix Online

[Citrix Online division](#)

[Produktinformation:](#)
www.citrixonline.com

[Säljfrågor:](#)
Nordic@citrixonline.com
Telefon: (+45) 47334123

[Mediefrågor:](#)
pr@citrixonline.com
Telefon: +441 49 454 1715

www.citrixonline.com

Mer information om Citrix
GoToAssist Corporate finns
på www.citrixonline.com

[Om Citrix Online](#)

Citrix Online erbjuder säkra, lättanvända onlinelösningar som gör det möjligt för människor att arbeta var som helst med vem som helst. Oavsett om de väljer GoToMyPC® för åtkomst och arbete på en fjärrdator, GoToAssist® för att ge support till kunder eller GoToMeeting® för att genomföra onlinemöten och webbaserade seminarier, ökar våra kunder – fler än 35 000 företag och hundratusentals privatkunder – sin produktivitet, minskar sina resekostnader och förbättrar försäljningen, utbildningen och servicen globalt. Företaget som är en division inom Citrix Systems, Inc. (Nasdaq: CTXS), har sitt huvudkontor i Santa Barbara, Kalifornien. För mer information, besök www.citrixonline.com eller ring +1-805-690-6400.

©2008 Citrix Online, LLC. Med ensamrätt. Citrix® är ett registrerat varumärke som tillhör Citrix Systems, Inc. i USA och andra länder. GoToMyPC®, GoToAssist® och GoToMeeting® är varumärken eller registrerade varumärken som tillhör Citrix Online, LLC i USA och andra länder. Övriga varumärken och registrerade varumärken tillhör respektive ägare.

18191/17.11.08/PDF

CITRIX® | online

www.citrixonline.com