GoToAssist

Security White Paper

GoToAssist provides robust end-to-end data security measures that defend against both passive and active attacks on confidentiality, integrity and availability.

www.gotoassist.com

by **CITRIX**

Scope and audience

This guide is for Citrix GoToAssist customers and other stakeholders who need to understand how GoToAssist impacts information security risk and compliance in their environment.

This document solely addresses the GoToAssist product. For information about GoToAssist Corporate, please see the GoToAssist Corporate Security White Paper.

Introduction

GoToAssist is a hosted service that enables IT and support professionals to deliver remote support to computers and servers. GoToAssist allows a support representative to view and control an end user's Windows-based PC or Mac computer remotely, from a PC, Mac or iPad.

GoToAssist's optional Monitoring module allows managed service providers, IT managers and consultants to monitor server health and performance, inventory IT assets, including software, and track network usage patterns.

This document focuses on the information security features of GoToAssist. The reader is assumed to have a basic understanding of the product and its features. Additional materials on GoToAssist may be found online at www. gotoassist.com or by contacting a Citrix Online representative.

Application security

GoToAssist provides access to a variety of resources and services using a role-based access control system that is enforced by the various service delivery components. The roles and related terms are defined in the table below:

Roles

Account Administrator	A Citrix Online employee who performs administrative functions pertaining to end users. Account administrators can create, modify and delete Support Provider accounts and modify subscription data.
Network Administrator	A Citrix Online employee who maintains the GoToAssist service delivery infrastructure. Network administrators can provision and maintain infrastructure components.
Customer	The person requesting support from the client company via GoToAssist.
Support Provider	The support person who initiates GoToAssist sessions in order to provide remote support to Customers.

Definitions

Support Provider Software

Installed Win32 software that resides on the Support Provider's computer and enables the Support Provider to create support sessions.

Customer Software

Endpoint application that executes on the Customer's computer and enables the Support provider to provide support.

Browser

Standard Internet web browser, such as Firefox®, Internet Explorer®, etc.

GoToAssist Website

Web application that facilitates the establishment of support sessions between the Support Provider and Customer.

GoToAssist Service Broker

Web application that provides GoToAssist account and service management and reporting functions.

Multicast Communication Server

One of a fleet of globally distributed servers used to realize a variety of high availability unicast and multicast communication services.

Endpoint Gateway

A special-purpose gateway used by the endpoint software to securely access the GoToAssist Service Broker for a variety of purposes using remote procedure calls.

Authentication

GoToAssist support providers are identified by their email address and authenticated using a strong password.

Passwords are governed by the following policies:

Strong passwords: A strong password must be a minimum of 8 characters in length and must contain both letters and numbers. Passwords are checked for strength when established or changed.

Account lockout: After five consecutive failed log-in attempts, the account is put into a mandatory soft-lockout state. This means that the account holder will not be able to log in for five minutes. After the lockout period expires, the account holder will be able to attempt to log in to his or her account again.

Protection of customer computer and data

An essential part of GoToAssist's security is its permission-based access control model for protecting access to the customer's computer and the data contained therein.

During customer-attended live support sessions, the customer is always prompted for permission before any screen sharing, remote control or transfer of diagnostic data, files or other information is initiated.

Once remote control and screen sharing have been authorized, the customer can watch what the representative does at all times. Further, the customer can easily take control back or terminate the session at any time.

Secure unattended support

The Unattended Support feature allows the support provider to fix problems on the customer's PC or Mac, even if the customer is not present to partici-pate in a GoToAssist session. Unattended Support can be set up in one of two ways – either during a customer-attended support session ("In-Session Setup" – available only with a customer on a Windows PC) or using an out-of-session installer (can be used on PC or Mac).

In-Session Setup: Once the customer and support provider have entered a support session, the support provider may request unattended support privileges. When a support provider requests unattended support privileges, the customer is prompted for approval and must give explicit consent – the support provider is not allowed to interact with the approval dialog on behalf of the customer.

Out-of-Session Installer: After securely logging in to the GoToAssist web-site, the support representative can download an installer, which allows installation of unattended support on any PC or Mac machines for which the support representative has Administrator access. This facilitates setup on a large number of machines on a LAN, for example.

In-Session Security: When the support provider initiates an unattended sup-port session, the customer's machine is automatically locked, and the support provider must provide any Windows or application authentication credentials required when establishing (or initiating) an unattended support session. Local security controls on the customer's computer are never overridden.

If the support provider requests an unattended support session while the customer is present at their computer, the customer may choose to disallow access. If the customer returns to the machine while a session is in progress, they may end the session at any time.

The customer can permanently revoke the support provider's unattended support privileges at any time.

Communications security features

Communication between participants in a GoToAssist session occurs via an overlay multicast networking stack that logically sits on top of the conven-tional TCP/IP stack within each user's computer. This network is provided by a collection of Multicast Communication Servers (MCS) operated by Citrix Online. The communications architecture is summarized in the figure below.

GoToAssist session participants ("endpoints") communicate with Citrix Online infrastructure communication servers and gateways using outbound TCP connections on ports 8200, 443 or 80, depending on availability. Because GoToAssist is a hosted web-based service, participants can be located any-where on the Internet — at a remote office, at home, at a business center or connected to another company's network.

GoToAssist Remote Support Technology Architecture
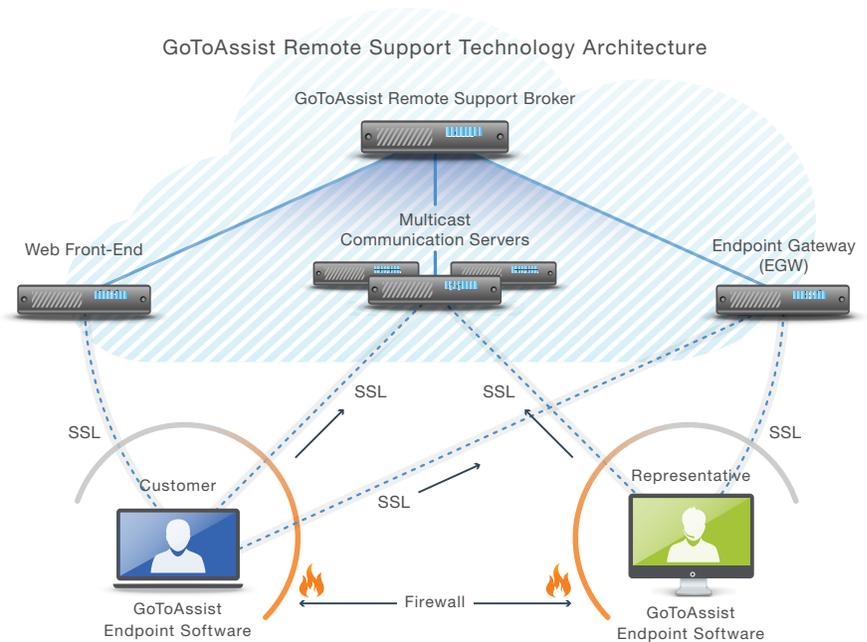
Figure 1: GoToAssist Remote Support Technology Architecture

Anytime/anywhere access to the GoToAssist service provides maximum flexibility and connectivity. However, to preserve the confidentiality and integrity of private business communication, GoToAssist also incorporates robust communication security features.

Communications confidentiality and integrity

GoToAssist provides true "end-to-end" data security measures that address both passive and active attacks against confidentiality, integrity and availability. All GoToAssist connections are "end-to-end" encrypted and accessible only by authorized support session participants.

Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are never exposed in unencrypted form while temporarily resident within Citrix Online communication servers or during transmission across public or private networks.

The GoToAssist session key is not kept on Citrix Online servers in any form and cannot be discovered or derived by Citrix Online servers or personnel. Thus, breaking into a server cannot reveal the key for any encrypted stream that the intruder may have captured.

Communications security controls based on strong cryptography are implemented at two layers: the "TCP layer" and the "Multicast Packet Security Layer" (MPSL).

TCP layer security

IETF-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to protect all communication between endpoints. To provide maximum protection against eavesdropping, modification or replay attacks, the only SSL cipher suite supported for non-website TCP connections

is 1024-bit RSA with 128-bit AES-CBC and HMAC-SHA1. However, for maximum compatibility with nearly any web browser on any user's desktop, the GoToAssist website supports inbound connections using most supported SSL cipher suites. For the customers' own protection, Citrix Online recommends that they configure their browsers to use strong cryptography by default whenever possible and to always install the latest operating system and browser security patches.

When SSL/TLS connections are established to the GoToAssist website and between GoToAssist components, Citrix Online servers authenticate themselves to clients using VeriSign/Thawte public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., MCS-to-MCS, MCS-to-Broker). These strong authentication measures prevent would-be attackers from masquerading as infrastructure servers or inserting themselves into the middle of support session communications.

Multicast packet security layer

Additional features provide complete "end-to-end" security for multicast packet data, independent of those provided by SSL/TLS. Specifically, all multicast session data is protected by "end-to-end" encryption and integrity mechanisms that prevent anyone with access to our communication servers

(whether friendly or hostile) from eavesdropping on a GoToAssist session or manipulating data without detection. This added level of communication confidentiality and integrity is unique to GoToAssist. Company communications are never visible to any third party, including Citrix Online itself.

Multicast packet security layer (MPSL) key establishment is accomplished using public-key-based SRP-6 authenticated key agreement, employing a 1024-bit modulus to establish a wrapping key. (See http://srp.stanford.edu/design.html.) This wrapping key is then used for group symmetric key distribution using the AES Key Wrap Algorithm, IETF RFC 3394.

All keying material is generated using a FIPS-compliant pseudo-random number generator seeded with entropy collected at run-time from multiple sources on the host machine. These robust, dynamic key generation and exchange methods offer strong protection against key guessing and key cracking.

MPSL further protects multicast packet data from eavesdropping using 128-bit AES encryption in Counter Mode. Plaintext data is compressed before encryption using proprietary, high performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value generated with the HMAC-SHA-1 algorithm.

Because GoToAssist uses very strong, industry-standard cryptographic measures, customers can have a high degree of confidence that multicast support session data is protected against unauthorized disclosure or undetected modification.

Furthermore, there is no additional cost, performance degradation or usability burden associated with these essential communication security features. High performance and standards-based data security is a "built-in" feature of every GoToAssist session.

Key points

- Public-key-based SRP authentication provides authentication and key establishment between endpoints.

- 128-bit AES encryption is used for session confidentiality.

- Session keys are generated by endpoints, and are never known to Citrix Online or its systems.

- Communication servers only route encrypted packets and do not have the session encryption key.

- The GoToAssist architecture minimizes session data exposure risk while maximizing its ability to link agents to those requesting help.

Firewall and proxy compatibility

Like other Citrix Online products, GoToAssist includes built-in proxy detection and connection management logic that helps automate software installation, avoid the need for complex network (re)configuration and maximize user productivity. Firewalls and proxies already present in your network generally do not need any special configuration to enable use of GoToAssist.

When GoToAssist endpoint software is started, it attempts to contact the GoToAssist service broker via the Endpoint Gateway (EGW) by initiating one or more outbound SSL-protected TCP connections on ports 8200, 443 and/or 80. Whichever connection responds first will be used and the others will be dropped. This connection provides the foundation for participating in all future support sessions by enabling communication between hosted servers and the user's desktop.

When the user attempts to join a support session, GoToAssist endpoint software establishes one or more additional connections to Citrix Online communication servers, again using SSL-protected TCP connections on ports 8200, 443 and/or 80. These connections carry support session data during an active session.

In addition, for connectivity optimization tasks, the endpoint software initiates one or more short-lived TCP connections on ports 8200, 443 and/or 80 that are not SSL protected. These network "probes" do not contain any sensitive or exploitable information and present no risk of sensitive information disclosure.

A complete list of the IP address ranges used by Citrix Online can be found at www.citrixonline.com/iprange.

By automatically adjusting the local network conditions using only outbound connections and choosing a port that is already open in most firewalls and proxies, GoToAssist provides a high degree of compatibility with existing net-

work security measures. Unlike some other products, GoToAssist does not require companies to disable existing network perimeter security controls to allow online support session communication. These features maximize both compatibility and overall network security.

Endpoint system security features

Online support session software must be compatible with a wide variety of desktop environments, yet create a secure endpoint on each user's desktop. GoToAssist accomplishes this using web-downloadable executables that employ strong cryptographic measures.

Signed endpoint software

The GoToAssist Remote Support endpoint software is distributed to user PCs as a digitally signed installer. A digitally signed Java® or Microsoft ClickOnce® applet is used to mediate the download, verify the integrity of the installer and initiate the software installation process. This protects the user from inadvertently installing a trojan or other malware posing as GoToAssist software.

The endpoint software is composed of several executables and dynamically linked libraries. Citrix Online follows strict quality control and configuration management procedures during development and deployment to ensure software safety. The endpoint software exposes no externally available network interfaces and cannot be used by malware or viruses to exploit or infect remote systems. This protects other desktops participating in a support session from being infected by a compromised host used by another attendee.

GoToAssist Monitoring Crawler

The GoToAssist Crawler is typically installed on one computer in your network and the Crawler will automatically scan every system that it detects. After inventorying every device, it continues to run, listening passively for any new devices. Whenever it discovers a new machine or application, the Crawler immediately gathers rich data about that device.

Although the Crawler runs continually, it uses few network and system resources after the first complete run, and it does not leave any footprints on the machines that it scans. By default, the Crawler rescans your network every 24 hours for any changes, such as new software installed or configuration changes. You can reconfigure the Crawler to gather data more frequently from your key systems.

The Crawler securely transfers the collected data to your Search Index, which is in a separate secure location that only you have access to. When you log in to your web account, all of this data is at your fingertips. No one else can view the data unless you give them your log-in password or invite them to join your account.

- GoToAssist uses the highest level of security standards to protect your data, which includes encryption, auditing, logging, backups and safe-guarding data.
- All communications between the GoToAssist Crawler and Citrix Online servers are sent using RSA public/private key encryption combined with AES encryption.

- GoToAssist communicates with your browser using 256-bit SSL.
- GoToAssist uses a tiered server architecture where search index data is two tiers away from the "untrusted" Internet. Access is through a mediating application server.
- Each company's search index is stored separately.
- GoToAssist continually monitors the system to ensure that it is working smoothly as designed.

Cryptographic subsystem implementation

All cryptographic functions and security protocols employed by GoToAssist client endpoint software are implemented using OpenSSL cryptographic libraries.
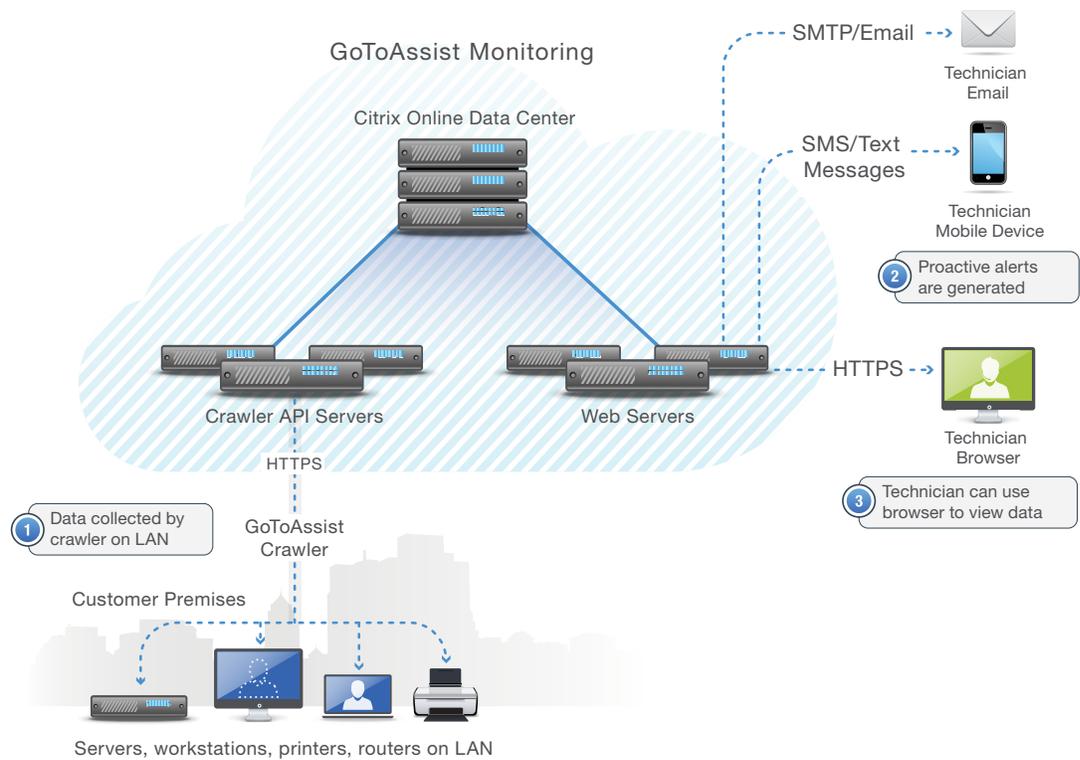
Figure 2: GoToAssist Monitoring Technology Architecture

Use of the cryptographic libraries is restricted to the GoToAssist endpoint application; no external APIs are exposed for access by other software running on that desktop. All encryption and integrity algorithms, key size and other cryptographic policy parameters are statically encoded when the application is compiled. Because there are no end-user-configurable cryptographic settings, it is impossible for users to weaken GoToAssist session security through accidental or intentional misconfiguration.

A company that uses GoToAssist can be certain that the same level of online support session security is present on all participating endpoints, regardless of who owns or operates each desktop.

Hosted infrastructure security features

Citrix Online delivers GoToAssist using an application service provider (ASP) model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

Scalable and reliable infrastructure

Citrix Online's global service architecture has been designed for maximum performance, reliability and scalability. The GoToAssist service is driven by industry-standard, high-capacity servers and network equipment with the latest security patches in place. Redundant switches and routers are built into the architecture to ensure that there is never one single point of failure. Clustered servers and backup systems help guarantee a seamless flow of application processes even in the event of heavy load or system failure. For optimal performance, the GoToAssist infrastructure load-balances the client/server sessions across geographically distributed communication servers.

Physical security

All GoToAssist web, application, communication and database servers are housed in secure co-location data centers. Physical access to servers is tightly restricted and continuously monitored. All facilities have redundant power and environmental controls.

Network security

Citrix Online employs firewall, router and VPN-based access controls to secure our private-service networks and backend servers. Infrastructure security is continuously monitored and vulnerability testing is conducted regularly by internal security staff and outside third-party auditors.

Through these measures and our comprehensive, state-of-the art communications security architecture, you can be assured that your data and local systems remain secure when you use GoToAssist.

Customer privacy

Because maintaining the trust of our users is a priority for us, Citrix Online is committed to respecting your privacy. A link to a copy of the current Citrix GoToAssist privacy policy can be found on the service website at www.citrixonline.com/privacy.tmpl.

Compliance in regulated environments

Because of its comprehensive set of application and communications security controls, including its customer-authorized, permission-based security model, GoToAssist may be confidently used to support computers and applications in environments subject to HIPAA, Gramm-Leach-BlileyAct or Sarbanes-Oxley regulations, where robust data confidentiality and integrity controls must be employed.

Citrix Online recommends that organizations carefully review GoToAssist in the context of their specific environments, user populations and policy requirements. In some cases, communicating additional usage guidelines to users may be advisable to ensure the security goals of all stakeholders are satisfactorily met.

Conclusion

GoToAssist's intuitive and secure interface and feature set make it the most effective solution for conducting online support sessions. Using GoToAssist, support, consulting, accounting and IT professionals can quickly and easily deliver technical help to customers across the globe.

Behind the scenes, Citrix Online's hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment.

As this paper shows, GoToAssist promotes ease of use and flexibility without compromising the integrity, privacy or administrative control of business communications or IT assets.

Appendix: Security standards compliance

GoToAssist is compliant with the following industry and U.S. government standards for cryptographic algorithms and security protocols:

- The TLS/SSL Protocol, Version 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
- AES Cipher Suites for TLS, IETF RFC 3268
- AES Key Wrap Algorithm, IETF RFC 3394
- RSA, PKCS #1
- SHA-1, FIPS 180-1
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2

CITRIX | online

Citrix Online Division
7414 Hollister Avenue
Goleta, CA 93117
U.S.A.
T +1 805 690 6400
info@citrixonline.com

Media inquiries:
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe
Middle East & Africa
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
United Kingdom
T +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific
Level 3, 1 Julius Avenue
Riverside Corporate Park
North Ryde NSW 2113
Australia
T +61 2 8870 0870
asiapac@citrixonline.com

3.23.12/b-82571/PDF