



Remote Support and Service Desk Security

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

GoToAssist consists of two integrated cloud-based IT support tools that are accessed from one easy-to-use interface.

The GoToAssist Remote Support module 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, iPad or Android device.

The GoToAssist Service Desk module encompasses the full spectrum of managing a service, from dealing with customer issues and implementing changes to mapping assets and infrastructure.

This document focuses on the information security features of GoToAssist Remote Support and Service Desk. The reader is assumed to have a basic understanding of the modules and their features. Additional materials on GoToAssist may be found online at www.gotoassist.com or by contacting a Citrix representative. For information about GoToAssist Corporate, please see the [GoToAssist Corporate Security White Paper](#).

GoToAssist Remote Support

Application security

GoToAssist Remote Support 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 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 employee who maintains the Remote Support service delivery infrastructure. Network administrators can provision and maintain infrastructure components.
Customer	The person requesting support from the client company via Remote Support.
Support Provider	The support person who initiates Remote Support sessions in order to provide tech assistance to Customers.

Definitions

Support Provider Software: Installed software that resides on the Support Provider's PC, Mac, iPad or Android device 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 deliver support.

Browser: Standard Internet web browser, such as Chrome, 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 Remote Support 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 Remote Support 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 participate 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 Remote Support website, 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.

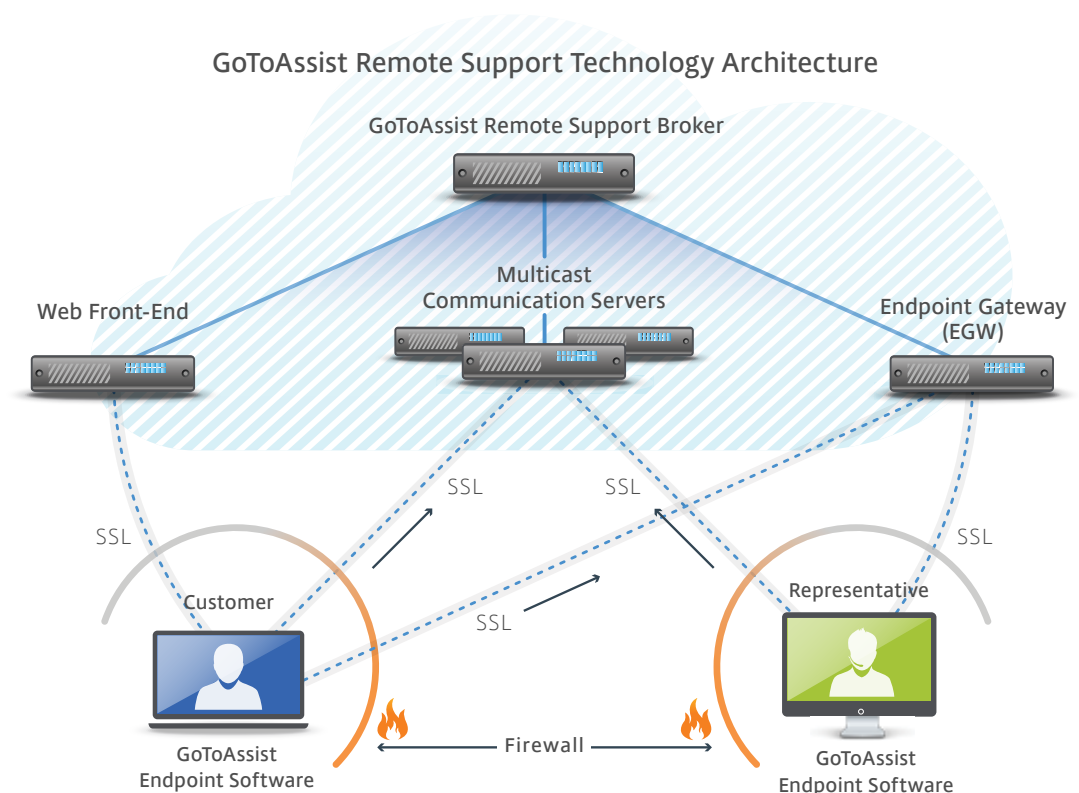
In-Session Security: When the support provider initiates an unattended support session, the customer's machine is automatically locked, and the support provider must provide any Windows or application authentication credentials required when establishing (or initiating) an unattended support session. 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 Remote Support session occurs via an overlay multicast networking stack that logically sits on top of the conventional TCP/IP stack within each user's computer. This network is provided by a collection of Multicast Communication Servers (MCS) operated by Citrix. The communications architecture is summarized in the figure below.



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

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

Communications confidentiality and integrity: GoToAssist Remote Support provides true “end-to-end” data security measures that address both passive and active attacks against confidentiality, integrity and availability. All Remote Support 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 communication servers or during transmission across public or private networks.

The Remote Support session key is not kept on Citrix servers in any form and cannot be discovered or derived by Citrix 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 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 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 (MPSL): 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 Remote Support session or manipulating data without detection. This added level of

communication confidentiality and integrity is unique to GoToAssist Remote Support. Company communications are never visible to any third party, including Citrix itself.

MPSL key establishment is accomplished using public-key-based SRP-6 authenticated key agreement, employing a 1024-bit modulus to establish a wrapping key. 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 or its systems
- Communication servers only route encrypted packets and do not have the session encryption key
- The Remote Support architecture minimizes session data exposure risk while maximizing its ability to link agents to those requesting help

Firewall and proxy compatibility: Like other Citrix products, GoToAssist Remote Support 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 Remote Support.

When Remote Support endpoint software is started, it attempts to contact the Remote Support 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, Remote Support endpoint software establishes one or more additional connections to Citrix 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 list of the IP address ranges used by Citrix 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, Remote Support provides a high degree of compatibility with existing network security measures. Unlike some other products, Remote Support 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. Remote Support accomplishes this using web-downloadable executables that employ strong cryptographic measures.

Signed endpoint software: The 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 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 Service Desk

Service Desk is a cloud-based application that enables IT organizations to manage their IT services from end to end. Service Desk covers the full spectrum of managing a service, from dealing with customer issues to implementing changes to a service and mapping your assets and infrastructure.

With Service Desk, support teams can also create a self-service portal where customers and employees can submit support requests and track the progress of their issue, as well as view knowledge-base documents to resolve issues on their own.

Service Desk is based on the internationally recognized [Information Technology Infrastructure Library \(ITIL\)](#) framework and is designed to enable the easy application of ITIL best practices to managing incidents, problems, changes, releases and configuration items. Unlike Remote Support, Service Desk does not access, control or scan other machines for purposes of monitoring or support.

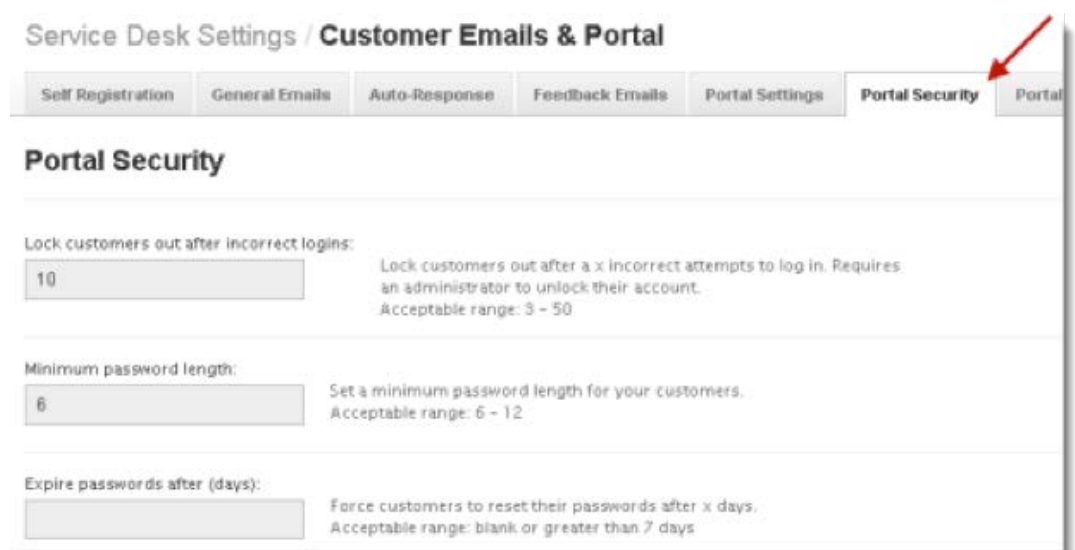
Authentication

No one can access a Service Desk account without proper authentication. GoToAssist Service Desk technicians 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.

GoToAssist communicates with your browser using Secure Sockets Layer (SSL) with strong encryption.



The screenshot shows the 'Service Desk Settings / Customer Emails & Portal' interface. The 'Portal Security' tab is selected and highlighted with a red arrow. The settings are as follows:

Setting	Value	Description
Lock customers out after incorrect logins:	10	Lock customers out after a x incorrect attempts to log in. Requires an administrator to unlock their account. Acceptable range: 3 - 50
Minimum password length:	6	Set a minimum password length for your customers. Acceptable range: 6 - 12
Expire passwords after (days):		Force customers to reset their passwords after x days. Acceptable range: blank or greater than 7 days

Customer portal security

Using the customer portal, customers and/or staff can submit an incident and track its status. This means they can view all updates and comments made to the incident. Access to this information is regulated by authentication and passwords. In addition, some or all the information on the status of the incident can be restricted to just the IT team and not shown to end users.

GoToAssist Service Desk has the same security architecture as all Citrix GoTo services: All session data is protected end-to-end with Secure Sockets Layer (SSL) and 256-bit Advanced Encryption Standard (AES) encryption. Strong passwords and ongoing infrastructure security scans guarantee the security of your information.

- GoToAssist Service Desk uses the highest level of security standards to protect your data, which includes encrypted transmission, auditing, logging, backups and safe-guarding data.
- Service Desk communicates with your browser using 256-bit SSL.
- Service Desk uses a tiered server architecture, where data is two tiers away from the “untrusted” Internet. Access is through a mediating application server.
- Service Desk continually monitors the system to ensure that it is working smoothly.

GoToAssist Remote Support and Service Desk

Cryptographic subsystem implementation

All cryptographic functions and security protocols employed by GoToAssist Remote Support client endpoint software are implemented using OpenSSL cryptographic libraries. All GoToAssist Service Desk HTTP traffic is encrypted using SSL/TLS encryption.

Use of the cryptographic libraries is restricted to the GoToAssist endpoint applications; 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 applications are 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 session security is present on all participating endpoints, regardless of who owns or operates each desktop.

Hosted infrastructure security features

Citrix 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: The Citrix global service architecture has been designed for maximum performance, reliability and scalability. The GoToAssist services are 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 datacenters. Physical access to servers is tightly restricted and continuously monitored. All facilities have redundant power and environmental controls.

Network security: Citrix 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 a GoToAssist solution.

Customer privacy

Because maintaining the trust of our users is a priority for us, Citrix is committed to respecting your privacy. 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-Bliley Act or Sarbanes-Oxley regulations, where robust data confidentiality and integrity controls must be employed.

Citrix 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, the Citrix hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment.

As this paper shows, GoToAssist Remote Support and Service Desk offer IT professionals 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
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2



Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud services to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of \$2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

Copyright ©2014 Citrix Systems, Inc. All rights reserved. Citrix, GoToAssist, GoToMeeting, GoToMyPC, GoToTraining, GoToWebinar, OpenVoice, Podio and ShareFile are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.

Mac and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. Android is a trademark of Google Inc.