CentraNow Security

CentraNow recognizes that Internet security is of major importance to many of our users. Businesses need protection for critical information delivered using CentraNow, individuals want confidentiality for any personal information they provide online, and System Administrators must maintain the security of their local networks.

CentraNow strives to provide the highest possible level of security. This paper reviews the systems and procedures we use to protect our physical environment, to deliver information safely, and to operate within our users' secure environments.

While CentraNow takes every precaution to protect your information and your computer hardware, please be aware that no information delivered over the Internet is 100% secure.

Physical security

All CentraNow servers are secured at Exodus Communications' Internet Data Center in Boston, Massachusetts, USA. Exodus provides the physical environment needed to provide CentraNow meeting services 24 hours a day, 7 days a week.

Exodus provides a wide range of physical security features, including secured access, state-of-the-art smoke detection and fire suppression systems, motion sensors, video camera surveillance, and security breach alarms. Exodus provides reliability through a number of redundant subsystems, such as multiple fiber trunks, fully redundant power, and multiple backup generators.

For more information about Exodus Communications, see http://www.exodus.com/idcs/.

The Microsoft Windows NT Servers used to deliver CentraNow are password-protected at the root level and contain no shared directories. The CentraNow portal uses a Cisco PIX firewall for protection from intrusion.

Web server

CentraNow uses Microsoft Internet Information Server (IIS) to deliver the web pages used to register, sign in, attend meetings, and create meetings. CentraNow maintains security on the IIS by restricting access to allow only CentraNow administrators with a password-protected account.

As an added layer of protection, CentraNow administrators cannot remotely access the server over the Web. Administrators must access the server directly from the client keyboard. Although CentraNow cannot block out "anonymous" access to the site, users who enter the site by this mode cannot edit or post files.

Database

Information obtained from member registration, meeting scheduling, and enrollment is stored in a Microsoft® SQL Server 7.0 (Service Pack 1) database. The database is located at a restricted IP address and utilizes Windows NT Authentication Mode to restrict access to allow only CentraNow administrators with a password account.

For more information on SQL Server, see http://www.microsoft.com/sql/default.htm.

Management Server

The Centra Management Server (CMS) stores and delivers PowerPoint content associated with a CentraNow meeting. To prevent an unauthorized user from accessing the CMS by resolving the domain name, the IP addresses is not DNS registered. The operating system and files on the server cannot be accessed by unauthorized users.

The CMS utilizes Sun's Java™ WebServer™ (JWS). When a user uploads PowerPoint content, JWS transfers the content to a database. During the meeting, the JWS identifies and delivers the associated content to the CentraNow client.

JWS features built-in authentication, encryption, and integrity. Some of the security features include Secure Socket Layer (SSL), secure area sandboxes, access control lists, and digital signatures. CentraNow limits access by browser to administrators with a username and password.

For more information about JWS, see http://www.sun.com/software/jwebserver/index.html.

Collaboration Servers

During a meeting, one of CentraNow's Centra Collaboration Servers (CCS) handles all real-time functionality such as audio broadcasting, raised hands, and application broadcasting. To block access to the CCSs, the IP addresses are not DNS registered. Web server access to each CCS is password-protected.

Protecting your personal information

The following sections describe the kinds of information that CentraNow collects from users.

Profile Information

When a user completes the CentraNow registration form to sign up as a member, CentraNow collects some personal information. We use information such as user name to customize the meeting service for each user. We use the e-mail address as a unique identifier, so that CentraNow Support can assist users who forget their password.

This information is strictly private. Centra does not share the personal information without a user's permission. If a user clicks "Yes" on the registration form, Centra may make information available to selected companies so that they may contact the user regarding products or services that may be of interest. CentraNow does not transfer or sell personal user information to third parties without approval from the user.

CentraNow does use e-mail addresses to occasionally notify users of new CentraNow services and features. In addition, we retain the right to collect and release non-personal information such as advertising impressions and traffic pattern reports.

Cookies

Web browser cookies extend the capabilities of a client-server application by enabling the server side to store and retrieve information on the client side of a connection. Cookies make CentraNow easier to use by saving a few pieces of information.

If a user clicks "Remember Me" when signing in, cookies save the user's e-mail address and password. This automates the sign in process so the user does not have to enter their e-mail address and password during future visits to CentraNow. Users who prefer not to use this feature can simply leave the "Remember Me" box unchecked and sign in manually each time they visit.

Feedback Information

CentraNow occasionally requests feedback information about the CentraNow service and the Centra Network. Users provide this information voluntarily. CentraNow also occasionally requests information when offering special promotions and prizes for using the service. CentraNow's Support and Product Marketing groups use the information to create the best service for our customers.

WebServer Access Logs

Like most public Web sites, CentraNow Web ervers record each user's IP address, source URL and time and date of visit. CentraNow uses this information to plan for system capacity and to monitor usage of the service.

Controlling meeting access

CentraNow recognizes the importance of allowing only preferred attendees into a CentraNow meeting. Our users require access-control mechanisms that enable them to limit who can participate in meetings that contain sensitive information, particularly if the information pertains to customers, partners, or other external entities. CentraNow employs several methods to ensure that only endorsed attendees can access meetings.

When a user schedules a meeting, CentraNow generates a unique, private meeting ID. The ID is a nine-character alphanumeric code that is the key for accessing the meeting. The meeting ID is not published in any list and no one can obtain the ID unless the meeting creator gives it to them. This ensures that only invited users can attend a meeting.

	Anyone with a meeting ID can browse to CentraNow, type in the ID, and attend a meeting. CentraNow strongly recommends that meeting creators protect their meeting ID.

A user who creates a meeting can use one of three ways to control access to the meeting.

If the meeting creator:

- Uses CentraNow's email notification, CentraNow automatically sends invited attendees the meeting ID and a direct hyperlink to CentraNow. Only invited users receive the notification. CentraNow also sends a confirming email to the meeting creator.
- Provides guests with the meeting ID by another means, such as private email or telephone, invited attendees can browse to CentraNow, click attend, and type the meeting ID. A meeting creator who uses this option must control who receives the meeting ID.
- Invites guests who are registered CentraNow users, invited attendees can access the meeting from the listing on their MyCentraNow home page. The meeting only displays for registered, invited users.

Protecting meeting content

A meeting creator maintains complete control over the content. During the meeting, the creator can upload Microsoft PowerPoint™ presentations, display and mark up individual slides, and broadcast live applications. Uploaded PowerPoint content is transmitted via a proprietary encoded format. This makes it difficult, but not impossible, for determined parties to intercept and decode the information.

A meeting creator can also share partial control over the meeting content by promoting one or more attendees to presenter. Presenters share the meeting creator's ability to import PowerPoint presentations, display and mark up slides, and broadcast live applications.

Meeting attendees do not have access to content until the meeting creator or a presenter displays a slide or broadcasts an application. Attendees can not display slides or otherwise access content. If users access the meeting before or after the scheduled session, they can view only the CentraNow Welcome slide.

CentraNow servers temporarily store uploaded PowerPoint content on the secure Centra Management Server as described in the *Physical Security* section of this document. CentraNow servers do not capture or store any information from applications that are broadcasted during meetings.

Meeting creators can delete any or all of the PowerPoint presentations during the meeting. Attendees who have been promoted to presenter can delete PowerPoint presentations during a meeting; however, they can delete only presentations that they imported.

Meeting creators can also delete an entire meeting by clicking Remove on their MyCentraNow home page. When the meeting creator deletes a meeting, CentraNow deletes all of the PowerPoint content in the meeting. Presenters cannot delete meetings.

Supporting network security

CentraNow's delivery technology optimizes connectivity and ensures compatibility with our users' existing security measures. CentraNow does not introduce any new security threats by requiring that organizations change their network configuration or reduce security standards.

Firewall and proxy server connectivity

Firewalls are devices that filter traffic between a protected environment and an external connection such as the Internet. Firewalls can be anything from a set of filtering rules to an elaborate application gateway consisting of one or more specially configured computers that control access. Firewalls permit desired services coming from the outside, such as Internet e-mail, to pass. In addition, most firewalls now allow access to the Web from inside the protected networks. Firewalls allow some services to pass but deny others.

CentraNow is compatible with the vast majority of corporate firewalls and other security systems because it utilizes standard Web protocols (TCP/IP and HTTP) to communicate and secure Java technology on the user's desktop. The CentraNow service uses a sophisticated adaptive network connection manager. The connection manager attempts to connect the user to the CentraNow meeting server via the best possible means.

In most cases, a primary or secondary port connection is successful. A direct and persistent connection is made to the Centra Collaboration Server (CCS) via HTTP protocol over either port 1709 or 80. A direct connection provides the user with full functionality of the CentraNow client, including audio conferencing and application sharing.

If a direct and persistent connection to the meeting server cannot be made, CentraNow's connection manager attempts to connect through the user's Web proxy server. If HTTP tunneling is enabled, the client makes periodic URL-based connections to a Centra Gatekeeper, which maintains a persistent connection to the CCS. This connection does not rely on the client to be persistent. However, the bandwidth of this connection is narrower than optimal for audio and other high-level interactivity. CentraNow displays a message informing the user that a connection is available, but that audio and application sharing performance may be impacted.

The adaptive network connection manager is completely firewall and Web proxy friendly. Users can access CentraNow from behind a corporate firewall or proxy server just as they would access any other Web site.

System Check

System Check is a browser-based utility that assesses a user's system for compatibility with CentraNow. By running System Check before a CentraNow meeting, users can evaluate their capability for participating.

System Check tests a user's hardware, software, and network for:

- Supported operating system
- Supported browser version, Java enabled, Javascript enabled, and Cookies enabled
- Network connection (direct over primary or secondary port or Web proxy tunnel), no applet or Java filtering
- Supported audio hardware and driver

If a user's system does not have optimal functionality, System Check provides troubleshooting instructions. System Check is available from links on a user's My CentraNow home page and other pages on the CentraNow Web site.

Security Warnings

Like many Web sites with client functionality, CentraNow temporarily downloads applets to a client computer. Applets are Java programs that run from inside a Web browser.

In general, applets cannot perform functions that require direct access to the client computer. Examples of prohibited functions are reading and writing files on the client computer, starting other programs, and making network connections except to the originating host. Applets with full restrictions are called *untrusted* applets.

In order to provide functionality like application broadcasting and IP audio, CentraNow must download *trusted* applets. To become trusted, applets must be *signed* by an identity marked as trusted and become part of the client's access control list. In other words, the user must give permission before the applets can download.

When a user clicks Attend to join a meeting, one or more message boxes display. In Internet Explorer, the message box displays a Security Warning that requests permission to install and run CentraNow. In Netscape, the box displays a Java Security message requesting privileges for JavaScript or a Java applet from Centra Software, Inc. Users must click Yes in Internet Explorer or Grant in Netscape to download signed applets and run the CentraNow client. To avoid displaying the message box in the future, users can click "Always trust content from Centra Software, Inc" in Internet Explorer, or "Remember this decision" in Netscape.

Conclusion

CentraNow takes every possible measure to provide protection for critical information over the Internet, confidentiality for personal information, and security of local networks. We continually upgrade the systems and procedures we use to protect our physical environment, to deliver information safely, and to operate within our users' secure environments.

In conclusion, please be aware that, while CentraNow takes every precaution to protect your information and your computer hardware, no information delivered over the Internet is 100% secure.