



White Paper

Secure Data Exchange

With the AutoCAD LT® 2004 software release, Autodesk has enhanced existing features and introduced new functionality to improve the security throughout the process of design data exchange, both inside and outside of your firm.

AutoCAD LT 2004 provides password protection capabilities for drawing sets and electronically published data in DWF™ (Design Web Format™) file format, supports personalized digital signatures, and delivers direct access to the Autodesk® Buzzsaw™ secure online project hosting environment. AutoCAD LT 2004 can also open DWG files that have been password-protected using the AutoCAD 2004 program. The details surrounding each of these three technologies are discussed in this white paper.

Design Web Format™ (DWF™) Security

DWF 6 is an enhanced collaboration and publishing format that is essential to Autodesk's collaboration strategy. DWF 6 file format enables design intelligence to be embedded into your drawings for non-editable, highly compressed CAD files. The updated DWF file format offers exceptional visual fidelity and plotting capabilities. With this updated format, DWF versions of your design files can plot with the same quality as native DWG files. DWF files are created as vector-based files that allow you to pan, zoom, turn layers on and off, and plot from within a web browser or a DWF-enabled application.

The DWF file format has evolved from a representation of a single plot to a container that can hold a multiplicity of sheets. This file format is the electronic representation of a drawing (or plan) set. The publishing tools inside the AutoCAD LT 2004 program enable you to create complete electronic drawing sets in a single DWF file. You can now minimize the number of files being transmitted and avoid confusion regarding file order for viewing and printing.

DWF is a fast, efficient way to distribute design data to anyone who needs it. With Autodesk® Express Viewer, a small, free¹, downloadable application, you can view and print that rich data. What you see is exactly what the designer intended, because the information cannot be changed.

Electronic Drawing Set (DWF) Password Protection

With AutoCAD LT 2004 software, you can assemble drawing sheets into a customized drawing set for publishing to the Internet or an intranet, or for exchanging via email. The electronic drawing set is saved as a single multi-sheet DWF 6 file that can be password protected. DWF passwords are case-sensitive and can be comprised of letters, numbers, punctuation, or non-ASCII characters. However, if you lose or forget the password, it cannot

¹ This product is subject to the terms and conditions of the end-user license agreement that accompanies download of the software.

be recovered. It is important to keep a list of passwords and their corresponding DWF file names in a safe place.

Digital Signatures

In today's business landscape, engineers and designers have to constantly improve their work processes to remain competitive. A key driver of improving productivity in the design space is the much hyped, but underachieving concept of design collaboration. Only recently has this technology moved out of the expensive, proprietary systems of large institutions to a point where it is accessible to and can benefit most organizations. Nowadays design collaboration is not just a tantalizing possibility but more and more a business necessity. This is primarily due to two advances: the rising capabilities of desktop computers and the falling costs of communication, especially on the Internet.

Inexpensive communication however, comes at a price. On proprietary networks, each team member can be trusted and the lines of communication between them can be trusted, but with the Internet the opposite is true. When dealing with sensitive data on the Internet you have to assume that every other person you encounter is hostile until proven otherwise.

Viruses, hacked systems, and denial-of-service attacks bear witness to the fact that there are smart people with dark motives out there, who will attack a system just because they can.

Digital signatures provide security in an insecure environment. A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an unforgeable piece of data attesting that a named person wrote or otherwise agreed to the document to which the signature is attached.

This provides security on three levels:

Identity—as a drawing recipient, I can be sure that the person or corporation that sent me the drawing is who it claims to be.

Data Integrity—I can be sure that the drawing has not changed in any way, either intentionally or accidentally, since it was signed.

Nonrepudiation—the signed drawing cannot be repudiated: The signer cannot later disown it, claiming the signature was forged.

The digital signature technology used in the AutoCAD® family of products is based on public-key cryptography, a widely accepted technology standard. Public-key cryptography is a relatively recent development in the science of cryptography, and to truly understand how public-key cryptography works, it helps to start with the basic principles of cryptography.

Cryptography is the science of mapping documents (commonly referred to as plaintext) into an unreadable format, called ciphertext, and vice versa. The mapping process is a sequence of mathematical computations that affect the appearance of the data without changing its meaning.

To protect a message, an originator transforms a plaintext message into ciphertext through a process called encryption. The ciphertext is transmitted to a recipient over the data communications channel where, if it is intercepted, an intruder will find it unintelligible.

Upon receipt, the message recipient transforms (or decrypts) the ciphertext into its original plaintext format. The algorithms used to map between plaintext and ciphertext are one-way mathematical functions that use a value, commonly referred to as a key, to control the mapping process. With the key it is a simple process to decrypt the ciphertext; without the key it is virtually impossible.

The process of using the same key for encryption and decryption is referred to as symmetric cryptography. Using symmetric cryptography, it is safe to send encrypted messages without fear of interception; however, there always remains the difficult problem of how to securely transfer the key to the recipient of the message, so they can decrypt the message.

A major advance in cryptography occurred in 1977 with the invention of the RSA Public Key Cryptosystem by Ronald Rivest, Adi Shamir, and Len Adleman, then professors at the Massachusetts Institute of Technology.

Rather than using the same key to both encrypt and decrypt the data, the RSA system uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation upon the data. Each key is the inverse function of the other; what one does, only the other can undo. The Public Key is made publicly available by its owner, while the Private Key is kept secret. To send a private message, an author scrambles the message with the intended recipient's Public Key. The message can only be decoded with the recipient's Private Key.

Inversely, authors can also scramble data using their Private Key; in other words, RSA keys work in either direction. This provides the basis for the "digital signature," for if one person can unscramble a message with someone's Public Key, that other person must have used his or her Private Key to scramble it in the first place. Since only key owners can utilize their own Private Keys, the scrambled message becomes a kind of electronic signature—a document that nobody else can produce.

Authentication: Public Keys, Private Keys, and Digital Certificates

Running plaintext through a hashing algorithm creates an expression called a message digest, which is then encrypted using the writer's Private Key and included in the writer's digital signature. The result can only be decrypted by the writer's Public Key. The recipient of the message decrypts it and then recalculates the message digest. The value of this newly calculated message digest is compared to the value of the message digest found from the signature. If the two match, the message has not been tampered with.

To ensure the trustworthiness of the key pairs, a digital certificate is normally used. A digital certificate, also known as a digital ID, is a kind of digital passport or credential. The Digital ID includes the user's Public Key, and can include other information, such as address or professional affiliation and is "digitally signed" by someone trusted to do so, typically called a Certificate Authority. Commercial Certificate Authorities include Verisign Inc. and British Telecommunications.

Every time someone sends a message, he attaches his Digital ID. The recipient of the message first uses the Digital ID to verify that the author's Public Key is authentic, and then uses that Public Key to verify the message itself. This way, only one Public Key, that of the certifying authority, has to be centrally stored or widely publicized. Thereafter, all others can simply transmit their Public Key and valid Digital ID with their messages.

The trusted root certificates of a number of certificate authorities are included with popular browsers such as Microsoft® Internet Explorer and Netscape® Navigator.

DWG Password Protection (Read Only)

One of the most requested features in the AutoCAD program is password protection, a tool that allows customers to share sensitive design information over an insecure medium such as the Internet or email. AutoCAD LT 2004 does not enable you to set DWG password protection, but gives you the ability to open drawings that have been password-protected

using AutoCAD 2004. This enables a seamless workflow between the AutoCAD and AutoCAD LT programs.

From AutoCAD 2004, a saved, password-protected drawing is encrypted and cannot be reopened until the password is entered. For greater security, you can also select an encryption technology and key length for password-protected drawings. Encryption providers vary, depending on operating system and country. When using this feature, you should confirm that the intended recipient of the password-protected drawing file has a computer with the encryption technology you have chosen. Customers using previous AutoCAD versions and derivative products will not be able to access DWG files that are password protected in the AutoCAD 2004 software program.

Like most software tools, passwords potentially can be used for malicious purposes. With this added level of control comes a risk that the data within the file is no longer accessible if the password is forgotten. We have avoided adding a "back door" or administrator's override to prevent compromising the security of the feature. Obtaining this administrator's password would enable someone to break into not just one, but all of a company's files. Recognizing that some companies may not want to deal with the administrative issues of users who have forgotten their passwords, we have made it possible to omit the feature during installation of AutoCAD 2004 (by using the 'Custom' install option).

Transmittal Set Password Protection

Within AutoCAD 2004, you can package an entire drawing file set, including reference files that can be password-protected using the eTransmit feature. Again, the transmittal set cannot be password protected using AutoCAD LT 2004, but can be opened if you know the password. Remember that passwords are case sensitive and the password or phrase can be made up of letters, numbers, punctuation, or non-ASCII characters. If you lose or forget the password, it cannot be recovered.

Project Hosting with Autodesk Buzzsaw

The Autodesk® Buzzsaw™ online collaboration service allows you to store, manage, and share your project documents from any Internet connection—thus enhancing team productivity and reducing costs. The Autodesk Buzzsaw online work environment integrates a secure project hosting service with CAD-related software, tools, and services from industry leaders. Using this powerful service, you can connect with your project team anytime, regardless of organizational or geographical boundaries.

AutoCAD LT 2004 provides a direct link into the Buzzsaw online work environment allowing you to securely participate in the design process with others involved on the project. The following describes the security infrastructure for the Buzzsaw online hosting environment.

Buzzsaw Network and Data Security

At Autodesk, our goal is to keep your project data secure and private and to make our services as reliable as reasonably possible. We use a range of technologies in our applications and services to keep your data secure. And to maximize reliability, we have bolstered our system's infrastructure with redundant storage, redundant connections to the Internet, off-site data backup, around-the-clock access to support personnel, firewall protection, and on-site security.

This section explains the security mechanisms Autodesk Buzzsaw uses to keep your data secure and private.

Security Technology

Our security lies in the technology of our multimillion dollar infrastructure, which includes

- Secure transfer: HTTPS, SSL
- Firewalls
- LDAP servers
- Application security
- Network security and availability
- Data storage and backup
- Physical security
- Privacy

Secure Transfer: HTTPS and SSL

Secure Hypertext Transfer Protocol (HTTPS) provides a secure method for transferring files over the Internet through the Secure Sockets Layer (SSL) protocol. All Autodesk Building Collaboration Services applications use SSL technology to communicate sensitive information over the Internet. Even passwords and login information are always transferred between your computer and our servers using SSL.

Firewalls

The Internet is like an interstate highway: it is open to whoever wants to travel it. Because Autodesk Buzzsaw does not want just anyone to travel into its section of the Internet, we have installed a set of redundant firewalls to further protect the data on our servers. A firewall is a combination of software and hardware that enforces an access control policy between two networks. The firewall performs two primary functions: blocking traffic and permitting traffic. Firewall technology allows a network administrator to decide who can and can't access data on an Internet-connected network.

Firewalls are important because they provide a single location where security can be imposed. Firewalls also provide an important logging and auditing function; they provide summaries about what kinds and what amounts of traffic passed through it, how many attempts there were to break into it, and so on.

LDAP Servers

Once data, using secure protocol and encryption, has passed through the firewall and has reached our servers, a Lightweight Directory Access Protocol (LDAP) server looks up user information. LDAP servers index all the data in their entries, and "filters" select and match a user's registered information. For example, an LDAP search translated into plain English may read "Search for the person located in XYZ Company whose name contains 'John T. Smith.' Please return their full name, e-mail, title, and description." From this search and authentication, the LDAP server maps the user to the user's project information on the servers. The LDAP server allows only your authorized users to access your data on the website.

Application Security

The Autodesk Buzzsaw website's firewall, SSL protocol capabilities, and LDAP servers provide external security on the Internet. Within our applications, we offer customizable and built-in security that further protects your data.

For example, the Autodesk Buzzsaw application offers security and user access options at the account or site, group, folder, and file levels. The Buzzsaw application stores files under the desired security permissions rules specified by the site administrator and tracks all versions and usage of files by users granted access. The administrator of a Buzzsaw site is the gatekeeper of the site and determines who is allowed access.

The administrator can specify from a menu of permissions the desired level of access for each member. Project members can be assigned different permission levels at any level in the site or project hierarchy at the project, folder, or individual file level as shown in the following table:

Permission	Access
No Access	Highest level of restriction. User is prevented from seeing the project folder or even whether a file exists.
List	User can see a list of project folders but cannot view their contents or edit them.
View	User can view project files but is restricted from adding, editing, or deleting a file.
Review	User can view all files in a project and add or edit Notes, comments, and links.
Edit	User can add, edit, or delete files.
Project Administrator	Project administrators can create and convert folders for the project they are responsible for and also assign and remove users to projects.
Site Administrator	Site administrators have full rights to the entire site including user and project administration.

The Autodesk Buzzsaw application offers a variety of security options to protect your data but still allows the flexibility necessary for your project group to function properly.

Another example of application-level security is found in Autodesk® Construction Manager, in which documents are visible only to those individuals that the administrator assigns. Construction Manager enables administrators to refine the security of the application by deciding who can communicate with whom and who may view documents. For example, an administrator can select an option so subcontractors cannot route Construction Manager documents directly to the architect and must go through the general contractor. The administrator can also make documents viewable only to members who either authored or received the document.

In addition to these security measures, every Autodesk collaboration services application uses HTTPS, SSL, and firewall technology to protect client/server communication.

Network Security and Availability

The Autodesk Buzzsaw service actively monitors its services around-the-clock. Third-party and colocation center monitoring services continuously track the performance and availability of IT infrastructure. Should any interruptions occur, our IT staff is immediately notified. IT staff is on call around-the-clock and follows strict escalation procedures to minimize any disruption.

We use many other safeguards to maximize network security and availability, including an Intrusion Detection System (IDS), network management software, and a secondary Internet provider.

An Intrusion Detection System alerts the Autodesk Buzzsaw IT staff to unusual network activity and unauthorized access. The IDS is designed to detect, report, and terminate unauthorized activity on a network.

Comprehensive network management software continuously monitors for faults within the network environment. The software provides a complete, detailed view of network activities that allows us to immediately isolate and troubleshoot our network and resolve any issues.

We contract with a secondary Internet provider for our data center. Not only does this service improve bandwidth and connection speed, it also provides a backup solution should our primary Internet provider experience downtime.

Data Storage and Backup

Autodesk is Tier 5 Proven by EMC, one of only 40 companies to receive EMC's highest honor. EMC is the leading provider of enterprise-level storage equipment. The Tier 5 EMC Proven™ designation means that Autodesk uses industry best practices to minimize site downtime and maintain data availability. Our application servers are clustered to provide redundancy and load balancing. Our databases are also clustered to provide speed and reliability. All project data is stored on redundant EMC® storage systems, a collection of hard disk drives with built-in redundancy that allows for extremely fast data retrieval. The EMC storage equipment uses a technique called *business continuance volume*, whereby data is seamlessly transferred to disk drives without interruption. Should a disk drive fail, missing data is automatically rebuilt on the remaining drives without requiring the site to be taken down.

Your project data is backed up and stored securely in five separate locations- four within our facility and one at an off-site storage facility. In addition to residing on redundant EMC systems, project data is backed up on the EMC Data Manager (EDM™). The seamless, state-of-the-art EDM system provides the fastest and most reliable backup and restore solution available. In addition to these safeguards, your data is backed up to tape four times a day and a fifth tape backup is archived daily to an off-site storage location.

Privacy

To safeguard your privacy online, we strive to make our site as safe and secure as possible. For more information, read our privacy policy, available on our website. If you have questions, you can send e-mail to bcs.support@autodesk.com. Customers in the United States can also call 800-892-0449.

Conclusion

With AutoCAD LT 2004 software, Autodesk has introduced and improved upon several features to improve security around the process of exchanging confidential design data members of the project team both inside and outside of your firm. Digital Signatures and DWF file format are two examples of technologies that can be used to make your process a more secure one.

By hosting your projects in a secure online environment like Autodesk Buzzsaw, from the moment you enter the site to the moment you leave, all data transferred between your browser and our servers is encrypted. All Autodesk Buzzsaw users can be confident that everything from user names and passwords to drawings and specifications to account and credit card numbers are always passed across the Internet with industry-standard security.

autodesk®

Autodesk, Inc.
111 McInnis Parkway
San Rafael, CA 94903
USA

Autodesk, AutoCAD, AutoCAD LT, Buzzsaw, Design Web Format, and DWF are either registered trademarks or trademarks of Autodesk, Inc., in the USA and other countries. All other brand names, product names, or trademarks belong to their respective holders.

© Copyright 2003 Autodesk, Inc. All rights reserved.

