

Entrust Entelligence Group Share

Secure Shared Files on Corporate Networks

Organizations regularly store sensitive information such as trade secrets, employee data and customer account information on internal corporate networks.

Typically, workgroups inside an organization use network file servers as the primary means of collaborating on projects, and these workgroups can extend beyond internal employees to external partners and suppliers. Anyone with access to the corporate network can, therefore, potentially gain access to sensitive data.

Traditional mechanisms designed to secure data on networks are insufficient to protect against a data breach of intellectual property. As part of a layered security model, organizations should deploy a network folder encryption solution that balances the need for employees to collaborate with the need to prevent data breaches.

The Workgroup Security Solution

Entrust Entelligence Group Share can help reduce the risk of a data breach by providing a convenient solution that secures shared data on corporate networks. This allows for the secure sharing of intellectual property, which can enable regulatory compliance. Entrust Entelligence Group Share is easy to deploy and manage because it only has a small client footprint and does not require a PKI.

Automatic Encryption

Once a document is moved or saved in an Entrust-protected folder on the network, it is automatically encrypted for access by only authorized users or groups.

Transparent Encryption

The encryption and decryption of files is done transparently for authorized users, which means that no training is required and employees can continue to share files as usual.

Persistent Encryption

Once a file is encrypted, it remains encrypted wherever it is stored. For example, if the file is dragged into an unprotected folder or desktop, or moved to a USB drive, it will remain encrypted.

Detailed Auditing Capability

Entrust Entelligence Group Share provides centralized audit capabilities for both folder access and folder permission changes. This allows organizations to easily track who is accessing sensitive information, when and from where.

Leverage Existing Groups

Seamlessly integrates with existing active directory workgroups.

Solution Benefits

- Protects sensitive data on corporate networks
- Helps in compliance with regulatory requirements
- Provides improved protection of intellectual property
- Easy to deploy and use
- Enables secure workgroup file-sharing

Dynamic Access

Provides simple management capabilities that allow owners to change permissions on folders without re-encryption — all in a single operation or automatically when using Active Directory groups.

Flexible Authentication

Supports a variety of authentication methods, including Microsoft® Windows® authentication and digital certificates (e.g., smartcards, tokens, etc).

Role Separation

Separates the network management role from document ownership role.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but affordable in today's uncertain economic climate.

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service. Discover how this will benefit you by contacting us at **888.690.2424** or via email at **entrust@entrust.com**

Technical Features

- Automatic encryption of files in local/network folders
- Encryption transparent to applications using files
- Encryption persistent across drag-and-drop operations and backups
- Support for Active Directory groups or Group Share groups
- Central auditing of system events, including folder access and user addition and removal
- On- or off-board Microsoft SQL Server 2008 R2 database
- Users/Groups added/removed to secure folders without touching encrypted files
- Authentication of users via Microsoft Windows authentication or certificate authentication
- Certificate user lookup in external LDAP directories
- Rich role/permission system to control creation of folders/groups
- Comprehensive Web administration interface
- Scalable/high availability Web service architecture

About Entrust

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Entrust® Securing Digital Identities & Information