SAGE ABRA

Sage Abra HRMS

Abra HRMS Security Considerations

August 2005

sage software

TABLE OF CONTENTS

August 2005 1

Introduction 1

Abra Application Security Considerations 1

Abra HRMS *1*

Logon and Password Security 1

Group Security 1

Security Levels 1

Audit Trail 2

Abra Workforce Connections (AWC) *2*

Logon and Password Security 2

Role Security 2

Types of Roles 2

System Administrator 3

Digital Signatures 3

Audit Trail 3

Network/Server Access Security Considerations 3

Windows Server and Abra HRMS *3*

Internet Information Server and Abra Workforce Connections *4*

Data Security Considerations 4

SQL Server Database Access Security *4*

Data Protection *5*

File System 5

File and Directory Level Encryption 5

Transparent Data Level Encryption 5

Network Data Protection 5

Firewalls and Multiple Server Security Considerations 6

Third Party Security Solutions 6

Conclusion 6

About Sage Software 7

SAGE ABRA

Introduction

Information security is a key concern for businesses today. This paper discusses several common considerations when planning the security of Abra HRMS and Abra Workforce Connections in typical SQL Server, Windows Server and networking environments.

Abra Application Security Considerations

The ability for users to view, add, delete and change data in the Abra HRMS and Abra Workforce Connections databases is controlled by the security features of these application programs.

Abra HRMS

Logon and Password Security

Abra HRMS users must log onto the system with a user name and password. The Abra system administrator assigns the user name, ID and password for each user. The administrator can change a user's password. Individual users can also change their own passwords unless they are restricted by their security group settings within Abra. Password maintenance can be scheduled in the System Organizer / Scheduler or can be prompted by Administrative Changes.

Group Security

The Abra HRMS system administrator controls security by assigning Abra users to security groups with the same access rights. The system administrator automatically has access to all functions.

Security Levels

The system administrator establishes access rights within Abra HRMS for each security group at the following levels:

- Employer – Access to the employers set up in the enterprise may be restricted
- Group – Groups defined in your organization levels can be used to define system access (Division, Department, Location, Floor, Branch, Wing, etc.)
- Product – Access to the modules installed and set up on the Abra HRMS system (HR, Payroll, Attendance, Train) may be restricted
- Activity – Access to Actions, Analyses, Details, Processes, Reports and Rules with each product/module may be restricted
- Task – Access to Tasks associated with each Activity may be restricted
- Step – Access to Steps associated with each Task may be restricted
- Field – Access to specific Fields in the Abra HRMS database may be restricted
- Ad Hoc Reporting - determines which fields in the Abra HRMS database are able to be accessed by users through Crystal or Abra Secure Query

sage software

SAGE ABRA

Audit Trail

The audit trail tracks changes made to any data field in Abra. Each monitored change is user stamped, date and time stamped and the old data and new data values are defined. A report reflecting these audit trail activities can be generated directly out of Abra via a standard report.

Abra Workforce Connections (AWC)

Logon and Password Security

AWC users must log onto the system with a user name and password. The system administrator defines logon and password parameters including:

- information an employee must provide to set up a login and access the system
- what types of employees (status) are permitted to log on
- employee login history
- password properties (for example, length, expiration)
- when an employee can be locked out

Role Security

The AWC system administrator controls security by assigning users to roles with the same access rights to menu options, pages and administrative functions. When a user logs on to AWC, the system recognizes the assigned role and provides access only to those menu options and pages authorized. Employee and Manager/Supervisor roles are defined in Abra HRMS. The administrator roles are defined in AWC.

Types of Roles

The system administrator establishes access rights and approval and notification settings for users in the following roles:

- Employee role -- can view and update information contained on employee pages, generate requests, etc. By default, all users are included in the employee role
- Manager role -- can view and update manager pages, act on employee requests and can be assigned access to some employee pages, such as emergency contacts, education or skills.
- Supervisor role -- can act on some employee requests. A supervisor does not have access to manager pages.
- Administrator role – different roles exist for HR, Benefits, Payroll and Training administrators to act on approval requests and receive notifications. Benefit Administrators can also set up open enrollment and life events. Administrators can hold multiple roles (i.e., a person can be both an HR administrator and a benefits administrator.)
-

sage software

SAGE ABRA

System Administrator

The AWC system administrator is also a role and is responsible for system administration tasks, including:

- Assign administrator roles to specific employees in specific employers
- Define the workflow settings for each page in the system on a per-company basis: View, update, approval and notification settings are available.
- Define requirements for employees logging on to the system
- Manage employee logons, including lockouts, deletes and password resets
- Review employee logon history as needed
- Set up Message Center reminders
- Set permissions for specific fields
- Perform customizations, e.g. add custom content or modify colors, fonts, graphics etc.
- Define how employee time off will function

Digital Signatures

AWC uses digital signatures to confirm critical information submissions made by users such as employee benefit enrollments and payroll W-4 elections. The data entered is stored in AWC but will not be accepted or processed unless the digital signature is correct.

Audit Trail

The audit trail provides the ability to track changes made to specific AWC pages. When a page is updated (and the changes have been approved, if the page is set for approval), the changed records are written to Abra HRMS and the audit trail information for the page is written to AWC.

Network/Server Access Security Considerations

Windows Server and Abra HRMS

Abra HRMS is a Windows application. Abra HRMS users are Windows clients. There are typically just a few Abra HRMS users (perhaps 5 to 10.) Windows user accounts should be established for each user who will require access to Abra HRMS. Standard Windows Server authentication and access control methods should be used to secure Abra HRMS within the network/server environment. The users will be further authenticated by Abra HRMS by user name and password.

sage software

SAGE ABRA

Internet Information Server and Abra Workforce Connections

Abra Workforce Connections (AWC) is a Web Server (IIS) application. By default it is installed in a separate virtual directory, and thus is isolated from other web applications on the server.

AWC is a self-service application. The users are employees, so there may be hundreds or thousands of users. Because the objective is to make user access flexible from within the network and externally from the Internet, the users are not required to authenticate to IIS.

For internal access from the network or through a VPN, the users will need to have already been authenticated onto the network by Windows Server authentication procedures.

For external (Internet) access, the IIS should be secured with a Server Certificate implementing Https (secure HTTP.)

Regardless of how the users access IIS, they will be authenticated by AWC using a user name and password.

Data Security Considerations

SQL Server Database Access Security

SQL Server has to be configured for mixed mode authentication. The Abra applications themselves are the database users. Set up SQL Server user accounts and passwords, and use SQL Server authentication to grant the applications access to the databases:

- Abra HRMS database – Abra HRMS clients, AWC application
- AWC database – AWC application

Note: If the Abra HRMS Visual FoxPro database option is being used instead of SQL Server, then Windows user accounts and passwords would be set-up with read/write access permissions for the Abra HRMS clients and the AWC application.

User access beyond the Abra applications themselves should be restricted to only those with absolute need to access the Abra data, such as database administrator, security administrator or network administrator accounts.

sage software

SAGE ABRA

Data Protection

File System

NTFS is the preferred file system for installations of SQL Server. It is more stable and recoverable than FAT file systems, and enables security options such as file and directory access control lists (ACL) and file encryption (EFS).

More information on NTFS and EFS can be found at http://www.microsoft.com/resources/documentation/Windows/2000/server.

File and Directory Level Encryption

The Abra SQL databases can be protected using the Windows Encrypting File System (EFS) feature. EFS uses public key encryption to encrypt the Abra data as it is stored on disk. Usually the performance impact is negligible, because the data files are decrypted when the server process starts.

Encrypt the Abra databases only at the file level, not the directory level. While it is often a best practice to encrypt at the directory level when using EFS so that new files added are encrypted, you should encrypt your Abra SQL Server data files at the file level only. This avoids encrypting your log files.

Transparent Data Level Encryption

EFS encrypts down to the file level. If additional encryption at the data level is required, then consider using a 3rd party vendor product capable of application transparent data encryption for Microsoft SQL Server databases such as Protegrity, Application Security, Inc. or Vormetric.

Network Data Protection

To encrypt data as it is transported over a TCP/IP network, two optional Windows Server utilities are available—Internet Protocol Security (IPSec) and PPTP encryption.

Abra network data passing in and out of a site (across intranets, extranets, or an Internet gateway) can be secured using the following Windows Server utilities:

- Internet Protocol Security (IPSec) -- A suite of cryptography-based protection services and security protocols. IPSec provides computer-level authentication, as well as data encryption, for virtual private network (VPN) connections that use the layer 2 tunneling protocol (L2TP).
- Routing and Remote Access -- Configures remote access protocols and routing. It is a full-featured software router, and an open platform for routing and internetworking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments, or over the Internet, by using secure VPN connections.
- Internet Authentication Service (IAS) -- Provides security and authentication for dial-in users.

Abra network data within a site (local network and subnets) is secured by the authentication protocol. For an additional level of security, you can also choose to encrypt Abra network data within a site using the IPSec Windows Server utility.

sage software

SAGE ABRA

All communication between Abra Workforce Connections clients and the server use HTTP(s). Setting up the server to only allow Https will automatically encrypt all data sent between the Internet Explorer client and Abra Workforce Connections.

Firewalls and Multiple Server Security Considerations

Abra HRMS and AWC can be installed in a variety of network and server configurations utilizing external and internal firewalls. The required inbound and outbound port information is included in the Abra product technical implementation guides.

While Abra HRMS and AWC can be installed together on a single server, for security and performance reasons multiple servers are often employed. For multiple server implementations, Abra uses DSN-less connections and supports TCP/IP, Named Pipe and multi-protocol configurations.

Third Party Security Solutions

In addition to the Abra application security features, and those of Windows Server and SQL Server discussed here, there are many third party security products available on the market that perform specific security functions (such as access control, encryption and key management) or provide enterprise-wide information security and system management. Some are platform independent and application, network and database transparent. Consult with the vendors of any security solutions you have deployed or plan to deploy for use with Abra HRMS and AWC to verify compatibility and support for Windows Server environments and SQL Server databases.

Conclusion

A very high level of information and system security can be achieved through the use of standard Abra HRMS and Abra Workforce Connections application security features, along with standard Windows Server and SQL Server security features. These include network/server access control, SQL Server database assess control, directory, file, data level encryption, network encryption and firewalls. Third party security solutions are also available to enhance both the level and management of security.

sage software

SAGE ABRA

About Sage Software

Sage Software offers leading business management products and services that give more than 2.3 million small and mid-sized customers in North America the insight for success throughout the lives of their businesses. Its parent company, The Sage Group plc (London: SGE.L), supports 4.3 million customers worldwide. For more than 25 years, Sage Software has delivered easy-to-use, scalable and customizable applications through its portfolio of leading brands.

The Sage Abra HRMS business is an important part of Sage Software's growth, and contributes the company's HR and Payroll domain expertise. Other well-known brands in Best Software's portfolio include ACCPAC, ACT!, BusinessVision, CPASoftware, FAS, MAS 90, MAS 200, MAS 500, MIP, Peachtree, SalesLogix, Timberline, among many others. For more information, please visit the Web site at www.sagesoftware.com/moreinfo or call (866) 308-BEST.

sage software

888 Executive Center Drive West, Suite 100
St. Petersburg, FL 33702
727-579-1111
www.sagesoftware.com/products/abrasuitepd

RY4O0016 07/05 05-4740