Vision Municipal Solutions

Software Authentication Policies

2014

Authored by: John Engebretson

Vision Municipal Solutions

Software Authentication Policies

Vision software is developed specifically to maximize the capabilities of Microsoft SQL Server and ensure compliance with the .NET framework. Therefore, we follow Microsoft's Best Practices for securely connecting our software.

Microsoft SQL Server offers Vision software two levels of performing user authentication: Windows authentication mode and mixed authentication mode.

- **Windows authentication mode** requires users to provide a valid Windows username and password to access the database server. In enterprise environments, these credentials are normally Active Directory domain credentials.

  When a user connects through a Windows user account, SQL Server validates the account name and password using the Windows principal token in the operating system. This means that the user identity is confirmed by Windows. SQL Server does not ask for the password, and does not perform the identity validation. Windows Authentication is the default authentication mode, and is much more secure than SQL Server Authentication. Windows Authentication uses the Kerberos security protocol, it provides password policy enforcement with regard to complexity validation for strong passwords, provides support for account lockout, and supports password expiration. A connection made using Windows Authentication is sometimes called a trusted connection, because SQL Server trusts the credentials provided by Windows.

  By using Windows Authentication, Windows groups can be created at the domain level, and a login can be created on SQL Server for the entire group. Managing access at the domain level can simplify account administration.

- **Mixed authentication mode** allows the use of Windows credentials but supplements them with local SQL Server user accounts that the administrator may create and maintain within SQL Server.

  When using SQL Server Authentication, logins are created in SQL Server that is not based on Windows user accounts. Both the user name and the password are created by using SQL Server and stored in SQL Server. Users connecting using SQL Server Authentication must provide their credentials (login and password) every time that they connect. When using SQL Server Authentication, you must set strong passwords for all SQL Server accounts.

Vision's Installation Team advocates the use of Windows Authentication primarily on stand-alone workstations individually connecting to our software with one exception.

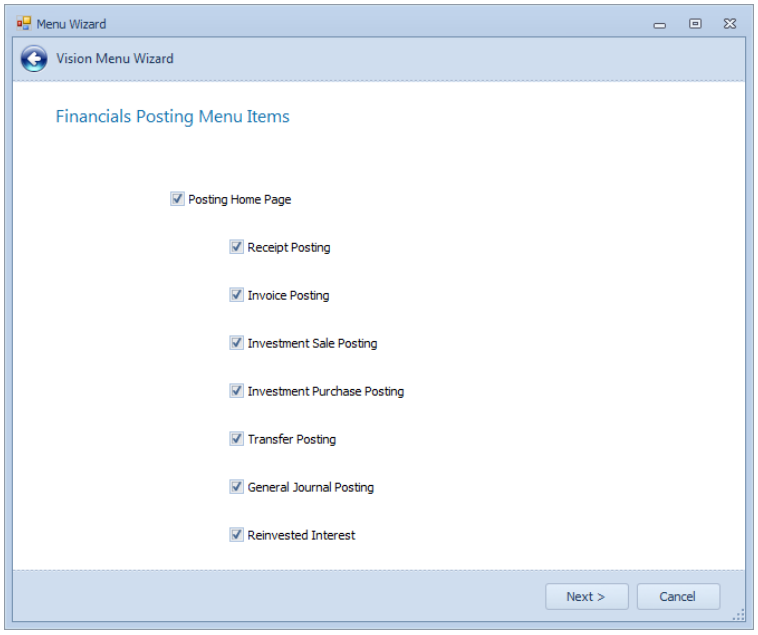
Our Cash Management software is configured using mixed authentication mode as typically a single computer is used by multiple employees at any given time. This requires an additional level of security to distinguish between users.

Vision Municipal Solutions

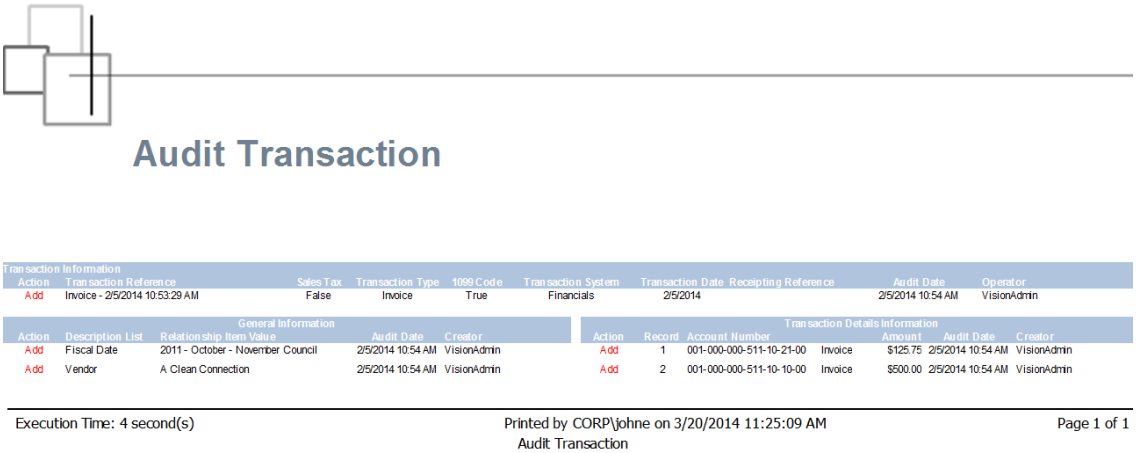
Software Authentication Policies

Vision also recognizes that internal controls are also required at times.

Once a user has passed the authentication methods described above, our software then passes through another set of credentials that limits the options that appear in the software for each individual user.. These controls are set by an Administrator and require specific login credentials to update.



Finally, a word about Auditing. Every transaction modification that occurs within any of our software products is extensively audited. Each table in our database is configured with Transaction Triggers that automatically track every addition, deletion, and change to each value within all tables. Each addition, deletion, and change is tracked by workstation, user, date, and time. This data can then be displayed in the form of both data grids and through Reporting Services as shown below.



Audit Transaction

Transaction Information

Action	Transaction Reference	Sales Tax	Transaction Type	1099 Code	Transaction System	Transaction Date	Receipting Reference	Audit Date	Operator
Add	Invoice - 2/5/2014 10:53:29 AM	False	Invoice	True	Financials	2/5/2014		2/5/2014 10:54 AM	VisionAdmin

General Information

Action	Description List	Relationship Item Value	Audit Date	Creator
Add	Fiscal Date	2011 - October - November Council	2/5/2014 10:54 AM	VisionAdmin
Add	Vendor	A Clean Connection	2/5/2014 10:54 AM	VisionAdmin

Transaction Details Information

Action	Record	Account Number		Amount	Audit Date	Creator
Add	1	001-000-000-511-10-21-00	Invoice	$125.75	2/5/2014 10:54 AM	VisionAdmin
Add	2	001-000-000-511-10-10-00	Invoice	$500.00	2/5/2014 10:54 AM	VisionAdmin

Execution Time: 4 second(s)

Printed by CORP\johne on 3/20/2014 11:25:09 AM
Audit Transaction

Page 1 of 1