

# Operating System authenticates logins in TRIM Context

**Date: 24/11/04**

TOWER Software has taken a fundamentally different approach to application level security in TRIM Context to that used by previous versions of TRIM. In TRIM Captura users were required to log in to TRIM explicitly. This login was required in addition to their corporate network login. TRIM Captura does provide an option use trusted database logins to provide "single sign-on". This process was to some extent a carry-over from the older versions of the Windows operating system, where a network login was not always required to access the machine's resources.

The login process has been streamlined in TRIM Context. The user's network login is automatically used to authenticate the user during the login process. Occasionally this has been referred to as using "trusted logins", due to the perception that TRIM Context was "trusting" the network login. However using this term creates some confusion as the term 'Trusted Logins' has a specific meaning within the database community. Trusted Logins imply that the database server is responsible for asking the host operating system to authenticate a user seeking access, effectively instituting a three-party handshake between client, database, and OS.

TRIM Context uses a different technique, and this new method should not be confused with any older method with which you may be familiar. To authenticate a user attempting to connect to TRIM Context, the following steps are taken:

- The TRIM Context client communicates its desire to connect with the TRIM Context Workgroup Server
- The Workgroup server ensures the client process is in possession of the correct key (built-in to the TRIM software – to prevent other processes impersonating a true TRIM Context client)
- The Workgroup server challenges the client to provide the full network credentials of the launching user
- The Client responds with the credentials
- The Workgroup server ensures the user is registered, with these credentials, as a known location within the desired dataset.

Access is granted if all the conditions are met.

The authentication check only involves: TRIM Context workgroup server (armed with the data from the database); the TRIM Context client; and the operating system, thus it is more accurately described as an Operating System Authentication Model.



By using an OS authentication model TRIM Context avoids many of the problems associated with a “trusted logon” model for example the limitations in the trusted-authentication abilities of certain databases. For example, some relational databases can't authenticate a user who has logged in to a Novell network from a windows workstation. TRIM Context will have no problems authenticating the user in this environment.

The authentication process is able to work this way because the TRIM Context clients do not directly connect to the database. Instead access is always moderated by a TRIM Context Workgroup Server.

From a user's perspective, this streamlined process makes using TRIM Context easier as they gain the benefits of secure single sign-on facilities, enabling seamless use of TRIM Context without the annoyance or delay of additional login steps or dialogs. TOWER Software believes this will encourage users to use TRIM Context more frequently, thus enhancing the value of the corporate record store.

This leads to the obvious question, how do the Workgroup servers themselves connect to, and authenticate with, the database. The workgroup servers connect to the database using the relevant database client for the chosen database, and therefore can use any of the authentication methods available from the database client (e.g. normal login/password techniques, trusted logins, directory-service controlled authentication, etc.). Workgroup server authentication with the database is completely invisible to the end-user.

In summary the use of an Operating System Authentication Model has several benefits for the implementing organisation;

- Smoother implementation
- Better user buy-in
- Increased usage

All of which ultimately lead to a better return on investment.

## **About TOWER Software**

TOWER Software delivers Electronic Document and Records Management (EDRM) Solutions, empowering organizations to take control of their corporate information assets. TOWER Software's award-winning TRIM Context® solution is a single, integrated platform that manages business information throughout its complete lifecycle. By relying on its proven domain expertise, strong strategic partnerships, and powerful solutions, TOWER Software enables organizations to maintain accuracy, maximize efficiency, and achieve and maintain standards compliance across industries, resulting in sustained competitive advantage. TOWER Software is a privately held company with operations in North America, Europe and Asia-Pacific. For more information, visit [www.towersoft.com](http://www.towersoft.com).



**TOWER Software - Asia Pacific  
Head Office - Canberra ACT**

[www.towersoft.com.au](http://www.towersoft.com.au)

TRIM Context is a registered trademark of TOWER Software. All rights reserved.

Copyright © 2003 TOWER Software