

# Business Justification

Last Revised: 08/08/2001



Effortless Enterprise Management for  
Windows NT, Windows 2000, and Beyond...

To print this Word document, please turn off the "Background Printing" option in Word.

Instructions: "Tools" menu, "Options" item, "Print" tab, uncheck "Background Printing", click "OK" to save settings, and print.

**AVATIER**  
COMMAND YOUR GREATEST ASSET  
111 Deerwood Road, Suite 200  
San Ramon, CA 94583

Phone: 800-609-8610  
925-831-4746  
Fax: 925-855-3266

Email: [support@avatier.com](mailto:support@avatier.com)  
Web: [www.avatier.com](http://www.avatier.com)

*Limited Warranty*

Avatier Corporation makes no warranty, representation, or promise not expressly set forth in this limited warranty. Avatier Corporation does not warrant that the software or documentation will satisfy your requirements, that the software and documentation are without defect or error, or that the operation of the software will be uninterrupted. Avatier Corporation disclaims and excludes any and all implied warranties of merchantability, title and fitness for a particular purpose.

This document may not be lent, sold, or given away without the written permission of Avatier Corporation. This document may be freely copied for internal distribution, as long as the copyright notice is not removed.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes will be incorporated in new editions of the document. Avatier Corporation may make improvements in and/or changes to the product described in this document at any time.

*Disclaimer*

The formulas and calculations provided to you here are provided 'AS IS' and are for illustrative purposes only. It must not be construed to mean that Avatier intends to honor such savings. Any reliance on the formulas or the information derived from use of these formulas are at your own risk.

Avatier will not be liable to you for any claims or damages, including but not limited to actual, consequential, special, incidental or punitive damages, lost profits, or lost savings that relate to your use of the formula or its results in this document.

Trusted Enterprise Manager, TEM, Virtual Organizational Units, and Active Collections are trademarks of Avatier Corporation. NetWare and NDS are trademarks of Novell Corporation. Microsoft, BackOffice, Win32, Windows and the Windows logo are registered trademarks and BackOffice and Windows NT are trademarks of Microsoft Corporation. Copyright © 1995-2001 Avatier Corporation. All rights reserved. Printed in the United States of America. **9000 Part No. 9900-00**

Avatier's Trusted Enterprise Manager software product (TEM) is the market leading administrative interface for enterprise Windows NT/2000 networks. Organizations that have purchased TEM are using it to productively and efficiently manage their Windows networks all over the world. This paper explains the business benefits that led to the independent decisions made by nearly 1,000 organizations to implement nearly 1 million licenses of TEM.

---

## Overview

The business benefits from TEM fall into four primary areas. Each of these areas is reviewed in this paper.

- dollar savings such as a reduction in the number of domain controller servers,
- productivity improvements through efficient user interfaces and automated operations,
- the value of new functions not found in native operating system,
- and risk reduction through elimination of errors and control of scope of powers.

TEM is also unusual in that its justification equation holds up even when considering full life-cycle implementation costs. This report contains specific calculations that can be used to generate a projected return on investment.

This cost justification model for TEM has been compiled by Avatier based on insights from a sampling of TEM customers. It is intended to quantitatively show the incremental cost savings of using TEM.

## Reduces Total Cost of Ownership (TCO)

TEM reduces total cost of ownership by simplifying the complexity of a native Windows NT/2000 environment.

### Domain Migration/Consolidation

The desire to create limited authority to appropriately align scope of control with job descriptions or different classes of Windows NT “administrators” has historically prompted large organizations to create several small account domains rather than one consolidated account domain. Size, network limitations, and geographical challenges are other reasons for having multiple NT account domains, but often it comes down to the basic need for division of control. Windows 2000 with Active Directory attempt to address this need, but the adoption rate of Active Directory has been extremely slow due to its complexity and limitations in real world environments.

Regardless of where you are on the NT4-Windows 2000-Active Directory path, TEM pushes security authority down to the global group level, thus eliminating the need for unnecessary domains (and unnecessary OU’s in Active Directory) in most organizations.

Global groups are the “glue” between NT4, Windows 2000 Active Directory, and your local file system security, so it is the best solution possible at any time along your migration path and afterwards.

In an NT4 example, each additional domain has fixed costs for additional hardware, software, licensing, and administrative overhead. For every additional domain, at least two additional domain controllers (a primary and backup) are required. Please feel free to insert actual figures from your organization into the worksheet below.

Cost Description	Sample Figures	Actual
Primary Domain Controller Server – 2 year cost of hardware	\$15,000	
Secondary Domain Controller – 2 year cost of hardware	\$15,000	
2 year cost of software	\$10,000	
2 year facilities @ 20 sq ft @ \$5/sq foot/month for 2 servers	\$5,000	
2 year cost of support (1/40 of administrator burden)	\$5,000	
Total Cost of Each Additional Domain	\$50,000	
Number of Extra Domains	5	
Cost for Extra Domains avoided with TEM deployment	\$250,000	

Additionally, the incremental administrative granularity gained by creating additional domains is very limited compared to that provided by TEM. In other words, even with the large cost of creating domains primarily for purposes of granularity, an implementation of TEM would have provided far more functionality and autonomy.

## Task Automation/Productivity Improvements

TEM's user interface capabilities and built-in task automation are designed to be the most efficient method of administering the enterprise Windows NT/2000/Exchange/Terminal Services network. Nearly every common task a Windows administrator performs has been provided and/or automated in the TEM GUI. TEM consolidates functionality from several disparate native tools such that TEM logically handles complete tasks that would take several manual steps in multiple tools to accomplish without it. Many of these productivity improvements can be quantified individually, and can be summed up en masse as they pertain to your organization.

However, immeasurable efficiencies, time savings, and productivity enhancements are introduced when considering the power of TEM's SQL-powered Details View and the ability to change mass properties via several advanced multi-select techniques throughout the GUI.

The Details View displays column based properties data from NT/2000 accounts, Exchange mailboxes, Terminal Service profiles and accurate Last Logon information in one "Admin-By-Report" view. The columns can be re-arranged, sorted, filtered, searched, frozen, and hidden to provide the desired report, export list, or custom view. It can then be used to make immediate administrative changes to just the filtered data as desired. No other product provides this advanced functionality.

TEM incorporates traditional and advanced methods of multi-selecting objects for the purpose of making similar property changes to all accounts with one quick action. A subset of user properties can be changed for multiple accounts at once with NT4 User Manager for Domains (UM4D), however, this is not true of Exchange Admin. Windows 2000's Active Directory Users and Computers (ADUC) takes a huge step backwards in this productivity area. The only tasks that can be completed to multiple user accounts in Active Directory at once are: Delete Account, Disable/Re-enable Account, Move Account to a new OU, and Send Mail (if Exchange 2000 is incorporated). Though more functionality is promised in Windows .NET (code named Whistler), that won't even be available until sometime in 2002. If you figure in a few Service Pack updates before trusting it to your network, you are in for a long wait that still will not match TEM's capabilities. Why wait for this functionality, when you can have it today regardless of your current position on the NT4-Windows 2000-Active Directory path?

---

The activity data presented on the following pages is a sample set of different administrative tasks. Many different tasks can be performed from within TEM, and we have attempted to estimate only a selected set of common or large tasks.

## Improving Windows NT/2000 Management

A significant portion of the productivity benefits that TEM provides come from improvements to common management tasks associated with Windows NT/2000.

- When a Windows NT/2000 account is created, the administrator must also create a home directory with appropriate permissions, create a home share with appropriate permissions, possibly create an Exchange mailbox, possibly create a Terminal Server profile, possibly run customized scripts, and assign group memberships for various directory or application access. With TEM, the secondary tasks are all automatically performed. The “Trusted Manager” that is allowed to create new accounts simply creates the account, and the potential error of leaving out a function is eliminated (NOTE: It is even more efficient to “copy” an existing “template” account with all desired settings for that “role” or job description). Naming conventions on the account ID, Full Name, Exchange Alias, Exchange Display Name, and home share can also be enforced or suggested.
- The most common help desk problem is that people forget their passwords. TEM provides a single taskbar button (Quick Password Reset icon) that resets a password, unlocks the account if necessary, and forces the end-user to provide a unique password for their next logon session...all without the help desk operator needing to type or confirm a single keystroke. Various statistics are available, but we have determined that between 35% and 45% of all help desk calls are related to this task.

<b>Per-Windows NT User Administrative Selected Activities</b>	<b>Time w/o TEM</b>	<b>Time w/TEM</b>	<b>operations /year</b>
Create user account, home directory, home share, Exchange mailbox, group memberships	20 minutes	1 minute	1 per user
Password reset	2 minutes	1 minute	5 per user
Time saved/year		24 minutes/user	
Administrator cost/minute		\$1	
Savings/Windows NT User/year		\$24	
Number of Windows NT Users		5,000	
Productivity Savings with TEM		\$120,000	

## Group Operations

TEM's group operations are a significant source of business justification. Through TEM's advanced GUI with multi-select, drag & drop, and cut/copy & paste features, TEM permits changes to be made to all members of a selection or an entire global group with one action.

Specific savings depend on the number of operations performed and on the number of groups and accounts in those groups.

<b>Group Administration Selected Tasks</b>	<b>Time w/o TEM</b>	<b>Time w/TEM</b>	<b>Operations /year</b>
Disable all accounts in a 45 member contractor group with removing the NTFS rights of the home-share and profile path	20 minutes	1 minute	4
Move 1,000 users and their group memberships between domains	4,800 minutes (4 weeks )	15 minutes	2
Synchronize specific BDC that a user's logon authenticates to following a password change (Organization w/ 1,000 users)	10 minutes for PDC to update all BDCs from Server Manager	1 minute	5,000
Time per year	59,680 minutes	5,034 minutes	
Administrator cost/minute		\$1	
Savings/year with TEM		\$54,646	

## Simplifying Network Management

With the additional domains (or Organization Units in W2K-ADS) typically required without TEM, the complexity of the network is increased. For NT4 domains, the trust relationships that are required to make the domains work together for administration and authentication sometimes break and must be restored. With TEM, the number of account domain trust relationships in an NT4 or mixed NT4/W2K environment can practically be reduced to zero.

The cost of NT trust downtime to organizations varies according to the business and the specific applications deployed. The indirect economic benefit of TEM in eliminating this source of failure is significant in most scenarios.

<b>NT Trust Activities eliminated with TEM Deployment</b>	<b>Reductions</b>
Creating trust relationship	15 minutes
Number of domains	5
Number of trusts (# of domains times # of domains minus 1)	20
Number of times per year each trust must be recreated due to breakage	2
Trust management time saved without extra domains	600 minutes/year
Cost of Administrative time/minute	\$1
Cost for extra Domain Trusts avoided with TEM deployment	\$600

<b>Productivity Cost due to NT Trust Downtime</b>	
Length of trust downtime	20 minutes
# of people affected by trust loss	100
Cost per person of productivity loss	\$20/hour
Number of avoided outages/year	10
Total cost of Trust Outages	\$6,667

## Centralized Logging/Auditing/Reporting

Monitoring a Windows NT/2000 network to determine which accounts have been added, deleted, modified, and to which groups people belong is an extremely time-consuming task without TEM. Although Windows NT/2000 keeps a security event log, it is kept in an unfriendly format that must be manually reviewed. TEM writes the appropriate detail on every TEM transaction to the Application log of the TEM host machine's Event Viewer and produces an external log file that can be imported into any product that handles comma-separated-value (.CSV) files.

TEM's SQL backend provides superior reporting capabilities such as filtering, sorting, and several controls over the data presentation. TEM combines data from NT/2000, Exchange, Terminal Server settings, and Last Logon data in one convenient interface.

We will assume that an environment that deploys TEM requires fewer domains (and domain controllers) on a conservative ratio of 3 to 1.

<b>Activities</b>	<b>w/o TEM</b>	<b>w/ TEM</b>
Prepare report covering group and user changes	15 minutes/domain controller	2 minutes/domain
Review Report	5 minutes	5 minutes
Tasks/year	12	12
Number of domain controllers	6	2
Audit time per year	1,440 minutes	168 minutes
Cost of Administrative time/minute	\$1	
Yearly cost for group and user change auditing	\$1,440	\$168

---

## Unique Functions Not in Operating System

TEM also provides new functions that are either unavailable in native Windows NT/2000 or would take a prohibitive amount of time to accomplish. These items include, but are not limited to:

- TEM enforces naming conventions on new User IDs, User Full Names, Exchange Mailboxes, Exchange Aliases, Exchange Display Names, NT/2000 global groups (including renames), user Home Shares, and computers (if wildcard delegation is used). This is not possible in native NT4 nor in W2K/Active Directory.
- TEM automates and logically links several functions that must be performed manually and singularly in NT/2000/Exchange with multiple tools:
  1. home directory permissions, renames, deletions;
  2. home share creations, share permissions, renames, naming conventions;
  3. Exchange mailbox creations and deletions;
  4. Terminal Server profile creations;
  5. Custom “exits” for customer-specific automation
- As explained in an earlier section, TEM uses several multi-select methods to change properties en masse with one action.
- TEM provides superior SQL-powered reporting capabilities for NT/2000/Exchange/WTS/Last Logon information and other integrated third party products if installed (i.e. Enterprise Security Reporter for file/directory/share security reports or RightFax for user FAX settings, etc.).
- TEM can rename global groups “in place” from the TEM Client. This function is not possible in NT4. Rename Group retains its user membership and its own membership in domain local groups and server local groups that affect file/directory/share/application security. If the managed global group is also “linked” to an Exchange distribution list in TEM, its name will be changed as well.

---

## Custom Automation Capabilities

Many enterprises have existing scripts or programs for automating administrative tasks, such as ensuring that when a Windows NT/2000 account is created, a record is added to the HR database and the account is then created on the enterprise's mainframe, Netware, and UNIX systems. TEM provides "User Exits" that can easily accomplish custom automation for the creation, copying, and deletion of user accounts.

This type of automation usually saves 5 to 10 minutes per account creation or deletion operation.

Per-user Automation Savings	Time w/o TEM	Time w/ TEM	Operations/year
Add user to 2 other systems when Windows NT account is created	15 minutes	0	0.5 per user
Remove user from 2 other systems when Windows NT account is deleted	15 minutes	0	0.2 per user
Time saved/year	11 minutes/user		
Administrator cost/minute	\$1	\$1	
Savings/Windows NT User/year	\$11		
Number of Windows NT Users	5,000		
Productivity Savings with TEM	\$55,000		

---

## Domain Administration over the WAN

The TEM user interface can be 500% to 1,200% faster in network performance on slow links than Windows NT User Manager for Domains (UM4D).

TEM uses memory-cached NT SAM information from the TEM service and other information pre-gathered and in the SQL-based Directory Shadow Repository (DSR). TEM's services can be deployed centrally or distributed to remote sites on the other side of slow WAN links for localized performance and fault tolerance. For those remote TEM services, the cached SAM information can be gathered from the closest domain controller on the network. This architecture allows for the fastest data structure available for while not needing to traverse the WAN for anything other than changes to the SAM on the actual PDC. The method for Windows 2000 Active Directory is very similar.

In addition, TEM Client only shows the managed groups by the particular Trusted Manager and also allows commands to be released to the background for processing while the Trusted Manager moves on to the next administrative task.

Jim Weider of Chevron states, "In addition, running User Manager over slow WAN links was unbearable. With 10,000 users, it would take an administrator several minutes to open User Manager and several minutes for screen refreshes after each change. TEM only displays groups under the administrator's control, so start and refresh time is seconds rather than minutes."

This not only makes domain administration over the WAN faster, but finally even feasible. In some cases, TEM might even prevent the need for upgrading costly WAN communications lines where remote administration is desired.

The following chart makes assumptions about line speeds that will need to be verified in each organization's WAN environment.

<b>Activity</b>	<b>w/o TEM</b>	<b>w/ TEM</b>
Start User Manager vs TEM over WAN link	10 minutes	1 minute
Number of times/year	250	250
Number of remote sites	25	25
Remote Admin time per year	62,500 minutes	6,250 minutes
Cost of Administrative time/minute	\$1	\$1
Savings in remote administration/year		\$56,250

## Global Group Rename

TEM provides the ability to truly rename groups, a function not allowed in Windows NT4's User Manager for Domains. This is an important capability for enterprises as they merge with other companies or simply re-organize internally with different functional group names and acronyms. Without TEM:

- 1) a new group would need to be created.
- 2) all of the members of the old group would need to be added to the new group.
- 3) all ACL/ACE security references on files, directories, shares, advanced user rights would need to be changed using the new group name.
- 4) all local groups in the current and all trusted domains that contained the old group must be updated to reflect the new group name.
- 5) Delete old group.

The cost of manually renaming a group could be as high as several hundred hours of administrator time. These estimates are extremely conservative.

<b>Activity</b>	<b>w/o rename</b>	<b>w/TEM rename</b>
Create a new group	1 minute	N/A
Add 100 members to new group	1 minute	N/A
Delete old group	1 minute	N/A
Grant new group read permissions to each group members home share	2 hours	N/A
Grant new group permissions on 20 subdirectories on 10 servers	2 hours	N/A
Rename a group	N/A	1 minute
Time to rename a group	4 hours	1 minute
Number of group renames/year	12	12
Cost of Administrative time/minute	\$1	
Annual savings in group renames		\$2,868

---

## Security & Data Integrity Risk Reduction

TEM reduces risks and deployment time of delegation capabilities in several ways.

- Allows precise definition of the both the scope of control and administrative permissions for a Trusted Manager that can be implemented in minutes for even the largest organization. This is not the case for Active Directory, which takes many months of planning for the one-shot implementation of ADS, its cumbersome Organizational Units, and the subsequently delegated powers. Compatibility issues of existing hardware and software, and other limitations of Active Directory discovered along the way can extend the implementation indefinitely. Why wait to get the security benefits and to delegate the scope of control desired?
- In TEM, non-Domain Admin Trusted Managers can only see the objects they have been defined to manage by a NT/2000 Domain Administrator and can only perform the precise functions over those objects that were granted to them. In a typical Active Directory implementation, anyone with delegated powers can still view objects outside of their assigned scope of management unless painstaking methods are used to hide them from the delegate.
- TEM significantly reduces the human error rate associated with repetitive manual operations by automating many common and related tasks. This ensures that these tasks are performed in accordance with organizational policies, rules, and naming conventions.
- In NT4, TEM allows the organization to demote all “Account Operators” and many “Domain Administrators” and “Server Operators” to regular “user” status, thus barring their use of User Manager for Domains and Server Manager and their default access to files, directories and shares on other servers. These “users” can then be granted the appropriate administrative scope and permissions that coincide with their job description/responsibilities. Security exposures are minimized to the highest degree.
- Another AVATIER product, Password Bouncer™, can be implemented to ensure strong password enforcement when passwords are changed by users or administrators. Password Bouncer incorporates advanced rules and extensive wordlist checks that are not available in NT4 or Windows 2000/Active Directory. This results in difficult-to-hack passwords on ALL accounts, thus better insuring network and data integrity.

Risk reduction is best measured in a business justification by considering the potential costs associated with the risk and the likelihood that the risk will occur.

## Delegating Administrative Scope and Permissions

A Windows NT Administrator account has complete access to every object, every system, every file on every computer for an entire domain. There is no method in NT4 to limit this power without either removing the ability for the person to perform administrative actions or creating a costly separate domain.

## Limit the number of Administrator/Operator Accounts

TEM permits users (or groups of users) to be given defined subsets of administrative powers over defined subsets of the objects within a domain. For most organizations that have implemented TEM, this has meant a tremendous reduction, up to 90%, in the number of Windows NT/Exchange Administrator accounts in use. A 100% reduction in "Account Operator" accounts is most often achieved.

The business exposure created by the misused powers in extra administrator accounts is compounded by frequency of use. The exposure will be different for different organizations, depending on the type of applications and data present on the Windows NT network. It is certain, however, that as more and more applications and data are migrated to the Windows NT network that the risk will rise.

We will estimate this exposure based solely on a need to re-create a number of user accounts that an imaginary disgruntled employee erased. We will compare that with the same set of operations with TEM.

Exposure Risk	Without TEM	With TEM
Re-create 1,000 user accounts	14,000 minutes	1,000 minutes
Time saved/incident		13,000 minutes
Administrator cost/year/minute		\$100,000
Savings/incident		\$13,000
Lost productivity for affected users (# users/2 * \$20/hr * minutes saved with TEM)/4 administrators working		\$540,000

## Error Reduction and Rules Enforcement

TEM's automation reduces the likelihood of error by making complex, multi-step procedures quick, simple, and/or completely automated. TEM also reduces risk by allowing administrators to enforce rules evenly across the organization.

### Dual Key Account Deletion

An account in a Windows NT/2000 domain cannot be deleted and restored with full functionality without a substantial amount of work. Windows NT/2000 does not use the account name when granting security permissions to files, it uses an underlying identifier called the SID. If an account is deleted, and a new account with the same name is created, the SID is different and security permissions must be re-established. Not all Windows NT administrators or Account Operators understand this initially (and most Help Desk operators have this authority to delete accounts!).

TEM can prevent accidental account deletions with a "dual key" account deletion setup. With this, most people using TEM cannot delete accounts, but can only disable and move them to a "To-Be-Deleted" global group. The precious few people with delete authority can easily recover accounts that were mistakenly disabled/moved, or actually delete the accounts only after they double-check.

We'll estimate the savings by considering the time to recreate the accounts for 100 accidentally deleted accounts vs. the time to move them back from the "To-Be-Deleted" global group.

Account Deletion Risk	Without TEM	With TEM
Re-create 100 accounts	1,400 minutes	15 minutes
Re-create security policies for 100 accounts	6,000 minutes	0 minutes
Time saved/incident		7,385 minutes
Administrator cost/year/minute		\$100,000
Savings/incident		\$7,385
Lost productivity for affected users (# users/2 * \$20/hr * minutes saved with TEM)/4 administrators working		\$30,700

## Rules enforcement

TEM provides for automated enforcement of some rules an Enterprise Manager may define. Example of rules enforcement include:

- Ensuring that global groups are all created and modified within established naming conventions that provide a logical hierarchical “Virtual Organizational Unit” structure if desired.
- Ensuring that user accounts and Exchange mailboxes are all created and modified within established naming conventions.
- Ensuring that home directories and home shares are all created and modified within established naming conventions and have the proper file/directory/share access permissions.
- Ensuring that no accounts are added to groups outside of an individual’s scope of control.

Automatic rules enforcement should be viewed as providing productivity gains by eliminating the possibility of error and providing order to the network.

Activity	Without TEM	With TEM
Number of domain accounts	5,000	5,000
Number of admin operations/year/account	5	5
Error rate/operation that could be prevented with automatic rule enforcement	1%	0
Discovery of errors in minutes	1 minute	0
Time to fix error	10 minutes	0
Time saved		2,750
Administrator cost/year/minute		\$100,000
Savings/incident		\$2,750