

Citrix® MetaFrame®  
Password Manager

---

A Technology Profile and ROI Analysis  
Prepared for Citrix Systems

September 2003



**ENTERPRISE MANAGEMENT**  
ASSOCIATES

© 2003 Enterprise Management Associates, Inc. All Rights Reserved.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc.

All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.



# Citrix MetaFrame Password Manager

---

## Table of Contents

Executive Summary .....	1
Introduction .....	2
Historical Perspectives on Password Management .....	3
Key User SSO Requirements .....	3
Key Enterprise SSO Requirements .....	3
The SSO Value Proposition .....	4
Citrix MetaFrame Password Manager .....	5
EMA Lab Analysis: MetaFrame Password Manager .....	6
MetaFrame Password Manager Value Proposition Model .....	8
EMA's Perspective .....	8
Pricing and Availability .....	8
Estimated ROI for Citrix MetaFrame Password Manager .....	9
Conclusions .....	11



# Citrix MetaFrame Password Manager

## Company Name:

Citrix Systems, Inc.

## Product:

MetaFrame Password Manager

## Target Market:

Enterprise Customers

## Return on Investment (ROI):

**Scenario A:** The most compelling business case is for Citrix customers that are fully invested in the MetaFrame Presentation Server architecture. These customers could realize a *payback on a MetaFrame Password Manager investment in six months*, with a three-year blended *ROI of 247%*.

**Scenario B:** Mixed customers, who choose both licensing models, can also expect an excellent *payback, in seven months*, and a three-year blended *ROI of 212%*.

**Scenario C:** Non-Citrix customers who choose the named user model can expect a *nine-month payback* and a three-year *ROI of 166%*.

## Executive Summary

Key challenges that IT faces today include reducing budgets, increasing demand to provide new services, and increasing demand on the existing infrastructure. How does today's IT manager and executive reconcile all of this without requesting additional funding? The answer lies in making better use of existing resources, including hardware, software, and people. Increasing IT productivity and empowering self-service can result in drastically reduced IT overhead, otherwise known as operational expenditures (OpEx). Reduced OpEx may then be applied to more strategic IT projects without increasing total IT budgets.

Enterprise Management Associates (EMA) research shows that one area costing the enterprise a substantial amount of money is password management. The average user in today's large enterprise utilizes five to fifteen major systems, many of which have their own authentication systems. Users that are forced to remember all of these passwords typically do not—they choose simple, easy to guess passwords, or store their passwords in an unsecured location. When users forget their passwords, they call the help desk, which drives up IT costs. EMA research has shown that, on average, password management costs \$250 per year for every technology user in an organization. The math is simple: in an organization with 3,000 users, the annualized help desk costs, just for password resets, equals \$750,000!

A major technical challenge that IT has been trying to solve since the early 1990s is single sign-on (SSO). The concept is simple: require users to provide their identity through a single authentication system, and then automatically provide access to all of the IT systems and information resources. In addition, SSO implies that password changes in the back-end systems are handled automatically, and that the changed passwords will be in compliance with company and legal policies and regulations. One criticism of centralized SSO systems is that they present a potentially large security risk. If hackers gain access to an SSO system, they would possess the "keys to the kingdom," allowing unfettered access to corporate resources. An enterprise-class SSO solution must therefore support strong password policy enforcement, high levels of encryption, and multi-factor authentication methods that are impervious to attack.

Traditional SSO technologies have been complex, expensive to purchase, difficult to implement, and expensive to maintain. This was primarily due to "boil the ocean" approaches, in which the vendor attempts to provide interfaces to and from virtually every security system in the enterprise, and also provides its own API for enterprises to interface their own applications to the system. These solutions required costly software modifications or the development of scripts and connectors. Despite these challenges, SSO is an important part of the overall security strategy for the enterprise.

Today, a new SSO solution is being brought to market by Citrix Systems. Citrix MetaFrame Password Manager takes the approach that the simplest SSO solution must be the correct one. MetaFrame Password Manager provides Single Sign-On by learning logins and passwords from the perspective of the end-user, instead of attempting to master each and every back-end system. Once trained, the system automatically enters the users' login and password information whenever needed. MetaFrame Password Manager also handles password changes automatically, generating new extremely strong passwords.



MetaFrame Password Manager is an extremely cost-effective, easy to implement SSO solution that requires no application changes, works with virtually every system including Web, Windows, and mainframes, and requires very little on-going maintenance. IT managers and executives who desire a cost-effective SSO solution that will provide rapid time-to-value and an excellent ROI should seriously consider Citrix MetaFrame Password Manager.

## Introduction

IT managers and executives face a major dilemma: How to fund strategic investments in an atmosphere of fiscal pessimism that has yielded flat or declining budgets, resource constraints, limited staff, and pressure from all sides to “do more with less?”

For many in IT, the answer is value. High-value, strategic investments that are inexpensive to acquire and implement, provide rapid time-to-value with a ROI measured in months, and provide a low on-going total cost of ownership (TCO), are sound business decisions, regardless of the economic situation. Investments that pay for themselves rapidly and deliver a positive, continuing ROI, not only free up IT dollars for other strategic projects, but they also benefit the whole organization through “soft ROI” benefits including increased worker productivity and higher levels of competitiveness overall.

A key pain point for users and IT alike is the issue of password management. EMA estimates that today’s corporate employee uses an average of ten business critical applications, including customer relationship management (CRM), enterprise resource planning (ERP), e-mail, and various Web applications. In most cases, these applications do not share common authentication mechanisms, forcing users to remember numerous individual passwords for each system that they access. As a result, the passwords that users choose are generally easy to guess (and easy to remember!), leading to tremendous security risks.

Even when users are forced to choose hard-to-guess passwords, they typically store them in an easy to access location (such as a sticky note or unencrypted file). This makes unauthorized access from the inside, which accounts for approximately 80% of all security breaches, very easy. Also, as the complexity of passwords increases, so does the frequency of forgotten passwords. When users forget their passwords, they usually call the help desk, resulting in added IT overhead and reduced worker productivity.

Enterprise Management Associates (EMA) research shows that average large enterprises spend \$250 per worker, per year, on password management and associated help desk overhead. In a 5,000-person organization (assuming 3,000 technology users), the annual cost for password management equals \$750,000! Over 50% of all help desk calls are related to password management, and an average user calls the help desk once per month with a password-related issue.

Add to these costs increasing corporate governance and regulatory compliance requirements, and the potential cost of not addressing the password management problem becomes very large, very rapidly. Enterprises must find a solution to this issue or suffer unacceptable levels of risk.

Unlike many IT investments, the business case for single sign-on solutions is crystal clear. For example, assume that SSO will result in a 50% reduction in password management spending for an organization with 3,000 computer users, primarily due to a reduction in help desk calls. This results in a net annual savings of \$375,000. Even small organizations can benefit—a 100-person business, spending approximately \$25,000 per year on password management, would benefit from a cost-effective SSO solution.

This paper addresses the password management problem, describing the history of the problem and solutions, followed by a description of the value proposition for SSO solutions. Next, a new solution in the SSO market, MetaFrame Password Manager by Citrix Systems, is described and compared with the overall

value proposition. The paper will conclude with EMA's perspective on the SSO market and Citrix's solution, along with information on the Citrix product and its estimated ROI in three deployment scenarios.

## Historical Perspectives on Password Management

Vendors have been trying to solve the SSO problem since enterprises began moving from monolithic to distributed systems in the early 1990s. Some approaches concentrate on providing centralized authentication mechanisms that back-end systems use for authentication, while others synchronize security information across multiple security mechanisms and domains. Other approaches concentrate on the user perspective, capturing and memorizing passwords as the user enters them and then automatically signing the user in on subsequent accesses.

Today, directory services such as Microsoft's Active Directory have solved many "back office" authentication and authorization problems, but the password problems outlined above still persist: it is simply too difficult for users to remember five, ten, or twenty complex passwords, and then be required to change those passwords on a frequent basis. What is needed is an elegant, inexpensive, and simple SSO solution. Vendors that can solve the SSO problem, inexpensively and with a minimal amount of integration and implementation costs, will gain a lot of traction in today's market, as the benefits of these investments is very easy to appreciate (and the associated ROI is very easy to calculate).

### Key User SSO Requirements

When user requirements for an SSO solution are distilled, there are two main features that SSO solutions that have gained traction in today's market provide:

1. Single sign-on across multiple, heterogeneous systems, including Web, Windows, and mainframe applications
2. Automated password changes and resets that comply with corporate password policies

### Key Enterprise SSO Requirements

In addition to the benefits provided from the user perspective, enterprises have the following key requirements of an SSO solution:

1. **Security strategy:** Risks due to potential security breaches must be minimized through enforcement of password change policies, including the use of random characters, frequent password changes, and the coordination of changes across the enterprise. SSO is a key part of an overall risk-mitigation security strategy.
2. **Productivity enhancements:** Today's worker is required to be more productive than ever before, and SSO is a key way to reduce the amount of non-productive overhead that a worker must endure. Reductions in help desk calls also increase IT productivity.
3. **Regulatory compliance:** Increasing scrutiny from stockholders and government regulators places tremendous pressure on corporations to prove that they are complying with (and exceeding) regulations such as HIPAA and the Sarbanes-Oxley Act of 2002. Of particular interest to CEOs and CFOs is the fact that the latter requires them to certify under penalty of law that their company is in compliance with the Act. This certainly raises the visibility of many security and audit-related IT projects to the executive level.

Citrix  
 MetaFrame  
 Password  
 Manager

## The SSO Value Proposition

EMA developed a methodology for determining the value proposition of a technology solution that utilizes decision-modeling (DM) theory. These theories center on the concept that every decision, whether personal or professional, is based upon two basic tenets: cost and benefit. In other words, any decision (such as an investment in technology) is ultimately based upon the expected benefits offset by the expected costs. Qualification and quantification of these two points results in a value proposition, which is modeled graphically. The various value points are shown in increasing orders of relevance, from left to right, with costs and benefits of the decision appearing as the ultimate “high order” values.

EMA has developed the following value proposition for SSO solutions, based on research with vendors and consumers of these technologies:

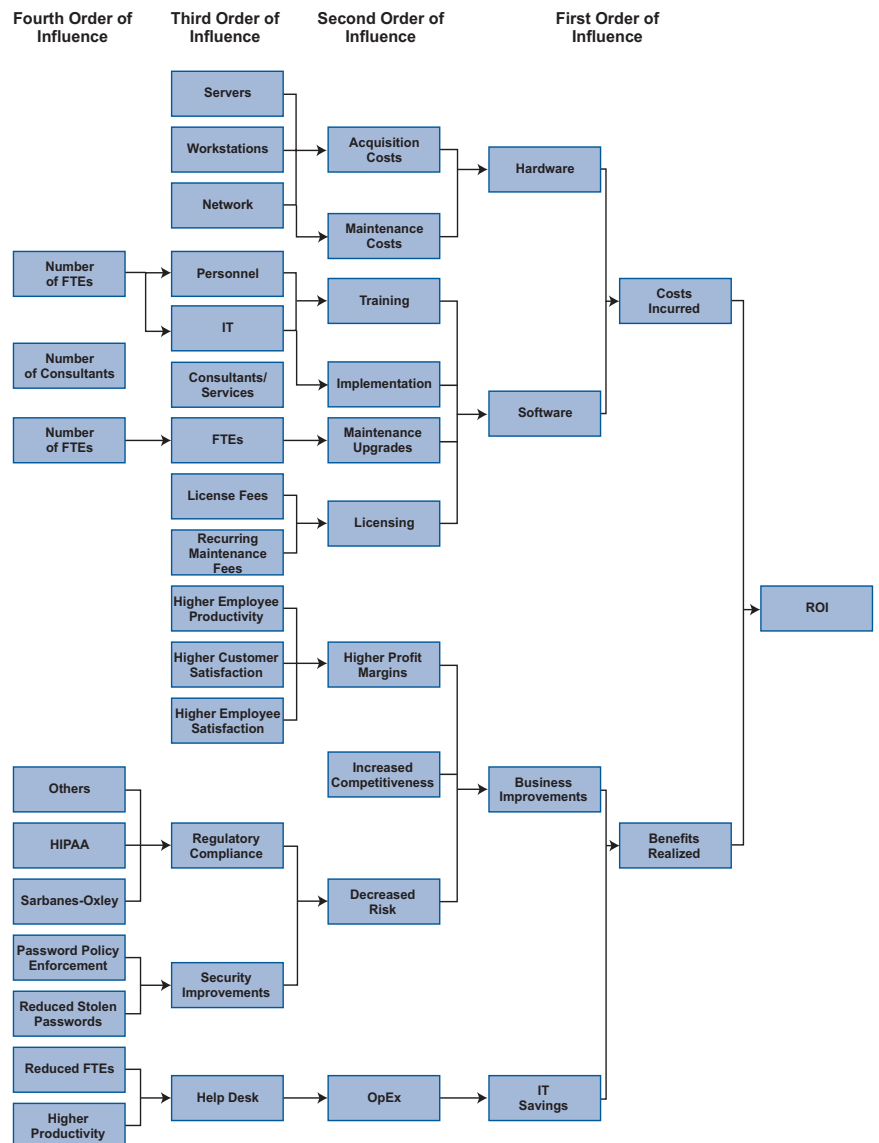


Figure 1: Single Sign-On Value Proposition

The value proposition should be clear: depending on the costs incurred to acquire and implement the SSO solution, a number of easily quantified hard-dollar benefits will result, in addition to numerous soft-dollar benefits.

It is important to note that SSO solutions can, in themselves, present a security risk. If an SSO system is breached and the passwords compromised, the “keys to the kingdom” would effectively be passed to the intruder. As a result, the security and integrity of the SSO solution must be absolutely guaranteed, and access to the SSO system must be very secure. Strong password policies for primary authentication are critical. Ideally, SSO solutions should not only support password-based authentication, but also optional authentication mechanisms such as token cards and biometrics.

The next section describes a new entry into the SSO market by industry veteran Citrix Systems. Citrix has provided solutions to the market for many years, and released the MetaFrame Password Manager solution recently, which provides an innovative SSO solution. MetaFrame Password Manager continues Citrix’ vision to eliminate the barriers between workers and information by providing a major access infrastructure component.

## Citrix MetaFrame Password Manager

Citrix has provided a highly integrated set of solutions to the market since 1989, beginning with its MetaFrame Presentation Server product, which hosts applications for multiple users on a single server platform. In the past few years, Citrix enlarged its MetaFrame Access Suite of products, adding remote secure access and application conferencing products to the mix.

Citrix’s MetaFrame Password Manager is a new member of the MetaFrame Access Suite that provides single sign-on and password policy enforcement. MetaFrame Password Manager, contrary to what the name implies, does not actually require Citrix MetaFrame Presentation Server, although Citrix is quick to state that its 120,000 existing customers are the most likely audience for the product.

MetaFrame Password Manager consists of two components: a client-based agent that is loaded on the MetaFrame Presentation Server or stand-alone PC, and a server component that runs on any Microsoft Windows 2003, Windows 2000 and Windows XP machine (including, of course, MetaFrame Presentation Servers). Interestingly, the client application does not require constant communication with the server component. The server process is used to define and push out password policies to the client agents, but does not require constant connectivity (resulting in very low network overhead).

- After installation, during which MetaFrame Password Manager is configured to integrate with the security subsystem of the Windows operating system, the MetaFrame Password Manager client runs passively on the PC or MetaFrame Presentation Server session. It silently watches for sign-on events, which include Web, Windows, and even mainframe applications.
- When a sign-on event is detected, MetaFrame Password Manager analyzes the application screens, seeking the classic ‘user name’ and ‘password’ fields. MetaFrame Password Manager then places a bold red window around the fields and asks the user if they would like to register the login information with MetaFrame Password Manager.
- If the user selects ‘yes’, then MetaFrame Password Manager leads the user through a screen that allows them to enter their current user name and password. After confirming the password, MetaFrame Password Manager then automatically populates the fields in the application and presses the ‘OK’ or ‘submit’ button.

- Future visits to the login screen cause MetaFrame Password Manager to spring into action, automatically logging the user into the application.

A key strength of MetaFrame Password Manager is the ability for the user (or administrator) to easily configure the product to automatically sign in to applications. Out-of-the-box, MetaFrame Password Manager ships with templates for configuring applications to work with a number of commercial software packages. In the event that an application is used that MetaFrame Password Manager is not familiar with, the screen layouts are extremely easy to add to the product via its wizard-based interface, requiring no scripting. Custom application logins are added via the standard MetaFrame Password Manager GUI configuration tool, and literally take about a minute to complete. Login information collected and managed by MetaFrame Password Manager is stored in an encrypted file on disk, and replicated centrally in a network file share or Microsoft Active Directory.

The server component of MetaFrame Password Manager, as mentioned previously, installs on either the MetaFrame Presentation Server (for Citrix clients) or any server-class Windows server. A GUI tool allows administrators to define and distribute password policies to the MetaFrame Password Manager agents, including items such as password format (length and format) and change intervals.



Figure 2: Citrix MetaFrame Password Manager Intelligent Agent Response and Login Capture

Once trained, MetaFrame Password Manager seamlessly handles subsequent logins to the application.

### Managing Password Changes

A key feature of MetaFrame Password Manager is its ability to automate the process of changing passwords based on pre-defined intervals or from messages generated by the application. When a password needs to be changed, MetaFrame Password Manager automatically navigates to the application's password change screens and generates a new password (based on policies defined either at the console or at the agent), and effects the change with no user interaction required. Since MetaFrame Password Manager manages the passwords (and the user does not need to remember them), a random, highly complex and compliant password is generated. This provides a high level of added security to the application—a feature that security auditors are sure to approve.

### EMA Lab Analysis: MetaFrame Password Manager

EMA was provided an early release version of MetaFrame Password Manager, which was installed in EMA's test lab. Installation of the server component was accomplished in about 15 minutes, and installation of the client agent took about five minutes. The product required no training, and only a basic read of the manual was all that was required in order to install and use the product.

EMA installed and tested the server and client components of MetaFrame Password Manager on vanilla Windows-based PCs. Once the agent was installed on a client PC, a MetaFrame Password Manager icon appeared in the system tray indicating that the agent was active.

From that point forward, accessing applications that required authentication almost always cause the MetaFrame Password Manager agent to open a window, prompting for login information. Subsequent login requests from the application were automatically (and seamlessly) handled by MetaFrame Password Manager. A number of different applications were tested with MetaFrame Password Manager, including several Web sites and Windows applications. In the event that MetaFrame Password Manager does not recognize a login request, it is possible to quickly train the agent to recognize the various application screens and fields.

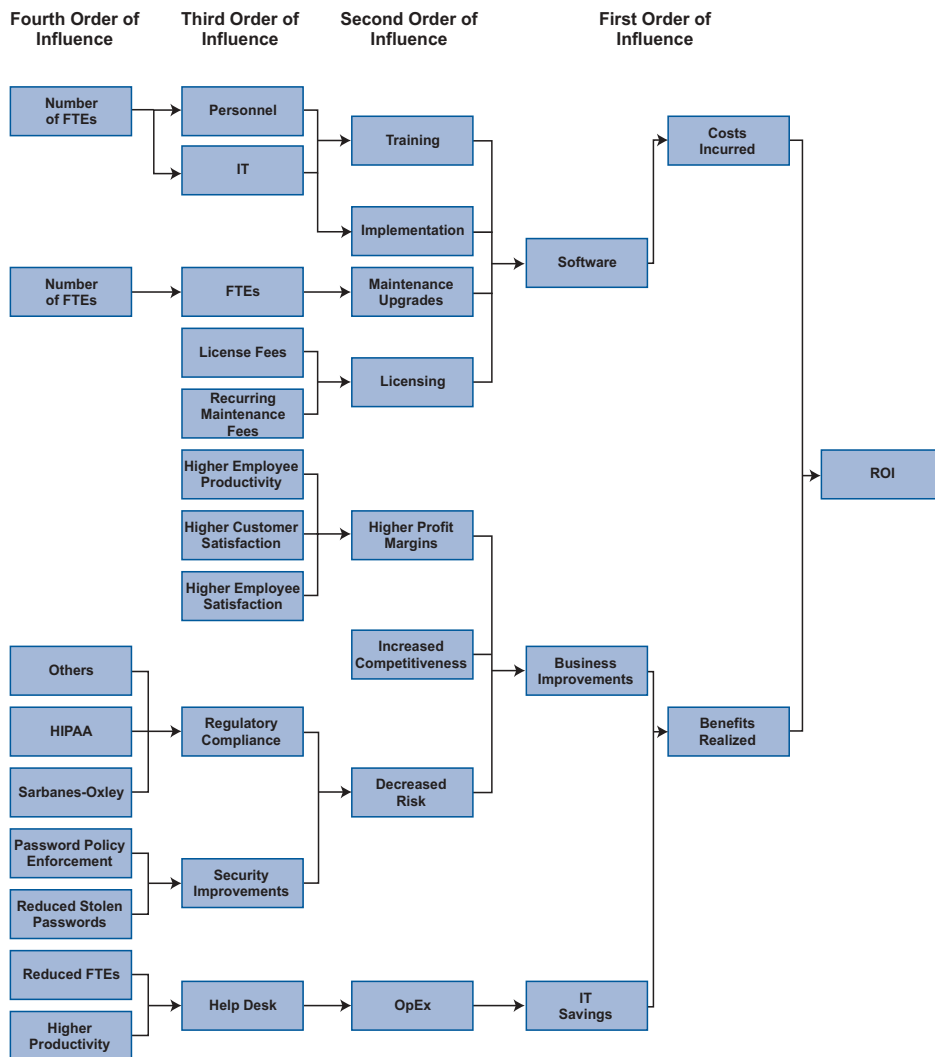


Figure 3. Modified Single Sign-On Value Proposition



Citrix  
MetaFrame  
Password  
Manager

The “acid test” for MetaFrame Password Manager is in the area of managing password changes. MetaFrame Password Manager ships pre-configured for a number of password detection and change events. If an application is not in this list, then the administrator must configure MetaFrame Password Manager for the password change process. This is a very simple process that involves clicking on an icon in the MetaFrame Password Manager agent, selecting which function to associate with which field on the screen (through a GUI interface), and then setting the appropriate change policy (e.g., change period and the structure of the new password).

### MetaFrame Password Manager Value Proposition Model

Based on EMA’s lab experience, combined with an interview of a Citrix customer that has installed and tested MetaFrame Password Manager in their lab, the following value proposition model for MetaFrame Password Manager was built. It is modified to show the major points of value that MetaFrame Password Manager customers can expect to receive from the product. Since MetaFrame Password Manager does not require a dedicated hardware investment (and the MetaFrame Password Manager server imposes a very small amount of overhead on the server that hosts it), the hardware components of the original model have been removed.

### EMA’s Perspective

EMA has evaluated a number of single sign-on solutions over the years, and most solutions have been expensive and difficult to implement, leading to high total costs of ownership and a murky ROI. Citrix offers an innovative, simple SSO solution that solves at least 90% of an organization’s SSO issues. By focusing on the front-end of the sign-on instead of the back-end, Citrix is able to solve the SSO problem without requiring extensive coordination between back-end security systems. This results in tremendous savings in implementation and maintenance costs, when compared with competitive solutions.

MetaFrame Password Manager licensing is based upon concurrent users, named seats, or a combination of the two. The concurrent pricing model is clearly targeted at Citrix MetaFrame Presentation Server environments, where additional economies of scale are realized due to the fact that Citrix users will only be accessing the MetaFrame Password Manager server on a sporadic basis. Citrix estimates that a three-to-one ratio of total users to concurrent users in this environment is sufficient, but this varies by organization. In mixed (Citrix MetaFrame Presentation Server and client desktop) or desktop only environments, Citrix estimates pricing concurrent users at the same three-to-one concurrency ratio described above for the MetaFrame Presentation Server users, and named-seat licensing for desktop users.

Since MetaFrame Password Manager is just being brought to market, and therefore MetaFrame Password Manager customers have not been using the product long enough to gather verifiable ROI data, EMA

### Pricing and Availability

**Product name:** Citrix MetaFrame Password Manager

**Product function:** Single sign-on; password change management

**Operating system under which it runs:** Windows 2003/2000/XP (server), Windows 9x/NT/2000/2003/XP (client)

**Vendor name:** Citrix Systems

**URL for product information:** <http://www.citrix.com/passwordmanager>

**Vendor contact info:** <http://www.citrix.com>

**Pricing information:** \$89 per named user or \$179 per concurrent connected user (suggested retail price)

**Availability:** Generally available Q3 2003

calculated an estimated ROI based upon anticipated savings and costs drawn from industry standard benchmarks. The estimated ROI for the environments mentioned above are as follows.

### Estimated ROI for Citrix MetaFrame Password Manager

As mentioned previously, EMA research shows that average large enterprises spend approximately \$250 per worker, per year, on password management and associated help desk overhead. In a 5,000-person organization (assuming 3,000 technology workers), the annual costs for password management is \$750,000. Industry studies have shown that approximately 50% of all help desk calls are related to password management.

#### Costs

Citrix prices MetaFrame Password Manager two ways: based upon concurrent connected users (at \$179 per user), and based upon named users (at \$89 per user). Concurrent connected user (CCU) licenses are shareable (each user consumes a license only when needed), whereas named user licenses are statically assigned. Customers are free to mix-and-match the two models in order to achieve the most benefit from the product. EMA generated three ROI models, or scenarios, based on the three possible combinations of MetaFrame Password Manager licenses, which are illustrated on the next page.

#### Citrix Licensing Scenarios

Estimates for the costs of the three Citrix MetaFrame Password Manager licensing scenarios are as follows for each organization type. Note that all three scenarios assume 3,000 total users; the concurrent user models are based on an assumption of a three-to-one concurrency ratio.

Scenario A: Pure Citrix MetaFrame Presentation Server environment

Scenario B: Mixed Citrix MetaFrame Presentation Server and desktop environment

Scenario C: Desktop only (non Citrix MetaFrame Presentation Server) environment

#### Concurrent Connected User (CCU) Model

For those organizations that will provide SSO functionality only to applications deployed on MetaFrame Presentation Server, the CCU model is the most cost-effective, as the MetaFrame Presentation Server platform enables a high level of concurrency (estimated at three-to-one) and results in economies of scale. In this model, a license is consumed only when needed. Citrix indicates that three-to-one is the concurrency ratio most commonly stated by its customers, although it is not uncommon to find ratios substantially higher.

#### Named User Model

In the named user model, users are licensed per primary login ID. This model is used for customers that do not access password-protected applications exclusively through Citrix MetaFrame Presentation Server.

#### Mixed (Concurrent and Named User) Model

Citrix allows MetaFrame Password Manager customers to mix concurrent and named user licenses. This licensing model benefits Citrix customers that have a mixture of MetaFrame Presentation Server and desktop users, allowing them to realize the benefits of the concurrent licensing model for Presentation Server users, while also deploying MetaFrame Password Manager to stand-alone desktop users.

#### Pricing Notes

These cost estimates are fully-loaded, including first-year maintenance, although the costs of rolling the agents out to the client PCs were not included. This, incidentally, is a significant added benefit for Citrix

customers, as the costs of rolling out the MetaFrame Password Manager agent to MetaFrame Presentation Server users is drastically reduced.

### Benefits

EMA estimates that password management costs large organizations \$250 per user per year. For 3,000 users, annual costs total \$750,000. Assume that Citrix' MetaFrame Password Manager will reduce the number of password-related help desk calls by 50% (which should be conservative), and the annual savings realized by the MetaFrame Password Manager solution are approximately \$375,000. This results in a three-year savings of \$1,125,000. Also consider that there are a number of "soft dollar" savings that are harder to quantify, yet significant. These include increased worker productivity (consider how long it takes for a help desk call, and that this is time that the worker is unproductive), and risk mitigation due to lower security exposures and greater levels of regulatory compliance.

### Estimated ROI

Based on the calculations above, EMA estimates the following ROI for the three licensing scenarios:

<b>Scenario A: Pure Citrix MetaFrame Presentation Server Environment Assumptions</b>	<b>Scenario B: Mixed MetaFrame Presentation Server and Desktop Environment Assumptions</b>	<b>Scenario C: Desktop Only Environment Assumptions</b>
<i>Number of CCUS: 3,000</i>	<i>Number of CCUS: 2,000</i>	<i>Number of CCUS: 0</i>
<i>Number of named users: 0</i>	<i>Number of named users: 1,000</i>	<i>Number of named users: 3,000</i>
<i>Acquisition costs: \$179,000</i>	<i>Acquisition costs: \$208,393</i>	<i>Acquisition costs: \$267,000</i>
<i>Estimated Year 2 and 3 maintenance (at 18%): \$64,440</i>	<i>Estimated Year 2 and 3 maintenance (at 18%): \$75,021</i>	<i>Estimated Year 2 and 3 maintenance (at 18%): \$96,120</i>
<i>Total three-year costs: \$243,440</i>	<i>Total three-year costs: \$283,414</i>	<i>Total three-year costs: \$363,120</i>
<i>Net three-year savings: \$881,560</i>	<i>Net three-year savings: \$841,586</i>	<i>Net three-year savings: \$761,880</i>
<i>Payback period: 6 months</i>	<i>Payback period: 7 months</i>	<i>Payback period: 9 months</i>
<i>Net present value of investment: \$432,333</i>	<i>Net present value of investment: \$364,114</i>	<i>Net present value of investment: \$228,086</i>
<i>Projected three-year blended ROI: 247%</i>	<i>Projected three-year blended ROI: 212%</i>	<i>Projected three-year blended ROI: 166%</i>

---

## Conclusions

The most compelling business case (and indeed, the sweet-spot for this product) is for Citrix customers that are fully invested in the MetaFrame Presentation Server architecture—scenario A in the model above. These customers, under the concurrent license model that fully leverages the benefits of the Citrix architecture, could realize a payback on an MetaFrame Password Manager investment in six months, with a three-year blended ROI of 247%. Mixed (scenario B) customers, who choose both licensing models, can also expect an excellent payback, in seven months, and a three-year blended ROI of 212%, and non-Citrix (scenario C) customers who choose the named user model can expect a nine-month payback and a three-year ROI of 166%. Keep in mind that these are very conservative, pragmatic ROI projections; more strategic, soft-dollar savings were not factored into the equation, and fully-leveraged ROI benefits will likely be higher.

EMA feels that the Citrix MetaFrame Password Manager product solves the single sign-on problem elegantly and inexpensively, and IT managers and executives tasked with solving this problem should seriously consider the Citrix solution as a part of their overall security management strategy. Add to that the fact that Citrix has a proven track record of delivering world-class, enterprise-scalable applications with a strong history of positive returns on investment, and the business case becomes even more compelling.

---

Citrix  
MetaFrame  
Password  
Manager

#### About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader in access infrastructure solutions for businesses, government agencies, and educational institutions. The most trusted name in enterprise access, the Citrix MetaFrame Access Suite enables people to easily and securely access the on-demand enterprise, from anywhere, anytime, using any device over any connection. Nearly 50 million people in more than 120,000 organizations around the world use Citrix every day. Citrix customers include 99 percent of the Fortune 500, 95 percent of the Financial Times European 100, and 95 percent of the Fortune Global 100. Based in Fort Lauderdale, Florida, Citrix has offices in 22 countries, and more than 7,000 channel and alliance partners in more than 100 countries. For more information visit <http://www.citrix.com>.

#### About Enterprise Management Associates, Inc.

Enterprise Management Associates, Inc. is the fastest growing analyst firm focused on the management software and services market. EMA brings strategic insights to both vendors and IT professionals seeking to leverage areas of growth across e-business, network, systems and application management. Enterprise Management's vision and insights draw from its ongoing research and the perspectives of an experienced team with diverse, real-world backgrounds in the IT, service provider, ISV and publishing communities.

---

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc.

All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

© 2003 Enterprise Management Associates, Inc. All Rights Reserved.



Corporate Headquarters  
851 West Cypress Creek Road  
Ft. Lauderdale, FL 33309

Phone: 954-267-3000  
Fax: 954-267-3100  
Email: [info@citrix.com](mailto:info@citrix.com)  
Web: [www.citrix.com](http://www.citrix.com)



ENTERPRISE MANAGEMENT  
ASSOCIATES

Corporate Headquarters  
2108 55th Street  
Suite 110  
Boulder, CO 80301

Phone: 303.543.9500  
Fax: 303.543.7687  
Email: [info@enterprisemanagement.com](mailto:info@enterprisemanagement.com)  
Web: [www.enterprisemanagement.com](http://www.enterprisemanagement.com)  
725.090803