

CA Access Control

CA Access Control is designed to provide a comprehensive solution to privileged user management, protecting servers, applications and devices across platforms and operating systems. It provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. CA Access Control helps to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. The result is a higher level of security, a lower level of administrative costs, easier audit/compliance processes and a better user experience.

Market Challenge

In 2008, the administrator of a large U.S. city's network was arrested for taking the city's network hostage; he refused to divulge the administrator password to anyone and, before being arrested, he disabled all the other administrative passwords so that no one had administrative access to a huge number of city servers and devices. This action locked down the city for days. Almost every organization is susceptible to this same risk. If the city had controlled the admin's access they would have been able to ensure that he - or any administrator - would have enough privileges to do their job, but not so many as to allow them to create a situation like this one.

Benefits

By combining host access control with privileged user management, CA Access Control can help reduce the risk and cost of managing privileged users. It is designed to help your organization to:

- › Grant access and control your privileged users providing more powerful control of privileged users over how they access and use enterprise data.
- › Authenticate your super users from one source streamlining your system access, reducing the cost of UNIX®/Linux account management.
- › Generate privileged user reports from secure activity logs in minutes, making audits easier.
- › Improve access security across the entire server network.
- › Address regulatory compliance.
- › Protect against the loss of sensitive data.
- › Enforce accountability and separation of duties.
- › Proactively report on the status of key compliance policies.
- › Reduce administrative cost and complexity.

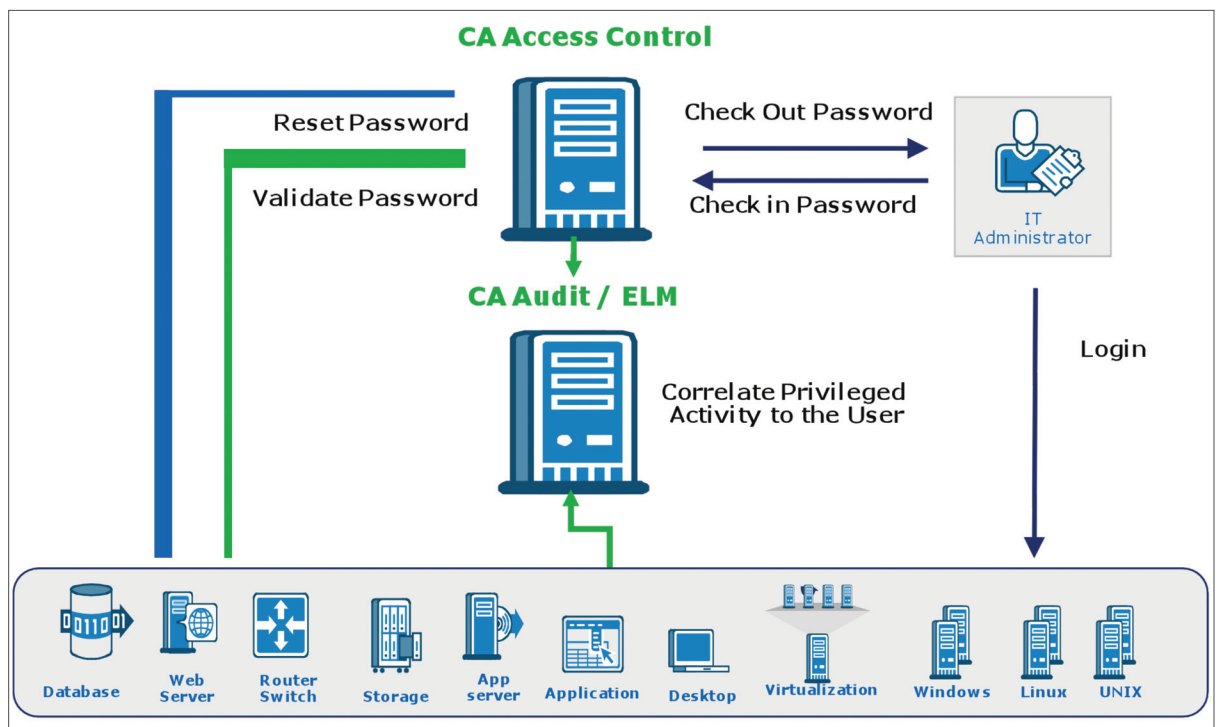
Capabilities

CA Access Control is the only solution that is capable of centrally controlling and auditing privileged users and providing temporary privileged access across servers, applications and devices — all from a single, central management console. Some of the highlights:

- **FINE-GRAINED CONTROLS** CA Access Control provides comprehensive access controls on all common operating systems. It is designed to control access to system resources, programs, files and processes through a stringent series of criteria: time, login method, network attributes and access program. These controls are required in order to enforce separation of administrative duties on the servers, consistent with industry best practices. For example: separating system administration from application administration or virtualization administration, providing controlled rights to developers or support personnel, etc.
- **PRIVILEGED USER PASSWORD MANAGEMENT (PUPM)** Even privileged users can make mistakes. By carefully segregating their duties and securely protecting the recording of their activities, organizations can protect against a privileged user making a mistake or committing a malicious act. PUPM provides secure access to privileged accounts and helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time use basis, or as necessary while providing user accountability of their actions through secure auditing.

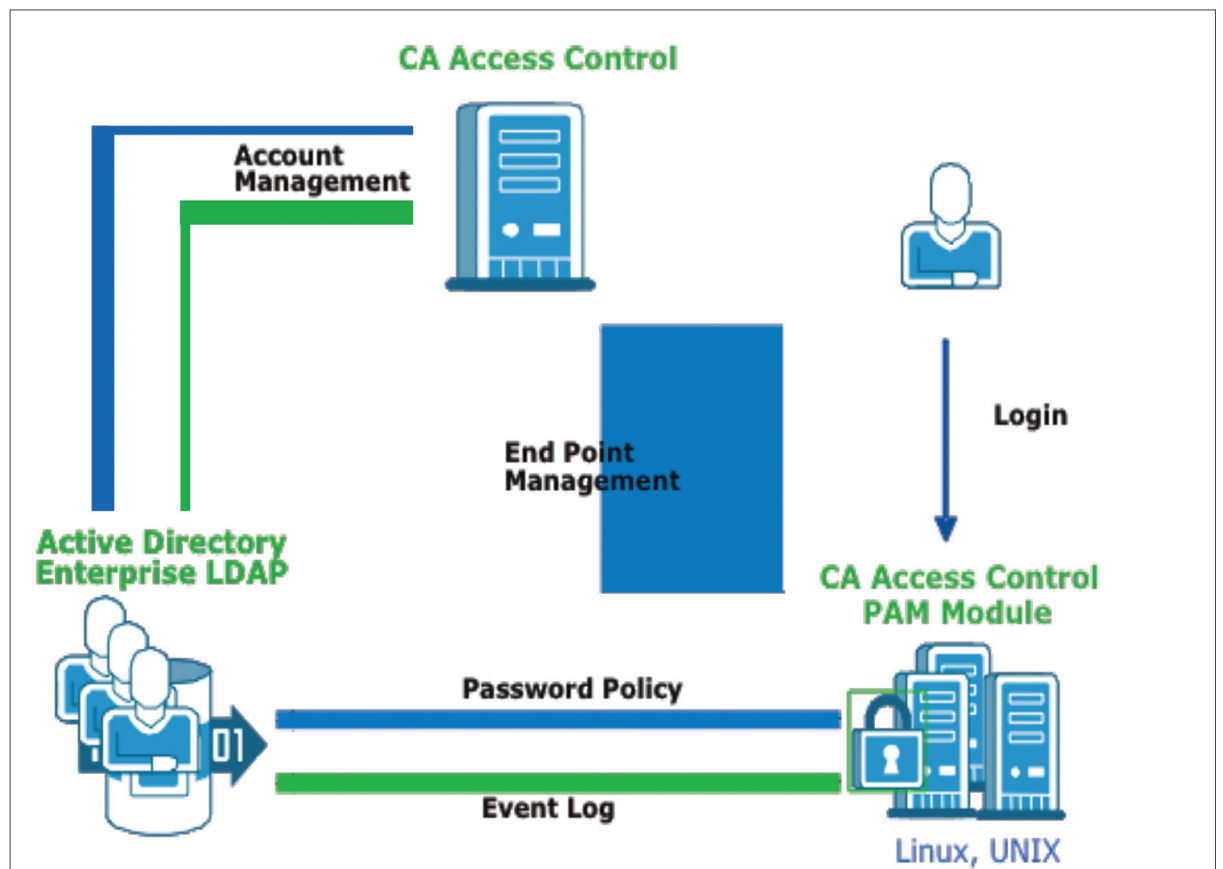
PUPM is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard coded passwords from scripts. Support for PUPM is available for a multitude of servers, applications (including databases) and devices in a physical or virtual environment. PUPM features a 'Discover Privileged Accounts' wizard as well as a feed that allows target systems and privileged accounts to be automatically fed into the system.

FIGURE A -PRIVILEGED USER PASSWORD MANAGEMENT



- **UNIX AUTHENTICATION BROKER (UNAB)** Authenticating UNIX/Linux users typically means maintaining records separate from Windows users. This complicates password synchronization and can get in the way of de-provisioning privileged users by adding time or errors. UNAB allows the management of UNIX users in Microsoft Active Directory (AD), which allows the consolidation of authentication and account information into the enterprise AD as opposed to having UNIX credentials on various systems.

FIGURE B -UNIX AUTHENTICATION BROKER



- **UNIFIED CONSOLE** CA Access Control r12.5 provides a single Web user interface that consolidates all aspects of privileged user management under a single console — host access control and privileged user management across physical and virtual systems, devices and applications.
- **DYNAMIC POLICY MANAGEMENT AND AUTOMATED DISTRIBUTION** CA Access Control is designed to streamline policy deployment and management by helping administrators to construct logical policy sets and deployment rules. Hosts can be associated to multiple logical host groups based on their characteristics, such as operating system, server type, or application. Thus when a new policy is added to a set it is automatically deployed to all of the appropriate hosts. Policy versions are maintained, changes are tracked and deviations from the policies are reported. This helps clarify complex, cross-platform policy environments and simplify administrative tasks while also providing a compliant and accountable policy management process.
- **BROAD PLATFORM COVERAGE** The diversity of server platforms, operating systems and applications across your enterprise each represent a potential vulnerability; your infrastructure is only as strong as the weakest link. CA Access Control is designed to raise the level of controls consistently across multiple supported platforms and helps to provide that distributed servers — including Linux, UNIX and Windows — are duly protected.
- **BROAD VIRTUALIZATION SUPPORT** Organizations leverage virtualization to consolidate servers and lower total cost of ownership. Visualization technologies introduce new risks associated with virtualization platform system administration. CA Access Control is designed to support a wide range of virtualization platforms including: VMware ESX, Solaris 10 Zones and LDOMs, Microsoft Hyper-v, IBM VIO and AIX LPAR, HP-UX VPAR, Linux Xen and Mainframe x/VM, providing for more consistent security management of access control risks across these virtual partitions.

- **PRIVILEGED ACCESS AUDITING AND REPORTING** CA Access Control is designed to audit all activity performed and track the activity based on the original user. All audit information is centralized and rich interactive investigative reports on user activity can be viewed from the CA Access Control Enterprise Management Console. The designed integration with CA Enterprise Log Manager allows you to more easily extend the auditing capabilities beyond CA Access Control Events to provide a holistic view of privileged activity performed in the IT environment. (A limited-use ELM license is included with AC for reporting on AC events only; the full Enterprise Log Manager product is separately licensed.)
- **ENTITLEMENTS REPORTING** Policy-based reports provide proactive views of who has access to what across your distributed and virtual server environment. These reports rely on the effective policy being enforced and allow you to more easily generate reports required by your auditors, such as User and Group Entitlement Reports, Policy Compliance Reports, Orphan Account Reports, and more. These proactive reports complement existing event-based auditing by allowing you to monitor compliance requirements and highlight existing discrepancies before incidents occur. Interoperability with external systems allows you to run policy reports through the reporting tool of your choice, create new reports based on a published schema, and customize report layouts to satisfy internal standards or auditor requests.
- **INTEGRATION WITH OTHER CA SOLUTIONS** Seamless integration with other CA Security Management solutions such as CA Identity Manager provides benefits such as rapid provisioning and de-provisioning. Integration with CA Service Desk allows the addition of a service desk ticket in both the request and break glass tasks, validation of the service desk ticket, and an approver can view the ticket for more information.

Delivery Approach

CA Services provides the CA Data & Resource Protection Rapid Implementation services for CA Access Control delivered through CA internal staff and a network of established partners chosen to help you achieve a successful deployment and get the desired business results as quickly as possible. Through our proven nine-stage methodology, best practices and expertise we can help you achieve faster time-to-value for your CA Access Control implementation.

Why CA

CA is a recognized market leader in UNIX host access control. CA provides a comprehensive solution for many aspects of privileged user management in one product and one console. CA Access Control provides the deepest controls on the widest range of devices with varying levels of controls, allowing you to get a fast return on your investment.

CA Access Control is part of the comprehensive and proven Resource Protection solution from CA that helps you control your privileged users across multiple platforms and environments. By controlling your privileged users, IT is better able to reduce risk of compliance failure and increase efficiencies.

This higher level of management control supports CA's vision for Enterprise IT Management (EITM), which is to unify and simplify IT management across the enterprise. EITM is a dynamic and secure approach that integrates and automates the management of applications, databases, networks, security, storage and systems across departments and disciplines to maximize the full potential of each. CA's comprehensive portfolio of modular IT management solutions helps the enterprise unify, simplify and secure IT to better manage risk, costs and service and ensure that IT meets the business needs of the enterprise.

Copyright © 2010 CA. All rights reserved. UNIX is a registered trademark of AT&T. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised in advance of the possibility of such damages. CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, requirement, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. The reader should consult with competent legal counsel regarding any Laws referenced herein.

