How Can I Control Privileged User Access Across The Extended Enterprise?
CA ControlMinder™ is a comprehensive solution for privileged identity management that enables you to manage privilege user passwords, report on user activities, and establish fine-grained segregation of duties across the enterprise.
Challenge

You are not alone in your worry about the growing challenges of protecting the sensitive data and applications residing on your servers. The increasing value of data, progressively more stringent regulations, and the number of privileged users that need access to critical servers, devices, and applications all make it more difficult to protect sensitive information and intellectual property. The challenge of managing privileged users includes managing secure access to critical data and passwords associated with each privileged user.

This is forcing you to work much harder to control privileged users across large, complex, and diverse environments. At the same time, your IT organization must remain responsive to business requirements, which at times requires you to make local exceptions while maintaining security and accountability. Organizations today are also faced with increasingly challenging and stringent auditing and regulatory requirements, which you must address.

You may be relying on the native security capabilities within your operating systems, but doing so presents security concerns regarding separation of duties, as well as manageability and compliance violations.

In addition to implementing security policies, you have to maintain and manage identities on UNIX®, which is another challenge. UNIX is typically managed in silos—which increases administration costs and overhead.

Opportunity

You need a single, central, and independent security system to protect server, device, and application resources across the extended enterprise, providing a flexible and accountable means to contain superuser accounts by delegating necessary privileges to authorized administrators. This security system should also be capable of providing robust controls to manage privileged users, centralize authentication and provide a robust auditing and reporting infrastructure.

CA ControlMinder™ operates at the system level to enable efficient and consistent enforcement across systems—including Windows, UNIX, Linux and virtualized environments. By distributing server security policies to endpoint devices, servers, and applications via an advanced policy management capability, you can control privileged users. Moreover, you can securely support auditing of each policy change and enforcement action in order to comply with global regulations. CA ControlMinder provides a holistic approach to access management as it includes key capabilities to protect and lock down critical data and applications, manage privileged identities, centralize UNIX authentication with Microsoft® Active Directory (AD) and provide a secure auditing and reporting infrastructure.
Benefits

CA ControlMinder allows you to create, deploy, and manage complex, fine-grained access control policies to enable only authorized privileged users to get at your most sensitive data and applications. With multi-platform (including virtual) support and integration with the rest of the CA Identity and Access Management product family, CA ControlMinder:

- Regulates and audits access to your critical servers, devices, and applications consistently across platforms
- Manages privileged user passwords
- Allows you to proactively demonstrate fine-grained control over privileged users
- Enforces your internal and regulatory compliance requirements by creating and reporting on server access policies
- Helps reduce administrative costs by centrally managing security across your globally distributed enterprise
- Enables you to authenticate UNIX and Linux privileged users from a single Active Directory user store
- Hardens the operating system which reduces external security risks and facilitates operating environment reliability
- Integrates OOTB with an auditing infrastructure that produces in-depth regulation specific reports

Section 1: Challenge

Servers: A source of complexity in today’s data center

Managing security policies across large environments remains a challenge, especially given the importance of being responsive to business requirements, which includes providing the flexibility to make local exceptions. Today’s data center requires extensive visibility across an ever-expanding set of server, device, and application resources, while providing accountability of changes and protecting the sensitive data that resides there.

Failure to manage privileged users has been directly responsible for high profile data breaches. Maintaining data integrity is one of the most important jobs of the IT professional. It is a critical mistake to embrace all of these new data center scalability and flexibility technologies without weighing the security and data protection requirements related to these new technologies.

The regulators are watching

According to the Privacy Rights Clearinghouse, since 2005 over 340 million records containing sensitive personal information have been involved in security breaches in the U.S.—resulting in significant costs
in compliance fines, to monitor the victims’ credit, reissue credit and bank cards and repair damaged brand reputation. These constant breaches have resulted in government organizations around the world mandating better practices for data protection and information security. Regulations like HIPAA, GLBA, Sarbanes-Oxley, the EU Data Privacy Directive, ISO27001, PIPEDA, and Basel II are focused on addressing these issues.

The Payment Card Industry Data Security Standard (PCI DSS) took many of these regulatory frameworks to the next level. Specifying a series of 12 requirements that must be in place to protect cardholder data, PCI DSS has forced another level of accountability on the IT organization.

Furthermore, Sarbanes-Oxley has firm requirements relative to segregation of duties, ensuring that the responsibility for complex business processes are distributed amongst many resources to provide checks and balances on these functions.

Thus, sophisticated resource protection must be implemented to meet these requirements. You also have to provide granular audit records and reports to substantiate controls, policy status and secure server access logs for each audit. These regulations specify fine-grained controls and cross-platform consistency to ensure the separation of duties, especially in mixed operating system environments. Additionally, in the event of a compromise, the ability to research the incident forensically is also mandated. This drives collection and consolidation of audit data in a central log repository.

Finally, as regulatory requirements become more stringent, compliance reporting becomes an important aspect of any server security solution. Reports should be precise, address the specific requirement in question and present the output in an easy-to-understand manner.

Sensitive data is on your servers

The type of adversary we face is evolving, as it is no longer valid to assume attackers are “out there” as nameless, faceless hackers. Today, the attacker is just as likely to be a disgruntled employee, saboteur or a business partner with questionable ethics and loyalties. Thus, you need to protect your server resources from both external attackers (who are still out there) and internal personnel—especially privileged users, who have access to all the sensitive data residing on every server, device or application they can access.

The complexity of protecting servers and enforcing accountability amongst these privileged users is significant. A common technique used by server administrators is to share privileged user accounts and use generic logins like “administrator” or “root.” This is problematic for a number of reasons:

Audit issues. Sharing user accounts prevents audit logs from really identifying which administrator made which changes on the servers, undermining the accountability that is so critical to meeting regulatory requirements.

Data access. These shared accounts typically result in providing privileged users with access to critical systems and data, predominately because it’s too hard to manage a policy across thousands of servers with granular access rules.

1 Source: Privacy Rights Clearinghouse January 2010.
The combination of privileged user access with administrator carelessness can often impact business continuity. Meanwhile, the lack of accountability makes it almost impossible to trace back to the specific administrator who committed the errors, resulting in both security and accountability issues.

**Complexity of managing privileged user passwords**

In addition to maintaining accountability for privileged user access, these shared passwords must be stored, changed and distributed in a timely and secure manner in order to comply with corporate security policy. Many applications also use hard-coded passwords in shell scripts and batch files, which actually make the problem worse. These passwords are static and available to anyone who has access to the script file including malicious intruders.

**Increased administrative burden of managing UNIX identities**

UNIX access today is managed in silos with multiple distributed account stores, where users have many accounts on different systems. This increases administration costs and overhead, and also the overall complexity of the environment, as a large number of mission-critical applications rely on UNIX for uptime and availability.

**Virtualization challenges**

In this diverse world, it’s all about enforcing a consistent policy and enabling consolidated logging across servers. A literal explosion in the number of servers and devices being managed has compounded these issues. Virtual machine sprawl means there are many more servers to manage, and since the hypervisors don’t care which operating system is a guest, this exacerbates the heterogeneity problem. Yet, maintaining the security of this expanded, virtualized data center is largely overlooked.

Virtualization also creates a new class of hypervisor privileged users that can create, copy move or otherwise manage these guest operating systems, further stressing the need for adequate separation of duties to prevent the data and applications running in these guests from compromise in addition to audit capabilities.

---

**Section 2: Opportunity**

**Manage and control privileged user access across the extended enterprise**

From a management standpoint, the old model of a system administrator responsible for a certain number of servers running a specific application is no longer sufficient. Administrators are now being increasingly specialized to deal with the inherent complexity of more distributed and complicated applications.

The decoupling of the server hardware, operating systems and applications using virtualization technology complicates this specialization. Now an email server and a database can run on the same physical server, dramatically increasing the complexity of the environment.
Thus, these administrators need to securely sign-on with privileged passwords and have different levels of access to their applications, operating systems, and hypervisors as well as devices like routers.

Providing all of these administrators with unrestricted capabilities is a serious security risk. Privileged accounts (administrator in Windows, root in UNIX) can run any program, modify any file, and/or stop any process. The inability to restrict these privileged users, so that they can only perform tasks within their job responsibilities, and to tie specific administrative actions to a specific person clearly results in a security and accountability gap and violates the key requirements of today’s security regulations. Privileged users can make errors, either by accident or maliciously. Effective privileged user management provides the ability to:

- Secure, manage and distribute privileged user credentials in an automated fashion
- Contain these users by delegating necessary privileges to the appropriate personnel only when they need them
- Maintain accountability of these users and have the ability to report on their actions

These administrators can do their jobs without exposing sensitive data or business critical resources. Additionally, such an approach provides an audit trail and enforcement of accountability over administrators and their actions. Furthermore, facing increased pressure for cost reduction, IT organizations are overcoming the internal barriers of unifying UNIX and Windows environments in the area of user authentication.

CA ControlMinder

CA ControlMinder satisfies internal policies and external compliance regulations by centrally controlling and managing privileged user access to a diverse set of servers, devices, and applications. Enabling cross-platform creation, deployment and management of complex, fine-grained access control policies, all from a single management console, CA ControlMinder surpasses the basic controls available to the native operating systems and meets the needs of the most stringent corporate policies and regulations.

The entire solution is named CA ControlMinder and is comprised of the following components:

- **CA ControlMinder Shared Account Management** provides secure storage and access to privileged user passwords
- **End-point protection and server hardening** includes the core elements of CA ControlMinder which are used to harden the operating system and enforce granular role-based access control
- **UNIX Authentication Bridge (UNAB)** allows UNIX and Linux users to authenticate using their Active Directory credentials
- **Integration with CA User Activity Reporting** allows you to centrally collect and consolidate all CA ControlMinder audit logs into a central repository that can be used for advanced reporting, event correlation and alerting
CA ControlMinder Shared Account Management

Figure A.
CA ControlMinder Shared Account Management.

Shared Account Management provides secure access to privileged accounts that helps provide 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. This is also referred to as **Administrative Check-out**.

CA ControlMinder is also designed to allow applications to programmatically access system passwords and, in so doing, remove hard coded passwords from scripts, batch files, ODBC and JDBC wrappers. This is referred to as **Applicative Check-out**.

Support for Shared Account Management is available for a multitude of servers, applications (including databases) and network devices in a physical or virtual environment.

**CA ControlMinder Shared Account Management features**

- **Secure storage of shared password.** Shared Account Management stores critical application and system passwords in a secure and protected data store. Users who need access to these sensitive passwords can “check-out” and “check in” these passwords using an intuitive, easy-to-use Web UI. Shared Account Management enforces “privileged access policies” that govern which users can use which shared accounts.

- **Shared account password policy.** Every password managed through Shared Account Management can have an associated password policy which defines its uniqueness. This ensures that the passwords generated by Shared Account Management are accepted by the end-point system, application or database. Password policies also determine an interval at which Passwordault automatically creates a new password for the account.

- **Automatic account discovery.** Shared Account Management automatically discovers all accounts on a managed end-point that is connected to the Shared Account Management Enterprise Management server. The Shared Account Management administrator can then decide which accounts are to be used. These accounts are then assigned to a “privileged access role,” which can be granted to end users as part of Shared Account Management policy.
• **Agent-less architecture.** CA ControlMinder Shared Account Management provides a server-based architecture for minimal deployment effort and risk. No agents are required on CA ControlMinder Shared Account Management managed end-points. All connections are handled from the CA ControlMinder Enterprise Management server using native capabilities. For example, databases use JDBC, UNIX and Linux use SSH, and Windows uses WMI.

• **Integration with ticketing and help-desk systems.** Integration with CA Service Desk Manager 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 to view the ticket for more information.

• **Privileged access auditing and reporting.** All privileged access is audited and logged within CA ControlMinder Shared Account Management. CA User Activity Reporting provides enhanced logging and correlation capabilities, including the ability to correlate the native logs generated from systems, applications or databases with Shared Account Management logs. Furthermore, if CA ControlMinder is installed on server end-points (UNIX, Linux and Windows), activity of all privileged users is also tracked and audited. These logs can also be centralized in CA User Activity Reporting and correlated to the check-out events generated by CA ControlMinder Shared Account Management.

• **Password restoration and rollback.** In case of a CA ControlMinder Shared Account Management end-point failure, the end-point will be restored from a backup which may not be current. In this case, Shared Account Management saved passwords will not match the restored passwords from the end-point. The CA ControlMinder Enterprise Management server displays a list of previous passwords used and has an option to restore the end-point back to the current Shared Account Management configuration.

**Shared Account Management administrative check-out**

• **Accountability of shared account access.** CA ControlMinder Shared Account Management features an “exclusive check-out” facility that only allows a specific individual to check-out an account at any given time. Furthermore, Shared Account Management can track the original user actions by correlating access events on the systems to the check-out event generated by Shared Account Management application.

• **Shared Account Management automatic login.** This feature is designed to streamline and secure the process by allowing a user to request a password and utilize it with a click of a button by automatically logging the user to the target system as the privileged user, all while not seeing the actual password. This prevents “over-the-shoulder” password theft and speeds up the process for the password requestor.

• **Shared Account Management advanced integration with CA ControlMinder.** Advanced Shared Account Management/CA ControlMinder integration lets you integrate your CA ControlMinder end-points with Shared Account Management to track the activities of users who check out privileged accounts. This feature is only supported when used in conjunction with the Shared Account Management automatic login feature, described above and lets you specify that a user must check out a privileged account through the Enterprise Management server, before they log in to a CA ControlMinder endpoint.
• **Privileged session recording and playback.** Privileged session recording and playback is now provided as part of CA ControlMinder Shared Account Management through integration with third-party software. This feature facilitates audits via DVR-type functionality for recording and playback of privileged user sessions.

• **Complete workflow capabilities.** CA ControlMinder Shared Account Management provides full dual-control workflow capabilities for regular and emergency access to privileged accounts. Workflow can be optionally enabled for certain end users and/or certain privileged accounts.

• **Break glass and emergency access.** Users perform a “break glass check-out” when they need immediate access to an account that they are not authorized to manage. Break glass accounts are privileged accounts that are not assigned to the user according to the user’s traditional role. However, the user can obtain the account password without intervention and delay if the need arises. In a break glass check-out process, a notification message is sent to the administrator. However, the administrator cannot approve nor stop the process.

**Shared Account Management applicative check-out**

• **Shared Account Management application to application.** CA ControlMinder Shared Account Management automates the management of service account passwords that would otherwise be manual (Windows Services), manages passwords used by Windows scheduled tasks that require login to the system (Windows Scheduled Tasks), and integrates with the Windows Run-As mechanism to retrieve the password of the relevant privileged user from Shared Account Management.

• **Shared Account Management application to database.** CA ControlMinder Shared Account Management can also automatically reset application ID passwords. Shared Account Management can manage service accounts used by an IIS or J2EE application server, and the applications hosted by them, by intercepting ODBC and JDBC connections and replacing them with the current credentials of privileged accounts. In most cases, CA ControlMinder Shared Account Management provides this functionality without requiring any changes to the applications. This functionality requires the Shared Account Management agent to be installed on the end-point where the application is running, or on the J2EE server, in case of a Web application.

• **Programmatic check-out from shell scripts and batch files.** You can use the Shared Account Management agent inside a script to replace hard-coded passwords with passwords that can be checked out from CA ControlMinder Shared Account Management Enterprise Management. This lets you avoid having to include hard-coded passwords inside scripts.

For more technical and in-depth details on Shared Account Management, please refer to the CA ControlMinder Shared Account Management Technical Brief.
End-point protection and server hardening with CA ControlMinder

The core elements of CA ControlMinder are the secure, hardened agents that integrate natively with the operating system to enforce and audit the granular policies required to meet compliance mandates. End-point agents are available for all the major operating systems, including all leading Linux, UNIX and Windows versions. The latest list of supported systems can be found on the CA Support website.

CA ControlMinder offers native package formats for installing and managing CA ControlMinder natively on supported operating systems. This facilitates a global enterprise environment to quickly deploy numerous managed servers.

Additionally, CA ControlMinder provides a user friendly and consistent web-based interface to manage end-point policies, applications, and devices. CA ControlMinder natively supports most virtualization platforms, including VMware ESX, Solaris 10 Zones and LDOMs, Microsoft Hyper-V, IBM VID and AIX LPAR, HP-UX VPAR, Linux Xen and Mainframe x/VM—protecting both the hypervisor layer and the guest operating systems that run on them.

In enterprise environments, using a directory for user management and directory-enabled application deployment has become common practice. CA ControlMinder supports enterprise user stores; that is, stores for users and groups that are native to the OS. This native integration allows you to define access rules for your enterprise users and groups without having to synchronize or import the users and groups into the CA ControlMinder database.
Cross-platform server protection

Many organizations deploy a diverse server infrastructure including Windows, Linux and UNIX systems. CA ControlMinder enables consistent, integrated management and enforcement of access security policies across all of these environments. The advanced policy architecture provides a single interface through which policies can be administered and distributed to Windows and UNIX subscribers at the same time. Consolidated management of Linux, UNIX and Windows servers decreases the amount of administrative work required and improves the system administrator efficiency, thus saving management cost.

Fine-grained access control

CA ControlMinder is an independent security enforcement solution, which means it does not rely on the underlying operating system to enforce server access control policies. By operating at the system level, CA ControlMinder monitors and regulates all access to system resources, including those originating from domain or local system administrators. These fine-grained access enforcement capabilities act to regulate, delegate and contain domain administrators or any other account in the IT environment and provide:

• Impersonation control. CA ControlMinder controls surrogate user delegation capabilities to reduce the exposure of unauthorized users running applications with enhanced privileges and achieve accountability of shared account activity. For example, an administrator could assume another person’s identity profile to change a file’s access control list (ACL) attributes without any accountability for their actions. CA ControlMinder protects on multiple levels by first limiting those who use Run-As and the UNIX “su” command and preserving the original user ID even after surrogate actions, ensuring user access records in audit logs show the original account. This allows users to login using their own ID and safely change their profile to a privileged account without loss of accountability.

• Superuser (administrator/root) containment. The root account is a significant source of vulnerability because it allows applications or users to assume a more powerful level of privilege than may be needed. CA ControlMinder inspects all relevant incoming requests at the system level, and enforces authorization based on the defined rules and policies. Not even the privileged root account can bypass this level of control. Thus, all privileged users become managed users and are accountable for their activities on the system.

• Role-based access control. Best practice dictates that each administrator has sufficient privileges to perform his or her job functions and no more. By providing a sophisticated role-based access control environment, administrators are unable to share an administrator password and potentially take advantage of its associated privileges. By default, CA ControlMinder provides popular administrative and auditing roles that can be customized and expanded to meet the needs of your IT organization.

• Fine-grained enforcement. Native operating systems (Linux, UNIX, and Windows) offer limited capabilities to granularly and effectively delegate certain system administration rights to less powerful user accounts. CA ControlMinder provides fine-grained enforcement and regulates access based on many criteria including network attributes, time of day, calendar or access program. Features include:
- Additional granular controls. Controls that offer specific privileges for file, services and other
  OS-level (rename, copy, stop, start) functions can be assigned to a specific administrator or an
  administration group.

- Different levels of enforcement. CA ControlMinder Warning Mode is commonly used by
  organizations to determine if proposed security policies are too strict or too lenient so they can be
  modified accordingly. Additionally, CA ControlMinder provides the ability to instantly validate the
  effects of a security policy without enforcing the restriction through the Validation Mode setting.

- Enhanced ACLs. CA ControlMinder provides many enhanced ACL capabilities to augment the
  security administrator’s ability to properly assign access rights to authorized users including
  Program Access Control Lists (PACL), which only allow resource access from a particular program
  or binary.

- Network-based access control. Today’s open environments require strong control over user access
  and information flowing over the network. Network-based access control adds another layer of
  protection to regulate access to the network. CA ControlMinder can manage access to network
  ports or network access programs and network security policies can manage bi-directional access
  by terminal ID, hostname, network address, segments or other attributes.

- Login control. CA ControlMinder can enhance login security by limiting user login by originating
  IP address, terminal ID, type of login program or time of the day. CA ControlMinder can also limit
  the concurrent login sessions of a user to enforce stringent user access to a server. Users can be
  automatically suspended after too many failed login attempts, protecting systems against brute
  force attacks. Additionally, CA ControlMinder provides secure suspension and revocation of user
  accounts in distributed environments.

**Managing and controlling access to virtual environments**

Virtualization consolidates multiple server instances on a single physical machine, delivering lower
total cost of ownership and improved machine utilization. Unfortunately, virtualization creates a
new class of hypervisor privileged users that can create, copy, move or otherwise manage these guest
operating systems. This produces an additional need for adequate separation of duties and consolidated
server resource protection to provide that all of the data and all of the applications running in these
guests are both audited and protected from compromise.

Using CA ControlMinder, these hypervisor administrators can be controlled and proper separation of
duties can be implemented.

This capability provides a critical layer of protection to mitigate virtualization risks. The end-point
agents support a long list of OS versions running as guests, as well as all major OS virtualization hosts,
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.

**Operating system hardening**

A critical layer to the defense-in-depth strategy is protecting the OS against unauthorized external
access or penetration. CA ControlMinder offers several external security measures to add an additional
layer of security for your servers.
• **File and directory controls.** Files and directories form the backbone of operating systems and any compromise can lead to denial of service and unexpected downtime. CA ControlMinder provides powerful wildcard and program access options that simplify file-level policy management. CA ControlMinder can enforce change control on critical file and directory systems, which increases data integrity and confidentiality. File-level protection is available for all types of files including text files, directories, program files, device files, symbolic links, NFS mounted files and Windows shares.

• **Trusted program execution.** To prevent the operating environment from being tainted by malware, particularly Trojans, CA ControlMinder provides first-line trusted program protection. Sensitive resources can be marked as trusted and these files and programs will then be monitored and CA ControlMinder will block execution should the program be modified by malware. Changes to trusted resources can be limited to specific users or user groups to further reduce the likelihood of unexpected change.

• **Windows registry protection.** The Windows registry is a clear target for hackers and malicious users because the centralized database contains operating system parameters, including those that control device drivers, configuration details and hardware, environment and security settings. CA ControlMinder provides registry protection through the support of rules that can block administrators from changing or tampering with the registry settings. CA ControlMinder can protect registry keys from deletion and their corresponding values from modification.

• **Windows services protection.** CA ControlMinder provides enhanced protection to limit the authorized administrators that can start, modify or stop critical Windows services. This protects against denial of service of production applications like Database, Web, File and Print, which are all controlled as services on Windows. It is essential to protect these services from unauthorized access.

• **Application jailing.** CA ControlMinder allows accepted actions to be defined for high-risk applications. Any behavior that exceeds these bounds will be restricted by an application jailing function. For example, an ACL can be built based on a logical ID which owns Oracle processes and services so its jailed behavior prohibits it from any actions besides starting Oracle DBMS services.

**UNIX/Linux keyboard logger (KBL)**

CA ControlMinder can restrict regular and sensitive user actions and can even track sessions of selective users, but what if you want to record everything done on a sensitive user’s session? The CA ControlMinder KBL feature gives you that option. KBL lies between the shell and the terminal / keyboard and captures whatever is typed in on the keyboard (input) and what is displayed on the terminal (output).

You can enable KBL simply by changing the audit mode of the administrator/user for whom you want to capture keyboard activity.
**KBL features**

- Replay the session (local mode on the CA ControlMinder end-point only)
- Print session output/input
- Print session commands
- Correlation with CA ControlMinder trace on user
- Central store with CA User Activity Reporting reports

**KBL reports** are now available in CA User Activity Reporting with drill-down views that display all commands typed in at the command prompt, and their respective output.
Centrally manage UNIX identities from active directory—UNAB

The UNIX Authentication Broker (UNAB) feature in CA ControlMinder lets you manage UNIX users from Microsoft AD. This allows for the consolidation of authentication and account information in AD as opposed to managing UNIX credentials locally on each system.

UNAB features

Centrally manage UNIX authentication. UNAB simplifies the management of local UNIX users by validating their authentication credentials against AD. User and groups need not be defined in NIS or locally in the `/etc/passwd` file. User attributes such as home directory, shell, UID, GECOS and password policies are retrieved from AD.

Lightweight PAM module. UNAB provides a small, lightweight PAM module on UNIX which is added to the end-point’s PAM stack.

Native packaging. UNAB provides native packaging for easy installation and deployment.

Integration with native Windows event log. All UNAB logs are routed to native Windows event logs. This consolidates and simplifies auditing, and also allows for integration with third-party SIM tools.

Flexible operation modes. UNAB can be configured to work in either partial or full integration mode, facilitating the migration process.

- Partial integration mode. In this mode the user password is stored in AD. At authentication time, only password validation is performed against AD. User attributes such as UID, home directory and primary group are taken from the local UNIX host or NIS and not from AD. When adding a new user to the organization, an administrator should create the user both on AD and in the local `/etc/passwd` file or NIS. Schema changes to AD are not required for UNAB to function in partial integration mode.
• **Full integration mode.** Here, user information is only stored in AD. There is no user entry in the local/etc/passwd file or NIS. User attributes such as UID, home directory and primary group are stored in Active Directory and not in the local UNIX host or NIS. When adding a new user to the organization, an administrator creates the user only in AD and provides the required UNIX attributes. Full integration mode requires Windows 2003 R2, which supports UNIX attributes.

**Dynamic LDAP attribute mapping.** In the event that your organization does not support Windows 2003 R2, which is required for full integration mode, UNAB offers a feature that allows you to dynamically map UNIX attributes to non-standard AD attributes. This avoids the complexity of extending or changing the AD schema.

**Enhanced caching capabilities and offline support.** UNAB caches every successful login into its local SQLite database. Information cached includes user name, user attributes, group membership and the password hash value. In the event that UNAB fails to connect to AD it will try validating user credentials against the local cache. That is called “offline login” support. User records will be retained in the local cache for a configurable amount of days. Local users, such as “root” and other system and application accounts can login, irrespective of AD connectivity.

**UNAB SSO.** Allows you to perform SSO between all Kerberosized UNAB hosts in the environment. If you log in to 1 UNAB host that is Kerberos-enabled, you can then automatically log in to any other UNAB host using your Kerberos credentials, which in effect provides an SSO type of solution within the environment.

**Centralized login policies.** Once UNAB is activated on a UNIX end-point, central login policies control which users can log in to which UNIX host or group of UNIX hosts. These login policies are managed and distributed using the CA ControlMinder Enterprise Management UI and stored locally on each end-point in the SQLite database. Login policies can be applied to either a single UNIX host or a logical “host group” of servers. Scoping rules can be based on AD users and groups, thereby simplifying administration overhead.

**Figure F.**

UNIX Authentication Broker.
Privileged user access auditing and reporting using CA User Activity Reporting

Compliance means that you have the correct policies in place, and that those policies are deployed, but most importantly, that you can provide proof of being compliant with both corporate policies and regulatory standards, while accounting for any deviations from the policy.

In order to prove compliance, server resource protection solutions must generate reports to substantiate password policies, entitlement levels and segregation of duties. A CA User Activity Reporting license is included with CA ControlMinder that lets you view the security status of users, groups and resources by gathering data from each end-point across the enterprise, aggregating it into a central location, analyzing the results against the corporate policy and then finally generating a report. This CA User Activity Reporting license is limited to collecting and reporting on CA ControlMinder events; if broader reporting capabilities are desired a full User Activity Reporting Module license must be acquired.

The reporting service works independently to collect the policies in effect on each end-point on a scheduled basis. Resilience is built into the system, as end-point status is reported without the need for manual intervention and whether the collection server is up or down. Additionally, the reporting service components are external to the CA ControlMinder enforcement system and do not require the end-point enforcement functions to be disrupted when reconfiguring or customizing any reports.

The reporting service is structured to allow reporting of the status of the policies that are enforced by each end-point. You can build custom reports for a variety of purposes, or use the more than 60 existing reports that CA ControlMinder provides out-of-the-box.

Policy compliance and entitlements reports

It is no longer sufficient to produce event-based reports about actions that have happened in the past for compliance reporting purposes. Instead, achieving compliance today also requires proactive reports that can highlight policy status at any point in time. To help, CA ControlMinder provides proactive reporting on user access privileges and proof of existing access controls.

Out-of-the-box, the CA ControlMinder reporting service comes with more than 60 standard reports detailing information on entitlements and the current status of (and deviation from) deployed policies as part of the default product installation. They provide immediate value by complementing existing event-based auditing to monitor compliance requirements and highlight existing discrepancies. The standard reports include:

**Policy management reports** allow you to view the status of policy deployment and deviations from the standard policies.

**Entitlements reports** allow you to view the entitlement users and groups have over system resources—or show who can access specific resources. A common use would be to see who has root access to the systems.

**User management reports** provide you the ability to view inactive accounts, user and group membership and administrative accounts, and manage segregation of duties.
Password management reports deliver information on password aging, password policy compliance, etc.

Privileged user access reports detail information on all privileged user activity including check-in, check-out, workflow approvals and other actions.

Figure G.
CA ControlMinder Shared Account Management report showing privileged accounts by endpoint type.

UNIX authentication reports provide all entitlement and report data related to the UNAB component of CA ControlMinder.

Figure H.
Detailed UNAB report showing global AD users with UNIX attributes.

Privileged user discovery wizard (user-completed wizard) will search for privileged users across the organization and automatically produce a report.
The open policy reporting provided by CA ControlMinder relies on a standard RDBMS. Interoperability with external systems allows administrators to run policy reports through the reporting tool of their choice and customize report layouts to meet internal standards or auditor requests.

**Policy deployment scorecard**

**Figure I.**
A sample report that shows a point in time snapshot of the hosts that are compliant with a specific policy.

**CA ControlMinder Enterprise Management**

Given the complexity and scalability required of today's server resources, it's critical to be able to implement and enforce a centralized policy for access control across the global, extended enterprise, while adjusting to local exceptions and business needs. CA ControlMinder has a number of sophisticated features to facilitate and streamline the management of access and allow exceptions in an accountable and visible manner.

**Logical host grouping**

You can group your end-points into logical host groups and then assign policies based on this host group membership, regardless of how your end-points are physically organized. Hosts can be members of a number of logical host groups depending on their properties and policy demands. For example, if you have hosts running a Red Hat operating system and Oracle, these can be members of a Red Hat logical host group to get the baseline Red Hat access control policies, and also members of the Oracle logical host group to get the Oracle access control policies.

Logical host groups can be used in both the Shared Account Management and UNAB components of CA ControlMinder. In Shared Account Management, logical groups of hosts such as database servers can have a common policy that allows access to privileged accounts on those servers. In UNAB, a common set of login policies can be applied to a logical host group that allows users to selectively login based on their Active Directory credentials.
Logical host groups

Figure J.
The security administrator can define logical host groups, assign policies to them and have full visibility into the compliance of these hosts with the policies.

Policy version control
CA ControlMinder lets you track policy changes by representing each policy as a single entity with multiple versions. When you create a new version of a policy, the last version remains stored and includes information on policy version deployment and un-deployment rules, who created the version (for auditing and accountability purposes) and when it was created. Additionally, an upgrade process lets you upgrade policy deployment on all assigned hosts to the latest policy version.

Common Enterprise Management Web user interface
The Enterprise Management web-based interface is simple, intuitive and allows you to perform advanced policy management, while providing an integrated view of your entire CA ControlMinder environment of servers. The web-based interface also helps you manage individual end-points or policy models and enables you to:

- Create hosts
- Assign hosts to host groups
- Create and update policies
- Assign and remove policies to hosts or host groups
- Directly deploy and remove policies from hosts or host groups
- Upgrade assigned policies to their latest version
- Audit policy deployment in the enterprise
- Browse the enterprise by host, host group or policy
- Manage discrete CA ControlMinder end-points via end-point management
- Discover privileged user accounts on managed Shared Account Management end-points
- Manage privileged user passwords on Shared Account Management end-points
- Create and manage login policies that control access to UNAB end-points
The user interface is consistent across all CA Identity and Access Management offerings utilizing the common CA Technologies framework for look-and-feel and administrative scoping and task delegation.

**CA ControlMinder Enterprise Management Console**

![Figure K. The Enterprise Management World View provides a view of the environment from an end-point perspective, a host group perspective, or a policy perspective—allowing you to browse the hierarchy down to the end-point management level if needed.](image)

**Integration with enterprise LDAP directories**

CA ControlMinder Enterprise Management can utilize Microsoft Active Directory and Sun-One LDAP as back-end user stores. Detailed steps about configuring either of these directories can be found in the CA ControlMinder product documentation.

![Figure L. Configuring CA Enterprise Management Console to use LDAP (Sun One) as a user store.](image)
Provide strong multi-factor authentication using RSA SecurID tokens

CA ControlMinder Enterprise Management Web UI can now utilize RSA SecurID tokens for strong authentication.

Following are the components required for this integration:

- Access Control 12.5 SP4 Enterprise Management running with JBoss
- Apache Web Server compiled with Proxy Module
- RSA Authentication Manager
- RSA Authentication Web Agent
- RSA Token Generator

Once verified by the RSA Authentication Manager, a user can then automatically login to CA ControlMinder Enterprise Management without supplying a User ID or password for the duration of the RSA cookie timeout period. Once the timeout period is reached, the user would then have to re-authenticate with RSA to gain access to CA ControlMinder Enterprise Management.

CA ControlMinder Enterprise Management can simultaneously support both RSA SecurID and regular User ID/Password authentication methods. If a user does not authenticate with RSA, he can still supply a UserID/Password to gain access to CA ControlMinder Enterprise Management.

Sophisticated, secure auditing capabilities

Compliance often requires critical user actions within the system to be controlled and provable through an audit trail. In order to efficiently address regular compliance audits, this data should also be centrally collected and securely managed. CA ControlMinder provides independent audit logs that cannot be modified by unauthorized users, including domain or system administrators.

CA ControlMinder generates secure and reliable audit logs which associate true user IDs to all protected resource actions (even after surrogate operations). Any action attempted by the user relating to an access policy can be recorded, including whether or not the user was allowed to successfully complete this request. If the need for an investigation arises, this detailed and accurate audit data can expedite the identification process of the attack source and activities.

Comprehensive audit modes

CA ControlMinder offers the following three auditing settings:

- Success, which generates an event anytime an audited resource is successfully accessed
- Failure, which tracks and records any and all access denials
- Warning, which generates an audit record anytime an access policy is violated, although CA ControlMinder does not deny access
You can define the auditing mode or combination of modes that should be enforced for each user, group or resource. For example, the auditing for the security administrators group and general audit level for files may be set to Failure, but specifically for the system configuration files, auditing events will be generated for both Success and Failure.

**Log routing**
Routing all relevant access events to a single, secure location is a key requirement for efficiently managing compliance. CA ControlMinder helps to provide the ability to route and centralize all access control logs. This has the benefit of not only log consolidation, but also enables the availability and integrity of these logs in case of network breach or system compromise.

**Real-time notification**
CA ControlMinder supports immediate notification about security events which can be routed to pagers or external consoles for problem resolution or other security information management systems.

**Self-protection**
Auditing daemons and logs themselves need protection from potential attacks, shutdowns or tampering. CA ControlMinder auditing services and logs are self-protected and cannot be shut down or modified. This results in log integrity and information availability for any future investigation.

**CA User Activity Reporting integration**
CA ControlMinder is integrated with CA User Activity Reporting; CA ControlMinder includes a license of CA User Activity Reporting for the purpose of collecting CA ControlMinder events only. Thus, events in CA ControlMinder are sent to CA User Activity Reporting for further handling, enabling aggregation of log files, correlation with other events across the enterprise IT environment and creation of policy specific reports. This facilitates the audit process and supports detailed investigations and verification of key compliance auditing and monitoring metrics. Features of CA User Activity Reporting also include:

**Cross-platform data collection** aggregates event data from an extensive variety of sources, including: operating systems, business applications, network devices, security devices, mainframes, access control systems and Web services.

**Real-time tools for collection, viewing and reporting** provides customizable views and reports relative to specific user roles.

**Alert management** filters and monitors critical events and executes alerts and other actions based on established policies.

**Central security data repository** stores audit data in a central repository, built around a scalable relational database for easy access, and provides reporting for historical analysis.
ControlMinder for Virtual Environments

CA ControlMinder for Virtual Environments is a single solution that manages privileged user access to virtual machines and hypervisors—helping organizations control privileged user actions, secure access to the virtual environment, and comply with industry mandates. It delivers key capabilities to manage privileged user passwords, harden the hypervisor, and audit privileged user activity.

Key benefits

By combining host access control with privileged user management, CA ControlMinder for Virtual Environments is capable of reducing the risk and cost of managing privileged users in a virtual environment. CA ControlMinder for Virtual Environments is designed to help your organization:

- Achieve compliance for your virtual datacenter
- Gain visibility and control over your virtual environment
- Automate your security operations and reduce security costs
- Expedite adoption of virtualization technology for critical applications
- Create a secure multi-tenant environment

Section 3: Benefits

CA ControlMinder—a robust solution for privileged user management

CA ControlMinder provides a solution to help manage and control privileged user access. As mentioned above, the three key components of CA ControlMinder, are:

- CA ControlMinder Shared Account Management to control privileged users
- End-point server hardening to enhance protection
- UNIX Authentication Broker (UNAB) for authenticating users from a single user store

These components can all be deployed independently or together as part of an overall solution. CA ControlMinder end-point server hardening, UNAB and Shared Account Management share the same Enterprise Management and reporting infrastructure, embedded policy store, identity and access management framework, delegation and scoping model and Web UI. This enables a rapid implementation and improved time-to-value.

CA ControlMinder addresses your concerns about the availability of applications, databases and servers by managing and controlling privileged user access, while delivering the flexibility to support local exceptions in an auditable and accountable manner. CA ControlMinder helps you:

- Mitigate risk
- Regulate and audit privileged user access
- Enforce server-based compliance and reporting
- Reduce administration cost and complexity
- Eliminate hard-coded passwords from scripts, batch files, ODBC and JDBC applications

**Mitigate risk**
CA ControlMinder mitigates risk by securing privileged user passwords and making users accountable for their actions. This reduces the risk of password cracking programs being used to gain illegal access to the server or application—thereby reducing risk and increasing data integrity.

**Regulate and audit privileged user access**
CA ControlMinder secures critical servers (both physical and virtual) by implementing fine-grained access policies that align with the user’s role in the organization, protecting against the loss of sensitive data. All administrative activities are tracked back to the specific user to enable true separation of duties at the systems level and to provide accountability via an audit trail.

**Enforce server-based compliance and reporting**
CA ControlMinder helps you secure critical servers with the ability to create and deploy specific access policies that match your organization’s internal and regulatory compliance requirements across the entire enterprise. More than 60 out-of-the-box reports cover key compliance elements, such as segregation of duties, entitlements and password policies, and allow organizations to proactively report on the status of key compliance policies. This provides visibility and accountability of the compliance and security polices while delivering flexibility to IT management.

**Reduce administrative costs and complexity**
Centrally administered server access policies, user accounts, UNIX authentication and automated management of privileged user passwords ease the burden of managing security across global, distributed, multi-platform enterprises—which is more complex in a virtual data center.

CA ControlMinder provides advanced policy management capabilities to set policies once and push them out to your servers anywhere in the world with the push of a button. The Shared Account Management feature of CA ControlMinder simplifies the process of managing and distributing privileged user passwords in real time. The UNAB feature of CA ControlMinder can lower the cost of management and strengthen security by consolidating user stores and maintaining a single account for all UNIX users.

**Eliminate hard-coded passwords from scripts, batch files and ODBC/JDBC applications**
The Shared Account Management feature of CA ControlMinder eliminates the need for hard-coding application passwords in scripts. The programmatic check-out feature of Shared Account Management dynamically retrieves passwords from the CA ControlMinder Shared Account Management server in real time, thus increasing efficiency and the overall security of the application and its corresponding data. This feature helps free up valuable system or application administration cycles which would otherwise have been required to maintain, change and distribute these password changes.
Section 4: Conclusions

CA ControlMinder enables powerful control of privileged users and enforces security compliance

CA ControlMinder provides a superior level of server, device, and application protection and eases the administrative burden of managing security across diverse systems distributed throughout a global enterprise. You no longer need to define and manage privileged user permissions user-by-user and server-by-server. With advanced policy management, logical host grouping, and a centralized point-and-click interface to deploy corporate policies, you (and your auditors) can be confident each privileged user only has the rights to the data and systems necessary for his or her job function.

You can enforce consistent security policies across diverse server environments by enabling user accounts, passwords and security policies to be shared across all managed servers, devices, and applications. To supplement this, CA User Activity Reporting enables secure, scalable and reliable audit information to be gathered to document interactions each user has with specific systems.

By providing such a broad set of supported platforms, enterprise scalability, highly available architecture, and a flexible policy management environment, organizations can be confident that CA ControlMinder will support their compliance and server protection needs both now and well into the future.

An essential part of the larger identity and access management solution

CA ControlMinder can be installed independently and provide full protection without dependencies on other CA Technologies or third-party products. However, all products in the CA Identity & Access Management solution share common approaches and components for Web user interface, administration concepts, delegation of responsibilities and reporting to ensure a consistent administrative experience.

Given that operating system access protection may be a single component of a defense-in-depth strategy, CA ControlMinder provides integration with security products from CA Technologies including CA IdentityMinder®, CA SiteMinder® and CA GovernanceMinder™.

CA IdentityMinder provides identity lifecycle management to manage identities across the enterprise. Features of CA IdentityMinder include:

- Provision users, accounts, privileges
- Manage change requests and workflow approvals
- Password and registration self-service
CA ControlMinder

CA SiteMinder provides secure Web access control for extranet applications. Features of CA SiteMinder include:

- Web SSO
- Authentication management
- Policy based authorization
- Broad Web application and server support

CA GovernanceMinder assesses, audits and cleans up access rights on systems and applications that help define and certify role models used in the organization. Features of CA GovernanceMinder include:

- Build centralized identity warehouse
- Audit, define/verify policies, certify entitlements and remediation
- Compliance reports and dashboards

To learn more about the CA ControlMinder architecture and technical approach, visit ca.com/controlminder

Agility Made Possible: The CA Technologies Advantage

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success.

For more information about CA Technologies go to ca.com.

Copyright © 2012 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 non infringement. 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, business interruption, goodwill or lost data, even if CA is expressly advised of such damages. CA does not provide legal advice. No software product referenced herein serves as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, standard, policy, administrative order, executive order, and so on (collectively, “Laws”)) referenced herein or any contract obligations with any third parties. You should consult with competent legal counsel regarding any such Laws or contract obligations.