Secure Business Intelligence on Apple® Mobile Devices

MicroStrategy Mobile for iPhone and iPad

MicroStrategy
MOBILE INTELLIGENCE

Secure Business Intelligence on Apple® Mobile Devices

Introduction

The mobile revolution is upon us. Our information gathering behavior has changed through the 100,000s of specialized mobile apps. Gone are the days of performing a keyword search in a browser. Now, we simply find the appropriate app and download it. These mobile applications are increasingly being leveraged by corporations to distribute relevant corporate data to their workforce. Mobile Business Intelligence ("BI") applications offer compelling ways for enterprises to share information with employees, customers, and partners wherever they need it. Due to the nature of mobile devices, these applications ("apps") present new security challenges that must be addressed by both the BI platform and the security capabilities of mobile devices. Data access, data transmission, and data storage must all be considered when deploying a complete and secure solution.

This paper will discuss the security capabilities of MicroStrategy Mobile on Apple's mobile devices. The combination of these two security feature sets provides enterprises with a flexible security architecture strong enough to protect your corporate information.

Securing Mobile Business Intelligence Applications

Securing mobile BI applications and the sensitive data they contain may be abstracted into three critical areas:

1. Mobile Device Security, including:
    A. Device control and protection
    B. Security of the MicroStrategy Mobile App
    C. Data protection
2. Multi-tier Architecture and Data Transmission Security, including:
    A. BI platform security
    B. Wireless and public network security
3. User Authorization for the BI application, including:
    A. Application functionality security
    B. Access control lists
    C. Data security

MicroStrategy provides a BI architecture that enables corporations to confidently address all mobile security requirements that maximizes flexibility and scalability, and minimizes administrative effort.

1. Mobile Device Security

In mobile business intelligence applications, it is essential to consider the security of the device itself, access to the BI application running on the device, and the security of any cached data persisted on the device. For the Apple iPhone, iPad, and iPod Touch, a complete security approach should include strategies for:

- Device control and protection
- Security of the MicroStrategy Mobile App
- Data protection

A. DEVICE CONTROL AND PROTECTION

Apple's iOS platform enables administrators to establish strong policies for device access. All devices have password[1] formats that can be configured and enforced over-the-air. Additionally, the iPhone provides secure methods to configure the device where specific settings, policies, and restrictions must be in place. These methods provide flexible options for establishing a standard level of protection for all authorized users.

Password Format

Apple mobile devices support password protection that prevents unauthorized users from accessing data stored on the device or otherwise gaining access to the device. An extensive set of password formatting options can be set to meet security requirements, including timeout periods, password strength, and how often the password must be changed.

[1] Apple uses the word "passcode" to refer to passwords.

The following table lists the password features configurable centrally by an administrator:

PASSWORD FEATURE	FEATURE CAPABILITY
Require Password	User must use a password. The administrator can set up the structure of the password, e.g., requiring a combination of alphabetic and numeric characters and whether to permit repeating, ascending/descending sequences.
Set Minimum Password Length	The smallest number of characters permitted in the password.
Set Minimum Number of Complex Characters	The smallest number of non-alphanumeric characters allowed.
Maximum Password Age	Number of days after password must be changed (1-730 or none).
Auto Lock Device	The amount of time it takes for the device to automatically lock when not in use.
Password History	The number of unique passwords required before password re-use is permitted.
Grace Period for Device Lock	The maximum amount of time that the device can be unlocked without prompting for password.
Maximum Number of Failed Attempts	The maximum number of times an incorrect password can be entered before all data on the device will be erased.

Policy Enforcement

Apple mobile device configuration is managed via the Configuration Utility, which allows an administrator to set up the corporate resources that the mobile users can use.

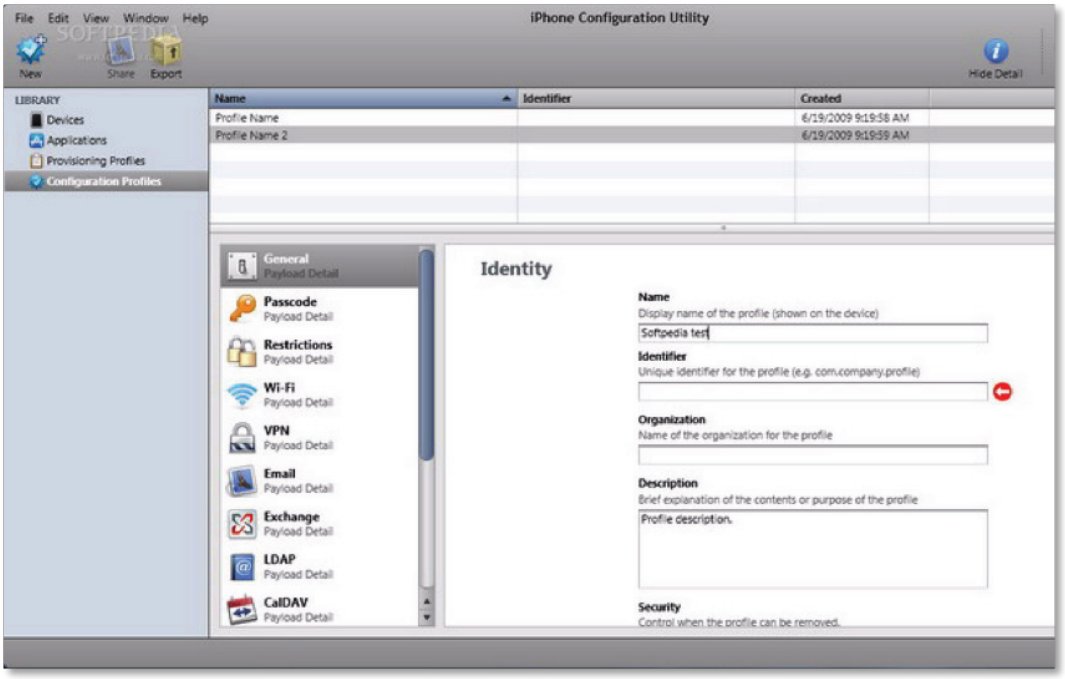


Figure 1: Apple's iPhone Configuration Utility enables administrators to establish settings for corporate iPhones. A similar utility configures corporate iPads.

Settings, such as WiFi network connectivity, corporate email access, LDAP authentication information, and secure access through VPN can all be configured centrally. The iPhone Configuration Utility can also load applications and provisioning profiles onto a device. The ability to establish password policies along with device and app settings in a configuration profile ensures that devices used within the enterprise are configured correctly and according to security standards set by your organization.

The configuration profile – an XML file that is distributed to users and loaded on the mobile device – is protected by a password only known to the administrator. Once the profile has been loaded on the device the settings cannot be changed from that profile without knowing the profile password. The profile can also be locked to the device and cannot be removed without completely erasing all of the device contents.

Configuration profiles can be both signed and encrypted. Signing a configuration profile ensures that the settings it enforces cannot be altered in any way. Encrypting a configuration profile protects the profile's contents and permits installation only on the devices for which it was created. Configuration profiles are encrypted using CMS (Cryptographic Message Syntax, RFC 3852), supporting 3DES and AES 128.

There are three ways that a configuration profile can be loaded on to the device.

1. The device can be connected directly to the machine that has the Configuration Utility installed.
2. A link can be provided on a web page which, when accessed from a web browser on the device, will load the profile onto the device.
3. A link can be provided in an email message that will load the configuration profile as if the user had accessed the link via the web browser.

For organizations that use Microsoft Exchange Server for email, Exchange ActiveSync can push certain policy updates to the device over-the-air, enabling automatic policy updates without any action needed by the user.

B. SECURITY OF THE MICROSTRATEGY MOBILE APP

MicroStrategy Mobile takes full advantage of Apple's iOS features to secure the MicroStrategy Mobile App running on the mobile device. MicroStrategy Mobile is signed to ensure that the App is authentic. iOS's "sandboxed" approach is used when MicroStrategy Mobile runs, which protects data used by other applications . MicroStrategy Mobile uses a secure encrypted keychain for storage of application credentials, extending this functionality with its own authentication options and policy controls.

iOS-Native Protection for Applications

Apple enhances security by strictly controlling how apps are developed and the application behavior at runtime.

All iPhone applications must be signed by Apple, contributing to the overall security of the device. The MicroStrategy Mobile App available on Apple's App Store has been signed by the developer using an Apple issued certificate. This ensures that applications haven't been tampered with or altered. Runtime checks ensure that an application hasn't become untrusted since it was last used.

The use of custom-configured versions of MicroStrategy Mobile can be controlled with a provisioning profile. Users must have the provisioning profile installed on their mobile device to use the application. Administrators can also restrict the use of an application to specific devices.

When applications run on Apple mobile devices, they are "sandboxed" so they cannot access data stored by other applications. In addition, iOS system files, resources, and the kernel are shielded from the user's application space. If an application needs to access data from another application, it can only do so using the APIs and services provided by iOS. Code generation is also prevented.

Secure Application Authentication

Apple provides a secure, encrypted keychain for storing digital identities, user names, and passwords. Keychain data is partitioned so that credentials stored by third-party applications cannot be accessed by applications with a different identity. This provides the mechanism for securing authentication credentials on mobile devices across a range of applications and services within the enterprise.

MicroStrategy Mobile enables administrative control of password policies for the MicroStrategy BI platform. These policies are configured by administrators via a web-based Mobile Configuration interface.

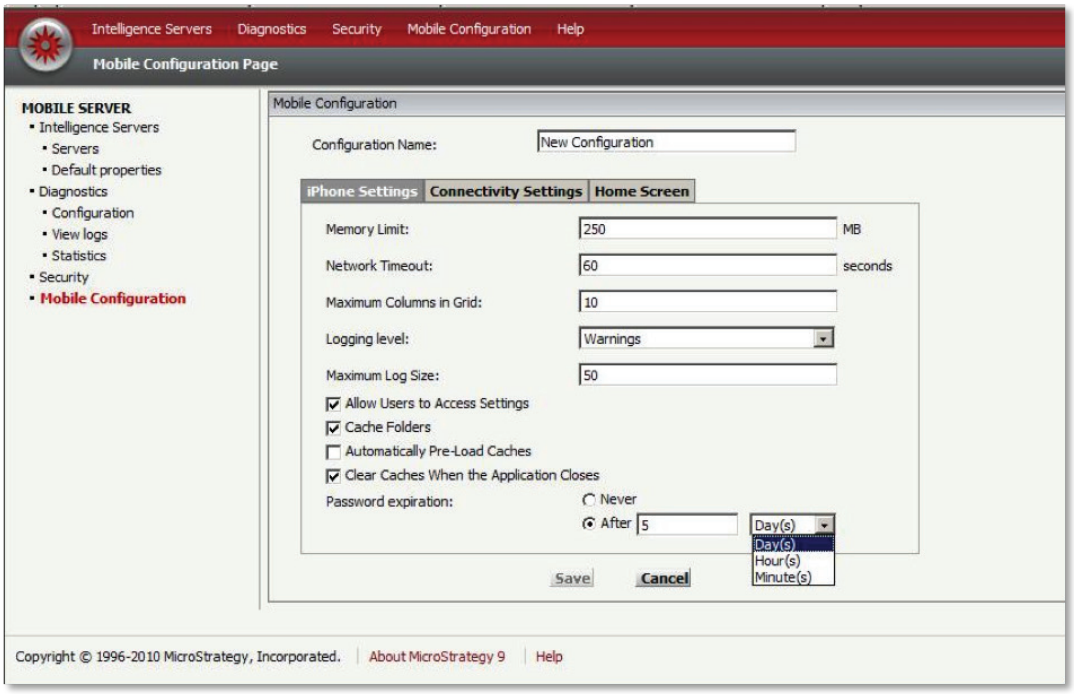


Figure 2: MicroStrategy's Mobile Configuration interface controls native client app settings for Apple Mobile devices.

The MicroStrategy BI platform maintains a profile for each user of the BI system. These are created using a graphical interface, scripts with textual commands, or synchronized directly with Windows or LDAP user directories. Validation of login credentials when the user initially runs the MicroStrategy Mobile App can be performed using:

a. *Standard Authentication.* With standard authentication, user logins, passwords in an encrypted hashed format, and security profiles are stored within MicroStrategy metadata. The login and password stored in MicroStrategy Mobile are sent to the MicroStrategy BI platform using a 160-bit one-way encryption algorithm, where they are compared to the login and password stored in the MicroStrategy metadata repository. If they match, the user is granted access to the BI system. Throughout the user's session, all security settings associated with the user will remain in effect, and be applied in a manner that is fully transparent to the user.

b. *Linked Authentication.* Many corporations have a single, centralized security directory which governs user access to internal systems and applications across the entire enterprise. MicroStrategy integrates seamlessly with security directories through linked authentication, which is also referred to as external authentication. Benefits of linked authentication include reduced administration and maintenance of users in the BI system and increased ease of use for end users. Linked authentication is often automatic, meaning the

MicroStrategy system detects the user credentials, and automatically validates those credentials against corporate security systems, such as Lightweight Directory Access Protocol (LDAP), Microsoft Windows Active Directory®, or Windows NT® LAN Manager (NTLM).

With automatic, linked authentication, users typically use a single login to access both the network and the MicroStrategy BI platform. Business users are able to move freely between all BI applications and other enterprise applications on their mobile device without maintaining multiple logins and passwords. This single sign-on capability further simplifies administration and maintenance of security profiles and groups, and complementary authentication technologies such as digital certificates are applied transparently to the MicroStrategy BI platform.

C. DATA PROTECTION

Apple's iOS-based mobile devices include a variety of security features designed to protect data stored on the device itself. These features enhance the security of a mobile BI implementation.

Encryption

iPhone 3GS, iPhone 4, and iPad offer hardware-based encryption. This encryption uses AES 256-bit encoding to protect all data on the device. Encryption is always enabled, and cannot be disabled by users.[2] MicroStrategy takes full advantage of iOS's encryption to protect application data cached locally.

Any mobile application data, including the MicroStrategy Mobile App, backed up in iTunes to a user's computer can be encrypted. When an encrypted configuration profile is stored on the user's device, this capability is enforced automatically.

Remote Wipe

If a device is lost or stolen, all the data can be removed from the device by issuing a remote wipe command. This also deactivates the device. If the device is configured with an Microsoft Exchange account, the administrator can initiate a remote wipe command using the Exchange Management Console (Exchange Server 2007) or Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 or 2007). Users of Exchange Server 2007 can also initiate remote wipe commands directly using Outlook Web Access.

Local Wipe

Devices can also be configured to automatically initiate a local wipe after several failed password attempts. This is a key deterrent against brute force attempts to gain access to the device. By default, Apple's mobile devices will automatically wipe the device after 10 failed pass-code attempts. As with other password policies, the maximum number of failed attempts can be established via a configuration profile or enforced over-the-air via Microsoft Exchange ActiveSync policies.

MicroStrategy Report Caches

The Mobile Configuration interface of MicroStrategy Mobile allows administrators to set a variety of local data caching options. Administrators can specify a maximum cache size on the device for users, automatically wipe the device of all locally cached every time the MicroStrategy Mobile app is closed, and set options for automatically re-building new caches for user subscriptions once the application is re-loaded.

---

[2] Per Apple Inc., *iPhone in Business Security Overview*, June 2009.

2. Multi-Tier Architecture and Transmission Security

MicroStrategy Mobile for iPhone and iPad leverages mobile device capabilities and incorporates architectural and cryptographic features that maximize the security of data transmission:

- Across the private networks where the MicroStrategy platform is managed
- Through private and public wireless 3G or WiFi transmission

A. BI Platform Security

MicroStrategy Mobile is based on a secure, multi-tier architecture. Within this architecture, six characteristics ensure the integrity of the data in the mobile BI system.

1. Secure communications across firewalls

The MicroStrategy platform is normally installed on more than one servers to distribute the BI workload. Secure communication across these servers is often governed by layers of firewalls constructed into Demilitarized Zones (DMZ). Using multiple firewalls, two distinct DMZ's are created with one DMZ protecting the Mobile and Web servers and the second DMZ securing the infrastructure of the data sources and MicroStrategy Intelligence Server.

2. No database connection from the MicroStrategy Mobile Server

An effective DMZ is characterized not only by the mere presence of firewalls. It is equally important that the architectural component that accesses the database should reside behind a firewall. MicroStrategy Intelligence Server is the core of MicroStrategy's BI platform, and is the only component that accesses the database. It resides between two firewalls in the same way that the MicroStrategy Mobile Server resides between two firewalls. Only in this configuration is a hacker who gains access to the MicroStrategy Mobile server prevented from accessing the database.

3. Single port control for data access

Firewalls protect corporate information assets by limiting which application has access rights to certain computer network ports. To take full advantage of this protection, the Web-based application must allow for granular port access control. MicroStrategy's Mobile and Web architecture allows administrators to configure which port is used for inter-server communication. Connections to other ports can be disallowed by the firewall, thus minimizing exposure.

4. No external Remote Procedure Calls (RPC) or Remote Method Invocation (RMI) calls

RPC and RMI calls are hazardous because they allow hackers to access and control remote and distributed computer processes. These calls often allow anonymous access through separate, open ports in the firewall. MicroStrategy Mobile uses only XML to communicate with the Intelligence Server, eliminating the need for RPC or RMI calls completely

5. Transmission Security

MicroStrategy's BI platform provides an option to encrypt communications between its server components, i.e., between the MicroStrategy Intelligence Server and MicroStrategy Mobile Server, using an AES 128-bit algorithm. As AES is in the class of block code ciphers (i.e., the same input plaintext will result in the same ciphertext), MicroStrategy has employed the algorithm in cipher block chaining mode (CBC), where previously transmitted

ciphertext is combined with the input plaintext in successive cipher blocks, which randomizes the input. This is particularly important for BI applications since the transmitted information tends to be primarily numeric. If CBC mode were not used, the likeliness that the cipher stream could be broken by a motivated attacker would be considerably higher.

6. Protection of Stored User Credentials

MicroStrategy follows industry standard security practices for the protection of sensitive user credential information that is stored in the MicroStrategy metadata repository. Rather than storing the actual user password a secure hash of the password is stored. Because the hash is a one-way secure operation, even if this data were compromised the information would not be useful as there is no known way to derive the original password from the hashed value in order to gain access to the system. MicroStrategy uses the RIPEMD-160 hashing algorithm for this purpose. This algorithm does not have any known attacks at this time.

B. WIRELESS TRANSMISSION AND PUBLIC NETWORK SECURITY

There are three primary network protocols and configurations that should be considered when investigating the security of wireless data transmission to iPhone and iPad mobile devices.

1. *Internal Use via Private WiFi.* The MicroStrategy App will only be used internally (i.e., only by enterprise employees) and MicroStrategy Mobile BI applications are only accessible via the internal WiFi Network.
2. *Internal Use via 3G and Public/Private WiFi.* The MicroStrategy App will be used internally and will be accessible by 3G (i.e., GSM) public wireless networks, and both internal (private) and external (public) WiFi networks via the internet.
3. *External Use via 3G and WiFi.* The MicroStrategy App will be used externally (e.g., by consumers or customers) and will communicate via the internet across both 3G and WiFi networks.

The Apple iPhone and iPad support proven encrypted networking technologies for ensuring that users are authorized and that data is protected during transmission.

Virtual Private Network (VPN)

Both the iPhone and iPad devices are capable of interoperating with a large majority of corporate VPNs. In particular these devices offer strong support for IPSec, L2TP and PPTP protocols. A VPN set up between the mobile device and the MSTR BI platform will provide the strongest security available for communications with the iPad and iPhone devices. VPN provides secure authentication using standard X.509 digital certificates to ensure that the devices can legitimately access the server, and also encrypts data communications. The VPN approach is recommended for secure internal BI applications. Implementation and set up should be relatively straightforward regardless of the corporate environment and extensions to existing corporate VPNs to support a compatible environment with the Apple devices are readily available.

HTTPS

The MicroStrategy Mobile supports HTTPS communications between the mobile device and the MicroStrategy Mobile Server. This communications is secure in that the server is authenticated by the client (i.e., the device) and all communications are encrypted. Authentication is based on validation of an X.509 digital certificate. The underlying communications protocol is based on SSL. At the outset of communications, the server is authenticated by the client and then a mutually-acceptable cipher for encrypting further data transmissions is negotiated between the device

and the server. Once the cipher has been chosen all communications between the device and the Mobile Server are encrypted using the chosen cipher. MicroStrategy recommends that the web server where the MicroStrategy Mobile Server will be hosted be configured to use only the subset of ciphers that have been proven to be highly secure. This will provide a high level of assurance that the selected cipher used for session communications is considered strong by most enterprises.

Wireless Local Area Network

Apple mobile devices support WPA2 Enterprise to provide authenticated, secure access to enterprise wireless networks. WPA2 Enterprise uses 128-bit AES encryption, protecting data that is transmitted over a Wi-Fi network connection. Apple mobile devices also support 802.1x standard enabling integration with organizations that use the popular RADIUS networking protocol.

Together, these technologies are typically applied to three wireless usage scenarios above as follows:

NETWORK	NETWORK SECURITY PROTOCOL
1. Internal Use via Private WiFi	WPA / WPA2
2. Internal Use via 3G and Public/ Private WiFi	VPN or HTTPS / SSL
3. External Use via 3G and WiFi	HTTPS / SSL

3. User Authorization for MicroStrategy Mobile

MicroStrategy Mobile determines and enforces security policies governing the business intelligence functionality, reports, and data for which the user is authorized. Authorization refers to the three-dimensional process by which the application determines:

- Application functionality privileges
- Object access permissions
- Data access security

MicroStrategy Mobile utilizes the same sophisticated user authorization management framework available in the MicroStrategy BI platform. This framework distinguishes between users based on each individual's knowledge, business needs and security level. User access to application functionality, reports, and data is managed dynamically based on these parameters.

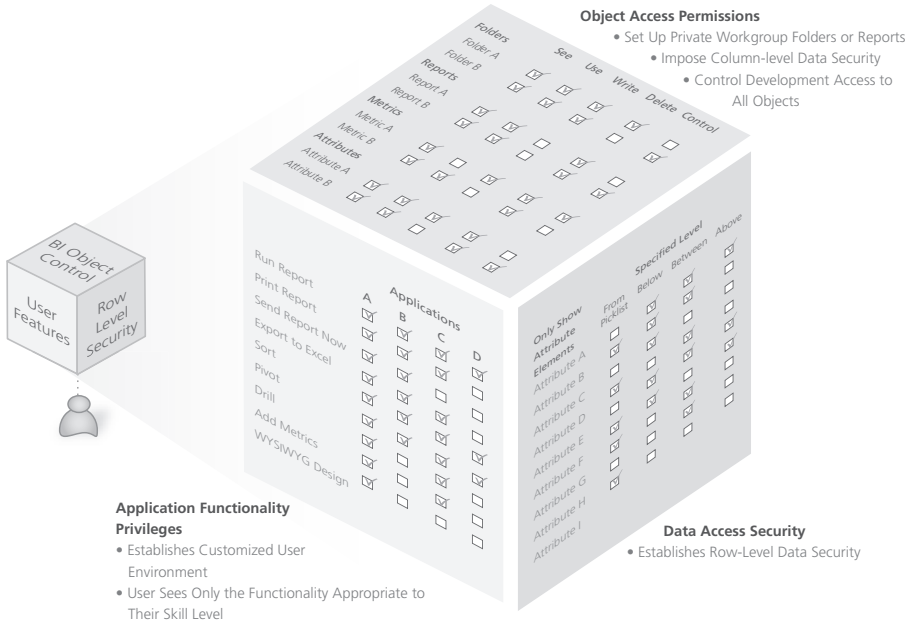


Figure 3: MicroStrategy's comprehensive application, object access, and data access security provides granular control for mobile BI administrators.

A. APPLICATION FUNCTIONALITY PRIVILEGES

Users fall into various types, including casual users, power users, application developers, and administrators. Depending on their levels of sophistication, certain users might need basic functionality such as running reports and sorting the results, while power analysts might need to create their own analyses and publish them. Application developers need object creation privileges, and administrators require specific monitoring and management functionality. MicroStrategy employs over 130 privileges to assign application functionality to user groups, user roles, and individual users. These privileges can be assigned to users, user roles, and user groups through a graphical interface or through text-based commands.

Such fine-grained control ensures that all users access the MicroStrategy platform according to their level of proficiency. With administrators setting various levels of application functionality security, users can start using the BI applications with minimal training. Over time, administrators may grant users more privileges as they become more experienced.

B. OBJECT ACCESS PERMISSIONS

Individual MicroStrategy metadata objects are governed by their own security permissions, called Access Control Lists (ACL). Each data abstraction object, business abstraction object, report component, and report definition may have its own unique ACL, which grants users or user groups a set of privileges for the object. To simplify application maintenance, an ACL can apply to many objects. MicroStrategy's object-oriented metadata allows ACLs to be inherited by child objects and applied recursively. Seven permissions can be combined to grant or deny object behavior to user groups or to individual users.

- Browse – view the object in a folder and viewer
- Read – view the object's properties (definition and, ACL settings)

- Write – modify the object's definition but not the ACL settings
- Delete – delete the object from the metadata repository
- Control – modify the object's ACL settings and take ownership of the object
- Use – reference the object when creating or modifying other objects
- Execute – reference the object when running documents and reports

These permissions have been arranged into predefined groups that reflect the most commonly used sets of permissions as follows:

- View – contains Browse, Read, Use, and Execute
- Modify – contains Browse, Read, Write, Delete, Use, and Execute
- Full Control – contains Browse, Read, Write, Delete, Control, Use, and Execute
- Denied All – explicitly denies all object access

For example, when a report contains many metrics, each metric's "Execute" permission determines whether a user can view that metric in the report. Developers can minimize the number of reports they create and store in the metadata repository by making use of this feature. When two users run the same report, they will receive different versions of that report from a single report definition in the metadata, based on their ACL settings. Different users may even be given access to completely different subsets of the data and business abstraction objects. For example, corporate expense attributes, metrics, and reports can be restricted to managers and finance department users. ACL settings can also be applied when drilling so that some users can drill down to detailed information while others cannot.

C. DATA ACCESS SECURITY

MicroStrategy Mobile supports mechanisms for securing data that can be incorporated as strategies during BI application development.

Securing Data using Database Security

In a database, security restrictions for database logins can be placed on tables, rows, and columns. MicroStrategy's BI platform accesses data sources using database connections. Separate database connections can be created to access the same data source with different logins. MicroStrategy users and user groups are linked to database connections using connection maps.

All users allocated to a database connection will log in to the database with the same credentials, and will be subject to the security setting in the data source. Furthermore, database views may include a restriction by database login in their definition. This login, obtained from the database connection information, limits the rows that are selected by the view when processing queries. These security views provide row-level security for every query submitted by the user. Since an administrator defines this security view inside the data source, all query tools accessing the data source with a particular login will use the view. The SQL statement used to create the database view can also be used within MicroStrategy to define a logical table in the metadata.

The main disadvantage of using database views to manage security is that performance may degrade because the view is processed at run-time. Security views must also be recreated every time new data is added to the tables in order to optimize the query that defines the view.

Securing Data with Security Filters

Security filters provide a method for ensuring cell-level data security. All the filtering sophistication available in

MicroStrategy can be used to limit the data that a user or user group can access. For every data request, including documents, reports, and prompt lists, additional filtering criteria is automatically added to the query to restrict the result set to information that the user is permitted to access.

Take an example of a new Northeast Regional manager who was transferred from the South at the beginning of 2010. She needs access to all current Northeast data, but may also need access to South data for prior years. A security filter using this criteria will restrict all data requests to the Northeast region for 2010 data, and the South region for prior years.

Security filter definitions may also specify Top and Bottom range attributes. A Top range attribute specifies the highest hierarchical level that the security filter allows the user to view. If a Top level is specified, the security filter expression is NOT raised to any level above the Top level. A Bottom range attribute specifies the lowest hierarchical level that the security filter allows the user to view. If this is not specified, the security filter can view every level lower than the specified top range attribute that otherwise meets the filter expression criteria.

Many companies use hand-coded SQL queries in their MicroStrategy BI applications to retrieve and distribute select information to groups of business users. The difficulty of ensuring appropriate data security on these freeform SQL queries is significant. MicroStrategy addresses this difficulty by embedding security filters within freeform SQL queries. Though these SQL queries are hand-coded and static, they can include a "wildcard" that will dynamically insert the appropriate user security condition at run time while leaving the rest of the custom SQL query unchanged.

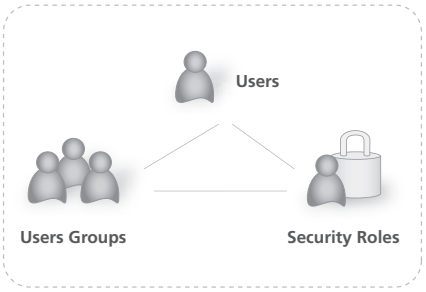
MicroStrategy also provides a user login condition that incorporates individual user logins as a condition in the SQL query. This ability integrates user data access based upon security tables inside the data warehouse with security profiles maintained inside the MicroStrategy BI platform. The user login condition can apply to all users of a BI application or to specific users or user groups. Even more fine-grained control is possible by including the user login condition on a report-by-report basis.

Organizing Users into User Groups and Security Roles

With all of the granular controls for user authorization described above, administrators can easily be overwhelmed by the task of assigning security parameters for every individual. While offering maximum flexibility with full control at the individual level, MicroStrategy's administration architecture also employs a far more powerful and scalable mechanism to organize security profiles into group- and role-based user assignments. All elemental building blocks of User Authorization – Application Functionality Privileges, Object Access Permissions, and Data Access Security – are first assigned to a series of user groups and security roles. Users are then assigned to any number of groups and roles, and the MicroStrategy BI platform dynamically merges privileges, permissions, and security filters to create an aggregate user profile for each user upon login.

User Groups
- Are a Set of Users
- Privileges and ACLs can be Assigned to User Groups
- User Group Privileges Apply to All Projects
- Example: Users with Common Information Needs:
  - Marketing Users
  - Sales Users
  - Finance Users

Security Roles
- Are a Set of Privileges
- Security Roles can be assigned to Users and/or Specific Groups
- Security Roles Apply to Specified Individual Projects and ACLs can be Assigned to User Groups
- Example: Users with Common Functionality Needs:
  - Executive Users Need to Run, Sort, and Print Reports
  - Business Analysts Need Additional Capabilities to Drill and Change Subtotal Definitions



Users
- Are Identified by a Unique Login and User Name
- Users are Defined in the Metadata Repository
- Users Exist Across Multiple Projects

Figure 4: All three dimensions of user authorization (application functionality privileges, object access permissions, and data access security) may be defined at the user, group or security role level.

With MicroStrategy Mobile, every user effectively has a personalized user profile that governs all privileges across all BI applications and reports. Each user sees only pertinent data, and interacts with the data in a controlled way, regardless of who created the report, and how the report is defined.

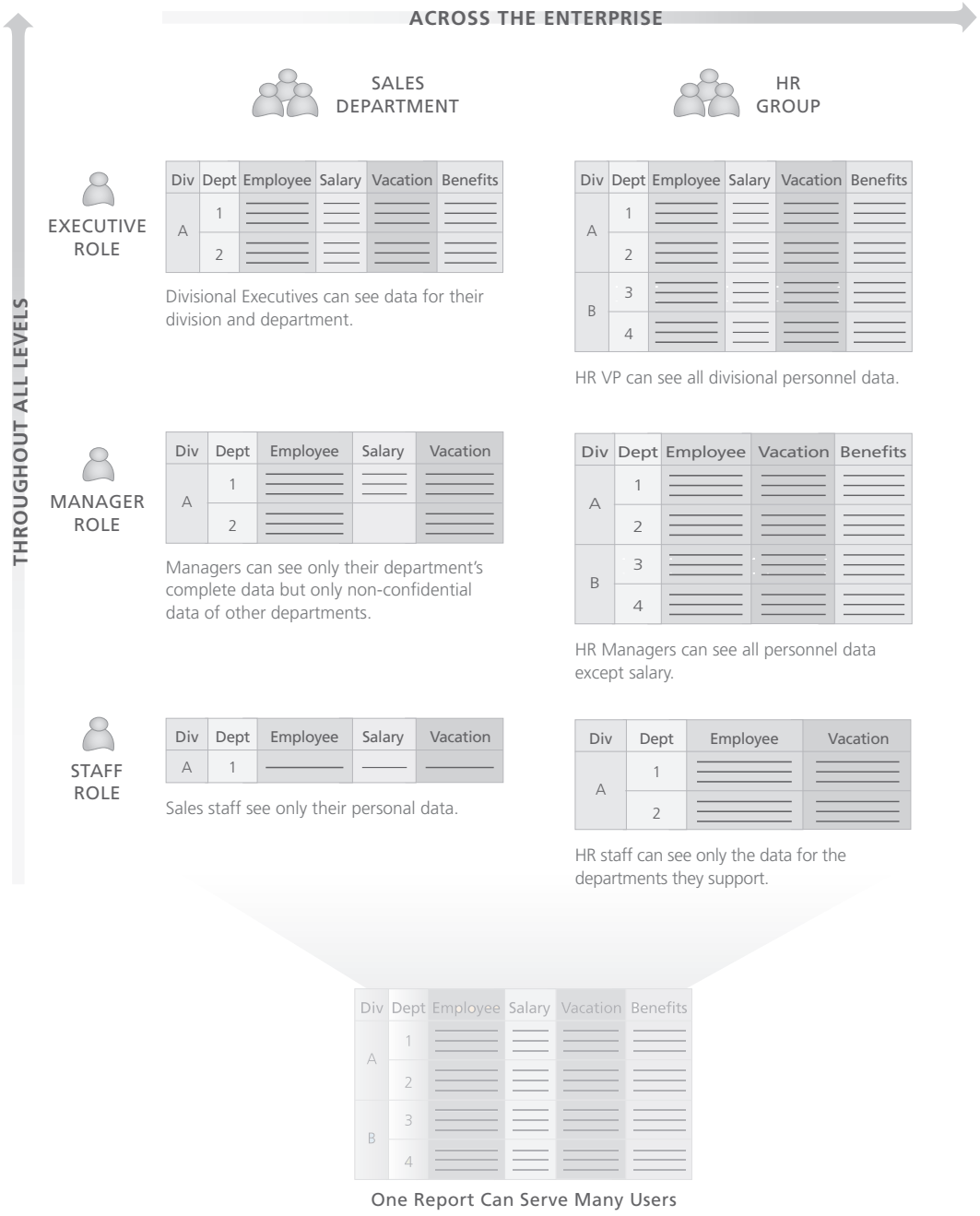


Figure 5: MicroStrategy's architecture enables a single report to securely serve the needs of individual users throughout the enterprise, across departments, in any functional role or level in the enterprise organizational structure, accessed through any client – web browsers, mobile devices, and more.

MicroStrategy – A Secure Mobile BI Solution

Secure mobile applications are already available in the Apple App Store. iPhone and iPad applications that deliver high-value to consumers in high-security industries, such as banking, electronic trading, healthcare, and insurance, are proliferating. This demand for data is extending to the corporate world. Enterprises need to share their information with employees, customers, and partners. MicroStrategy Mobile business intelligence is at the forefront to deliver on this vision in a safe, secure manner. MicroStrategy Mobile is built to meet the security requirements of any organization and is designed to integrate seamlessly with the proven security features of the Apple iPhone and iPad. Robust features for device security, data security, authentication, authorization, and transmission security combine to provide a layered approach to protect sensitive data in mobile business intelligence applications.

COLL-0967 0910

MicroStrategy Incorporated • 1850 Towers Crescent Plaza • Vienna, VA 22182 • 703.848.8600 • www.microstrategy.com