

What's new in MicroStrategy 10.6

TABLE OF CONTENTS

WHAT'S NEW IN MICROSTRATEGY 10.6	4
MICROSTRATEGY ANALYTICS 10.6 RELEASE FEATURES:	4
NEW IMPROVED DISTRIBUTION CAPABILITIES	4
Distribute and share interactive dashboards (.mstr files)	4
NEW EXPORT ENGINE	5
Support for export of maps, custom visualizations	5
Support for HTML tags	5
Support for multi-page export	6
Support for bookmarks	6
Installation of a separate micro-service for the PDF export engine	7
NEW MAPPING CAPABILITIES	7
One map visualization that supports multiple base maps	7
Multiple layers on maps in dashboards	8
Plot pie chart markers on maps	9
Attribute multi-form support with JSON data PI	10
Support for large cubes/datasets	10
Support for 3rd party API to upload data and create a new dataset	11
MICROSTRATEGY PLATFORM ENHANCEMENTS	11
New data sources certified	11
SAML authentication support for MicroStrategy web and mobile	12
Enhanced authentication support for URL sources (JSON/oData/text files)	12
Share a database instance with a subset of users	13
MOBILE	13
Unified mapping for easier maintenance and seamless user experience	13
View multiple layers on maps in dashboards	14
Support for different marker types and corresponding thresholds in maps	15
Switch marker type using metric toggler in maps to get the most insightful view	15
Support for metric data labels in Visual Insight dashboards	16
Secure Android apps with native Airwatch integration	16

TABLE OF CONTENTS

MICROSTRATEGY SECURITY	17
Usher Professional: Two-way communication enhancements	17
Usher security client: iCloud and google drive badge recovery	18
Usher for Android: fingerprint biometric	19
Usher network manager: Digital certificate expiration notifications	20
Usher VPN Proxy Module: High performance universal VPN proxy services	20
Usher gateways: Office 365 login	21
Usher gateways: Amazon Web Services (AWS) directory services integration	21
Usher gateways: Okta universal directory integration (early adopter)	21
Usher gateways: OpenID connect (early adopter)	21
Usher for Mac: Unloack via push notification (early adopter)	22
Usher for Windows: Unloack via bluetooth or push notification (early adopter)	22

What's new in MicroStrategy 10.6

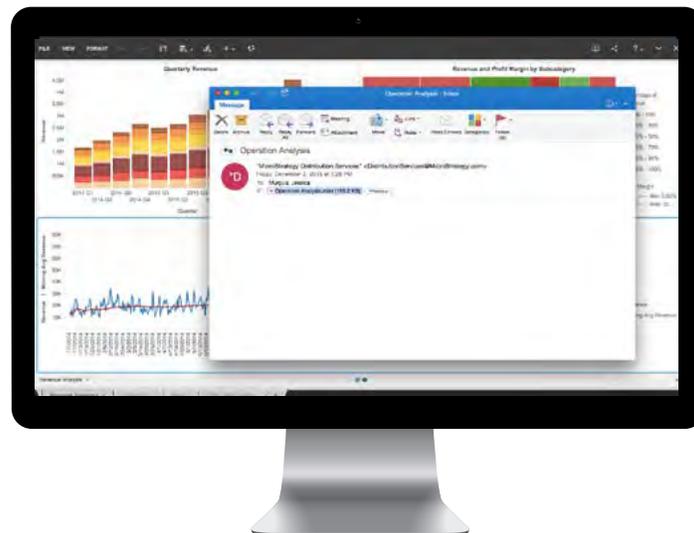
The release of MicroStrategy 10.6 offers several new features and follows the announcement of MicroStrategy Desktop™, that was made available for free to everyone, including existing customers and users who are new to MicroStrategy. This update complements the announcement made in October 2016, by offering completely revamped distribution services and an export engine that greatly enhances the delivery of personalized dashboards to end-users across the enterprise.

This release also offers several other enhancements and features across MicroStrategy Desktop™, MicroStrategy Web™, MicroStrategy Mobile™ and Usher™. The top features available with this release are highlighted in this document. The complete list of features and fixes are available on the MicroStrategy community.

MicroStrategy Analytics 10.6 Release features: New improved distribution capabilities

Distribute and share interactive dashboards (.mstr files)

With revamped dashboard distribution capabilities in MicroStrategy 10.6, it is now possible to share completely interactive dashboards for offline analysis! For customers who would like send more than a static PDF file to end users, and would like to send fully interactive dashboards, now have the option to share an .MSTR file as an attachment. It's as simple as "File, Send". Recipients can leverage the free MicroStrategy Desktop tool to easily open the dashboard and have full interactivity for data discovery. It is now also possible to schedule dashboards through distribution services in this latest version, making it possible to reach more end users. Every business user can now slice and dice data with complete interactivity, edit the dashboard, swap out visualizations and even blend new data into existing dashboards – even when offline.

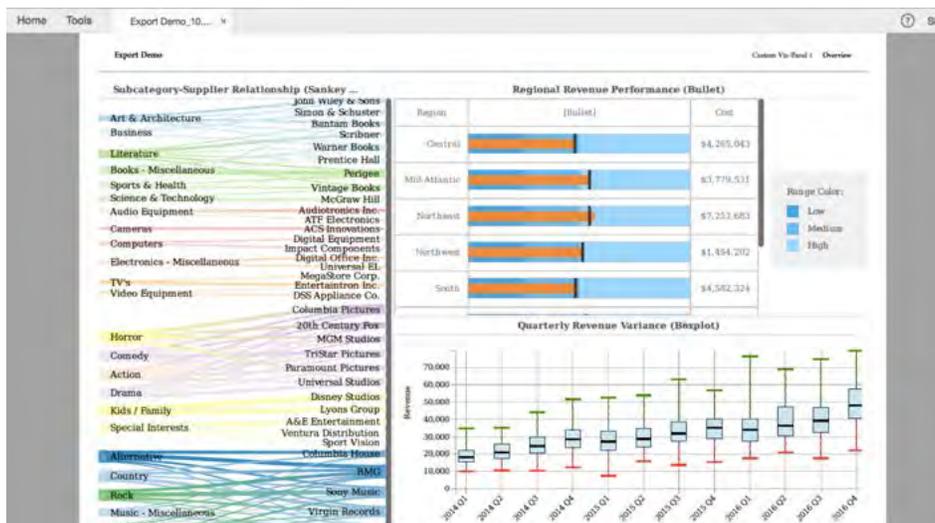


New export engine

MicroStrategy 10.6 delivers a completely revamped export engine with new capabilities that enhance the ability to share dashboards in PDF format. The new feature, that is installed a separate micro service with the Server installation, provides MicroStrategy Web users the ability to generate high-fidelity PDF files with support for maps, D3 and custom visualizations, HTML containers and other HTML-tag based content. Additional highlights include smart pagination, support for dashboards with multiple sheets and panels, PDF bookmarks, and embedded images.

Support for export of maps, custom visualizations

In version 10.6, the new capabilities provide MicroStrategy Web users the ability to export any graph, HTML (including tags), geography maps or D3 visualizations (including other custom visualizations). This greatly enhances the user experience, by allowing any user to share identical PDF versions of the dashboards they create, regardless of the chart type contained in the dashboard.



Support for HTML tags

The new PDF export engine also supports cases where text strings with HTML tags are displayed on the dashboard. The formatting from HTML tags as seen on dashboards on MicroStrategy Web, will be retained when exported to PDF format.

Support for multi-page export

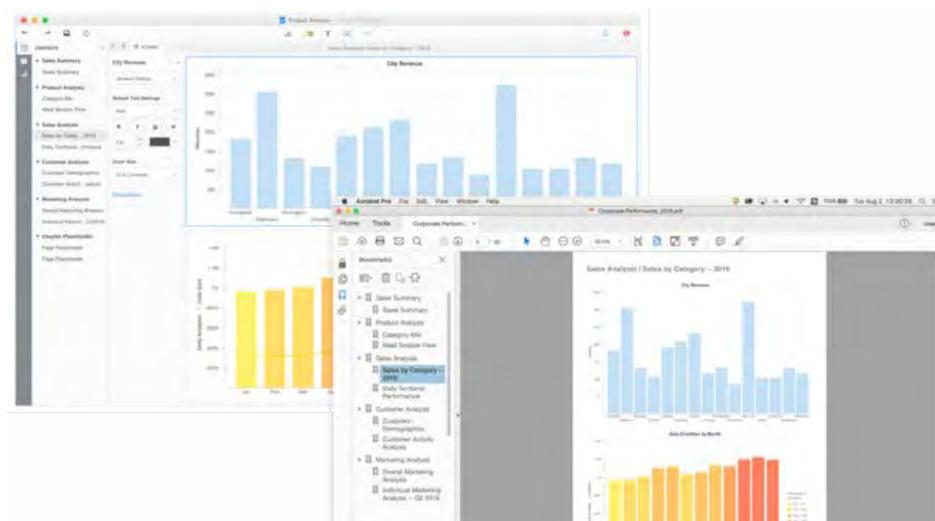
With version 10.6, users will be able to export dashboards that contain multiple visualizations on a single page, dashboards that contain multiple sheets and panels, and dashboards that contain large grid reports – into highly formatted and readable PDF files.

Every visualization on a dashboard will be exported as a separate page, making it extremely easy to read information on multiple charts and graphs. Smart pagination for PDFs expands all content of the dashboard into separate pages, making it incredibly easy to deliver large grid reports in PDFs that clearly display every row and column in a highly formatted manner; and also making it easy to clearly displace multiple panels and sheets on a dashboard.



Support for bookmarks

With version 10.6, dashboards exported to PDF will support bookmarks, for better content organization and navigation.



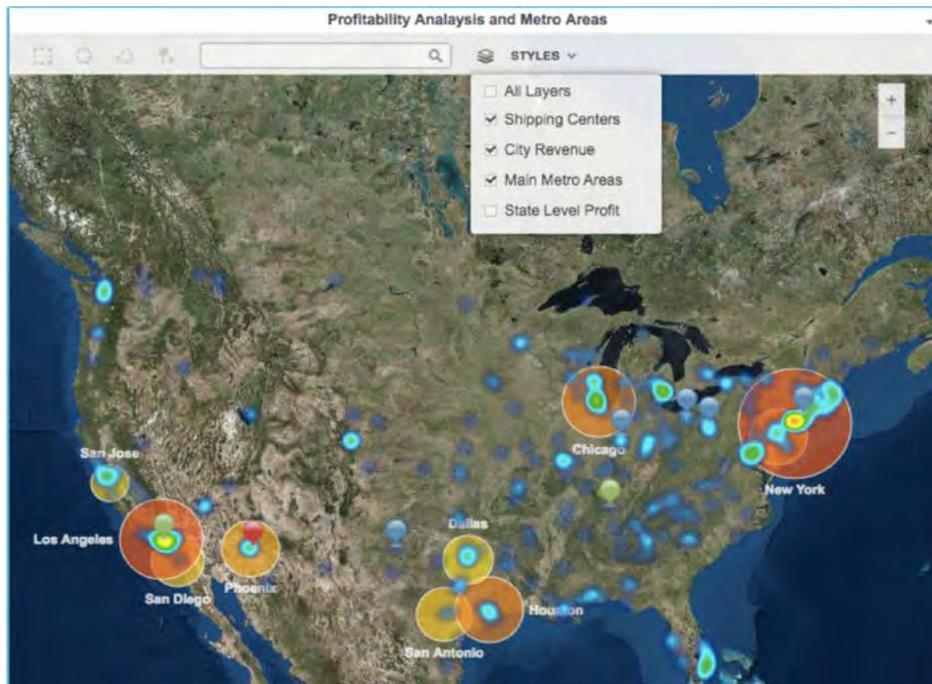
Installation of a separate micro-service for the PDF export engine

The export engine with MicroStrategy 10.6 is installed with the Server as a separate micro-service. This offers the ability to be installed on a separate machine, reducing the load on the server and ensuring that the distribution jobs will not compete for Server resources.

New mapping capabilities

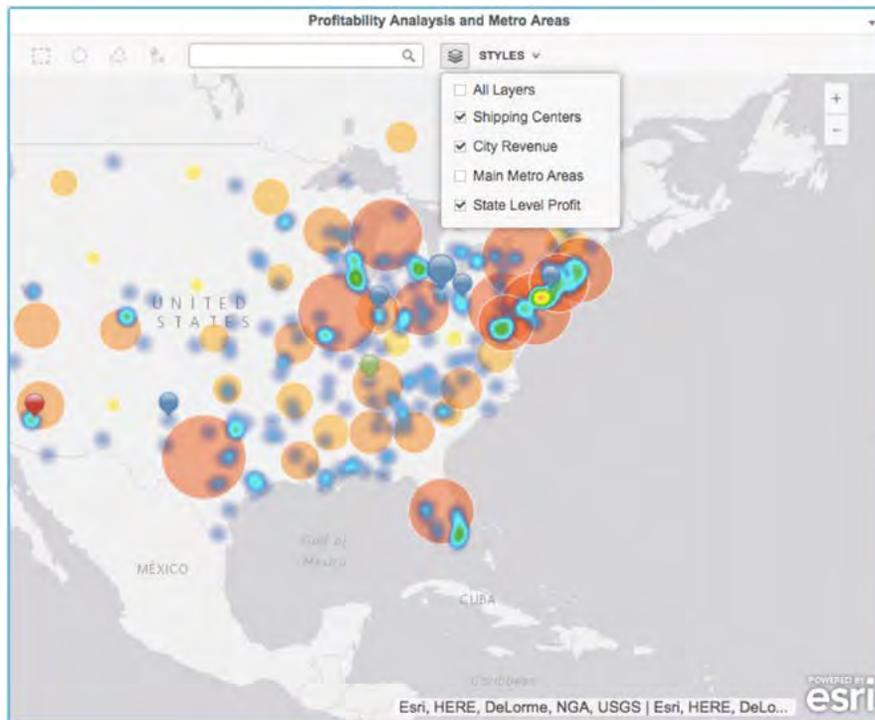
One map visualization that supports multiple base maps

The new map visualization will meet all of your needs for geospatial analysis. It offers support for both Google and ESRI base maps with a consistent set of features working well in dashboards (Visual Insight) and documents (Report Services), across all interfaces - Desktop, Web and Mobile. No matter which mapping service users choose, the new and unified map visualization will support both Google and ESRI base maps.



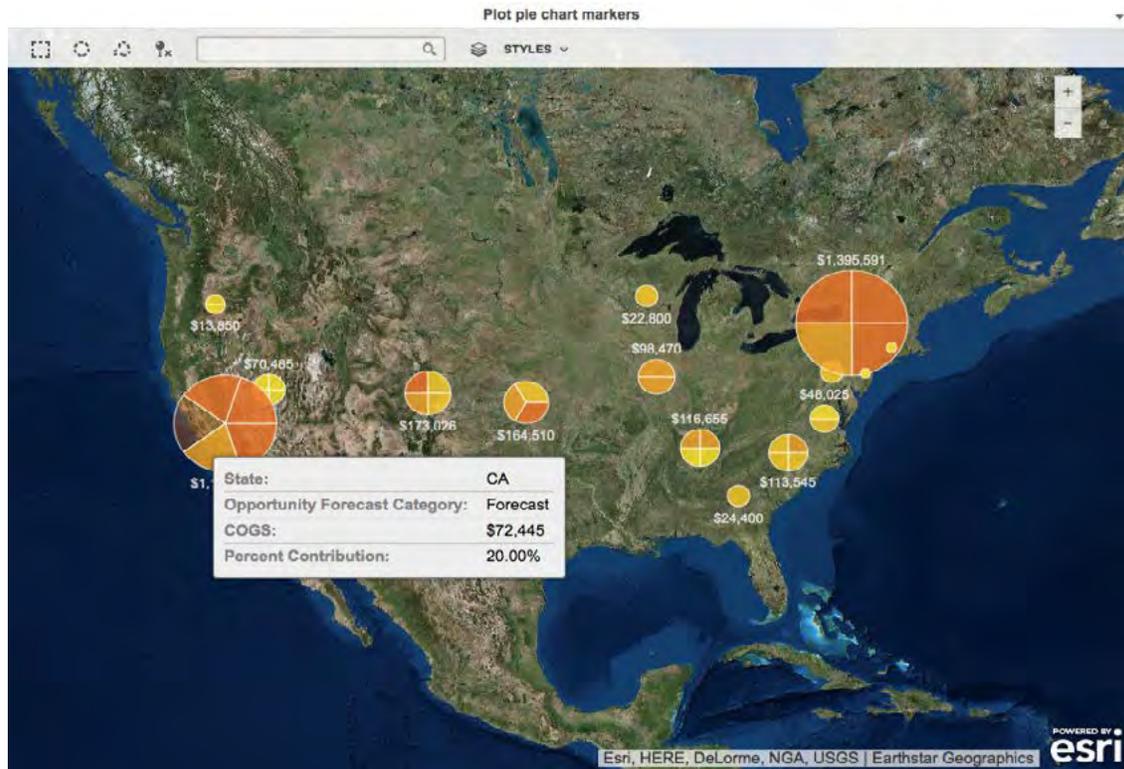
Multiple layers on maps in dashboards

MicroStrategy map visualization no longer limits you to a single layer of data at a time. With version 10.6 it is possible to have multiple layers of information on the out-of-the-box maps. Users can display markers, bubbles, and/or areas simultaneously in the same map visualization. It is easy to toggle each of these layers independently, with the full design flexibility to modify the order on which the layers appear. In the example below, you can note a density map that displays bubbles with thresholds.



Plot pie chart markers on maps

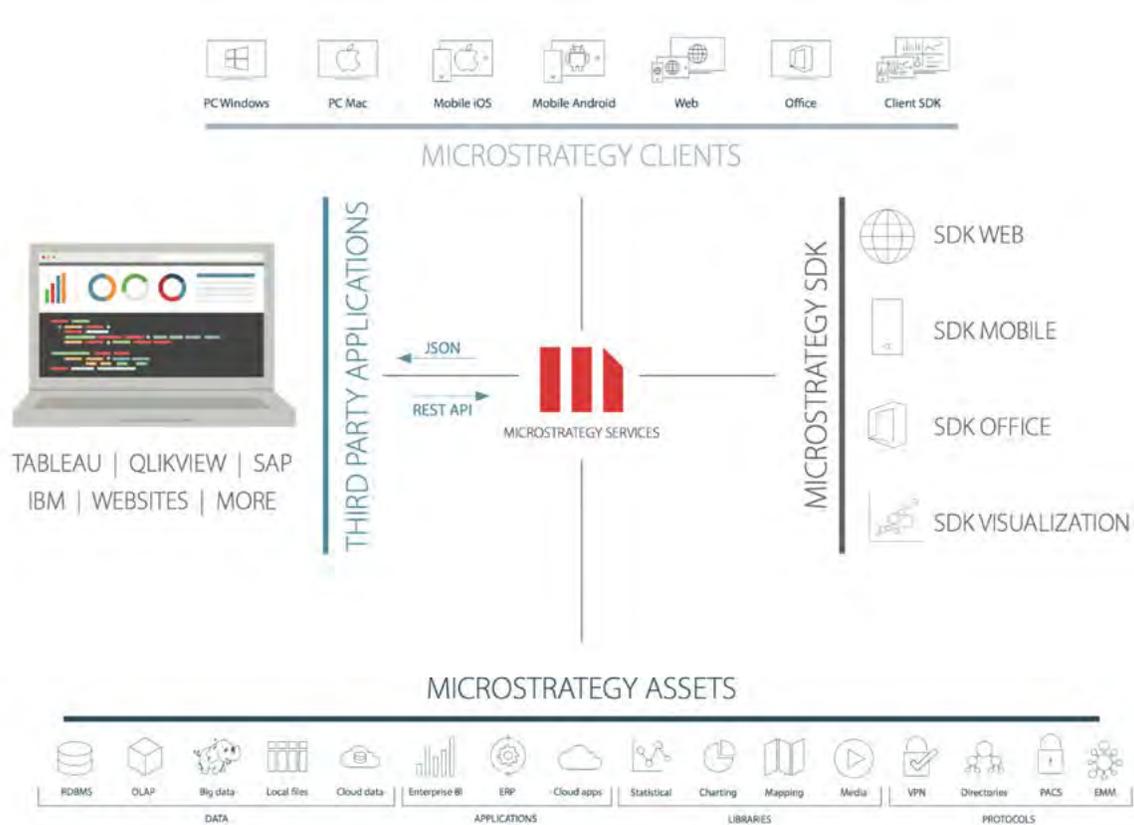
The new ESRI map that is available out of the box for data discovery, allows you to display pie charts and ring charts on top of maps. Users can specify the dimension that will slice the pie chart using drag and drop options, and easily compare multiple attributes on a single map.



MicroStrategy SDK enhancements

Attribute multi-form support with JSON data PI

MicroStrategy offers native support for RESTful APIs to allow access to data from the MicroStrategy Server in JSON format. The RESTful API can be used to easily access subsets of preprocessed data by 3rd party and custom applications, very commonly used across OEM customers and large enterprises. With the latest version, MicroStrategy 10.6 extends the functionality of the RESTful JSON Data API by adding support for attributes with multiple forms, and allow their use in the definition of filter expressions. This provides additional flexibility and allows for all attribute forms to be included in the result set.

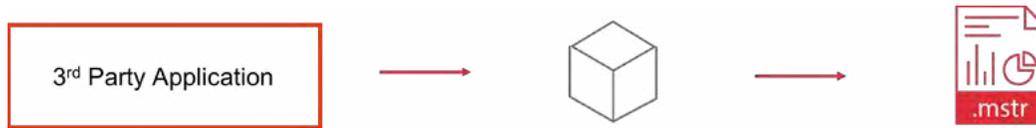


Support for large cubes/datasets

With MicroStrategy 10.6, users can run a large cube and get the definition in JSON format prior to execution. Instead of using server resources to query the entire cube before getting the column definitions, users can retrieve them before submitting a query, allowing for a more streamlined query process.

Support for 3rd party API to upload data and create a new dataset

For the first time, it is possible to push datasets directly into the MicroStrategy platform from 3rd party applications. MicroStrategy 10.6 delivers the ability to create MicroStrategy datasets and populate it with data using RESTful API calls, making it possible to leverage investments in other technologies.



New URL API

The latest version of MicroStrategy delivers a new URL API that offers more control while embedding dashboards into 3rd party applications and portals. It offers enhanced layout and UI controls to easily specify what functionality to expose when dashboards are embedded into external applications.



MicroStrategy platform enhancements

New data sources certified

MicroStrategy 10.6 offers support to more data sources, and certifies the latest versions. New certifications available in version 10.6 include:

- Microsoft Azure SQL Database (certified as a data warehouse)
- IBM DB2 11 (certified as a data warehouse, metadata, and Enterprise Manager)
- Teradata 16 (certified as a data warehouse, metadata, and Enterprise Manager)

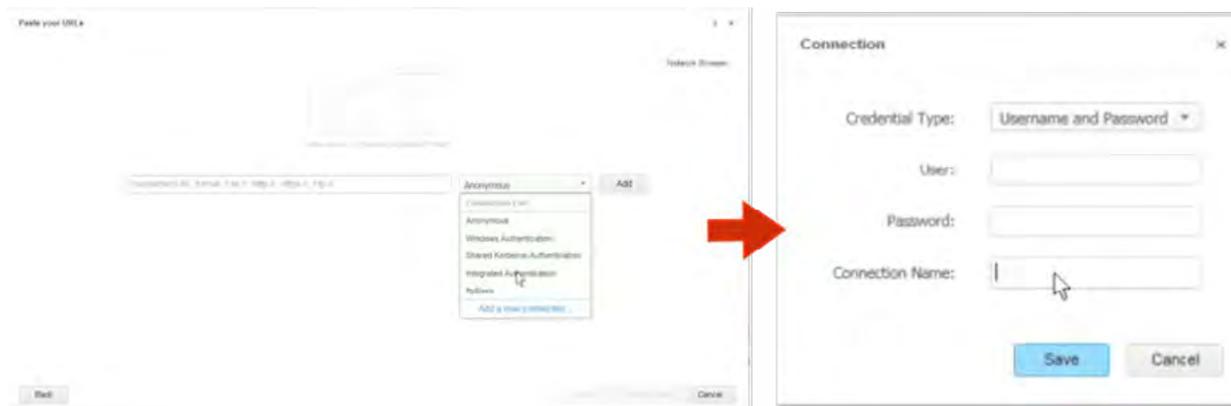
SAML authentication support for MicroStrategy web and mobile

MicroStrategy 10.6 easily integrates with IDPs such as Usher and ADFS, to deliver single sign on capabilities using industry-standard SAML-based authentication protocol, without writing code. This functionality is supported only for MicroStrategy Web JSP. Currently certified SSO solutions are Usher and ADFS, and additional services such as Ping and Okta will be certified in future versions.



Enhanced authentication support for URL sources (JSON/oData/text files)

MicroStrategy 10.6 supports new authentication modes for users accessing data from URL sources. This applies to users accessing JSON, OData, or text files via URLs with basic authentication, Windows Pass-through authentication, and Kerberos authentication.



Share a database instance with a subset of users

With MicroStrategy 10.6, users have more control to share their database connections by setting privileges for other users who can access the shared connections. With MicroStrategy web, administrators can allow users to choose from multiple options to deliver view or edit access, full control or have a customize access to a particular database instance.



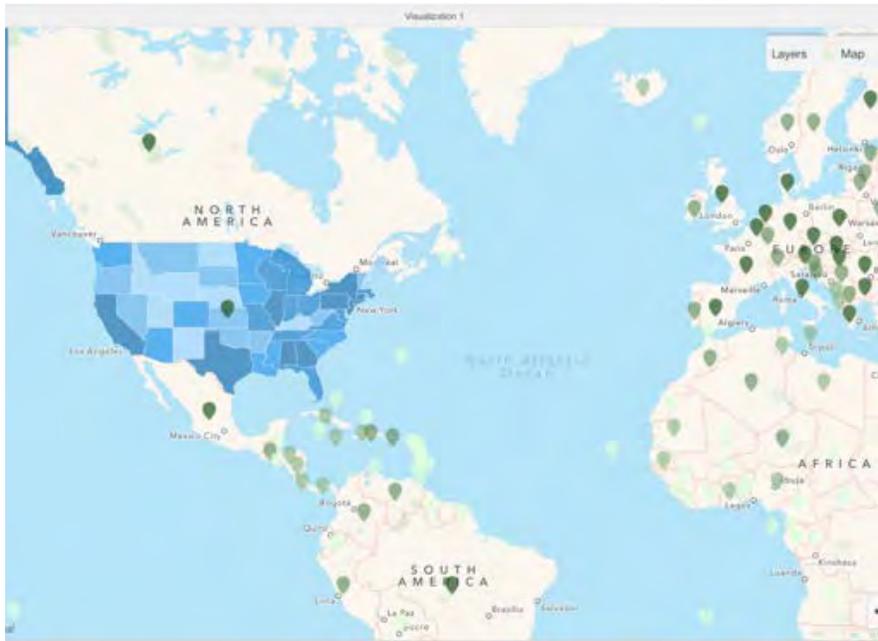
Mobile

Unified mapping for easier maintenance and seamless user experience

As in MicroStrategy Web 10.6, a single, unified map visualization supporting both ESRI and Google basemaps, will now render all functionality seamlessly on iOS and Android devices. Consolidating two map visualizations into one reduces long term maintenance cost and improves map usability and the deployment process for users.

View multiple layers on maps in dashboards

On iOS, users can now leverage multiple layers to visualize different metrics or datasets, each using a different visualization type (i.e. areas, bubbles, markers or density map). This capability enables users to overlay information and to visually correlate data points on a single map view.



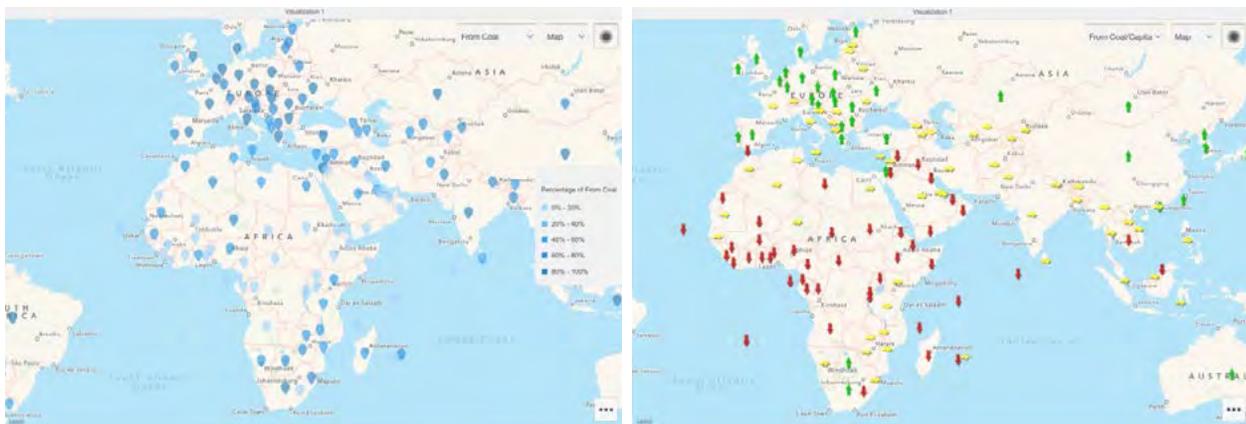
Support for different marker types and corresponding thresholds in maps

On both documents and dashboards, users can now render pin, square, and diamond markers and apply color thresholds on iOS maps. Users can also display image markers and thresholds. This feature provides variety in the representation of the metric values in maps.



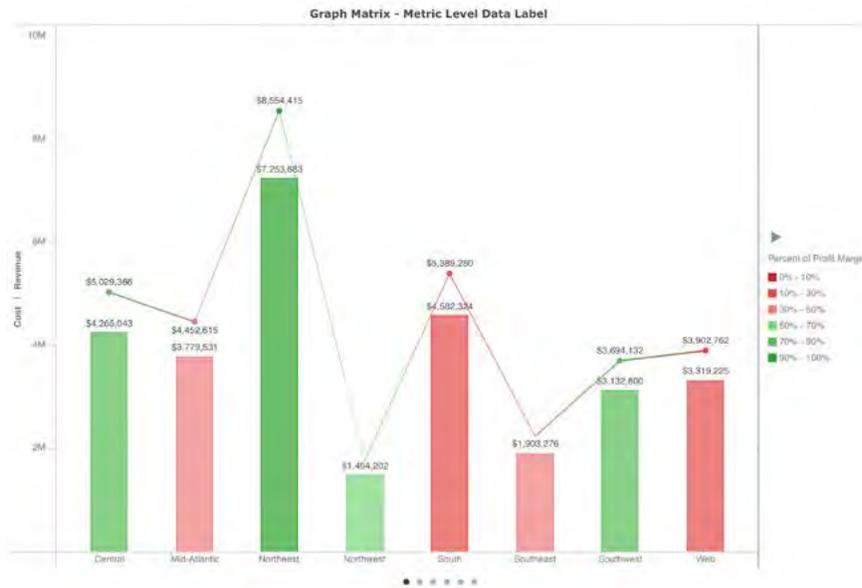
Switch marker type using metric toggler in maps to get the most insightful view

Users can now display mixed types of images and shapes—defined by advanced thresholds—as markers on one map visualization. Users have the flexibility to easily switch between markers using the new metric toggler.



Support for metric data labels in Visual Insight dashboards

Legends can now be displayed in iOS VI maps for user reference. Prior to 10.5, iOS VI maps used color by metric for both size-by and color-by functions. With 10.5, iOS VI maps will use separate size-by and color-by metrics, providing more dimensions in data representation.



Secure Android apps with native Airwatch integration

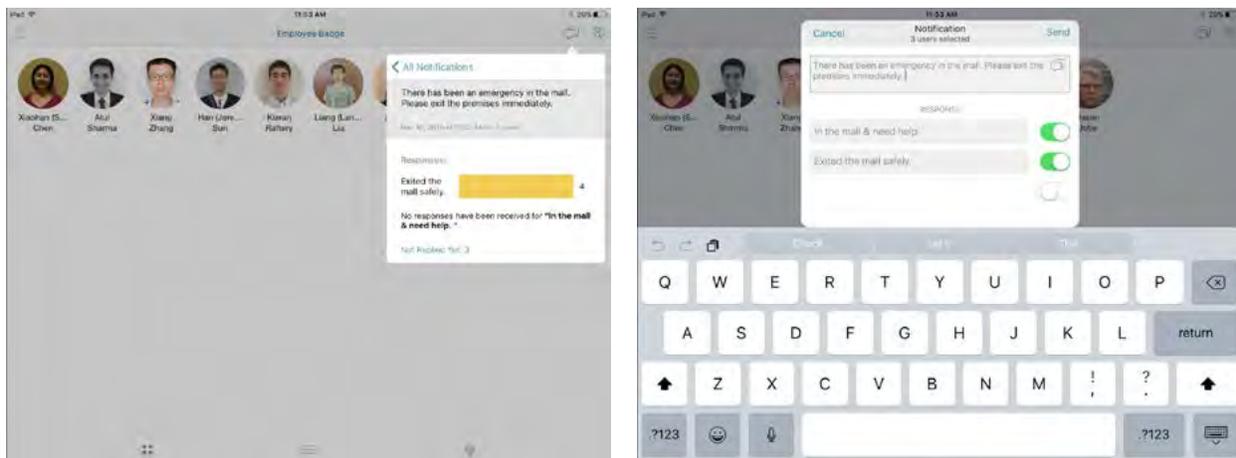
MicroStrategy is releasing a new Android AirWatch SDK. This native SDK will provide customers with a reliable integration with AirWatch to deploy Android apps to authorized devices and users. Using the the new Android AirWatch SDK, Enable Data Loss Prevention settings to protect sensitive data and restrict moving content outside the app.



MicroStrategy security

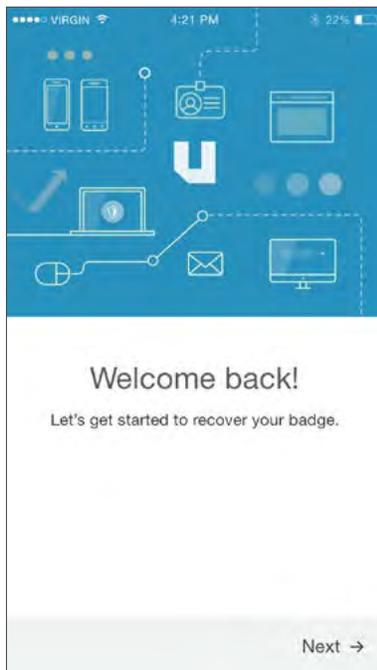
Usher Professional: Two-way communication enhancements

In MicroStrategy 10.6, Usher's two-way communication capability has been enhanced to include the ability to re-use previously written messages and to edit and resend these messages to the same users, a subset of the same users, or entirely new users. Two-way communication enables Usher Professional users to communicate directly with end users and have the individual(s) respond back with a multiple-choice selection. This feature supports a number of use cases including employee communication, mustering and security. For example, a standard message asking a group of users if they require assistance can now be sent to a new group of users if dealing with an incident at a different time or in a different location, or the same message can be sent again to any recipients of the original message who failed to provide a response verifying their safe evacuation.

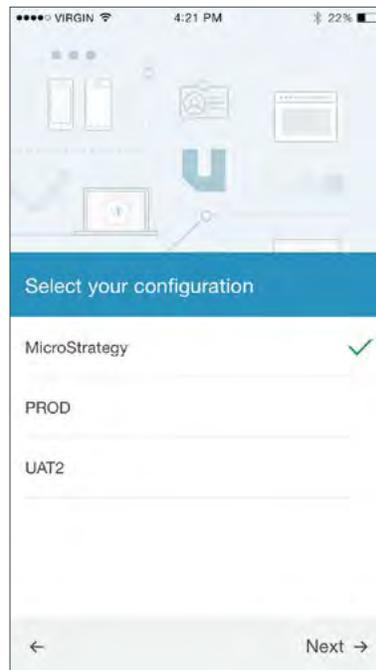


Usher security client: iCloud and google drive badge recovery

Self-service functions in the Usher mobile app empower users to easily install and recover Usher Badges, including when restoring a device, or switching to a new device, resulting in productivity gains and lower helpdesk costs. Starting with MicroStrategy 10.4, Usher has leveraged the iOS Keychain and Android Keystore to make it easier for users to restore Usher badges and security certificates. Starting in MicroStrategy 10.6, the Usher mobile app will also automatically backup or restore Usher server configuration data to iCloud (iOS) or Google Drive (Android) so that it never needs to be reentered or reprogrammed. Upon installation or recovery, the Usher mobile app automatically checks for any saved server configurations in the iCloud or Google Drive account of the user and downloads them. By downloading the configuration from iCloud or Google Drive, the entire recovery process can be managed inside the application by the user. This eliminates the need to search for an external configuration source (QR code, email invite, system admin) in order to regain access to their credentials.



User launches the Usher client



User selects a server configuration for restoration



Badges begin recovering

Usher for Android: fingerprint biometric

Usher continues to support TouchID™ from Apple (iOS 8.0 and later). Starting in MicroStrategy 10.6, Usher also supports a variety of Android devices with built-in fingerprint scanners. Users of devices running Android 6.0 (Marshmallow) and later can now be enabled or required to use their fingerprint-enabled device to access logical and physical access systems and applications, improving both security and convenience simultaneously. This includes configurable support for multi-factor and 'step-up' authentication for a given transaction. Incompatible Android devices and devices without a fingerprint sensor can use a configurable PIN / passcode as an alternative.

Usher network manager: SMS badge distribution

Starting in MicroStrategy 10.6, Usher administrators can automatically or manually distribute a 'deep-link' via text message to each Usher user to install or recover Usher Badges. This can be done in addition to - or in place of - an email communication. Provisioning via SMS communications improves Usher's security posture, more tightly binding the Usher badge to a known, registered mobile device. Although not used by Usher for identity authentication purposes (per NIST SP 800-63-3), device ownership and presence can be routinely confirmed using a one-time verification code, including prior to unlocking the Usher Badge for first time use. In fact, many organizational security policies prohibit the use of email for issuing credentials. It is harder for a hacker to gain access to a specific smartphone than it is to gain access to an email account which can be accessed from anywhere without physical theft. Additionally, this feature allows Usher Badges to be distributed to users without an Active Directory or other Usher supported directory profile. Out of the box, Usher has integrated with our preferred partner, Slooce (<http://www.sloocetech.com>), to deliver this functionality. Please contact MicroStrategy to find out if your existing in-house or third-party Short Message Service (SMS) service provider is supported.

Manage Badge Properties

Basic

Requirements

Authentication

Location

Time

Device Security

Policy

Provisioning

AD Agent

HID

Zero-Click

Provisioning

Please select a method of how you want to send badge invitation(s) to the end user.

Email

SMS

Both

Configure the SMS gateway with your SMS vendor account information in order to send messages. At this time, we support integration with Slooce Technology.

URI

User ID

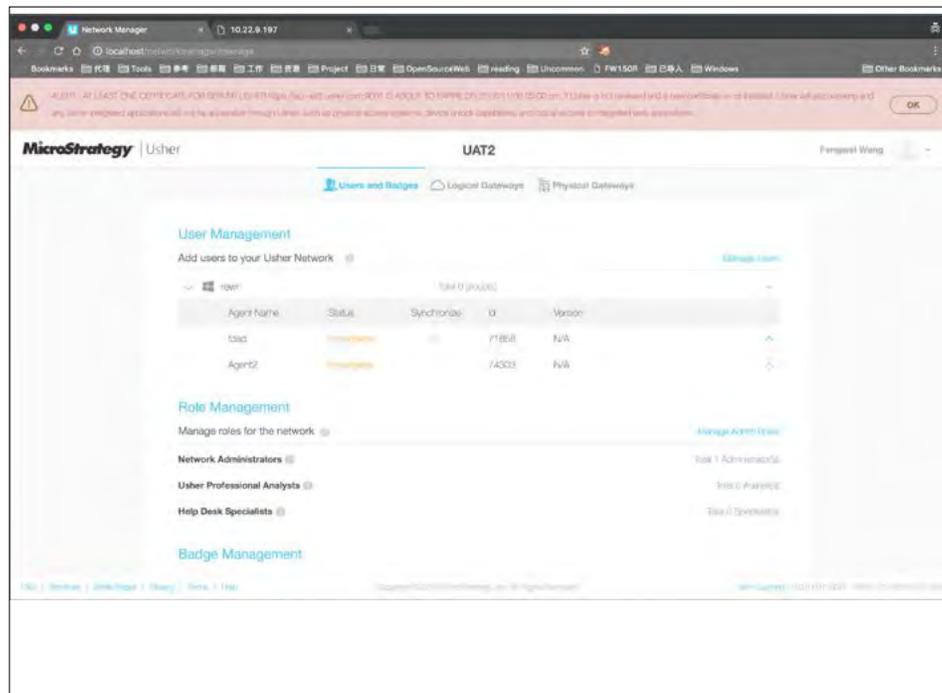
Password

Keyword

Badge distribution can be done via email, SMS, or both methods concurrently

Usher network manager: Digital certificate expiration notifications

Many Usher components and connections rely on the use of various security certificates (TLS) which expire at regular time intervals. To help prevent customer environments from becoming unavailable unexpectedly due to expired certificates, starting in MicroStrategy 10.6 Usher Network Manager will now check digital certificates on a daily basis. When a certificate reaches 60, 30, or 3 days from expiration, an email will be sent to all Network Admins warning them of this so that they can renew Usher and install a new certificate before expiration, therefore averting a temporary loss of Usher access to a variety of connected resources. In addition to email alerts, when a user with Network Administrator role logs into the system, an alert will be displayed if the Usher certificate is due to expire in 30 days or less.



Administrators can respond to flags to ensure continuity of service

Usher VPN Proxy Module: High performance universal VPN proxy services

Starting in MicroStrategy 10.6, Virtual Private Networking (VPN) support within Usher has been completely re-architected to deliver higher performance, more versatility and increased reliability. Usher's new VPN Proxy module supports multi-factor authentication, or password replacement, depending on the VPN provider. Both server-centric and client-centric VPN providers are supported including Cisco, Fortinet, Juniper Networks, Citrix and PulseSecure. This enhancement will also make it easier to integrate Usher with more VPN protocols and providers in the future.

Usher gateways: Office 365 login

To enhance the pool of widely-adopted corporate applications supported by Usher, MicroStrategy 10.6 includes a new Office 365 SAML gateway integration for Usher. Usher users can now authenticate using SAML 2.0 into all Office365 web applications whether their organization uses “Synchronized Identity” or “Federated Identity” with Office 365. Native Office365 applications including Outlook running on Windows 7, 8 and 10 are also supported using an Usher Badge for authentication. Usher supports the use of Outlook and native mail apps on Android, iOS and MacOS leveraging either an Usher Badge or traditional Office365 username and password so that customers do not need to segregate their Exchange servers off of Office365/Azure, as many organizations have bundled their email services with their Office365 accounts as opposed to isolating mail on-premise.

Usher gateways: Amazon Web Services (AWS) directory services integration

Thousands of organizations leverage AWS to operate their SaaS or Cloud business. Starting in 10.6, Usher supports native integration with AWS Directory Services. Usher synchronizes to AWS Directory Services as an authoritative source for person-records and attributes, supporting the enforcement of AWS provisioning as an authoritative source for authorization (privileges, entitlements and restrictions). Usher also continues to support other AD/LDAP directories as needed in addition to AWS Directory Services.

Usher gateways: Okta universal directory integration (early adopter)

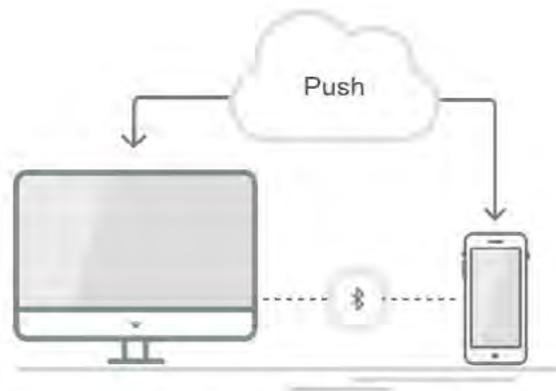
Thousands of organizations are using Okta as their corporate user identity repository, that is, how these organizations aggregate multiple directories and govern internal access. Starting in MicroStrategy 10.6, Usher also supports Okta Universal Directory as a supported Identity Management source, allowing organizations that are a customer of Okta to leveraging their investment in Okta as an authoritative directory service. Usher synchronizes to Okta Universal Directory as an authoritative source for person-records and attributes, supporting the enforcement of Okta provisioning as an authoritative source for authorization (privileges, entitlements and restrictions). Usher also continues to support other AD/LDAP directories as needed in addition to Okta. The new Okta integration adds to Usher support for Okta 'Inbound SAML' (released in MicroStrategy 10.5) to establish Usher as the identity provider for the enterprise while still leveraging all preexisting Okta integrated systems and applications.

Usher gateways: OpenID connect (early adopter)

Starting in MicroStrategy 10.6, Usher will support OpenID Connect, which is fast becoming the international standard for logical access. OpenID Connect is on track to replace Security Assertion Markup Language (SAML) in the enterprise as a richer, more secure means of externalized identity management. For example, OpenID Connect is optimized to integrate a wider variety of native mobile applications with Usher, both with greater speed and better performance in addition to web-based applications. It also offers separate identity and transaction tokens for a more privacy-enhancing and robust exchange. However, both standards are likely to coexist for some time. Usher will support both SAML and OpenID Connect to ensure interoperability with a wide variety of customer deployments.

Usher for Mac: Unlock via push notification (early adopter)

Since MicroStrategy 10.3, Usher has supported the proximity unlock of MacOS devices by transmitting a password from the Usher mobile app client to the paired Usher desktop agent on a MacOS computer via Bluetooth connectivity. In MicroStrategy 10.6, if the Bluetooth communications are slow or fails, the Usher end-user taps a button on the screen of Mac computer, approves the subsequent Usher push notification sent to his/her phone, and immediately unlocks his/her computer. The mechanism, at a high level, is that the Usher mobile client transmits its copy of the computer's password, encrypted with a public key on the computer, to the Usher server, which in turn relays it to the client on the computer. Thus, the performance of Mac Unlock has been improved when both the Usher-enabled mobile device and Mac computer are online and can communicate with the Usher Identity Server.



Server-based Push when Mac is Online

Asynchronous to the Bluetooth connection, the server will attempt to contact the Phone via Push and push the password out of band. The fastest method wins.

Usher for Windows: Unlock via bluetooth or push notification (early adopter)

Usher mobile app users can already scan a QR code to login to Windows 7, 8 or 10. Starting in MicroStrategy 10.6, Usher mobile app users are now able to also seamlessly unlock Windows 10 computers leveraging Bluetooth pairing or push notifications when both the Usher-enabled mobile device and Windows computer are online and can communicate with the Usher Identity Server. No password or QR code scanning is required to unlock the Windows 10 computer. The Usher end-user taps a button on the screen of the Windows 10 computer, and approves the subsequent Usher push notification sent to his/her phone, and immediately unlocks the computer. Usher can additionally proximity-unlock Windows computers by transmitting a password from the Usher mobile app client to the paired Usher desktop agent via Bluetooth connectivity.

