FILE SYNC & SHARE

SECURITY ARCHITECTURE GUIDE

The Autotask Workplace™ Approach to Service Virtualization

PARTNER | Autotask Workplace™

Table of Contents

Dedicated Geo-Redundant Data Center Infrastructure 02

SSAE 16 / SAS 70 and SOC2 Audits 03

Logical Access Security 03

Dedicated Geo-Redundant Data Center Infrastructure 04

Testing, Risk Assessment and Compliance 04

Data Encryption and Authentication 05

Admin Policy and Account Management 06

Password and Two-Factor Authentication Policies 07

Content Policies 08

Virus Scanning & Other Policies 09

Computer and Mobile Device Policies 10

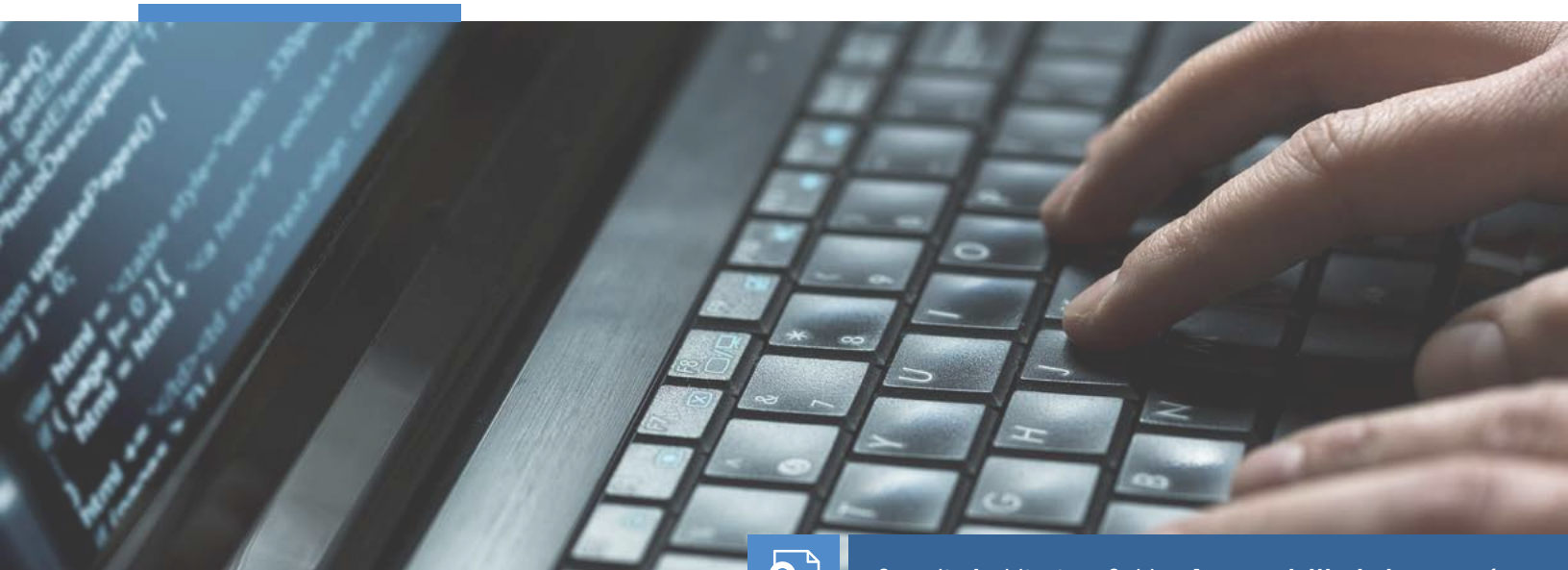
Mobile Device Access and Usage Policies 11

Mobile Device Enhanced Authentication Policies 12

Active Directory Integration for User Deployment 12

Application Management Authentication 13

Reporting 13



Dedicated Geo-Redundant Data Center Infrastructure

As opposed to the common virtualized approach to cloud services, wherein cloud service providers lease processing and storage capacity from Internet infrastructure providers, **all Autotask Workplace™ (AWP) hardware and software in each data center is 100% owned, operated, and managed by AWP.** In typical virtualized cloud environments, service applications and customer data actually share processing and storage platforms in a virtual time-sliced manner, resulting in a minimum of separation between independent operating domains. With the dedicated data center approach that AWP has invested in, nothing operates on any AWP hardware or software processing or storage platform except AWP services.

True 100% isolation of the AWP service eliminates the possibility of experiencing any service interruption, performance degradation, or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level regional and data center redundancy, the AWP infrastructure represents one of the most secure, reliable, and available cloud service architectures available today.

AWP uses a co-location model for deployment of AWP owned and operated equipment and software, utilizing the rack space, power, cooling, and physical security of major world-class SSAE 16 audited data centers. These facilities are a classified as Tier 3 or better with N+1 fault tolerant systems guaranteeing 99.982% availability. The AWP network architecture deployed to these facilities includes multiple levels of redundant application servers and storage arrays, thus ensuring High Availability, Failover support, and Load Balancing.

AWP operates data centers in several different geographical regions, including the United States, Canada, Denmark and Australia, and is planning further expansion into other regions. Within each region, two levels of redundancy are provided. First, within each data center, redundant servers and file storage ensure that data center level failures can be isolated and resolved quickly. Second, within each region, at least two independent data centers are physically distanced and isolated from each other, thus providing protection from higher-level data center failures, regional disasters, or broader Internet related failures. This dual-level geo-redundancy ensures the greatest possible availability and protection against data loss.

The physical presence of data centers in separate regions also means that data does not leave the region; it stays in the United States for U.S.-based customers, in the European Union for EU-based customers (in compliance with EU Safe Harbor and EU Country policies), in Australia for AU-based customers, and in Canada for Canadian customers (in compliance with PIPEDA and local regulations).

SUMMARY

- Co-location model with HW and SW 100% owned, operated and managed by AWP
- Geo-redundant, Tier 3, SSAE16 Audited data centers (two per region)
- Complete, redundant, regional data set in each data center
- Complete regional server setups in each data center
- Data center redundancy using RAID6 mirrored backup with replication
- Modular clustered server farms for service load-balancing, scalability, and failover protection
- SLAs for availability (99.982%), response time, service restoral

SSAE 16 / SAS 70 and SOC2 Audits

In the rapidly changing landscape of cloud services, companies that handle sensitive information, such as in the legal, finance, and medical sector, find that they are under increasing scrutiny over their information processing controls. **AWP data centers are audited against both AICPA SSAE 16 / SAS 70 and ISAE 3402 criteria for system availability and security,** thus providing assurances regarding adequate oversight over the controls utilized in the processing of information. Similarly, AWP's own internal security controls are audited against SSAE 16 / ISAE 3402 criteria for employee policies, physical and logical access controls, intrusion detection and testing, service reporting, security incident procedures, training, change control, and configuration management.

AWP's SOC2 Type 2 examination report is issued in accordance with both the SSAE 16 attestation standards established by the American Institute of Certified Public Accountants and also the attestation standards established by the International Standard on Assurance Engagements (ISAE) 3402, known as "Assurance Reports on Controls at a Service Organization." Accordingly, AWP services can serve as a foundation upon which customers can build their SSAE 16 / SAS 70 / ISAE 3402 compliant data processing and storage policies and practices.

Logical Access Security

All AWP application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.

All connection pathways within the AWP infrastructure are highly regulated as to the kinds of traffic that are allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns, in terms of source, destination, and traffic type, is immediately interrupted and reported to monitoring personnel through alerts. All known attack vectors are specifically prohibited.

Comprehensive Monitoring

All of the AWP regional data centers are monitored 24 hours a day, 365 days a year, by equipment service and operations staff, who also have immediate access to AWP engineering personnel in the event that it becomes necessary. Co-location with major world-class data center industry partners ensures that physical and environmental security is unsurpassed.

AWP utilizes dedicated software monitoring components that are designed to track and evaluate the operation of servers, networking equipment, applications and services within the AWP service infrastructure. This also includes monitoring of resources such as processor load, memory usage and disk space usage.

Alerts regarding performance or potential security issues are automatically distributed to several on-call staff via SMS and email.

Testing, Risk Assessment and Compliance

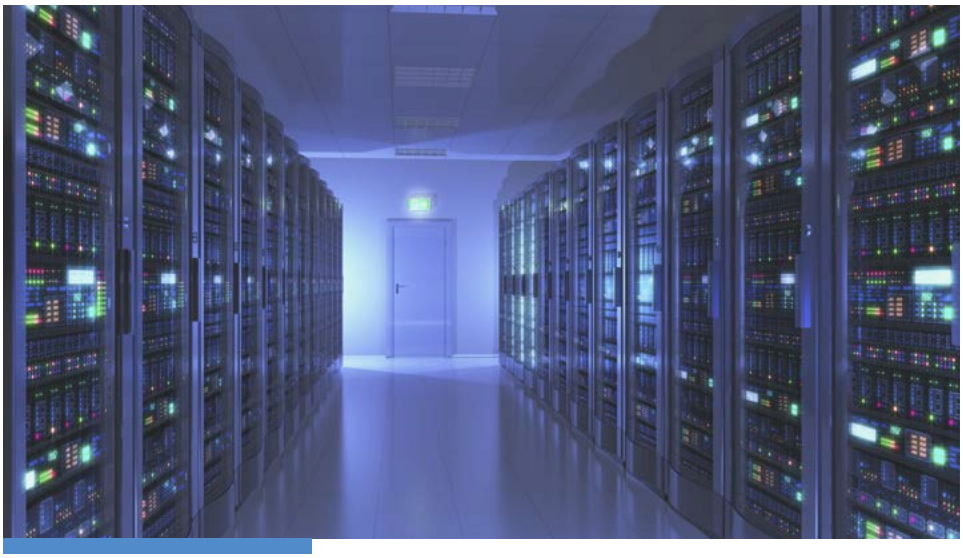
AWP makes use of independent 3rd-party testing, analysis and assessment services. AWP's multi-faceted approach to testing and risk assessment incorporates the following elements; ongoing 3rd party penetration testing of Web, Agent, and APIs, Periodic SAS/SSAE audits, and Daily Hacker Safe updates.

AWP follows the Safe Harbor Principles published by the United States Department of Commerce with respect to the transfer of personal data from the European Union to the United States of America. AWP's Privacy Policy, available at http://www.autotask.com/privacy-policy, details certain policies implemented throughout AWP to comply with Safe Harbor.

AWP is 100% compliant with all Security Rules specified in the Technical Safeguards, Administrative Safeguards, and Physical Safeguards from the Health Insurance Portability and Accountability Act (HIPAA) of 1996. AWP's Privacy Policy provides specific details regarding the policies implemented throughout AWP in order to comply with HIPAA. Furthermore, AWP engages health care provider customers as a HIPAA Business Associate through BAA agreements. AWP is also compliant with PCI DSS requirements, and therefore can be used as the foundation of a compliant infrastructure that end-customers might certify and deploy.

Data Encryption and Authentication

All files handled by the Autotask Workplace™ service are secured, both in transit and in storage, using 256-bit AES-encryption. Furthermore, in order to maximize the separation between teams, users, and files, a different unique rotating encryption key is used for each individual file. None of the encryption keys are stored "in the clear" in any non-volatile storage, but rather are encrypted and stored under the protection of a master key. Authentication is ensured through the use of VeriSign certificate-based server authentication, which ensures that the user's agent will neither connect, nor cooperate, with any server other than those that comprise the AWP service. Even in the unlikely event of a successful attack on Internet DNS or routing infrastructure, which is quite outside the control of AWP or any other SaaS provider, AWP's certificate-based authentication will ensure that no malicious agent could successfully connect to the AWP service.



All of the Autotask Workplace™ regional data centers are monitored 24 hours a day, 365 days a year.

Admin Policy and Account Management

Administrative Policy and Account Management are particular strengths within the context of Autotask Workplace™ service administration. These represent Role-Based Access Control (RBAC) mechanisms by which specific named accounts can be provided with varying levels of administrative permissions. Administrators can be assigned either Super Admin or Admin privileges, providing an extensive set of controls and processes that will ensure flexible and effective security policy enforcement. Super Admin / Admin level account management and policy control includes mechanisms that allow administrators to:

- **Create, edit, disable and delete** Members, Connections, Groups and other Admins
- **Configure** AD for importing Users and Groups
- **Convey** to full Members the right to create Connections
- **Control** the ability of Members to create private Backups
- **Review, assign and manage** storage quota among Members
- **Set and enforce** Password Policies
- **Establish Session Policies:** Used to control the lifecycle of login sessions
- **Configure mobile device & data** policies for access and usage
- **Configure mobile device approval** and device wipe policies
- **Wipe** specific computer or mobile devices
- **Configure integration points** with 3rd party apps such as Salesforce, Google Docs, and Office 365

In addition to these team-wide and account-oriented policies and features, AWP provides an additional set of powerful features that facilitate extensive Project control capabilities. Known as the "Manage Projects" feature, which is available as part of the Enterprise plan, and accessible only by Super Admins, this is a set of highly-privileged controls. These controls permit Super Admins to review and modify sharing and device synchronization rights for all users, and also to access and modify any Project or document resources. Specifically, Super Admins can:

- **Review and modify** the sharing of Project resources that was established by other Members, including through public links
- Review and modify the s**ynchronization status** of any Member devices
- **View, download, copy, and delete** any Projects, Folders, or Files owned by any Member

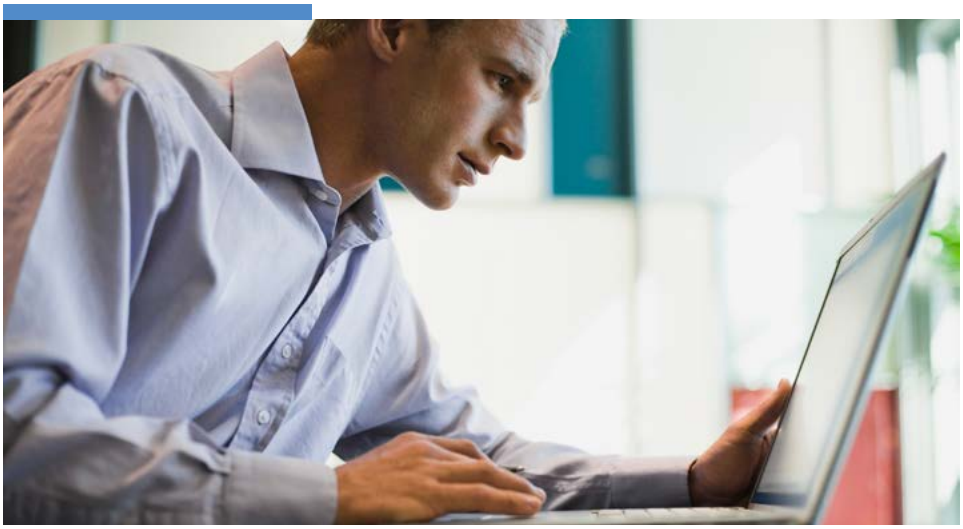
This set of administrative controls thus allows IT personnel to audit resource sharing and modify such Member sharing activities as necessary in order to enforce compliance with company guidelines.

Password and Two-Factor Authentication Policies

Autotask Workplace™ Team Members are authenticated into the AWP service against databases in AWP, Active Directory, or a number of standard-compliant SSO-based 3rd party systems that have been integrated with AWP. **When user authentication is performed against AWP databases, AWP Enterprise Team Admins can set global policies** for password expiration (days), re-use cycle times, recent password interval (days), as well as password complexity and failed login thresholds for account lockout.

Two-Factor Authentication, also known as 2FA, two-step verification, or TFA, is an extra layer of security that is more generally known as "multi-factor authentication." 2FA requires not only a password and username, but also something that a AWP Team Member has with them. This can be a physical "hard" token or a piece of information only they know or have immediately at hand, which may have been obtained through a "soft" token. AWP Enterprise Team Admins can set policies to require 2FA as part of the web, agent, and mobile device login flow into AWP services for added layer of access control. AWP supports the delivery of 2FA tokens through either SMS or with the use of an RFC-6238 compliant mobile app, which utilizes Time-based One-time Password Algorithm (TOTP) tokens (such as Google Authenticator).

AWP's 2FA feature also supports a **2FA IP Address Whitelist,** which is separate and apart from the session-based IP Address Whitelist described later in this document. The 2FA IP Address Whitelist allows Admins to specify one or more source IP addresses that can be exempted from 2FA authentication requirements. This feature is commonly used to "whitelist" corporate headquarters or other remote offices, where there is reasonably high confidence that login attempts are from valid users that are physically located on company property, and behind company firewalls.



Content Policies

Access to content stored within AWP is controlled and policed at different levels within the security architecture. Within the confines of overarching user policies that are established by Admins and enforced by the AWP service, users are free to establish their own content access policies as they share Projects with others, effectively dictating the type and method of access afforded to others.

When Projects or sub-folders are shared with other Members or Connections, their access permissions can be specified at the appropriate level of granularity. In both the AWP Pro and Enterprise Plans, access permissions to Projects or Sub-folders can be specified as Read-Only, Modify, Create & Modify and Full Access (including delete) based on the role of the Member. In addition, **content owners can also control the ability for other Members to Re-share resources that they have shared, and to create public links.**

If permitted by Admins, AWP Team Members can establish and manage URL-based Public Links to Project, Folder and File resources, thereby establishing a significant degree of granular control over content access. Public Links can be Member-specified with expiration dates, access count limits, as well as access passwords, and can also be specified to either constrain or expand the access methodology as follows:

- View-only on web (AWP Online)
- Download Enable / Disable
- Read-Only (No edit)
- Read-Only PDF Version (Source files converted to PDF by AWP)
- Upload new or modified files through either web upload or email

Additional protection of user content includes several cooperating mechanisms that defend against accidental deletion or overwriting of user files. While the File Lock mechanism enables users to voluntarily cooperate during the collaborative editing of documents, the file versioning and file branching mechanisms operate automatically to ensure that, even in the event of file conflicts or overwriting of files, no content is lost.

As Members edit and save subsequent versions of a file, **the file versioning feature is a back-end AWP service process that automatically retains the older over-written versions of all files for up to 180 days.** At any point during that period, Members are able to access old versions through the web (AWP Online). This feature has been particularly useful in circumstances where customers have been affected by Crypto-locker type viruses. Because previous file versions are retained in the team account, inaccessible to PC-based viruses, users have the ability to recover damaged content.

File branching, a similar back-end automatic process, ensures that any attempt by two people to edit and save the same file at the same time will be captured as a file conflict, and will result in a branching of the file name at that point. One file will retain the original filename, while the second file will have the second Member's name appended to the file. This ensures that both sets of edits are retained.

Automatically retains the older over-written versions of all files for up to 180 days.

Virus Scanning

All emails that pass through the Autotask Workplace™ servers, including attachments, are scanned in real time for the presence of viruses. If a virus is detected, the operation ceases immediately. Since incoming data streams are purged immediately if a virus is detected, it is not possible for infected files to be written to the AWP Service. In combination with PC-based anti-virus protection, the AWP service represents a wall of protection that prohibits entry of malware into the protected environment.

Global and Group Policies

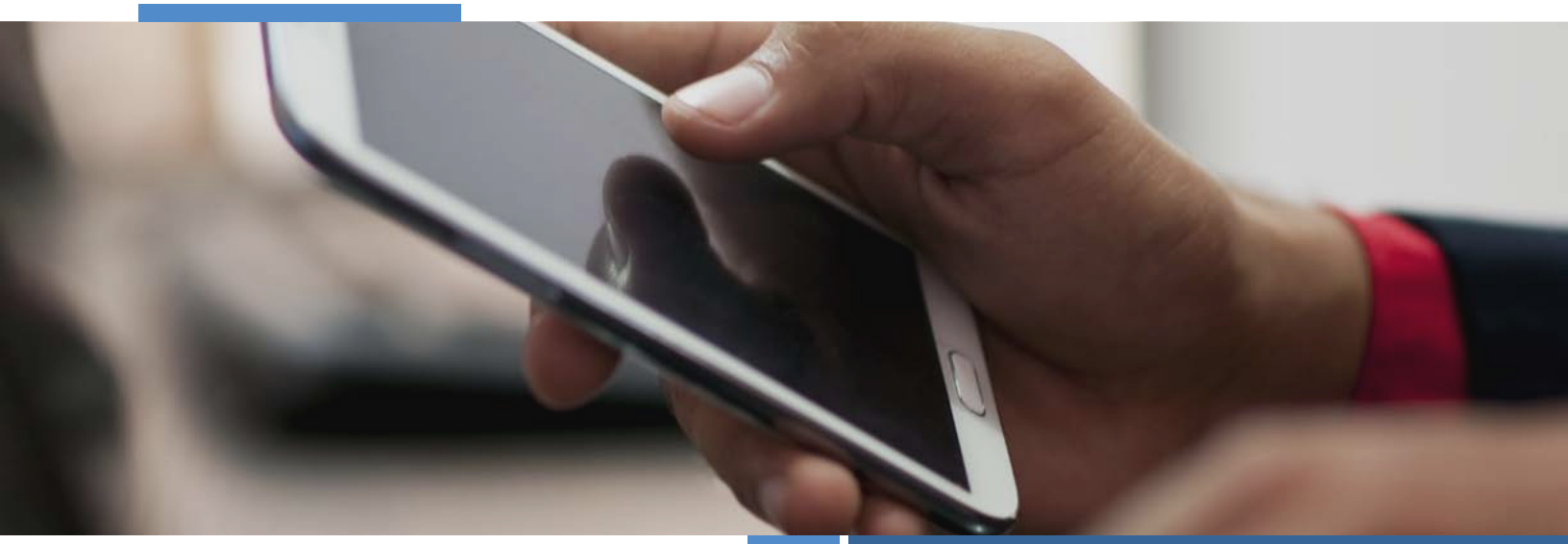
Global Policies allow a AWP Enterprise Admin to set global policies for allowing Public Links, restricting unlock over-ride to only the Project Owner, disabling PC backup, and disabling PC Remote Access. PC Remote Access refers to the ability to remotely access a computer from any web browser, and requires the installation of the AWP Desktop Agent onto the target computer. While this is an exceedingly useful feature, some Admins might feel that higher security and better control are achieved by disabling PC Remote Access. Group Policies allow a AWP Enterprise Admin to set group-by-group policies for such important features as Device Approval, Mobile Sync, and others.

Session Policies

Session Policies allow a AWP Enterprise Admin to specify **global session timeout, the remember-me feature, and IP address display policies** for added control of user sessions into AWP services.

IP Address Whitelist Policies

The IP Address Whitelist is also commonly referred to as an Access Control List (ACL) in computer networking security terminology. This feature enables the AWP Enterprise Admin to place a flexible set of restrictions on service login. Specifically, service login can be prohibited or allowed based upon a combination of the mode of access (browser, mobile app, desktop agent) and the source IP address. For example, this might be configured to allow browser and mobile device based access from anywhere, while restricting desktop agent access to occur only from behind the public IP address of company offices.



Computer and Mobile Device Policies

Cloud-based file sync and share has provided business customers with significant advantages in terms of access mobility, ease of sharing, and real-time collaboration. However, with this expansion of access, the virtual data boundaries of the business organization have expanded to encompass a greater variety of devices over a wider geographical area. Furthermore, this includes both business-owned as well as personal devices. AWP mitigates the potential for increased security threats by providing a set of device management features, including "essential MDM" features, which are integrated into the AWP. These essential Computer and Mobile Device Management policy features include the following items, as described further below. In addition, other important components of AWP's "Essential MDM" feature set are described in the next sections.

- **Explicit Device Approval** for Computer and Mobile Devices
- **Explicit or Automatic Remote Wipe** for Computer and Mobile Devices

AWP supports an active mechanism for device approval, allowing Admins to ensure that Computers and Mobile Devices must obtain specific administrative permission before being configured to operate with the AWP service. Using one or more permit/deny Group-based policies, Administrators have the flexibility of including or exempting Groups from Device Approval requirements. Furthermore, **these policies can be applied to either Desktop Computer devices, Mobile Devices, or both.**

For lost or stolen devices, and for devices used by departing employees, businesses have a critical need to ensure that all company data is securely and completely removed on demand. The proliferation of mobile devices, as well as the hybrid use of personal devices in business environments, only serves to underscore this need. AWP supports the wiping of company data from Desktop Computer and Mobile Devices both manually and automatically, through a variety of potential triggers.

The Device Wipe capability supported by AWP is an "atomic" feature, and encompasses the entire process from the initial manual request or automatic trigger to the final positive confirmation. After a Device Wipe is manually initiated for a target device, the AWP service monitors for a connection from that device. Upon connection, the AWP service quarantines the connection while commanding the remote device agent to wipe all Projects, Folders, and Files under the control of the AWP agent. After the wipe is completed, the device status is flagged with a positive confirmation so that administrative personnel can be assured that the operation was successful.

The automatic Device Wipe operates similarly, but can be triggered after the following events occur:

- Disabling or deleting a User Account
- Excessive login attempts on a Mobile Device
- Excessive period of non-contact for a Mobile Device (Poison Pill)

Autotask Workplace™ supports the wiping of company data from Desktop Computer and Mobile Devices

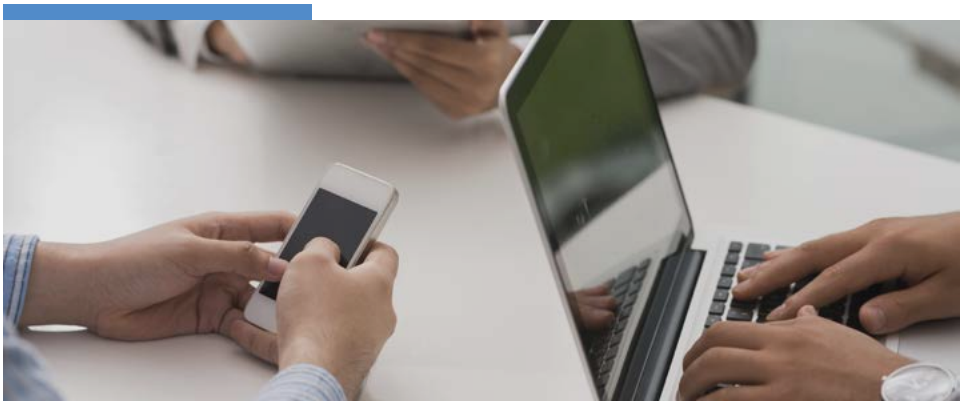
Mobile Device Access and Usage Policies

In combination with the Device Approval and Device Wipe features described in the previous section, the Mobile Device Access and Usage Policies described herein round-out the complete set of essential MDM features, ensuring complete policy control over the access to, and usage of, company data on mobile devices.

AWP Mobile Apps begin with a strong foundation of security, using local encryption of all stored data under the control of AWP. Furthermore, **AWP uses Device Pinning techniques to ensure that the "approved" mobile device/app is permanently associated with the approved user account.** These techniques are fundamental to ensuring control and management of both company data and user activities.

Mobile Device Policies allow the AWP Enterprise Admin to set global team policies on allowing/disallowing a variety of mobile activities. The following policy settings are available:

- **Enable/Disable Mobile Sync** - Controls the ability of users to sync files to the mobile device
- **Enable/Disable Mobile Content Adding & Creating** - Controls the ability of users to add or create content on the mobile device and upload it to AWP
- **Enable/Disable Mobile Editing** - Controls the ability of users to edit any company files that have been downloaded or synchronized to the mobile device
- E**nable/Disable Mobile Exporting** (Open-In 3rd Party Apps) - Controls the ability of users to export company files to 3rd party apps that are installed on the mobile device
- **Enable/Disable Disable Legacy Mobile Apps** - Allows the Admin to disable legacy AWP mobile apps which do not support some of the enhanced security mechanisms



Mobile Device Enhanced Authentication Policies

While some mobile apps provide the ability to protect access with the use of PIN codes, **AWP has implemented an extended set of authentication mechanisms, providing a far greater degree of mobile security.**

The Mobile Authentication Policy can be configured to require entry of either a PIN code or a Password, and can be configured to require re-authentication after a configurable period of non-use (for example, 1 minute to 1 hour). In addition, the policy allows the setting of a login failure threshold from 3 to 20 attempts, after which all data under the control of the AWP mobile app will be locally wiped.

In circumstances where lost or stolen mobile devices do not attempt to connect to the service, and thus cannot be commanded to perform a wipe operation, it is nevertheless desirable to provide remote wipe capabilities. In support of this, **AWP implements a periodic Account Validation policy, also often referred to as a Poison Pill policy.** When enabled, each AWP mobile app must connect to the service with a minimum period, settable from 1 day to 30 days. If a mobile app exceeds the Account Validation period, then the local decryption key for all stored files is deleted, rendering the encrypted data useless (analogous to the operation of Crypto-Locker viruses). However, in the event that the user subsequently logs-in to the account with the valid password, and if the account has not been disabled, then the decryption key is redelivered to the mobile app, thus restoring access to the local encrypted repository.

Active Directory Integration for User Deployment

Enterprise-class account management and authentication for users and groups is supported within Autotask Workplace™ through the Active Directory Integration feature, which is available as part of the Enterprise plan. This feature enables IT personnel to import user and group account metadata from Active Directory into AWP, and to force all AWP user authentication through Active Directory. AWP does not maintain any log-in information during user authentication, but acts as a proxy between the user and Active Directory servers. Within the AWP service, AWP extends the use of AD Groups to include both access control and policy enforcement (Group Policies).

Application Management Authentication

Mobile device data is encapsulated within the mobile app for greater content control. One of the more unique aspects of the Autotask Workplace™ service offering includes **integrated Office-style viewing, creation and editing tools for mobile devices.** Currently supported on iOS and Android platforms, these integrated apps ensure that mobile viewing, creation and editing by users is done within the confines of the AWP Mobile App. This effectively ensures that mobile-accessible data remains within an envelope of privacy, minimizing exposure of company data to 3rd-party applications.

Reporting

Beyond privacy-oriented security features such as encryption, access policies and account management, **AWP implements a set of advanced reporting capabilities that are specifically designed to support auditing for compliance with company policies.** These advanced reporting features, which are available as part of the Enterprise plan, enable Admins to generate and export custom reports in order to establish audit trails and analytics on the following types of events:

- **Team Events** - Account management events for all users and groups
- **User Access Events** - Device access, PC access, User logins, IP address mapping
- **Project Events** - All changes to any Projects, folders, or files
- **User Report** - List of all Team Members, their roles, storage quota, creation timestamp and last login
- **Computer Report** - List all desktop agents by Member, computer type, OS and Agent versions, installation timestamp and last connect timestamp
- **Mobile Device Report** - List of all mobile clients by Member, mobile device type, OS, and App versions, number of logins and last login timestamp

Reports can be customized and filtered to include or exclude a variety of events based upon various criteria, such as date range, user ID, file name, IP address, method of access and more. Reports can be either viewed on-screen or exported to either PDF or XLS formats. When reporting on user accesses, any user access event can be mapped to specific source IP addresses, and can be viewed on a geographical map.