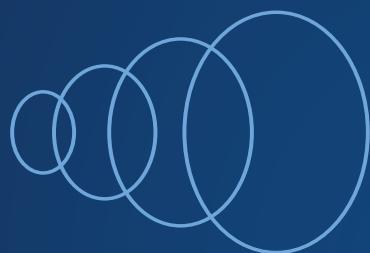


Acronis



ACRONIS ACCESS

Secure Content
for **the Mobile**
ENTERPRISE

Introduction

When enterprise mobility strategies are discussed, security is usually one of the first topics on the table. So it should come as no surprise that Acronis Access Advanced was designed top to bottom to meet the needs of mobile users while providing enterprise class security.

Acronis Access Advanced enables enterprise IT to provide their users using any device - desktop, laptop, tablet or smartphone - to securely access, sync and share corporate content while maintaining control over security and compliance. Content can be accessed from file servers, NAS, SharePoint, and personal devices, and shared with internal and external constituents. Acronis Access Advanced empowers IT to control the level of security needed and promote end user productivity anywhere, anytime, from any device - desktop, laptop, tablet, or smartphone.

Configurable and deployable across the enterprise within minutes, Acronis Access Advanced promotes efficient IT management while ensuring corporate security and compliance standards are met. Enterprise end-users of Acronis Access Advanced can access, browse, search and interact with corporate documents as well as sync and share files with other constituents, improving productivity regardless of job function.

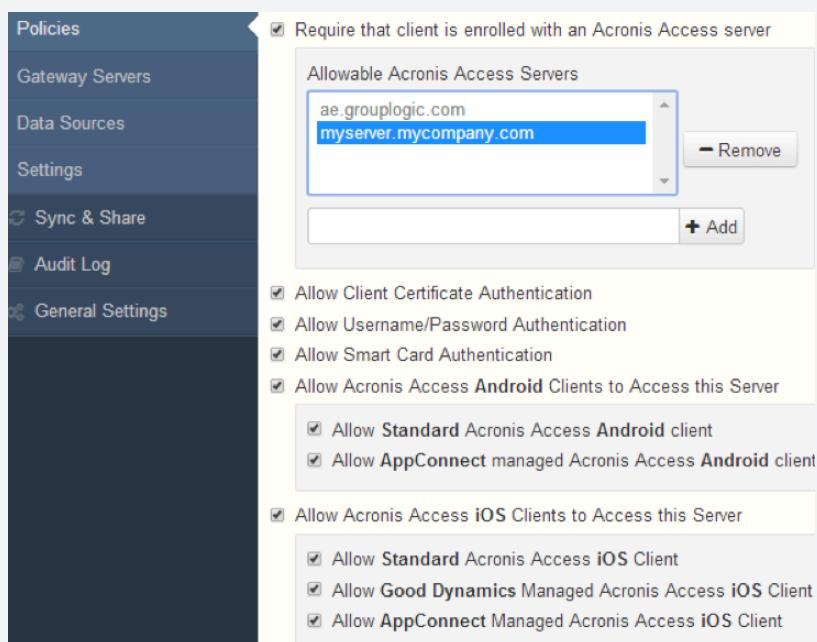
Specific to security, Acronis Access Advanced takes into consideration three critical elements that need to be secured: the server itself, the network and the client. In addition, the user community is composed of various stakeholders - the end-user, the IT administrator, and the security/ compliance teams - each with different needs, workflows and requirements.

Acronis Access Advanced addresses each of them independently and as a whole. This document describes how Acronis Access Advanced enables simple, secure and managed mobile file access, sync and share.

Server Side Security

Acronis Access Advanced security starts on your corporate servers and data sources. Unlike consumer and cloud-based solutions, Acronis Access Advanced runs on-premise and allows the IT group to have total control, since your valuable business content and documents remain on corporate-controlled servers and devices. The Access Advanced server software runs on all editions of Windows® server, including 2003, 2008, 2012 and integrates with capabilities of the existing environment. Acronis Access Advanced uses the already existing NTFS permissions to marshal file access and seamlessly integrates with Active Directory for user authentication, permissions and provisioning.

Acronis Access Advanced includes the Access Advanced Management Console, which allows all aspects of the solution, policies and security settings to be remotely managed by IT, on a per-user or per-group, per data source basis. When a user logs in from their device, their encrypted credentials are securely sent across the network. Access to directories and documents is governed by your existing Active Directory permissions, and can optionally be shaped further by setting user or group based policies with the Acronis Policy Engine. For instance, you could decide to allow read-only access to users from mobile devices in certain groups that may normally have full read/write access from their desktop computers. This restriction may be put in place to prevent mobile users from deleting files, for example. All clients connecting to your data sources are constrained by the policies that you have configured. There are many options available to the administrator for controlling policies and access. See the Management Capabilities section below for more details. The server administrator can require that connected iOS or Android devices be managed by an Acronis Access Advanced Client Management server.



Network Side Security

Acronis Access Advanced ensures that all data transfer to and from source and device is secure. All Access traffic is sent end-to-end as encrypted HTTPS, so it's as secure as Internet financial transactions. It doesn't matter whether your user is connecting from the office, over cellular data lines or from a public WIFI hotspot. All data is always encrypted and secure.

Following standard enterprise practices, to allow access from outside your firewall, there are several options:

1. Port 443 access: Acronis Access Advanced uses HTTPS for encrypted transport by default, so it fits in naturally with common firewall rules allowing HTTPS traffic on port 443. If you allow port 443 access to your Access Advanced server, authorized clients can connect while inside or outside of your firewall. Acronis Access Advanced can also be configured to use any other port you prefer.
2. VPN: Mobile devices support VPN connections, so if you prefer to run all remote traffic through a VPN tunnel, Acronis Access Advanced supports it. Both the built in VPN client and third-party VPN clients are supported. Management profiles can be applied directly or through Mobile Device Management (MDM) systems to configure certificate-based "VPN-on-demand", for seamless access to Acronis Access Advanced and corporate resources.
3. Reverse proxy server: If your organization has a reverse proxy server set up, clients can connect without the need for an open firewall port or a VPN connection. The Acronis Access client supports password and certificate authentication with a reverse proxy server, providing the opportunity to require 2-factor authentication before gaining access to corporate file servers, NAS or SharePoint resources. The Acronis Access Policy Engine has the ability to configure the client application to only allow connections using X.509 SSL certificates.

Mobile Device Client Side Security

Access security extends from server to network to the mobile device. On the device, multiple layers of security can be established to protect your corporate documents and data:

Reverse Proxy: If a reverse proxy solution is used to provide mobile client access to Acronis Access Advanced server(s) inside the datacenter, a password or certificate authentication can be required before the client can reach the Acronis Access Advanced server. This allows for requiring 2-factor authentication before gaining access.

Login Password: To log into an Acronis Access Advanced server, a user must provide valid credentials, username and password, which is then authenticated through Active Directory (or a local user account on the Acronis Access Advanced server). The login credentials are transmitted encrypted from the mobile app to the server and stored encrypted in the device itself, if the saving of passwords is allowed by Acronis Access Policy Engine.

App Password: The Acronis Access mobile client app can be set to require a password every time it is launched or after a certain period of inactivity. An App Password can be required through an Access Client Management profile. In addition, password complexity and mandatory wipe of the app after a number of failed login attempts can be configured.

Mobile Device Passcode: Setting a Passcode Lock on the device itself adds more layers of security. First, it forces the user to enter a password to unlock the device, protecting the entire device. In iOS devices, it also activates the Apple® Data Protection file encryption capabilities (For more information about Apple Data Protection see <http://support.apple.com/kb/HT4175>).

Enrollment and Remote Management: Administrators can enforce the use of Acronis Access app passwords and device passcodes as well as permissions and settings through Acronis Access policies and mobile device management profiles.

For instance, all on-device file storage within Acronis Access app can be disabled, ensuring files are never saved in case a device is lost or stolen.

Remote Wipe: Administrators can selectively remote wipe the Acronis Access app files and settings on a mobile device the next time it tries to connect.

This ensures all corporate data is destroyed and resets the app to a blank, un-configured and unmanaged state. The mobile client can specify password and cache settings, or they can be set and enforced by the server.

The screenshot shows a user interface for managing application policies. At the top, there are tabs: Security Policy, Application Policy (which is selected), Sync Policy, Home Folders, and Server Policy. The Application Policy tab is active, displaying several configuration options:

- Require Confirmation When Deleting Files
 Allow User to Change This Setting
- Set the Default File Action 
Default Action: Show Action Menu
 Allow User to Change This Setting
- Allow Files to be Stored on This Device
 - Allow User to Store Files in the 'My Files' On-Device Folder
 - Cache Recently Accessed Files on the Device 
Maximum Cache Size:
 Allow User to Change This Setting
- Content in My Files and File Inbox Expires after days 

The Acronis Access app includes built in PDF annotation and Office document creation and editing. These features allow most common business documents to be opened and edited within the secure sandbox of the app, greatly enhancing security and data protection.

Management Capabilities

The Acronis Access Policy Engine provides comprehensive tools to allow administrators to set policies and permissions for users, groups and devices that access the server and provisioned data sources. These tools ensure IT has full control over mobile device access to corporate files.

Examples of Policy Engine controls and options include:

- One or two-factor Access client app enrollment.
- Client device/app status tracking.
- User & Group Profiles.
- Application lock password policies.
- File caching and iTunes backup policy.
- Application-level file permission policies (create, copy, move, delete, rename).
- Application-level file distribution policies (allow emailing, printing, editing in other applications, copying & pasting text).
- Whitelisting and blacklisting of the 3rd-party apps permitted to open Acronis Access files.
- Assignment of servers and home directories.
- Assignment network folders (including 1-way and 2-way sync folders) displayed in the client application.
- Remote application lock password reset.
- Remote wipe capability.

Acronis Access Advanced allows profiles to be assigned to Active Directory users or groups. Group profiles are assigned an order of precedence and a user is governed by the highest priority group profile they are a member of. Once Acronis Access management profiles have been established on the server, IT can send enrollment invitations to users. This action launches the Acronis Access app and conveys the required Access management server name and one-time use activation PIN to the app.

The user is prompted for their username and password, and their management profile is applied. They are asked to set an application lock password if required, and warned of any restrictions. From that point and on, each time the Acronis Access client is started, it calls home to the Acronis Access Advanced server and is updated with any policy, setting or resource changes. In addition to Acronis Access policies, administrators can use a Mobile Device Management (MDM) system to enforce device level policies for corporate devices. For example, you can require the use of an iOS Passcode Lock through an iPad Configuration Profile set up through an MDM server.

Management Options

The screenshots below illustrate some of the management options available with Acronis Access Advanced.

An IT administrator can require the use of Acronis Access application lock passwords through a profile setting on the Acronis Access Advanced server's Policy Engine. When that option is enabled, users will be required to enter an Access app password each time they start the Access application. App whitelists and blacklists can also be specified, restricting Access files to only be opened third party or custom apps deemed appropriate.

The screenshot shows the 'Application Policy' tab selected in the top navigation bar. The main configuration area is titled 'App Password Creation' with three radio button options: 'Optional' (selected), 'Disabled', and 'Required'. Below this, there are several configuration fields:

- 'App Will Lock:' dropdown set to 'Immediately upon exit', with an unchecked checkbox 'Allow User to Change This Setting'.
- 'Minimum Password Length:' input field set to '0'.
- 'Minimum Number of Complex Characters (such as \$,&,!):' input field set to '0'.
- 'Require One or More Letter Characters' checkbox (unchecked).
- 'Mobile client app will be wiped after [10] failed app password attempts' checkbox (unchecked).

At the bottom, there is a section for 'Wipe or Lock After Loss of Contact' with two options:

- 'Mobile client app will be [locked] after [30] days of failing to contact this client's Acronis Access server' checkbox (unchecked).
- 'Warn user starting [5] days beforehand' checkbox (unchecked).

If a mobile device is lost or stolen, the files on that device can be remotely wiped the next time an Acronis Access connection is established with the server. Remote wipes are accepted by the Access application before the application password is even entered. This ensures that a wipe will occur, even if the device is in the hands of someone who cannot log into the app.

Through Acronis Access policies, it is possible to restrict the capabilities of clients to fit your security requirements. Corporate files can be sandboxed into Access's securely encrypted storage by disabling the ability to email files, print, copy and paste text, or open files in other applications.

The ability to store or cache files locally on the device can also be disabled completely, ensuring that sensitive files are never on the device if it is lost or stolen.

File Operations <input checked="" type="checkbox"/> File Copies / Creation <input checked="" type="checkbox"/> File Deletes <input checked="" type="checkbox"/> File Moves <input checked="" type="checkbox"/> File Renames	Data Leakage Protection <input checked="" type="checkbox"/> Opening Acronis Access Files in Other Applications App Whitelist/Blacklist: None ▾     <input checked="" type="checkbox"/> Sending Files to Acronis Access from Other Apps  <input checked="" type="checkbox"/> Sending Files to Acronis Access Using Quickoffice 'Save Back'  <input checked="" type="checkbox"/> Emailing Files from Acronis Access   <input checked="" type="checkbox"/> Printing Files from Acronis Access    <input checked="" type="checkbox"/> Copying text From Opened Files   
Folder Operations <input checked="" type="checkbox"/> Folder Copies <input checked="" type="checkbox"/> Folder Deletes <input checked="" type="checkbox"/> Folder Moves <input checked="" type="checkbox"/> Folder Renames <input checked="" type="checkbox"/> Adding New Folders <input checked="" type="checkbox"/> Bookmarking Folders	Annotation and Editing <input checked="" type="checkbox"/> Allow PDF Annotation <input checked="" type="checkbox"/> Editing & Creation of Office Files <input checked="" type="checkbox"/> Editing & Creation of Text Files 
'mobilEcho' File Links <input checked="" type="checkbox"/> Emailing 'mobilEcho' File Links   <input checked="" type="checkbox"/> Opening 'mobilEcho' File Links  	

Acronis

About Acronis

Acronis sets the standard for New Generation Data Protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OS across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products have been named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit www.acronis.com.

Follow Acronis on Twitter: <http://twitter.com/acronis>.

Copyright © 2002-2014 Acronis International GmbH. All rights reserved.
"Acronis" and the Acronis logo are trademarks of Acronis International GmbH.
Other mentioned names may be trademarks or registered trademarks of their
respective owners and should be regarded as such. Technical changes and differences from the
illustrations are reserved; errors are excepted. 2014-07