3188 Airway Avenue
Costa Mesa, CA 92626

Active Cypher File Fortress (ACFF)

Installation Guide

for the Azure Marketplace

Introduction

All too often, file protection which incorporates encryption as part of the solution is avoided due to complex installation, deployment and administration; or because the solution applies itself too broadly or specifically to the location of the files (such as whole-disk encryption).
Our goal is to provide a robust solution that applies encryption and protection at the level of each **file** which has been selected for protection, and which continues to protect those selected files, *regardless of their whereabouts*.

Active Cypher File Fortress (ACFF) provides this capability with Microsoft Azure and Azure Active Directory (AAD) at its center. ACFF can be deployed entirely in Microsoft Azure. ACFF can also be deployed in a hybrid configuration, integrating across your file server(s) and Domain Controller. In either implementation, Azure Active Directory (AAD), your on-premises Active Directory (AD), plus other resources in Microsoft Azure, all work together seamlessly.

The ACFF installation process is automated, including adding and configuring the necessary resources in your Azure tenant. During installation, you will be prompted to provide information regarding your domain and organization and select shared folders to protect and encrypt, but the real work will be done by the ACFF Installer.

Once the installation is complete, the protected file share(s) will be encrypted automatically on the file server. Once you deploy the ACFF *User Agent* MSI file on your workstations, your users authenticate themselves to Active Directory as they have been doing, and the protected files decrypt when needed for users who have the proper AD Security Group authorization.

Active Cypher's only requirement of IT administrators is that they continue to perform their regular duties of managing Users, Groups, File Shares, and Permissions within Active Directory, just as they have always done. ACFF works silently in the background, shadowing and applying those administrative changes instantly, thus limiting the decryption of files to only users that Active Directory has been configured to allow.

Deployment of Active Cypher File Fortress (ACFF)

Software requirements

- Microsoft Domain Server 2008 R2 or newer
- Windows 7 or newer client (Windows 10 preferred)
- A Microsoft Azure or Office 365 subscription

Architecture

Secure Private Cloud – ACFF creates a secure private cloud for the client. All the resources are located in the client's Azure tenant. As a result of the secure private cloud, no 3rd party (including Active Cypher) has access to your data.

Key Management – As part of ACFF, we created a multi-layered implementation of AES-256 that is tied to a multi-factored authorization which is based on device, user identity, and thousands of bits of intelligence gathered in Azure Log Analytics and Microsoft Graph Security data. Together, the ACFF API and user validation challenges result in a state-of-the-art secrets information exchange process. This ensures that keys cannot be stolen or compromised, and that data cannot be accessed by any unauthorized persons or systems.

Microsoft Active Directory – ACFF is deeply integrated with your Active Directory – Security Groups & Users organizational structure which already protects your corporate assets stored in the file system. Working in tandem with Active Directory's access control and auditing features to encrypt each file as it is stored in the Shared Folders which are shared out to users, ACFF allows IT to govern the protection directly and unambiguously through Active Directory Security Groups. The ACFF rules engine connects via an API to assess risk threats whenever a file decryption request is presented.

Deploying ACFF in your environment

Phase 1: Run the **AC Scout** utility from a workstation PC that is domain joined.

Phase 2: Authorize the custom-generated **Active Cypher setup packages** to run

Phase 3: Deploy the **Active Cypher User Agent** to the appropriate workstations.

Phase 1: Running AC Scout

Why do I need to run Active Cypher Scout?

Active Cypher is a software solution that protects your enterprise data by encrypting it and making it available only for authorized users. In order to protect your data, Active Cypher components are deployed onto your file servers. The deployment process is very intuitive; however, since the software is integrated with your file servers, we need to make sure that it best suits your existing IT configuration. We would like to solve any potential configuration issues before deployment. Therefore, we have created **Active Cypher Scout**.

Active Cypher Scout is a combination of management tool (**Active Cypher Scouting Manager**), reporting tool (**Active Cypher Scouting Reports**), and on-prem inspection tool (**Active Cypher Scouting Agents**), that work together as an application that checks your enterprise IT configuration and helps you adjust it to optimize your data protection. Once the corporate IT configuration is verified, Active Cypher Scout displays a report with its findings. Based on the results of the report, the Active Cypher team will be happy to work together with you to solve any remaining obstacles to the successful protection of your data.

What does this tool install, and what will it be doing?

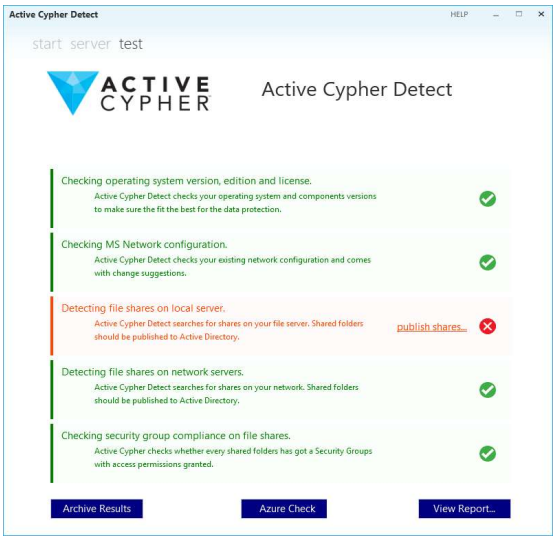
Active Cypher Scout is a standalone application run from a file server to inspect your IT enterprise configuration for compatibility with Active Cypher. Active Cypher Scout does not require any installation.

Active Cypher Scout shows a wizard which guides you through any configuration changes required for activating the Active Cypher data protection. At its conclusion, the application displays a report with its findings.

All the information collected, analyzed and displayed by Active Cypher Scout is retained in the local folder in which it runs. The information collected cannot be shared externally unless the "Send Results" button in Active Cypher Scout has been clicked, granting permission to transport the collected data to the Active Cypher Crypto-License Service for further analysis.

In addition to inspecting the architecture configuration of the local Active Directory, Active Cypher Scout will query the Azure Active Directory tenant linked with the local domain and inspect it. Active Cypher Scout also checks whether synchronization between the local Active Directory and the Azure Active Directory is configured properly. Active Cypher Scout does not make any changes to your Azure Active Directory subscription. It only reads information from Azure. The information read from Azure is never shared with the outside world.

What is required before I run Active Cypher Scout?



Active Cypher Scout should be run by a user who is a member of Domain Admins, Enterprise Admin and Schema Admins groups in Active Directory of your local domain. In addition, the user should be a local Administrator on the file server machine where Active Cypher Scout will be run.

Active Cypher Scout should be run on a Windows Server machine (a file server that is joined to the local Active Directory domain). The file server should contain NTFS Shares. The shared folders should be published to Active Directory.

The Azure inspection functionality requires credentials to log into the Azure tenant linked with the local domain. To run the check successfully, the credentials provided need to be for the Azure Global Administrator.

How do I run Active Cypher Scouting Agent?

The user running Active Cypher Scout should have permissions on both the domain and on the file server machine. On the local Active Directory, the user should be a member of Domain Admins, Enterprise Admins and Schema Admins groups. On the file server machine, the user should be a member of the local Administrators group.

The application can be started by double clicking the Active Cypher Scout.exe icon.

On the first screen, the Active Cypher Scout wizard informs the user of the safe and secure system queries that the application will run on the file server. The verification starts once the Start button is pressed.

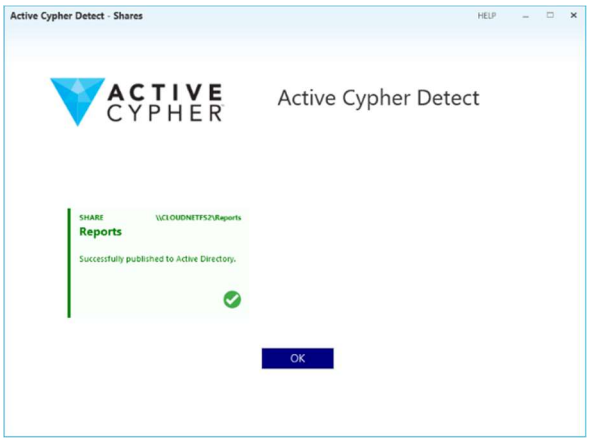
In the example case being demonstrated in the screenshots here; the application detects a configuration concern (as indicated by the red shading) and provides the user with detailed info and suggested actions. In many cases, Active Cypher Scout can also assist with configuration concern, if granted consent.

On the screenshot above you can see the application detecting shared folders that are not published to Active Directory.

The image to the left shows how the user can click the publish link to fix the issue.

Once the shared are published into Active Directory, Active Cypher Scout will show an updated report.

The next required action is to click the "Azure Check" button.

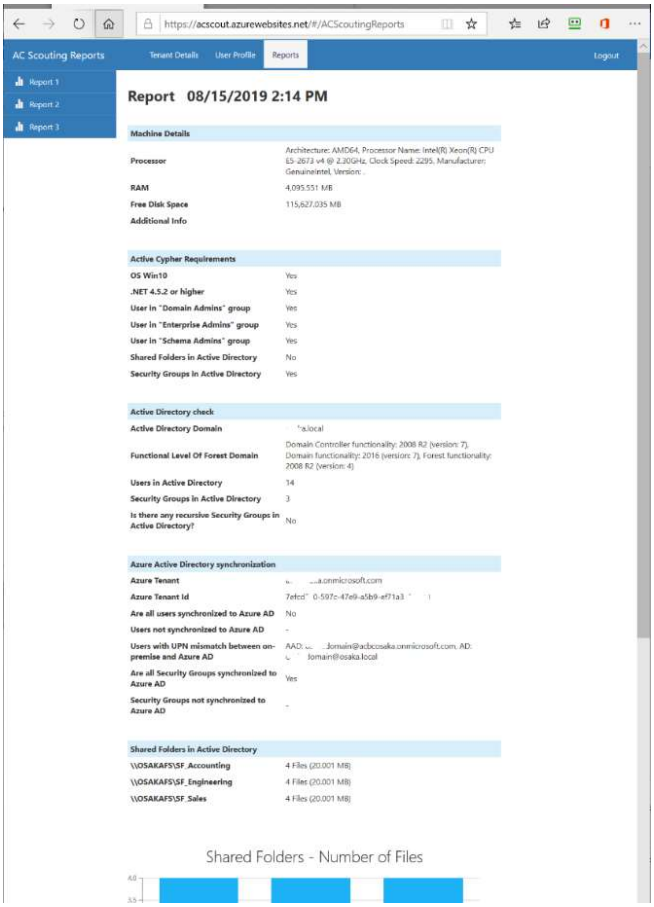


This allows the Azure Active Directory inspection and confirms the synchronization between Azure Active Directory and the local domain is established.

The inspection of Azure requires authenticating to Azure to verify if the Active Directory is properly synchronized with the Azure Active Directory.

The user clicks the Login button and is requested to provide credentials of the Global Administrator account.

After a successful login, Active Cypher Scout runs the Azure verification and displays a result on the screen.



The final step is the option to display a report with the findings by clicking View Report button. The report will be shown in the form of two graphical dashboards displaying information about shared folders, files and Security Groups.

What data is collected by the AC Detect tool?

Active Cypher Scout gathers data in a few areas:

- Information about your file server machine, its CPU, RAM memory, configuration, version of Microsoft Windows and .NET Framework.
- Data related to the shared folders of your file server, their details, and the type and size of data stored in the folders.
- Information regarding your Active Directory Forest and Domain, as well as Users and Security Groups configuration and their access to Shared Folders on the file server.
- If explicitly requested by the user, Active Cypher Scout gathers data about the Azure Active Directory tenant and the status of its synchronization with the local domain.

What about privacy? Does this tool communicate with the outside world at all?

Active Cypher Scout does not communicate with the outside world on its own and does not send any results out unless explicitly told to do so.

The user can explicitly request sending the results out to Active Cypher by clicking the Archive Results button at the final step of the application. Once submitted, the results will be available solely to the Active Cypher team allowing us to work together on adjusting the enterprise IT configuration.

The results will **ONLY** be available to authenticated administrators of your tenant on the Active Cypher Crypto-License Service.

Phase 2: Active Cypher installation via the File Server

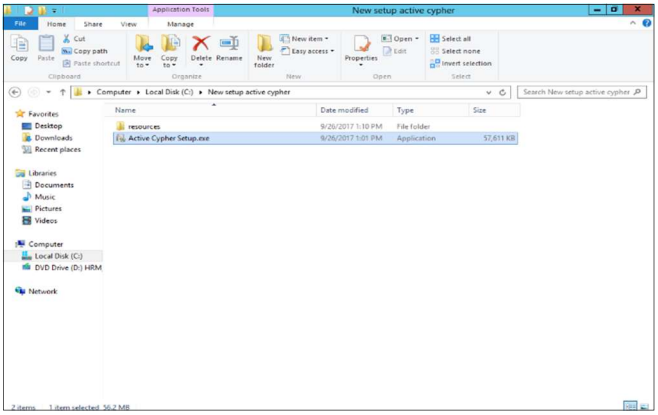
Active cypher installation should be done in File Server where Microsoft Azure Active Directory connect was installed.

2.1 Pre-requisite

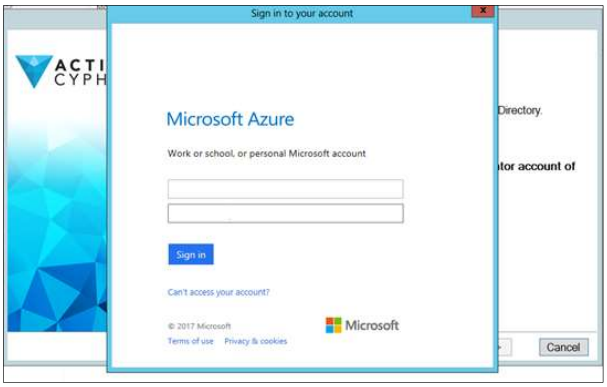
a. Navigate to https://resellers.activecypher.com/#/home
b. Login to Active Cypher Reseller Portal
c. Create a new client for the global admin used to configure AD Connect
d. Build and download Azure setup

2.2 Active Cypher Azure setup installation

a. Build and download Azure setup
b. Extract and Run the Azure Setup.exe file



Enter Azure global admin credentials to connect to Microsoft Azure



c. Choose the required Azure tenant, Azure Subscription on the dropdown and click Next button

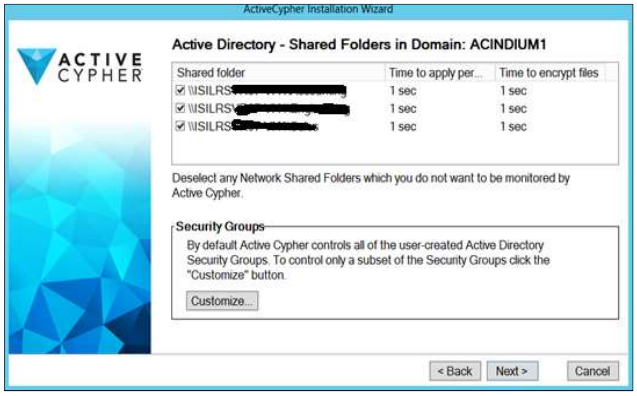
d. On successful completion of Azure piece installation, click File Server Setup button

e. In File Server setup, enter Email address that matches the licensed domain, Phone number and set password for ACServices account

f. Verify File Server Log is generated in the Active Cypher setup folder

g. Verify Active Directory Environment and click Next button

h. Verify Active Directory Shared Folders and Security Group in the domain and click Next button



i. Verify Installation is completed successfully

j. Click Finish button in the Installer

Phase 3: User Agent installation on the Workstations

3.1 Pre-requisite

a. Navigate to https://resellers.activecypher.com/#/home
b. Login to Active Cypher Reseller Portal
c. Build and download User Agent setup for the global admin used to configure AD Connect

3.2 User Agent Installation

a. Run the User Agent setup exe file in the Work Station
b. Verify the User Agent is installed successfully without any errors
c. Verify the Log files are created for the User Agent
d. In the mapped shared folder verify whether the files are decrypted successfully

Verifying the Installation

1. On the File Server

   Drop any files (For e.g., .doc, .pdf, .mp4 etc.) to the folder which was shared with Active directory and verify that the files got encrypted in .amt file format.

2. On the Workstation

   Open the files present in the network shared drive and verify that the files got decrypted with the original text.