Tech Brief: Actifio VDP Data Security

All components of Actifio Copy Data Virtualization have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

This tech brief describes:

Secure Operating System Access to Actifio Appliances

Actifio systems run on a hardened Linux software stack. Linux user accounts and direct access to the operating system are not required nor employed for normal operations and support of the Actifio systems. Direct access to the operating system can only be obtained via the use of time and system-limited cryptographic credentials obtainable by select users within Actifio support and engineering who have been undergone extensive background checks. Certificates are stamped with the identity of the user to whom they are issued, the issuing is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. Actifio employs a locked-down operating system that minimizes the possibility of unauthorized access. Even privileged users with direct access to the appliance's operating system can not access customer data unless they have access to a host on the storage fabric which can mount and understand the data.

Actifio VDP in a vSphere Environment

When Actifio VDP is deployed on a public cloud, the instance itself is protected by the cloud's security architecture. When deployed in an on-premises vSphere environment, the security of the instance is dependent on the configuration of the vSphere environment which hosts it. Insufficient security controls of the vSphere environment could allow an attacker to perform a side-channel or side-loading attack and gain unauthorized access to data or privileges on the Actifio appliance(s).

While specific vSphere hardening is outside of the scope of this document, Actifio recommends customers follow VMware's best practices including, but not limited to, ensuring that the server BIOS and firmware be kept up-to-date along with the ESXi and vCenter versions to mitigate the "Meltdown/Spectre" class of side-channel vulnerabilities. Additionally, virtual machine encryption (available in vSphere 6.5+), can mitigate unauthorized tampering or side-loading of the Actifio appliance(s) virtual disks. Customers should consult with their internal IT and/or security teams, VMware, or other resources with regard to security of a vSphere environment.

Internet Protocol (IP) Network Security

All components of Actifio Copy Data Virtualization have been designed from the ground up with security in mind and the IP interfaces as traditional attack vectors have been given particular focus in hardening efforts.

Standard Network Services

The following services are deployed and listening on open network ports:

- HTTP (80): Actifio appliance resource center. provides local downloads of the Actifio Desktop and Connector software. No appliance control or data access is possible on this portal.
- HTTPS (443): Provides TLS-encrypted communication between Actifio GUI clients and the appliance, as well as some appliance-to-appliance communication. SSL certificates may be customer replaced.
- ssh (22): for user CLI
- ssh (26): for support CLI
- Actifio replication (5103): encrypted appliance-to-appliance data replication traffic. Both sides of this link utilize strong mutual authentication of the partner appliance.
- iSCSI, iSNS (3260, 3205): iSCSI target
- cimserver (5989): SSL encrypted WBEM (CDS only and utilized for SRM integration)
- svrloc (427): service location for WBEM (CDS only)

Appliance Outbound Connections

The appliance may make outbound connections to the following services, but not does not listen on or run a service for these ports unless listed above:

- LDAP/LDAPS (389/tcp, 636/tcp) Authentication of user accounts against a central directory if configured
- DNS (53/udp) Resolution of addresses for hosts, VMs, vCenters, and other customer infrastructure
- NTP (udp/123) Clock synchronization against a customer-provided or public source
- SMTP (25/tcp, 465/tcp) Optional transmission of events via a customer-provided SMTP email relay server, can optionally utilize SSL encryption.
- SNMP (162/udp) Optional delivery of events in the form of SNMP traps to a customer-provided trap receiver
- SSH (26/tcp) Encrypted intra-cluster communication between CDS nodes
- vSphere API (443/tcp) Required to communicate with vCenter servers and ESX hosts for snapshot and image management during backup and mounts over an encrypted link.
- ESXi data connectivity (902/tcp) Encrypted connectivity to VMware ESXi hosts for data movement operations.
- Actifio Connectors (5106/tcp) Encrypted control channel between Actifio appliance and hosts running the Actifio Connector.
- Appliance-to-appliance Replication (5103/tcp, 5107/tcp) Encrypted replication data and control between two Actifio appliances.
- SecureConnect (optional feature) remote support (1194/udp, 443/tcp) Encrypted remote support access to Actifio data centers. As the connection is mutually authenticated with strong cryptography, it is recommended that the destination not be limited by a firewall.

SNMP

Most SNMP code on Actifio appliances is outgoing only, sending traps to a configured receiver to notify events and failures.

The exception is when integrated with Actifio Optimized Storage or SAN Fabric, Actifio CDS and CDX Appliances listen on UDP 162 for SNMP traps from specified IPs that are whitelisted for Actifio CDS Integrated Storage components.

A list of whitelisted IP's can be viewed with the following commands. Currently SNMP v1 and v2 are supported.

```
udsinfo
lsmonitoreddevice
id
name
type
address
5847
Brocade--}SAN
switch
X.X.X.X
5850
DS3512--}A
storage
X.X.X.X
5852
DS3512--}B
storage
X.X.X.X
```

No Actifio configuration will ever accept any SNMP walk or write (e.g. GetRequest, SetRequest, GetNextRequest, GetBulkRequest) and this configuration of community names is not required or supported.

Cross Cluster Communication and Replication

All Actifio appliances utilize strong mutual authentication of the partner appliance with verification of 2048-bit RSA public keys.

Once authenticated, data in flight between appliances is encrypted using 256-bit AES encryption with session keys protected by Diffie-Hellman algorithms affording Perfect Forward Secrecy (PFS) over a TLS v1.2 channel.

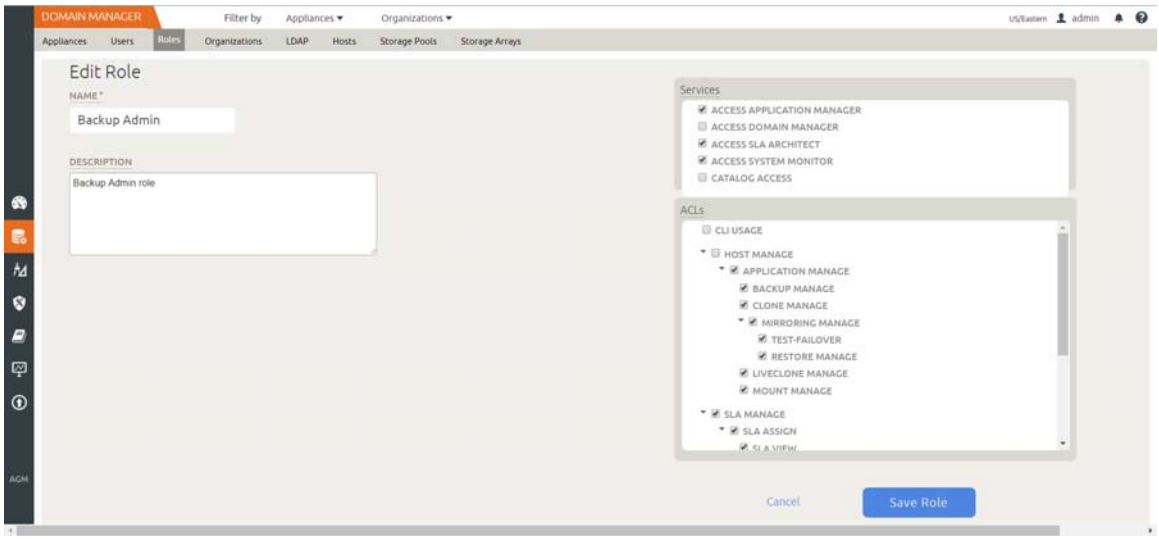
Access and Authentication to Actifio Systems

Actifio uses a very rich role-based access control mechanism that allows an administrator to assign rights to users to operate on objects. These users and rights are constrained to operating on objects owned by 'Organizations' of which they are members.

A role consists of a group of rights. Roles are assigned to users to use those rights on specific objects.

Users, Roles, Rights, and Organizations can all be modified and managed from either the CLI or the Actifio Desktop.

Coupled together, roles and organizations allow the customer to define a specific group of servers/hosts/applications that a given user can perform specific actions on.



A Role Called Backup Admin as Created in AGM

Authentication and Authorization

Actifio appliances can either utilize an internal user directory or integrate with an external LDAP source, including Active Directory. This allows users to leverage their existing usernames and passwords, ensuring compliance with corporate password standards such as complexity and expiration. SSL encryption may optionally be utilized between the Actifio appliance and the external LDAP server. LDAP/AD groups may be mapped to specific user-defined roles within the appliance.

Actifio Secure Connectivity and Data Movement with iSCSI in the Public Cloud

When Actifio is deployed in the public cloud, iSCSI is utilized to transfer data between instances and the Actifio appliance(s). Actifio establishes in-depth secure data transfer at multiple levels to ensure that no Connector-equipped Host or Appliance can access unauthorized data.

Actifio recommends that both the appliance(s) and instances communicate over the provider's private network, using non-routable IP addresses. Under these conditions, the traffic will be protected by the provider's software-defined network and subject to all of the protections and external accreditations (e.g. SOC2 and ISO27001) most public cloud providers offer.

Actifio also recommends:

- Firewall rules at the Public Cloud level that restrict iSCSI and/or control channel communication (5106/tcp) between the authorized appliance(s) to authorized instances only.
- Enable bi-directional iSCSI authentication (CHAP) utilizing pre-shared secrets that must be known to both the appliance(s) and the authorized instances before any data can be accessed.
- Install the appliance(s) certificate(s) in the Connector's trusted certificate directory on each instance.
- Some providers automatically encrypt all data at-rest (e.g. Google Cloud). On public clouds where such encryption is optional (e.g. EBS encryption on Amazon Web Services), it should be enabled to protect the appliance(s) virtual disks.

When properly configured, multiple levels of cryptographic authentication and security protect both the control and data movement channels. Additionally, only instances that have been pre-registered with the appliance(s) will be able to access data. All data operations are subject to the appliance(s) Role Based Access Control (RBAC) that validate that a user is authorized to perform a certain operation, with certain data, on a specific instance or host.

Access Logging and Auditing

Actifio maintains a full audit log of every command that has been executed on the platform, including logging requester's IP address and method of access (CLI or Actifio Desktop). The audit log can also be retrieved via the Actifio REST API for automatic ingestion into a central log or event correlation repository.
The audit log can be viewed from the CLI using the following command:

```
sa--hq1:~
$
udsinfo
lsaudit
id username stat status component issuedate proxy command ipaddress privileged
172675 admin 0 UI 13/12/2013 03:24:13.707 loginadmin 192.168.225.2 true
172675 admin 0 CLI 13/12/2013 03:24:25.707 loginadmin 192.168.225.2 true
172676 admin 0 UI 13/12/2013 03:24:14.124 lsprincipaldata1 192.168.225.2 false
172677 admin 0 CLI 13/12/2013 03:24:26.578 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2
false
172678 admin 0 CLI 13/12/2013 03:24:28.469 lsdiskpooldatamdiskgrpLIKE'act_pri% 192.168.225.2
false
172679 admin 0 UI 13/12/2013 03:24:18.737 lsdiskpooldatamdiskgrpLIKE'act_per% 192.168.225.2
false
172680 admin 0 UI 13/12/2013 03:24:19.037 lsdiskpooldatamdiskgrpLIKE'act_ded% 192.168.225.2
false
172681 admin 0 UI 13/12/2013 03:24:24.579 appgroupingregular 192.168.225.2 false
172682 admin 0 UI 13/12/2013 03:24:25.384 appgroupingremote 192.168.225.2 false
172683 admin 0 UI 13/12/2013 03:24:25.900 appgroupingorphan 192.168.225.2 false
```

Data Encryption

Encryption In Flight

Data inflight traveling between Actifio appliances, as well as remote support (SecureConnect) sessions, is encrypted in flight using AES-256 with session keys exchanged via Diffie-Hellman.

Management (GUI or CLI) sessions are protected utilizing the highest cipher negotiated between the client computer and the Actifio appliance.

Data traveling between Actifio and VMware environments is protected using the strongest cipher negotiated between the Actifio appliance and VMware ESXi/vCenter hosts up to and including AES-256. For hosts protected out-of-band using the Actifio Connector, the control channel between the appliance and the host is encrypted utilizing TLS and strongest cipher negotiated between the host and the appliance, however data movement occurs over iSCSI, which is not encrypted. If sensitive data is being transmitted via this mechanism it is recommend that this traffic be isolated to a given VLAN or subnet, or configured to use Fibre Channel, so that it cannot be intercepted.

Encryption At Rest

Administrative end-user credentials are hashed with a strong one-way SHA-256 hash in the appliance database. Credentials used by the appliance to access other systems (vCenters, databases, etc) are stored in an AES256 encrypted form.

Actifio Sky appliances encrypt customer data (snapshots and dedup) utilizing AES 256-bit encryption. Actifio CDS and CDX Appliances rely on optional encryption at the hardware layer through the use of Self Encrypting Drives (SED)-containing storage arrays. Internal system drives on CDS, including optional SSD cache, do not store customer data.

> ***Note:*** *Actifio CDX Appliances have a heartbeat connection between the two nodes. This connection is not encrypted.*

Command Line (CLI) Access to Actifio VDP

Following the security principle of separation of duties, Actifio uses two command line (CLI) interfaces for customer end-users and Actifio support personnel. These are described in detail below.

User CLI Access

One CLI interface is for general user access and is only accessible by users defined in the Actifio appliance. This is accessible via an SSH based login via port 22 on either the primary cluster IP address or node IP addresses. All CLI access is via key based authentication only. This avoids the threat of brute force password attacks and social engineering of password theft.

A user must generate an SSH public key, and that public key must be installed on the user's account by an administrator before CLI access is granted.

The User CLI login allows authenticated users access to a heavily restricted shell where only Actifio-specific commands are available to be run. The full list of commands is documented in the Actifio Documentation Library available from the Actifio Resource Center on each Actifio appliance (http://<cluster-IP>). Users (including admin) have no ability to upload and execute arbitrary binaries, nor can users escape the restricted shell to escalate their privileges.

Support CLI Access

The second CLI interface is for use by Actifio Support only. The time and system-limited login certificates required to use this service can only be acquired via a secure portal. The username of the user who generated the SSH certificate is embedded within the certificate and all actions are audited with this information allowing all activity to be positively tied to a specific individual.

Any Actifio employees granted authorization to generate these access certificates is subject to rigorous scrutiny including a background check for every individual.

The nature of this access mechanism means it's both very secure and fully traceable making it easy to identify which individuals have logged in using the support credentials and what actions they have performed.

Console CLI Access

Access to the Actifio CLI is also available the console on the Actifio appliance. Use of this is restricted to Actifio staff who can leverage the key based login approach described above with the key loaded on a USB stick to gain a support login to the system.

Vulnerabilities with Actifio VDP

Actifio Engineering routinely monitors multiple sources for vulnerability information and makes available to all customers hotfixes to mitigate any discovered vulnerability in a component utilized by the appliance:

- Common Vulnerabilities and Exposures
- Security Focus - Vulnerabilities Search - http://www.securityfocus.com/bid
- National Vulnerabilities Database (NVD).

United Stated Government Usage

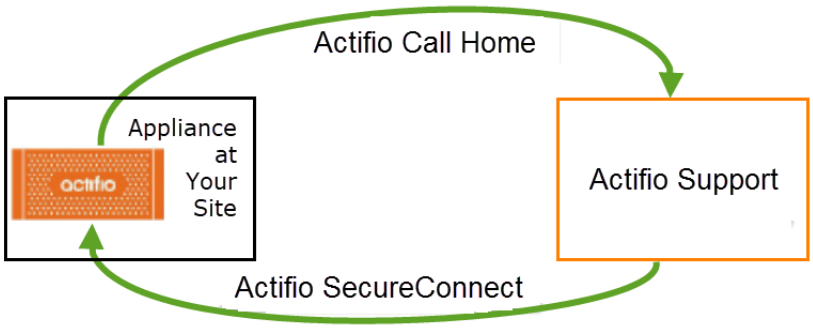
Actifio meets or exceeds a variety of NIST and FIPS standards required for deployment on United States Government networks and holds several agency Authority to Operate certifications. Actifio is compliant with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) when installed and hardened accordingly. Contact your Actifio Federal representative for more information on US Government deployment and security certifications.

Actifio Remote Support

Actifio offers two optional remote support features:

Call Home remote event notification: When you enable the Actifio Call Home feature, your Actifio appliance sends alerts and other diagnostic data to Actifio. Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you.
Actifio Call Home is detailed in Actifio Call Home Remote Event Notification.

SecureConnect remote service access: When you enable Actifio SecureConnect, Actifio Customer Support engineers can access your system remotely on an as-needed basis. As a situation requires, they can manage major upgrades and service pack updates and hotfixes, phase out failing hardware, collect log data on history of failures, restart data and I/O modules, change the configuration of ports, and more. All actions are documented in the Actifio appliance audit log and in the Actifio installation/problem reporting databases for further review. Actifio SecureConnect is detailed in Actifio SecureConnect on page 9.



Actifio Call Home and Actifio SecureConnect

Actifio Call Home Remote Event Notification

Actifio Call Home sends an email to Actifio Customer Support every six hours. In the event of a problem, Actifio Support can refer to this information to minimize time to recovery. The email includes these statistics:

- Actifio appliance version information
- Uptime of the Actifio appliance
- Status check of services
- Process summary
- Logs of various processes
- Failed jobs and total jobs
- Storage pool and deduplication statistics

Actifio Customer Support engineers monitor system alerts and conduct impact assessments. Based upon the alert level, the system may even initiate a problem resolution case and an associated escalation plan for you. Due to the redundant design of an Actifio appliance, most alerts do not require immediate service attention.

Can I Enable Call Home Without Enabling SecureConnect?

Yes. Call Home provides data, and SecureConnect provides access. Enabling Call Home without enabling SecureConnect ensures that Actifio Customer Support has excellent monitoring, alerting, and analytics data, without the access that might be needed to perform further diagnostics or remediation. The data lets Actifio Customer Support know when a problem has occurred and prepare a response if needed, but investigation and troubleshooting has to be performed via WebEx or conference call.

Most investigations require additional data to be gathered from the appliance, and without SecureConnect, the cycle of gather-analyze-followup-analyze can become cumbersome.

Call-Home Network Requirements

Actifio Call-Home requires a TCP connection on port 25.

Configuring Actifio Call Home

To send Actifio appliance statistics to Actifio Support every 6 hours, refer to the AGM online help, reachable from the **?** icon in the top right corner of the AGM.

Actifio SecureConnect

Actifio SecureConnect is a secure method for remote support that employs dedicated ports and encrypted data. These built-in security features greatly reduce the risks associated with a connection to an external network. The SecureConnect protocol allows Actifio Customer Support engineers to access your system on an as-needed basis to manage cases and updates while meeting your SLA requirements.

Your Actifio account team is kept up to date on a repair status as the case progresses. If hardware replacement is required, parts & local support are shipped to the site and an Actifio Services engineer is dispatched to handle the installation. When the incident is resolved to your satisfaction, the Actifio Customer Support engineer logs out of your Actifio appliance, disconnects from the remote access line, and creates a summary report of problem root cause and repair actions that is delivered to your account team and to you.

Advantages to using Actifio SecureConnect include:

- **Accelerated problem solving**: By leveraging Actifio follow-the-sun support, you can resolve problems without extending the wait time that invariably gets generated by relying on log files, dumps, and traces being transmitted across the globe.
- **Fine-grained monitoring and collaboration**: You can monitor remote support activities and join in conference calls with Actifio Customer Support engineers as the problem determination process proceeds.
- **Real-time learning**: Remote Actifio Customer Support engineers provide you with ongoing assistance in the setup, configuration, and management of your Actifio appliances.

Without SecureConnect enabled, you can still contact Actifio Customer Support. Actifio support engineers can work with you via WebEx and other remote support tools for log file gathering and other forensics to help resolve the issue.

Can I Enable SecureConnect Without Enabling Call Home?

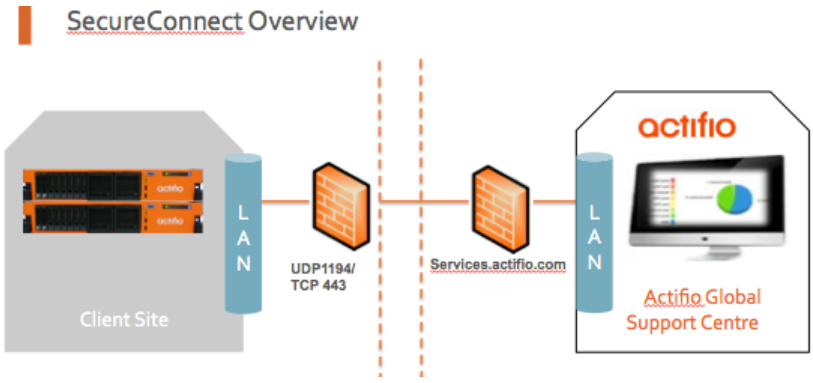
Yes. Call Home provides data, and SecureConnect provides access. Enabling SecureConnect without enabling Call Home allows Actifio Customer Support engineers to respond and investigate issues after you tell us a problem exists. Without Call Home, Actifio Customer Support has no way to know of problems with your system. There is no proactive data collection associated with activating SecureConnect.

How SecureConnect Works

SecureConnect uses client/server architecture. The SecureConnect client comes built into your Actifio appliances, to be enabled and disabled by you.

After you enable the connection through the Actifio Desktop, your Actifio appliance establishes a secure point-to-point connection to a secure server at the Actifio Global Support Center, enabling remote access from the Actifio Global Support Center to your Actifio appliance. You must configure a firewall rule to allow the Actifio appliance to connect to Actifio Support over UDP on port 1194.

As a client connection, SecureConnect does not bridge networks or perform any form of routing. Connections initiated at the Actifio Global Support Center communicate with your Actifio appliance and no other systems on your network.



How Secure Is Actifio SecureConnect?

SecureConnect utilizes 2048-bit RSA cryptography for strong mutual authentication and encryption, 256-bit AES for encryption of data in flight, and Diffie-Hellman for Perfect Forward Secrecy (PFS) key exchange. Each connection is a point-to-point link and none of your equipment can access another endpoint. Intrusion detection software continually monitors the connection for any anomalous activity. Authentication records are replicated in real-time to off-site locations. The SecureConnect servers are routinely monitored for emerging threats and vulnerabilities.

Only select users within the support and engineering organizations are authorized with this level of access. Actifio employees who have a business need to access your systems must pass a third-party background check and sign a security, compliance, and confidentiality agreement. Access is reviewed annually and terminated immediately in the event of separation or role change. Authorized employees authenticate to SecureConnect with a 2048-bit X.509 certificate stamped with the identity of the user. A two-factor challenge is required after cryptographic authentication in the form of a smart phone push or code-generating token. The certificate must be renewed annually. Issuance is logged to an audit log, and all activities on a system while logged in using the certificate are logged along with the identity of the user. The VPN connection is protected using NIST-approved strong cryptography including AES-256 data encryption.

No Access to Your Business Data

Appliance service credentials are completely independent from SecureConnect and are generated on entirely separate systems. To gain access to a customer system, an Actifio Support staff member generates a time-limited, passphrase-protected authentication token which is locked specifically to the machine they have been granted access to log into. The system generating these tokens is on a secure network separate from the SecureConnect network and itself authenticates against a robust corporate directory. The ability to generate authentication tokens is limited to Actifio Support staff members who have been approved by a rigorous screening process.

Actifio SecureConnect Network Requirements

Actifio SecureConnect is a strong 2048-bit RSA mutually authenticated service not subject to redirection or man-in-the-middle attacks. SecureConnect requires a UDP connection over port 1194 **from** the Actifio appliance IP address **to** secureconnect2.actifio.com and a setting of "any" IP address. If you cannot use 'any', then contact Actifio Support.

Actifio Appliance IP Address depends on the type of appliance:

Actifio Sky Appliance: the Actifio Appliance IP is the IP address of the Sky appliance.

Actifio CDX Appliance: the Actifio Appliance IP must include the IP addresses for both CDX nodes.

Actifio CDS Appliance: the Actifio Appliance IP must include the IP addresses for primary CDS node.

Enabling Actifio SecureConnect

To enable SecureConnect mode, refer to the AGM online help, reachable from the **?** icon in the top right corner of the AGM.