Tech Brief

Actifio Remote Support Options

Actifio offers two 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 2.

Actifio Call Home Remote Event Notification

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.

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

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 almost all possible 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.

Actifio SecureConnect

Security is a significant issue for companies of all sizes, particularly when it comes to applications and systems that manage corporate data. Each year, the risk of malicious activity from both external and internal sources continues to rise. Any connection from your corporate network to the public Internet raises valid security concerns.

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.

What if I Do Not Enable Actifio SecureConnect?

Without SecureConnect enabled, you can still contact Actifio Customer Support when you have a problem. The 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.

Tell Me More about Actifio SecureConnect

To learn more about Actifio SecureConnect, see:

How SecureConnect Works on page 3

How Secure Is Actifio SecureConnect? on page 4

How SecureConnect Works

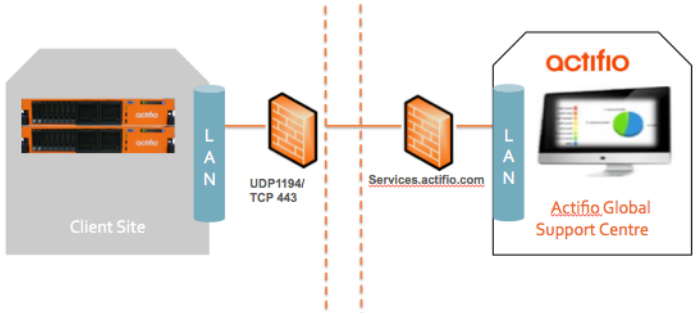
SecureConnect uses client/server architecture:

- The SecureConnect client comes built into your Actifio appliances, to be enabled/disabled by you
- The target server is in the Actifio Global Support Center in Waltham, Massachusetts, USA

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.

As a client connection, SecureConnect does not bridge networks or perform any form of routing. Connections initiated at the Actifio Global Support Center can communicate only with your Actifio appliance, not with other systems on your network.

You must configure a firewall rule to allow the Actifio appliance to connect to secureconnect2.actifio.com over UDP on port 1194.



SecureConnect Overview

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 configured as a point-to-point link and none of your equipment can access another endpoint. Additionally, a two-factor challenge is required after cryptographic authentication in the form of a smart phone push or code-generating token. Intrusion detection software continually monitors the connection for any anomalous activity and authentication records are replicated in real-time to off-site locations. The SecureConnect servers are routinely monitored for emerging threats and vulnerabilities.

How Secure Is Actifio SecureConnect?

Actifio Appliances run on a hardened Linux software stack. Linux user accounts and root access are not required nor employed for normal operations and support of these systems. In the rare cases where root access is required, there is no console root access and root login can be obtained using an SSH key pair with a certificate signed by Actifio. These certificates are only issued with a short (1 to 7 day) expiration, and each is tied to a specific Actifio appliance.

Only select users within the support and engineering organizations are authorized with this highest level of access and all undergo background checks. 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 personal 2048-bit X.509 certificate that expires and must be renewed annually.

Certificates are stamped with the identity of the user to whom they are issued. The 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.

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 must first generate a time limited, pass-phrase protected authentication token which is locked specifically to the machine they have requested and been granted access to login to. 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 these authentication tokens is limited to Actifio Support staff members who have been approved by a rigorous screening process.

The VPN connection is protected using NIST-approved strong cryptography including AES-256 data encryption. Authorized Actifio employees must possess a signed cryptographic certificate and private key as well as prove their identity using an out-of-band second factor (two-factor login).

No Access to Your Business Data

Actifio personnel who access an Actifio appliance do not have the ability to access customer business data. In order to access this data, an application image or volume needs to be presented to a host using the relevant credentials, which are not available to the support personnel.