Documentation

Acquia Cloud

- What's new - Acquia Cloud
- Getting started with Acquia Cloud
- Getting started with Acquia Cloud Free

Acquia Cloud architecture and key concepts

- Acquia Cloud technology platform and supported software
- Key concepts in Acquia Cloud
- Comparing Acquia Cloud Professional and Acquia Cloud Enterprise
- Security and compliance
- Using multi-region failover
- Using Acquia Cloud Edge Powered by CloudFlare

Using Acquia Cloud Shield

- Managing websites with Acquia Cloud
- Creating a new site on Acquia Cloud
- Developing websites on Acquia Cloud
- Improving website performance
- Known issues in Acquia Cloud

Acquia Cloud Site Factory

Acquia Dev Desktop 2

Acquia Lift

Acquia Platform APIs
Using Acquia Cloud Shield

Using Acquia Cloud Shield, your Acquia Cloud Enterprise websites run in a dedicated, logically isolated section of Acquia Cloud, adding more network level security and capabilities to the stack. Acquia Cloud Shield is available as an additional service to Acquia Cloud Enterprise subscriptions.

Benefits of using Acquia Cloud Shield

Acquia Cloud Shield gives you the benefits of Acquia Cloud platform-as-a-service, combined with extra security benefits and capabilities. Acquia Cloud Shield provides a higher degree of isolation for your Acquia Cloud instances in the cloud. With Acquia Cloud Shield, your Acquia Cloud instances exist in a dedicated, logically isolated section that is not shared with any other users.

Optionally, you can use Acquia Cloud Shield with a VPN, which provides a secure bidirectional connection between your Acquia Cloud Enterprise websites and your internal IT systems. In this case, instances within the dedicated cloud section can be accessed only by other instances within the same dedicated cloud section, or else over a secure internet gateway (VPN).

If you use Acquia Search, note that your search installation can be accessed from your Acquia Cloud Shield websites, but the Acquia Search servers will not be located within your Acquia Cloud Shield dedicated section. Therefore, your search index will not be covered by Acquia Cloud Shield.

Getting started with Acquia Cloud Shield

To use Acquia Cloud Shield, simply purchase Acquia Cloud Shield with your Acquia Cloud
Enterprise subscription. Acquia then provisions your servers within your dedicated cloud section.

**Getting started with Acquia Cloud Shield with VPN**

To use Acquia Cloud Shield with VPN, you must have an Acquia Cloud Enterprise subscription and must have purchased Acquia Cloud Shield. The following are the main steps in setting up Acquia Cloud Shield with VPN:

1. You purchase and deploy a VPN device. See [VPN device requirements](#).
2. You provide Acquia with detailed information about your VPN device and your network. See [Network information](#).
3. Acquia provisions and configures a dedicated cloud section for your websites.
4. Acquia provides you with the IPSec (Internet Protocol Security) /IKE (Internet Key Exchange) information you need to properly configure your VPN.

**Network information you provide to Acquia**

In order for Acquia to configure Acquia Cloud Shield with VPN, you need to provide Acquia with the following information:

1. Contact information (name, phone, and email) for the members of your internal network team.
2. VPN device details:
   - VPN device type (vendor and model)
   - The Gateway IP address of the customer VPN device
   Confirm that your VPN device meets the requirements described in [VPN device requirements](#).
3. Network details, including:
   - A network diagram, showing which systems Acquia Cloud Shield will connect to
   - Maintenance plan or schedule for these services
   - CIDR IP blocks
   - Subnet allocations
   - A list of networks that need traffic statically routed to them
4. A private non-routable /16 or /20 private address space for Acquia Cloud Shield.
5. A name for the Acquia VPN. This is optional. However, if you have multiple VPNs, providing a name to Acquia may be useful for later communication.

Contact your Acquia account manager for more information.
VPN device requirements

In order to connect to Acquia Cloud Shield with VPN, your network must use a VPN, a secure Internet gateway, that uses IPsec. Your VPN device must be capable of each of the following:

- Establish IKE Security Associations using pre-shared keys
- Establish IPsec Security Associations in Tunnel mode
- Use the AES 128-bit encryption function
- Use the SHA-1 hashing function
- Use Diffie-Hellman Perfect Forward Secrecy in "Group 2" mode
- Perform packet fragmentation prior to encryption

The following gateway devices are compatible with Acquia Cloud Shield with VPN.

- Cisco ASA 5500 Series version 8.2 (or later) software
- Cisco ISR running Cisco IOS 12.4 (or later) software
- Dell SonicWALL Next Generation Firewalls (TZ, NSA, SuperMassive Series) running SonicOS5.8 (or later)
- Juniper J-Series Service Router running JunOS 9.5 (or later) software
- Juniper SRX-Series Services Gateway running JunOS 9.5 (or later) software
- Juniper SSG running ScreenOS 6.1, or 6.2 (or later) software
- Juniper ISG running ScreenOS 6.1, or 6.2 (or later) software
- Microsoft Windows Server 2008 R2 (or later) software
- Yamaha RTX1200 router

Your network’s gateway must be properly configured to connect to Acquia Cloud Shield with VPN. Once your dedicated cloud section is provisioned, Acquia will provide you with the IPSec/IKE information you need to properly configure your VPN.

WAS THIS HELPFUL?