# Security Considerations

https://campus.barracuda.com/doc/78156761/

This article includes a number of recommendations to help you prevent potential security issues and reduce the risk of compromising sensitive data in your organization.

When deploying Backup appliances for site-to-site replication, you need to ensure the physical security of these systems. Configure Barracuda Backup appliances behind corporate firewalls with appropriate restrictions in place. All data transmitted between Barracuda Backup appliances is sent encrypted using 256-bit AES.

For additional security measures, customers may choose to set up a private VPN tunnel between sites, however this is not a requirement.

## Securing Your Barracuda Backup Device

A potential source of vulnerability is the backup device itself. To secure data stored on your backup devices, consider the following recommendations:

- Ensure physical security of the Barracuda Backup devices. Check that only authorized personnel have access to the room where your devices reside.
- Restrict user access to Barracuda Backup devices. Check that only authorized users have permissions to access certain backup devices and data.

## Data Communication Channel

The Barracuda Backup device is deployed behind your corporate firewall, and is protected by the same security as your primary data sources.

#### Communication and Configuration

Administration and backup configuration that is set using the Barracuda Backup web interface is sent to the Barracuda Backup device via a 256-bit encrypted VPN tunnel. The Barracuda Backup device uses HTTPS port 1194 to send status updates to Barracuda Backup. Data transfers are initiated by the Barracuda Backup device rather than by Barracuda Cloud Storage or a remote Barracuda Backup devices.

#### Data Transmission and Storage

Data transfers from the local Barracuda Backup device to a receiving Barracuda Backup device are always encrypted. Data is stored compressed and encrypted at rest on the receiving Barracuda Backup device; the local Barracuda Backup device data stored on the local appliance is encrypted at-rest using AES 256-bit encryption. Barracuda Backup utilizes an aggressive combination of symmetrical and asymmetrical encryption. The United States government recently approved 192-bit AES encryption as the preferred method for protecting top-secret information. The Barracuda Backup solution starts with even higher 256-bit AES encryption. In addition, Barracuda Networks has developed a proprietary advanced digital cataloging system that breaks down your data into small pieces and tracks the changes of these parts over time, and strips the original meta identifiers from your files.

As data is transmitted to the remote Barracuda Backup device, your symmetrically-encrypted data parts are compressed and sent over your Internet connection with an asymmetrically-encrypted key.

## Integration with External Systems and Services - Security Considerations

Barracuda Backup integrates with other systems and services in your environment, like your authorization server and email system. Barracuda Networks recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy. For more information, see Security for Integrating with Other Systems - Best Practices.

## Access and Privileges

Restrict user access to Barracuda Backup devices. Check that only authorized users have permissions to access certain backup devices and data.

#### Monitor Activity

You can check user activity in two locations:

- The Barracuda Cloud Control Audit Log by clicking on the Home bar on the left-hand side and then the **Audit Log** page. Here you can see authentication attempts, changes to settings, and updates to account information.
- For user activity specific to a Barracuda Backup device, see the Audit Log under the Reports tab of your Barracuda Backup device.

#### Restrict Privileges

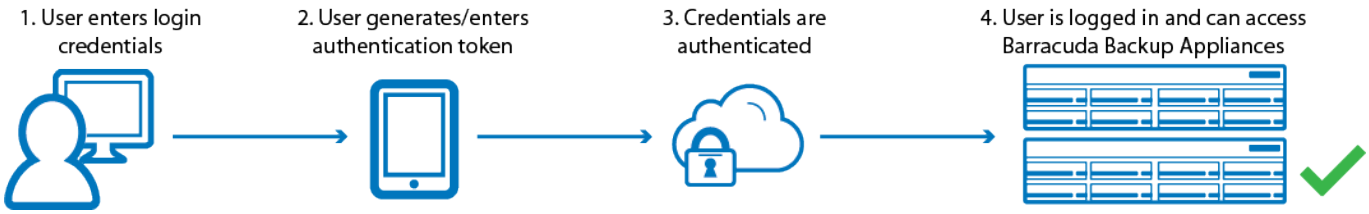
Use the **Admin > Users** page to administer the privileges that users have within the Barracuda Backup web interface.

#### Restrict Logins by IP Address

You can restrict access to Barracuda Backup to one or more IP addresses. On the Admin > Users page, click Edit to edit a user account; enter an IP address or a range.

#### Multi-Factor Authentication

Multi-factor authentication (MFA), also known as two-factor authentication, is a security feature that requires two forms of authentication to access Barracuda Backup. When enabled, MFA provides an extra layer of security to your account:




Even if a user's login credentials are stolen, without the trusted device, an attacker cannot access the account. If a user's device is taken, the attacker cannot access the account without the login credentials.

MFA is optional by default, allowing the account administrator to determine whether to enable MFA. When enabled, users must download and install Google Authenticator or Duo Mobile authentication tool to their mobile device to log in to Barracuda Backup using MFA. These free authentication tools are available for download from iTunes and the Google Play Store.

For details, see Multi-Factor Authentication in Barracuda Cloud Control.

## Barracuda Backup Appliance Security - Hardware and Virtual

Barracuda Backup appliances are typically deployed as cloud-connected appliances, enabling customers to remotely manage their Barracuda Backup appliances from a web browser without requiring a physical connection to the appliance. The Barracuda Backup Appliance is typically deployed behind the customer's corporate firewall and is protected by the same security that the customer uses to protect primary data sources. Communication between the appliance and Barracuda Cloud utilizes a 256-bit encrypted VPN tunnel for administration and backup configuration, and a "lifeline" status check that runs over https port 443, which provides details of the server status in the

event the tunnel is down.

There are several ways the Barracuda Backup Appliance can be accessed locally:

- The local web interface provides access for basic system maintenance, and as of Barracuda Backup firmware version 5.0, also provides Restore and Reporting functionality.
- A monitor and keyboard provide access to the terminal configuration for network setup and troubleshooting. Command-line access to the unit is disabled locally.

The Barracuda Backup Appliance runs on a hardened Linux kernel. In the event that a security flaw is discovered, updates are pushed out to cloud-connected Backup Servers in a security definition administered by Barracuda.

Starting with Barracuda Backup firmware version 6.0, customers have the option to deploy Barracuda Backup appliances in Local Control mode. In this mode, the Barracuda Backup appliances require connection to the Barracuda Cloud only during the initial appliance configuration.

## Barracuda Backup Access Controls

Barracuda Backup provides the following features to give customers additional flexibility to limit access to their Barracuda Backup appliance and account when operating in cloud-connected mode:

- IP login restrictions can be set for each user who has access to the Barracuda Backup account. Those restrictions prevent access to the hosted web user interface from an IP address outside the range specified.
- Customers use the Barracuda Cloud Control interface to access and manage their Barracuda Backup appliances. The Barracuda Cloud Control supports Multi-factor Authentication. See Multi-Factor Authentication in Barracuda Cloud Control for more information.
- By request, Barracuda can enable an advanced option in the web user interface which gives customers the ability to grant or deny Technical Support remote access to a backup server. This will prevent access to both the command line and to the user interface. This tool does not lock out the Barracuda Cloud engineering team.

## Data Transmission and Storage

In order to perform deduplication, Barracuda Backup breaks files down into parts that are variable in size and fingerprints those parts for analysis and comparison. Before transmission to the Barracuda Cloud or a secondary Barracuda Backup appliance, those parts are AES 256-bit symmetrically encrypted and AES keys are securely transmitted. These parts are written into storage at the Barracuda Cloud or a secondary Barracuda Backup appliance in an encrypted state and remain

encrypted until requested for restore. When replication is active, the process of replicating data begins immediately after data is written to disk on a Barracuda Backup appliance and runs continuously.

## Data Location

Barracuda maintains a network of cloud-scale datacenters by geographic location around the globe, and requires that each meets defined security requirements. The cloud infrastructure for Barracuda Backup is deployed in the following geographical regions:

- United States of America: infrastructure deploys in this region stores data for all customers in the United States as well as any region not specifically configured to send data to an available local location
- United Kingdom: stores data for all customers in the United Kingdom, Europe, Middle East, and Africa
- Canada: stores data for all customers in Canada
- Germany: stores data for all customers in Germany, Austria, Belgium, Netherlands, and Luxembourg
- Australia: stores data for all customers in Australia
- Japan: stores data for all customers in Japan

## Figures