AOS

Configuring SSH Public Key Authentication

Basic Configuration Guide

October 2018

6AOSCG0060-29B

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Revision History

Rev B	October 2018	Initial release of document in this format. Document updated to include added support for SSH security algorithms and ciphers that were introduced in AOS firmware R13.4.0 release.

Table of Contents

List of Tables

1 Overview

This guide describes how to configure and use Secure Shell (SSH) public key authentication on products running the ADTRAN Operating System (AOS). This guide provides instructions using the AOS command line interface (CLI).

1.1 Intended Audience

The intended audience for this information is the network administrator using ADTRAN AOS products. The instructions assume familiarity with the intended use of the equipment, basic required installation and configuration skills, and knowledge of local and accepted networking practices.

1.2 Document Structure

Table 1 lists the topics contained in this document.

Table 1. Topic List

Section	Topic	See Page…
1	Overview	7
2	Overview of SSH Public Key Authentication	10
3	Hardware and Software Requirements and Limitations	11
4	Configuring SSH Public Key Authentication	12
5	Troubleshooting	16
6	Warranty and Contact Information	19

1.3 Hazard and Conventional Symbols

The following Hazard symbols are used throughout this guide:

⚠ **WARNING!**
Warning: Service affecting. Possible risk of system failure.

⚠ **CAUTION!**
Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.

❗ ***NOTICE!***
Notice: Provides information that is essential to the completion of a task.

ℹ **NOTE**
Note: Information that emphasizes or supplements important points of the main text.

1.4 Related Online Documents and Resources

Refer to Table 2 for additional information for this product.

Documentation for ADTRAN AOS products is available for viewing and download directly from the ADTRAN Support Community website.

Go to: https://supportforums.adtran.com

Table 2. Related Online Documents and Resources

Title	Part Number	Description
SSH Public Key Authentication Related Documents and Resources		
Upgrading AOS Firmware	61200990L1-29	This guide contains steps on how to update the firmware of an AOS device.
Configuring SSH Port Forwarding for Remote AOS Device Management	6AOSCG0067-29	This document describes how to configure SSH port forwarding for remote device management in AOS using the CLI.
AOS Command Reference Guide	6000CRG0-35	This guide contains descriptions of all commands that pertain to AOS products. Content is listed in an easy to reference format.

2 Overview of SSH Public Key Authentication

When using SSH to communicate with an AOS device, key-based authentication provides additional security over simple password authentication. Key-based authentication uses asymmetric encryption for secure communication between a computer (the SSH client) and an AOS device (the SSH server). Asymmetric encryption relies on two components: a private key and a public key. With key-based authentication, the public key is used to encrypt transmitted data in a way that it can be decrypted only by the private key paired with that public key. Each user who will log in to an AOS device using key-based authentication needs to generate a public/private key pair on the computer connecting to the AOS device. For more information about generating public/private key pairs for individual users, refer to Step 1. Generating User Public/ Private Key Pairs on a Linux Computer on page 12. A user's private key should not be shared with anyone. However, each user's public key will need to be installed on the AOS device (refer to Step 5. Installing User Public Keys on an AOS Device on page 14 for more information).

Each AOS device generates its own public/private key pair when the device boots for the first time. New DSA keys can be generated on an AOS device using the **ssh key regenerate** command.

NOTE
AOS products support authentication with Digital Signature Algorithm (DSA) keys. By default, DSA keys are 1024 bits. However, keys up to 2048 bits are supported. To generate 2048-bit DSA keys, you will need to use a third-party application such as PuTTYgen.

3 Hardware and Software Requirements and Limitations

SSH public key authentication with AOS products requires the following:

- SSH client supports SSH-2 public key authentication.
- AOS product is running firmware version R10.10.0 or later. (Refer to Step 3. Checking the Firmware Version on the AOS Device on page 13.)
- SSH is enabled and public key authentication is enabled. (Refer to Step 4. Verifying that SSH is Enabled on page 14.)

In AOS firmware release R13.4.0, support for the following SSH security algorithms and ciphers was added to AOS products:

- diffie-hellman-group14-sha1 KEX algorithm
- hmac-sha2-256 HMAC algorithm
- aes128-ctr cipher
- aes256-ctr cipher

4 Configuring SSH Public Key Authentication

Since SSH Public Key Authentication is used between a computer and the AOS device, both units will require configuration. You will configure the computer to generate public/private key pairs and then install the public key in the AOS device. Prior to installing the public keys, verify that the AOS device is running the minimum required firmware version R10.10.0 or later and that SSH is enabled.

NOTE

This guide assumes that the computer used to connect to the AOS device is running the Linux Operating System. If you are using a non-Linux computer to connect to the AOS device, refer to the documentation for the SSH client being used for information on generating key pairs.

4.1 Step 1. Generating User Public/Private Key Pairs on a Linux Computer

To use SSH key authentication, you must create private and public keys for each user on the computer used to connect to the AOS device.

1. If your home directory does not have the .ssh folder, create this folder:

   ```
   $mkdir .ssh
   ```

2. Generate the DSA public/private key pair in the .ssh directory:

   ```
   $ssh-keygen -t dsa
   Generating public/private dsa key pair.
   ```

3. When prompted to enter a file in which to save the key, enter a file name or press **Enter** to accept the default name **id_dsa**:

   ```
   Enter file in which to save the key (/home/user/.ssh/id_dsa):
   ```

4. When prompted to enter a passphrase, enter the passphrase or press **Enter** for no passphrase:

   ```
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /home/user/.ssh/id_dsa.
   Your public key has been saved in /home/user/.ssh/id_dsa.pub.
   The key fingerprint is:
   78:95:0a:f8:85:67:a3:91:27:f8:b3:10:ed:46:7e:3c user@host
   ```

5. The private key is created in the file indicated in Step 1. This file is located in the .ssh directory and should be readable only by the user. Verify the file permissions on the private key file:

   ```
   $ls -l ~/.ssh/id_dsa
   ```

   ```
   -rw------- 1 user user 668 Oct 18 01:52 id_dsa
   ```

   If the permissions do not match those listed above, modify the permissions to **600** using the **chmod** command:

   ```
   $chmod 600 ~/.ssh/id_dsa
   ```

   The private key is created in the file name used in Step 1 followed by a **.pub** extension (for example, **id_dsa.pub)**.

6. Display the public key file using the **cat** <*filename*> command, for example:

   ```
   $cat ~/.ssh/id_dsa.pub
   ```

   ```
   ssh-dss AAAAB3NzaC1yc2EAAAADAQABAAABAQDMtHG9jIGE3CV8/
   3nAJwyn9tZCwL5Y0TXlpebGnvZV
   C84efqjmbOANpadLqcOMRoP6FANkOIXcfPA0SohBEg8sxAKLK7CzIiZxQ8g/
   HKNYuj5FnRGTGq+CUb8d
   42caAggs5YNfSFbLbuVAmXIRo2HRXdqrQOgSKxxr5z73CHDTuSlKfND/
   DnmHGV7LFBfCkUVDpO3+kWTx
   RMk8o3Sjg8qysDlANpZIGMGrSKkYudjvH3BJs5bBjpW0NB97z3lBDRd4LUBwuSQJ
   DiKnL9Xhmv+DkzQZ
   GDW9LKUymvn8MYJ06H4Oqxz49NPYug84ptfTx0LbpT+PSLsZ+GPbcl23AF3f
   user@host
   ```

7. Copy the displayed key string output into your buffer. Be sure to include the entire key beginning with **ssh-dss** and ending with the host name.

4.2 Step 2. Connecting to the CLI

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>). For example:

   ```
   telnet 10.10.10.1
   ```

NOTE

The default IP address is 10.10.10.1. If this address was changed during the unit's setup process, use the configured IP address.

3. Enter your user name and password at the prompt.

NOTE

The AOS default user name is **admin** and the default password is **password**. If the device no longer has the default user name and password, contact your system administrator for the appropriate user name and password.

4. Access Enable mode by entering **enable** at the prompt as follows:

   ```
   >enable
   ```

   ```
   #
   ```

5. If configured, enter the Enable mode password at the prompt.
6. Access Global Configuration by entering the configure terminal command as follows:

   ```
   #configure terminal
   (config)#
   ```

4.3 Step 3. Checking the Firmware Version on the AOS Device

The steps outlined in this guide are compatible with AOS products running firmware version R10.10.0 or later.

NOTE
Support for 2048-bit keys began with AOS firmware version R10.11.0.

To check the firmware version:

1. Log in to the CLI. (Refer to Step 2. Connecting to the CLI on page 13 for more information.)
2. From Enable mode, enter the **show version** command to display the firmware version:

```
>enable
#show version
ADTRAN, Inc. OS version R10.11.0.
```

4.4 Step 4. Verifying that SSH is Enabled

By default, the SSH port and public key authentication are enabled. Verify that SSH is enabled using the **show running-config** command from the Enable mode:

```
#show running-config | begin line ssh
line ssh 0 4
  login local-userlist
  no shutdown
```

NOTE
Using the **| begin line ssh** option of the **show running-config** command starts the output at the SSH line configuration information.

Use the following to verify that SSH public key authentication is enabled:

```
#show running-config | include ssh-server authentication
ssh-server authentication password pubkey
```

NOTE
Using the **| include ssh-server authentication** option of the **show running-config** command limits the output to the SSH server authentication information.

If the SSH server is not enabled, use the **no shutdown** command from Line SSH Interface mode to enable it:

```
#configure terminal
(config)#line ssh 0 4
(config-ssh0-4)#no shutdown
```

If public key authentication has been disabled, use the **ssh-server authentication password pubkey** command from Global Configuration mode to enable it:

```
#configure terminal
(config)#ssh-server authentication password pubkey
```

4.5 Step 5. Installing User Public Keys on an AOS Device

The public key for each user who logs in to an AOS device using public key authentication must be installed on the AOS device. In the following steps, you will use the key information copied in Step 7 on page 13.

1. Enter the public key input mode:

```
(config)#ssh-server pubkey-chain
(config-pubkey-chain)#
```

2. Add the user name and key string using the **username** <*username*> **key-string** command, where <*username*> indicates the user name installing the public key:

```
(config-pubkey-chain)# username <username> key-string
```

3. After you press **Enter**, the system will prompt you for the key:

```
Enter user’s public key (DSS). End with two consecutive
carriage returns or the word “quit” on a line by itself:
```

4. Paste the public key copied in Step 7 on page 13.
5. Make sure to save the configuration file changes:

```
(config-pubkey-chain)#do write
```

4.6 Step 6. Logging in from the Linux Client

To log in to an AOS device using public key authentication, use the **ssh** <*username*>**@**<*IP address*> command, where <*username*> is the user name used to log in and <*IP address*> is the IP address of the AOS device. In the following example, user **fjones** is logging in to an AOS device with the IP address of **10.10.10.1**:

```
$ssh fjones@10.10.10.1
```

NOTE
If you are using a non-Linux computer to connect to an AOS device, refer to the documentation for the SSH client you are using for information on using public key authentication with that application.

5 Troubleshooting

AOS troubleshooting commands for SSH public key authentication are shown in Table 3.

Table 3. AOS SSH Public Key Authentication Troubleshooting Commands

Command	Description
show ssh-server	Displays the AOS device's public key for SSH connections. This command can use the following keywords: **key-hash** - Displays the SHA-1 key hash of a given key string. **mypubkey** - Displays the key string for the public key. **mypubkey fingerprint md5** - Displays the public key's MD5 fingerprint. **mypubkey fingerprint sha1** - Displays the public key's SHA-1 fingerprint.
debug ssh	Displays debug messages associated with SSH client and server information. This command can use the following keywords: **client events** - Displays SSH client events. **client scp** - Displays SSH client Secure Copy (SCP) information. **server events** - Displays SSH and SCP server events.
ssh key regenerate	Generates a new key pair on the AOS device for SSH connections.

NOTE
The output of all **show** commands can be limited by appending the following modifiers to the end of the command: **| begin** *<text>*, **| exclude** *<text>*, and **| include** *<text>*. The include modifier limits output to lines that contain the specified text, the **exclude** modifier excludes any lines with the specified text, and the **begin** modifier displays the first line of output with the specified text and all lines thereafter.

NOTE
Turning on a large amount of debug information can adversely affect the performance of your device.

5.1 Using the show ssh-server Command

Use the **show ssh-server** command to display information about the AOS device's public key for SSH connections or the hash of a user-provided SSH key. This command can use the keywords **mypubkey fingerprint md5** or **mypubkey fingerprint sha1** to display the fingerprint of the SSH server public key.

NOTE
If necessary, the key file can be regenerated using the **ssh key regenerate** command.

Used with the **key-hash** keyword, the command displays the SHA-1 key hash of a user-provided SSH key:

```
#show ssh-server key-hash
Please enter the public key (DSS) to see the resulting SHA1 Hash.
End with two consecutitve carriage returns or the word “quit” on
a line by itself:
```

Used with the **mypubkey** keyword, the command displays the key string for the public key:

```
#show ssh-server mypubkey
```

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: Adtran DSA Public key
AAAAB3NzaC1kc3MAAAEBALq7iC0mltbBGo2EzQ3ZDekHl3t2DLa08mP1AxrDdZdl
0HPTjHbVWrLOFnd3Om2yv8LXrKIKnlM0GhMlAB6ZcDjQjyr8s/Ey9fLZmxBdYKt3
8GP0OFLk2zEeYRv6XzFIYAu1sbcfmTU18SV+9m3X+TkhKvP/1jKYSSwDRyNDYTWJ
9Ap+HLRY09tLIvn9cL9mwDCG1rNSlsZ+y0uuYGOwGECLfCxuPc9gZbtMzdd6URqz
tze37XZTBOKyvz2AQrjRux9LNp13DZOB+R1SzNw2fhbPxalzeOXVVLxA7Gvty3YX
8PtyDfxu8KOqNIUVkhXxFf3OJMSyoXSCKC6GPIgxQSkAAAAVANrLmgntjpU7H2Ln
4jFsjjRekvP1AAABAGc4rfqF1ivIJ+AZlRlYRmtjk47zoZ2AU7alotVnaM8jK+U7
qJOWccGZeIUl69Y7xOZ9H3QG0W+LD4bpERJVCrUQxWWxdITOIphAM/OIeIcE1czW
tDUemFoAeg503n9rQuvNiSQ5+qhVsGWC9zhdo4AAZ2Crw/Epn54K778rpDjvzxcW
sesX7Vp3tsXHbZ6RGxdqFCJHytY0xNj033RaKSeAq4aZwbUMCYmrb1iS1hl1CHYM
b1kTsd7MYZQQ12e5UvVPySSNrN1R4ocDQy5qDi/UC5HfKe5MdLp5tM9ZWAjipDGk
3XjKO6UKMPT9cPa6iZ1fUXgwnam7xOSwtFU1HiEAAAEADaeYe3fHOR0RvqAO3aV1
ZNXg7DxdioKJDdzuqS0v1D+LHS8rMHdzvcFCgjStrpj4HJQIFuxaOTmoflSu8DBc
z7oLUVxoFsRoWVHq6HmAupAD0wmw/5VxswYKVrru/kxkZyyD6EgOOR5cFXSDJ4ZQ
AYfo+Q4lNPLiUXDhEV6ZOH5PNaZTlMpca/iTGdrDoaZ3G6IcpxTmyu+mevQBp+H+
ij+0dDaHzfUKNb9aq2CVBiFihWojo6Ll2SnqN99j2PyKOwCXYUNtMQ1dt3S+hoM5
rfE6RRw52SU8FlI7j4cYEHG7dh8SfRbWX78T3s6mRLSRp4q75JCzPa74+nfty4Jc
gA==
---- END SSH2 PUBLIC KEY ----
```

Used with the **fingerprint md5** keyword, the command displays the Message Digest 5 (MD5) fingerprint of the SSH server public key:

```
#show ssh-server mypubkey fingerprint md5
```

```
25:d4:36:52:8f:ca:b0:31:b0:6f:95:49:37:b1:f0:c6
```

5.2 Using the debug ssh Command

Use the **debug ssh** command to activate debug messages associated with SSH client and server information. Debug messages display in real time on the terminal screen. Use the **no** form of this command to disable debug messages. The **debug ssh** command can use the following keywords to activate display of their respective events: **client events**, **client scp**, and **server events.**

NOTE
Turning on a large amount of debug information can adversely affect the performance of your system.

5.3 Common Problems

I regenerated the public key on my AOS device and now I can’t connect using my SSH client.

If the AOS key has been regenerated, you may need to update the known host file (**known_hosts)** located in the .ssh directory on the SSH client. The known host file contains a list of all of the servers the client has connected to previously. Some SSH clients do not prompt to update this file with updated host information when establishing a connection. In these cases, you will need do one of the following:

- Edit the known host file and remove the old server information.
- If the known host file contains no other needed host information, delete the file and let the system generate a new one with the updated information.

I see the full key body on my client, but the AOS server only displays the SHA-1 hash of the key for a user. How can I know if the key on my server matches the one on my client?

Use the **show ssh-server key-hash** command to input the key from your client. This utility will display the SHA-1 hash for a given key and will also tell you if it matches any configured users on the system.

6 Warranty and Contact Information

6.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

6.2 Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S.	1.888.4ADTRAN (1.888.423.8726)
	From outside the U.S.	+ 1.256.963.8716
	Technical Support:	
	■ Web:	www.adtran.com/support
	Training:	
	■ Email:	training@adtran.com
	■ Web:	www.adtran.com/training
		www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807