Forward audit logs to syslog/splunk servers

REST API reference

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-96/forward_audit_logs_to_syslog/splunk_servers.html on February 11, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Forward audit logs to syslog/splunk servers . . . 1
Defines remote syslog/splunk server for sending audit information . . . 1
Learn more . . . 1
Parameters . . . 1
Response . . . 2
Error . . . 3
Definitions . . . 4
Configures remote syslog/splunk server information . . . 6
Required properties . . . 6
Optional properties . . . 6
Learn more . . . 7
Parameters . . . 7
Request Body . . . 7
Response . . . 8
Error . . . 9
Definitions . . . 10
Deletes remote syslog/splunk server information . . . 12
Learn more . . . 12
Parameters . . . 12
Response . . . 12
Error . . . 13
Definitions . . . 13
security_log_forwarding_get: Defines remote syslog/splunk server for sending audit information . . . 14
Learn more . . . 14
Parameters . . . 14
Response . . . 15
Error . . . 16
Definitions . . . 16
Updates remote syslog/splunk server information . . . 17
Learn more . . . 17
Parameters . . . 17
Request Body . . . 18
Response . . . 18
Error . . . 19
Definitions . . . 20

Forward audit logs to syslog/splunk servers

Defines remote syslog/splunk server for sending audit information

learn more

- [`doc /security/audit/destinations`](#docs-security-security_audit_destinations)

GET `/security/audit/destinations`

Defines remote syslog/splunk server for sending audit information

Learn more

- DOC /security/audit/destinations

Parameters

Name	Type	In	Required	Description
port	integer	query	False	Filter by port
protocol	string	query	False	Filter by protocol
facility	string	query	False	Filter by facility
address	string	query	False	Filter by address
verify_server	boolean	query	False	Filter by verify_server
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[security_audit_log_forward]	

Example response


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "address": "string",
      "facility": "string",
      "protocol": "string"
    }
  ]
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

security_audit_log_forward

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
port	integer	Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514.
protocol	string	Log forwarding protocol
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Configures remote syslog/splunk server information

required properties

all of the following fields are required for creating a remote syslog/splunk destination * `address` # optional properties all of the following fields are optional for creating a remote syslog/splunk destination * `port` * `protocol` * `facility` * `verify_server` (can only be "true" when protocol is "tcp_encrypted")

learn more

- [`doc /security/audit/destinations`](#docs-security-security_audit_destinations)

POST `/security/audit/destinations`

Configures remote syslog/splunk server information.

Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- `address`

Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- `port`
- `protocol`

- `facility`
- `verify_server` (Can only be "true" when protocol is "tcp_encrypted")

Learn more

- DOC /security/audit/destinations

Parameters

Name	Type	In	Required	Description
force	boolean	query	False	Skip the Connectivity Test • Default value:

Request Body

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
port	integer	Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514.
protocol	string	Log forwarding protocol
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

Example request

```
{
  "address": "string",
  "facility": "string",
  "protocol": "string"
}
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[security_audit_log_forward]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "address": "string",
      "facility": "string",
      "protocol": "string"
    }
  ]
}
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
15661	The object specified could not be found
13114	Internal error
13115	Invalid input
4522285	Server verification cannot be enabled because it requires a protocol with encryption. Encryption can be selected using the protocol field.
9240603	Cannot ping destination host. Verify connectivity to desired host or skip the connectivity check with the -force parameter.
327698	Failed to create rpc client to destination host
9240609	Cannot connect to destination host.
9240604	Cannot resolve the destination host.

Name	Type	Description
error	error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

security_audit_log_forward

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
port	integer	Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514.
protocol	string	Log forwarding protocol
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Deletes remote syslog/splunk server information

learn more

- [doc /security/audit/destinations](#docs-security-security_audit_destinations)

DELETE /security/audit/destinations/{address}/{port}

Deletes remote syslog/splunk server information.

Learn more

- DOC /security/audit/destinations

Parameters

Name	Type	In	Required	Description
address	string	path	True	
port	integer	path	True	

Response

```
Status: 200, Ok
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

security_log_forwarding_get: Defines remote syslog/splunk server for sending audit information

learn more

- [`doc /security/audit/destinations`](#docs-security-security_audit_destinations)

GET `/security/audit/destinations/{address}/{port}`

Defines remote syslog/splunk server for sending audit information.

Learn more

- DOC /security/audit/destinations

Parameters

Name	Type	In	Required	Description
address	string	path	True	IP address of remote syslog/splunk server

Name	Type	In	Required	Description
port	integer	path	True	Port number of remote syslog/splunk server
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
address	string	Destination syslog|splunk host to forward audit records to. This can be an IP address (IPv4|IPv6) or a hostname.
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
port	integer	Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514.
protocol	string	Log forwarding protocol
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server’s certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server’s certificate. Setting "verify_server" to "false" will not enforce validation of remote server’s certificate.

Example response


```
{
  "address": "string",
  "facility": "string",
  "protocol": "string"
}
```


Error

```
Status: Default, Error
```

Name	Type	Description
error	error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


Definitions

See Definitions

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Updates remote syslog/splunk server information

learn more

- [`doc /security/audit/destinations`](#docs-security-security_audit_destinations)

PATCH `/security/audit/destinations/{address}/{port}`

Updates remote syslog/splunk server information.

Learn more

- DOC /security/audit/destinations

Parameters

Name	Type	In	Required	Description
address	string	path	True	IP address of remote syslog/splunk server.

Name	Type	In	Required	Description
port	integer	path	True	Port number of remote syslog/splunk server.

Request Body

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

Example request

```
{
  "facility": "string"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.

Name	Type	Description
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

Example response


```
{
  "facility": "string"
}
```


Error

```
Status: Default, Default
```

Name	Type	Description
error	error	

Example error


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

security_audit_log_forward

Name	Type	Description
facility	string	This is the standard Syslog Facility value that is used when sending audit records to a remote server.
verify_server	boolean	This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.