NPM Probe SSL Diffie Hellman Keys APIs v1.1

Created Jan 16, 2024 at 02:01 PM

Resource: dh_key

PFS Diffie-Hellman Key.

http://{device}/api/npm.ssl_dh_keys/1.1/keys/items/{id}

JSON


```
{
  "ced_secret": string,
  "ch_secret": string,
  "client_ip_addr": string,
  "client_port": integer,
  "client_random": string,
  "ct_secret": string,
  "id": string,
  "master_key": string,
  "server_ip_addr": string,
  "server_port": integer,
  "sh_secret": string,
  "st_secret": string
}
```


Property Name	Type	Description	Notes
dh_key	*<object>*	PFS Diffie-Hellman Key.	Required properties: [client_random];
dh_key.ced_secret	*<string>*	TLS1.3 Client early data secret of the session.	Optional;
dh_key.ch_secret	*<string>*	TLS1.3 Client handshake secret.	Optional;
dh_key.client_ip_addr	*<string>*	The IP address of the client.	Optional;
dh_key.client_port	*<integer>*	The port of the client.	Optional;
dh_key.client_random	*<string>*	Hex encoded client random.	
dh_key.ct_secret	*<string>*	TLS1.3 Client traffic secret of the session.	Optional;
dh_key.id	*<string>*	A unique id for the Diffie-Hellman key.	Optional;
dh_key.master_key	*<string>*	Master secret of the session.	Optional;
dh_key.server_ip_addr	*<string>*	The IP address of the server.	Optional;
dh_key.server_port	*<integer>*	The port of the server.	Optional;
dh_key.sh_secret	*<string>*	TLS1.3 Server handshake secret.	Optional;
dh_key.st_secret	*<string>*	TLS1.3 Server traffic secret of the session.	Optional;

Links

Resource: dh_keys

PFS Diffie-Hellman Keys.

http://{device}/api/npm.ssl_dh_keys/1.1/keys

JSON


```
{
  "items": [ dh_key ]
}
```


Property Name	Type	Description	Notes
dh_keys	*<object>*	PFS Diffie-Hellman Keys.	
dh_keys.items	*<array of <dh_key>>*		Optional;
dh_keys.items[items]	*<dh_key>*	PFS Diffie-Hellman Key.	

Links

dh_keys: bulk_create

Adds associations between multiple client random and secrets values for TLS connections encrypted with Diffie-Hellman.

```
POST http://{device}/api/npm.ssl_dh_keys/1.1/keys/bulk_create
```

Request Body

Provide a dh_keys data object.

Response Body

Returns a dh_keys data object.

dh_keys: create

Adds an association between the client random and the secrets for a single TLS connection encrypted with Diffie-Hellman.

```
POST http://{device}/api/npm.ssl_dh_keys/1.1/keys/create
```

Request Body

Provide a dh_key data object.

Response Body

Returns a dh_key data object.