INFINIDAT

INFINIDAT REMOTE SUPPORT USER GUIDE

LAST UPDATED: 12/07/2025

Important Note

When this document is viewed in PDF format, links to other Infinidat Support Portal pages are not available.

Table of Contents

1 Introduction

The Infinidat Remote Support Application (RSA) is software that runs on the Support Appliance (SA). It is not related to array controllers and their functionality.

1.1 Purpose

Infinidat Remote Support provides a means of creating a secure point-to-point connection for supporting InfiniBox systems in the field. This accelerates the resolution of support cases.

The connection through the Remote Support Server (RSS) provides Infinidat Support with access to the management interfaces and the backend code only. This is equivalent to attaching a keyboard and a screen to the InfiniBox with the added benefit of exposing a full audit trail of the support session.

Remote Support provides the following:

- On-demand secured connection to the InfiniBox on the customer site
- End-to-end encrypted channel
- Full customer control of the connection
- Full visibility and auditing of the session logs

1.2 Terminology

RSA	Remote Support Application
SA	Support Appliance
RSS	Remote Support Server

1.3 Security

Outbound tunnel	The outbound tunnel connection from the Support Appliance (SA) to the Remote Support Server (RSS) is encrypted with TLS 1.2 (2048 bit AES encryption).
RSA tunnel	On top of that protocol, the RSA tunnel's regular SSH traffic is itself encrypted with SHA-256.
Authentication	The authentication is handled by OpenSSH, which is one of the leading solutions in the world for secure login.

1.4 Architecture

The Support Appliance (SA) requires a connection to the Infinidat RSS. The connection can be either direct or through a web proxy.

The storage administrator initiates the connection either through the GUI, or by accessing the SA using a standard browser. We recommend using port 9000 (HTTPS) because it is secure, although port 8000 (HTTP) is acceptable.

> ⚠ Starting from Support Appliance version 3.3.1, port 8000 always redirects to port 9000.

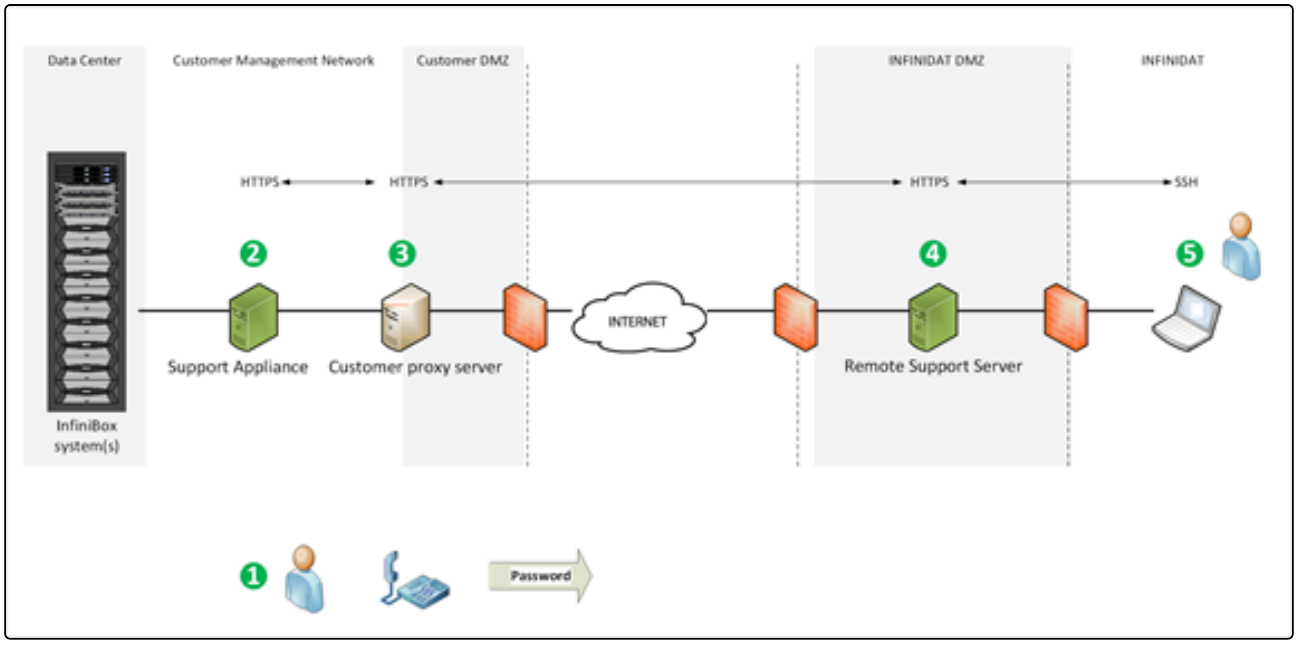
The storage administrator is required to create an RSS Secret that will be used for the connection through the tunnel.

The internal SSH daemon that serves the session listens only to local connections, and only accepts connections coming through the RSS. It is the RSA (and not the RSS) that validates the RSS Secret. Even if the RSS was jeopardized, it does not allow access to any of the open sessions.

Once a tunnel is stopped, the local process that relays communications to the internal SSH socket ends, and it is no longer possible to create a connection into the SA.

1.5 Network topology

The Support Appliance (SA) is a separate server within the InfiniBox rack. It has its own dedicated Ethernet ports.



1	The customer initiates the connectivity via the Support Appliance and sends the RSS Secret to the Infinidat support representative.
2	The Support Appliance sends a request to the customer's Proxy Server.
3	The Support Appliance logs into the customer Proxy Server.
4	The Support Appliance creates a tunnel to the Remote Support Server.
5	The Support personnel locate the connected InfiniBox system and use the provided RSS Secret to connect to the Support Appliance via the Remote Support Server.

The outbound connection can go through the same network that the administrator connects from, or through another network.

It is assumed that the Support Appliance (SA) can either:

- Directly reach RSS:443.
- Reach a proxy (HTTPS/SOCKS4/SOCKS5) that enables it to access the RSS.

The web UI allows the customer to directly configure the connectivity.

Note	We recommend restricting the SA outgoing connection, either: • to the RSS or to the Proxy only • based on the customer's policy Both methods of restriction are carried out by the customer's network or firewall settings.

2 Setting up the Remote Support

It is always preferred to use the InfiniBox GUI to connect to the Remote Support. If the InfiniBox GUI is not available, use the direct Support Appliance web interface (port 8000 or 9000) and the Challenge Authentication option.

2.1 Port connectivity

Direction

The Direction column in the table indicates whether the Support Appliance needs an inbound firewall rule or an outbound firewall rule to allow the connection.

Source	Target	Direction	Purpose	Port	Protocol
Client (Browser)	Support Appliance	Inbound	HTTP Remote Support Management HTTPS Remote Support Management	8000*, 9000	TCP

Support Appliance	Remote Support Servers**:
	• rss.infinidat.com
	  • IP Addresses: 15.197.204.67, 3.33.245.240
	• rss-us.infinidat.com
	  • Only when instructed by Infinidat Support
		Outbound	Remote Support session	443	TCP

Support Appliance	callhome-eu.ramen.infiniops.com	Outbound	Authenticate for file fetches	443	TCP
Support Appliance	drop.infiniops.com	Outbound	Fetch upgrade files See InfiniDrop	443	TCP
Customer workstation, Linux host, another system SA, or similar	Support Appliance	Inbound	Local troubleshooting	22	TCP

* Starting from Support Appliance version 3.3.1, port 8000 always redirects to port 9000.

** The following Remote Support Server targets are no longer used:

- rss02.infinidat.com
- rss05.infinidat.com
- rss07.infinidat.com
- rss08.infinidat.com

2.1.1 Importing SSL certificate for Firewall/Proxy

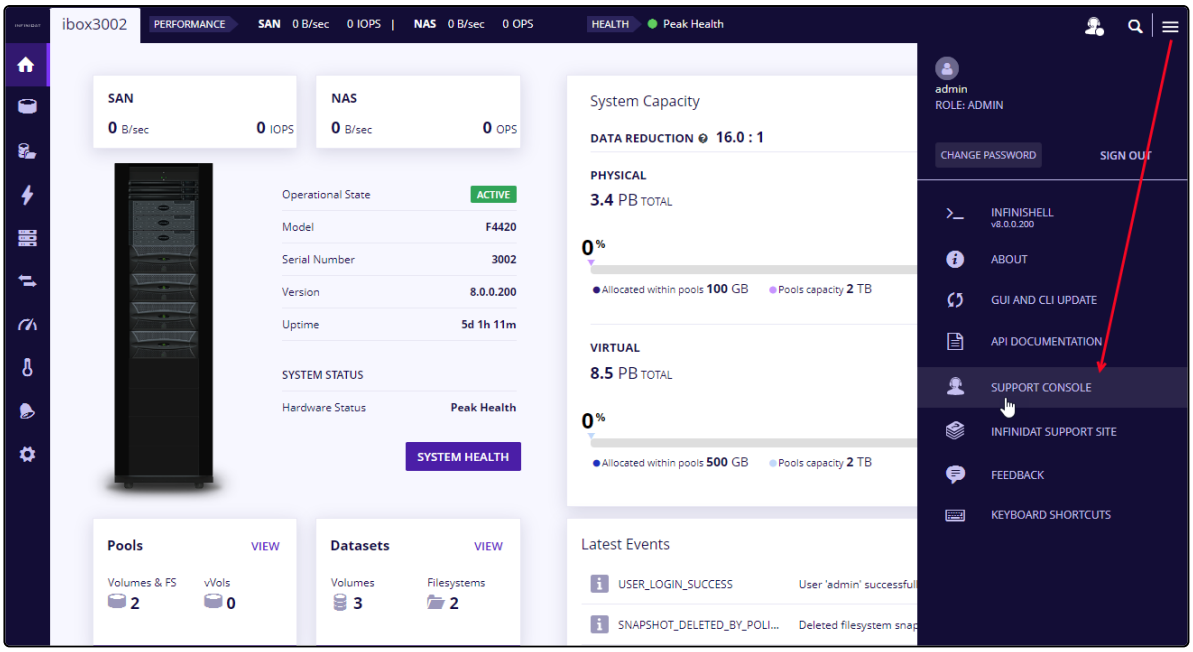
If the firewall or proxy requires importing the `rss.infinidat.com` certificate to allow the connection, you can run the following command from any OS that supports openssl client:

```
openssl s_client -showcerts -connect rss.infinidat.com:443 </dev/null 2>/dev/null|
openssl x509 -outform PEM >rss_cert.pem
```

2.2 Setting up a Remote Support connection from the InfiniBox GUI

To set-up a Remote Support connection from the InfiniBox GUI:

1 In the InfiniBox Management Console GUI, click the menu icon at the top-right corner of the screen and select **Support Console**.



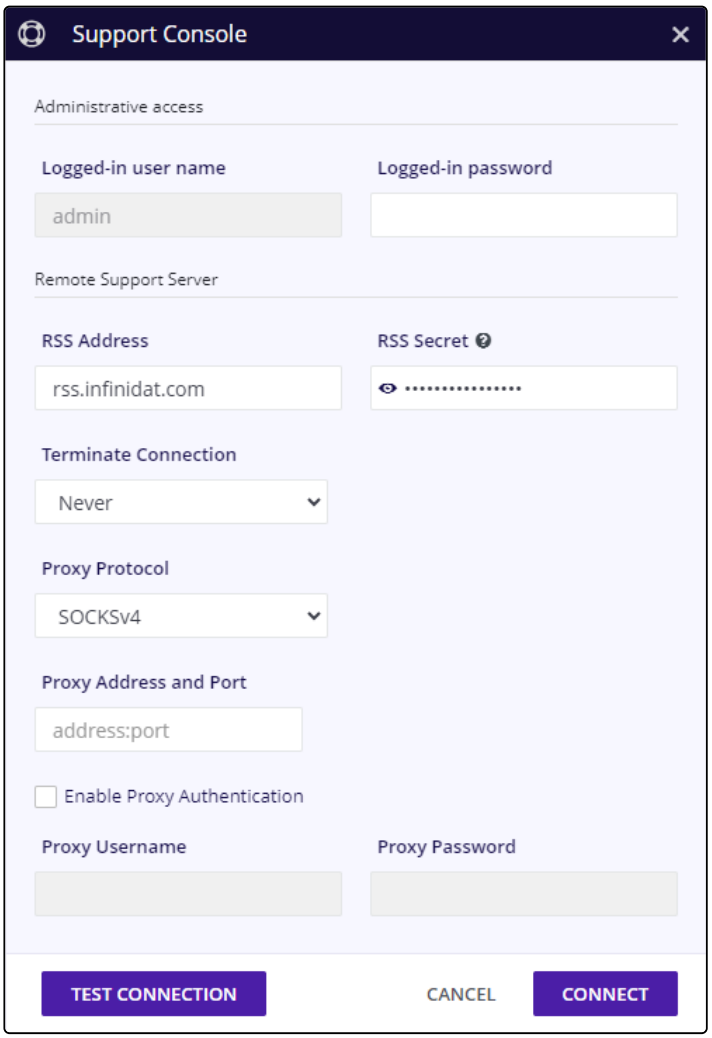
The **Support Console** window opens.

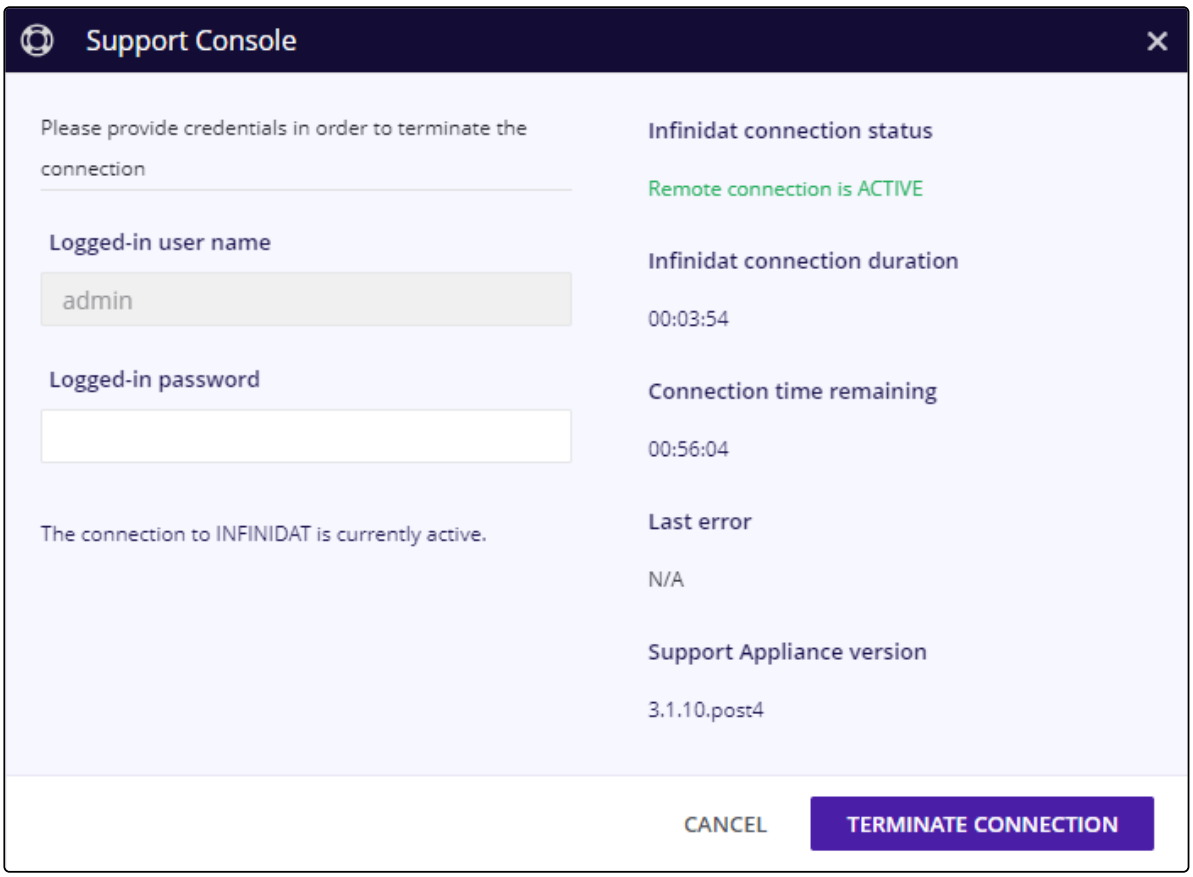
2 Fill in the following fields.

- **Logged-in user name** - a username with an Admin role.
- **Logged-in password** - the password of this username.

> **SSO user authentication**
>
> Starting from Support Appliance version 3.3.1, SSO users can open a support tunnel by entering the 3 characters '**SSO**' in the **Logged-in password** input field. During SSO login, changes to the RSS Address input field are ignored.

- **RSS Address** - the address of the RSS server, in the format `RSS.infinidat.com`.
- **RSS Secret** - a new password for the tunnel to be generated. You will need to send this secret to Infinidat Support once the tunnel is open to enable them to connect.
- **Terminate Connection** - when to automatically terminate the connection.
- **Proxy Protocol** - which proxy, if any, is used
- **Proxy Address and Port** - the address or the DNS name of the proxy server, if used
- **Proxy Username** and **Proxy Password** - proxy credentials, if required



3	To test the connection, click **Test Connection**.
4	Click **Connect**. The connection is established.
5	To view the remote connection status or to terminate the connection, click the menu icon at the top-right corner of the InfiniBox Management Console GUI, and select **Support Console** again.  To terminate the connection, enter the password, and click **Terminate Connection**. Otherwise, click **Cancel** to close the window.

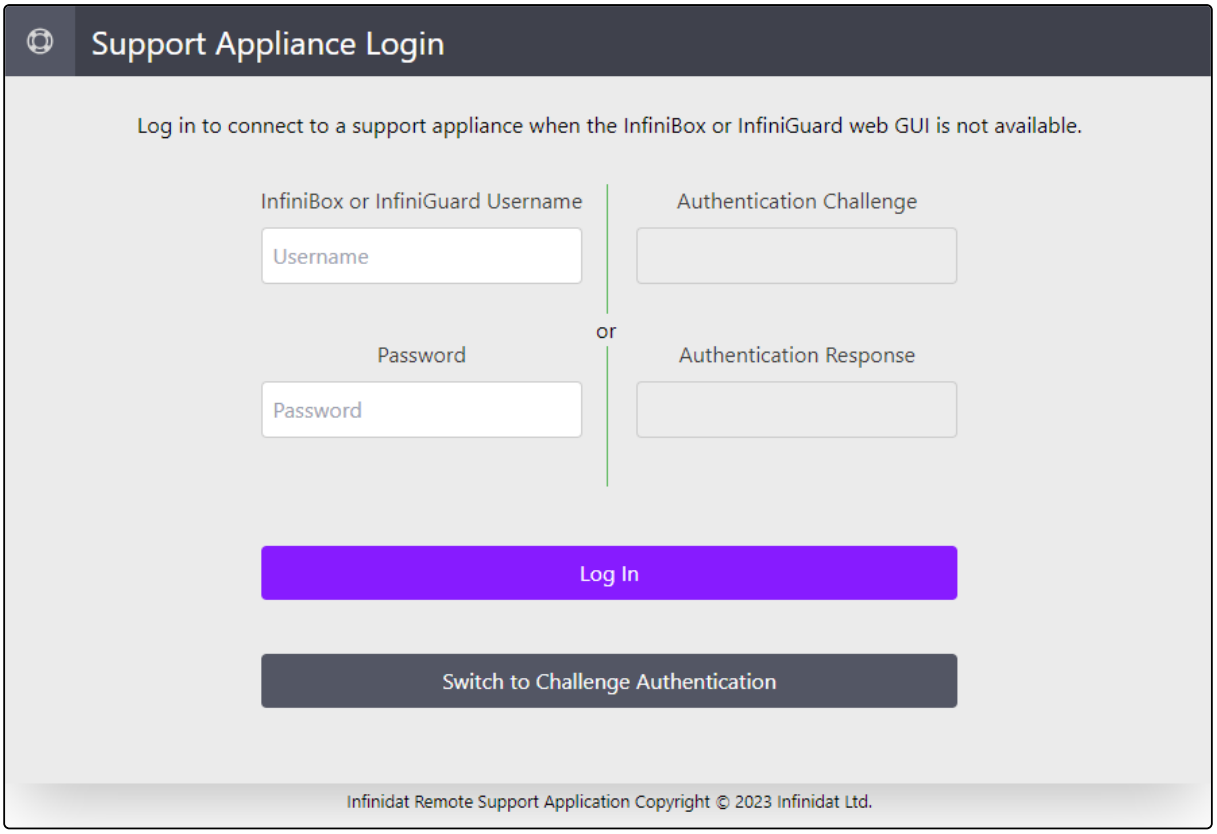
3 Logging in to the support appliance

3.1 Username and password authentication

The Remote Support Appliance login is performed against the system management layer. To create a support connection, log in to the Support Appliance using https on port 9000 or http on port 8000.

⚠ Starting from Support Appliance version 3.3.1, port 8000 always redirects to port 9000.

1. If you know your InfiniBox or InfiniGuard credentials, enter them in the Login window, and click the **Log In** button.

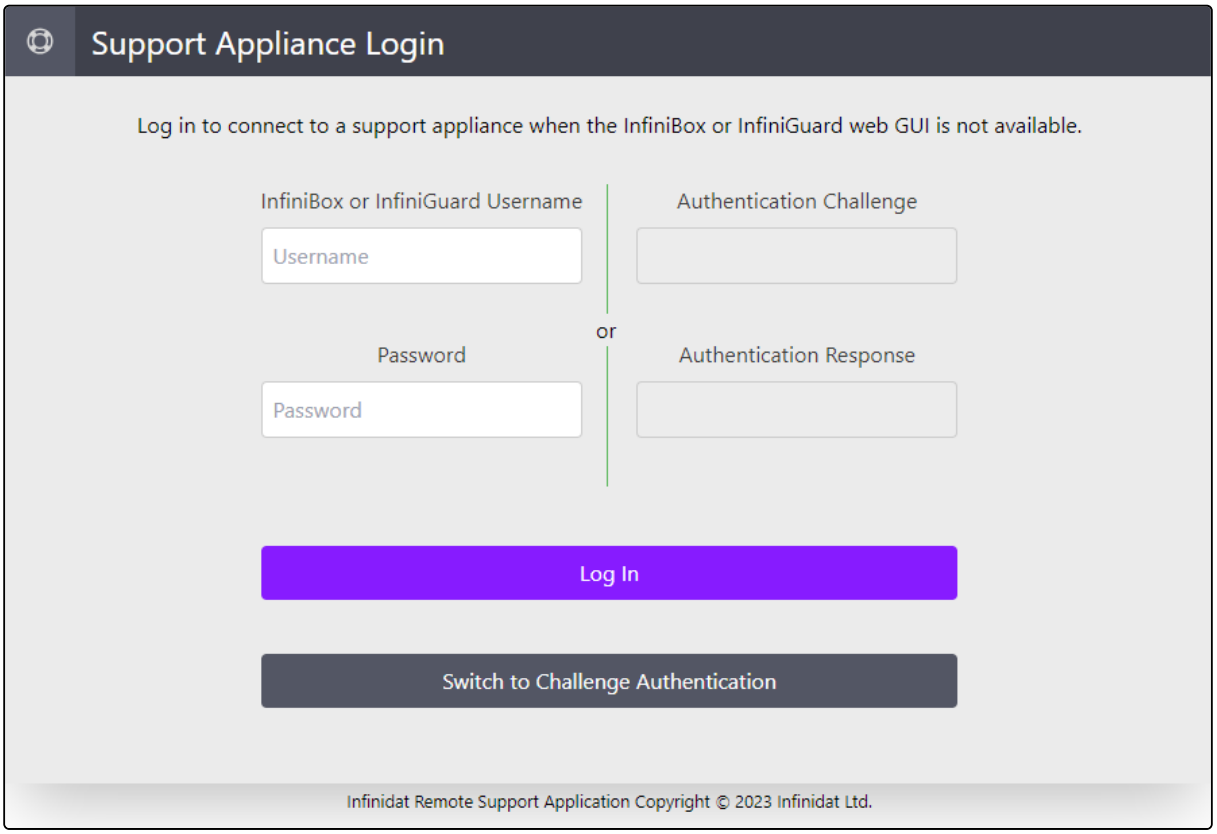


3.2 Challenge-response authentication

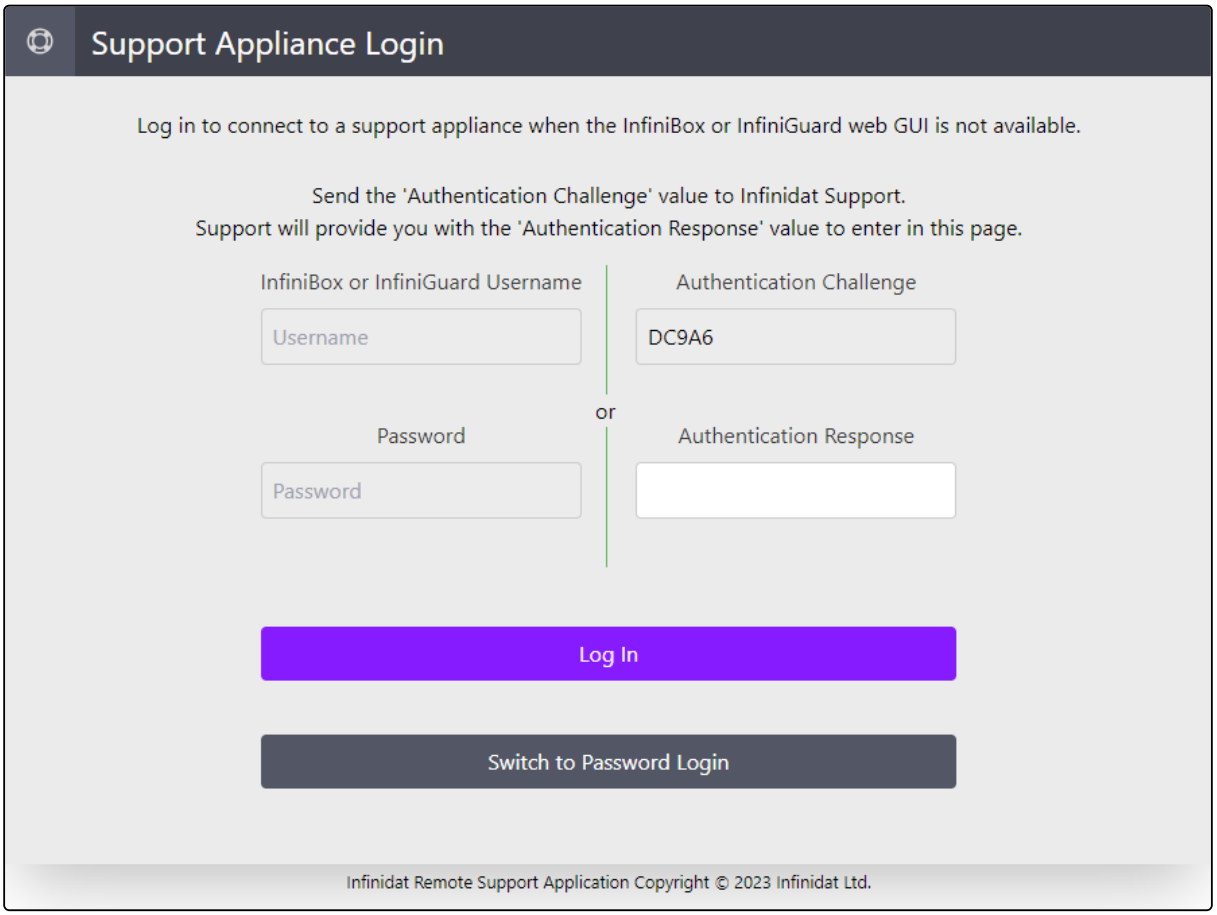
If the system management layer is not available, log in to the Support Appliance using https on port 9000 or http on port 8000 to create a support connection, and use the Challenge Authentication option.

⚠ Starting from Support Appliance version 3.3.1, port 8000 always redirects to port 9000.

1. At the bottom of the Support Appliance Login window, click **Switch to Challenge Authentication**.



2. An **Authentication Challenge** value is automatically generated and displayed. Do not click anything else on this page.



3. Send the **Authentication Challenge** value to Infinidat Support. They will send you another value to enter into the **Authentication Response** field on this page.
   Do not click anything else on this page.
4. When you receive the **Authentication Response** value, copy it into the the appropriate field, and click the **Log In** button.

3.3 Initialize a connection

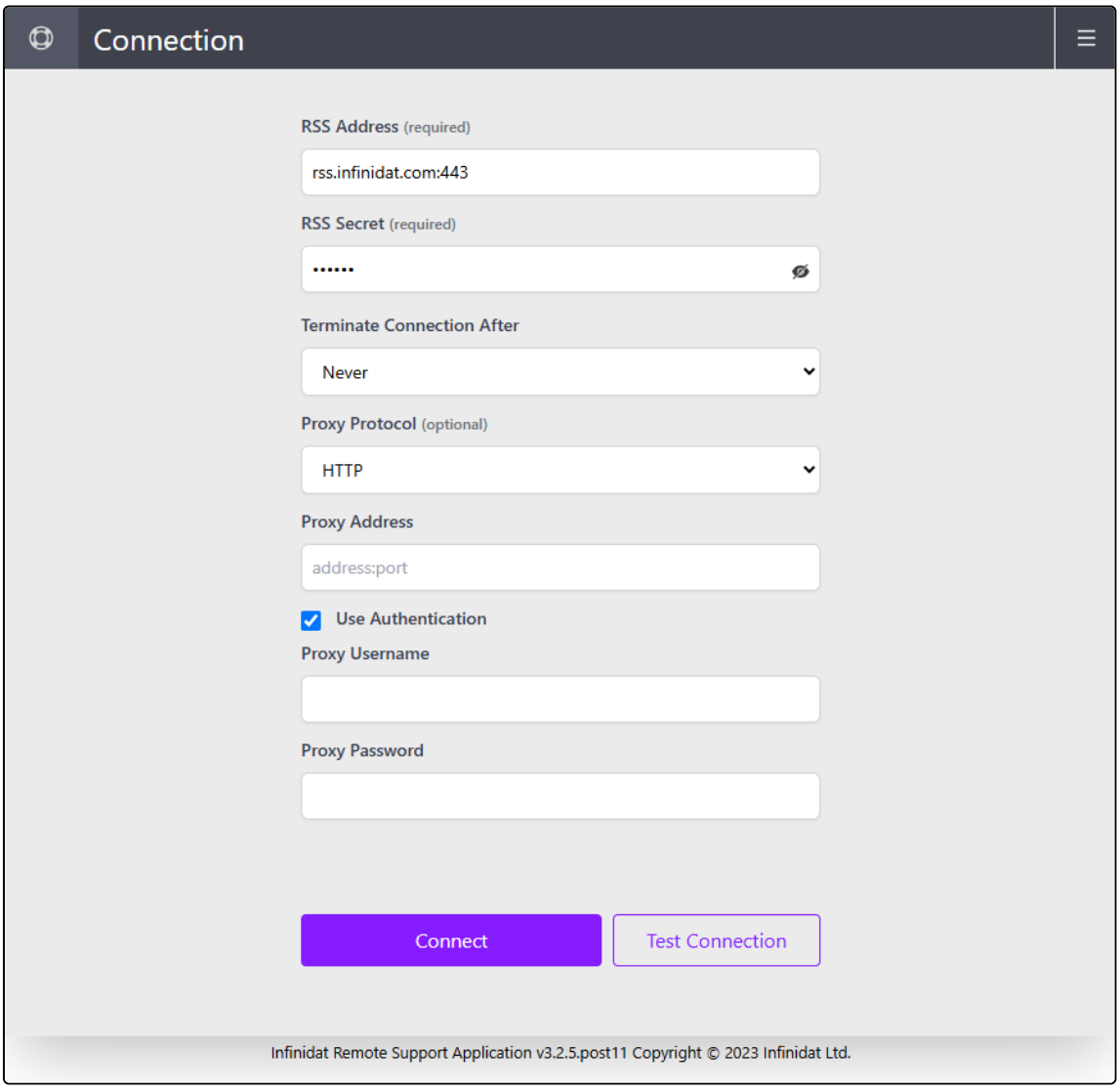
After you have been authenticated, the **Connection** window opens.

1

To initialize a connection, enter the RSS address, and set an RSS Secret for the session. You will need to send this secret to Infinidat Support once the tunnel is open to enable them to connect.

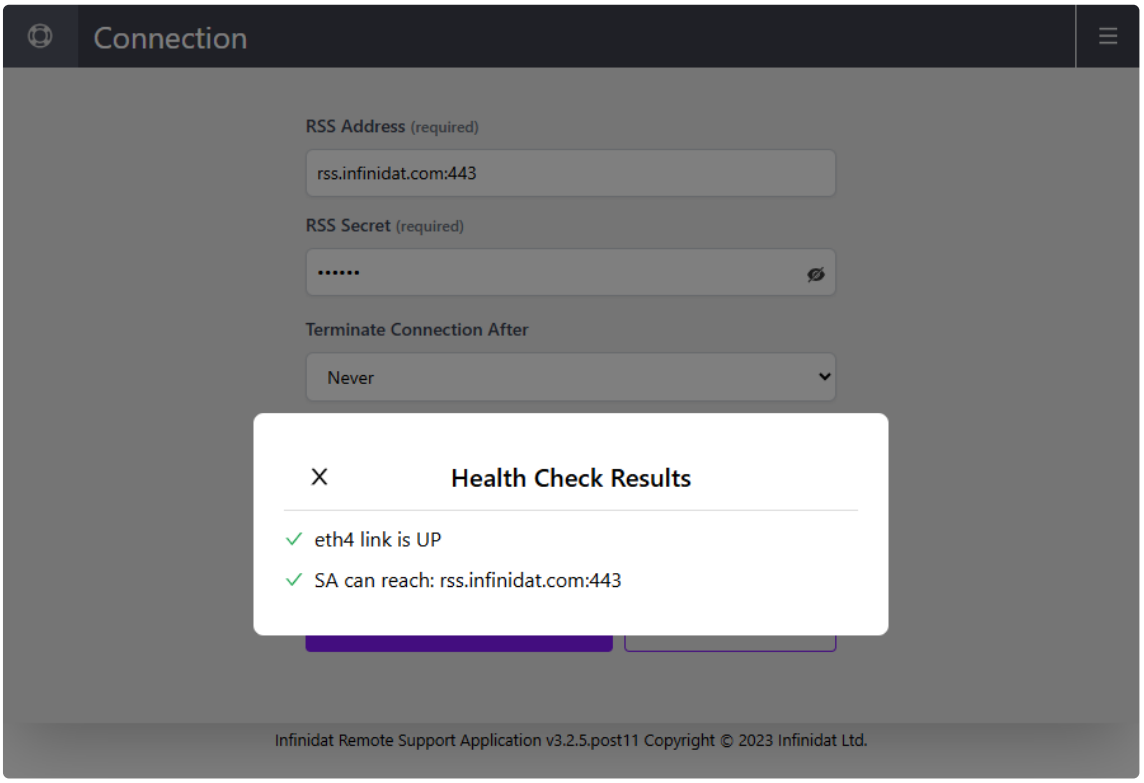
Optional session details:

- In the **Terminate Connection After** field, you can select a session timeout. Once the timeout expires, the session automatically disconnects regardless of any activity taking place.
- You can select a proxy protocol for reaching the internet, and optionally require credentials to authenticate to the proxy.



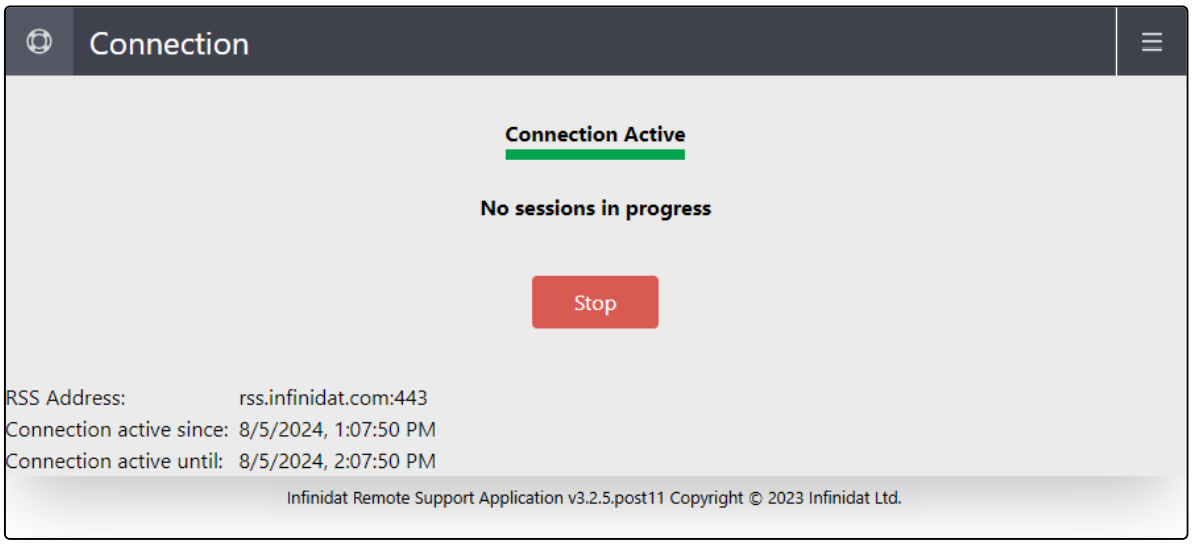
- Starting from Support Appliance version 3.3.0, you can install an SSL certificate for the Support Appliance (SA) webserver (port 9000) from the SA GUI.
  See 'Managing SSL certificates'.

- Starting from Support Appliance version 3.1.5, you can test the connection before attempting to connect to the RSS address.
  Click the **Test Connection** button, and verify that the health check results indicate that the SA can connect to the RSS address.

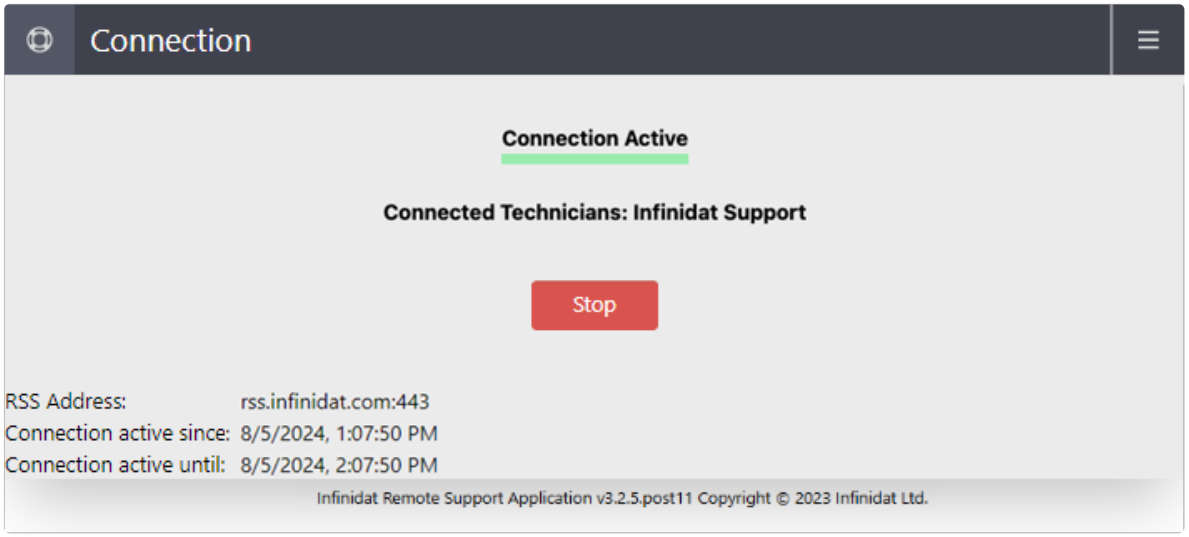


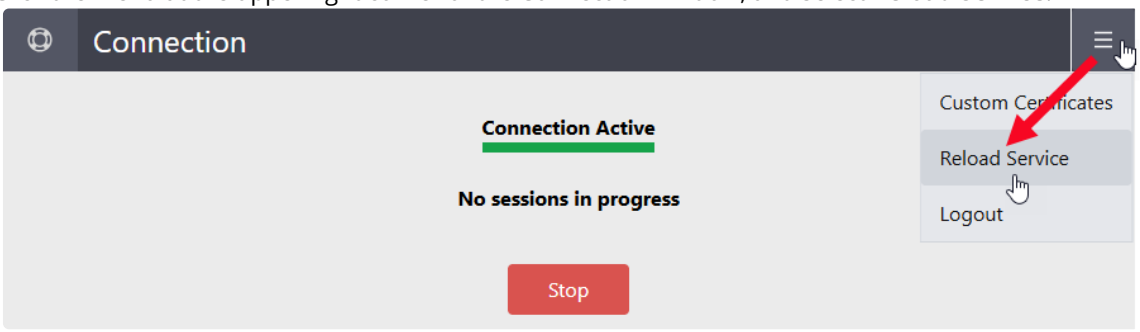
- Click **Connect**.

2 When the connection is established, inform Infinidat Support, and send them the RSS Secret.



3 A message is displayed when Infinidat Support accesses the connection.

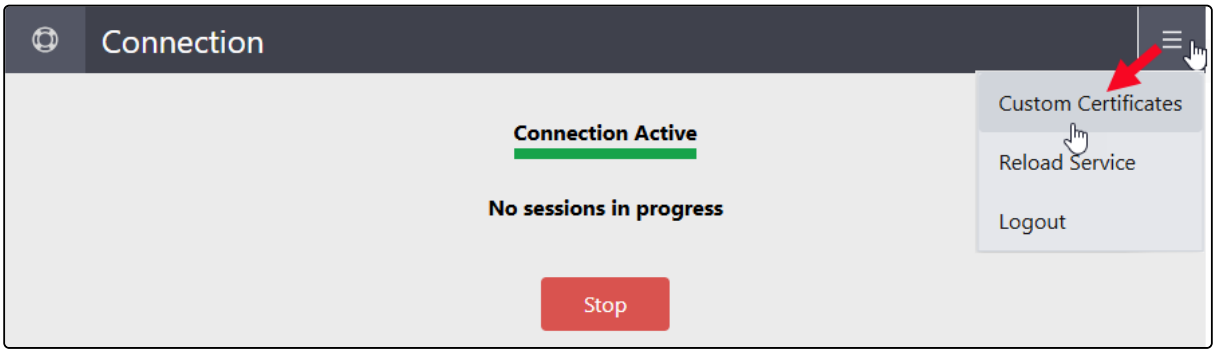


4	If the remote support client stops responding, you can reload it. • Click the menu at the upper right corner of the Connection window, and select **Reload Service**.  • Click **Yes**, and refresh your browser.
5	When the connection is no longer needed, click the **Stop** button to close the connection.

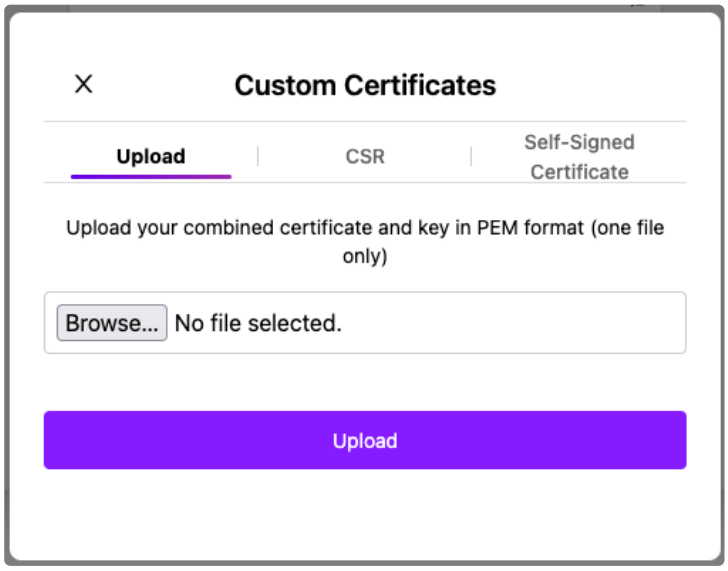
3.4 Managing SSL certificates

3.4.1 Accessing the Custom Certificates window

1. After logging into the support appliance, click the menu at the upper right corner of the Connection window, and select **Custom Certificates**.



2. Select an option in the Custom Certificates window.
   - Upload a combined certificate and key in PEM format.
   - Generate a CSR.
   - Generate a new self-signed certificate.



3.4.2 Preparing a certificate file

If the private key was not generated through the remote support application CSR request, prepare the certificate file to be uploaded.

To prepare a file for upload, combine ("concatenate") the characters in the signed certificate and the characters in its private key into one long list of characters.

- The first list of characters is a PEM-encoded private key file of 2048 or 4096 bits whose first line starts with `-----BEGIN`
  For example:

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDkn8E97lOj2pvt
...
lhR3fQ/lri/LVetY3VtcnOUL91l6Sp/AJgHTAfzigcWC0UZABqiXwxRWp6S9fRue
bGPa+xf11oTIIqEq2qrGlAtwrA==
-----END PRIVATE KEY-----
```

- The second list of characters is a PEM-encoded X509 signed certificate whose:
  - first line starts with `-----BEGIN`
  - public key matches the private key in the first list of characters
  - CN matches the system's FQDN. For example:

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIJAMhgnI/1w772MA0GCSqGSIb3DQEBCwUAMG4xCzAJBgNV
...
/prJK/r5mA7Uvttga7vI2Sv4lZySonmWN5bkKCxbsxRWk1WusxJ0MyR2xEwXHo/E
to5uReXFUBYNLab/tWU+EuQTSzKLJYerSSCc7eq6PDTbeek=
```

```
-----END CERTIFICATE-----
```

- For the list of characters shown in these examples, the combined (concatenated) file would be:

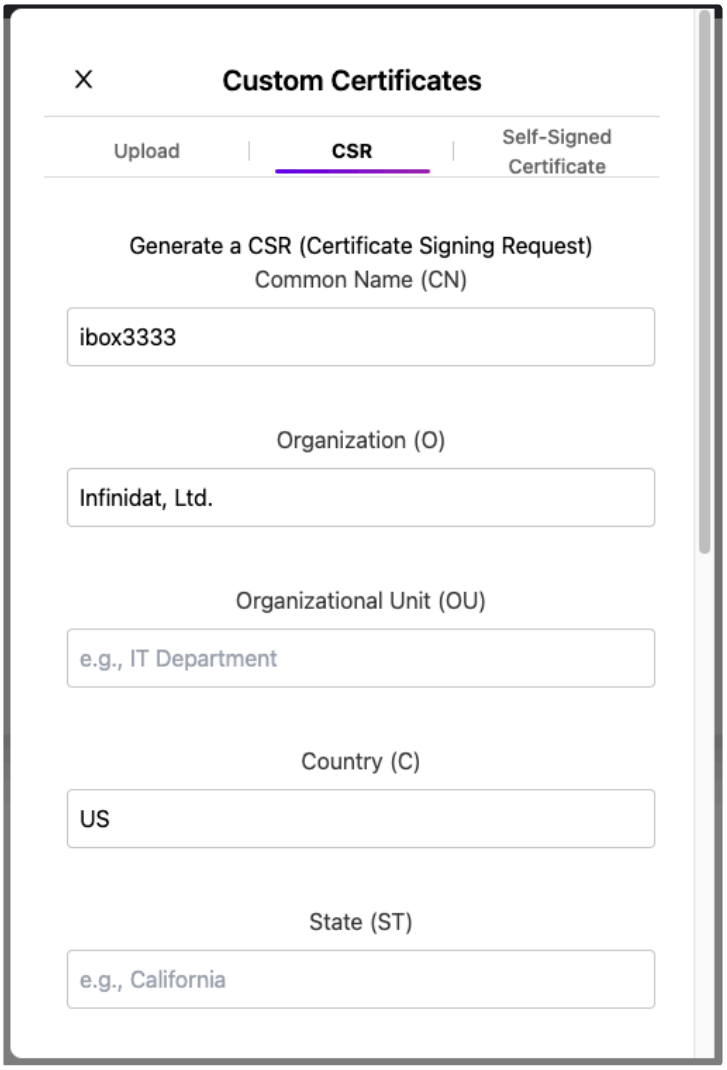
```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDkn8E97lOj2pvt
...
lhR3fQ/lri/LVetY3VtcnOUL91l6Sp/AJgHTAfzigcWC0UZABqiXwxRWp6S9fRue
bGPa+xf11oTIIqEq2qrGlAtwrA==
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIJAMhgnI/1w772MA0GCSqGSIb3DQEBCwUAMG4xCzAJBgNV
...
/prJK/r5mA7Uvttga7vI2Sv4lZySonmWN5bkKCxbsxRWk1WusxJ0MyR2xEwXHo/E
to5uReXFUBYNLab/tWU+EuQTSzKLJYerSSCc7eq6PDTbeek=
-----END CERTIFICATE-----
```

The certificate file is ready to be uploaded.

3.4.3 Generating a new Certificate Signing Request

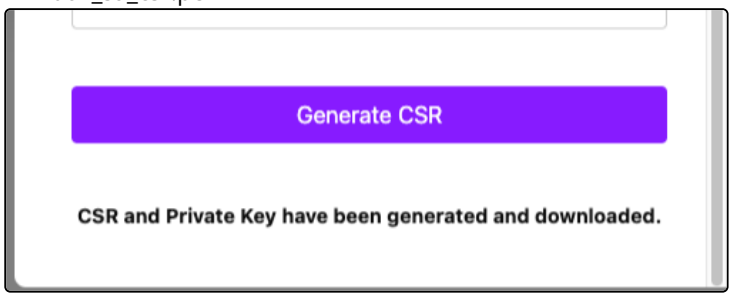
To generate a remote support application CSR request:

1. In the Custom Certificates **CSR** tab, complete the fields.



2. At the bottom of the window, click **Generate CSR**.

3. When the generation is completed, two files are downloaded:
   - infinibox_sa_private_key.key
   - infinibox_sa_csr.pem

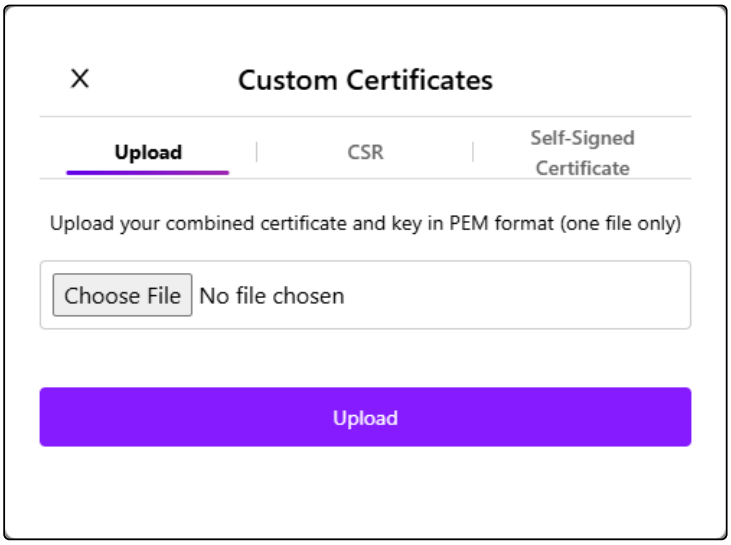


3.4.4 Uploading a certificate file

Upload either a manually concatenated certificate file, or a certificate generated by a remote support application CSR request.

To upload a certificate file:

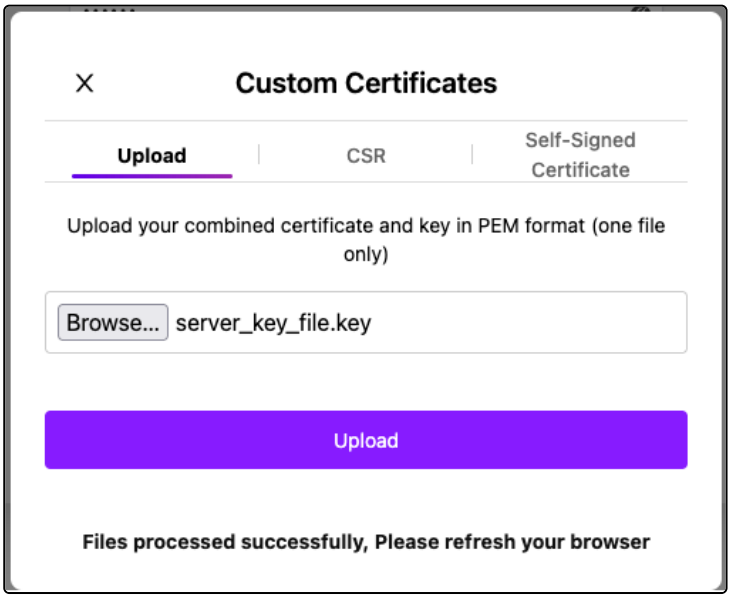
1. In the Custom Certificates **Upload** tab, click the **Choose File** button.



2. Browse to the location of the certificate file and select it.

3. Click the **Upload** button.

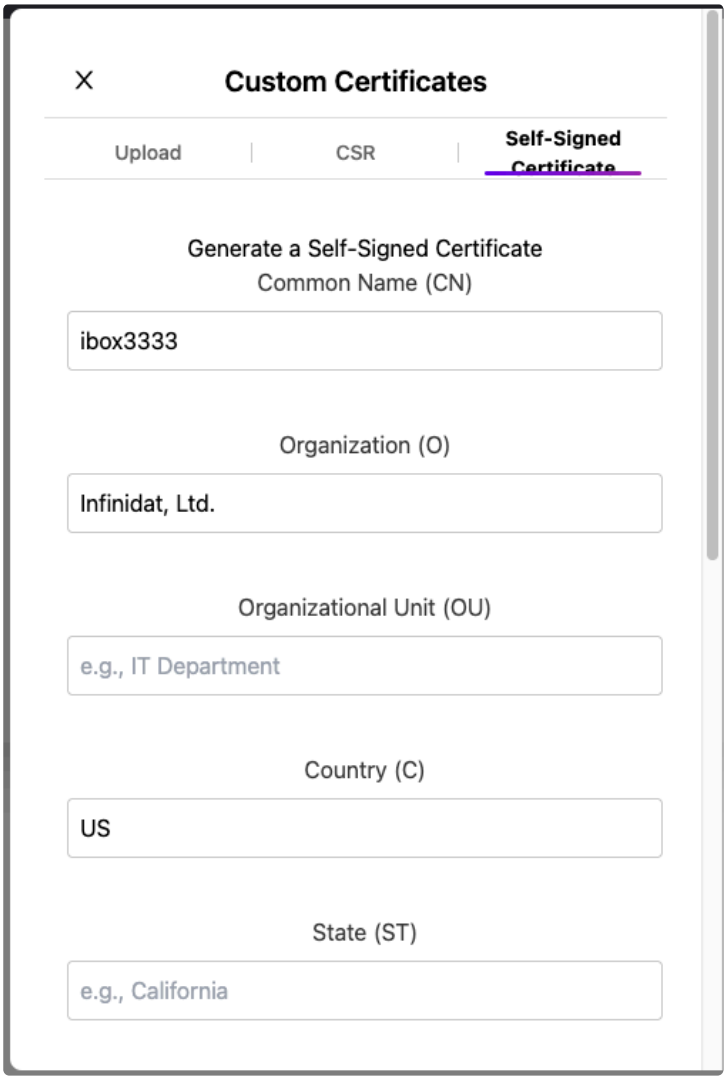
   When the file is verified and the certificate is applied, refresh your browser.



3.4.5 Generating a new self-signed certificate

Self-signed certificates are generated in a similar way as a CSR.

1. In the Custom Certificates **Self-Signed Certificate** tab, complete the fields.



2. At the bottom of the window, click **Generate Self-Signed Certificate**.

3. When the generation is completed, refresh your browser.

3.5 Session logs

Each of the sessions is fully recorded with ttyrec. The logs are kept on the RSS and are available to the customer on demand.

4 Auditing the support sessions

Remote Support creates custom events on the InfiniBox when:

- A Remote Support connection is opened.
- Infinidat Support connects to the system.

4.1 CUSTOM_INFO_EVENTS

- Event code: CUSTOM_INFO_EVENT
- Depending on the reported action, the event description is one of the following:
    - Support session started
    - Infinidat Support connected to the system
    - Infinidat Support disconnected from the system
    - Support session ended

4.2 Separate events for session started and ended

SUPPORT_CONNECTED	Infinidat Support connected to the system
SUPPORT_DISCONNECTED	EXTERNAL Infinidat Support disconnected from the system
SUPPORT_SESSION_STARTED	EXTERNAL Support session '{session_name}' started, will automatically be closed on {session_expiry_time}
SUPPORT_SESSION_ENDED	EXTERNAL Support session '{session_name}' ended

5 Infinidat support notifications

5.1 Purpose

Every InfiniBox and InfiniGuard system is configured to notify Infinidat Support whenever a hardware failure event occurs. This notification is sent via the SMTP entry configured for event notifications.
See Configuring event notifications in InfiniBox.

5.2 SMTP connectivity

For notifications to reach Infinidat Support, the SMTP configuration entry named **infinidat-smtp** must allow emails to be relayed to **callhome@infiniops.com**.

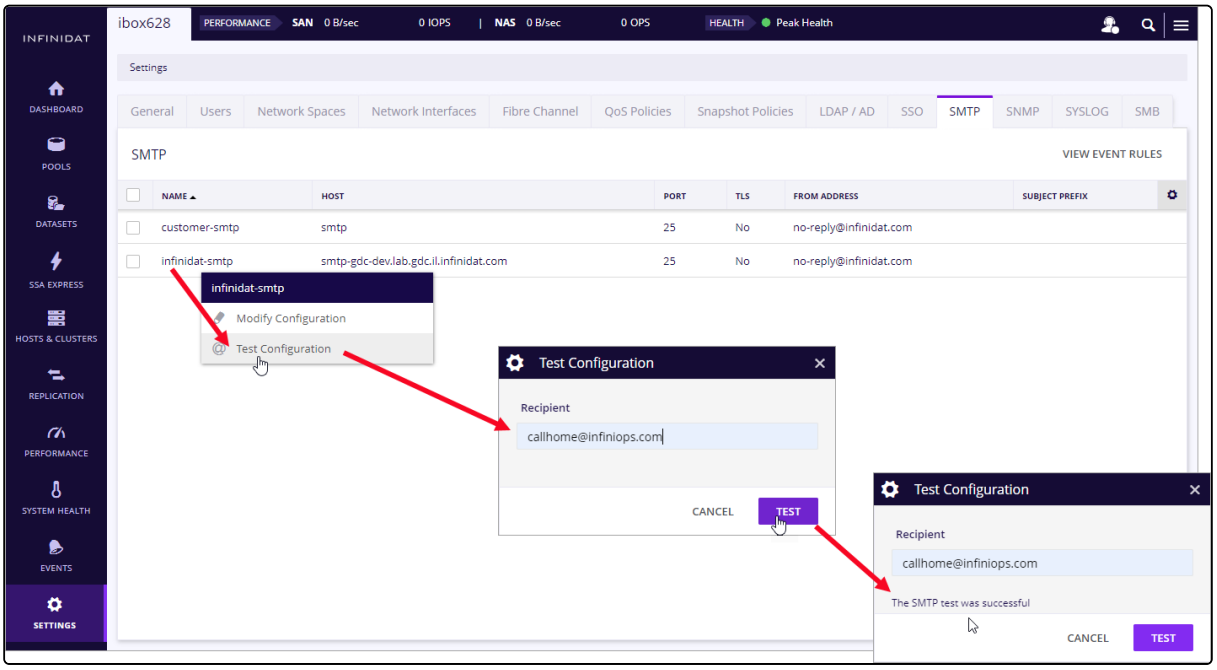
This is **in addition to** allowing outbound TCP port 25, or any other port that is used by the SMTP entry, as described in TCP and UDP ports required for Infinidat products.

5.3 Verify connectivity

To verify the connectivity:

1. From the InfiniBox management console GUI, click the Settings icon on the left toolbar, and open the SMTP tab.
2. Right-click **infinidat-smtp** and select **Test Configuration** from the menu.
3. In the Recipient field, enter **callhome@infiniops.com**
4. Click **Test**.

   A message confirms that events can be sent to this email.



If an error message is displayed:

- Ensure that the email address is allowed on your mail relay.
- Ensure that the outbound TCP port used by SMTP is open. By default, this is TCP port 25. For more information, refer to TCP and UDP ports required for Infinidat products.