

Erstellen von Secure Malware Analytics Support Snapshot und Aktivieren von Live-Support-Sitzungen

Inhalt

[Einleitung](#)

[Support-Snapshots](#)

[Erstellen von Support-Snapshots über die Admin-Benutzeroberfläche](#)

[Erstellen von Support-Snapshots über die TGSN-CLI](#)

[Live-Support-Sitzung](#)

[Aktivieren der Live-Support-Sitzung über die Admin-Benutzeroberfläche](#)

[Live-Support-Sitzung über die TGSN-CLI aktivieren](#)

Einleitung

Dieses Dokument beschreibt die Schritte zum Sammeln von Support Snapshot und zum Aktivieren von Live-Support-Sitzungen von der Cisco Secure Malware Analytics-Appliance für weitere Untersuchungen.

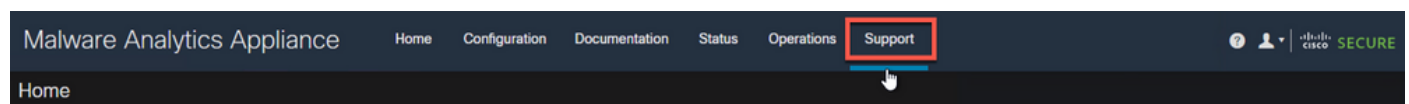
Support-Snapshots

Erstellen von Support-Snapshots über die Admin-Benutzeroberfläche

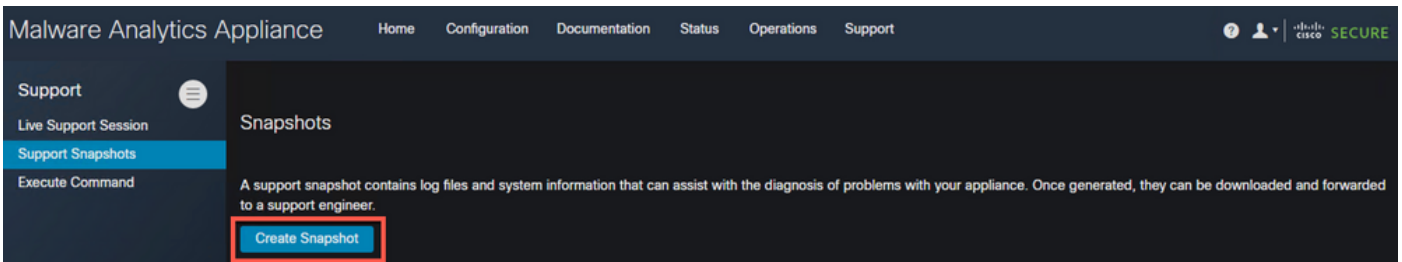
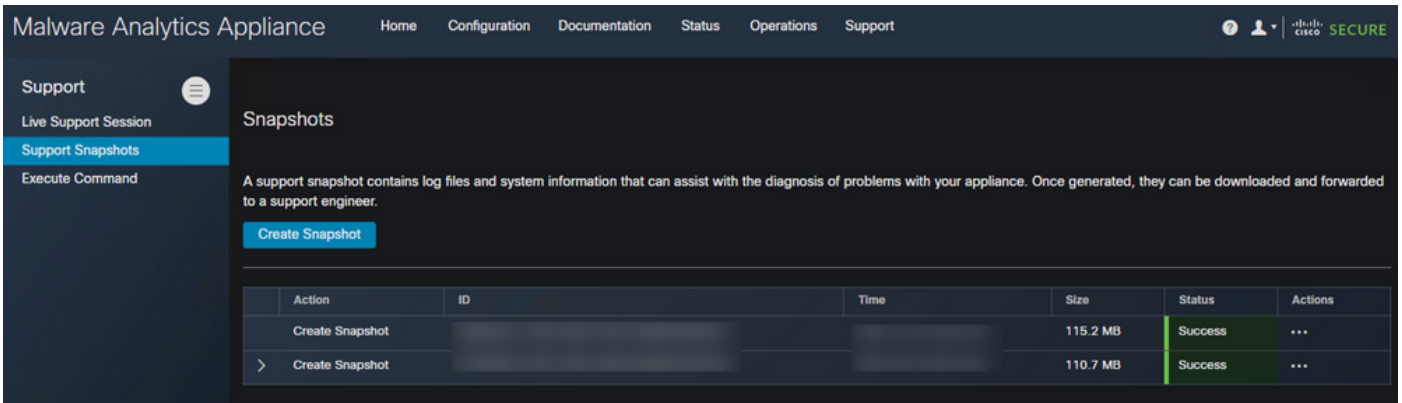
Führen Sie die folgenden Schritte aus, um einen Snapshot für die Unterstützung zu erstellen:

Schritt 1: Anmeldung bei der Administratorbenutzeroberfläche für sichere Malwareanalysen

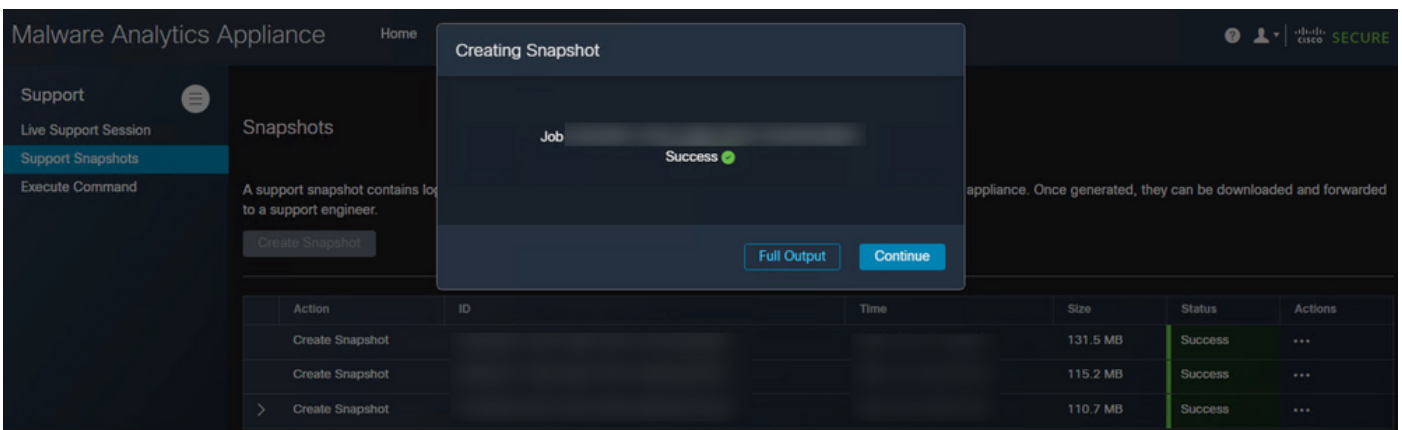
Schritt 2: klicken oder **Support** auswählen



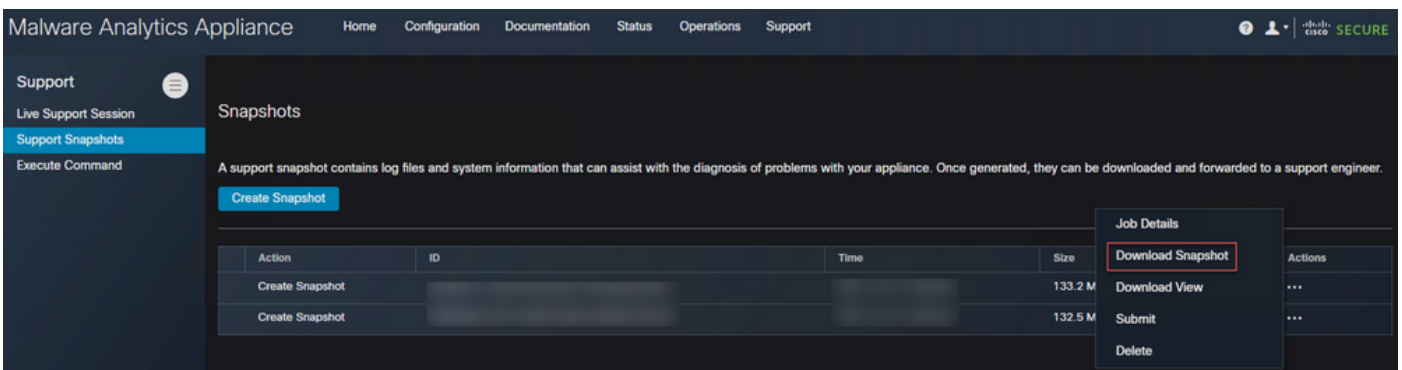
Schritt 3: Klicken Sie auf oder wählen Sie **Support Snapshots aus**, und klicken Sie dann auf **Create Snapshot (Snapshot erstellen)**, um einen Support-Snapshot auf dieser Appliance zu erstellen.



Schritt 4: Wenn der Snapshot abgeschlossen ist, wird eine Meldung **Success** angezeigt, wie im Bild gezeigt:



Schritt 5: Klicken Sie unter **Aktionen** auf oder wählen Sie **Snapshot herunterladen aus**, um den Snapshot auf Ihrem Computer herunterzuladen, von dem Sie sich bei der Benutzeroberfläche angemeldet haben.



Erstellen von Support-Snapshots über die TGSH-CLI

Führen Sie die folgenden Schritte aus, um einen Support-Snapshot von der TGSH-CLI zu erstellen:

Schritt 1: Melden Sie sich über SSH bei der TGSH-CLI an. Anweisungen zur Konfiguration dieses Zugriffs finden Sie im [Benutzerhandbuch](#).

Schritt 2: Wählen Sie nach der Anmeldung die Option **Snapshots** aus.

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[redacted]
Application URL / MAC: https://[redacted]
Password:            *** set by user ***

(n) Network
    Configure the system's network interfaces
(r) Support Mode
    Allow remote access by customer support
(u) Updates
    Download and optionally install updates
(s) Snapshots
    Generate and submit snapshots
(a) Apply
    Apply configuration
(c) Console
    CLI-based configuration access
(e) Exit
    Exit the management tool
```

Schritt 3: Wählen Sie die Option **Erstellen**, um den Snapshot zu erstellen. Nun können Sie den Snapshot gemäß dem für die Admin-Benutzeroberfläche dokumentierten Prozess von der Admin-Benutzeroberfläche herunterladen.

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[redacted]
Application URL / MAC: https://[redacted]
Password:            *** set by user ***

-----Snapshots-----
Latest snapshot: [redacted]

(c) Create
    Create Support Snapshot
(v) View
    View Support Snapshot
(s) Submit
    Submit Support Snapshot
(b) Back
    Back to main menu
```

Live-Support-Sitzung

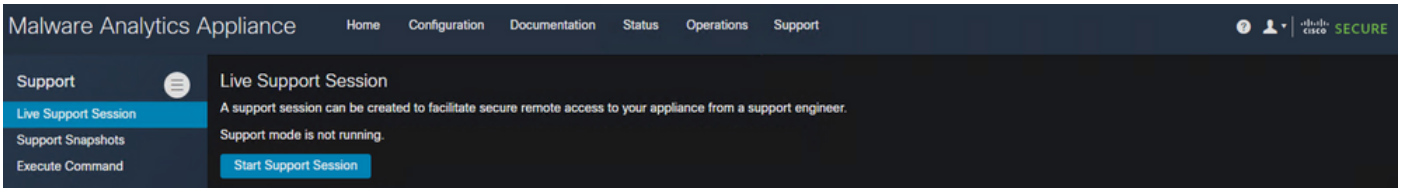
Aktivieren der Live-Support-Sitzung über die Admin-Benutzeroberfläche

In den meisten Fällen bittet das TAC Sie möglicherweise, eine Live-Support-Sitzung mit der Secure Malware Analytics-Appliance für weitere Untersuchungen zu aktivieren.

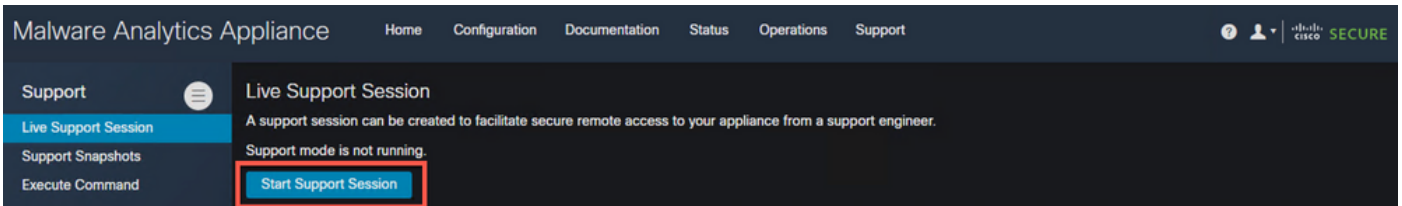
HINWEIS: Geben Sie die Seriennummer an, die Sie für die Live-Support-Sitzung an das TAC aktivieren, damit diese remote auf das Gerät zugreifen können.

Um diesen Zugriff auf die Appliance zu aktivieren, gehen Sie wie folgt vor:

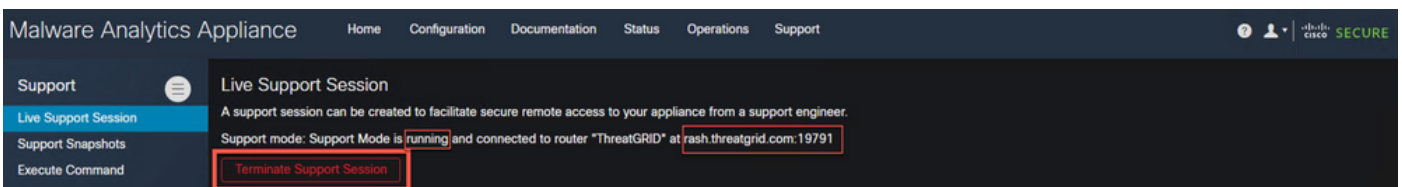
Schritt 1: Klicken Sie auf der Admin-Benutzeroberfläche auf oder wählen Sie die **Live Support Session** unter der **Support**-Registerkarte aus.



Schritt 2: Klicken Sie auf oder wählen Sie die Option **Support-Sitzung starten** aus.



Schritt 3: Sobald die Verbindung hergestellt ist, müssen Sie die Meldung wie im Bild gezeigt sehen:



Anmerkung: Sie müssen Outbound Connectivity from the **Dirty** interface to **rash.drohgrid.com** zulassen, damit dieser Zugriff ordnungsgemäß funktioniert. Weitere Informationen finden Sie im [Diagramm für die Netzwerkschnittstellen-Einrichtung](#).

Live-Support-Sitzung über die TGSH-CLI aktivieren

Um diesen Zugriff auf die Appliance über die TGSH-CLI von SSH aus zu aktivieren, gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich bei der TGSH SSH CLI an.

Schritt 2: Wählen Sie die Option **Supportmodus aus**.

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[REDACTED]
Application URL / MAC: https://[REDACTED]
Password:            *** set by user ***

(n) Network
    Configure the system's network interfaces
(r) Support Mode
    Allow remote access by customer support
(u) Updates
    Download and optionally install updates
(s) Snapshots
    Generate and submit snapshots
(a) Apply
    Apply configuration
(c) Console
    CLI-based configuration access
(e) Exit
    Exit the management tool
```

Schritt 3: Wählen Sie **Start** aus, um die Live-Sitzung zu aktivieren.

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[REDACTED]
Application URL / MAC: https://[REDACTED]
Password:            *** set by user ***

Support Mode-----
Status: inactive

(s) Start
    Start support mode
(b) Back
    Back to main menu
```

Schritt 4: Sie müssen sehen, dass der Status als **aktiv** angezeigt wird.

```
-----Cisco Secure Malware Analytics - Appliance Administration-----
Your Malware Analytics appliance can be managed at:
Admin URL / MAC:      https://[REDACTED]
Application URL / MAC: https://[REDACTED]
Password:            *** set by user ***

Support Mode-----
Status: active

(t) Stop
    Stop support mode
(b) Back
    Back to main menu
```

Anmerkung: In Situationen, in denen der Zugriff auf die Admin-Benutzeroberfläche oder die TGS-CLI nicht verfügbar ist, kann die Live Support Session auch im Appliance-Wiederherstellungsmodus aktiviert werden.