



Secure Remote Access

*Tom Ziegmann - Sr Solutions Engineer
@tziegmann on Slack*

May 19, 2021



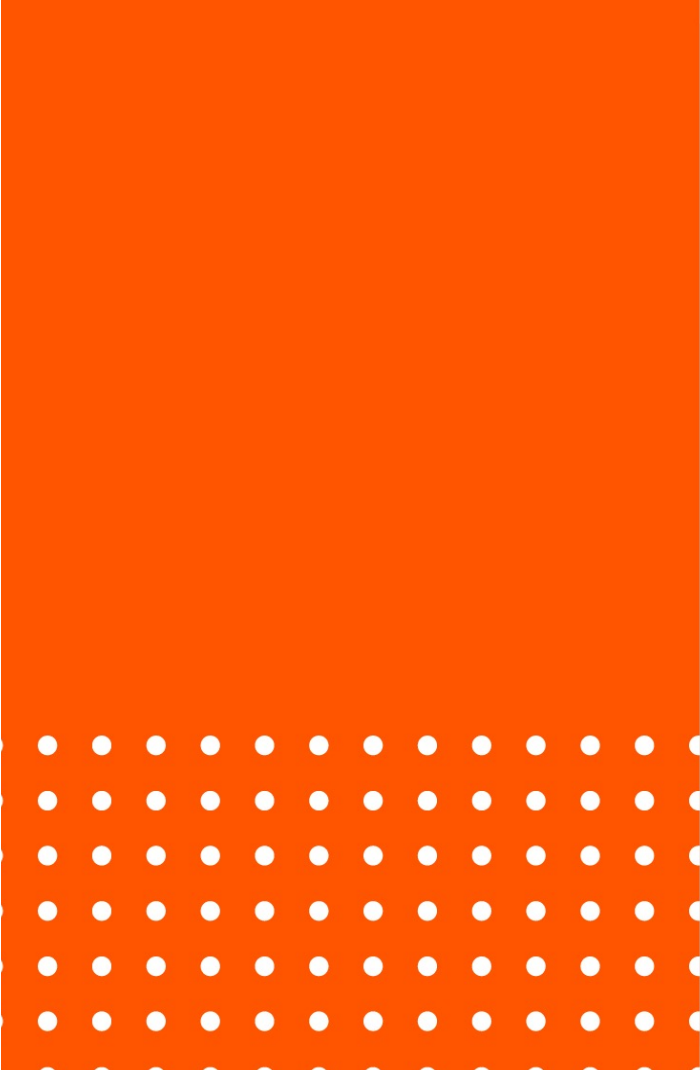
About Me

- Started as a Mac Admin in 2007 managing Mac labs in high school
- Joined full-time staff at Arizona State University in 2011
 - 535-seat all Mac facility supporting the Cronkite School of Journalism
 - Led initial Jamf implementation and support
 - ACMT – Does everyone remember CRT safety?
- Later owned Mac Client Engineering efforts at major insurance company
- Moved to InfoSec in 2013
 - ~5 years at McAfee as a consultant
 - ~18 months in at BeyondTrust as a Senior Solutions Engineer



<https://www.linkedin.com/in/tziegmann>



- 
- Introduce BeyondTrust
 - What's new in Remote Support
 - Jump Client Deep Dive
 - Active vs. Passive
 - Managing PPC
 - Deploying the Jump Client
 - Q&A



BeyondTrust

COMPANY OVERVIEW

- **1,000+** employees in **18** countries
- Founded in **2003**
- Headquartered in **Atlanta, GA**
- Privately held by **Francisco Partners**



Market Leader

Ranked as a PAM leader by Gartner, Forrester & KuppingerCole



Broadest Portfolio

Best-in-class products that cover the entire PAM journey



Global Presence

~20k customers in 100+ countries & an extensive partner network



Integrated Platform

Unified PAM platform with seamless third-party integrations



Customer Driven


















90%+ gross retention & exceptional customer support



Technology Pioneers

Heritage of innovation with 75+ patents & commitment to R&D

INNOVATIVE PRODUCT PORTFOLIO

Category	 Privileged Password Management		 Endpoint Privilege Management			 Secure Remote Access	
Products	 Password Safe	 DevOps Secrets Safe	 Privilege Management for Windows & Mac	 Privilege Management for Unix & Linux	 AD Bridge	 Privileged Remote Access	 Remote Support
Customer	Security IT Admins Compliance	Security DevOps Engineers	Security IT Operations Desktop Admins	Security IT Operations Server Admins	Security IT Operations Server Admins	Security IT Operations MSPs	Service Desk Support Centers
Capabilities	Password Vaulting Privileged Account & Session Management Auditing	Secrets Management & Security	Least Privilege & Advanced Application Control	Root Access Control Auditing & Governance for Unix/Linux	Extension of AD Authentication SSO to Unix/Linux	Session Management & Auditing for Remote & Vender Access Without VPN	Remote Support Screen Sharing Chat Support ITSM Integration
Deployment Options		 2021		 2021			

Feature parity between all on premises & cloud solutions



REMOTE SUPPORT 21.1

WHATS NEW

Overview – Remote Support 21.1

**CHATBOTS
INTEGRATION**

**OUTBOUND PROXY
CONNECTIVITY**

LINUX JUMPOINT

**CHROME BROWSER
SCREEN SHARING**

**MDM
INTEGRATIONS**

BASE TLS 1.3

**ASSOCIATE
CREDENTIALS WITH
AN ENDPOINT**

**VAULT ENCRYPTION
AWS SUPPORT**

**SCHEDULE
ROTATION OF
SUPPORTED ACC.**

Mac Support

What is it?

BeyondTrust has supported Mac OS X since 2007. And, unlike some remote support solutions that stop with basic support, BeyondTrust offers largely the same functionality for Mac as it does for Windows. With BeyondTrust, remote Mac support is integrated into all your other support systems and processes. In this release we have included:

- Mac Support Overlay
 - New overlay during a support session to address the configuration requirements in real time for macOS operating systems so they can be supported and controlled. This new help menu is for guiding end users to the correct location so that the required task as part of the support function can be enabled or disabled.
- MacOS Big Sur Support
 - The macOS Representative Console and the Customer Client now fully support macOS Big Sur, including changes to support its new security requirements. The Apple Silicon architecture is also supported through Apple's Rosetta 2 technology.

Copy Jump Items

What is it?

Today, admins and users must create new Jump Items in order to provide access to multiple Jump Groups, or to associate different Session Policies with each Jump Item. This is especially problematic for Jump Clients, as this requires separate Jump Client installations for each use case.

Technical Summary

Jump Items can now be copied and can belong to multiple Jump Groups. This new functionality does include Jump Client items, providing administrators with the ability to set separate policies and group permissions without requiring an additional Jump Client installation on the target endpoint.

Raspberry Pi OS Support

What is it?

BeyondTrust Remote Support enables Raspberry Pi secure access to allow privileged users to connect to more types of unattended systems, perform administrative actions, and secure who has access to manage these devices.

Technical Summary

32-bit only. RPi4 is the only version that supports 64-bit, but the current recommendation is that you install the 32-bit RPi OS unless you truly have something 64-bit specific.

Not a Vault User Yet?

VAULT IS INCLUDED WITH REMOTE SUPPORT

**CREDENTIAL
DISCOVERY**

**CREDENTIAL
MASKING**

**CREDENTIAL
ROTATION**

**CREDENTIAL
INJECTION**

**AUDIT
&
COMPLIANCE**

**CHECK IN
&
CHECK OUT**



Jump Clients

Enables technician-initiated support of end-users

Active

- Maintains a persistent connection to appliance
- Sends system statistics at regular interval (default – hourly)
- Number of Active clients limited only by resources
 - B200 / Virtual Appliance (small) – up to 1,000
 - B300 / Virtual Appliance (medium) – up to 10,000
 - B400 / Virtual Appliance (large) – up to 50,000
 - Cloud – 150 per Technician license
 - Add'l jump clients, sold separately – speak to account team for more detail

Passive

- Listens for an inbound access request from the appliance
- Sends system statistics once per day
- 50,000 passive Jump Clients supported on all models
 - Passive Jump Clients are not supported in BeyondTrust Cloud deployments

Jump Client Notes

- Installed to ***/Applications/.com.bomgar.scc.{random 8-char ID}/***
- LaunchDaemon created in ***/Library/LaunchDaemons/com.bomgar.scc.{random 8-char ID}.xxx.plist***
- For ad-hoc / customer-initiated sessions, installed to ***/Users/Shared/.com.bomgar.scc.{random 8-char ID}/*** and removed after the session has ended
 - To ensure session survives a reboot, a launchagent is created in ***~/Library/LaunchAgents/ (non-elevated) or /Library/LaunchAgents (elevated)*** and removed after session has ended

Managing PPC Settings

- New client overlay added in Remote Support 21.1
 - Will prompt user to grant **Accessibility**, **Screen Recording**, and **Full Disk Access**
- Permissions can be managed via MDM profile
 - **Screen Recording (ScreenCapture)** – Needed for **Screen Sharing**
 - **Big Sur** – “Allow Standard User to Set” can be granted to enable non-admins to grant permission
 - **Accessibility** – Needed for **Screen Sharing**
 - **Full Disk Access** – Needed for **File Transfer**

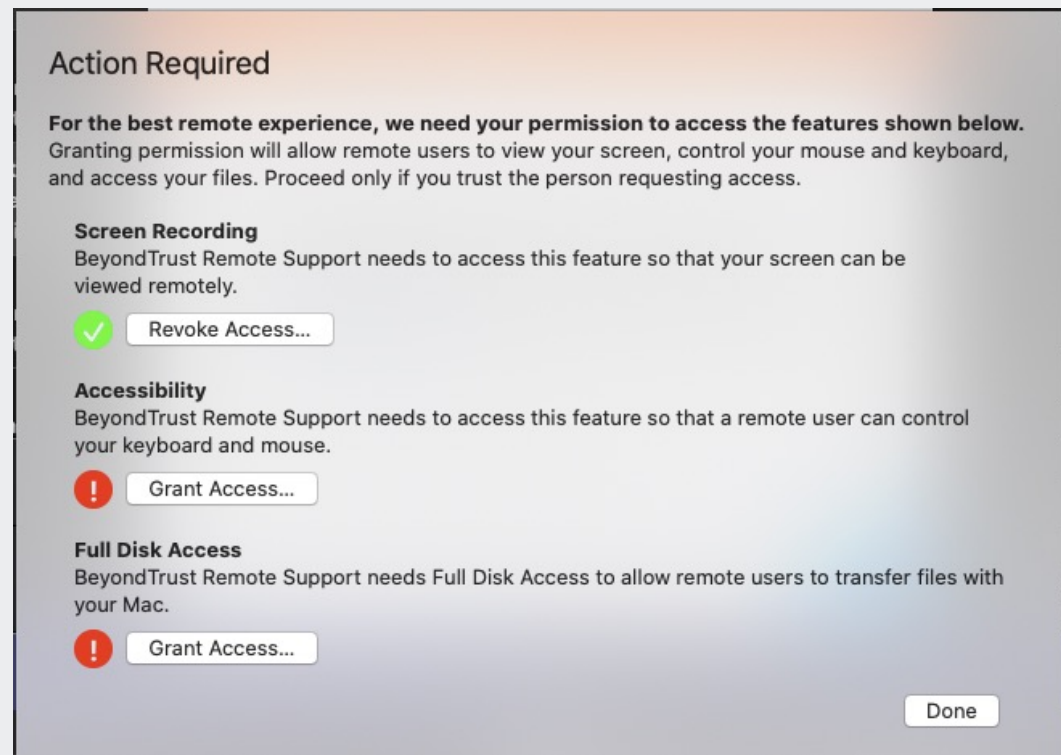
Identifier: com.bomgar.bomgar-scc

Identifier Type: Bundle ID

Code Requirement: identifier "com.bomgar.bomgar-scc" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = B65TM49E24

Managing PPC Settings

New overlay in Remote Support 21.1 to guide user through granting PPC settings



Managing PPC Settings

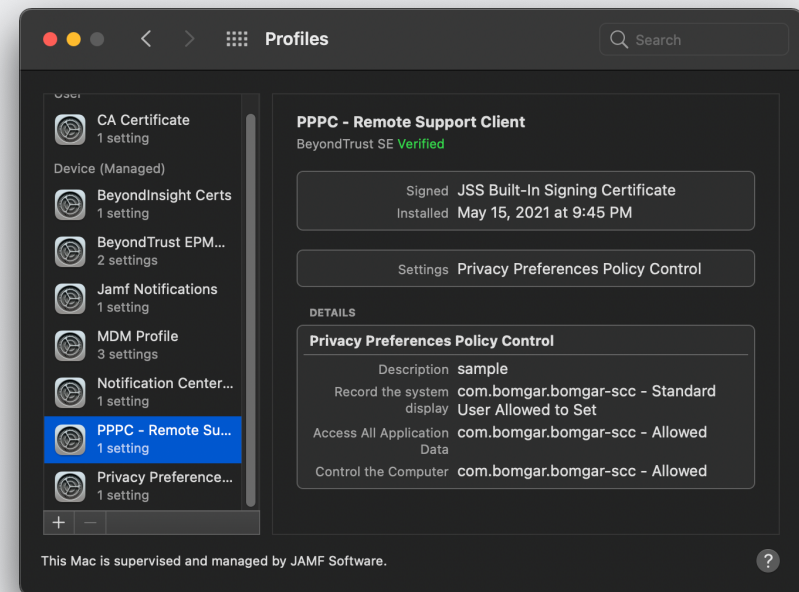
Identifier
com.bomgar.bomgar-scc

Identifier Type
Bundle ID

Code Requirement
Identifier "com.bomgar.bomgar-scc" and anchor apple generic and certificate "[field.1.2.840.113635.100.6.2.6]" exists "/" and certificate leaf[field.1.2.840.113635.100.6.1.13] "/" exists "/" and certificate leaf[subject.OU] = B65TM49E24

☐ Validate the Static Code Requirement

APP OR SERVICE	ACCESS		
Accessibility	Allow	Edit	Delete
SystemPolicyAllFiles	Allow	Edit	Delete
ScreenCapture	Allow Standard Users to Allow Access	Edit	Delete



Deploying the Jump Client

**CREATE JUMP
CLIENT INSTALLER**

IMPORT INTO MDM

**CACHE AND
INSTALL JUMP
CLIENT DMG**

Deploying the Jump Client

Create Jump Client Installer

- From **/login** interface -> **Jump** -> **Jump Clients**
 - **TIP:** Jump Client installers inherit the Jump Group permissions of the user who created the installer. Ensure the **Manage** permission is applied to each jump group that a user should be able to add new clients to
- Check the **Allow Override during installation** box to add flexibility during install to specify parameters
 - --jc-jump-group
 - --jc-session-policy-present
 - --jc-session-policy-not-present
- Installers are valid for the length of time specified or until the appliance is upgraded, whichever comes first
 - **TIP:** The jump client installer does not require connectivity to the appliance at install, but must connect at least once prior to the expiry time specified on the installer

Jump Clients

Jump Group

Team A ▼

☒ Allow Override During Installation

Name

☒ Allow Override During Installation

Jump Policy

None ▼

☒ Allow Override During Installation

Jumpoint Proxy

None ▼

Currently, none of your Jumpoints have proxying enabled.

☒ Attempt an Elevated Install If the Client Supports It

Password

Create

This Installer Is Valid For

1 Day ▼

Comments

☒ Allow Override During Installation

Customer Present Session Policy

Jump Client: Do Not Prompt for Screen Sharing ▼

☒ Allow Override During Installation

☒ Prompt for Elevation Credentials If Needed

Confirm Password

Public Portal

Default: tziegmann.beyondtrustcloud.com ▼

☒ Allow Override During Installation

Tag

☒ Allow Override During Installation

Customer Not Present Session Policy

Jump Client: Do Not Prompt for Screen Sharing ▼

☒ Allow Override During Installation

☒ Start Customer Client Minimized When Session Is Started

Deploying the Jump Client

Import into MDM

- Download the **MacOS (for programmatic execution)** DMG
 - File will be named **bomgar-scc-<uuid>.dmg**
 - **TIP:** Do not rename the DMG. The string on the end is used by the client at run-time
- Upload into Jamf, Munki repo, etc. following vendor process
- Because we need to call **sdcust** binary located inside the app bundle, the installation must be scripted to run after the DMG is cached to system
 - Basic sample script shown, there are many examples in the #bomgar channel on Slack
- Once installed, Jump Client will automatically update each time the appliance is updated

Computers : Policies

← BeyondTrust Remote Support Jump Client 21.1.2

Options

Scope

Self Service

User Interaction

Packages

1 Package

Software Updates

Not Configured

Scripts

1 Script

Printers

0 Printers

Disk Encryption

Not Configured

Dock Items

0 Dock Items

Local Accounts

0 Accounts

Packages

Distribution Point

Distribution point to download the package(s) from

Each computer's default distribution point

bomgar-scc-w0edc30iiy68g8y1d5hifgiw8y5778jfx8x7xec40hc90.dmg

Action

Action to take on computers

Cache

☐ Fill user templates (FUT)

Fill new home directories with the contents of the home directory in the package's Users folder. Applies to D

☐ Fill existing user home directories (FEU)

Fill existing home directories with the contents of the home directory in the package's Users folder. Applies t

☐ Update Autorun data

Add or remove the package from each computer's Autorun data

Computers : Policies

← BeyondTrust Remote Support Jump Client 21.1.2

Options

Scope

Self Service

User Interaction

Software Updates

Not Configured

Scripts

1 Script

Printers

0 Printers

Disk Encryption

Not Configured

Dock Items

0 Dock Items

Local Accounts

0 Accounts

Management Accounts

Not Configured

Directory Bindings

Scripts

Remote Support Jump Client (Install Cached)

Priority

Priority to use for running the script in relation to other actions

After

Parameter Values

Values for script parameters. Parameters 1–3 are predefined as mount point, computer r

Parameter 4

Parameter 5

Parameter 6

Parameter 7

©BeyondTrust 2021 | 22

Deploying the Jump Client

Cache and Install

```
#!/bin/zsh
```

```
# Mount Remote Support DMG
```

```
hdiutil attach /Library/Application\ Support/JAMF/Waiting\ Room/bomgar-scc-<uuid>.dmg
```

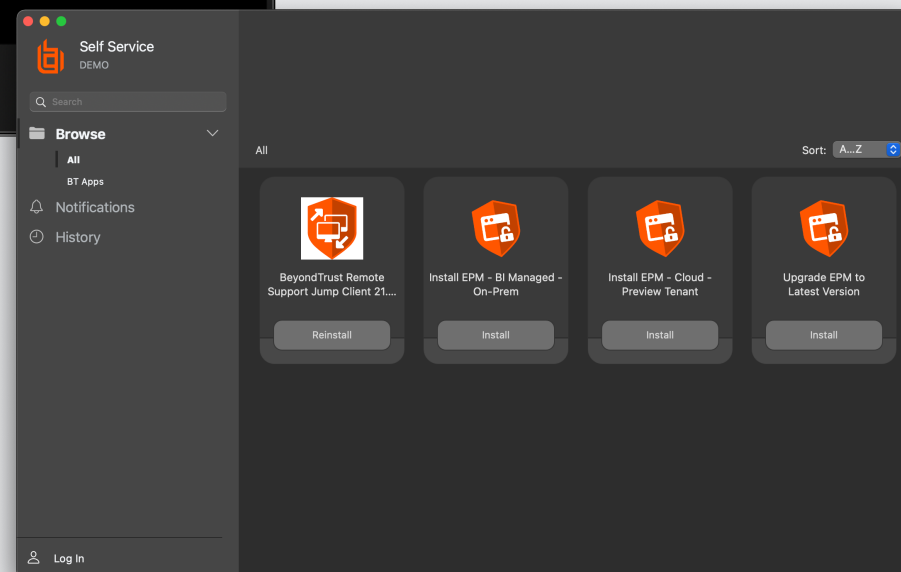
```
# Run sdcust to install Jump Client
```

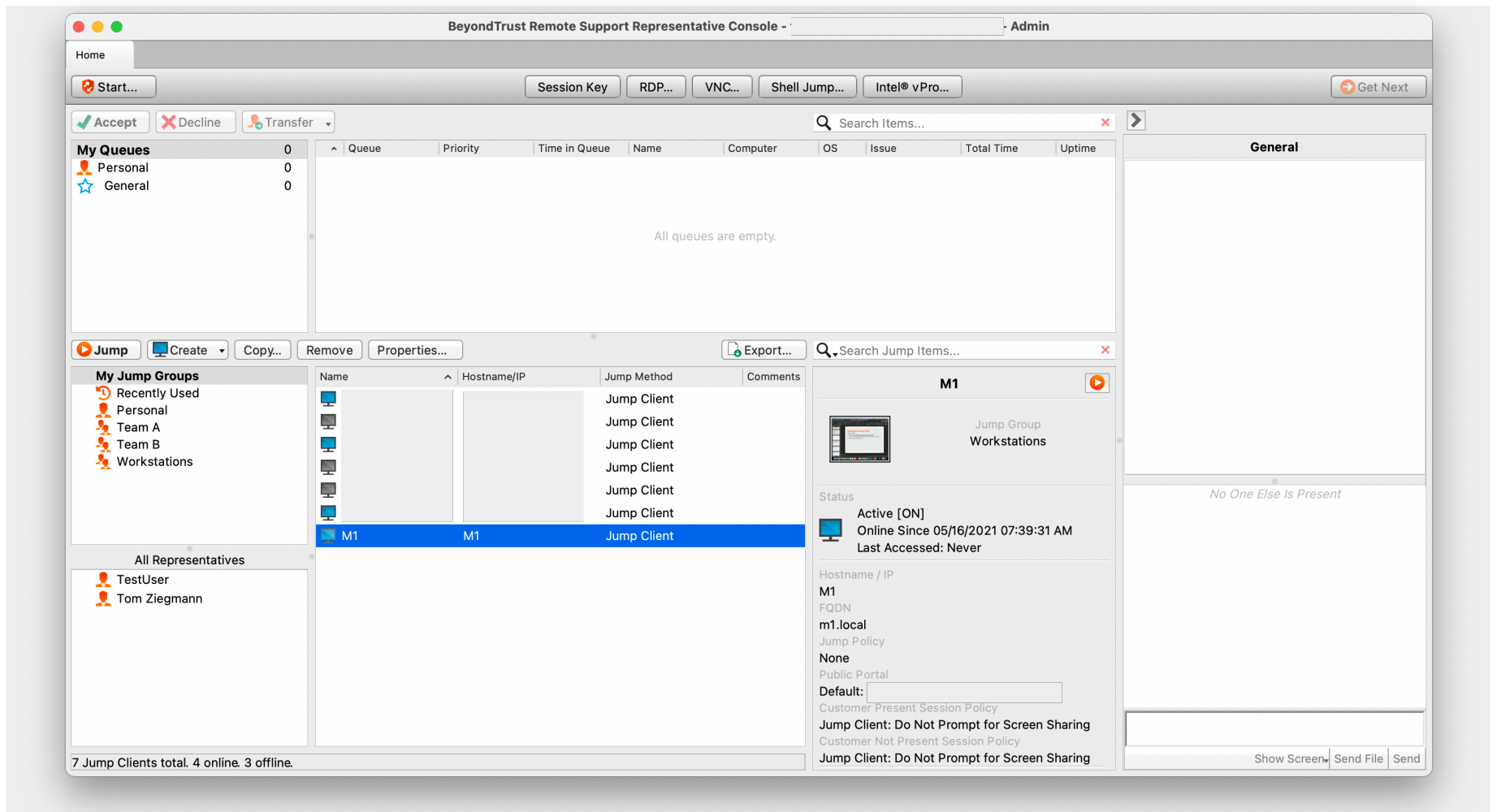
```
sudo /Volumes/bomgar-scc/Double\ -Click\ To\ Start\ Support\ Session.app/Contents/MacOS/sdcust --silent
```

```
# optional sleep to ensure DMG unmounted and install process complete
```

```
sleep 15
```

```
[redacted]@M1 Resources % sudo jamf policy -event installjump
Checking for policies triggered by "installjump" for user "[redacted]" ...
Executing Policy BeyondTrust Remote Support Jump Client 21.1.2
Caching package bomgar-scc-[redacted].dmg...
Downloading https://use1-jcde.services.jamfcloud.com/download/ed46bc3f714940f29d8c129264dbeb5c/bomgar-scc-[redacted].dmg
Verifying DMG...
Running script Remote Support Jump Client (Install Cached)...
```







Ask me Anything

The answer is always 42 😊



NEXT STEPS



Community

- Join #bomgar on Slack
 - [MacAdmins.org](https://macadmins.slack.com) – to sign up for MacAdmins Slack
- Attend a regional user group
 - Contact your account rep to be notified of upcoming events
- Join us at Go Beyond – June 7-11, 2021
 - <https://go.beyondtrust.com>

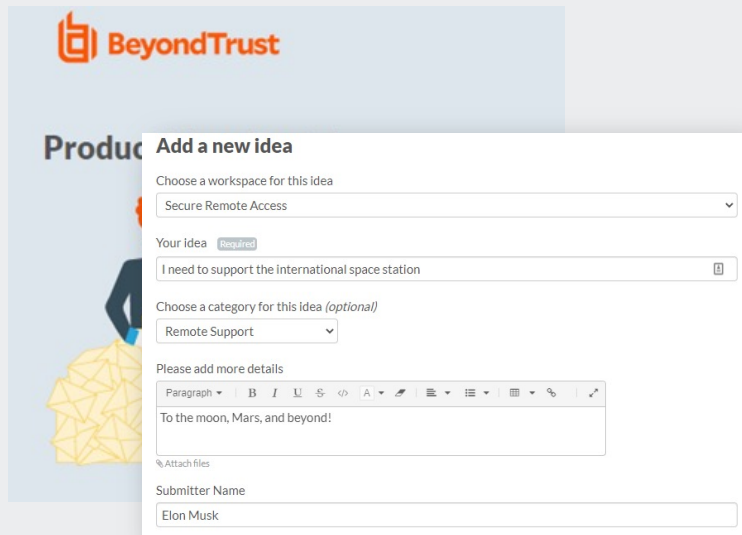


We Need NEW Ideas!

Got an idea?

Let your voice be heard at

ideas.beyondtrust.com



Want to get your hands dirty?

Be a part of the development process at

beyondtrust.com/user-research

