

# Privileged Remote Access 20.1.1 Release Notes

April 7, 2020

## Requirements:

- This version of Privileged Remote Access has been certified for physical BeyondTrust Appliances, virtual BeyondTrust Appliances, and cloud deployment models.
- This release requires Base software Base 5.5.0.

## New Features and Enhancements:

- Added RDP Session Forensics, which provides administrators with additional logging details for RDP Jump sessions.
- Added Bulk Credential Rotation, which allows users and administrators to rotate all credentials in a selected group of Vault credentials and rotate them with a single click.
- Increased the number of credentials shown to the user from 250 to 2000 during credential injection.
- Web Access Console users can now cancel Remote Jump and other start-session operations.
- Jump Authorization requests can now be canceled in the Web Access Console.
- **Jump Item Approver** has been added to the exported session reports.
- **Jump Request Reason** has been added to the exported session reports.
- The option to send invitation emails via client or server has been added.
- When viewing reports, the column headers are now fixed while scrolling.
- Session alerts are now logged with a unique ID and response per session alert.
- Added a toolbar button to allow copy and pasting of files and folders from RDP sessions to local Mac and Linux file systems.
- Microsoft Edge Chromium is now supported.
- Vault columns are now resizable:
  - Vault Discovery result columns are now resizable.
  - Vault Account list columns are now resizable.
- SCIM updates:
  - Added **User Activate** and **User Deactivate**.
  - **Delete User** has been updated to be a hard delete.
  - Deactivated users now display in **GET Users** API calls.
  - Deactivated users now get an appropriate message when attempting to login.

## Issues Resolved :

### Administrative Interface

- **Reporting**
  - Resolved a formatting issue that could cause some session reports downloaded in .xlsx format to display a warning when opened in Excel.
  - Resolved an issue in which non-admin users could not see the option to run Session Forensics reports.
  - Resolved an issue with downloading session reports that did not have an end time.

- **API**
  - API version increased to 1.19.2.
  - Resolved an issue with saving API permissions.
  - Resolved an issue with `/api/reporting` AccessSession report not always returning all of the sessions.
- **Security Providers**
  - Resolved an issue in which duplicated nodes within a clustered RADIUS provider were not displaying that the duplicated node was using external group lookup.
  - We now use the SCIM User provided displayName as the public\_display\_name.
- **Group Policies**
  - Resolved an issue with a link to the **Teams > Group Policy** page not opening a new browser tab.
  - Resolved an issue with the Group Policy list not scrolling while dragging a Group Policy.
  - Resolved an issue with editing Group Policies that had Vault accounts added to them during a Vault trial and the trial had expired.
- **Vault**
  - Resolved an issue with Discovery, in which it sometimes showed negative numbers when dealing with larger numbers of accounts.
- **Text Updates**
  - Updated the message for Teams filtering when *No users found*.
  - Resolved an issue with a link on the **What's New** page for an older release.
- **Miscellaneous**
  - Resolved an issue in which clicking links to session recordings required logging in, even when already authenticated.
  - Resolved an issue in which a user had only the permission **Allowed to edit Skills** being able to edit the skills, but was not able to view who had the skills.
  - Resolved an issue with the `/login` interface not behaving well when display scaling was set greater than 100%.

## Clients

- **Access Console**
  - When clicking on the key icon during screen sharing, a new dialog appears in place of the dropdown menu. This provides a better experience when selecting credentials from a large number of accounts.
  - Resolved an issue with the Video Optimized screen sharing setting altering the Show window Contents while dragging Performance Options setting.
  - Resolved an issue with injecting large character passwords.
  - Resolved an issue with a *Failure to display security and shut down options* window being displayed if a screen sharing session is ended while the lock screen is visible.
  - Resolved an issue with Jump Group sorting after renaming a Jump item tag.
  - Resolved an issue with abnormal behavior when using Microsoft RDP to connect to a remote machine, running the Access Console on that machine, and then starting a screen sharing session in that Access Console.

- **Customer Client**

- Resolved an issue with detecting *remote* sessions similar to VMWare View.
- Resolved an issue with starting Command Shell through the Access Console, causing the Customer Client to crash on some Windows 7 POSReady systems.

- **Web Access Console**

- Resolved an issue with the Jump Client version and Jump Client revision information not being displayed in the Web Access Console.
- Resolved an issue with the mouse's scroll wheel not working properly in the Web Access Console.
- Resolved an issue in which the verbiage of the Remote RDP Jump Items did not match the verbiage of the native Access Console.

- **Virtual Smart Card**

- Resolved an issue with Local Jump sessions timing out when VSC drivers were installed. Now we only check whether the VSC service is running, if it was determined to be installed.

- **VNC**

- Resolved an issue with connecting to a VNC server by disabling unused extensions.

- **Web Jump**

- Resolved an issue with injecting credentials through Web Jump to sites that use older frames.
- Resolved an issue with drag and drop during Web Jump sessions.
- Resolved an issue with Web Jump injecting credentials where there were multiple authorization prompts.
- Resolved an issue to allow popup windows to be closed without ending the session, thus taking the user back to the original page.
- Adobe Flash has been deprecated in Web Jump and will be removed in a future release.
- Resolved an issue with Web Jump sometimes not showing **Username** and **Password** fields when authentication is requested.

- **Jumpoint**

- Resolved an issue with Bad Password counts sometimes getting incremented more than once during a failed authentication attempt.

- **Shell Jump**

- Resolved an issue in which recording Protocol Jump sessions caused the text to be thin and sometimes unreadable.
- Resolved an issue in which users were removed from session while still in Protocol Tunneling sessions.

- **Mac**

- Resolved an issue in which Access Console was interfering with the Dock and Menu bar on Macs.
- Resolved an issue in which the Customer Client was crashing when starting screen sharing on macOS 10.13 and macOS 10.14.
- Resolved an issue in which the Jump Client menu bars displayed only sometimes on Mac login screens.
- Resolved an issue in which Admin prompts appeared on top of the Privacy Screen on Macs.

- **RDP**

- New Remote Desktop Agent installer. This new Remote Desktop Agent must be installed for RDP SecureApp Jumps to work properly. This Remote Desktop Agent installer also moves all *Bomgar* related files/directories/registry entries to *BeyondTrust* named files/directories/registry entries.

- **Linux**
  - Resolved an issue with using **sudo** in a command shell in a Linux Service Mode session.
  - Resolved an issue with starting an RDP session from a Linux user to a Windows target.
- **Miscellaneous**
  - Resolved an issue in which messages were being repeatedly sent to the ECM. Now the messages will stop sending after twenty-four hours.
  - Resolved an issue in which the endpoint domain/FQDN was not being sent to the ECM.

**Known Issues:**

- Session times out when attempting to Remote RDP to a Windows 10 1903 endpoint when the **Session Forensics** box is checked and the **Ignore Untrusted Certificate** box is unchecked.
- Older Remote Desktop Agent installs do not work with the new Jumpoint, and no error message is displayed. The Remote Desktop Agent must be manually updated to use this feature.
- RDP Session Forensics session will fail if you attempt to connect over RDP to the machine that is running the Jumpoint initiating the session (i.e. localhost).

**Notes:**

- Supports upgrades from Privileged Remote Access 18.3.3+.
- Supports ThinClient Protocol 2.1 and 2.2.
- Requires Integration Client 1.7.2.
- Requires Endpoint Credential Manager (ECM) 1.5.0.
- Supports ECM Protocol 1.5.
- This release is certified with the following mobile versions:
  - [iOS Access Console 2.2.4+](#)
  - [Android Access Console 2.2.4+](#)
  - [Android Unattended Access Client 2.2.0+](#)