SonicWall Capture Client 3.6

Release Notes

These release notes provide information about the SonicWall (Capture Client) 3.6 release.

Versions:

Version 3.6

May 2021

Important

If some software applications have interoperability issues with Capture Client and SentinelOne, you can work around those issues by creating an exclusion and pushing it to the clients. For more information, refer to Capture Client Inter-Operability With Third Party Applications.

Compatibility and Installation Notes

Refer to Capture Client - System Requirements for the latest information on hardware requirements, operating systems, and browser levels.

What's New

- Filtering can be performed based on pending actions for devices.
- A new **Device Alert** option is available in the **Notification Settings**. Notification is provided if reboot is pending for a device for more than a defined number of days.
- The **Analyst Verdict** option can be used to mark threats as **True Positive**, **False Positive**, **Suspicious**, and **Undefined**.
- A new option in the **Notification Settings** allows you to send email in plain text format.
- Capture Client supports macOS client with System Extensions (Big Sur or later) - for Intel chip set only.

Resolved Issues

Issue ID	Issue Description
UC-4902	Console-OneDrive KFM mapping fails when S1 is installed with default decoydocs option
UC-4894	Clickjacking vulnerability for the URL *https://captureclient.sonicwall.com/login*.
UC-4861	OpenSSL 1.1.1 versions are vulnerable to the denial of service and the users should upgrade to OpenSSL 1.1.1k.
UC-4839	OneDrive KFM mapping fails when S1 is installed with default decoydocs option
UC-4816	Adding a device to a Static group does not remove it from other static groups.
UC-4750	Threats page in Account Scope does not load threats and throws error.
UC-4736	The requested URL returns error: "404 Not Found". S1 4.1.6.118 installer is missing.
UC-4732	A change in the date or time on the system triggers license expiry and uninstalling the client.
UC-4702	Allow adding the domain in pattern "xyz.com" for web content filtering.
UC-4677	Threat Report does not contain a Custom Logo.
UC-4676	Schedule Reports are getting stuck endlessly.
UC-4674	Discrepancy in the count of Vulnerable Applications on Dashboard.
UC-4673	Discrepancy in the count of Offline Devices on Dashboard.
UC-4667	List View under Assest/Devices has pagination issues.
UC-4604	Wild Cards Entry are not allowed for Allowed/Forbidden domains.
UC-4603	In the Global Dashboard, the threats in the section Most Recent Detection are not sorted in the proper order.
UC-4602	Resolved threats are getting displayed in the global dashboard under the section Most Recent Detection.
UC-4572	Issues with trusted certificate policy (zero certificates found/No trusted certificates updated).
UC-4345	The CC portal displays duplicate device entries for the client PC.
UC-4306	Location Information is displayed blank in Assets->Devices page in Prod server 35.
UC-4303	Device Status is displayed as Connecting after the fresh installation of CC 3.5.18 in Prod server 35.
UC-4289	Duplicate device entries for multiple devices in CMC.
UC-4225	The capture client goes into a connecting state, as shown in the below screenshot, when DPI SSL Enforcement is enabled in firewall.
UC-4165	S1 upgrade fails from version 3.6.6.104 to 4.1.5.97 for windows 32 bit Operating System.
UC-4157	Windows Cleaner Utility do not work for Windows 10 32 bit operating system.
UC-4133	In CMC Devices page, the Network protection field shows "SonicWall firewall not detected" for devices behind the firewall.
UC-4084	Tenant License Count and Expiry Date updates from MSW are frequently failing.
UC-4056	Request fails intermittently with the status code 502 on multiple pages on CC Portal.

Issue ID	Issue Description
UC-3796	The CATP report does not display verdict for suspicious files on CMC
UC-3791	Initiate Scan is not working for the Linux devices.
UC-3737	Some email notifications do not have the Device Name
UC-3695	The newly created policies and the Default Threat Protection Policies displays error "Sentinel Policy not found".
UC-3521	The Reports are getting stuck.
UC-3398	Native Application works only when both WFE && WCF are disabled, though the Exclusion for Native Application exists.
UC-3062	Threat notification email does not include the device information.
UC-3042	Major Alert Emails do not include the Machine Name.

Known Issues

Issue ID	Issue Description
UC-5054	Endpoint requires a reboot to enable WCF on MacOS
UC-5050	Device Control Rules do not block the Devices on MacOS.
UC-5044	A wrong prompt is displayed after installing S1 in system preferences. on Fresh Catalina operating system.
UC-5003	The FILE FETCH filter checkbox should not be available for version 3.6.
UC-4909	The **Search** field in **Assets > Devices** page is not working as expected
UC-4815	Safe search is making internal resources inaccessible through VPN
UC-3263	CC and S1 upgrades are not working based on the schedules
UC-3142	Network protection status of CC UI is not reflecting under CMC when the Endpoint is behind the firewall.