SonicWall® Capture Client 3.1.4

Release Notes

January 2021

These release notes provide information about SonicWall® Capture Client 3.1.4 release. Capture Client 3.1.4 is a maintenance release that resolves issues from previous versions.

NOTE: Existing Capture Client implementations are not automatically updated. You need to actively update your Capture Client policy and select the appropriate version for your configuration.

To update Capture Client:

1. Navigate to **Security Policies > Capture Client**.
2. Hover over the Capture Client policy.
3. Click **Edit**.
4. Select the **Settings** tab and choose the **Capture Client version** from the drop-down list.
5. Click **Update**.

Topics:

About Capture Client

SonicWall Capture Client is a unified client offering that delivers multiple client protection capabilities through a unified interface. With a next-generation malware protection engine powered by SentinelOne, the SonicWall Capture Client delivers advanced threat protection with these key features:

- **Continuous behavioral monitoring** of end users that helps create a complete profile of file activity, application, and process activity, and network activity. This protects against both file-based and fileless malware, delivering a 360° attack view with actionable intelligence relevant for investigations.
- **Multiple layered signatureless techniques** include techniques for protecting cloud intelligence, advanced static analysis and dynamic behavioral protection. They help protect against and remediate well known, little known, and even unknown malware, without regular scans or periodic updates. This maintains the highest level of protection at all times, without hampering user productivity.
- **Unique roll-back capabilities** support policies that not only remove the threat completely but also restore a targeted client to its original state, before the malware activity started. This removes the effort of manual restoration in the case of ransomware and similar attacks.

- **Cloud-based management console** reduces the footprint and overhead of management. It improves the deployability and enforceability of endpoint protection, irrespective of where the endpoint is.

The size of your Capture Client tenancy is only limited by the number of endpoint licenses procured.

System Requirements

Capture Client is a comprehensive endpoint security solution that protects Windows and macOS devices. It is administered from the SonicWall Cloud Management Console, a cloud service requiring only a web browser and an internet connection. To get maximum performance and protection, the following standards are recommended:

- Minimum Hardware Requirements
- Supported Operating Systems
- Installation Notes
- Browser Levels
- Third Party Software Interoperability

Minimum Hardware Requirements

To install Capture Client on a PC or Mac, the device must meet the following hardware requirements:

Specification	Minimum	Recommended
CPU requirements	1 GHz or better	Dual-core processor is recommended. Beginning with Capture Client 1.0.24 for Windows and macOS, you can install on a single-core CPU, but performance is not optimal.
Memory requirements	1 GB RAM or more	3 GB RAM is recommended
Storage requirements	2 GB free disk space on the Windows partition.	

To install Capture Client on a system running Linux, the device must meet the following hardware requirements:

Specification	Minimum	Recommended
CPU requirements	1 GHz or better	Dual-core processor is recommended.
SSE4.x instruction support CPU	**NOTE:** Some virtual environments mask support for advanced CPU capabilities. See your VM vendor documentation.	
Memory requirements	1 GB RAM or more	2 GB RAM is recommended.
Storage requirements	1 GB free disk space	3 GB in /opt/sentinelone

Supported Operating Systems

Capture Client supports endpoints (PCs, laptops, tablets, and other devices) running the following operating systems. Capture Client's advanced threat protection is powered by SentinelOne, and the SentinelOne agent is automatically installed and configured according to the Threat Protection security policy. The recommended SentinelOne agent version is listed below.

Operating System	Version	Preferred SentinelOne Agent
Windows Operating System		
Windows Server	2019 2016 2012 R2, 2012 2008 R2	4.0.4.81 or later is preferred for all Windows versions listed here.
Windows 10	32- and 64-bit Windows 10 RS5 on 32- and 64-bit	
Windows 8	Version 8.1 on 32- and 64-bit	
Windows 7	Version 7 SP1 on 32- and 64-bit	
mac Operating System		
macOS 10.15.4	Catalina	4.0.3.3085 or later
macOS 10.14 and newer up to 10.14.6	Mojave	4.0.3.3085 or later
macOS 10.13 or later	High Sierra	4.0.3.3085 or later
macOS 10.12	Sierra	4.0.3.3085 or later
Linux Operating Systems		
Amazon Linux	2018.03 2017.03 AMI 2	4.0.3.11
Red Hat Enterprise Linux (RHEL)	8 7.x 6.4+	4.0.3.11
Ubuntu	19.04, 19.10 18.04 16.04 14.04	4.0.3.11
CentOS	7.x 6.4+	4.0.3.11
Oracle Linux (OL) (formerly known as Oracle Enterprise Linux or OEL)	7.x 6.9, 6.10	4.0.3.11
SUSE Linux	Enterprise Server 12	4.0.3.11
Fedora	25, 26, 27, 28, 29, 30	4.0.3.11
Debian	8, 9, 10	4.0.3.11
Virtuozzo	7	4.0.3.11
SELinux		4.0.3.11
Scientific Linux	7 6	4.0.3.11

Installation Notes

To ensure Capture Client operates effectively, the following guidelines are recommended:

- To understand version compatibility between Capture Client and the SentinelOne agents, refer to the knowledge base article SentinelOne Agent Version Availability with SonicWall Capture Client. This also includes information on new features and resolved issues for each SentinelOne agent.
- All agents running on Windows that are supported according to SentinelOne's life cycle are tested for compatibility with each Windows 10 Redstone release. Supported editions of Windows 7, 8, 8.1 and 10 include Home, Pro, Pro for Workstations, Enterprise, Education, Pro Education, and Enterprise LTSC. Core and Mobile editions are not supported.
- Due to Apple Notarization requirements, macOS 10.15 up to 10.15.2 requires Capture Client 2.0.20 or later and SentinelOne 3.2.1.2800 or later. macOS 10.15.3 or later requires SentinelOne 3.6.1.2964 or later to be installed before upgrading macOS to 10.15.3.
- The SentinelOne macOS 2.6.3 or later is required for macOS Mojave. An existing SentinelOne 2.6.2 or 2.6.0 version must be upgraded to 2.6.3 or later, before upgrading to macOS Mojave.
- macOS 10.14.5 or later requires Capture Client 2.0.10 or later and SentinelOne 3.0.4 or later due to Apple Notarization requirements.
- SELinux OS policies have preference over Sentinel One agent functionality.
- .NET Framework 4.0 or later needs to be installed. For Windows 7 and Windows 2008 R2, you may be prompted for .NET 4.0 to be installed.
- On Windows 7, install the update to enable TLS 1.1 and TLS 1.2 as the default secure protocols in WinHTTP in Windows. Add the registry subkey. These options are not supported in the default Windows 7 installation.
- For Windows 7 SP1 and Windows Server 2008 R2, the Microsoft Security Advisory 3033929, https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3033929, must be installed to meet the minimum requirements for the Capture Client installer. It provides SHA-2 Code Signing Support.
- When the following Microsoft Security Updates are installed, you must restart the endpoint and run the Agent installation again.
    - Update 2758857 for Windows 7 and Windows Server 2008 R2 (https://www.microsoft.com/en-us/download/details.aspx?id=35973)
- Configure Microsoft Windows Volume Shadow Copy Service (VSS) before you install the agent. More information is available in this knowledgebase article: https://www.sonicwall.com/support/knowledge-base/configuring-windows-vss-for-rollback/180614060954053/.

Browser Levels

Based on the operating system you are using, the following browser levels are supported.

NOTE: These browser levels apply to the browser running the Cloud Management Console.

Browser Supported	Windows Server	Windows 10	Windows 8	Windows 7	Vista	Linux	macOS
Internet Explorer 11	✓	✓	✓	✓			
Microsoft Edge (latest version)	✓	✓					
Mozilla Firefox (version 52.5 ESR or later)	✓	✓	✓	✓	✓	✓	✓
Google Chrome (latest version)	✓	✓	✓	✓	✓	✓	✓
Apple Safari (latest version)							✓

Third Party Software Interoperability

Some software applications are known to have interoperability issues with Capture Client and SentinelOne. You can work around these issues by creating an exclusion and pushing it to the clients. Refer to this knowledge base article for more information: https://www.sonicwall.com/support/knowledge-base/180514100738172/.

Resolved Issues

This section provides a list of issues resolved in this release.

Resolved issue	Issue ID
Malicious activity was detected in the endpoint interface, but the threat details are not showing up in CMC Console.	UC-4393
User search does not return desired results when trying to add a specific user to the CC policy.	UC-4226
Device Not Found error is seen when **View Threat Details** of endpoints is invoked.	UC-4102
Request failed with status code 502/504 seen on multiple pages Intermittently.	UC-4056
Sometimes the following error is shown: **Sentinel One policy not found. It might not be possible to edit this policy at the moment**.	UC-3965
One of the reports is getting stuck and never made available.	UC-3521
The Capture Client tenant exists in mySonicWall, but not in the Capture Client portal. Capture Client tenant provisioning failed.	UC-3440
While marking threats resolved, an alert is shown indicating the change affects too many objects, even though only a few threats were selected.	UC-3347
When adding a new Threat Prevention policy or adding a File Exclusion or Path Exclusion on the CMC, the system sometimes shows a communication error with SentinelOne.	UC-3342
Autodesk AutoCAD 2020/2021 only works by disabling both WFE and WCF even though the exclusion for AutoCAD exists.	UC-3341
A web content filter safe search is blocking access to Microsoft Direct Access.	UC-3340

Resolved issue	Issue ID
Unable to add a device to a group and unable to add a user to policy, followed by an error that the request failed with status code 504.	UC-3339
Threat Details Page is not getting loaded; the page getting stuck and keeps loading infinitely.	UC-3337
While editing a Capture Client policy, the action to View Threat Details failed with status code **Device Not Found**.	UC-3276
Vulnerable Applications details are not available on the reports. The following error occurred: **Generation of this section has been interrupted**.	UC-3257
While downloading threat data in csv format, the request failed with status code 404.	UC-3249
Unable to download the CSV threat data file.	UC-3199
User notifications are not being delivered when threats are detected on an endpoint and the threat detection count is greater than 50.	UC-3136
When CC is uninstalled from MacOS 10.14.x, the system returns an error on one of the library extensions.	UC-3121
Duplicate device entires appear in the CMC for multiple devices.	UC-3075

Known Issues

This section provides a list of known issues in this release.

NOTE: The **Upgrade Client** option doesn't work if the endpoint device is enforced with either the default/custom client policy and the endpoint Capture Client version is less than 3.x.

Known issue	Issue ID
The function **Trust Certificates** in Firefox certificate store is not adding certificates in the Firefox store.	UC-4575
Email notification for **Offline Device** is not being sent.	UC-4511
Network Protection status is showing **Unknown** in exported CSV from the **Protection > Devices** page on the CMC.	UC-4480
Scan status shows the date as **Invalid Date** in **Devices > Overview** tab for the Scan started, in progress, aborted, and completed.	UC-4421
On the **Devices > World Map**, the **Device Status** and **Network Status** shows as **Offline** (yellow) **and Unavailable** even when the device is active in **All Tenants View**.	UC-4391
The Console version is showing as 3.1.0 in the Capture Client Report where the CMC version is listed as 3.1.1(10900).	UC-3301
Capture Client Reports do not show all of the Device List.	UC-3258
Vulnerable Applications details are not available on report. When an error occurred, generation of this section was interrupted.	UC-3257
On Windows endpoints, file type exclusion functionality is not working for files with a **.exe** extension.	UC-3167
Network Protection status not is not being shown properly in CMC.	UC-3142
When checking the **SentinelOne Agent Version** under **Security Policies > Threat Protection**, the old Linux agent version is coming with latest Windows agent version, and the new Linux version is coming with an old Windows agent version.	UC-3105
The **Capture Client** tab in the **Upgrade Client** window is not grayed out after having the Latest version installed in endpoint.	UC-3092
Infected Device function on the **Dashboard** page is not working when **All Tenants** are selected.	UC-2897

Known issue	Issue ID
City is showing as **NA** in **Most Common Locations** section in **Devices** tab of **Overview > Statistics** page.	UC-2855
When generating the THREAT DETAILS report, an error occurs in Analysis section: **Generation of this section has been interrupted** and the error appears in Threat Report.	UC-2725
On Devices, **CURRENT USER** is showing as **none** for Linux devices.	UC-2665
Unable to add Devices to Dynamic group using rule as **Current City** as the current city information are not mentioned in device details page.	UC-2659
After clicking the reboot prompt in Windows 8.1 32-bit and Windows 2016 Server, the alert **No client policy has been found on device. The device should be updated.** is showing in the **Device Details** page on the CMC.	UC-2212
The Network Protection status in the **Summary** page of Capture Client interface displays **SonicWall Firewall Enforced** even though **Anti-Virus Enforcement** is disabled on **Zones**.	UC-2092
SentinelOne stays **Active** on endpoint after Capture Client gets automatically decommissioned.	UC-1965
The **Dock** icon is not removed for Capture Client after successful uninstall on Mac OS 10.14.x.	UC-1802

Licensing

SonicWall Capture Client can be licensed as a security service associated with a SonicWall network security appliance or as a standalone service without an associated appliance.

Topics:

Licensing with a Network Security Appliance

To license SonicWall Capture Client with a network security appliance:

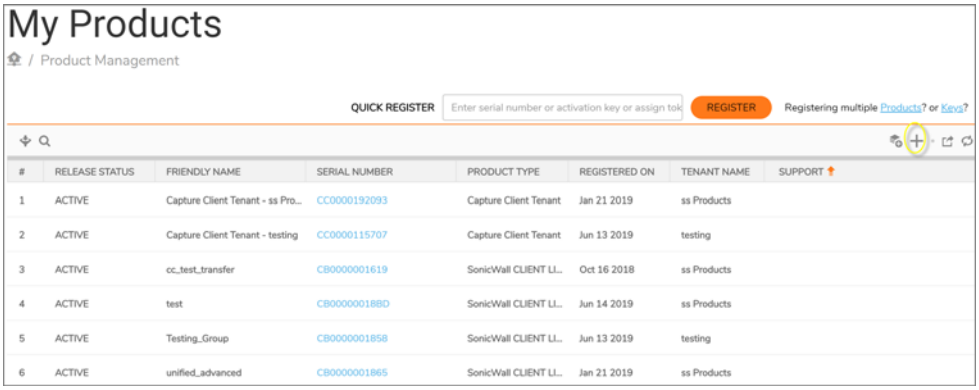
1. Log into your network security appliance as an administrator.
2. Navigate to the **MANAGE | Updates** > **Licenses** page.
3. In the pane to **Manage Security Services Online**, click the link to log into mySonicWall and activate the Capture Client license.
4. Click the **SYNCHRONIZE** button to synchronize all your licenses on the appliance.

Licensing without a Network Security Appliance

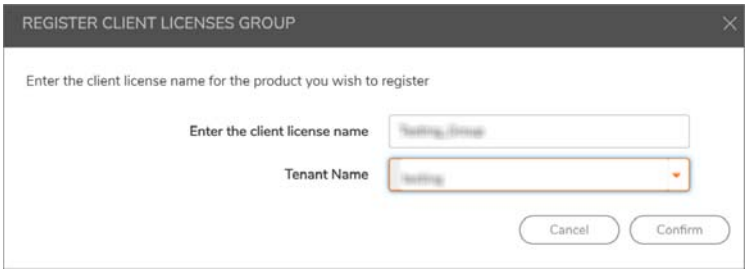
To provision Capture Client without a network security appliance:

1. Log into mySonicWall at https://www.mysonicwall.com/muir/login/step2.
2. Navigate to **Products Management > My Products**.

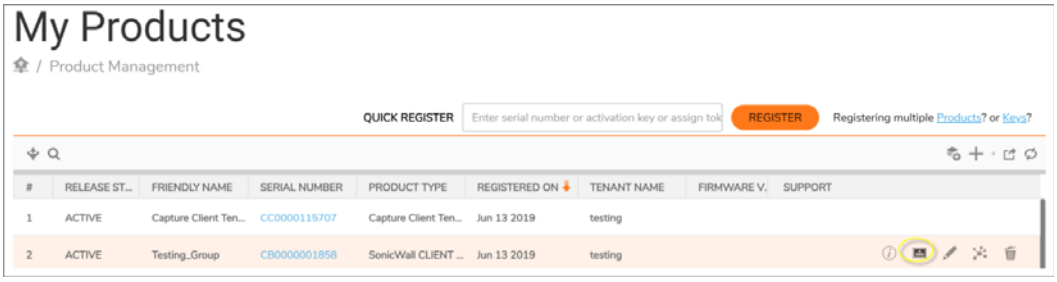
3 Click the **+** (**Add Client Licenses**) icon.



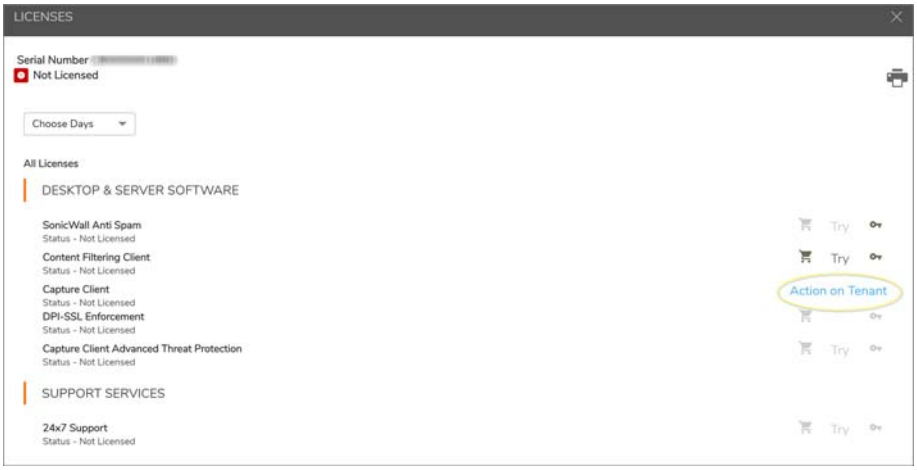
4 To register a client licenses group, **Enter the client license name**, select the appropriate **Tenant Name** from the drop-down list, and then click **Confirm**.



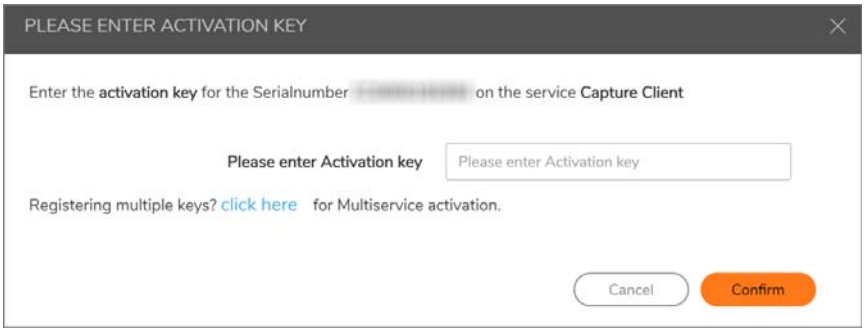
5 Click **Licenses** icon on the newly created client license in the table.



6 On the **LICENSES** page, scroll down to the **DESKTOP & SERVER SOFTWARE** section, find **Capture Client** in the list, and click **Action on Tenant**.



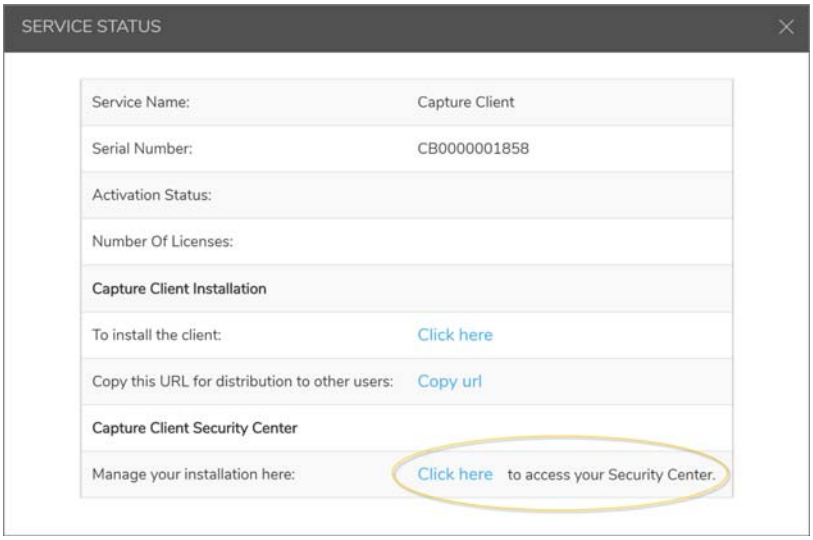
7 Enter the activation key if you have and click **Confirm**, or click **Cancel.**



8 Click the **Cart** icon to purchase a license for Capture Client, click **Try** for a free trial, or click the **Key** icon to activate your license with a key from your provider.

9 Once the server has been licensed, click on the **Service Status** icon.

10 Select **Click here to access your Security Center**. This redirects you to the Client Management Console for login.



Upgrading Information

When initially setting up your Capture Client implementation, you can opt for self-managed updates or SonicWall-managed updates. For the self-managed option, you control which version of the client get installed on your devices by manually updating the required client version in the Capture Client policy. If you choose SonicWall-managed under the Capture Client Policy, client systems are automatically upgraded when SonicWall releases and promotes a new version of Capture Client. Refer to the *Capture Client Operations Guide* for details on how to configure this.

NOTE: The **Upgrade Client** option is available beginning with the Capture Client 3.1.4 release. Customers running older versions should not try the **Upgrade Client** option.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- View video tutorials
- Access mySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 1/13/21

232-005573-00 Rev A