

SonicWall® Capture Client 1.5

Release Notes

October 2018

These release notes provide information about SonicWall® Capture Client 1.5 release. Capture Client 1.5 has new features and enhancements and resolves known issues found in prior releases. Refer to [New Features and Enhancements](#) and [Resolved Issues](#) for more details.

NOTE: Existing Capture Client 1.0.x clients are not automatically updated unless the Capture Client policy is changed to choose the 1.5.x version.

- [About Capture Client](#)
- [System Requirements](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Licensing](#)
- [SonicWall Support](#)

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 the client that helps create a complete profile of file activity, application & process activity, and network activity. This protects against both file-based and file-less malware and delivers 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

Since Capture Client is a cloud service, you only need access to a web browser and an internet connection to access the Client Management Console. Based on the operating system you're using, the following browser levels are supported:

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)							✓


Capture Client only supports endpoints (PCs, tablets, etc) running the following operating systems:

Operating System	Details
Windows Server	2016 2012 R2, 2012 2008 R2 SP1
Windows 10	On 32- and 64-bit
Windows 8	Versions 8 and 8.1 on 32- and 64-bit
Windows 7	Version 7 SP1 on 32- and 64-bit
macOS 10.13 or later	High Sierra
macOS 10.12	Sierra

New Features and Enhancements

Capture Client has been updated with several new features and enhancements to improve its client protection capabilities.

Capture ATP

 **IMPORTANT:** Capture ATP support is only available for Windows systems.

If licensed for Advanced Threat Protection, Capture ATP settings for threats and suspicious activities can be configured on the Client Management Console:

- 1 Log into the Client Management Console as an administrator.
- 2 Create or edit a threat protection policy.
- 3 Select **Protection Modes** tab.
- 4 In **Threats or Suspicious Activities** settings, select **Capture ATP (Auto-mitigation)** option.
- 5 Set the values for **Malicious Verdict**, **Not Malicious Verdict** or **Undetermined Verdict**. The options are:

Option	Values
Malicious Verdict	Kill and quarantine
	Remediate
	Rollback
No Malicious Verdict	Mark as Benign
	Detect (Alert only)
Undetermined Verdict	Detect (Alert only)
	Protect (Kill & Quarantine)

6 Click **Update**.

7 Verify that the changes are saved.

When the Capture ATP setting is changed, it applies to the client once the policy is updated on client side.

NOTE: The settings under Suspicious Activities are only applied to the Windows client as suspicious detection is only available for Windows client.

Administrator Alerts and Notifications

Additional alerts and notifications have been added to Capture Client. The system administrator can configure settings so that an email is sent when certain conditions are met. The following parameters can be set:

- Enable or disable notification for the tenant. This option must be enabled for the other settings to take affect.
- Enable or disable notification for alerts from SentinelOne.
- Enable or disable notification for Client Management Console alerts for errors and warnings,.
- Enable or disable notification for client device logs based on level of log entry (warning, error, and so forth).

NOTE: Only alerts having a priority of warning or higher are allowed to have notification configured.

Whitelisting Enhancements


The whitelisting feature has been enhanced so that processes can be added directly to or deleted from the whitelist. It also includes an exclusion to the global whitelist.

NOTE: Exclusions to the global whitelist may change the behavior of the clients connected to this tenant.

To add a process:

- 1 Navigate to **Protection > Devices**.
- 2 Click the **Option** icon (the gear icon) to the far right of the device name and select **View Details**.
- 3 Click on the **Processes** tab.
- 4 Select a process or set of processes.
- 5 Click on **Add paths to Exclusions** icon.
- 6 Verify that the processes were added to the global exclusions list by viewing **Configuration > Exclusions**.

To remove exclusions from whitelist:

- 1 Navigate to **Protection > Devices**.
- 2 Click the **Option** icon (the gear icon) to the far right of the device name and select **View Details**.
- 3 Click on the **Processes** tab.
- 4 Select a process or set of processes to remove.
- 5 Click on the Settings tab and select **Remove Paths to Exclusions** icon.

- 6 Verify that the processes are removed from the global whitelist by viewing **Configuration > Exclusions**.

Improved Static and Dynamic Group Management

The **Group** section (at **Protect > People > Groups**) has been completely refurbished to make a better distinction between static groups (which contains a static list of devices) and dynamic groups (where devices are added or removed based on rules). You can create a new static or dynamic list by clicking the + sign and adding users directly to the group. You can also create rules directly for the dynamic groups. Rules for static groups are disabled by default, but you can redefine a static group as a dynamic group. Select **Make dynamic** on the **Rules** tab at **Protection > People**.

Device Threat Integration

This feature adds links on the Threat page to the device that is infected by a threat. Navigate to **Protection > Devices** to see the infected device; it is displayed with the highest severity icon (red). Expand the row of the infected device to see the number of threats detected. Click on the threat to see the details.

Threat Notice

Whenever threats are detected on the user endpoints, a notice is displayed to the system administrator and to the user of the device. Alerts can be detected on mac OSX, Windows 10 or Windows 7.

Firefox Support for Trusted Certificates

The Trusted Certificates option has been enhanced for using Firefox. You can set the options so that certificates can be added to the Firefox certificate store. Alternately, you can configure Firefox so it trusts Windows certificate store and/or trusts the macOS keychain.

Resolved Issues

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

Capture Client for Windows

Resolved issue	Issue ID
When testing user-based policies for Capture Client, the policy does not update when switching from one user to another.	210186

Capture Client for Windows

Resolved issue	Issue ID
When a threat has been detected on a Windows system, the alert notification is not triggered.	209479
Marking a threat as Benign fails for signatures having only File full path as the resolving type.	207867

Cloud Management

Resolved issue	Issue ID
A device ID is added to a Dynamic Group even after a custom rule has been defined that should cause that device to be excluded.	209454
On the client side, the policy mode is not changing to the default policy as it should.	206287
Device type information not displayed in Overview tab under Protect > Devices .	205467
Process details are overlapping under Processes tab in IE and EDGE browsers.	205078
User Profile page isn't displaying correctly in IE and EDGE Browsers.	205073
The automatic decommission option under Threat Protection is not working for devices that go offline and stay offline for more than the specified period of time.	202227

Known Issues

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

Capture Client for Mac

Known issue	Issue ID
Trusted Certificates under Capture Client window of MAC client is showing Valid dates unknown .	210379
Blacklist supports only binary and executable software on macOS.	204840
The SentinelOne Mac agent does not detect all malicious signatures.	201799

Capture Client for Window

Known issue	Issue ID
Trying to upgrade from 1.0.19 to 1.5.6 on a Windows system failed. The work around is to reboot Capture Client after it upgrade to 1.5.6 to force the SentinelOne agent upgrade to fully complete.	210326
Users are not becoming part of dynamic group automatically.	210286

Cloud Management

Known issue	Issue ID
Certificates that have been assigned to the Default Trusted Certificates Policy are not getting deleted from the Certificates page.	210501
Default Capture client policy is allowing custom Threat protection and Trusted certificates custom policies to be default policies. This results in a conflict since the default threat protection policy on S1 site is mapped to the default Threat protection policy in the Capture Client.	206482
Blacklisting a threat that is already listed in the Blacklist is not showing an error.	205591
Blacklisting of text, mp3, image and video is not supported.	201692

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](#)
- [Licensing without a Network Security Appliance](#)

Licensing with a Network Security Appliance

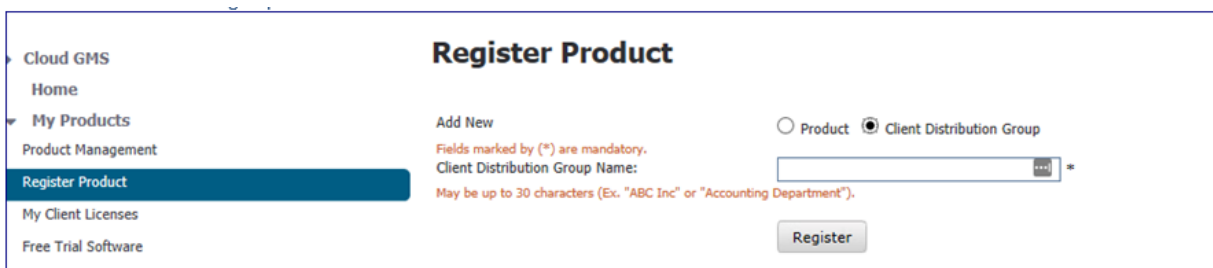
To license SonicWall Capture Client with a network security appliance:

- 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 Switch to **Classic mode**, if it's not presented by default.
- 3 Navigate to **My Products > Register Product**.



- 4 Select **Client Distribution Group** in the **Add New** field.
- 5 Enter a name for the **Client Distribution Group Name**. The name may be up to 30 characters.
- 6 Click on **Register**. The window for **Manage Client Distribution Group Services** is displayed.

NOTE: You can also get to this window by navigating to **My Products > My Client Licenses** and selecting the **Client Distribution Group** that you just created

Manage Client Distribution Group Services



SonicWall Client Distribution Group Registered Successfully. Click on Try button for service trial.

Delete Transfer Rename

Client Distribution Group Name: Lyns Test
Serial Number: CB0000001188
This Serial Number will be required to obtain SonicWall Support.

You have no pending tasks

This product does not belong to any Product Group.

Technical Resources

[Documents and Resources Knowledge Base](#)

Applicable Services

[Format for printing](#)

Service Name	Download	Status	Count	Expiration	Action
▼SERVICE BUNDLES					
▶ McAfee: Client/Server Anti-Virus Suite		Not Licensed			0=>
▼DESKTOP & SERVER SOFTWARE					
McAfee: Enforced Client Anti-Virus and Anti-Spyware		Not Licensed			try 0=>
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware		Not Licensed			try 0=>
Content Filtering Client		Not Licensed			try 0=>
Capture Client Advanced Protection		Not Licensed			0=>
SonicWall Anti Spam		Not Licensed			0=>
▼SUPPORT SERVICES					
24x7 Support		Not Licensed			

- 7 Click on the **Key** icon for Capture Client Advanced Protection to activate the service.
- 8 Enter the activation key provided by the SonicWall team.
- 9 Click **Submit**.
- 10 Click on the link for **Capture Client Advanced Protection**.
- 11 Select **Click here** to access the Security Center. This redirects you to the Client Management Console for login.

SonicWall Support

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

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 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>.

Copyright © 2018 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.


The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.


For more information, visit <https://www.sonicwall.com/legal>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>. Select the language based on your geographic location to see the EUPA that applies to your region.

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: 10/1/18

232-004534-00 Rev A