AutoFocus™ What's New Guide
Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

• For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.

• To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.

• Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2018-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 15, 2019
### Table of Contents

**Latest AutoFocus Release Information** ................................................................. 5
- Latest AutoFocus Features ....................................................................................... 7
- AutoFocus Known Issues ......................................................................................... 8
- Changes to Default AutoFocus Behavior .............................................................. 11
- System Requirements ............................................................................................. 12

**AutoFocus Release History** .................................................................................. 13
- New Features: March 2019 .................................................................................. 15
- New Features: February 2019 ............................................................................. 17
- New Features: November 2018 .......................................................................... 19
- New Features: October 2018 .............................................................................. 21
- New Features: September 2018 ......................................................................... 25
- New Features: August 2018 ............................................................................... 29
- New Features: July 2018 .................................................................................... 32
- New Features: June 2018 ................................................................................... 37
- New Features: May 2018 .................................................................................... 40
  - Dashboard and Report Filters ........................................................................... 40
  - Simplified AutoFocus Searches ..................................................................... 40
  - Scheduled Reporting ....................................................................................... 42
  - New Widgets to Visualize Threats and Sessions .......................................... 43
  - Enhanced Widget Display Controls ............................................................... 45
  - New AutoFocus Upload Sources ................................................................ 45
  - Enhancements to Search Sessions View ........................................................ 46
- New Features: January 2018 .............................................................................. 48
  - Export Dashboard Page Contents ................................................................. 48
  - New Visualization Options for Widgets ....................................................... 48
  - Customizable Reports ..................................................................................... 49
  - Enhanced Dashboard Control ...................................................................... 51
  - Support for Windows 10 Analysis Environment ......................................... 52
- New Features: October 2017 ............................................................................. 54
  - Report Incorrect Sample Verdicts ................................................................ 54
  - New Widgets to Visualize Sample Verdicts and Sources ......................... 55
- New Features: August 2017 ............................................................................. 57
  - Support for WildFire Phishing Verdicts ....................................................... 57
  - Searchable APK and Mac Embedded URLs ............................................... 58
  - Filter WildFire Dynamic Analysis Processes and Activities .................... 59
  - Support for Archives (RAR / 7zip) and ELF File Types ............................ 61
- New Features: June 2017 .................................................................................. 64
  - Search Keyboard Shortcuts .......................................................................... 64
  - AutoFocus Tag Groups .................................................................................. 64
  - Export AutoFocus Tag, Search, and Indicator Data ..................................... 67
  - Secure AutoFocus Alerts ............................................................................. 69
  - Indicator Page Enhancements ..................................................................... 73
  - API Support for Enhanced Tag Retrieval .................................................. 74
- New Features: February 2017 .......................................................................... 80
  - AutoFocus-Hosted MineMeld .................................................................... 80
  - Indicators View for Search Results ............................................................. 83
  - Threat Summary Report ............................................................................... 85
  - New Artifact Type ......................................................................................... 87
<table>
<thead>
<tr>
<th>New Features: October 2016</th>
<th>88</th>
</tr>
</thead>
<tbody>
<tr>
<td>WildFire Cloud Artifacts</td>
<td>88</td>
</tr>
<tr>
<td>Customizable Dashboard</td>
<td>89</td>
</tr>
<tr>
<td>Customizable Landing Page</td>
<td>90</td>
</tr>
<tr>
<td>Visual Cues for Search Results</td>
<td>91</td>
</tr>
<tr>
<td>New Artifact Types</td>
<td>92</td>
</tr>
<tr>
<td>API Support for Session Aggregate Data by Upload Source</td>
<td>93</td>
</tr>
<tr>
<td>API Support for Greater than 4,000 Results Using Pagination</td>
<td>93</td>
</tr>
<tr>
<td>New Features: August 2016</td>
<td>95</td>
</tr>
<tr>
<td>Session-Based Tagging</td>
<td>95</td>
</tr>
<tr>
<td>Single Search for All Tag Conditions</td>
<td>96</td>
</tr>
<tr>
<td>Support for Mac OS X File Types</td>
<td>97</td>
</tr>
<tr>
<td>New Artifact Types</td>
<td>97</td>
</tr>
<tr>
<td>New Features: June 2016</td>
<td>100</td>
</tr>
<tr>
<td>New Tag Colors and Icons</td>
<td>100</td>
</tr>
<tr>
<td>Improved Workflow to Export Artifacts</td>
<td>102</td>
</tr>
<tr>
<td>API Support for Sample Behavior Evidence</td>
<td>104</td>
</tr>
<tr>
<td>API Support for Signature Coverage</td>
<td>105</td>
</tr>
<tr>
<td>Search Enhancements</td>
<td>105</td>
</tr>
<tr>
<td>WildFire DNS History for Domains, URLs, and IP Addresses</td>
<td>107</td>
</tr>
<tr>
<td>Process Tree</td>
<td>108</td>
</tr>
<tr>
<td>Default Search Scope</td>
<td>109</td>
</tr>
<tr>
<td>Sort by Column Headers</td>
<td>110</td>
</tr>
<tr>
<td>Remote Search Enhancements</td>
<td>111</td>
</tr>
<tr>
<td>Find Tags with the Most Recent Comments</td>
<td>112</td>
</tr>
<tr>
<td>New Features: March 2016</td>
<td>114</td>
</tr>
<tr>
<td>AutoFocus API STIX Support</td>
<td>114</td>
</tr>
<tr>
<td>Signature Coverage for Samples</td>
<td>114</td>
</tr>
<tr>
<td>Sample Behavior Evidence</td>
<td>116</td>
</tr>
<tr>
<td>Remote Search</td>
<td>117</td>
</tr>
<tr>
<td>Quick Search</td>
<td>120</td>
</tr>
<tr>
<td>Multiple Active Searches</td>
<td>122</td>
</tr>
<tr>
<td>API Request for a Search</td>
<td>123</td>
</tr>
<tr>
<td>Search Filter Enhancements</td>
<td>125</td>
</tr>
<tr>
<td>Tag Filter Enhancements</td>
<td>125</td>
</tr>
<tr>
<td>AutoFocus Feedback Tool</td>
<td>129</td>
</tr>
<tr>
<td>New Features: December 2015</td>
<td>130</td>
</tr>
<tr>
<td>Display File Analysis Results in Sequence</td>
<td>130</td>
</tr>
<tr>
<td>Filter Tags and Alerts</td>
<td>131</td>
</tr>
<tr>
<td>Attribute Sources For Tags</td>
<td>133</td>
</tr>
<tr>
<td>Search Based on Android Suspicious Actions</td>
<td>134</td>
</tr>
<tr>
<td>New Features: November 2015</td>
<td>135</td>
</tr>
<tr>
<td>Search Based on Observed Behavior</td>
<td>135</td>
</tr>
<tr>
<td>Export Artifact Metadata</td>
<td>136</td>
</tr>
<tr>
<td>Share Links to Saved Searches</td>
<td>136</td>
</tr>
<tr>
<td>Find Tags with an Unspecified Tag Class</td>
<td>137</td>
</tr>
</tbody>
</table>

### Getting Help

<table>
<thead>
<tr>
<th>Related Documentation</th>
<th>141</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requesting Support</td>
<td>142</td>
</tr>
</tbody>
</table>
Latest AutoFocus Release Information

The following topics provide important release information about AutoFocus, including new features introduced, a list of open issues, and changes to default behaviors from the previous release.

- Latest AutoFocus Features
- AutoFocus Known Issues
- Changes to Default AutoFocus Behavior
- System Requirements
Latest AutoFocus Features

The following topics provide a snapshot of the AutoFocus features introduced in May 2019. This list provides context for the new features, with steps to get started. For information about past releases, refer to AutoFocus Release History.

<table>
<thead>
<tr>
<th>Latest AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
</table>

**Support for DNS Security**

AutoFocus™ now supports domains analyzed by the DNS Security service. DNS Security is a continuously evolving threat prevention service designed to protect and defend your network from advanced threats using DNS. By leveraging advanced machine learning and predictive analytics, the service provides real-time DNS request analysis and rapidly produces and distributes DNS signatures that are specifically designed to defend against malware using DNS for C2 and data theft. For more information, see DNS Security.

AutoFocus samples that have been determined to launch a request to connect to a domain analyzed by DNS Security are shown in the sample **Coverage** tab, under the **Domain Signatures** heading.

You can also perform an AutoFocus Search of suspicious DNS domains to view all detected instances of the artifact. You can use this information to help assess whether a domain is associated with suspicious behavior.
# AutoFocus Known Issues

The following list includes known issues found in the current AutoFocus release.

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATF-6015</td>
<td>Some threat signatures might not be available to view in AutoFocus under certain operational conditions.</td>
</tr>
<tr>
<td>ATF-6012</td>
<td>The <strong>Malware Session Percentage By Day</strong> widget does not auto-zoom to the proper level when opened using a saved search.</td>
</tr>
<tr>
<td>ATF-5985</td>
<td>The AutoFocus license exception page does not correctly display the user entity name.</td>
</tr>
<tr>
<td>ATF-5945</td>
<td>In some instances, AutoFocus might not allow you to create a new private tag because it erroneously believes the 100 tag limit was reached.</td>
</tr>
<tr>
<td>ATF-5837</td>
<td>AutoFocus upload sources (aside from the firewall) might not populate certain data fields for a given sample.</td>
</tr>
<tr>
<td>ATF-5635</td>
<td>In some instances, an AutoFocus search using the <strong>Tag</strong> identifier might produce results that do not match the selected tag(s).</td>
</tr>
<tr>
<td>ATF-5633</td>
<td>In some instances, the <strong>Updated</strong> field in the AutoFocus tag detail page might not properly reflect the actual revision date.</td>
</tr>
<tr>
<td>ATF-5584</td>
<td>Every instance of a SHA256 has an unexpected line break when exporting sample search results from browsers operating under OS X.</td>
</tr>
<tr>
<td>ATF-5570</td>
<td>In some instances, creating a search using the File Type indicator and subsequently adding an additional indicator before the first one finishes loading, might result in the second indicator converting to a File Type indicator.</td>
</tr>
<tr>
<td>ATF-5493</td>
<td>In some instances, selecting samples with unknown verdicts might result in a blank page.</td>
</tr>
<tr>
<td>ATF-5366</td>
<td>MineMeld might send double the number of entries in an EDL link to a connected firewall running PAN-OS 8.0.</td>
</tr>
<tr>
<td>ATF-5333</td>
<td>When the AutoFocus interface font size is increased, some elements of the information panel (such as the <strong>Give Feedback</strong> link) might not display correctly.</td>
</tr>
<tr>
<td>ATF-5331</td>
<td>The filetype counts shown in the <strong>Top Filetypes</strong> widget do not always match the figures provided through the API.</td>
</tr>
<tr>
<td>ATF-5254</td>
<td>When the maximum allowable tag limit of 100 is reached, subsequent attempts to add tags will fail without an displaying an error.</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ATF-5074</td>
<td>In some instances, deleted scheduled reports might continue to automatically generate and send reports to specified recipients.</td>
</tr>
<tr>
<td>ATF-4881</td>
<td>Certain APK samples might not show the <strong>Suspicious Pattern</strong> section in the <strong>File Analysis</strong> page.</td>
</tr>
<tr>
<td>ATF-4859</td>
<td>In some instances, scheduled email reports might not be sent as configured.</td>
</tr>
<tr>
<td>ATF-4751</td>
<td>New custom reports are not displayed in <strong>Reports</strong> until the page is refreshed.</td>
</tr>
<tr>
<td>ATF-4750</td>
<td><strong>Threat Name</strong> searches using the <strong>is in the list</strong> operator do not generate consistent search results.</td>
</tr>
<tr>
<td>ATF-4723</td>
<td>Submitting a new quick search IOC value while viewing the search <strong>Session Summary</strong> does not refresh the page contents.</td>
</tr>
<tr>
<td>ATF-4682</td>
<td>The sort functionality present in <strong>Open Saved Search</strong> does not properly display content, depending on the sort settings used.</td>
</tr>
<tr>
<td>ATF-4435</td>
<td>Certain widgets displaying verdicts are not impacted by the dashboard and report verdict filter settings.</td>
</tr>
<tr>
<td>ATF-4323</td>
<td>In some instances the column widths in the sample details page might be improperly configured, making it difficult to view.</td>
</tr>
<tr>
<td>ATF-4252</td>
<td><strong>Top Malware Family Tags</strong>, <strong>Top Campaign Tags</strong>, and <strong>Top Malicious Behavior Tags</strong> widgets are preconfigured to display only Unit 42, Private, and Commodity tags. However, the <strong>Top Tags</strong> widget can be configured using any and all tags.</td>
</tr>
<tr>
<td>ATF-3813</td>
<td>Exported PDF reports with widgets containing at least 10 items in a data set and using the <strong>Chart</strong> visualization option results in the right-most section of a widget being cropped off.</td>
</tr>
<tr>
<td>ATF-3796</td>
<td>In some instances, exported PDF reports containing a <strong>Malware Percentage by Day</strong> widget might result in the data graph overlapping with the explanatory key, depending on the browser used.</td>
</tr>
<tr>
<td>ATF-3748</td>
<td>External links contained in exported PDF reports have limited functionality.</td>
</tr>
<tr>
<td>ATF-2833</td>
<td>The <strong>Disk</strong> widget located in the MineMeld System tab does not show accurate disk space usage.</td>
</tr>
<tr>
<td>ATF-2284</td>
<td>Trying to add more than 2,000 artifacts to an export list at a time may not work when viewing the WildFire® sample analysis details in sequence or in the process tree.</td>
</tr>
<tr>
<td>Issue ID</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>ATF-2191</td>
<td>The AutoFocus™ API for STIX sample analysis (/stix/sample/{sample_id}/analysis) currently does not return Android artifacts. Refer to the AutoFocus API Reference for a full list of Android artifacts.</td>
</tr>
<tr>
<td>ATF-2187</td>
<td>The AutoFocus API for STIX sample analysis (/stix/sample/{sample_id}/analysis) currently does not support requests that include signature coverage.</td>
</tr>
</tbody>
</table>
Changes to Default AutoFocus Behavior

There are no changes to default behavior in this release of AutoFocus.
System Requirements

**Supported Browsers**

For enhanced security and full access to new AutoFocus™ features, we recommend using the latest release of one of the following browsers:

- Chrome
- Firefox
- Internet Explorer / Microsoft Edge
- Safari

**Associated Software Versions**

To use AutoFocus features that integrate with Palo Alto Networks® firewalls or Panorama™ appliances, we recommend the following software versions:

- PAN-OS® 9.0 or a later release
- Panorama 9.0 or a later release
- MineMeld 0.9.52
AutoFocus Release History

The following section lists past major releases of AutoFocus and the associated feature set for that version.

- New Features: March 2019
- New Features: February 2019
- New Features: November 2018
- New Features: October 2018
- New Features: September 2018
- New Features: August 2018
- New Features: July 2018
- New Features: June 2018
- New Features: May 2018
- New Features: January 2018
- New Features: October 2017
- New Features: August 2017
- New Features: June 2017
- New Features: February 2017
- New Features: October 2016
- New Features: August 2016
- New Features: June 2016
- New Features: March 2016
- New Features: December 2015
- New Features: November 2015
New Features: March 2019

The following topics provide a snapshot of the AutoFocus™ features introduced in March 2019. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>March AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional WildFire Static Analysis Data in Sample Reports</td>
<td>AutoFocus™ now displays additional WildFire analysis data that can be viewed under the Static Analysis section of an AutoFocus sample details page:</td>
</tr>
<tr>
<td></td>
<td>• <strong>PE Metadata</strong>—Portable executable file metadata details extracted during WildFire analysis. This includes the section header details, including the name, virtual address, virtual size, and raw size. You can add any of the metadata values to a search by hovering over an artifact and selecting one of the associated search tasks. To add all values to a search, select the left-most drop down. From here, you can also add the artifact to an AutoFocus export list for further analysis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Embedded Files</strong>—Hashes of files that are embedded within document files are displayed, along with the WildFire verdict.</td>
</tr>
<tr>
<td></td>
<td><strong>Static Analysis</strong></td>
</tr>
<tr>
<td></td>
<td>• Suspicious File Properties</td>
</tr>
<tr>
<td></td>
<td>• Behavior Type</td>
</tr>
<tr>
<td></td>
<td><strong>Embedded Contents</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bing</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Bing</strong></td>
</tr>
<tr>
<td></td>
<td><strong>PE Compilation Timestamp</strong></td>
</tr>
<tr>
<td></td>
<td>• Export AutoFocus Artifacts</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>March AutoFocus Features</td>
<td>About Each Feature</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td>To view the PE sample compilation timestamp, <strong>start a search</strong> for a PE file and click on a sample for details.</td>
</tr>
</tbody>
</table>

You can also use the **Compilation Timestamp** indicator listed under Analysis Artifacts to search for samples based on a PE file creation date and time.
New Features: February 2019

The following topics provide a snapshot of the AutoFocus™ features introduced in February 2019. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>February AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAN-DB Multi-Category URL Filtering Support</td>
<td>PAN-DB now assigns multiple categories to URLs to classify websites based on content, features, and safety. Each URL entry supports up to four category types and a risk category, an additional security-focused URL category that indicates its overall threat level. AutoFocus supports this enhancement by displaying all matching categories for a specified URL.</td>
</tr>
</tbody>
</table>

**PAN-DB Categorization**

<table>
<thead>
<tr>
<th>URL</th>
<th>Category</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>firefoxinstaller.com</td>
<td>Financial Services, Personal Sites and Blogs</td>
<td>Low Risk</td>
</tr>
</tbody>
</table>

For more information about the concepts referenced in this feature, refer to:

- Drill Down in Search Results
- AutoFocus Search
- Multi-Category URL Filtering
- New Security-Focused URL Categories

| Improved Tag Group Categories | An AutoFocus™ tag group is a collection of tags defined by Unit 42 researchers that are shown to connect to each other. The tags in a particular group can show relationships, such as family, type, and shared usage via attack campaign. AutoFocus now provides an expanded and enhanced list of tag groups. These tag groups have been restructured to provide better categorization and feature a more detailed description of the type of tags included in the group. |

1. Click Tags > Groups to view a list of tag groups.
2. For each tag group, a description and the number of associated tags are shown. Click on ( ) next to a group to expand a list of tags. You can hover over a tag for additional details.
February AutoFocus Features

<table>
<thead>
<tr>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Tags</td>
</tr>
<tr>
<td>Group Name</td>
</tr>
<tr>
<td>AutoFocus Tags</td>
</tr>
<tr>
<td>File Infection</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Malware</td>
</tr>
<tr>
<td>Malware</td>
</tr>
</tbody>
</table>

For more information about the concepts referenced in this feature, refer to:

- AutoFocus Tags
- Tag Group
New Features: November 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in November 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>November AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamically Filter your Dashboard and Reports</td>
<td>The AutoFocus dashboard and reports can now be dynamically filtered based on any widget artifact data point. This allows you to quickly customize your dashboard and reports based on the visualized data points populated within a widget. Currently, the following widgets support dynamic filtering: Custom Aggregation, Top Firewalls, Top Malware, Top Applications, Bottom Applications, Upload Sources, Top Filetypes, Bottom Filetypes, Target Industries, Top Tags, Flexible Map, Sample Verdicts, and Download Sessions.</td>
</tr>
</tbody>
</table>

- **Add Filter:** Shift-click on a widget data point to add a filter based on that artifact. Filters are highlighted in orange and also appear to the right of the quick-filters at the top of the page.
- **Remove Filter:** Shift-click on a previously highlighted filter or, alternatively, click x from the filter list at the top of the page.

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Reports
- AutoFocus Dashboard

| Support for Script Sample Analysis | The WildFire® cloud now analyzes script samples (.js, .vbs, .ps1, and .sh) using static and dynamic analysis. This helps protect users against script-based malware, which has become a common vector of attack. In AutoFocus™, you can now search for script samples and view related sessions, statistics, and WildFire analysis report information. |

1. Start an AutoFocus search based on **File Type**.
2. Select one of the following to find samples of a given file type:
   - PowerShell
   - VBScript
   - Shell Script
3. View the search results. When you view the sample details for a script file, you can examine the specific behavioral characteristics and properties that were observed during sample analysis.

For more information about the concepts referenced in this feature, refer to:

- **AutoFocus Search**
New Features: October 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in October 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>October AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recent Research Widget Improvements</strong></td>
<td><strong>The AutoFocus Recent Research widget now allows you to add tags from a blog entry to a search query with a single click.</strong></td>
</tr>
<tr>
<td></td>
<td>1. Click ( ) to add tags referenced in a blog entry to a search query, as necessary.</td>
</tr>
<tr>
<td></td>
<td>2. The tag(s) are automatically added to the search query. Run the search query or add additional conditions.</td>
</tr>
<tr>
<td></td>
<td>For more information about the concepts referenced in this feature, refer to:</td>
</tr>
<tr>
<td></td>
<td>• AutoFocus Search</td>
</tr>
<tr>
<td></td>
<td>• First Look at the AutoFocus Portal</td>
</tr>
<tr>
<td><strong>Save Searches from the Dashboard and Reports</strong></td>
<td><strong>You can now save your quickfilter settings and apply them to any of your AutoFocus Dashboard and Reports. Quickfilter settings include Verdict, First Seen, and Source.</strong></td>
</tr>
<tr>
<td></td>
<td>1. Open the Dashboard or select a Report.</td>
</tr>
<tr>
<td></td>
<td>2. Configure your quickfilter settings as necessary.</td>
</tr>
</tbody>
</table>
|                            | 3. Open Saved Search and click Save Current Search.
### October AutoFocus Features

<table>
<thead>
<tr>
<th></th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="AutoFocus Features" /></td>
</tr>
</tbody>
</table>

#### 4. Provide the **Name** and **Description** for the new saved search profile and then click **Save Search**.

- ![Save Search](image)

  **The conditions of the saved search are shown at the bottom of the Save Search window.**

#### 5. From the dashboard or after opening a report, select a **Saved Search** profile to filter the widget contents based on the saved search conditions.

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Reports
- AutoFocus Dashboard

---

### Editable Report Description

<table>
<thead>
<tr>
<th></th>
<th>You can now update your AutoFocus report description after it has already been defined during the report creation process. This allows you to change your report description to reflect updates made to the report configuration.</th>
</tr>
</thead>
</table>
|   | 1. **Open the Report** menu.  
|   | 2. **Click on the report description** to edit the text. |
You can only edit the description for user-defined reports.

3. Update your report description and press enter to save the change. You can exit without saving changes by pressing Esc or clicking on a different element of the AutoFocus interface.

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Reports

**Device Serial Search Improvements**

AutoFocus now pre-populates a list of firewalls when you search based on Device Serial numbers. This allows you to select a firewall from a preloaded list of serial numbers or, alternatively, auto-completes based on a partial match.

1. Run an advanced AutoFocus search using the Device Serial artifact.
2. When using search operators that require a value, you can:
   - Enter an incomplete firewall serial number value to retrieve a list of partial matches.
   - Select from a list of firewall serial numbers.
<table>
<thead>
<tr>
<th>October AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you have more than 1,000 devices attached to your account, AutoFocus does not pre-populate device list searches; as a result, you cannot select from a preloaded list or retrieve a list of partial matches. Instead, search results are returned based on the selected operator and serial number input.</td>
</tr>
</tbody>
</table>

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Search
New Features: September 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in September 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>September AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
</table>
| New Widgets to Visualize Top Tags | AutoFocus is introducing two new dashboard and report widgets to help users visualize recent sessions and samples. The contents of the widgets are based on the filter settings and can be updated to suit your reporting requirements. You can add these new widgets to AutoFocus by customizing your Dashboard or Reports.  

1. To customize your AutoFocus widget layout and contents:  
   - Dashboard—Go to the Dashboard and click Edit Page.  
   - Reports—Go to Reports, Run the report you want to add the new widgets to, then click Edit page.  

2. Add Row and then Add Widget based on your dashboard layout preferences. Add the new widgets labeled Top Actors Tags and Top Exploit Tags to your dashboard.  

   ![Image of dashboard widgets]

   3. When you are finished making your dashboard changes, click Editing. If you would like to restore the dashboard settings, click Reset.

4. The new dashboard widgets display the following information:

   - You can use the filters located at the top of the report and dashboard pages to define the content shown in the widgets.

   - Top Actors Tags—Displays a list of actor tags based on the dashboard or report time range settings. You can further customize the widget by changing the sample display settings.
<table>
<thead>
<tr>
<th>September AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Top Actor Tags" /></td>
</tr>
</tbody>
</table>

- **Top Exploits Tags**—Displays a list of exploit tags based on the dashboard or report time range settings. You can further customize the widget by changing the sample display settings.

![Top Exploit Tags](image)

For more information about the concepts referenced in this feature, refer to:

- AutoFocus Dashboard
- AutoFocus Reports

<p>| Recent Research Widget Improvements | The AutoFocus™ recent research widget has been improved to show additional blog entries as well as the related AutoFocus tags. |</p>
<table>
<thead>
<tr>
<th>September AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support for WildFire Sample Removal Requests</strong></td>
<td>Users who submit unique samples to the WildFire cloud for analysis can issue a request for removal. Sample data includes session / upload data and the sample file itself. Samples that have been successfully removed from the WildFire cloud are now also removed from AutoFocus. <strong>The AutoFocus cloud service does not retain sample files; as a result, only session data is deleted when a request for sample removal is completed in WildFire. Remnant sample meta data will continue to be available in searches.</strong></td>
</tr>
</tbody>
</table>
| **Support for Samples that have Undergone Dynamic Unpacking** | AutoFocus™ now allows you to leverage analysis data from files that have undergone WildFire® analysis using dynamic unpacking. Dynamic unpacking is a cloud-only environment that unpacks and deobfuscates files that have been encoded using custom and open source file compression or packing tools. This provides improved coverage by analyzing files that might have previously dropped as a result of code obfuscation. The nested analysis report section has tabs for the environments used to analyze a file. Selecting the **Dynamic Unpacking** tab displays the sample’s observed behavior and lists each activity the sample performed when executed in the WildFire cloud.  
1. Start an AutoFocus search to view a list of samples.  
2. Click a sample to view detailed analysis information about the file. |

Hover over a tag to reveal additional details and actions you can take on the specified tag.

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Dashboard
- AutoFocus Reports
<table>
<thead>
<tr>
<th>September AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. If a sample was analyzed using dynamic unpacking, a tab labeled <strong>Dynamic Unpacking</strong> is shown as one of the analysis environments. The subheadings show the analysis details associated with the new environment. You can expand any of the subsections for additional information.</td>
<td></td>
</tr>
</tbody>
</table>

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Search
New Features: August 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in August 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>August AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Access to Saved Searches</td>
<td>You can now apply your saved searches to quick searches, reports and dashboards, report email schedules, and to advanced searches. This allows you to apply complex or frequently used search conditions to several AutoFocus contexts without having to manually apply each setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Quick Search</strong>—From the quick search menu, select a Saved Search setting to run the search.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Report and Dashboard Filter</strong>—From the dashboard or after opening a report, select a Saved Search setting to filter the widget contents based on the saved search conditions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Scheduled Report Context</strong>—When defining your scheduled reporting details, select a Saved Search setting. This setting filters the emailed report contents based on the saved search conditions.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Advanced Search Condition</strong>—Add a Saved Search setting to an advanced search. This allows you to apply additional search conditions to what has already been defined by the saved search.</td>
</tr>
<tr>
<td>August AutoFocus Features</td>
<td>About Each Feature</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td><em>Pivot from Tag to Sample Searches</em></td>
<td>You can now quickly perform a search for samples based on the results of a tag search.</td>
</tr>
</tbody>
</table>

1. Start an AutoFocus tag search.  
2. Click **Search for these tags**.

![AutoFocus tag search interface](image)

*The number of tags used in the sample search is based on the number of results shown on the tag search results page. For example, if there are 82 tag results but the page is set to show a maximum of 50 tags, only 50 tags will be used by the sample search.*

3. AutoFocus automatically initiates a sample search based on the tag search results.
<table>
<thead>
<tr>
<th>August AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
</table>

For more information about the concepts referenced in this feature, refer to:

- AutoFocus Search
- AutoFocus Tags
# New Features: July 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in July 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>Latest AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Additional Date Options for Searches</strong></td>
<td>You now have the option to search for samples based on relative dates, in addition to absolute dates. Using a relative date allows you to select a date range based on the current time as a reference point. For example, you can configure a search to find malicious samples first seen three days ago.</td>
</tr>
</tbody>
</table>
| ![AutoFocus Search](image)                 | For more information on using the AutoFocus search, refer to:  
  * AutoFocus Search                                                                                                                                   |

| **New Widgets to Visualize Search Sessions and Samples** | AutoFocus is introducing two new dashboard and report widgets to help users visualize recent sessions and samples. The contents of the widgets are based on the filter settings and can be updated to suit your reporting requirements. You can add these new widgets to AutoFocus by customizing your Dashboard or Reports.  
  1. To customize your AutoFocus widget layout and contents:  
     * Dashboard—Go to the Dashboard and click Edit Page.  
     * Reports—Go to Reports, Run the report you want to add the new widgets to, then click Edit page.  
  2. Add Row and then Add Widget based on your dashboard layout preferences. Add the new widgets labeled Recent Samples and Recent Sessions to your dashboard. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest AutoFocus Features</td>
<td>About Each Feature</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. When you are finished making your dashboard changes, click **Editing**. If you would like to restore the dashboard settings, click **Reset**.

4. The new dashboard widgets show the following information:

You can use the filters located at the top of the report and dashboard pages to define the content shown in the widgets.

- **Recent Samples**—Displays a list of recent samples based on the widget and dashboard / report filter settings. You can further customize the widget by changing the **sample** display settings.

- **Recent Sessions**—Displays a list of recent sessions based on the widget and dashboard / report filter settings. You can further customize the widget by changing the **session** display settings.
**Latest AutoFocus Features**

<table>
<thead>
<tr>
<th><strong>About Each Feature</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can export widget contents into text, CSV, and JSON formats by selecting ( ), configuring your export details, and then clicking Download.</td>
</tr>
</tbody>
</table>

For more information about the concepts referenced in this feature, refer to:
- AutoFocus Dashboard
- AutoFocus Reports
- Export AutoFocus Page Content

**New Hash-based Search**

You now have the option to search for samples based strictly on the sample hash value.

This excludes the search from returning hashes that might be contained within other files, such as those found in the File Activity section of a sample details page.

1. Create a new advanced AutoFocus search using the new Hash Lookup identifier.

   Hovering over the Hash and Hash Lookup identifiers opens a tooltip with a description.

2. Configure the search options and click Search.

The search returns a result that matches only with the hash value of the primary sample (hashes contained in the file are not included in the results).
Latest AutoFocus Features | About Each Feature

Customizable Widgets

You can now add a custom widget to your dashboard or any of your AutoFocus reports. This widget is populated by data from user-selectable artifacts and can be further tailored using one of five visualization options.

1. Open an AutoFocus report or dashboard and add a widget.
2. Select **Custom Aggregation** under **Aggregates** from the widget list.
3. Provide a name to identify the custom widget.
4. Click **Editing** to exit the dashboard / report editing mode.
5. Configure the custom widget artifact and display options:
   - **Number of values**—Configures the number of artifacts of a given type that are displayed by the widget.
   - **Visualization**—Toggles between different widget display options. Options include charts, bars, grids, pies, and treemaps.
   - **Artifact**—A searchable AutoFocus property, activity, or behavior associated with samples and sessions. Examples include upload sources, source IPs, WildFire verdicts, and file types.

For more information about the concepts referenced in this feature, refer to:

- **AutoFocus Search**
<table>
<thead>
<tr>
<th>Latest AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• AutoFocus Dashboard</td>
</tr>
<tr>
<td></td>
<td>• AutoFocus Reports</td>
</tr>
</tbody>
</table>
New Features: June 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in June 2018. Each section includes context for the new feature, with steps to get started.

<table>
<thead>
<tr>
<th>June AutoFocus Features</th>
<th>About Each Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhancements to Scheduled Reporting</td>
<td>You can now apply filters to your preexisting AutoFocus reports to narrow down the results that are shown in a scheduled email report. You can now specify the Verdict, Source, and the Tag Group, in addition to the existing Time Frame setting. When configuring the Email Schedule, the following new filters are available:</td>
</tr>
<tr>
<td></td>
<td>• Verdict—Select from Malware, Grayware, Benign, Phishing, and Any Verdict to filter the report data based on a verdict. • Time Frame—Sets the emailed report to display sample data (based on the time stamp of when the sample was first forwarded or uploaded to WildFire for analysis) for the last 1, 7, 30, 90, or 180 days. • Source—Select from Firewall, Proofpoint, Traps, Magnifier, Manual API, Traps Android, WF Appliance, and Any Source to filter the report data based on the upload source. • Tag Group—Select from a pre-populated AutoFocus tag group list to filter based on the specified tag group.</td>
</tr>
</tbody>
</table>
### June AutoFocus Features

#### About Each Feature

You can only specify a single filter for a given context type. If you want to generate reports showing additional context configurations, you can create additional email schedules.

For more information on creating and configuring scheduled reports, refer to:

- [AutoFocus Scheduled Reporting](#)

### Additional Search Filters

You can now filter AutoFocus search page results based on tag groups and classes, in addition to standard tags.

Use the Tag drop-down to filter the results of your report. Whenever new parameters are selected, the report is automatically refreshed to reflect the updated data set.

From the Search, select from the following new tag filter options:

- **Tag Class**—Select from *None, Actor, Campaign, Malware Family, Exploit,* and *Malicious Behavior* to filter the data set based on the tag class.
- **Tag Group**—Select from a pre-populated AutoFocus tag group list to filter the data set based on the specified tag group.

For more information on using the AutoFocus search, refer to:

- [AutoFocus Search](#)

### Additional Searchable Field in the Sample Details View

You can now search based on a static analysis property description from the sample details view.

When you hover over a Risk description under Static Analysis, a drop down menu displays. Click on the drop down to open additional tasks. From here, you can:

- **Add to Search**—Adds a condition to an existing search using the selected behavior value.
- **Add to New Search**—Opens a new search window and adds a search condition using the selected behavior value.
For more information on using the AutoFocus search, refer to:

- AutoFocus Search
New Features: May 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in May 2018. Each section includes context for the new feature, with steps to get started.

- Dashboard and Report Filters
- Simplified AutoFocus Searches
- Scheduled Reporting
- New Widgets to Visualize Threats and Sessions
- Enhanced Widget Display Controls
- New AutoFocus Upload Sources
- Enhancements to Search Sessions View

Dashboard and Report Filters

You can now filter the contents of your dashboard and reports based on the sample verdict, samples/session source, and the time frame (first seen and time). This allows you to create and view dashboard contents and reports with greater specificity based on selected criteria.

**STEP 1** | Select Dashboard or Reports and then select a report.

**STEP 2** | Use the drop-downs to filter the results of your report. Whenever new parameters are selected, the report is automatically refreshed to reflect the updated data set. You can select the following options:

- **Verdict**—Select from Malware, Grayware, Benign, Phishing, and Any Verdict to filter the data set based on a verdict.

- **First Seen** and **Time**—First configure the data set to include samples based on when it was First Seen (the time stamp of when the sample was first forwarded or uploaded to WildFire for analysis) or by Time (the time stamp of when the session started) and then set the dashboard to display data for the last 1, 7, 30, 90, or 180 days. You can also set the dashboard to display all data by default, regardless of the time period that the data was collected, by setting the time range to Any Time.

   The time setting does not filter the scope (My Samples, (private), Public Samples, or All Samples (private and public samples)) of the sample data set.

- **Source**—Select from Firewall, Proofpoint, Traps, Magnifier, Manual API, Traps Android, WF Appliance, and Any Source to filter the data set based on the upload source.

Simplified AutoFocus Searches

You can now find AutoFocus artifacts using the simplified quick search option in the Search menu. Quick search allows you to configure a search using frequently used conditions. These conditions include: verdict, timeframe (first seen and time), source, tags, and IOC (indicators of compromise). Should you need to add additional variables, you can switch to the advanced search mode, and add items based on the initial simple search.

**STEP 1** | Start an AutoFocus search.
STEP 2 | AutoFocus defaults to the search mode that was last used. If AutoFocus is in the advanced search mode, switch to Simple mode.

STEP 3 | Configure your search by selecting the desired search variables from the drop-down menus. You can select from the following categories: Verdict, First Seen, Time, Source, Tags, and IOC (indicators of compromise). AutoFocus automatically refreshes after each variable is selected or modified.

- **Verdict**—Select from Malware, Grayware, Benign, Phishing, and Any Verdict to search for samples based on a verdict.
- **First Seen** and **Time** —First configure the search to find samples based on when it was First Seen (the time stamp of when the sample was first forwarded or uploaded to WildFire for analysis) or by Time (the time stamp of when the session started), then set the search to display data for the last 1, 7, 30, 90, or 180 days. You can also set the search to display data by setting the time range to Any Time.

  The time setting for a search does not filter the scope (My Samples, (private), Public Samples, or All Samples (private and public samples)) of the sample data set.

- **Source**—Select from Firewall, Proofpoint, Traps, Magnifier, Manual API, Traps Android, WF Appliance, and Any Source to search for samples based on the upload source.
- **Tag**—Select from a list of tags or filter the list by entering a keyword to search for samples associated with a tag.
- **IOC**—Search based on the following indicators of compromise: Hash, IP Address, Domain, URL, User Agent, Email Address, and Filename

STEP 4 | If you want to add other conditions to the search, you can switch to Advanced mode. Switching to advanced mode retains the condition values selected from the simple search mode. From here, you can add additional search conditions that are not available in simple search mode.
If you add search conditions that are not available in simple mode while in advanced mode, you will be prompted to reset your search when returning to simple mode.

Scheduled Reporting

You can now configure AutoFocus to automatically generate and send reports to a series of recipients via email. You can specify the date and interval at which the reports are sent, as well as the specific coverage timespan of the report. This eliminates the need for you to manually generate and send the reports to relevant people in your organization.

STEP 1 | Click **Reports** on the navigation pane.

STEP 2 | On the report you want to create an schedule for, click **Email Scheduler**.

STEP 3 | Add an email schedule profile.

STEP 4 | Configure your email schedule. You can define the recipient email address, the **Frequency** of the reports, the **Time** when it is sent, and the **Context** (length of time the report covers). On the bottom-left, you will see the date when the next report is to be sent. Click **Save** to continue.

STEP 5 | From the email schedule profile window, create additional email schedules as well as manage existing ones. You can also send a test email to verify the report and configuration is acceptable for your organization. Click **Close** when you have finished creating and updating email schedules. Select **Add** if you want to configure additional recipients for emailed reports.
New Widgets to Visualize Threats and Sessions

AutoFocus is introducing new dashboard and report widgets to help users visualize the sources and destinations of threats as well as the most frequently encountered tags. You can add these new widgets to AutoFocus by customizing your Dashboard or Reports.

**STEP 1** | To begin customizing your AutoFocus widget layout and contents:
1. Dashboard—Go to the Dashboard and click Edit Page.
2. Reports—Go to Reports, Run the report you want to add the new widgets to, then click Edit Page.

**STEP 2** | Add Row and then Add Widget based on your dashboard layout preferences. Add the new widgets labeled Source Countries Map and Destination Countries Map to your dashboard.

**STEP 3** | When you are finished making your dashboard changes, click Editing. If you would like to restore the dashboard settings, click Reset.

**STEP 4** | The new dashboard widgets show the following information:
1. **Source Countries Map**—Displays a map highlighting the countries where the most threats originate.
2. **Destination Countries Map**—Displays a map highlighting the countries that have received the most malware.
3. **Top Malware Family Tags**—Displays the top 10 Malware Family class tags and the instance count.

4. **Top Campaign Tags**—Displays the Top Campaign class tags and the instance count.

5. **Top Malicious Behavior Tags**—Displays the Top Malicious Behavior class tags and the instance count.
**STEP 5** | **Next Steps:**

- Learn more about how to create or customize AutoFocus reports.
- Learn more about how to customize the AutoFocus dashboard.

**Enhanced Widget Display Controls**

Widgets that display ranked items can now be configured to show more values than the previous default setting of 10.

**STEP 1** | **To begin customizing your AutoFocus widget display options:**

1. Dashboard—Go to the **Dashboard**.
2. Reports—Go to **Reports**, then run the report in which you want to update the widget display options.

**STEP 2** | **Widgets containing a series of ranked items now have a `show` drop-down menu to the left of the widget display toggle. You can select the number of items to display per widget.**

**STEP 3** | **Next Steps:**

- Learn more about how to create or customize AutoFocus reports.
- Learn more about how to customize the AutoFocus dashboard.

**New AutoFocus Upload Sources**

*Cortex XDR – Analytics* (formerly Magnifier) and *Traps* for Android can now forward suspicious samples to WildFire for analysis. You can search for samples that have been forwarded from these sources, as well as view the WildFire analysis details and the related sessions from AutoFocus.

**STEP 1** | **Start an AutoFocus search.**
STEP 2 | Configure your search to find samples that were sent to WildFire from Traps Android or Cortex XDR – Analytics. For example, Upload Source > is > Traps Android | Cortex XDR – Analytics, and then click Search.

Toggle between My Samples, Public Samples, and All Samples to change the scope of the search results. Selecting My Samples will limit the results to samples detected by Traps and Magnifier instances associated with your support account.

STEP 3 | Click on a sample hash to view the sample details. For more information about reviewing and understanding your search results, see Drill Down in Search Results.

STEP 4 | Next steps:
- Learn about how to customize your search with the AutoFocus search editor.
- Learn more about AutoFocus Sample Details.

Enhancements to Search Sessions View

AutoFocus now displays a list of tags associated with a sample in the Search > Sessions tab. This allows you to quickly reference the tags associated with a sample without having to switching views. Optionally you can also add the tag groups data column to the Sessions view.

STEP 1 | After performing an AutoFocus Search, select Sessions to view the session overview. The new Tags column is shown to the right.

STEP 2 | The new Group Tags column is not displayed by default. To add the Group Tags column, click Column and then select Group Tags.
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/24/2018 12:07:33am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:21:55am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:27:34am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:00:17am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:12:43am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 11:19:09am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:39:09am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:41:17am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 11:42:11am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:46:42am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:12:34am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
<tr>
<td>03/24/2018 12:06:30am</td>
<td>web-browsing</td>
<td>wildfire.paloaltonetworks.com/publicapi/test/pe</td>
</tr>
</tbody>
</table>

- **Application**: unknown
- **File URL**: wildfire.paloaltonetworks.com/publicapi/test/pe
New Features: January 2018

The following topics provide a snapshot of the AutoFocus™ features introduced in January 2018. Each section includes context for the new feature, with steps to get started.

- Export Dashboard Page Contents
- New Visualization Options for Widgets
- Customizable Reports
- Enhanced Dashboard Control
- Support for Windows 10 Analysis Environment

Export Dashboard Page Contents

AutoFocus™ now allows you to export the selected dashboard page into a PDF document. Only the content that is displayed on a given dashboard page can be exported. For example, if the selected dashboard contains the Sample Verdicts, Malware Download Sessions, Top Applications, and Top Malware widgets, only those items using the selected visualization options are displayed in the PDF.

**STEP 1** | Go to your AutoFocus Dashboard and select the report you want to export from the report tabs.

**STEP 2** | Configure your widgets with the appropriate data and visualization options, as well as the date range.

**STEP 3** | Click Download PDF to generate and download the exported file.

New Visualization Options for Widgets

AutoFocus™ is introducing new ways to view the information shown in data-reporting widgets. You can now toggle between different display options, allowing you to further customize your dashboard and threat summary reports. The new charts include the following: pie chart, tables, tree maps, and horizontal and
vertical bar charts. Visualization settings are retained session to session so there is no need to save or reapply settings every time you view your reports.

STEP 1 | Select Dashboard or Reports (Threat Summary Report) and then select a report.

STEP 2 | On the upper-right corner of a widget, click on the drop-down to toggle between the new display options. The following example shows multiple instances of the Top Malware widget using various display options.

STEP 3 | Next steps: Learn more about how to customize AutoFocus reports

Customizable Reports

AutoFocus™ now allows you to create and edit custom Reports using enhanced widgets. You can customize default reports, such as the Threat Summary Report, or create your own. Add widgets or remove them based on your preferences, and pick the order in which they appear on the dashboard.

Dashboard settings are unique and saved for each user in a support account.

STEP 1 | Open Reports to manage and create new custom reports.
From here you can:

- Create a new report (1). Add a report title and description and then select **Create** to add a new report. A new blank report opens in editing mode.
- Search for a report by keyword (2). This search feature displays keyword matches found in titles only.
- Manage default reports (3).
  - Run—Opens the selected report.
  - Clone—Creates and opens a duplicate of the selected report. You can edit the report from this page. If you do not provide a new name for the report, AutoFocus creates a name by appending the name on which the report is based with the word clone. For example, Custom Report 1 Clone.
  - Upgrade—When Palo Alto Networks® updates the settings for a default report, select this option to synchronize the report with the latest version. This option is displayed only when an update is available.
  - Pin—Adds the selected report to the dashboard tabs for quick reference. You can also pin (and unpin) reports from the dashboard.
- Manage custom reports (4). Run, Clone, and pin operations function as described in Manage default reports, however you cannot upgrade a report as these reports are not managed by Palo Alto Networks. Additionally, you have the option to delete a report. Selecting this permanently deletes the report from AutoFocus.

**STEP 2** | Create a new Report or edit an existing report by selecting Run or Clone.

**STEP 3** | Click the Page Editor (2) to edit the report.
STEP 4 | Edit the widgets and widget placement on the report.

- Update the name of the report (1).
- Edit the name of a widget (3).
- Remove a widget.
  
  Click X to remove a widget (4).

  Removing a widget frees up a slot on the dashboard so you can add a widget.

- Add a new row of widgets.
  
  Choose an area on the dashboard where you would like to insert a new row of widgets, and click Add Row (5). The newly added row includes two blank slots for widgets by default.

- Add a widget.

  Find a blank widget slot, and click Add Widget (6). Then select a widget type.

- Remove a row of widgets.

  On the right side of the row you want to remove, click Remove Row (7).

- Change the number of widgets in a row.
  
  Change Columns (8) in the row to show up to 4 widgets.

STEP 5 | Save your changes to the report. When you are finished making your changes, click the Page Editor (2).

STEP 6 | (Optional) Restore the default report settings. Click the Page Editor drop-down and Reset Page to Default.

STEP 7 | (Optional) Clone the selected report. Click the Page Editor drop-down and Clone Page to create a report based on the selected report.

STEP 8 | Next steps: Learn more about the new Widget Visualization Options

Enhanced Dashboard Control

AutoFocus™ now gives you finer control over your dashboard with the option to manage reports. These are the same threat summary reports available under AutoFocus > Reports. As a result, any changes made to a given report under the Dashboard will also be reflected in Reports as well. The new options include pinning reports so they quickly accessible, as well as being able to update and clone pages.

STEP 1 | Go to your AutoFocus Dashboard and select the configure button to add an existing report to your dashboard view. Selecting a report adds a new tab with the report name to the dashboard.
STEP 2 | You can reorder the report tab list by dragging and dropping the report into a new order. The report at the top of the list corresponds to the leftmost report in the tab.

STEP 3 | *(Optional)* For default reports, you can **Upgrade Page** to sync with the latest version of the report from Palo Alto Networks®. From here, you can also **Clone Page** to create another version of the selected report.

STEP 4 | Next steps: Learn more about how to create AutoFocus reports.

---

Support for Windows 10 Analysis Environment

AutoFocus™ now allows you to leverage analysis data from files that have undergone WildFire® analysis using the Windows 10 analysis environment. This virtual environment is configured using the following system attributes: Windows 10 x64, Flash 22, Adobe Reader 11, and Office 2010.

The nested WildFire Dynamic Analysis section has tabs for the VM environments used to analyze a file. Selecting a tab displays the sample’s observed behavior and lists each activity the sample performed when executed in the WildFire analysis environment.

STEP 1 | Start an **AutoFocus search** to view a list of samples.

STEP 2 | Click a sample to view detailed analysis information about the file.

STEP 3 | If a sample was analyzed using the Windows 10 analysis environment, a column labeled **Windows 10 x64** is shown next to **WildFire Dynamic Analysis**. Select **Windows 10 x64** to view the dynamic analysis details associated with the new Windows 10 VM. You can expand any of the subsections for additional information.
### WildFire Dynamic Analysis

<table>
<thead>
<tr>
<th>Category</th>
<th>Windows 7 x64 SP1</th>
<th>Windows 10 x64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observed Behavior</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Behavior Type</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Registry Activity</td>
<td>82</td>
<td>120</td>
</tr>
<tr>
<td>DNS Activity</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>File Activity</td>
<td>78</td>
<td>74</td>
</tr>
<tr>
<td>Process Activity</td>
<td>56</td>
<td>31</td>
</tr>
<tr>
<td>Connection Activity</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>HTTP Requests</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>User Agent String Fragments</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**STEP 4** | **Next steps:** Learn more about **Viewing Sample Details**.
New Features: October 2017

The following topics provide a snapshot of the AutoFocus™ features introduced in October 2017. Each section includes context for the new feature, with steps to get started.

- Report Incorrect Sample Verdicts.
- New Widgets to Visualize Sample Verdicts and Sources

Report Incorrect Sample Verdicts

AutoFocus™ now allows you to submit correction requests for suspected incorrect sample verdicts.

**STEP 1** | Start an AutoFocus search and click on a sample hash that has undergone Wildfire® analysis.

**STEP 2** | Click Report as Incorrect.

**STEP 3** | Select a Suggested Verdict based on information you have about the file and provide a contact Email with any additional Comments regarding the sample.
New Widgets to Visualize Sample Verdicts and Sources

AutoFocus™ is introducing two new dashboard widgets to help users visualize the verdict makeup based on their entire sample database or by specific sample sources, such as a firewall, Traps, Proofpoint, or manual uploads. You can add these new widgets to AutoFocus by customizing your dashboard.

**STEP 1** | To begin customizing your AutoFocus dashboard layout and contents, go to the Dashboard and click the Page Editor ( ).

**STEP 2** | Add Row and Add Widget based on your dashboard layout preferences. Add the new widgets labeled Device Verdicts Grid and Sample Verdicts to your dashboard.

**STEP 3** | When you are finished making your dashboard changes, click the Page Editor ( ). If you would like to restore the dashboard settings, click the Page Editor drop-down and Reset Page to Default.

**STEP 4** | The new dashboard widgets show the following information:

1. **Device Verdict Grid**—Provides a table showing a list of sample sources with basic identification along with corresponding sample data. The sample data includes the total number of samples sent from the device and the verdict makeup. The Unknown column indicates samples that have not been analyzed.

<table>
<thead>
<tr>
<th>Source</th>
<th>Total</th>
<th>Malware</th>
<th>Benign</th>
<th>Grayware</th>
<th>Phishing</th>
<th>Name</th>
<th>IP Address</th>
<th>Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>008BC100223</td>
<td>2,683,384</td>
<td>114,414</td>
<td>2,568,479</td>
<td>404</td>
<td>19</td>
<td>172.168.119.114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001701004772</td>
<td>2,302,024</td>
<td>5,437</td>
<td>2,975,134</td>
<td>63</td>
<td>2060</td>
<td>10.8.2.109</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008BC100600</td>
<td>2,445,208</td>
<td>488,596</td>
<td>1,054,546</td>
<td>153</td>
<td>13</td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00910102301</td>
<td>740,650</td>
<td>693</td>
<td>720,379</td>
<td>6</td>
<td></td>
<td>172.168.119.114</td>
<td></td>
<td></td>
</tr>
<tr>
<td>008BC1010504</td>
<td>695,117</td>
<td>10,609</td>
<td>685,602</td>
<td>206</td>
<td>13</td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001701005288</td>
<td>683,313</td>
<td>659</td>
<td>682,841</td>
<td>13</td>
<td>15</td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001401002172</td>
<td>783,896</td>
<td>1,400</td>
<td>782,169</td>
<td></td>
<td></td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001010320151</td>
<td>354,702</td>
<td>11,794</td>
<td>422,083</td>
<td>15</td>
<td>15</td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
<tr>
<td>001010320151</td>
<td>550,411</td>
<td>7,456</td>
<td>454,222</td>
<td>13</td>
<td>13</td>
<td>192.168.126.254</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. **Sample Verdicts**—Provides a color-coded pie chart showing the sample verdict makeup based on the specified date range. Hovering your mouse cursor over any of the color-coded sections displays the number of a sample verdicts and a percentage based on the total number of samples.
STEP 5 | Next Steps: Learn more about how to customize the AutoFocus dashboard.
New Features: August 2017

The following topics provide a snapshot of the AutoFocus™ features introduced in August 2017. Each section includes context for the new feature, with steps to get started.

- **Support for WildFire Phishing Verdicts**
- **Searchable APK and Mac Embedded URLs**
- **Filter WildFire Dynamic Analysis Processes and Activities**
- **Support for Archives (RAR / 7zip) and ELF File Types**

**Support for WildFire Phishing Verdicts**

The WildFire® phishing verdict classifies credential phishing links found in emails separately from emailed links found to be exploits or malware. WildFire classifies the link as phishing based on properties and behaviors the accompanying website displays and assigns the link the new phishing verdict. In AutoFocus™, you can now view and search for samples that have been classified as phishing or have been scanned using the phishing analyzer.

**STEP 1** | Start an AutoFocus search based on **WildFire Verdict**.

**STEP 2** | Select **Phishing** from the verdict options list and click **Search**.

**STEP 3** | Click on a sample hash to view the sample details.
You can search for URLs that you suspect are phishing links by using the Filename indicator in an AutoFocus search.

**STEP 4 | Next steps:**

- Learn about how to customize your search with the AutoFocus search editor.
- Learn more about other AutoFocus Sample Details.

**Searchable APK and Mac Embedded URLs**

You can now search for APK and Mac embedded URLs from the AutoFocus search. Two new artifacts have been added for each of the new embedded URLs: Mac Embedded URLs and APK Embedded URLs. You can also drill down into the sample details to view a list of the embedded URLs in a file.

**STEP 1 | Start an AutoFocus search** and select one of the new identifiers, either Mac Embedded URLs or APK Embedded URLs. Add any additional relevant search conditions and click **Search**.

**STEP 2 | Click on a sample hash to view the sample details.** The embedded URLs listed under a given sample are part of the file while the **Path** column indicates where the URL is located within the file.

The following example shows a list of Mac Embedded URLs in a DMG file.
STEP 3 | **Next steps:**

- Learn about how to customize your search with the AutoFocus search editor.
- Learn more about other AutoFocus artifacts types.

**Filter WildFire Dynamic Analysis Processes and Activities**

You can now filter the nested processes and activities content displayed in the WildFire Dynamic Analysis section of the sample details page. This allows you to remove extraneous or unnecessary content from cluttering up the sample details page.

**STEP 1** | **Start an AutoFocus™ search** and click on a sample hash that has undergone WildFire® dynamic analysis.

**STEP 2** | Scroll down to the WildFire Dynamic Analysis section and click on the filter icon ( ).
**STEP 3** | Add analysis filters options.

1. **Add Filter** to begin adding filter rules.
2. Select the analysis filter **Type**.
   - **Line Counts**—AutoFocus filters activities that exceed the user specified artifact limits.
   - **Regular Expression**—AutoFocus filters activities matching with the specified regular expression. Items in the Parent Process and Parameters columns are evaluated for matches.
3. Specify the analysis filter values.
   1. *(Line counts only)* Specify the limits for each of the activity artifacts (Benign, Malware, and Grayware) and click **Add**. If you do want to specify limits for certain activity artifacts, you can leave those input boxes blank.
   2. *(Regular expressions only)* Specify a regular expression in the RegExp text input box and click **Add**.
4. Repeat steps 1-3 for additional analysis filters, otherwise **Save changes**.

**STEP 4** | Scroll back down to WildFire Dynamic Analysis and view the activity sections. Filtered content is hidden by default but you can display them by clicking **Show filtered lines**.
STEP 5 | Filtered items that are displayed can be distinguished by the filter icon (✓).

STEP 6 | Remove analysis filters conditions.

1. Click on the filter icon (✓) to view the Analysis Filters.
2. Click on the (🗑️) next to the condition you want to delete, then Save changes.

Support for Archives (RAR / 7zip) and ELF File Types

WildFire® now analyzes RAR / 7zip archives and ELF files. In AutoFocus™, you can now search for archive and ELF samples and view related sessions, statistics, and WildFire analysis reports.
STEP 1 | Start an AutoFocus search based on File Type.

STEP 2 | Select any of the following file types to find samples based on the supported file types:
  - RAR Archive
  - 7zip Archive
  - ELF

STEP 3 | View the search results.

When you view the sample details for an archive file (RAR / 7zip), the archive contents are displayed showing the following:
  - # Files—The number of files in the archive file.
  - # Directories—The total number of directories in the archive file.
  - Max Directory Depth—Displays the number of subdirectories below the root directory.
  - File Information—Shows the details of the file, including verdict, size, type, and hashes.
Archive files that are multi-part or password protected cannot be analyzed.

- The archive file verdict is determined by the highest severity verdict of the archive contents.

**STEP 4 | Next steps:**

- Learn about how to customize your search with the AutoFocus search editor.
- Learn more about other AutoFocus Sample Details.
New Features: June 2017

The following topics provide a snapshot of the AutoFocus™ features introduced in June 2017. Each section includes context for the new feature, with steps to get started.

- Search Keyboard Shortcuts
- AutoFocus Tag Groups
- Export AutoFocus Tag, Search, and Indicator Data
- Secure AutoFocus Alerts
- Indicator Page Enhancements
- API Support for Enhanced Tag Retrieval

Search Keyboard Shortcuts

You can now change the placement of search conditions using the keyboard directional arrows. Using the keyboard can be a quicker and more efficient alternative to the mouse for changing the location of search conditions.

**STEP 1** | Open the search editor and begin a search.

For more information on configuring AutoFocus searches, refer to [Work with the Search Editor](#).

**STEP 2** | Add search conditions, child queries, and parent queries.

**STEP 3** | Adjust search condition placement using the keyboard.

Place the cursor over the left edge of a condition to display a directional icon. Click on the icon next to the condition or condition group you want to move and then use the keyboard arrows to change the placement. You can exit the keyboard movement mode by pressing the escape key or by clicking the selected condition.

Select and move a search condition up or down to position it. Depending on the placement of a search condition, you can use the keyboard to:

- Include it in a child or parent query.
- Remove it from a child or parent query.
- Create a parent or child query by pressing the right arrow key.

Refer to the AutoFocus Search for more information on using AutoFocus searches.

AutoFocus Tag Groups

An AutoFocus™ tag group is a collection of tags that are shown to connect to each other. The tags in a particular group can show relationships, such as family, type, and shared usage via attack campaigns. Tags are produced based on research done by the Unit 42 Palo Alto Networks® threat research team. If your organization has private tags that are related to a tag group, you can also add them to a group by editing the private tag settings.
There is a new Groups column in the group view (Tags > Groups) that indicates whether a tag is part of a group. A new parameter has also been added to allow searches by tag group.

Each WildFire cloud—global, regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.

*AutoFocus tag groups are continuously added as they are created by Unit 42.*

- Tag Group Search
- View Tag Groups
- Add Private Tags to a Tag Group

**Tag Group Search**

You can search for Samples, Sessions, Statistics, Indicators, and Domain, URL, & IP Address Information based on a specified tag group. In the following example, we’ll search for information related to the Ransomware tag group.

**STEP 1** | Start an AutoFocus search and select the new Tag Group artifact type in the search condition. In this example, we’ll looks for matches with Ransomware.

![AutoFocus Tag Group Search](image)

**STEP 2** | Search results matching with the tag group Ransomware display in the results pane. Hover over a tag group to view a list of specific tags associated with the group:

![AutoFocus Tag Group Result](image)

**View Tag Groups**

You can view a list of AutoFocus tag groups (Tags > Groups) as well as details about the groups.

**STEP 1** | Click Tags > Groups to view tag groups.
STEP 2 |
For each tag group, a description and the number of associated tags are shown. Click on ( ) next to a group to expand a list of tags. You can hover over a tag for additional details. For more information on using tags, refer to: AutoFocus Tags.

Add Private Tags to a Tag Group

If you have private tags with relevance to a tag group, you can add them to the group by editing your private tag settings.

STEP 1 | Select the private tag you want to add to the tag group. For more information on using tags, refer to: AutoFocus Tags.

STEP 2 | In the Tag Detail view (Tags > Groups > <tag-name>), edit ( ) the tag settings.

STEP 3 | Select the tag group(s) that you want to associate with your private tag.
STEP 4 | **Save changes** to commit the updates.

**Export AutoFocus Tag, Search, and Indicator Data**

You can now export AutoFocus™ tag, search, and indicator information into text, CSV, and JSON formats. Only the content that is displayed on the given page can be exported. For example, if you configure your sample search screen to show **First Seen**, **WildFire Verdict**, **SHA256**, and **Tags** with up to 50 results, your data export options are limited to those items. If you want to export more data elements, then configure the page to display the relevant options.

To export the tag page data, you must select an output format (options include Text, CSV, and JSON) and then the data type. Only one data type can be selected per text file-based export, however the CSV and JSON formats support exportation of all available columns shown on a page.

**STEP 1** | Navigate to a Search, Tag, or Indicator Store page and configure it to display the information you want to export. For example, add additional columns to a search page to export that content.

In the following example, **Threat Type** has been added to the **Indicator Store** page and becomes available as a data element for exportation.
STEP 2 | Click ( ) to open the Export Data page.

STEP 3 | Select the export data options.

1. Select the export file format. The number of data types that AutoFocus can export depends on the file format.
   - **Text**—AutoFocus exports a single user-selected data type into a text file format.
   - **CSV**—AutoFocus exports all information on a page into a table format using the comma-separated values (CSV) file format.
   - **JSON**—AutoFocus exports either all information on a page or a single user-selected data type into the JavaScript Object Notation file format.

2. Select the data type and sorting arrangement.
   1. Select a data type option from the Data drop-down.
   2. (Optional) Select Sort to rearrange the entries in ascending order except for dates, which are in descending order.
   3. (Optional) Select Unique to remove duplicate entries from the export list.

   *Sorting and arrangement options are available depending on the selected data type and file format.*
STEP 4 | **Download** the JSON, text, or CSV file.

STEP 5 | Next step:
- Use the Indicator Store to:
  - Manage Threat Indicators.
  - AutoFocus Search.
  - AutoFocus Tags.

**Secure AutoFocus Alerts**

Previously, AutoFocus™ HTTP alerts were transmitted in clear text over the Internet. You now have the option of sending notifications within a secure communications channel using HTTPS requests. Additionally, AutoFocus can authenticate a user on the web server receiving the HTTPS alerts with basic user authentication, providing another layer of security. All HTTPS requests use TLS 1.2 ciphers to negotiate security settings.

- **Supported TLS Ciphers**
- **Supported Trusted Certificate Authorities**
- **Create a Secure HTTPS Alert Action**

**Supported TLS Ciphers**

AutoFocus HTTPS alerts support only TLS 1.2 with the following ciphers:
TLS Ciphers Supported by AutoFocus

**TLSV1_2**

- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- AES128-SHA
- AES256-SHA
- AES128-SHA256
- AES256-SHA256
- AES256-GCM-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384

**Supported Trusted Certificate Authorities**

To enable HTTPS alerts, the server receiving the AutoFocus alerts must be signed by a trusted certificate authority (CA). To view a list and the details of trusted AutoFocus root certificate authorities (CAs), click Settings > Default Trust Certificate Authorities.

![Settings](image)

**Create a Secure HTTPS Alert Action**

In the following example, an HTTPS alert named **AutoFocus-alerts** is configured to send AutoFocus alerts to a web server using basic user authentication to enforce alert uploads.

**STEP 1** | Select Alerts > Settings.

**STEP 2** | Add Alert Action:
STEP 3 | Give the alert action a descriptive Name.

STEP 4 | Select HTTPS as the alert Type to configure AutoFocus to use a secure communications channel.

STEP 5 | Set the alert destination server URL.

Enter the URL of the server that you configured to receive HTTPS alerts. You can then test the connectivity to the server (Test URL). If the connection is valid, you will see ✔ Success.
Self-signed server certificates are not supported. Server certificates must be signed by one of the trusted certificate authorities (CAs). Refer to Supported Trusted Certificate Authorities for more information.

You can View supported cipher suites to see the list of supported TLS 1.2 trusted certificate authorities.

**STEP 6 |** Set the alert **Digest** to **5 Minutes** or **Daily**.

Digest sets the frequency with which AutoFocus checks for samples that match the alert criteria. AutoFocus collects all samples that match the alert criteria during the digest period and sends them in a single notification.

**STEP 7 |** Define the authentication method.

For HTTPS alerts using basic authentication:

Enter the credentials of an account that you configured on the server receiving the AutoFocus alerts.
STEP 8 | **Save Changes.**

The Action drop-down contains all saved alert actions, which you can apply to samples matched to Unit 42, public, and private tags.

---

STEP 9 | **Next steps:**

- Enable Alerts by Tag Type.
- Create Alerts.
- Learn more about AutoFocusalerts.

---

**Indicator Page Enhancements**

The AutoFocus Indicators Store (Indicators) now allows you to take action on a selected indicator. When you hover over an indicator, a drop-down (···) displays. Click on the drop-down to open additional tasks. From here, you can:

- **Add to Search**—Adds a condition to an existing search using the selected indicator value.
- **Add to New Search**—Opens a new search window and adds a search condition using the selected indicator value.
- **Domain and URL info (IP addresses and domains only)**—Retrieve detailed information about the indicator from PAN-DB, the Palo Alto Networks URL filtering database.

The following shows the new indicator drop-down with the new options.
API Support for Enhanced Tag Retrieval

The AutoFocus™ API can now filter a list of tags using the new query parameter. This parameter requires the use of tag identifiers along with corresponding parameter types and operators to change the scope of a search. To use this parameter, refer to the tag identifiers and compatible parameter types and operators.

For more information on using this API resource, refer to Get Tags.

- Tag Identifiers
- Parameter Types and Operators
- Request Sample

Tag Identifiers

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Artifact Type as it Appears on AutoFocus Web Portal</th>
<th>Field Type</th>
<th>Acceptable Values and Examples</th>
</tr>
</thead>
</table>
| alias      | Alias                                               | typeAheadSelect | Valid AutoFocus tag.  
Example: Cekar |
| customer   | Author Company                                      | String      | Valid organization that created the tag.  
Example: |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Artifact Type as it Appears on AutoFocus Web Portal</th>
<th>Field Type</th>
<th>Acceptable Values and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>author</td>
<td>Author Email</td>
<td>exactString</td>
<td>Valid email address of the tag creator. Example: <a href="mailto:john.doe@company.com">john.doe@company.com</a></td>
</tr>
<tr>
<td>tag_class</td>
<td>Class</td>
<td>Select</td>
<td>Valid tag class. Example: Malware Family</td>
</tr>
<tr>
<td>created</td>
<td>Created</td>
<td>Date</td>
<td>The creation date of a tag. Example: 2015-09-21T11:33:20</td>
</tr>
<tr>
<td>description</td>
<td>Description</td>
<td>String</td>
<td>The description contained in a tag. Example: advertising banners</td>
</tr>
<tr>
<td>comments</td>
<td># Comments</td>
<td>Number</td>
<td>The number of comments associated with a tag. Example: 2</td>
</tr>
<tr>
<td>lastComment</td>
<td>Last Comment</td>
<td>Date</td>
<td>The date of the last comment added to a tag. Example:</td>
</tr>
<tr>
<td>Field Name</td>
<td>Artifact Type as it Appears on AutoFocus Web Portal</td>
<td>Field Type</td>
<td>Acceptable Values and Examples</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------</td>
<td>------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>lastHit</td>
<td>Last Hit</td>
<td>Date</td>
<td>The time at which the most recent sample matched to the tag was detected. Example: 2016-19-21T11:31:10</td>
</tr>
<tr>
<td>matchCriteria</td>
<td>Match Criteria</td>
<td>String</td>
<td>The definition contained within a tag. Example: sample.exe</td>
</tr>
<tr>
<td>tag_name</td>
<td>Name</td>
<td>String</td>
<td>The name of an AutoFocus tag. Example: Sconato</td>
</tr>
<tr>
<td>reference</td>
<td>References</td>
<td>String</td>
<td>External references providing more information or context for the given threat. Example: Symantec</td>
</tr>
<tr>
<td>numSamples</td>
<td># Samples</td>
<td>Number</td>
<td>The total number of private and public samples matched to the tag. Example: 4</td>
</tr>
<tr>
<td>Field Name</td>
<td>Artifact Type as it Appears on AutoFocus Web Portal</td>
<td>Field Type</td>
<td>Acceptable Values and Examples</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------</td>
<td>------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>tagType</td>
<td>Scope</td>
<td>Select</td>
<td>A valid tag type. Example:</td>
</tr>
<tr>
<td>source</td>
<td>Source</td>
<td>String</td>
<td>Organization or individual that discovered the threat defined in the tag. Example: Secureworks</td>
</tr>
<tr>
<td>status</td>
<td>Status</td>
<td>Select</td>
<td>The current operational status of a tag. Example: Removing</td>
</tr>
<tr>
<td>upVotes</td>
<td># Up Votes</td>
<td>Number</td>
<td>The number of up-votes the tag has received from the AutoFocus community. Example: 2</td>
</tr>
<tr>
<td>updated</td>
<td>Updated</td>
<td>Date</td>
<td>The date and time that the tag was most recently modified. Example: 2016-19-21T11:31:10</td>
</tr>
</tbody>
</table>

**Parameter Types and Operators**

The following table lists the parameter types and corresponding operators for Tag Identifiers:
<table>
<thead>
<tr>
<th>Parameter Type</th>
<th>Available Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>contains, does not contain, proximity</td>
</tr>
<tr>
<td>bool</td>
<td>is true, is false, has no value, has any value</td>
</tr>
<tr>
<td>date</td>
<td>is in the range, is after, is before, is, has no value, has any value</td>
</tr>
<tr>
<td>exactString</td>
<td>is, is not, has no value, has any value</td>
</tr>
<tr>
<td>exactStringList</td>
<td>is, is not, is in the list, is not in the list, has no value, has any value</td>
</tr>
<tr>
<td>exactStringListRegexp</td>
<td>is, is not, is in the list, is not in the list, has no value, has any value, regexp</td>
</tr>
<tr>
<td>ipAddress</td>
<td>is, is not, is in the range, has no value, has any value</td>
</tr>
<tr>
<td>number</td>
<td>is, is not, is in the range, greater than, greater than or equal, less than, less than or equal, has no value, has any value</td>
</tr>
<tr>
<td>numberString</td>
<td>is, is not</td>
</tr>
<tr>
<td>select</td>
<td>is, is not, is in the list, is not in the list, has no value, has any value</td>
</tr>
<tr>
<td>simpleSelect</td>
<td>is, is not, is in the list, is not in the list</td>
</tr>
<tr>
<td>simpleStringList</td>
<td>is, is not, is in the list, is not in the list</td>
</tr>
<tr>
<td>singleSelect</td>
<td>is, is not</td>
</tr>
<tr>
<td>singleSelectVal</td>
<td>is, is not, has no value, has any value</td>
</tr>
<tr>
<td>string</td>
<td>contains, does not contain, has no value, has any value</td>
</tr>
<tr>
<td>stringList</td>
<td>contains, does not contain, is in the list, is not in the list, has no value, has any value</td>
</tr>
<tr>
<td>stringProx</td>
<td>contains, does not contain, has no value, has any value, proximity, regexp</td>
</tr>
<tr>
<td>tagList</td>
<td>is in the list, is not in the list, has no value, has any value</td>
</tr>
<tr>
<td>typeAheadSelect</td>
<td>is, is not, is in the list, is not in the list</td>
</tr>
</tbody>
</table>

**Request Sample**

The following example uses query to filter tags based on the inclusion of the string `4h`. It also includes optional request body parameters to further filter the results:
curl -X POST -H "Content-Type: application/json" -d '{
    "apiKey": "apikey",
    "scope": "unit42",
    "pageNum": 0,
    "pageSize": 3,
    "sortBy": "name",
    "order": "asc"
    "query": [{"field": "tag_name", "operator": "contains", "value": "4h"}]
}' 'https://autofocus.paloaltonetworks.com/api/v1.0/tags'
New Features: February 2017

The following topics provide a snapshot of the AutoFocus™ features introduced in February 2017. Each section includes context for the new feature, with steps to get started.

• AutoFocus-Hosted MineMeld
• Indicators View for Search Results
• Threat Summary Report
• New Artifact Type

AutoFocus-Hosted MineMeld

You can now use MineMeld directly in the AutoFocus™ interface, removing the need to deploy and host it in your own environment. MineMeld is an open-source threat intelligence processing tool that extracts threat indicators from various sources and compiles the indicators into multiple formats that are compatible with AutoFocus, the Palo Alto Networks® next-generation firewall, and other security information and event management (SIEM) platforms. An indicator is an artifact that security experts typically observe to detect signs that a network has been compromised.

Three types of MineMeld nodes make it possible to automate the flow of indicators from source to recipient:

• Miners extract indicators from sources of threat intelligence, such as a threat indicator feed or a threat intelligence service like AutoFocus.
• Processors receive indicators from miners and can aggregate indicators, eliminate duplicated indicators, and merge different sets of metadata for the same indicator. For example, a common type of processor is one that receives only IPv4 indicators.
• Outputs receive indicators from processors. Output nodes format the indicators and allow MineMeld to dynamically send the indicators to one or more destinations (for example, MineMeld can send indicators from external threat feeds to AutoFocus).

Nodes are the building blocks of MineMeld, and you can create the most basic MineMeld connection by connecting a single miner node to a processor node and connecting the processor node to an output node. For more information on MineMeld basics, view a Quick Tour of the MineMeld Default Configuration.
A major benefit of using AutoFocus-hosted MineMeld is the ability to forward indicators from AutoFocus to MineMeld and vice versa. You can now store up to 180 million indicators from external sources in AutoFocus, and AutoFocus highlights indicators in your samples that match these stored indicators.

MineMeld is available on a per support account basis. Follow the procedure below to get started with MineMeld.

**STEP 1 | Start MineMeld (Apps).**

**STEP 2 |** When MineMeld finishes deploying, access MineMeld from the navigation pane.
• Get an overview of miner, processor, and output nodes currently in use on the Dashboard.
• View a library of miner, processor, and output Prototypes you can clone to Create a MineMeld Node.
• View a complete list of Nodes you’ve created.
• Choose other nodes from which a node will receive indicators. Edit the inputs of the node Config to Connect MineMeld Nodes. The Config tab also allows you to Delete a MineMeld Node.
• View the Logs, which is a record of indicators that MineMeld extracted from feed sources.

For more guidance on how to use MineMeld, see MineMeld.

STEP 3 | To determine if any WildFire analysis artifacts for your samples match indicators from external threat feeds, Forward MineMeld Indicatorsto AutoFocus.
• Find sample indicators that match indicators from MineMeld.
• Click on the indicators tag to view all sample indicators that match indicators from MineMeld.

**STEP 4** | **Click Indicators** on the navigation pane to **Manage Threat Indicators** from MineMeld.

**STEP 5** | **To use AutoFocus as a source of indicators for MineMeld, Forward AutoFocus Indicators to MineMeld.**

You can forward indicators from:

- Samples that meet the conditions of an AutoFocus search.
- The Indicators Store (**Indicators**), if you need to forward indicators that MineMeld previously forwarded to AutoFocus to a destination outside of AutoFocus.
- An AutoFocus export list.

**Use AutoFocus Miners with the Palo Alto Networks Firewall, so that the firewall can dynamically retrieve AutoFocus indicators for an external dynamic list.**

**STEP 6** | **(Optional) While MineMeld is running, it extracts and processes indicators based on the nodes that are connected. To pause the retrieval of indicators through MineMeld or to restore MineMeld to its default configuration, learn how to Start, Stop, and Reset MineMeld.**

**Indicators View for Search Results**

AutoFocus™ now provides a way for you to view the **indicators** that WildFire® observed in your search results. Indicators help you identify the areas of activity in your network that are more vulnerable to attacks than others. The following types of artifacts are considered indicators in AutoFocus:
• IPv4
• Mutex
• URL
• Domain
• User agent

AutoFocus determines which artifacts are indicators through a statistical algorithm based on tendency of the artifact to be seen predominantly in malware samples.

STEP 1 | Start or continue an AutoFocus search.

STEP 2 | View the Indicators for the currently displayed page of search results. In the example below, you can see a consolidated view of the indicators from the fourth page of search results.

• Note the number of samples associated with suspicious and highly suspicious indicators.
• If you previously forwarded indicators from MineMeld to AutoFocus, indicators that match the forwarded indicators are marked with an indicator tag. Click on the tag to view the full list of matches.
• Expand an indicator to view the SHA-256 hash of the sample(s) in which AutoFocus detected the indicator.

View a complete overview of the Indicators tab.

STEP 3 | Return to the Samples search results, and view the Indicators for a sample.
STEP 4 | (Optional) Forward indicators from the search results to MineMeld.

**Threat Summary Report**

You can now view a threat summary report that provides a visual overview of malware trends in your network. The threat summary report also allows you to compare your malware trends with the overall trend for other AutoFocus™ customers in an industry. To reveal more about the nature of threats, the report includes the top AutoFocus tags that AutoFocus matched with your malware samples. You have the option to download a PDF of the report to view the report details offline.

STEP 1 | Click Reports on the navigation pane.

STEP 2 | Filter the data that the report displays.

1. Click Configure.
2. Select a time Period for the report data.
3. Generate the threat summary report.
STEP 3 | View the threat summary report details. For a more detailed explanation of each chart in the report, refer to the Threat Summary Report Overview.

- Observe the growth or decline of malware over a time period. Compare your trend with the trend for the industry associated with your AutoFocus support account.

- See a breakdown of your samples grouped by WildFire® verdict: malware, grayware, and benign. Compare the number of tagged malware samples against untagged malware samples.

- Determine which applications attackers most frequently used to deliver malware and the file formats in which they were delivered.
• Note the top tags matched with your malware samples to identify the most predominant threats in your network. The tags are sorted by tag class (malware family, campaign, and malicious behavior)

**STEP 4 | Download PDF** to generate a printable PDF version of the report.

**New Artifact Type**

You can now use the artifact type Status to find all samples that a Palo Alto Networks® firewall blocked. The AutoFocus API also supports this new artifact.
New Features: October 2016

The following topics provide a snapshot of the AutoFocus™ features introduced in October 2016. Each section includes context for the new feature, with steps to get started.

- WildFire Cloud Artifacts
- Customizable Dashboard
- Customizable Landing Page
- Visual Cues for Search Results
- New Artifact Types
- API Support for Session Aggregate Data by Upload Source
- API Support for Greater than 4,000 Results Using Pagination

WildFire Cloud Artifacts

AutoFocus™ receives sample and session information from WildFire™ clouds. Now, sample and session information in AutoFocus includes the WildFire cloud to which a sample was submitted for analysis.

- Find samples submitted to a specific WildFire cloud.
  1. Start an AutoFocus search with the sample artifact type **Region**.
  2. Select a WildFire cloud, and click **Search**.
  3. Click on a sample hash, and verify that the Region associated with the sample matches your selection.

It’s possible for different users to forward the same sample to more than one WildFire cloud; in this case, the Region information for the sample lists all WildFire clouds that received the sample.

To find samples that have been submitted to only a single WildFire cloud (and no other WildFire clouds), set up a search for a WildFire cloud. Then, add another search condition excluding samples submitted to the other clouds from the search results. For example, to search for samples that users submitted to the WildFire global cloud only,
search with the condition Region > is > US combined with the condition Region > is not for each of the other WildFire clouds.

- Find sessions associated with a specific WildFire cloud.
  1. Start an AutoFocus search with the session artifact type Region.
  2. Select a WildFire cloud, and click Search.
  3. Click Sessions to view session search results.
  4. Click on a session time stamp to view sessions details, and verify that the Region listed for the session matches your selection. A session can only be associated with a single WildFire cloud.

Customizable Dashboard

You can now customize the AutoFocus dashboard to display the types of information that are relevant to your organization. Add widgets or remove them based on your preferences. You can also now choose the order in which they appear on the dashboard. For example, to prioritize the most recent alerts triggered by samples on your network, add the Alerts Log widget to the top of your organization’s dashboard.

You can customize your organization, industry, and global dashboards. Dashboard settings are unique and saved for each user in a support account.
STEP 1 | To start customizing the dashboard layout and contents, click the Page Editor (1).

STEP 2 | Remove (2) or add a widget (3) based on your preferences. For more information on the different dashboard widgets, review the overview of the AutoFocus portal.

Add the new widget for the artifact Upload Source for a graphical overview of the top sources that requested a WildFire® verdict for a sample or submitted a sample to WildFire.

STEP 3 | Add (4) or remove a new row of widgets (5), and choose the number of widgets that appear in a row (6).

STEP 4 | When you are finished making your dashboard changes, click the Page Editor. To restore the dashboard settings, click the Page Editor drop-down and Reset Page to Default.

STEP 5 | View more details on how to customize the AutoFocus dashboard.

Customizable Landing Page

You can now choose the portion of the AutoFocus™ portal that displays by default after logging in to the portal. Choose a frequently used page, such as Search, as your default landing page. This setting is unique and saved for each user in a support account.

STEP 1 | View your portal settings and select a Landing Page.
STEP 2 | **Save changes.**

STEP 3 | To confirm that the new default landing page is in effect, log out of AutoFocus and log back in. The new landing page that displays should match your selection.

**Visual Cues for Search Results**

Visual cues now help you find the sample and session artifacts that match the conditions of your search. Visual cues are useful when viewing search results for artifact types that WildFire detects in both samples and sessions.

STEP 1 | **Start an AutoFocus search with a general artifact,** an artifact that WildFire detects in both samples and sessions.

STEP 2 | **Click a sample hash from the search results to view sample details.**

Spyglass icons now indicate the areas where a possible match for the artifact can occur. For example, when you search for a domain, spyglass icons indicate that AutoFocus may have found a matching domain in specific WildFire dynamic analysis categories or in the sessions associated with the sample.
STEP 3 | (Optional) Learn more about how to use AutoFocus artifact types to search for samples and sessions, and drill down in search results.

New Artifact Types

AutoFocus™ now provides the following artifact types that you can use to perform an AutoFocus search. The AutoFocus API also supports these new artifacts.

<table>
<thead>
<tr>
<th>Artifact Type</th>
<th>Search with this Artifact Type to Find...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Embedded File</td>
<td>Internal files in a Mac app installer or a Mac app bundle. Details for an embedded file can include the SHA256 and name of the installer or bundle, the file's SHA1 hash, filename, file format, file location, SHA256 hash, the signature associated with the file and the name of the signer, the SHA1 hash for the signature, signature status, and the file size in bytes. You can find this artifact in the file analysis details of a sample, under the WildFire® Static Analysis section.</td>
</tr>
<tr>
<td>Region (Sample)</td>
<td>The WildFire cloud that analyzed a sample. See WildFire Cloud Artifacts for more information. You can find this artifact in the file analysis details of a sample.</td>
</tr>
<tr>
<td>Region (Session)</td>
<td>The WildFire cloud associated with a session. See WildFire Cloud Artifacts for more information. You can find this artifact in session details.</td>
</tr>
<tr>
<td>Upload Source</td>
<td>The source that requested a WildFire verdict for a sample or submitted a sample to WildFire. You can find this artifact in session details. Choose from a list of possible upload sources:</td>
</tr>
</tbody>
</table>
### Artifact Type

<table>
<thead>
<tr>
<th>Artifact Type</th>
<th>Search with this Artifact Type to Find...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall</strong></td>
<td>Samples that a Palo Alto Networks® firewall forwarded to WildFire.</td>
</tr>
<tr>
<td><strong>Proofpoint</strong></td>
<td>Samples submitted to WildFire through Proofpoint products.</td>
</tr>
<tr>
<td><strong>Traps</strong></td>
<td>Samples submitted through Traps.</td>
</tr>
<tr>
<td><strong>Manual API</strong></td>
<td>Samples uploaded manually through the WildFire API or through the WildFire public portal.</td>
</tr>
<tr>
<td><strong>WF Appliance</strong></td>
<td>Samples that a WildFire WF-500 appliance submitted to the WildFire public cloud.</td>
</tr>
</tbody>
</table>

*For a graphical overview of the top upload sources in your network, industry, or globally, add the Upload Source widget to the AutoFocus Customizable Dashboard.*

### API Support for Session Aggregate Data by Upload Source

The AutoFocus™ API now allows you to view counts of most popular upload sources within sessions using the `upload_src` parameter. Possible upload sources include Firewall, Traps, Proofpoint, Manual API, and WF Appliance.

#### Request sample:

```bash
curl -X POST -H "Content-Type: application/json" -d '{
  "apiKey": "apikey",
  "field": "upload_src",
  "size": 10,
  "scope": "public",
  "query": {
    "operator": "all",
    "children": [
      {
        "field": "sample.malware",
        "operator": "is",
        "value": 1
      }
    ]
  }
}' "https://autofocus.paloaltonetworks.com/api/v1.0/sessions/aggregate/search"
```

### API Support for Greater than 4,000 Results Using Pagination

The AutoFocus™ API now allows you to get search results of up to 200,000 samples or sessions (normally 4,000) using pagination. When you enable pagination, each response contains a new page of results until the search is complete. To enable pagination, include the optional `type` parameter and set it to `scan`. You can change the size of each page using the optional `size` parameter, which defaults to 50 results. This feature is not available with STIX, and the `from` and `sort` parameters are also not available with pagination.

#### Example:

```bash
curl -X POST -H "Content-Type: application/json" -d '{
  "apiKey": "apikey",
  "query": {
    "operator": "all",
    "fields": [
      {
        "field": "sample.malware",
        "operator": "is",
        "value": 1
      }]
  }
  "type": "scan",
  "size": 50
}' "https://autofocus.paloaltonetworks.com/api/v1.0/search"
```
"children": [  
  
  
  
  
  
  
  
  
  
  
  "field": "sample.malware",
  "operator": "is",
  "value": 1
  }
],
"size": 50,
"type": "scan",
"scope": "public"
}' "https://autofocus.paloaltonetworks.com/api/v1.0/samples/search"
New Features: August 2016

The following topics provide a snapshot of the AutoFocus™ features introduced in August 2016. Each section includes context for the new feature, with steps to get started.

- Session-Based Tagging
- Single Search for All Tag Conditions
- Support for Mac OS X File Types
- New Artifact Types

Session-Based Tagging

You can now tag search conditions that pertain to session information. You can find session information when you view the network sessions related to a sample or session details in your search results.

**STEP 1** | Start an AutoFocus™ search for session information.

- The list of **Session Identifiers** includes types of artifacts that pertain exclusively to session-related information:

  ![Session Identifiers](image)

  - The following types of artifacts pertain to information that you can find in both sample and session search results: Domain, Email Address, Filename, Hash, IP Address, URL, and User Agent.

**STEP 2** | Click the tag icon to create a tag based on your search conditions.

**STEP 3** | Verify that you created the tag successfully.

1. Click **Tags** on the navigation pane.
2. Type the name of the tag you just created in the quick search field to quickly locate the tag.
3. Click on the tag to view the search conditions in the tag details. New tags are private by default.
Single Search for All Tag Conditions

You can now add all of the conditions that define a tag to an AutoFocus™ search with a single click. Searching with the tag itself returns all samples and sessions that match at least one of the tag conditions; adding all tag conditions to a search allows you to disable or delete tag conditions that you would like to exclude from the search. It also provides a quick way to create a new tag, as you can modify the conditions of an existing tag and save them under a different tag name.

**STEP 1 |** In the Tags view, click a tag.

**STEP 2 |** Click the Search All icon, located after the last set of tag conditions, to add all of the tag conditions to an AutoFocus search. The example below has three sets of tag conditions.

**STEP 3 |** View the search results to see samples and sessions that match the tag conditions. Notice in the figure below that the three sets of tag conditions from Step 2 were added to a new search.

To view samples and sessions that only match some tag conditions and not others, Disable the tag conditions you want to exclude from the search and click Search. Alternatively, you can delete some of the tag conditions and create a new tag.
STEP 4 | Next step:
   Learn more about how to customize your search with the AutoFocus search editor.

Support for Mac OS X File Types

WildFire™ now analyzes Mac OS X files. In AutoFocus™, you can now search for samples that are Mac OS X files and view related sessions, statistics, and WildFire analysis reports.

STEP 1 | Start an AutoFocus search based on File Type.

STEP 2 | Select any of the following file type options to find Mac OS X samples:
   - Apple's Universal binary file
   - Mac OS X app bundle in ZIP archive
   - Mac OS X app installer
   - Mac OS X DMG
   - Mach-O

STEP 3 | View the search results. When you view the WildFire analysis section for a Mac OS X sample, the new artifact type Mac Embedded URLs displays any URLs that are found in the sample.

New Artifact Types

New types of artifacts allow you to search based on new WildFire® static analysis information for APK files and embedded URLs in Mac samples. The AutoFocus™ API supports searches with these new artifacts.

For guidance on how to search effectively in AutoFocus, refer to Search Operators and Values and the Guidelines for Partial Searches.

To navigate to an artifact type in the search editor quickly, Find an Artifact Type.

<table>
<thead>
<tr>
<th>Artifact Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>APK App Icon</td>
<td>The file path for the icon of the app that the APK file installs.</td>
</tr>
<tr>
<td>Artifact Type</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>APK App Name</td>
<td>The name of the app when it displays on an Android device.</td>
</tr>
<tr>
<td>APK Certificate File</td>
<td>The file path for the certificate(s) that the app owner used to sign the APK file, information about the certificate owner and issuer such as name and location (if available), and the MD5, SHA1, and SHA256 hashes used to sign the certificate.</td>
</tr>
<tr>
<td>APK Internal File</td>
<td>The file format, file path, and SHA256 of the files included in the APK file.</td>
</tr>
<tr>
<td>APK Suspicious Behavior</td>
<td>A sequence of actions that the APK file exhibits, the target of the actions (if there is one), and the location of the files that exhibited the actions. For example, for the suspicious behavior “APK files sends an SMS to a fixed number,” the target is the phone number that received the SMS.</td>
</tr>
<tr>
<td>APK Suspicious Pattern</td>
<td>A class of patterns observed in the APK file, a description what the pattern does, and the location of the files where the pattern occurred.</td>
</tr>
<tr>
<td>Artifact Type</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Suspicious Pattern</strong></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Suspicious Pattern Table" /></td>
<td></td>
</tr>
<tr>
<td><strong>Mac Embedded URLs</strong></td>
<td>URLs that are part of a Mac file. The Path column contains the path for the section of the app where the URL is located.</td>
</tr>
<tr>
<td><img src="image" alt="Mac Embedded URL Table" /></td>
<td></td>
</tr>
</tbody>
</table>

**Mac Embedded URLs**

<table>
<thead>
<tr>
<th>URL</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://mail.google.com/mail">http://mail.google.com/mail</a></td>
<td>installer.app/Contents/MacOS/AppRC</td>
</tr>
<tr>
<td>com.apple.xbs/Sources/arc4ite/arch-65/libexec</td>
<td>installer.app/Contents/MacOS/AppRC</td>
</tr>
<tr>
<td><a href="https://www.apple.com">https://www.apple.com</a></td>
<td>installer.app/Contents/MacOS/AppRC</td>
</tr>
<tr>
<td><a href="https://mail.google.com/mail">https://mail.google.com/mail</a></td>
<td>installer.app/Contents/MacOS/AppRC</td>
</tr>
</tbody>
</table>
New Features: June 2016

The following topics provide a snapshot of the AutoFocus™ features introduced in June 2016. Each section includes context for the new feature, with steps to get started.

- New Tag Colors and Icons
- Improved Workflow to Export Artifacts
- API Support for Sample Behavior Evidence
- API Support for Signature Coverage
- Search Enhancements
- WildFire DNS History for Domains, URLs, and IP Addresses
- Process Tree
- Default Search Scope
- Sort by Column Headers
- Remote Search Enhancements
- Find Tags with the Most Recent Comments

New Tag Colors and Icons

New colors and icons for AutoFocus™ tags allow you to quickly determine the tag type and tag class.

- Tag Color and Icon Enhancements
- Tag Class Icons

Tag Color and Icon Enhancements

Changes to the tag colors and icons now clearly set apart the different tag types. For all tag types:

- The icon now changes into a tag class icon when you link a tag to a tag class (see Tag Class Icons). For example, Unit 42 tags that are linked to a particular tag class have Tag Class Icons instead of the Unit 42 icon.
- The icons are larger for improved visibility.

<table>
<thead>
<tr>
<th>Tag Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Unit 42 Tag]</td>
<td>Unit 42 (alerting) tags are created by Unit 42 (the Palo Alto Networks® threat intelligence and research team) for threats and campaigns that pose a direct security risk.</td>
</tr>
<tr>
<td>![Unit 42 Tag]</td>
<td>Unit 42 now creates alerting tags for threats discovered by individuals or organizations outside of Unit 42. These tags have a pointed and marked top right corner.</td>
</tr>
<tr>
<td>![Unit 42 Informational Tag]</td>
<td>Unit 42 informational (non-alerting) tags are created by Unit 42 for commodity threats.</td>
</tr>
<tr>
<td>![Unit 42 Informational Tag]</td>
<td>Informational tags now have a faded orange instead of faded gray outline.</td>
</tr>
<tr>
<td>![Unit 42 Informational Tag]</td>
<td>Unit 42 now creates informational tags for threats discovered by individuals or organizations outside of Unit 42. These tags have a pointed and marked top right corner.</td>
</tr>
</tbody>
</table>
Tag Type | Description
--- | ---
[My Tag] | Your private tags (blue outline) that are visible only to your organization.
[Public Tag] | Public tags (gray outline) are shared and visible to all AutoFocus users.

### Tag Class Icons

New tag icons based on tag class let you see at a glance whether a tagged sample is:

- ![Spider](tag-class-icon-spider.png) Linked to threats that belong to a certain **Malware Family**
- ![Airplane](tag-class-icon-airplane.png) Part of a larger **Campaign** of attacks
- ![Police Hat](tag-class-icon-police-hat.png) Linked to a threat **Actor**
- ![Skull](tag-class-icon-skull.png) Linked to an **Exploit**
- ![Biohazard](tag-class-icon-biohazard.png) A type of **Malicious Behavior** that indicates that your system has been compromised

Note that the color of the tag class icon depends on the **Tag Type**. For example, a public tag linked to malicious behavior will have a gray malicious behavior icon:

![Example Tag](example-tag-1.png)

### STEP 1 | Find a tag to link to a tag class.

Edit an existing tag. You can only edit tags that you created; you cannot edit tags created by others, such as by Unit 42.

1. Click a tag to view the tag details.
2. **Edit** the tag details.

You can also **tag a sample or a search**.

### STEP 2 | Select a **Tag Class** for the tag.
STEP 3 | **Tag Results** that match the conditions of the tag.

STEP 4 | Verify that the changes you made to the tag were saved.

1. Click **Tags** on the navigation pane.
2. Type the tag name in the quick search field to quickly locate the tag.
3. Verify that the tag icon matches the tag class you selected in Step 2.

STEP 5 | Next steps:
- Learn more about the different **tag classes**.
- Find samples based on tag class.

**Improved Workflow to Export Artifacts**

You can now choose multiple artifacts to add to an export list (instead of adding artifacts to an export list individually). In addition, enhancements to the AutoFocus™ Exports page streamline the process for exporting artifacts.

- Add Multiple Artifacts to an Export List
- Get Started with the New Exports Page

**Add Multiple Artifacts to an Export List**

You can now select multiple artifacts from a WildFire® analysis category to add to an export list.

STEP 1 | Start an **AutoFocus™** search.

STEP 2 | Drill down on the sample details, and view the **behaviors and activities** that were observed in the sample when it executed in the WildFire analysis environment.

STEP 3 | Open the drop-down for a WildFire analysis category and **Select for Export List**. Notice that the drop-downs next to the artifacts turn into check boxes.
STEP 4 | Select one or more artifacts from the list.

STEP 5 | Re-open the drop-down for the category and Add Selected to Export List.

STEP 6 | Next steps:
- Continue to build an export list.
- Create a CSV file based on an export list to use with a Palo Alto Networks® firewall or a security information and event management (SIEM) tool.

Get Started with the New Exports Page

STEP 1 | View the new Exports page:

1—Click Exports on the navigation pane to view your export lists.
2—Previously, the Exports page displayed a comprehensive list of all artifacts added to an export list. Now, the page displays all of your export lists:
- Sort by Column Headers to change the order by which you view the lists.
- View an export list: The export list will display all artifacts that were added to it.
3—In the Actions column, click **Export** to:

- Export all artifacts added to the export list.
- Export artifacts that were added to the export list within a date range.

**STEP 2 | View an export list:**

![AutoFocus exports page](image)

1—Display:

- View the export list name (Label) and the list of artifacts that have been added to it.
- **Sort by Column Headers** to change the order by which you view the artifacts.

2—Export action (dynamically updates depending on the artifacts selected):

- Select one or more artifacts and **Export Selected Items** to a comma separated value (CSV) file.
- If no artifacts are selected, you can **Export All Items** in the export list to a CSV file.

3—Delete action (dynamically updates depending on the artifacts selected):

- Select one or more artifacts you want to remove from the export list and **Delete Selected Items**.
- If no artifacts are selected, you can **Delete All Items** to remove all artifacts from the export list. This also deletes the export list.

**STEP 3 | Next steps:**

- **Build an export list.**
- **Create a CSV file** based on an export list to use with a Palo Alto Networks® firewall or a security information and event management (SIEM) tool.

**API Support for Sample Behavior Evidence**

The AutoFocus™ API now provides a summary of behavior evidence, when applicable, in sample analysis. This is an extension of behavior evidence that is available through the AutoFocus portal. Behavior evidence lists the behaviors seen for a given sample in the WildFire® analysis environment, such as whether a sample has created files, started a process, or modified registry settings.

Truncated response:

```json
{}
```
API Support for Signature Coverage

The AutoFocus™ API now allows you to view the WildFire® signatures that are available to identify a malware sample. In addition to the observed properties, behaviors, and activities included in sample analysis results, the API request can specify "coverage": "true" to include WildFire signature coverage in sample analysis:

```
curl -X POST -H "Content-Type: application/json" -d "{"apiKey":"apikey","coverage":"true"}" "https://autofocus.paloaltonetworks.com/api/v1.0/sample/0759049506430d46304c84f757e4e8e3b0f634a9e9fc06f6db01ce8c0bcb856daa/analysis"
```

Truncated response:

```
"coverage": {  "wf_av_sig": [  {
   "name": "Worm/Win32.mydoom.nszw",
   "create_date": "2016-05-05T14:33:12.000Z",
   "first_added_daily": 1868,
   "last_added_daily": 1868,
   "first_added_15min": 96265,
   "last_added_15min": 96265,
   "first_added_5min": 33799,
   "last_added_5min": 33799,
   "currently_present_daily": false,
   "currently_present_15min": false,
   "currently_present_5min": false
  }
],
"dns_sig": "Not Available",
"fileurl_sig": "Not Available",
"url_cat": [  {
   "url": "nserver3.apple.com",
   "cat": "Computer and Internet Info",
   "importance": 1
  }
}
```

Search Enhancements

- Search with New APK Artifacts
- Clear a Search Condition Value
Search with New APK Artifacts

WildFire® now categorizes new properties when performing static analysis on an Android Package (APK) file. In AutoFocus™, you can search for APK files based on these properties.

**STEP 1** | Start an AutoFocus search with any of the following new types of APK artifacts:

- APK Certificate
- APK Embedded Libraries
- APK Package Name
- APK Repackaged
- APK Signer
- APK Version

**STEP 2** | View the WildFire analysis information for the APK artifact type you selected in the previous step.

1. Click a sample hash from the list of search results, and view sample details.
2. In the WildFire Static Analysis section, expand the APK property to view more details.

**STEP 3** | *(Optional)* Start a new search for any suspicious or highly suspicious artifacts (see Multiple Active Searches).
Clear a Search Condition Value

You can now clear a value you have entered for an artifact type with a single click. Click the x in the search field to clear it.

![Search Field]

WildFire DNS History for Domains, URLs, and IP Addresses

When you search for a domain, URL, or IP address, you can now view an active DNS history from WildFire® (in addition to related URLs from PAN-DB and passive DNS history). The WildFire DNS history is a log of DNS activity collected from all WildFire submissions that contain instances of the domain, URL, or IP address. Review the WildFire DNS history to assess whether the domain, URL, or IP address is associated with malicious activity.

**STEP 1 |** Start an AutoFocus™ search for a domain, URL, or IP address.

*If you are viewing a domain, URL, or IP address in the File Analysis details for a sample, you don’t have to add it to a new search; you can simply click the drop-down next to it, select Domain and URL info, and skip to Step 3.*

**STEP 2 |** Click the target icon or the search result listed in Domain, URL & IP Address Information.

**STEP 3 |** Notice the new WildFire DNS History section, which lists domain to IP address mappings. The mappings are based on all samples that launched a request to connect to a domain during WildFire analysis. Find matches to the domain, URL, or IP address you searched for in the Request and Response columns.
• **Request**—The domain to which the sample attempted to connect.
• **Response**—The domain or IP address mapped to the domain Request.
• **Type**—The DNS record type, which describes the file that was used to map the domain Request to the IP address or domain Response. For example, an A record type maps a domain to an IP address, while a CNAME record type maps a domain to another "alias" domain.
• **First Seen**—The date and time that WildFire first detected the Request, Response, and DNS record Type.
• **Last Seen**—The most recent date and time that WildFire detected the Request, Response, and DNS record Type.

**STEP 4** | Next step:
Learn more about domain, URL, and IP address information.

**Process Tree**

The process tree allows you to distinguish the groups of parent and child processes that occurred when the sample launched in the WildFire® virtual sandbox. For each sandbox operating system in which the sample was executed, the processes that took place in the operating system kernel space and user space are provided.

**STEP 1** | Start or continue an AutoFocus™ search to find a sample.

**STEP 2** | Click a sample hash to view its WildFire analysis details.

By default, the analysis results for a sample are sorted based on WildFire behavior and activity categories.

**STEP 3** | Click the new option Tree.
STEP 4 | Expand the kernel space and user space sections to view the processes that occurred when the sample executed in the WildFire analysis environment. Refer to the File Analysis section of sample search results for more information on kernel space and user space.

Notice that child processes are indented and grouped under the parent process that spawned them. If a child process launched other child processes or activities, they are listed under the child process and indented accordingly.

STEP 5 | Minimize and expand processes as you view them.

Click the minus sign (-) next to a parent process to hide the child processes under it; click the plus sign (+) next to a parent process to display its child processes.

STEP 6 | Next step:

Select Sections to view sample details based on WildFire analysis categories or Display File Analysis Results in Sequence.

Default Search Scope

When you perform an AutoFocus™ search, you can filter the search results to display only your samples (private samples), only public samples, or both private and public samples. Previously, AutoFocus displayed private samples by default. A new Preferred Scope setting now allows you to choose the default scope for filtering search results.

STEP 1 | On the Settings page, select a Preferred Scope for your search results.
STEP 2 | Save changes.

STEP 3 | To verify that the new default scope is in effect, start or continue a search. The search results will match the scope that you selected in Step 1. You can click any of the other scope options to change the scope of the displayed search results.

Sort by Column Headers

You can now click the column headers in AutoFocus™ search results, alerts, tags, and export lists to sort (instead of clicking Sort by).

STEP 1 | Choose Columns to display in your search results, alerts, tags, or export lists.

STEP 2 | Click a column header to sort by the column contents. The contents of each column are sorted in Ascending order by default:

- Dates and times—Oldest or least recent dates and times are displayed first.
- Numbers—Lowest values are displayed first.
- Alphanumeric—Values are sorted alphanumerically starting with numbers 0-9, followed by letters A-Z.
The arrow next to the column header indicates the direction that the table is sorted. The up arrow indicates that the column is sorted in **Ascending** order; the down arrow indicates that it is sorted in **Descending** order.

In general, when you sort search results in **Ascending** order, rows with no reported values for the column header category are displayed first; however, when you sort the tags list, rows with no reported values for the category are displayed last regardless of the sort order.

**STEP 3** | Click the column header again to reverse the order of the column contents and corresponding rows (**Descending** order).

### Remote Search Enhancements

- **Add a Search Condition to a Remote Search**
- **Increased Limit for Remote Systems**

#### Add a Search Condition to a Remote Search

Previously, you could only add artifacts found with search results to a remote search. Now, you can add a condition from an existing search to a remote search as long as it is one of the following artifact types: SHA256 hash, IP address, user agent, filename, or URL.

> The remote search feature is supported with firewalls running PAN-OS® 7.1 or later release versions.

**STEP 1** | Start or continue an **AutoFocus™** search.

**STEP 2** | To look for matches to a search condition in a targeted firewall or system, select the ellipsis icon for the condition and **Add to Remote Search**.

You can only add a condition to a remote search if it is one of the following artifact types: SHA256 hash, IP address, user agent, filename, or URL.

**STEP 3** | Open the current **Remote Search** to verify that the search condition was added.
STEP 4 | Next steps:

- Set up a remote search.
- Learn more about the different ways to perform an AutoFocus search.

**Increased Limit for Remote Systems**

You can now save up to 500 remote systems to search remotely with AutoFocus. Navigate to the AutoFocus portal **Settings** to view your remote systems and to add more.

Learn more about how to set up a remote search.

**Find Tags with the Most Recent Comments**

You can now sort tags based on the date and time of the most recently submitted comment. This allows you to find tags with the most recent feedback from the AutoFocus™ community.

**STEP 1 |** Click **Tags** on the navigation pane.

**STEP 2 |** Choose **Columns** and select **Last Comment** to display dates and times for the most recently submitted tag comments.
STEP 3 | Continue to Sort by: Last Comment.

When you sort by Last Comment, tags with no comments (and, therefore, no Last Comment information) are listed in no particular order after the final tag with comments.

You can Sort by Column Headers to sort the rows by Last Comment more quickly.

STEP 4 | Click Sort Descending to view tags with the most recently submitted comments; click Sort Ascending to view tags with the oldest or least recently submitted comments.

STEP 5 | Next steps:

- Continue to find tags, including tags with the most hits, the top tags detected during a selected date range, and the top tags found with search results.
- Vote for, Comment on, and Report Tags.
New Features: March 2016

The following topics provide a snapshot of the AutoFocus™ features introduced in March 2016. Each section includes context for the new feature, with steps to get started.

- AutoFocus API STIX Support
- Signature Coverage for Samples
- Sample Behavior Evidence
- Remote Search
- Quick Search
- Multiple Active Searches
- API Request for a Search
- Search Filter Enhancements
- Tag Filter Enhancements
- AutoFocus Feedback Tool

AutoFocus API STIX Support

The AutoFocus™ API now supports STIX (Structured Threat Indicator eXpression) responses. STIX is an easily consumable and standardized data model for cyber threat information expressed through structured XML.

STIX support is currently available through the following API resources:

- /stix/samples/search/—Search samples
- /stix/samples/results/{af_cookie}—View the current search results of the given ID (af_cookie). This resource returns the latest results of /stix/samples/search/.
- /stix/sessions/search/—Search sessions during which samples match search conditions.
- /stix/sessions/results/{af_cookie}—View the current search results of the given ID (af_cookie). This resource returns the latest results of /stix/samples/search/.
- /stix/sample/{sample_id}/analysis/—View file analysis data related to a specified sample. The results of this search correspond to the File Analysis tab shown when you click a sample hash on the search editor.
- /stix/tags/—View a list of all tags.
- /stix/tag/{public_tag_name}—View tag details for the given public tag name.

Refer to the AutoFocus API Reference for more information on viewing STIX responses through the AutoFocus API.

Signature Coverage for Samples

WildFire® generates signatures to identify newly-discovered malware and distributes these signatures to Palo Alto Networks® firewalls. The firewalls compare incoming traffic against WildFire signatures to protect against known malware. Now, when viewing details for a specific sample in AutoFocus™, you can find the WildFire signatures that the sample triggers. You can check signature coverage to assess the level of protection in place for malware.

**STEP 1** | Perform an AutoFocus search and view the samples matched to your search.

**STEP 2** | Select a specific sample hash to view sample details and then select Coverage:
STEP 3 | Review the signatures that match the sample:

Depending on the sample, all or some of the following signature types provide coverage:

1. **WildFire AV Signatures**—WildFire antivirus signatures identify malicious files. Examples of malware for which antivirus signatures provide protection include viruses, worms, Trojans, and spyware downloads.

2. **C2 Domain Signatures**—Command and control (C2) domain signatures identify malicious domains that the sample attempted to resolve to when executed in the WildFire analysis environment.
3: **Download Domain Signatures**—Download domain signatures identify domains that host malware (and from which the sample was downloaded).

4: **URLs**—URLs the sample visited when executed in the WildFire analysis environment, and the PAN-DB categorization for each URL.

5: **Signature Dates and Content Versions**—WildFire antivirus, C2 domain, and download domain signatures also include the following information:

- **Create Date**—The date WildFire created the signatures (depending on the WildFire updates schedule configured on the firewall, the firewall could have retrieved this signature within 5 minutes of the creation date).
- **Content Versions**—Signatures are packaged in content updates and made available for Palo Alto Networks firewalls to automatically download and install. The available content updates and the frequency the firewall can get the latest updates depend on the subscriptions you have.
- Check the content versions which included the signature. The content versions vary depending on whether the signature was distributed as part of a **daily**, **15 min**, or **5 min** signature update.
- For example, if the firewall retrieves WildFire signatures as part of the daily Antivirus content updates, select **daily** to see the content version that included the signature. If the firewall has a WildFire license and gets WildFire 5-minute updates, select **5 min** to view the content version that included the signature.
- Check the **First** content version that included the signature, and the **Last** content version to include an update to the signature.
- Check whether the signature is included in the most **Current** content version.

**Sample Behavior Evidence**

AutoFocus™ provides a summary of the behaviors samples displayed in the WildFire® analysis environment. Now, for each observed behavior, you can see the specific sample activities that are evidence of that behavior.

**STEP 1** | Perform an **AutoFocus search** and view the samples matched to the search.

**STEP 2** | Select a sample hash to view sample details.

**STEP 3** | Select **Observed Behavior**:

[Diagram of WildFire Dynamic Analysis]

**STEP 4** | Check the new **Evidence** column for the total number of sample activities that substantiate each observed behavior, and expand a single behavior for the list of matching activities.
For each activity listed, the Type column indicates the activity category and the Value column includes activity artifacts. The artifacts displayed might vary depending on the activity category. In the example below, the File Activity artifacts provided include the parent process that showed activity, the action the process performed, and the file that was altered.

STEP 5 | (Optional) Add the activity artifacts to an existing search or a new search.

AutoFocus supports Multiple Active Searches. Adding the artifacts to a new search does not clear the existing search; instead, the new search is opened in a new browser tab.

Remote Search

You can now use AutoFocus™ to find suspicious IP addresses, SHA256 hashes, URLs, user agents, and filenames in a specific Palo Alto Networks® firewall or a set of Panorama-managed firewalls. AutoFocus looks for matches to the suspicious artifacts in the firewall log entries. When you launch a remote search, the firewall or Panorama™ web interface opens in a new window and displays the search results in Unified log view.

The remote search feature is only supported in firewalls running PAN-OS® 7.1 or later release versions.

AutoFocus also now supports the ability to integrate with third-party log management systems. When you configure your custom system to work with AutoFocus remote search, you can filter log or event repositories with AutoFocus search conditions.

STEP 1 | Log in to the firewall or Panorama you want to search with your administrator username and password.

STEP 2 | Configure the settings of the remote system.

Allow HTTP or HTTPS service on the management interface of your firewall or Panorama. Select the service that matches the address of the remote system you want to search.
STEP 3 | Add a remote system to search with AutoFocus.
   1. Select **Settings** on the navigation pane.
   2. **Add new** remote systems.
   3. Enter a descriptive **Name** for the remote system.

![Add Remote System](image)

4. Select a System Type:
   1. Select **PanOS** to add a firewall or Panorama.
   2. Select **Custom** to add a custom system that has been configured to integrate with AutoFocus remote search.
5. Enter the IP **Address** or URL of the remote system.
6. **Save changes**.
7. **Save changes** again to finish adding the remote system. You can add up to ten remote systems.

![Remote Systems](image)

STEP 4 | *(For Panorama Device Group and Template Administrators Only)* For Panorama Device Group and Template administrators (not superusers), an AutoFocus remote search targeted to Panorama returns results based on the current Panorama **Access Domain** setting. Panorama administrators with role-based access control must first open the Panorama web interface, select **Monitor > Logs** and set the **Access Domain** for which to view search results. Return to the AutoFocus portal to execute your remote search.

STEP 5 | Start a remote search.
   1. Select **Search** on the navigation pane.
   2. Click **Remote Search**.

![Search](image)

3. Add IP addresses, URLs, user agents, SHA256 hashes, or filenames to the remote search.
You can add artifacts from the results of an existing search to the remote search. Open Remote Search again to verify that the artifact was added as a search condition.

4. Set the remote search to find Any or All of the artifacts on the targeted system.
5. Select one or more Remote systems to search.
6. Click Search.

**STEP 6 |** View the search results. A new browser tab opens for each remote system.

If no browser tabs open when you launch remote search, change the settings on your browser to allow pop-ups from AutoFocus.

The Unified log displays all log entries that contain the artifacts added to the remote search.
If the remote search is for Panorama, the Unified log displays log entries from all managed firewalls, including those that are running PAN-OS 7.0 and earlier release versions.

If the remote search is for a custom system, the custom system opens in a new tab, with the URL formatted to include the conditions specified in the remote search.

**STEP 7 |** Next steps:

- Learn more about working with **Unified logs** on the firewall.
- View more details on how to set up **remote search**.
- Explore more ways to use **AutoFocus with the Palo Alto Networks firewall**.

**Quick Search**

Previously, the only way to start an AutoFocus search was to navigate to the search editor. With quick search, you can start searching for an artifact from any page on the AutoFocus portal. Quick search also lets you narrow down the scope of the search for the artifact.

[Watch the tutorial.](#)

**STEP 1 |** Click the spyglass icon in the support account area of the portal.

*You can also press Alt+s to open quick search. To close quick search, click the x on the top right corner of the search box or click anywhere on the dimmed area of the interface.*
STEP 2 | Enter an artifact to search.

When an artifact is incomplete, quick search suggests a list of artifact types that it recognizes.

STEP 3 | Select the scope of the search based on the artifact type.

For example, the string `ImASampleFile.pl` can be a **Filename**, a **Domain**, or a **URL**. To search for the file `ImASampleFile.pl`, select an area to search under the artifact type **Filename**.

STEP 4 | View the search results.

STEP 5 | Next steps:

- Refine your search.
- Drill down in search results.
- Learn more about **high-risk artifacts** indicated in search results.
Multiple Active Searches

AutoFocus now supports the ability to perform multiple, simultaneous searches. Previously, you could only have a single active search in AutoFocus. Now, you can preserve the conditions of an existing search and launch a separate search in a different window.

- **Add a search condition to a new search.**
  
  Click the ellipsis icon next to a search condition and select **New Search**. An AutoFocus search for the condition opens in a new browser tab.

- **Add an artifact to a new search.**
  
  Click the down arrow next to an artifact and select **Add to New Search**. Instead of adding the artifact as a condition to the existing search, AutoFocus starts a new search for the artifact in a new browser tab.

  *Find artifacts to add to a new search in the File Analysis and Session Summary tabs of the search results.*
Next step:
Refine your search.

API Request for a Search

You can now view the API request for initiating an AutoFocus Search directly from the AutoFocus interface. The API request is for retrieving samples, sessions, or statistics that meet the conditions of the current AutoFocus search. This feature is useful for quickly generating API requests for complex searches to use with your external application. Note that the API request provided by this feature is only to start an AutoFocus search; a different API request is required to view the search results.

STEP 1 | Start or continue an AutoFocus search.

STEP 2 | View the API request for initiating the search.

- View (>_ API) the API request for Samples or Sessions that have been filtered according to the current search condition(s).
• View (>_) the API request in any of the Statistics widgets for artifacts that meet the conditions of the current search and widget. In the following example, the API request for Top Malware is only for retrieving the ten most prevalent malware samples in your network.

![API request example](image)

**STEP 3** | Toggle between Python and Curl to select the format of the API request that you want to copy to clipboard.

The API request reflects the parameters of the search you performed. For example, the sample Curl URL Request Library (cURL) API request above is from the Top Firewalls widget (Statistics). We can tell from the code that the API request:

- Retrieves the top ten firewalls ("size":10) with the most sessions that use the **web-browsing** application ("field": "device.serial", "operator": "is", "value": "web-browsing").
- Retrieves the **Serial** numbers of the firewalls ("field": "device.serial").
- Limits the scope of the request to private samples only ("scope": "private").

**STEP 4** | Next steps:

- Refer to the AutoFocus API Reference Guide for more information on how to view the results of an API request.
- Learn more about how to use cURL and Python to integrate the AutoFocus API with your application. To use the AutoFocus API with Python, install the pan-python package, which provides a Python and command line interface for AutoFocus.
Search Filter Enhancements

In the search editor, you can now clear your current search with one click (instead of clearing each search condition individually). You can also now navigate more quickly to the type of artifact you need to perform a search.

- Find an Artifact Type
- Clear a Search

Find an Artifact Type

Filter the list of artifacts you can use to perform a search.

STEP 1 | Start or continue an AutoFocus search.

STEP 2 | In the search editor, start typing the name of the artifact you want to find.

For example, type file to find the artifact type File Size.

STEP 3 | Select an artifact type from the filtered list of options.

You can use the arrow keys to scroll up and down the list. To select a highlighted option, press Enter.

Clear a Search

Click the x icon to clear an existing AutoFocus search (including all search conditions) in a single step:

Tag Filter Enhancements

You can now find tags based on any value included in the tag definition and sort tags based on the date when the tag was created and last updated.
Find Tags by Match Criteria

STEP 1 | Select Tags on the navigation pane to view the complete list of AutoFocus tags.

STEP 2 | Click the filter icon and add a tag filter.

STEP 3 | Select the artifact type Match Criteria and set up a search condition:

AutoFocus looks for samples with tag definitions that match the search condition:
STEP 4 | View the Tag Detail of the resulting tags to verify that AutoFocus applied the filter.

For example, when you filter for any tag that contains the Match Criteria sample.exe, the results include the Unit 42 tag Blackpos because its definition has instances of sample.exe.

STEP 5 | Next step:
Learn about other ways to find and filter AutoFocus tags, including finding tags with the most hits, the top tags detected during a selected date range, and the top tags matching to search.

**Find New and Recently Updated Tags**

You can sort tags based on the date and time the tag was created and most recently modified. Only tags created and updated since this feature was introduced will display the date and time created and last updated.

**STEP 1** | Select **Tags** and Choose Columns to display the date and time each tag was **Created** or was most recently **Updated**:

**STEP 2** | Continue to Sort by: Created or Sort by: Updated.

**STEP 3** | Click Sort Descending to display the newest or most recently updated tags first; click Sort Ascending to display the oldest or least recently modified tags first.

**STEP 4** | Next step:

Continue to find tags, including tags with the most hits, the top tags detected during a selected date range, and the top tags matching to search.
AutoFocus Feedback Tool

A new feedback tool is now built into the AutoFocus portal, making it easier for you to request features and send comments about your AutoFocus experience to Palo Alto Networks.

**STEP 1** | Click *Give Feedback* on the bottom of the navigation pane.

**STEP 2** | Select a *Subject* to describe the type of feedback.

*Selecting Bug Report as the Subject disables the feedback field. To report an AutoFocus bug, follow the link to the Customer Support Portal.*

**STEP 3** | Enter your comment or feature request in the provided field.

**STEP 4** | Send Feedback and then Close the window confirming that your feedback was successfully submitted.
New Features: December 2015

The following topics provide a snapshot of the AutoFocus™ features introduced in December 2015. Each section includes context for the new feature, with steps to get started.

- Display File Analysis Results in Sequence
- Filter Tags and Alerts
- Attribute Sources For Tags
- Search Based on Android Suspicious Actions

Display File Analysis Results in Sequence

By default, WildFire™ dynamic analysis results for a sample are grouped based on activity type (the WildFire analysis category).

Now, you can also view WildFire dynamic analysis results based on the order in which activities were seen when the sample was executed in the WildFire sandbox. For each operating system in which the sample was executed, the sequence of events that took place in the operating system kernel space and the operating system user space is provided.

**STEP 1** | Start or continue an AutoFocus search to find a sample.

**STEP 2** | View samples matched to your search.

Notice that the analysis results for the sample are sorted based on WildFire behavior and activity categories:

**STEP 3** | Click the new option Show in Sequence:
STEP 4 | Select the drop-downs to view the user space and kernel space event sequences:

- **User Space Event Sequence**—Chronologically lists the user space activities recorded when the sample underwent WildFire dynamic analysis. User space is the memory area outside of the operating system kernel, where applications and other user processes are executed.

- **Kernel Space Event Sequence**—Chronologically lists the kernel activities recorded when the sample underwent WildFire dynamic analysis. The kernel is the core of the operating system; the kernel space is a memory area where the kernel runs operating system processes and manages other processes.

STEP 5 | Next steps:

- Add high risk artifacts found in an event sequence to a search or an export list.
- Learn more about the properties, behaviors, and activities found to be associated with samples during WildFire analysis.

Filter Tags and Alerts

Advanced filtering is now provided on the Tags page and the Alerts page in AutoFocus.

- **New Tag View and Filters**
- **New Alert Filters**

**New Tag View and Filters**

Tags are now displayed collectively in a single view to enable quick and easy filtering:
New Tag View and Filters

1. Unified Tag View

The new unified tag view displays all Public, Private, and Unit 42 tags in a single view.

Previously, Public, Private, and Unit 42 tags were displayed on different tabs, and could not be filtered collectively.

2. Quick Search

Enter a single value in the new quick search field to find matching tags across all tag types.

3. Advanced Filter

Click on the filter icon to find tags based on multiple search conditions, including tag fields, the number of votes a tag has received, and the number of sample hits:

Related topic:
Learn about AutoFocus tags.

New Alert Filters

STEP 1 | Select Alerts on the left-hand navigation pane to view the Alerts Log.

STEP 2 | Select the filter icon:
STEP 3 | Search for alerts based on the following alert criteria:

- **Time Sent**—Find alerts based on the time that AutoFocus sent the alert.
- **SHA256**—Enter the SHA256 hash for a sample to find alerts related to that sample.
- **Tag Class**—Enter a tag class to find all alerts for tags with that class. For example, filter for alerts on tags that are classified as part of a malware family.
- **Tag Name**—Enter a tag name to find alerts based on that tag.
- **Tag Scope**—Find alerts based on tag types: Unit 42, Unit 42 informational, public, and private.
- **Send Status**—Find alerts based on the alert delivery status (success, failure, or no action).

STEP 4 | Next step:

Learn about AutoFocus alerts.

Attribute Sources For Tags

You can now attribute tags to the organizations or individuals that identified a threat by defining the new tag Source field. The new tag source field is also searchable; you can find tags based on source, and find samples matched to those tags.

- **Attribute tags to a source.**
  1. Vote for, comment on, and report tags.
  2. Enter the organization to which you want to attribute the tag in the Source field.
  3. Click Save Changes.

- **Find tags based on source.**
  1. Select Tags and click the filter icon:
  2. Set up a search condition based on the tag Source:

- **Find samples based on tag source.**
  1. Start or continue an AutoFocus search.
  2. Select the artifact type Tag Source and either enter or select a tag source to add to your search.
• Next steps:
  • Learn more about AutoFocus tags.
  • Get started working with the AutoFocus search editor.

Search Based on Android Suspicious Actions

You can now find samples based on the suspicious actions performed by an Android application during WildFire analysis of the samples.

**STEP 1** | Start or continue an AutoFocus search.

**STEP 2** | Add a search condition with the artifact type APK Suspicious Action:

![Image of search condition]

**STEP 3** | View samples matched to your search, and select a sample hash to view the file analysis details for that sample.

The file analysis details include the Suspicious Action details, and the results matched to your search condition are highlighted.

![Image of WildFire Dynamic Analysis]

**STEP 4** | Next steps:
  • Get started working with the AutoFocus search editor.
  • Learn more about the properties, behaviors, and activities associated with samples.
New Features: November 2015

The following topics provide a snapshot of the AutoFocus™ features introduced in November 2015. Each section includes context for the new feature, with steps to get started.

- Search Based on Observed Behavior
- Export Artifact Metadata
- Share Links to Saved Searches
- Find Tags with an Unspecified Tag Class

Search Based on Observed Behavior

You can now find samples based on behaviors seen when the sample was executed in the WildFire™ analysis environment. For example, you can search for samples that created and modified files, started processes, spawned new processes, modified the registry, or installed browser help objects (BHOs).

STEP 1 | Start or continue an AutoFocus search.

STEP 2 | Select the artifact type Observed Behavior:

STEP 3 | Browse the complete list of possible behaviors. Select at least one behavior to find samples for which that behavior was seen when executed in the WildFire sandbox.

STEP 4 | Next steps:
- Get started working with the AutoFocus search editor.
- Learn more about the properties, behaviors, and activities observed during WildFire analysis of a sample.
Export Artifact Metadata

When exporting artifacts from AutoFocus to a CSV file, you can now also export the following information in the CSV for each artifact:

- the export list label used to group artifacts,
- the time the artifact was added to the export list,
- the user who added the artifact to the export list,
- the artifact activity category,
- and the SHA-256, SHA-1, and MD5 hash for the sample with which the artifact is associated.

You can then filter the generated CSV file based on this metadata.

For example, a threat researcher who plans to circulate the CSV file across a global IT department where regional offices might have different security requirements could create regional labels to group artifacts. She could then generate a CSV file on a daily or weekly basis, and the regional IT departments can filter the list accordingly based on the regional label (the labeled artifacts can then be added to the appropriate regional block list).

**STEP 1 | Build an AutoFocus exportlist.**

**STEP 2 | Generate a CSV file from the export list.**

1. Select Export List on the navigation pane.
2. Select the artifacts you want to export.
3. Click Export.
4. Select Export Metadata and Export.

The generated CSV file with metadata includes the following additional columns for each artifact row: *Added Time*, *Section* (this is the activity category during which WildFire observed the artifact), *Label*, *SHA256*, *SHA1*, *MD5*, and *User*.

Share Links to Saved Searches

You can now share your saved searches with other users within your organization.

**STEP 1 | Select Search and open your saved searches.**

**STEP 2 | Click the link icon to generate a shareable link:**
STEP 3 | Copy the link to share it with other AutoFocus users in your organization.

You can now also search within your saved searches, sort saved searches, and toggle searches to show or hide search details.

Find Tags with an Unspecified Tag Class

A tag class can be defined to associate a tag with a known actor, targeted campaign, malware family, malicious behavior, or an exploit. While previously you could search for tags based on the tag class, you can now also search for tags that do not have a specified tag class.

STEP 1 | Start or continue an AutoFocus search.

STEP 2 | Add a condition with the artifact type Tag Class, the operator is, and select None Specified.

STEP 3 | Next step:

Learn more about AutoFocus tags, including the different types of tag classes.
Getting Help

The following topics provide information on where to find more about this release and how to request support:

> Related Documentation
> Requesting Support
Related Documentation

Refer to the following documents on the AutoFocus documentation portal using the links below. You can also search the documentation for more information on our products:

- **AutoFocus Administrator’s Guide**—Provides detailed information about using the AutoFocus portal.
- **AutoFocus API Reference**—Learn how to use the AutoFocus RESTful API to programmatically query the threat intelligence clouds.
Requesting Support

For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
https://www.paloaltonetworks.com/company/contact-support
Palo Alto Networks, Inc.
www.paloaltonetworks.com