WatchGuard Cloud Release Notes

Latest WatchGuard Cloud Update	13 June 2019
Release Notes Revision Date	13 June 2019

Introduction

WatchGuard Cloud allows you to see and manage all your products and services in one place. From WatchGuard Cloud you can configure and manage your security services such as AuthPoint and see related metrics and reports. For a full description of WatchGuard Cloud features and functionality, see WatchGuard Cloud Help.

WatchGuard periodically updates WatchGuard Cloud to provide additional functionality and resolve reported issues. For information on the enhancements and resolved issues in each update, see the *Enhancements and Resolved Issues* section.

These release notes also include information about updates made to security services managed from WatchGuard Cloud. For information about the enhancements and resolved issues for specific security services managed from WatchGuard Cloud, such as AuthPoint, see the Enhancements and Resolved Issues section for the relevant security service.

Enhancements and Resolved Issues

Latest Release

Release Date: 13 June 2019

- An audit log is now generated when an operator adds, edits, or deletes a scheduled report. *[DC-1879]*
- WatchGuard Cloud Visibility
  - The Interface Summary scheduled report now includes the reports by interface type (zone). *[DC-2568]*
  - Bugfixes:
    - Corrected an issue with Allowed virus counts in the Virus report *[DC-2571]*

Previous Releases

Release Date: 6 June 2019

- WatchGuard Cloud Visibility
  - Reports enhancements:
    - Web reports (Most Active Clients, Most Popular Domains, Web Audit, Web Activity Trend) now include HTTPS traffic. *[DC-1795]*
    - The Interface Summary report has a new pivot to by interface type (Zone) *[DC-766]*.
    - New Audit Trail report shows device configuration changes. *[DC-2451]*
  - Bugfixes
    - Resolved an issue that caused display errors for Firebox visibility in Firefox and Edge browsers. [DC-2551]

Release Date: 30 May 2019

- Minor updates and bug fixes.

Release Date: 23 May 2019

- WatchGuard Cloud Announcements now appear in Subscriber view, on the **Administration > Notifications** page. *[WCD-3144]*
- WatchGuard Cloud Visibility
  - Usability enhancements:
    - In Device Manager, the second column label has been changed to **Fireboxes**. *[WCD-3753]*

    Bug fixes:

    - When you add a FireCluster, you must now select at least one member from the list of activated devices. You cannot type the serial number to add both members. *[DC-2494]*
    - Device Manager no longer shows statistics for a Firebox with the status **Never Connected**. *[DC-2487]*

Release Date: 16 May 2019

- The Licenses tile now correctly shows the allocation percentage. *[WCD-3737]*
- WatchGuard Cloud Visibility
  - Resolved a device display issue when adding a FireCluster. *[DC-2494]*

Release Date: 9 May 2019

- In Subscriber view, in the Monitor and Configure top navigation menus, Devices is now called Fireboxes. *[DC-2324]*
- WatchGuard Cloud Visibility
  - Log Manager and Log Search improvements. *[DC-1933]*
    - Log message filters now appear in a drop-down list.
    - Improved page navigation controls make it easier to go to a specific page in the search results.
  - New reports:
    - Policy Usage report *[DC-2161]*
  - Bug fixes:
    - The Virus (GAV) scheduled report now includes the Virus (IAV) report. *[DC-2442]*

Release Date: 2 May 2019

- Improved validation for Service Provider account addresses. *[WCD-2222] [WCD-3699]*
- Exported audit logs now download in a compressed ZIP file. *[WCD-3703]*
- The **Allocation** page for AuthPoint now shows the number of over-allocated users. *[WCD-3697]*
- WatchGuard Cloud Visibility
  - Bug fixes:
    - The **Dashboard** page no longer appears after you generate or enter a verification code for account delegation. *[DC-2424]*
    - The **Submit** button is now enabled when Subscribers re-enter a verification code. *[DC-2373]*
    - Improved the appearance of reports when no data is available. *[DC-2438] [DC-2430]*

Release Date: 25 April 2019

- Improved the appearance of large numbers in Dashboard tiles. *[WCD-3551] [WCD-1681] [DC-2192]*
- Removed the left navigation menu from the My Account, License Details, and Managed Access Administration pages. Navigation between pages is available in the top menu. *[WCD-3583]*
- WatchGuard Cloud now supports Operator names longer than 15 characters. *[WCD-3611]*
- WatchGuard Cloud Visibility
  - New reports:
    - IntelligentAV pivot added to the Virus report *[DC-225]*
    - URL Audit Detail report added to Per Client Reports *[DC-2385]*
  - Usability enhancements:
    - Improved pagination in device reports. *[DC-3609]*
    - The Data Retention licenses tile no longer appears on the Subscriber Dashboard if no Data Retention licenses are activated or allocated to the account. *[WCD-3583]*
  - Bug fixes:
    - Log Search performance has been optimized. Log Search now finds log messages that contain the search text at the start of each part of the log message. For log message types that include a long Message, to find log messages with a specific Message, you must search for the text at the start of the Message within the log message. *[DC-2440]*
    - Reports that do not have data for all pivots now display 'No data available' for pivots without data. *[DC-2094]*
    - Dashboard filters now remain in effect when you switch from the root level folder to a device. *[WCD-3662]*

        - The Botnet Detection report now refreshes data after you select a different date range. *[DC-2395]*
        - The Botnet Detection report now appears when it is the only enabled service, and report data exists. *[DC-2392]*
        - Device reports now show “No data available” when no data is available in the current pivot. *[DC-2094]*

Release Date: 18 April 2019

- WatchGuard Cloud Visibility
    - New reports:
        - Alarms summary and detail report *[DC-1382] [DC-1385]*
        - Denied Quota report *[DC-1392]*
        - DHCP Lease Activity report *[DC-1381]*
    - Bug fixes:
        - Application Usage Detail report is now available in the **Detail** report list. Previously, this report was only available through the **View Details** link in the Application Usage Summary report *[DC-2377]*

Release Date: 11 April 2019

- WatchGuard Cloud Visibility
    - Bug fixes:
        - An allocated device with an expired license now appears in the **Add Device** list of the Subscriber account. *[DC-2327]*
        - The Per Client Report bar charts in the PDF output have been improved. *[DC-2296]*
        - Policy Map now resizes when you collapse the device list. *[DC-2284]*
        - In Device Manager, the device list shows the correct status after you refresh the status for a FireCluster. *[DC-2242]*
        - In the **Device Status** tile, the Inactive device count no longer includes inactive members of a FireCluster. *[DC-2225]*
        - This release also fixes several minor UI issues.
    - New reports:
        - Denied Packets summary and detail reports

Release Date: 4 April 2019

- WatchGuard Cloud Visibility
    - Usability enhancements:
        - New onboarding tips for accounts with no provisioned Fireboxes or AuthPoint users. *[WCD-3554]*
        - Updated tile styles. *[UX-326]*
        - Removed ‘Root’ from the device folder label in Device Manager. *[DC-2275]*
        - In the IPS Summary report, private port ranges are now aggregated. *[DC-2153]*
    - This update includes several new reports:
        - Intrusions summary report *[DC-809]*
        - Intrusions detail report *[DC-1405]*
        - POP3 Proxy summary report *[DC-1351]*
        - POP3 Proxy detail report *[DC-1393]*
        - Blocked Default Threats report *[DC-1354]*

- Bug fixes:
  - Removed 'Z' from timestamps on VPN Bandwidth report. *[WCD-3606]*
  - Improved an error message for Add FireCluster failures. *[DC-2302]*
  - Search in Per Client Reports now ignores leading and trailing spaces. *[DC-2287]*
  - DLP search is now available in the Per Client Summary report if DLP data is available. *[DC-2286]*
  - Changed the first column label in CSV exports from Timezone to Event Time. *[DC-2282]*
  - In the Add FireCluster wizard, hyphens in the manually entered serial number are now automatically removed. *[DC-2273]*
  - The minimum manufactured version required for RapidDeploy is now Fireware v12.3.1. *[DC-2216]*

Release Date: 28 March 2019

- WatchGuard Cloud Visibility (Beta)
  - Usability enhancements:
    - Primary navigation for the Subscriber view has moved to the top of the page.
      - **Reports** menu is now called **Monitor**, with submenus for Devices and AuthPoint.
      - The **Configure** menu now has submenus for Devices and AuthPoint.
      - Licensing, Alerts, and Audit Logs are now available in the **Administration** menu.
    - Completed scheduled reports now show file size next to the PDF link. *[WCD-3539].*
  - This update includes several new reports:
    - VPN Bandwidth report *[DC-802]*
    - Blocked Application Summary report *[DC-806]*
    - Blocked Application Detail report *[DC-2104]*
  - Bug fixes:
    - Resolved several issues related to FireCluster support.
    - POP3 detail report can now be successfully exported to a CSV file. *[DC-2087]*

Release Date: 21 March 2019

- WatchGuard Cloud Visibility (Beta)
  - New feature — FireCluster support
    - On the **Add Device** page, the **Add FireCluster** option enables you to select each cluster member, or to specify the serial number of the second member.
    - The **Device Summary** for a FireCluster shows status and statistics for both cluster members.
    - Log Manager and Log Search for cluster members are consolidated.
    - Reports for cluster members are consolidated.
  - Bug fixes:
    - Attachments are now included in the e-mail for one-time scheduled reports. *[WCD-3570]*
    - The **Add Device** option now appears in the root folder menu for operators with the Owner role. *[DC-2199]*
    - The **Add Device** option is no longer available to operators with the Sales role. *[DC-2182]*
    - The Log Manager chart now resets to the original date and time if the Start and End date and time are the same. *[DC-1999]*
    - RapidDeploy no longer shows an incorrect error message when you upload an unnamed configuration file and then choose to select an existing configuration file. *[DC-1876]*

- Usability enhancements:
  - The Firebox status in WatchGuard Cloud is changed from Online/Offline to Connected/Not Connected to more clearly indicate that this represents only the status of the connection between the Firebox and WatchGuard Cloud. *[DC-2171]*
  - The Audit Log message for a Deallocate action now includes account name information. *[DC-2106]*
- This update includes several new reports:
  - Zero-Day Malware (APT) Detail report *[DC-1406]*
  - Application Usage report *[DC-1396]*
  - Interface Summary report *[DC-1387]*
  - Advanced Malware report *[DC-1337]*
  - Blocked Application report *[DC-807]*
  - Application Usage report *[DC-805]*

Release Date: 14 March 2019

- WatchGuard Cloud Visibility (Beta)
  - This update includes several new reports:
    - Botnet Detection Detail report *[DC-1407]*
    - Botnet Detection Summary report *[DC-1338]*
    - Spam Summary report *[DC-808]*
    - Intrusions Detail report *[DC-1405]*
  - Scheduled reports now include all data from the specified time range (determined by the **Frequency**). The **Start Time** no longer impacts the data included in the report. *[DC-2075]*
  - You now see the correct error message if there is an error when you generate a new Verification Code to add a device to WatchGuard Cloud. *[DC-2069]*
  - The Proxy Traffic, Top Clients, and Search Engine reports now have context-sensitive help links. *[DC-1874, DC-2055]*
  - This update includes several bug fixes for Per Client Reports. *[DC-2154, DC-2136. DC-2134, DC-2130, DC-2128, DC-2051, DC-2052]*

Release Date: 7 March 2019

- For Service Providers, on the **Dashboard** page, the date in the **License Expiration** tile now reflects the next expiration date among all active services. Previously, this only showed the next AuthPoint license expiration date. *[WCD-3526, WCD-3443]*
- In the Subscriber view, a new **Data Retention License** widget has been added to the **Dashboard** and **Administration** pages, the **Device License Details** widget has been added to the **Administration** page, and the **License Details** widget is now called **AuthPoint License Details**. *[WCD-3444]*
- WatchGuard Cloud Visibility (Beta)
  - Audit logs are now generated when you assign or unassign a Data Retention License to a Firebox. *[DC-1737]*
  - A new Alert Rule has been added for when a Firebox license or allocation is about to expire. *[DC-1549]*
  - An SMTP Proxy Summary report has been added. *[DC-1339]*
  - An SMTP Proxy Detail report has been added. *[DC-1395]*
  - A RED Summary report has been added. *[DC-1336]*
  - Performance improvements have been made to Firebox logging and reporting. *[DC-2002, DC-2029]*

Release Date: 28 February 2019

- You can now resize the **Inventory** and **Device Manager** tree menus. You can also expand and collapse items in the tree menus. *[DC-1998]*
- WatchGuard Cloud Visibility (Beta)
  - An error message now displays when you try to export more than 10,000 log messages. *[WCD-2805]*
  - Alerts are now created when you deallocate a Firebox or a Data Retention License. *[DC-1997]*
  - The alerts related to the allocation and deallocation of Fireboxes and Data Retention Licenses have been updated to provide more context. *[DC-233]*
  - When you switch between the **Category** and **Client** view for any Detail report, the list now returns to the first page. *[DC-2001]*
  - The Packet Filter report now has a context sensitive help link. *[DC-1899]*
  - On the **Log Manager** page, when you set the start time and the end time to be the same, the graph now correctly displays no data when the API returns no data. *[DC-1995]*
  - The **Hits** axis label on the Web Activity Trend report graph now displays correctly. *[DC-1650]*
  - The issue that caused the Most Active Clients report to not display both MB and Hits on the graph has been resolved. *[DC-1468]*
  - A Data Loss Violation Summary report has been added. *[DC-1408]*
  - A Data Loss Violation Detail report has been added. *[DC-1409]*
  - A Top Clients report has been added. *[DC-801]*
  - A Firebox Authentications report has been added. *[DC-793]*
  - A Blocked Websites Summary report has been added. *[DC-807]*
  - A Blocked Websites Detail report has been added. *[DC-1397]*
  - A Proxy Traffic report has been added. *[DC-800]*

Release Date: 21 February 2019

- Updated an error message about account delegation to be more specific. *[WCD-3479]*
- WatchGuard Cloud Visibility (Beta)
  - You can now schedule reports in WatchGuard Cloud. *[WCD-3280]*
  - In **Device Manager**, the **Quick Actions** widget has been removed from the **Device Summary** page. *[WCD-3469]*
  - On the **Add Device** page, the **Name** of a device is now a link to add that device to WatchGuard Cloud. *[WCD-3466]*
  - When you hover over a list item in an **Activity Trend** report, the hover text now displays the local time instead of UTC. *[DC-1969]*
  - On the **Log Manager** page, you no longer receive an error message if you set the start time and the end time for the graph to be the same. *[DC-1980]*

Release Date: 7 February 2019

- You can now see packet filter traffic reports for your devices in WatchGuard Cloud. *[DC-799]*
- For Service Providers, audit logs are now generated when you allocate a Firebox to a managed account. *[DC-232]*
- On the **Add Device** page, the **Name** of a device is now a link to add that device to WatchGuard Cloud. *[WCD-3466]*
- The issue that caused the Search Engine for devices to show duplicate items has been resolved. *[DC-1881]*

Release Date: 31 January 2019

- The **Configure Services** page in the Subscriber view now shows AuthPoint tiles only for accounts that have activated an AuthPoint license. *[DC-1577]*

Release Date: 10 January 2019

- A new Alert Rule has been added for when inventory is deleted from your account. *[WCD-3302]*
- The **Reports** page in the Subscriber view only shows AuthPoint widgets for accounts that have an AuthPoint license. *[DC-1576]*

Release Date: 13 December 2018

- The Subscriber dashboard only shows AuthPoint if your account has an active AuthPoint license or trial.

Release Date: 15 November 2018

- When an operator navigates to a page they do not have permissions for, they are now redirected to the **Dashboard** page. *[WCD-2618]*
- Inventory management has been updated to provide better visibility and make allocation easier. *[DC-3]*
- For Tier-1 accounts, the text in the **Invite Operator** dialog box has been updated. *[WCD-3271]*

Release Date: 1 November 2018

- The **Authentication** graph on the **Reports** page now displays correctly when you refresh the page. *[WCD-3125]*

Release Date: 18 October 2018

- You can now successfully acknowledge alerts. *[WCD-3274]*
- Minor bug fixes and improvements.

Release Date: 11 October 2018

- NFR licenses for AuthPoint can now be updated without issue. *[WCD-3267]*
- The issue that caused the **Alert Details** and **Audit Log Detail** windows to not display has been resolved. *[WCD-3253]*

Release Date: 20 September 2018

- This release resolves an issue that caused the WatchGuard Cloud navigation menu to overlap the AuthPoint navigation menu when a browser window was resized. *[WCD-3164]*

Release Date: 30 August 2018

- WatchGuard Cloud now supports MSSP AuthPoint licenses. *[WCD-3111]*

Release Date: 23 August 2018

- For Service Providers, NFR users allocated to your account are now included in the **AuthPoint Users** column on the **Inventory** page. *[WCD-3114]*

Release Date: 16 August 2018

- Alert Rules have been added for Account Delegation. *[WCD-1565] [WCD-1564]*
- When you add or edit a Rule, the **Recipients** text box now accepts delimiters so that you can type multiple email addresses. *[WCD-3087]*
- The issue that caused the **My Account** page to not load for some Service Providers has been resolved. *[WCD-3116]*

Release Date: 8 August 2018

- Minor bug fixes and improvements.

Release Date: 2 August 2018

- Duplicate rules and alerts are now allowed. *[WGC-3028]*
- General improvements to alerting functionality.

Release Date: 26 July 2018

- Improvements in handling our NFR AuthPoint Licenses.
- The date picker now shows the date properly on the **Reports** page.

Known Issues and Limitations

To find known issues for WatchGuard Cloud, look in the Technical Search > Knowledge Base tab.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at https://www.watchguard.com/wgrd-support/overview.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375

AuthPoint Release Notes

Latest AuthPoint Update	13 June 2019
Release Notes Revision Date	13 June 2019
Mobile App for Android	1.6.0
Mobile App for iOS	1.5.1
AuthPoint Gateway	4.2.2-119
ADFS Installer	1.1.67
Logon App for Windows 64-bit	1.7.2.110
Logon App for Windows 32-bit	1.7.2.110
Logon App for Mac OS	1.4

Introduction

AuthPoint is WatchGuard's multi-factor authentication (MFA) service. With AuthPoint, you can require users to authenticate with a mobile app when they log in to a protected resource, such as a computer, VPN, or a cloud service or application. Because AuthPoint requires users to authenticate before they log in, data in your cloud applications and services is protected.

For a full description of AuthPoint features and functionality, see AuthPoint Help.

WatchGuard periodically updates the AuthPoint service to provide additional functionality and resolve reported issues. For information on the enhancements and resolved issues in each update, see the *Enhancements and Resolved Issues* section.

Enhancements and Resolved Issues

Latest Release

Release Date: 13 June 2019

- The **Remember Password** and **Synchronization Interval** options have been removed from the **Logon app** resource page. *[AAAS-7277]*
- Minor bug fixes and improvements.

Previous Releases

Release Date: 6 June 2019

- The AuthPoint agent for ADFS has been updated to version 1.1.67. You can now configure safe locations for ADFS. Download and install the updated agent for ADFS to use this feature. *[AAAS-7471]*
- The company name now displays correctly on the authentication page for ADFS. *[AAAS-6606]*
- Minor bug fixes and improvements. *[AAAS-7757, AAAS-6439, AAAS-7751]*

Release Date: 30 May 2019

- Minor bug fixes and improvements. *[AAAS-7693]*

Release Date: 23 May 2019

- RD Web has been added as a new resource type. *[AAAS-5821]*
- The AuthPoint agent for RD Web has been added to the **Downloads** page. *[AAAS-5835]*
- These applications have been added to the Application Type drop-down list for SAML resources. Each of these applications has a context-sensitive help link to the integration guide. *[AAAS-7553]*
  - BMC Remedy Force
  - Cisco ISE
  - Cisco Webex
  - CylanceProtect
  - Globalscape EFT
  - ITGlue
  - Stride
  - Thycotic Secret Server
- These applications have been renamed in the Application Type drop-down list for SAML resources. *[AAAS-7441]*
  - Cisco is now Cisco Umbrella
  - LogMeIn is now LogMeIn Central
  - Lucidchart is now LucidChart
  - ManageEngine is now ManageEngine PMP
- For Service Providers, in the Subscriber view, the **Certificates** page in the AuthPoint management UI now correctly updates when you pivot to view a different Subscriber account. *[AAAS-7673]*
- Minor bug fixes and improvements.

Release Date: 16 May 2019

- The Logon app for Mac OS has been updated to version 1.4.
  - The Logon app for Mac OS now supports safe locations. *[AAAS-6556]*
  - When you authenticate with QR code or OTP, you no longer have to select the Offline Authentication option to authenticate without an Internet connection. This option has been removed from the UI. *[AAAS-7262]*
- Citrix Sharefile has been added to the **Application Type** drop-down list for SAML resources. *[AAAS-7362]*
- Minor bug fixes and improvements.

Release Date: 9 May 2019

- A new Alert Rule has been added to notify you when an AuthPoint identity provider certificate is about to expire. *[AAAS-7256, AAAS-7258]*
- Minor bug fixes and improvements.

Release Date: 30 April 2019

- Minor bug fixes and improvements.

Release Date: 30 April 2019

- The AuthPoint mobile app has been updated to version 1.6.0.
  - You can now manually activate third-party tokens in the AuthPoint mobile app.
  - You can now migrate third-party tokens from one mobile device to another.
  - The time stamp of your token is now synced when you respond to a push and receive an authentication error.
  - You can now tap your screen to focus the camera when the QR code reader is open.
  - Minor bug fixes and improvements.

Release Date: 25 April 2019

- You can now create and manage the certificates used for SAML authentication. From the **Resources** page, click **Certificate** to see the new **Certificate Management** page. *[AAAS-6960]*
- The issue that caused the Pending token status to not show for new users has been resolved. *[AAAS-7309]*

Release Date: 18 April 2019

- Minor bug fixes and improvements.

Release Date: 11 April 2019

- Minor bug fixes and improvements.

Release Date: 4 April 2019

- You can now configure safe locations on the **Edit Group** page. When you configure a safe location, users can access SAML resources from the specified IP addresses without MFA. *[AAAS-48]*
- Audit logs are generated when you add, edit, or remove a safe location. *[AAAS-6715]*
- Minor bug fixes and improvements.

Release Date: 28 March 2019

- Minor bug fixes and improvements.

Release Date: 21 March 2019

- You can now download the ADFS installer on the **Downloads** page. *[AAAS-702]*

Release Date: 14 March 2019

- The Logon app for Windows has been updated to version 1.7.2.110. This update resolves the issue that caused some push notifications to take a long time to time out. *[AAAS-6400]*
- When you enable the **Basic Authentication** option in the access policy of an Office 365 resource, the access policy now operates correctly and users must authenticate with an allowed authentication method. *[AAAS-6602]*
- For SAML resources, the **Application Type** drop-down list now has context-sensitive help links to the integration guides for Adobe, ConnectWise Control, FreshService, KnowBe4, Manage Engine, Splunk, and SugarCRM. *[AAAS-6700]*

Release Date: 28 February 2019

- You are now redirected to the SSO login page if the IdP portal is open when your session expires. *[AAAS-6510]*
- When you restart your computer, your session is no longer remains active. You must log in and authenticate to access a resource or the IdP portal. *[AAAS-6611]*

Release Date: 22 February 2019

- The AuthPoint Gateway has been updated to version 4.2.2-119.
- You can now install the AuthPoint Gateway on a Windows 2008r2 server. *[AAAS-6324]*
- The correct log message is now shown for successful RADIUS authentication attempts with an OTP. *[AAAS-6627]*
- The correct log message is now shown when you update an ADFS resource that is associated with a Gateway. *[AAAS-6617]*
- RADIUS authentication with an incorrect OTP is now logged as a failed authentication attempt instead of a timeout. *[AAAS-6325]*
- Performance improvements have been made for LDAP sync functionality. *[AAAS-6318]*
- You no longer see the command screens when you install the AuthPoint Gateway. *[AAAS-4828]*
- The issue that caused RADIUS authentication with just an OTP to fail has been resolved. *[AAAS-5970]*

Release Date: 7 February 2019

- The Windows Logon app has been updated to version 1.7.0-102.
- Minor bug fixes and improvements.

Release Date: 31 January 2019

- MFA now works with Splunk. *[AAAS-6195]*
- AuthPoint now supports basic authentication (ECP). You can enable this option in the **Access Policy** window. *[AAAS-6099, AAAS-6100]*
- On the **Downloads** page, you can no longer download the installer and the configuration file for the Logon app unless you have configured a Logon app resource. *[AAAS-5333]*
- You can now choose whether encryption is enabled or disabled when you upload a certificate for a SAML resource. *[AAAS-5912]*

Release Date: 24 January 2019

- When an IdP session expires, your web browser is now automatically directed to the login page. *[AAAS-6052]*
- IdP portal applications are now displayed alphabetically. *[AAAS-5905]*
- This release improves how SAML sessions are handled when you log out of a service provider account. *[AAAS-5954]*

Release Date: 15 January 2019

- Users can now delete blocked tokens in the AuthPoint mobile app. *[AAAS-5864, AAAS-5797]*
- The OTP for ConnectWise tokens now refreshes successfully on Android devices. *[AAAS-5858]*

Release Date: 10 January 2019

- Minor bug fixes and improvements.

Release Date: 4 January 2019

- The Windows Logon app has been updated to version 1.7.0-102
- The Logon app now compares the time difference between your Windows computer and WatchGuard Cloud to minimize failed authentication attempts due to timeout. *[AAAS-5032]*
- Users can now successfully log back on to a Windows computer with the Logon app installed and a GPO policy that does not remember the last user logged in. *[AAAS-5425]*
- The Forgot Token feature for the Windows Logon app now works for local users. *[AAAS-5309]*
- If the time on a computer or VM is changed while Forgot Token is enabled, AuthPoint now evaluates the time difference and the time frame set by the operator to the determine if the Forgot Token feature is still enabled. *[AAAS-5298]*

Release Date: 20 December 2018

- The AuthPoint Gateway has been updated to version 4.1.1-111
- A **Certificate Fingerprint** button has been added to the **Resources** page. Use this to copy the certificate fingerprint, which some applications require to configure MFA. *[AAAS-2547]*
- You can now use the Forgot Token feature for RADIUS authentication. *[AAAS-5554]*
- The **User ID** text box has been removed from the **RADIUS Client** and **IdP Portal** resource pages. *[AAAS-5862]*
- When you add a SAML resource, the **Application Type** drop-down list now has context sensitive help links for applications that do not have an integration guide. *[AAAS-5585]*
- Concur and KnowBe4 have been added to the **Application Type** drop-down list for SAML resources. *[AAAS-5863, AAAS-5925]*
- For SAML resources, the **Application Type** drop-down list now has a context sensitive help link to the Confluence integration guide. *[AAAS-5867]*

Release Date: 13 December 2018

- You now block and unblock tokens from the **Token Management** window. *[AAAS-4921]*
- PasswordPro has been added to the **Application Type** list for SAML resources. *[AAAS-3205]*
- You can now create users with @ in the user name. *[AAAS-5606, AAAS-5607, AAAS-5623]*

Release Date: 6 December 2018

- You can now authenticate with user name or email for all RADIUS, SAML, and ADFS resources. You no longer have to configure this option for each resource.
- ADFS has been added as a new resource type. *[AAAS-694]*
- Bug fixes for the AuthPoint Gateway. *[AAAS-5326]*
- Wrike has been added to the **Application Type** drop-down list for SAML resources. *[AAAS-5563]*
- The AuthPoint mobile app now supports Kraken as a third-party token for Android and iOS. *[AAAS-5017, AAAS-4751]*
- You can now successfully activate a token on an Android device that has the language set to Turkish. *[AAAS-5515]*
- You now have the option to set a new PIN when you disable biometric protection for a token. *[AAAS-4807, AAAS-5393]*

Release Date: 29 November 2018

- You can now download the configuration file for the Logon app on the **Downloads** page.
- For SAML resources, you can now select **Email Prefix** for the **User ID**. *[AAAS-5415]*
- When you click on a token on the **Users** page, the **Token Management** window now shows information about the device the token is activated on. *[AAAS-4621]*
- New applications have been added to the **Application Type** drop-down list on the SAML page. *[AAAS-5181]*
- The SSO page now shows you an error code and message when authentication fails. *[AAAS-4234]*
- The **Back** button no longer appears on the initial SSO page where you type your user name or email. *[AAAS-5289]*
- For external identities, you can now edit the Active Directory attribute values. *[AAAS-5452]*
- The **Forgot Token** window no longer populates with previously filled values. *[AAAS-5292]*
- AuthPoint now validates password length when a manually created user resets their password. Passwords must contain at least 6 characters. *[AAAS-5581]*
- The SSO page for SAML resources now shows the correct page name when you type an incorrect password. *[AAAS-5401]*
- Minor bug fixes and improvements.

Release Date: 8 November 2018

- The accuracy of the geolocation information shown for push notifications and QR codes is improved. *[AAAS-4301]*
- Advanced queries for external identities are now validated to prevent the creation of duplicate queries. *[AAAS-4557]*
- The option to unregister a Gateway has been removed from the **Edit Gateway** page. You no longer have to unregister a Gateway when you uninstall it. *[AAAS-5285]*

Release Date: 1 November 2018

- On the **Users** page, the **Token** column now shows a Pending status for a user who has not activated their token. *[AAAS-4009]*
- The issue that caused users to be sent to the IdP portal when their session expired has been resolved. This resulted in an error for users who did not have the IdP portal. *[AAAS-5268]*
- The Logon app for Windows now works for users with less than three characters in their user name. *[AAAS-5128]*
- You no longer have to download a new configuration file when you upgrade the Logon app. The Logon app installer can now use the existing configuration file. *[AAAS-5209]*
- If the Logon app resource is removed, MFA is no longer required and users can log in with their password. *[AAAS-4957, AAAS-5125, AAAS-5129]*
- The Logon app page now displays a message that tells the user if the Forgot Token feature is active and how long it is active for. This message appears whether the machine is online or offline. *[AAAS-4483]*
- On the Logon app page, the message that indicates how long the Forgot Token feature is active for now shows the correct time. *[AAAS-5105]*
- Users synced from Active Directory are now able to successfully change their password when it expires. *[AAAS-5188]*

Release Date: 25 October 2018

- The memberOf attribute in SAML authentication responses now includes the user's group name. *[AAAS-5026]*
- You can now activate tokens on iOS 9.x and 10.x mobile devices that do not support touch ID. *[AAAS-5163]*

Release Date: 11 October 2018

- The WatchGuard AuthPoint mobile app for Android has been updated to version 1.4.0.
- Minor bug fixes and improvements.

Release Date: 4 October 2018

- The AuthPoint Gateway and the Logon app for Windows have been updated.
- For external identities, you can now use the Group Sync feature to sync users from specific AD/LDAP groups without a query. You must download and install the updated AuthPoint Gateway to use this feature. *[AAAS-4933, AAAS-4608, AAAS-4906, AAAS-4969, AAAS-4238]*
- Overallocation no longer affects all users. If your account becomes overallocated, the status of unlicensed users is changed to Overallocated and those users cannot authenticate until your allocation is fixed. *[AAAS-4627]*
- AuthPoint now supports MSCHAPv2 RADIUS authentication for manually created users (not AD/LDAP users). You must download and install the updated AuthPoint Gateway to use this feature. *[AAAS-891, AAAS-4511]*
- The **Download** page is renamed to **Downloads**. *[AAAS-4795]*
- The **Token Information** window is renamed to **Token Management**. *[AAAS-4922]*
- AuthPoint now updates the DN for AD/LDAP users that are moved if they remain in the same group. [AAAS-4888]
- This release resolves an issue with the Logon app that caused the Forgot Token feature to not work for local users. *[AAAS-4878]*
- General improvements have been made to AuthPoint log messages. *[AAAS-4731, AAAS-4911, AAAS-4926]*

Release Date: 27 September 2018

- On the **Download** page, you can now see when each installer was last updated. *[AAAS-4796]*
- For external identities, the Query function has been renamed Advanced Query. The reason for this is to avoid confusion when we release a new feature to sync users without a query. *[AAAS-4906]*
- The **Push Timeout** text box was removed from the **Settings** page. *[AAAS-4827]*
- General improvements to how AuthPoint installers are downloaded. *[AAAS-4755]*
- User passwords that include "\" now work correctly for authentication. *[AAAS-4891]*
- You can now validate queries that contain multi-byte characters. *[AAAS-4862]*
- General updates have been made to error messages on the **Download** page. *[AAAS-4196]*
- All instances of the term OTT in the UI have been updated to Gateway Registration Key. The term OTT is no longer used. *[AAAS-4817]*

Release Date: 20 September 2018

- The Forgot Token feature now works for LDAP users. *[AAAS-4861]*
- Users are now shown an error message when they try to migrate a token without first activating a previously migrated token. *[AAAS-4639]*
- The format of the Set Password and Token Activation emails have been updated. *[AAAS-4654]*

Release Date: 13 September 2018

- The IdP Portal now validates different levels of authentication. If the user has an active session (they have already authenticated and logged in), they are required to authenticate again only for resources with different MFA requirements. *[AAAS-2485] [AAAS-3668]*
- When the Forgot Token feature is active for a user, the single sign-on page now displays a message that tells the user that the Forgot Token feature is active and how long it is active for. *[AAAS-4484]*
- The notification email about denied pushes for RADIUS client resources no longer indicates the location where the push was denied (the location was not accurate because the origin of the push is the trusted IP of the firewall). *[AAAS-4509]*
- On the **Download** page, the minimum Java version listed for the Gateway has been updated to JRE 8u162. *[AAAS-4353]*
- This release resolves an issue that caused operators to see the Subscriber view for the wrong account when they navigated back from the IdP Portal. *[AAAS-4543]*

Release Date: 3 September 2018

- The Gateway has been updated to improve LDAP synchronization. *[AAAS-4389] [AAAS-4390] [AAAS-4391]*
- User passwords for manually created users that include “=” now work correctly for RADIUS authentication. *[AAAS-4248]*

Release Date: 30 August 2018

- MFA now works with Adobe. *[AAAS-3486]*
- New applications have been added to the **Application Type** drop-down list on the **SAML** page. *[AAAS-4219]*
- When you add a SAML resource, the **Application Type** drop-down list now has context sensitive help links to the AuthPoint integration guides. *[AAAS-3027]*
- When an LDAP/AD user selects **Forgot Password** on the single sign-on page, they now see an error message. *[AAAS-4485]*
- The **Forgot Token** single sign-on page now shows the **Change Time Period** link. *[AAAS-4371]*
- The text in the Set Password email has been updated. *[AAAS-4255]*
- The Windows Logon app installer can now get the required configuration file from the System32 directory. *[AAAS-4135]*
- On the **LDAP Configuration** page, the **Password** text box was renamed to **Passphrase** and the text for the **System Account** slider has been updated. *[AAAS-4057]*
- The Logon app for Windows has been updated. On the logon screen, the **Forgot Token** link has been changed to an icon and users can now log in with only their password if the access policy for the Logon app does not require authentication. *[AAAS-4055]*
- General improvements have been made to the **Download** page. *[AAAS-4352]*

Release Date: 23 August 2018

- When you select **Forgot Token** for a blocked user, you now see an error message. *[AAAS-4322]*
- You can now successfully disable an LDAP external identity. *[AAAS-4264]*
- The issue that caused the **External Identities** page to appear when you tried to add a redundant address to an existing external identity has been resolved. *[AAAS-4358]*
- MFA now works correctly with BlueJeans. *[AAAS-3553]*
- The **Edit Group** page now loads correctly for groups that have a SAML resource without a custom attribute value. *[AAAS-4361]*
- Users with two or more tokens on the same mobile device no longer receive multiple push notifications when they authenticate. *[AAAS-4063]*

Release Date: 16 August 2018

- The WatchGuard AuthPoint mobile app for Android has been updated to version 1.3.2 (the mobile app for iOS has not been updated).
- Performance improvements have been made to reporting functionality. *[AAAS-3930]*
- On the **Users** page, the user account menu no longer shows the **Resend Set Password Email** option for LDAP users. *[AAAS-3948]*
- The issue that caused the **Add Policy** window to close if you used your keyboard to select a resource has been resolved. *[AAAS-3983]*
- The **Add** button on the **Resources** and **External Identities** pages was updated to match the other pages in the UI. *[AAAS-4066]*
- When you disable an external identity, the **Synchronization Interval** text box and **Add Redundant Address** button no longer remain enabled. *[AAAS-4292]*
- The issue that prevented you from selecting an image when you edit your token in the mobile app has been resolved. *[AAAS-4351]*
- General updates have been made to error messages. *[AAAS-4320] [AAAS-4323]*

Release Date: 8 August 2018

- AuthPoint now validates your active sessions when you log into a resource to determine if you must authenticate again. *[AAAS-2485]*
- Password Manager Pro can now enable integration with AuthPoint for SAML authentication. *[AAAS-3205]*
- The issue that caused the **Download** page to sometimes not load has been resolved. *[AAAS-4218]*
- The agent connection handler has been improved so that it does not send update events to AuthPoint Gateway. *[AAAS-4249]*

Release Date: 2 August 2018

- Auto scaling improvements. *[AAAS-4038]*
- Set password bug fix. *[AAAS-3853] [AAAS-4073]*
- The endpoints used by unencrypted versions of the AuthPoint Gateway to communicate with WatchGuard Cloud have been removed. *[AAAS-4031]*
- Various other bug fixes and UI improvements.

Release Date: 26 July 2018

- The WatchGuard AuthPoint mobile app has been updated. Download the updated app from the app store (you do not have to uninstall the current version before you update).
- The alert notification for LDAP sync now shows the number of users created, updated, and quarantined.
- The **Forgot Token** window now has a link to instructions that tell the user how the Forgot Token feature works and what they must do.
- The Windows Logon app no longer crashes if your Support Message contains characters reserved for JSON. The characters are: " , [ ] , { }
- Users no longer have to activate their token to authenticate and log in to resources that only require a password.
- The Activation report shows the users that have not activated their tokens. *[Center Code Bug 0054]*
- When you navigate back to the IdP portal with a valid session (you are still logged in), you no longer see the logon screen when the portal loads.

Known Issues and Limitations

To find known issues for AuthPoint, the AuthPoint mobile app, the AuthPoint Gateway, and the Logon app, including workarounds where available, look in the Technical Search > Knowledge Base tab.

Upgrade Notes

AuthPoint includes three installable components, the AuthPoint Gateway, the Logon app, and the mobile app for Android and iOS. None of these components automatically update. You must manually update to the latest version when a new version is released.

Upgrade the AuthPoint Gateway

The AuthPoint Gateway does not automatically upgrade to the latest version. To upgrade the AuthPoint Gateway, you must download and install the updated version of the AuthPoint Gateway.

If you have the current version of the AuthPoint Gateway installed or a version that is newer than 3.1.3-83:

1. In the AuthPoint management UI, select **Download**.
2. In the **Gateway Installer** section, next to your operating system, click **Download**.
3. Run the downloaded Gateway installer.

If the version of the Gateway you have installed is older than version 3.1.3-83, you must unregister and uninstall the AuthPoint Gateway before you download and install the updated version.

To update a version of the AuthPoint Gateway older than 3.1.3-83:

1. Uninstall the Gateway on your network.
2. In the AuthPoint management UI, select **Gateway**.
3. On the **Gateway** page, click the **Name** of your Gateway.
4. On the **Edit Gateway** page, click **Unregister Gateway**.
5. Click **Generate New Key**. Copy the new **Gateway Registration Key** value.
6. Select **Download**.
7. In the **Gateway Installer** section, next to your operating system, click **Download**.
8. Run the downloaded Gateway installer. Type or paste the new **Gateway Registration Key** value when prompted.
9. In the AuthPoint management UI, on the **Gateway** page, verify that the status icon next to your Gateway is green. This indicates that WatchGuard Cloud can successfully connect to the Gateway.

Update the Logon App

To upgrade the Logon app, you must download and install the updated version on your computer or server.

1. In the AuthPoint management UI, select **Download**.
2. In the **Logon App** section, next to your operating system, click **Download**.
3. Run the downloaded Logon app installer (.msi file).

Update the Mobile App

To update the mobile app for Android or iOS, go to the App Store or the Play Store and search for WatchGuard AuthPoint. Tap update to download and install the latest version of the app.

You do not have to uninstall the app before you update.

Operating System Compatibility for AuthPoint Components

Last revised: 7 May 2019

You must log in to WatchGuard Cloud to download these components. This software is not available from the WatchGuard Software Downloads page.

AuthPoint Components for Windows

AuthPoint Component	Microsoft Windows 7	Microsoft Windows 8 and 10	Microsoft Windows Server 2008 R2	Microsoft Windows Server 2012 R2	Microsoft Windows Server 2016 R2
ADFS				✓	✓
Gateway*		✓	✓	✓	✓
Logon App for Windows (64-bit)		✓		✓	✓
Logon App for Windows (32-bit)		✓		✓	✓

* The AuthPoint Gateway requires Java Runtime Environment 8u162 or newer.

AuthPoint Components for Mac OS

AuthPoint Component	El Capitan (10.11)	Sierra (10.12)	High Sierra (10.13)	Mojave (10.14)
Logon App for Mac OS	✓	✓	✓	✓

AuthPoint Mobile App

AuthPoint Mobile App	Supported OS
Android	4.4 and higher
iOS	9.0 and higher

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at https://www.watchguard.com/wgrd-support/overview.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375