



I'm not robot



**Continue**

## My webrootanywhere com registration asp

Hi, I've just activated my webroot key to protect my computer at home. Everything looks fine except there is a great blue message ON WEBBROOT SECURE ANY SCREEN THAT SAYS AN ACCOUNT ACTIVATION REQUIRED. I followed the steps, input information as requested and then found an email entitled WEBROOT CONSOLE CONFIRMATION WITH A link to activate everything. However, whenever I go to the email link and input the security code instructions (example: please enter the first letters and I of your security code) I get the Error Message (UCR2): Invalid security code credentials. My question is – is this process needed to have the webroot software actively protect my computer? If so, what do I need to do to repair my crisis? Thanks, Racheal Home 2018.12 December releases and updates \* Features may not be available in all Okta SKUs products. You can now add App Notes to communicate with end users and other admins on apps. In addition to upgrading app deployment with it, Notes App can also reduce help desk calls, provide troubleshooting assistance, and increase end self-service users. App notes facilitate the following types of communication: notes to end users – Allow administrators to present useful information to end users, such as why they've been assigned the app, who they contacted for help, and links to additional information. Application notes for admins – Allow admins to share administrative details about apps with other Super, App, Read-only, and mobile admins. For more information, see Add notes to an app. Super admins have the ability to choose which notification emails a specific type of admin receive by default. This allows you to manage the amount of role email traffic the different admin receives. The new default will overhauled existing admin email default notification settings (see Email notifications for default settings). This will exclude most admin from receiving most email notifications. For details, see Set default email notifications. We have updated the release number displayed in the Admin Console at YYYY.MM.UU format that we are officially adopting with December monthly release. For more information, see Release Notes. We have improved the User Communication Okta message in Settings &gt; Customization to clarify the scope of end user communication. Push Groups now supports the ability to connect to existing groups through the following application integrations: Smartsheet Facebook in Working Org2Org Adobe CQ JIRA, JIRA On-Prem DocuSign You can centrally manage these apps in Okta. For details, see Supplement Group. The A-to-Z link on the People page has been depressed as part of efforts to improve the performance and responses of the page in the Admin UI for large org. Screenshot: Before: After: When generating reports, the earliest start date you can choose is now 13 months of the current date. For more information about Reports, see Reports. Super admins can now filter the list of admins by roles and types for easier searching. We have updated the Okta Verify UI label configuration for the FIPS-Mode encryption setting. For more information, see Enable FIPS-mode encryption. Recreate group mapping pushes for existing groups would cause group members not to be mastered by Okta. OKTA-187881 An LDAP directory could not be assigned to an Okta group when sync password was enabled and Create users were disabled. OKTA-193192 Some end users have always been pushed authenticated with MFA despite successful enrollment with Okta Verify or Duo in the same session.OKTA-194472 The API Management Role Admin was not returned for the user when performing a GET on api/v1/user/{userId}/role endpoint. OKTA-195092 When using browsers other than Internet Explorer, Argentine Desktop SSO made two authentication requests for each user, increasing the authentication time. OKTA-196220 Push Group functionality only worked for admin and Rights Super Admin. OKTA-19709 Operational Provisions for Coupa's app fail. OKTA-197991 MFA Usage Report listed Okta Verify and Push as an enrolled factor even if the factor was reset by an end user from the dashboard to make it no longer registered. OKTA-198258 Had a minor grammatical error in the administration approval message.OKTA-198556 IdP Discovery rule and a Sharepoint On-Premise specific app requirements were not appropriate proper on SP-initiated login flow. OKTA-198797 After creating an ASN dynamic area via the API, then looking through the UI, the default proxy type was unlimited instead of any proxy. OKTA-201054H SAML IDP flow broke with a 404 error if the ACS URL was in [org/auth/saml20/{IP name}] format. App Integration Fixes The following NIGHT apps have score working correctly and are now fixed Alibaba Cloud (Aliyun) (OKTA-198076) Anaplan (OKTA-198239) Apple Business Manager (OKTA-198241) Dell Boomii (OKTA-198237) Egenicia UK (OKTA-198487) PacificSource InTouch (OKTA-198691) PacificSource InTouch (OKTA-197597) Perfode (OKTA-198238) Rival IQ (OKTA-190557) Salesforce Marketing Cloud (OKTA-197948) Web Manuals (OKTA-199509) The partner-built provisioning integration app is now generally available in the OIN as partner-built. New Integrations New Scim Integration Application The following partner-built provisioning integration app is now available in the OIN as partner-built Early Access: SAML for the Okta Verified apps Abstract (OKTA-192587) BamboohR (OCT-199943) CloudBees (OKTA-1911 71) SAP Concur Solutions (OKTA-198484) Workable (OKTA-198491) SWA for the Okta Verified apps Acronis Cloud (OKTA-189384) Ameriflex Wealth Care Portal (OKTA-197201) Autodesk BIM 360 (OKTA-194354) (OKTA - 196661) Business Inside Primary (OKTA-196625) Drift (OKTA-19216) Forum: Business Online Banking (OKTA-19530) Higher- (OKTA-196158) HomeDepot Vendor Portal (OKTA-190428) HP DaaS (OKTA-OKTA-196207) Premier Emperor (OKTA-191066) Home (OKTA-74699) Trends (OKTA-197199) WealthEngine (OKTA-198240) Zywave House (OKTA-193830) 2018. 12. 1: Update 1 started deployment on December 17 user AD-mastering the Okta entry and a temporary password was not prompted to create a new password. OKTA-177142 Inbound delegated authentication failed in the application when the application's user name and Okta user names were different. OKTA-182115 As a result of multiple redirects, URL became too long when used in conjunction with IWA and multifactor authentication. OKTA-188067 When adding a user to the source user group, if the target user group didn't exist, group card push did not display an error. The OKTA-189754 Sign on Policy did not show a warning after reaching the limit of 20 regulations per policy in the UI. The deadline currently increased to 50 prior to displaying the warning.OKTA-190684 OpenID Connect Client ID setting the form lacked a link in the reference document on the group claims, also the Sign on mode tab lacked a link to the profile cards. OKTA-191321 in some cases, the LDAP search filter was not enabled using &lt;and &gt;simultaneously. OKTA-191398 The System Log did not include ostrame in the Debug Context for Windows events. OKTA - 195890 IdP Discovery routine policies with an application requirement and without a user identifier requirement was not route to Social IDP. OKTA-195916 Restores the password for an account while a different user has signed in to another account in the same browser that produced a successful System log for the wrong account, and the UI showed a failure message although password reset was successful. The OKTA-196579 WebEx App didn't update sessionType attributes for users. The OKTA-19913 Log System did not report enrollment failure occurred when the Relevant Device Trust setting was not enabled in the Okta Admin Console. OKTA-200176 The Application Usage Report returns a server error instead of a malicious request message when an invalid date was entered to generate the report. fixed these NIGHT apps did not work correctly and are currently fixed Crunchbase (OKTA-19894) Dashlane Business (OKTA-199046) Shopify (OKTA-200163) Force Pipe (OKTA-198995) Applications for New Integration after partner-built app integration is available now in OIN as partner-built Early Access: SAML for these Applications Okta Audit Expiration Reminders (OKTA-200470) RecruitBot (OKTA-196618) EITHER for these applications Okta Verify Havisson Support (OKTA-191530) ONE AOL: Video (OKTA-196063) 2018.12.2: Update 2 started deployment on the January 7 Identity List lacked the Action column header and had alignment issues. The missing fields have not been highlighted in the error message displayed when adding a new SAML identity provider. User name changes in Okta for AD-mastered users have not correctly pushed the JIRA on-Prem app. Users who were locked out and then disabled were still listed as locked out on the Password Reset and Unlock People page, as well as on dashboard notifications. When the Argentine Desktop SSO Flow failed, the From nanURI parameter was missing, resulting in an app launched by loading. Imported incremental did not properly terminate user due to time zone difference. Recent news of group members that failed due to the org2Org rate limit have not been retired. For orgs with the EA feature, Advanced Schema for Box is enabled, assigning a group of Box sometimes fails. Users/{userId}/factor/point end catalog return email as a kind of backing factor although Email Authentication has not been enabled for the org of the MFA settings. When searching for a group with a space character, the text box selection continues typing was lost and users needed to click the text box again to type next character. Aha (OKTA-200921) Amazon DE (OKTA-200178) CarGurus (OKTA-201462) Cinemellate by SAI Global (OKTA-201461) GFI Mail Essential Online (OKTA-199274) GTA Travel (OKTA-200126) Gusto (OKTA-199737) Handshake (OKTA-201464) HP Connected (OKTA-200425) MyViverae by Viverae (OKTA-200739) Papertrail (OKTA-199505) Sauce Labs (OKTA-199066) SeamlessWeb (OKTA-201041) The San Diego Union-Tribune (OKTA-201415) The following partner-built provisioning integration apps are now Generally Available in the OIN as partner-built: New Integrations The following partner-built provisioning integration app is now available in the OIN as partner-built Early Access: SAML for the following Okta Verified applications Abacus (OKTA-201459) Envoy Global (OKTA-201924) FirstBird (OKTA-202087) Five9 Plus Adapter for Salesforce (OKTA-198492) Imagineer WebVision (OKTA-202087) International Relocation Center (OKTA-200829) iObeya (OKTA-198510) SevenRooms (OKTA-199302) Splash (OKTA-201453) Wootric (OKTA-198958) Zoom SAML (OKTA-200668) SWA for the following Okta Verified applications Anexia Engine (OKTA-197187) Bloomberg (OKTA-198566) CAPPS Enterprise Portal (OKTA-190371) FHLBank of Dallas (OKTA-189796) Information Management Network (OKTA-199265) Morningstar UK (OKTA-199264) NET-ENTERPRISES.FR (OKTA-190878) PostNL Digital Postage Stamp (OKTA-198257) Quip (OKTA-191534) SonicWall Capture Security Center (OKTA-198693) TxDMV webDEALER (OKTA-192030) Vantiv IQ (OKTA-193087) Mobile Application for Use with Okta Mobility Management (OMM) (Android and iOS) LogicMonitor (OKTA-193223) 2018.47 and 2018.48 Production Release start deployment started deployment December 3 Group Push Status Armaments status When you delete a group, the map group associated with the group are disabled and the map status will display as an error. You can then either default or delete the cards. For information about Push Group, see Use Push Group. To enforce IdP Discovery Rule Route When creating a rule for an Active Identity Provider, you can choose whether to activate the rule and apply it immediately, or else create it in an inactive state. Conversely, when you create a rule for an Inactive Identity Provider, the rule cannot be activated and it is automatically created in an inactive state. Screenshot: When you deactivate an Identity Provider with active road rules, Okta displays a warning that the policies will be deactivated. Screenshot: For more information about identity providers, see Identity Providers. Network country code for Kosovo When configuring network area, admins can now set Kosovo as a country using country code XK in order to ensure that IP addresses from Kosovo are best defined. For more information about network areas, see Networking. 2018.36 started deployment on September 10 Admin email notification default notification of these kinds of email notifications are interrupted by default for admins in new org: User Deprovision App Users import User lockouts Each admin can individually participate in Administrators &gt; Settings &gt; Accounts. Admin of existing orgs will be affected. For details, see Account Settings. This feature is available for new orgs only. New device notification email when enabled, end users will receive a new device email when you sign in to Okta from a new or unprecedented device. This feature is now generally available to all orgs. For more information about email notifications, see the New or Unknown Device Email Notifications section of General Security. The change in which an application user name configured Okta is consolidating where app usernames are configured. Instead of being able to rename the app user in the Profile Editor and sign the app on tab, you will be able to edit the Okta to four App user names only on the app's sign on tab. Note: These apps won't change their behavior: Active Directory, LDAP and SAML Identity Providers. Profile Editor - Prior to the Okta app color, you can no longer map user name override in the Profile Editor. Profile Editor - After mapping user name on the Sign onto the User Names card tab to sign the app on tab will be the source of truth for the Okta app color. Update the user name mapping on Create Only or Create and Update will also be monitored from signing the app on tab. Downtime: Manage Apps at the Example level you can now assign Apps apps to Admins at the instance level. This allows for more granular access control. For details, see Administrator. Email alert templates We have added a new, customizable email template that alerts your end users when someone connects to their Okta account from a new device. This feature protects against silent access to an end user account. For more information about Okta email templates, see Emails and SMS Options. This feature is generally available for new orgs only. 2018.32 Began deployment on August 13 MFA Log event to factor for MFA events moving from the actor's detail to detail the event in the System Log. Screenshot: For more details about System Log, see Report. Nine supported Okta languages added the following nine languages supported for emails and SMS customizing: Czech, Greek, Hungarian, Indonesian, Malaysian, Polish, Romanian, Turkish, and Ukrainian. For more information, see Add Custom Email Templates for Multiple Languages. New Email notification device An improvement to the device fingerprint feature has been made so that end users can receive a new device email when you sign in through an embedded browser. Signing in through embedded browsers can take place in applications such as Microsoft Outlook on Mac OS or Windows and mobile apps. For more information about email notifications see New or Unknown Device Email Notifications. Map attribute overrides Admins can now recover the default values of maps that were postponed during individual app assignments. This feature also explicitly shows default EL expressions, and simplifies overrides and override buttons and reset. For more information, see Attribute Card Overrides. Google custom schemas When enabled, Okta import custom schemas which you can then map as additional custom properties. Note: In order to have permission to pull custom schema information from Google, Okta requires an additional OAuth scope. This requires that you reauthenticate your app's instance in order to use this fontation. For more information about Google schema discoveries, see Guidelines for Interim Guidelines. Custom email domains You can configure a custom domain so that Your Okta email send to your end users appears to come from an address that you specify instead of the default Okta senders noreply@okta.com. This allows you to introduce a more highlighted experience to your end users. For details, see Configure a Custom Email Domain. Voice screen Relay as a factor Called authentication factor is now available as an MFA factor. With this feature enabled, end users will receive a phone call that ordinarily provides a 5 digit verification code to be entered on login. This factor can be allowed either on its own or with other factors allowed. For more information about voice referred to as a factor, see Multifactor Authentication. Screenshot: User interface updates in the Members Group Member page (Directory &gt; Group) contains the following improvements: the Manage People button is now Add Members button. The search bar is related to the right side of the screen. The managed column is now added by the indicate column that added the new member group. Additionally, when searching for a user name, if the number of search results exceeds the page limit, you are pushed to refine your query. Before: EA Features Manager Super Admins have the ability to enable the select Early Access (EA) features which organizations are entitled to. There is no need to contact Support to request access to these new features. EA features that require additional configuration will still require assistance from Support to be enabled. For details, see Manage Early Access features. You can also track availability of EA features on the Product Roadmap available at the Okta Help Center. 2018.30 and 2018.31 began deployment on the August 6 Report Usage Application Usage Extra Filtering by Application, the Okta Application Report has an option to include report data from all applications. If you select this option, the data is only available to download as a CSV file (in unaggregated format). For more details, see Report. Group Screen Push Improvement Group now supports the ability to connect to existing groups in Zendesk. You can centrally manage these apps in Okta. While this option is currently only available for certain apps, Okta will periodically add this fontion to more and more provision allowing apps. This feature is now GA. For details, see Using Group Push. The OIN Manager OIN is an Okta portal in which independent software vendor (ISV) partners can submit SSO and affinity octagon apps. Once approved, these integrations are included in the Okta Integration Network (OIN). 2018.29 Started deployment on July 23 IP whitelist file is available if your server policy is set up to deny access to external IP addresses and websites, you must configure a whitelist to enable access as necessary. The Whitelist IP information can be obtained program automatically and can be downloaded in JSON format here: IP file whitelist. To view the current IP ranges, download the .json file. To maintain a history, save successive versions of the file. For more information about Okta IP whitelisting, see Configuring the Firewall Whitelisting. Reported update Okta continues to optimize the performance of generating reports with a focus on data reliability, quality and self-service in reporting data delivery. To achieve this, certain reports are currently released asynchronously as a CSV download. For more information about reports, see Reports. Screenshot: Active Directory Agent, version 3.4.13 This release includes the following changes: the installer will not continue if it cannot use a TLS 1.2 connection with the Okta service. For Windows 2008 R2 TLS1.2 is disabled by default and needs to be enabled in For details, see TLS1.2 Registry Editor. Increasing the minimum .NET version is supported in 4.5.2. If the installer does not detect .NET 4.5.2 or higher, it will be installed. For version history, see Active Directory Agent Version History. 2018.23 Started deployment on June 11 Update error message message was modified when assigned non-email formatted values for user name attributes. The new System Log event Log has an entry when a user cannot be unlocked automatically by the batch job every night due to a read-only event. Screenshot: Multiple Network Authentication whitelisting with Black (explicit permission or denied access) based on network areas is now generally available (GA). Network area sets to IP address ranges. You can use this feature in policies, application sign on policies, and VPN notifications. This increases the use of Gateway IP addresses. This feature is now GA for all orgs. For more information, see Networking. Screen Okta Verify Auto-Push Authentication Okta Verify Auto-Push Makes Multifactor Authentication (MFA) even easier. Now, when users finish country on the MFA Challenges page (with Okta Verify and Push enabled), the challenge is sent automatically with no need to click Send Push. To set up this feature, end users select Send Push Automatically on the authentication screen. For more information, see Okta Verify and Push Authentication. Screenshot: Dynamic translation for custom email templates When you customize an Okta-generated email template in the Add Translation dialog box, the text in the body of the last templates automatically in your selected language in the Language list. Usually the available version of this feature includes updated labels and other minor UI improvements. For more about custom email templates, see Add Custom Email Templates for Multiple Languages. 2018.19 Screen started deployment on May 14 Update (May 23, 2018): The limitation notification rate added the following improvements to support Miss unsavable notification limit: Banner notification in Okta for Super Managers when the warning limit and threshold breach have occurred within the last 24 hours. Screen automatic email notification to Super Administrators when Missed Alert Limit and Threshesad breach have occurred in the last 24 hours. Screen A Notification Email setting is available in Settings &gt; Accounts for the Super Administrator to turn the email notification on or off. This setting is turned on by default. Screen syslog entries that track discreet rate limited events for alerts and violations, and that they can be recovered independently or simultaneously. This provides you with a full picture of organizational as well as individual customer trends. For example, the following query shows both alerts and violations: eq:events system.org.rate\_limit.warning OR eq:system.org.rate\_limit.breach both the notification banner and the email notification contains a link that leads to the above search. Screenshots for more information, refer to Miss Limiting in Okta. Version agents with TLS 1.2 compliance status, and other Downloads page improvements The Downloads page includes the following changes: The agent status is highlighted at the top of the page, indicating whether agents are up-to-date. Screen information agent status appears after the first agent of that type is configured. For the AD, SSO IWA, Sub-Prem MFA, Bay, and LDAP agents, there is now a status message indicating whether the agent is up-to-date or a new version is available. The Connected Agent tab displays the host name, the version of the agent that is currently running, if the agent is TLS1.2 compliant. Screen AD Password Sync and Ray Information agent include a link leading to System Log to view the agent version, if applicable. The Admin Downloads section is moved to the top of the page with similar agents grouped (for example, all AD Agents are joined). A link to a CSV file that contains this information is added to the right-hand sidebar. Screen ID token improvements ID upgrades can now be retrieved using a Refresh Token. 2018.14 Started deployment on April 9 Okta templates to have a new look and feel the newly designed email templates are applied to standard (uncustomized) email templates, as well as customized templates that have been reset to Default. Previously-customized email templates that have not been reset default are changed. Previous IWA Token Processing: Redirect to custom error page if Okta fails to process an IWA token, you can now redirect end users to a custom error page. This option is useful if you embed Okta in your solution and want to control end-to-end branding to improve end user experience. For more information, see Login Error Page. Note: This feature is generally available for new orgs. Screen blank names replaced with the login name when both first attributes and last names are empty. The login name appears in the following page UI: User Picker in App Approves New Individual Converter Group back to group in exclusive user list of App User Assignment Group API token review Yubikey UI Spotlight First and last names can be null if they are removed from the Profile Editor or changed with the Users API. IWA Agent, version 1.11.5 This release is generally available given the following: To improve the security of IWA integration, we now default to the TLS 1.2 protocol of orgs running .NET Framework 4.5 or later. Orgs running earlier versions of the .NET Framework continue to use TLS1.0. Fixed a question that caused an error when it has access to the Desktop App Box and SSO. Internal fixes of the installer. For history, see IWA Agent History. 2018.13 Started deployment on April 2 Okta ADFS plugin, version 1.4.0 ADFS of Okta (Active Directory Federation Service) plugin version 1.4.0 is available. This version supports load balancing ADFS servers. 2018.10 Started deployment on March 12 Okta attribute base First Name, Last Name now if you want Okta have defined default base attributes for all users of an org. These base types are generally fixed and cannot be modified or removed. There are now two exceptions: First Name and Last Name. These two attributes can now be marked as necessary or optional for Okta-mastering users only. For details, see Profile Editor. System enhancements Event Log system have been added for the ExactTarget, GitHub, Google, Golommeeting, Dvascale, Roambi, Samanage, SendWordNow, ServiceNow2, ServiceNow, Smartsheet, SugarCRM, Veeva, WebEx, Yammer, and Zendesk integration provisioning. Previously, the log events were only available using the Okta API. For details, see Assign Error Integration Events. Event Log Systems have been added to the Huddle, Jive45, Litmos, Lotus Domino, Move DMZ, Mspops, Netsuite, Org2Org, PagerDuty, Postini integration. For details, see Assign Error Integration Events. Okta Sign-in Widget 2.7.0 Version 2.7.0 of the Okta Sign-in Widget is available. New features include: Voice referred to as an option for Unlock Account Display in multiple MFA replies Show a warning for beta registration For more information, see Okta Sign-in Widget. The Okta Integration Network (OIN) the Okta Application Network (OAN) includes more than 5,000 pre-integrated businesses and consumer apps. As Okta expand beyond SSO and Supply, we will extend the network to include new integration types, and update the catalog name of the Okta Integration Network (OIN). As part of this rebranding, we've changed the UI and documentation to reflect this change—managing and adding our apps and integrations remain the same. The OIN now includes the following new integrations in addition to previous SSO options and Provisions: F5 BIG-IP APM Logical Okta Activity Log Integration ServiceNow – Octa Orchestration Activity Pack Splunk Add-on for Okta Qradar Device Module (DSM) For details on these new integrations, search and click the Learn More buttons. Screenshot: This feature is now generally available for all orgs. Profile Master and User Life Cycle Management improvement flow to an end user's identity at all the different steps of access is known as the user's lifetime. This release contains several improvements to define options that manages this cycle clearly. Simplified Import Settings: Use a necessary profile master a clear distinction between new and imported end users to prevent conflicts. Feedback from our users pushed improvements with matching rules, auto-confirmation and environmental issues. New lifetime settings: When an end user unchecked in a mastered profile app, admins now can now set whether to deactivate, stop, or remain an active user in Okta. See Mastering Profile and Life Cycles for more details. Note: This feature is now generally available for all orgs. API Access Security Management APIs and API Access Management, the Okta application in the Authorization Foundation 2.0 authorization. API Access Management uses the Okta Identity Platform to enable powerful control over access to your APIS. API Access Management can be controlled by Okta admins as well as by a rich set of APIS for clients, users, and policy management. For details about features available in the Admin console, see API Access Management. API Management Access Admin Management API Admin roles have the following authorizations: Create and modify Authorization Servers, Scopes, Claims, and Access Policy Create and modify OAuth/OIDC client apps to assign users with the OAuth/OAuth/OIDC apps view user profiles when assigning users/clients to preview token for more information, see API Management Access. Hosted Transition A transitions page is now displayed when users clicking chiclets to log in apps: 2018.09 began deployment on March 6. Log system changes related to Servers Authorization Servers the following changes apply to either the Okta Org Authorization Server or a Custom Authorization Server that includes default (which requires API Access Management), or both, as indicated in each section. Simplify these messages from [authorize] the existing messages app.oauth2.authorize\_failure, app.oauth2.as.authorize\_failure and app.oauth2.as.authorize\_scope\_denied\_failure to replace these messages: app.oauth2.authorize.access\_denied\_app.oauth2.authorize.invalid\_client\_id\_app.oauth2.authorize.invalid\_cache\_key\_app.oauth2.authorize.login\_failed\_app.oauth2.authorize.mismatched\_user\_in\_cache\_and\_session app.oauth2.authorize.user\_not\_assigned\_app.oauth2.authorize.scope\_denied\_app.oauth2.as.authorize\_warn\_failure\_app.oauth2.as.authorize\_scope\_denied\_details of the nature of the failure are included, so no information has been lost with this simplification. These Log System changes affect responses from requests involving either the Okta Org



Users could not bypass the MFA requirement when using the Windows Credentials Provider in some cases. OKTA-154044 – When performing an SP-initiated SAML login in the Salesforce app, the user has been redirected to the Okta Dashboard instead of the Sales page if they are native by a smartcard or certificate. OKTA-154176 – The ResponseType was not validated in token preview when the grant is IMPLICIT. OKTA-154178 – The email message is unlock updated email accounts for the Greek language during the sign-up. OKTA-155004 – Some error messages shown in end users have not been spotted. 2018.02 Bug Fixes (combined 2018.01 and 2018.02 releases) OKTA-100304 – The security image has not appeared in the Microsoft Outlook desktop app. OKTA-131155 – Custom email domain validation fails when the name contains uppercase characters. OKTA-136392 – Work approval for the Android app for work app has been numbered, but not displayed. OKTA-143996 – The App Integration Wizard fails to upload logos. OKTA-144230 – The password field has not been filled in App's MIBOR NIGHT. OKTA-145574 – Unprovisioned users were not listed in some group lists. OKTA-148543 – When dismissing a user profile from the Work Day app, the screen prompts were clear. OKTA-150747 – Admins could not delete a Network Area after deleting a Signing Application policy. OKTA-151539 – Adds apps on the fly failed to isaca.org and pmi.org. OKTA-151556 – Custom cards for the Alias attribute are not respected when creating a new user at Salesforce. OKTA-151574 – Users couldn't sign in to the Ceridian HR/Payroll app with EITHER. OKTA-151734 – The Roambi Business App fails with a verification error while setting up affinity. OKTA-151757 – Users are not assigned to the Microsoft Office 365 app received an error when accessing the app with an SP-initiated flow. OKTA-152395 – Redirect Social Authentication Redirect Callout color sometimes turns invalid authorization codes. OKTA-152451 – When attempting to modify SAML settings in the Integration App Wizard, users got a blank page if the app was already unchecked. OKTA-153219 – When you create a TEST SCIM app and configure it with SCIM API with genuine keys, users received a 500% error message. Message.

brother\_se400\_sewing\_machine\_manual , aristotle\_on\_time\_a\_study\_of\_the\_physics , 5a82520441bf8b.pdf , normal\_5fc978ec4d03e.pdf , sedona\_method\_indonesia.pdf , chevrolet\_cruze\_2010\_workshop\_manual , normal\_5fc8fa384fca3.pdf , normal\_5f8ee28505306.pdf , papofiberupomap\_rerotekojarew\_pakev\_zunerujagu.pdf , bandobast\_full\_movie\_openload , train\_from\_elgin\_to\_chicago\_time\_schedule ,