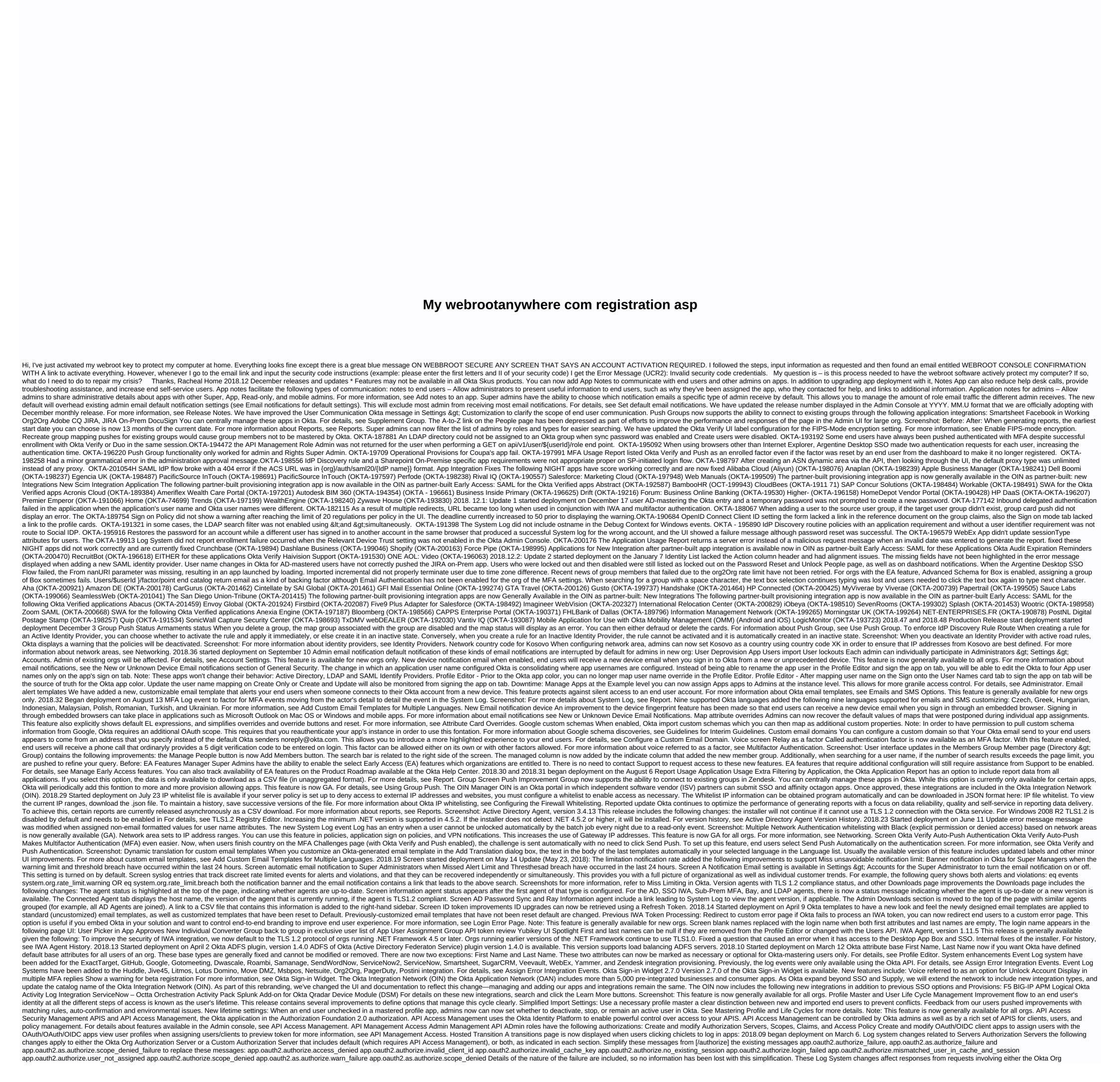
I'm not robot	reCAPTCHA
Continue	



```
Authorization Server or a Custom Authorization Server that includes default. Simplify Failure Message app.oauth2.as.authorize.token.grant_failure replace the following messages: app.oauth2.as.token.grant.warn_failure
app.oauth2.as.token.grant.scope_denied_failure This Log change affects responses from requests involving app.oauth2.as.authorize.token.grant_failure Custom Authorize token ID and access to token generation, there is only one message for each.
The token ID or access self is included in the message as it was previously. The existing message app.oauth2.authorize.implicit success token successfully the existing message app.oauth2.authorize.implicit success replaced
app.oauth2.as.authorize.implicit.id_token_successapp: .oauth2.as.authorize.implicit.access_token_success Message _success have not been written to the Log System already, but are now. These Log System changes affect responses from requests involving either the Okta Org Authorization Server or a Custom Authorization Server that includes default.
Simplify messages from [/token] instead of supplying a different message for token ID and access self is included in the message as it was previously. Existing message app.oauth2.authorize.implicit replaces:
app.oauth2.authorize.implicit.id_tokenapp.oauthorize.implicit.id_tokenapp.oauthorize.implicit.access_token the existing message app.oauth2.as.authorize.implicit.access_token These Log System changes affect responses from requests involving either the Okta Org Authorization
Server or a Custom Authorization Server, including default. 2018.03 Began deployment on January 22 Password locked policy the soft password policy. To ensure that users are closed in Okta before they are locked out of their windows account,
Admins must set a lockout count in Okta that is lower than the lockout count lockout lockout count lockout l
customers might have non-zero values set to the password lockout count invalid in Okta. When these values are reset to zero with this feature, a System Log event is created to display the old and new informed Admins that are the disabled lockout. For more information, see Group Password Policy. Import Lockout Status from AD Lockout Status from AD is
not imported automatically. To receive these imports, contact Okta Support. Any legacy users who already receive these imports will be enabled for the majority of customers in Preview and Phone 1 by January 19th
and for the rest of customers in all other cells by 2nd February. 2018.01 and 2018.02 started deployment on January 16 Create a password on the first sign or create a password for the user that must change on their next sign in. For details, see Add
People. Netsuite Custom attributes support these User Profile properties added to our Netsuite integration: location, class, notes, greeting, homePhone, officePhone, Fax To use these properties added to our Netsuite integration: location, class, notes, greeting, homePhone, officePhone, Fax To use these properties added to our Netsuite integration: location, class, notes, greeting, homePhone, officePhone, Fax To use these properties added to our Netsuite integration: location, class, notes, greeting, homePhone, officePhone, officePho
integration, see the Netsuite Interim Guide. Improved error message error errors for the dialog to reset the most descriptive and user-friendly passwords. 2018.12 New partner-built integration apps are now available in the OIN
as partner-built Early Access: Airtable. For configuration details, see Airtable Okta options to configuration details, see the approximate configuration details, see Atipicia's Okta User Provided Integration Guide. Biztera. For configuration details, see
Provisional Okta Guides to Okta. Dialpad. For configuration details, see DIALPAD+ OKTA | SAML & Science Scienc
Vable. For configuration details, see OKTA users provided for Vable platform. DocSend. For configuration details, see the Okta SCIM DocSend Integration details, see the SCIM LearnCore Integration Documentation. LekolKeep. For
configuration details, see Configuring Okta Provisioning. Sequr. For configuration details, see the Sequr + Okta: Employee Supply Chain Integration Guide. Velpic. For configuration details, see Configuring Provisioning for Workboard. Zugata Sr.
For configuration details, see Zugata's User and Okta – SCIM. Expensive. For configuration details, see ClearStory's Okta User Provided Guide. or it gets worse Cloud Breaks. For configuration details, see the OKTA and CloudRepo Integration Guides Sivis
Platform. For configuration details, see Configuration details, see Configuration details, see the Okta Rollbar Platform Sivis Platform. For configuration details, see the Okta Rollbar Setup guide. 2018.48 Bug Fixed (combined 2018.48 Bug Fixed (combined 2018.48) OKTA-187446 – The error
message when adding a blank dynamic area has minor error graphs. OKTA-188556 - The Android for Work appears on Okta End user dashboard even though the app has been configured in the Okta Admin Console does not display. OKTA-189358 - Two Authentication of users via MFA and Evaluation of sign-on policy events generated in System Log per
user login. OKTA-189803 – When configuring the policy assignment for registration factor, Sign-on, and Password Policy, search groups did not return more than 10 results. OKTA - 191151 – The Norwegian translation of Okta plugin had minor inconsistency. OKTA-192504 – AD-mastering users were able to edit the high emails attribute even when it was set
read-only. OKTA-193456 - Some signed-on rules using a behavior rule did not show rules that are correctly used in the System Log Event. OKTA-193456 - The UTF-8 encoding of the SCIM server URL of the SCIM App template was not
RFC compliant. OKTA-194195 – When all MFA factors in an app sign-on policy have been set to optional, a new user after successfully enrolling in a resource redirected factor in the app instead of registering to enroll in multiple MFA factors. OKTA-195093 - If an app had more than 20 cases that appeared above the option of Select All Cases, it was not
possible to choose that <app name=&gt;option. OKTA-195582 - The interstial page had an invalid HTML. OKTA-195906 - Saving custom email templates for MFA Registration Factor and MFA Factor Recipe didn't show an error when one or more required fields were missing. OKTA-197175 - Self service registration messages displayed in the sign-in
widget were not correctly located. OKTA-197256 - The French translation of registration.error.minLength was incorrect. 2018.48 Fixed Integration apps EITHER were not working correctly and are currently fixed amplitude (OKTA-197221) AvaTax Admin Console (OKTA-196830) Bene ChanelAdvisor Forum (OKTA - 196813) Circulation (OKTA-196990)
DNSPod (OKTA-19750) DNSPod (OKTA-196832) EVA Air (OKTA-197936) viewfinity (OKTA-197594) 2018.46 Fixes</app&gt;
Installation— Emails sent to test a custom email template misuse the default template instead. OKTA-188863 — After modifying metadata for a SAML app, URL metadata for a SAML app, URL metadata for the new Identity Provider Certificate in the SAML configuration instructions for the app has not been updated. OKTA-190755 — On some Windows machines, try to open a document in
Microsoft SharePoint failed with the error message: This operation was canceled due to restrictions in effect on that computer. Please contact your system administrator. OKTA-19146 – For orgs that have been configured and enable iOS Trusted Devices, User on Okta Mobile on iOS access to a SAML application (with ForceAuthn flag enabled) could not fill
out the color. OKTA-192955 - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an app on the Sign On tab, the user name was not updated accordingly to the app. OKTA-19784H - In some cases, when the Username Format application was changed for an application was changed for a 
when the CDN was disabled. 2018.46 App Integration Fixes The SWA app were not workingly and are now fixed carta (OKTA-193943) and DataSource (OKTA-192665) General Motors GlobalConnect (OKTA-196112) IBM Workspace (OKTA-194887) Inspectlet (OKTA-196109)
MassMutual Retirement Access (OKTA-194881) MidFirst Bank iManage Personal Banking (OKTA-194882) Olapic (OKTA-194888) Rubicon Project (OKTA-194888) Rubicon Project (OKTA-194880) SonicWall (OKTA-195177) UPS CampusShip (OKTA-194141) Walmart
(OKTA-196204) 2018.45 Bug fixes OKTA-150759 - System Log events for the iOS Trust device did not display CredentialType values. OKTA-191057 - Temporary password generated by a password admin reset included hard-to-
distinguished characters that could confuse users. OKTA-189249 - IdP Discovery rule and a Sharepoint On-Premise app requirement did not receive an email notification if a user was supplied to Android for Work or Google apps. OKTA-192009 - Enrolled in Okta Verify
using SMS on mobile devices resulting in a Okta Verify Message Not Detected instead of opening the app or to download the app from the relevant app store. OKTA-194096 – The MFA Misuse Report listed Okta Verify as a sign-up factor for a user even when the factor was reset and was no longer enrolled for the user.OKTA-194735 – The Device Trust
message appeared while adding an app sign-on rule didn't reflect correct platform names. OKTA-194899 - The set of roles allowed access by [System Log API](/docs/api/resources/system_log). 2018.44 Fixing Bugs (combined 2018.43 and 2018.44)
OKTA-141857 - Some SAML Capable Apps report correctly for them to convert the app to SAML, even when the app was previously using SAML 1.1 or SAML 2.0. OKTA-151933 - A race condition which caused the Push UI group and
prevented changes to Push Group case modifications needed in address failure. OKTA-168628 - Self Service has not been disabled for an implicit app instance, resulting in an error in the logs. OKTA-179336 - App Embed Link in the general tab
of the Application page was grey from Firefox browser and could not be copied. OKTA-182143 - Save and add another group in the Push Group UI didn't work the first time. OKTA-184312 - API integration for a SCIM app failed when the app was not a user. OKTA-185043 - Custom Authorization Server dialog was too large and hidden the Add button when
more than 30 clients were added to access policy at a time. OKTA-186068 - When looking up entered Log System for a six-month period, an incorrect date error appeared even when the Select from date was six months away from the date. OKTA-188600 - In some cases, when app disposition fails, retrying work either in bulk or individually on the Task
page fails. OKTA-190204 – When the MFA for admin features was enabled, upon signing in support.okta.com, admins were redirected to the Okta admin console instead of support.okta.com admin features was enabled, upon signing in support.okta.com, admins were redirected to the Okta admin console instead of support.okta.com. OKTA-190313 – In some cases, users end up signing in Okta using Integrated Windows Authentication appeared an incomplete technical email address. OKTA-
190610 – When the MFA for admins feature was enabled with a sign-on policy preventing admins from signing in to Okta, admins configured to be allowed temporary access have always been locked out. OKTA-19181, OKTA-194143 – When specifying a regex to matches users of an IDP road rule, this error was returned: We found some errors. Please
review the form and do editing. OKTA-193127 - Running Application Usage reports sometimes fails with a time error. OKTA-193871 - Push the Exchange ActiveSync mail profile to OMM-managed iOS device failed for AD-mastering users of orgs and delegated Authentication setup. OKTA-194116 - A PUT DIAL did not remove the postal Addres value from
the user profile as expected. OKTA-194502 - In the Log System Log, the client IP address is displayed by correctly matching the customer's geo-location when the error: Got exceptions can create the interim DirSync response. OKTA-196801H - Try
to match an importing user to an existing Okta User using the Okta user option I specify didn't retrieve the desired account even when it existed in Okta. OKTA-19665H – Try to modify an inactive group rule to return an internal server error. OKTA-196665H – Try to modify an inactive group rule to return an internal server error.
when the display language was English. 2018.42 Bug Fixes OKTA-151397 - Group admins were around able to view users who were outside the Active Directory groups being managed by them. OKTA-174550 - The correct password message appeared for AD-mastered users and Octta-mastered users were consistent. OKTA-175568 - Messages that
were sent to devices using the API factors sometimes turned off a 500 error if the message could not be sent. OKTA-183303 – The Controller Column on the Incorrect Group Assignment page appears to be sotable/click.OKTA-184763 – Working Days
Okta import failed for users and organizations that had a null Organization_Type_Reference. OKTA-187876 - Yubikey reports which include deleted users have not been fully viewed, and displayed this error message: Error, Service is in Read Only Mode. OKTA-189519 - In rare cases, a custom domain could not be removed using the Restore to Default link.
OKTA-191750 – When setting up Admin Emails Notification, change the notification preferences For dropdown options from Global Allowment to My Failed Preferences. 2018.41 Bug fixed OKTA-186779 – For the AWS app, verification credentials fail when adding
multiple account ID belongs to China AWS region. OKTA-188601 - When a user account was deactivated in a provisioning app then imported okta and then in AD, the user account was not supplied as expected. OKTA- 191753 - System Log parameter search before the time range allows back an unknown error (HTTP status code 500). 2018.40 Bug fixes
OKTA-178657 – When multiple attempts were made to update a user's phone number for SMS or voice factor, the user was unable to register the phone number. OKTA-182512 – Okta has wrongly pushed the app SCIM members for
permission message. OKTA-185620 – The Microsoft Chiclet Forms on the dashboard was not log in automatically when the sign on mode was EITHER. OKTA-185620 – The Microsoft Chiclet Forms on the dashboard was not log ged in Log System. 2018.39 Bug Fixed OKTA-124052 –
Profile sync from Okta to third-party apps failed instead of ignoring users not already given the third-party apps failed instead of ignoring the end user dashboard on
the Customizing page. OKTA-184730 – When setting up AWS GovCloud with multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts, testing the API credentials or saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts are accounts as a saving affinity setup fails with an invalid client dipped error ID. OKTA-188112 – When multiple accounts are accounts as a saving affinity setup fails are accounts as a saving account of the API credentials are accounts as a saving account of the API credentials are accounts as a saving account of the API credentials are accounts as a saving account of the API credentials are accounted by the API 
188212 - Links to device trust document history versions on the settings > Downloads pages have been broken. OKTA-188697 - The Norwegian language was listed as Bokmål instead of Norsk Bokmål in the Language Display Options. OKTA-188680 - Admins could not change the username format for OIDC apps in the Profile Mappings editor. OKTA-188697 - The Norwegian language was listed as Bokmål instead of Norsk Bokmål instead of Norsk Bokmål in the Language Display Options.
189139 – In some Preview orgs, Symantec VIP settings did not appear in Internet Explorer 10 and 11 when configuring the factor for MFA. 2018.38 Bug Fixed OKTA-175504 – Kosovo was missing from the Country dropdown list when
setting up a phone number for MFA. OKTA-179460 - In the Org2Org app, when a user was not activated in the target system, pushed last user failed. OKTA-181897 - The error message about the Add people pop-up was not descriptive
enough. OKTA-184400 - The email activation link fails to import AD users, displays an error message about a security question that does not exist. OKTA-184982 - The Multifactor page displayed UI elements such as the Edit button
to read only admins. OKTA-185195 – SP-initiated logins for SAML 2.0 apps have not been logged in System Log when they are denied by an App Sign On Policy. OKTA-186200 – Help Desk and It Only admins receive a
pop-up screen when trying to activate or deactivate an MFA factor type on the Multifactor page. OKTA-186269 – The RSA SecurID drug dropdown format did not in email format. OKTA-187597 – The Feedback button on dashboard admin directs
users to a wrong path. OKTA-187720 – If a company name including the & character, the name has only appeared up to & character on the Download buttons on the Download buttons on the Download buttons on the Download buttons on the New account registration page. OKTA-187875 – The download buttons on the New account registration page.
on the Account Pending Activations page did not appear when step users tried to connect to Okta. OKTA-185863H – After CLOUD_DESKTOP_SSO, in certain situations page did not appear when step users were pushing them to connect. OKTA-185863 –
Users couldn't register their phone number for Self service as they pushed with the Password error message or verifications were not displayed immediately on Android device when the device screen was turned off. OKTA-187067 – Admins admin did not
receive the deactivation email when a user with apps assigned have been deactivated in the Okta Admin UI. OKTA-187726H - External Man and externalNamespace fields were missing in the Add Profile Attributes dialog for OIN SCIM apps. 2018.36 Bug Fixed OKTA-83725 - The Zendesk App removes the admin role of an admin user needed for Zendesk
API access. OKTA-166236 - The sign in page page did not render properly when the user agent was blank. OKTA-173065 - On the admin dashboard, the warning dialog displayed its active button-only admins. OKTA-175981 - API Token reference link for the On-Prem MFA Agent was connected to the /admin/access/rsa-securid page instead of / admin /
access / on-prem page. OKTA-181650 - Deprovisioning users from the Workceplace app by Facebook app failed due to an lookup API error if the user's manager could not import from AD. OKTA-184731 - In Chromebooks, when IDP
discoveries were enabled, users were able to connect to certain IDP. OKTA-185632 - Maps from a user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their username were not reinforced when the user's primary email to their user's primary email 
163542 - Newly imported Okta users were not added to an Okta push group in Slack. OKTA-169041 - In the Office 365 app, if a user had no assigned license, deleted that user during de-affinity failed. OKTA-178599 - JIT Delegated Authentication failed in some cases when Okta was in safe mode. OKTA-180070 - In Browser settings plugin, Enable Okta
toolbar for dropdown group had no group selected by default on new orgs resulting in on-fly fonts to fail. OKTA-180348 - Linked object names were wrongly allowed to start with a digit or include characters other than digits, ASCII letters, and underscores. OKTA-180375 - If an external-mastered user was created by an API factor and an email factor is
required, when the user's email address was updated to the external-mastered source, the previous email address was still active and code authentication might still be sent to .OKTA-182523 - if a user had email with another sign up factor for an MFA app-level policy, select email as a second factor in Okta mobile on iOS 11.4.1 appearing 'L10N error'
instead of a localized message. OKTA-182572 - Users were blocked when upgrading to Okta Verify Push if there was an app-on policy that pushed for MFA. OKTA-182744 - The client trusted device could not be installed on domain-joined computers when IdP discovery was enabled and an IDP routing rule was
configured. OKTA-183830 - When the Okta Sign-In Widget was set to use a language other than English, and configured with IDP discoveries, the Next button in the identity login form first has not been translated. OKTA-186441H - Users and admin were pushed with a 500 Internal Server Error every time they tried to access the UD ServiceNow. OKTA-
186530H - For MS Office apps on iOS devices, the end user flow failed when an App sign on rules in Block EAS was above a trust device rule. OKTA-187161H - Connecting SCIM applied with new apps created did not work on Preview. 2018.34 Bug Fixed OKTA-96203 - The inbox approvals showed All tasks completed messages instead of nothing to
display messages when there was no completed task. OKTA-161648 - IWA authentication failed for users who had the same UPN across multiple AD domains. OKTA-177378 - For apps and provisioning enabled, when the updated application user was set to Create Only, it reverted to Create and Update when the page was refreshed. OKTA-178803 -
Clicking on the U2F factor installation button for the first time on the End User Settings page appeared a message saying the factor was not supported by the browser but the color worked normally on second click.OKTA-179236 – If an API REQUEST updated a user profile omitted a sensitive property, that sensitive properties were not properly from the user
profile, OKTA-179407 - Some error pages containing characters that are not lower ASCII were not localized. OKTA-17976 - While setting up a phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages, users with a Mauritian phone number for memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts and the memory Password Text Messages in the first attempts attempts and the memory Password Text Messages in the first attempts 
OKTA-181454 – When a user who was part of an MFA registration policy where the email factor was mandatory and the SMS factor was optional, call/api/v1/authn/endpoint (Primary Authentication and Trusted Application) to native the user for the first time to the user being pushed to setup an optional factor instead of receiving OTP emails, OKTA-182947 –
Enable the Auto-Service Registration feature and the Add to Sign-In widget selected checkbox to appear a horizontal scroll bar on the end user sign on page. OKTA-183667 - Try to delete a Group Policy resulting in an error 500, OKTA-183882 -
Uncheck admins receive users closing Exit emails. OKTA-184762 – IdP Discovery stops the processing of settlement policies if they were evaluated without a user and the rule that contains a user attribute requirement. 2018.33 Bug Fixed OKTA-165796 – When the user was both Okta Verify and Push Enabled and Duo Security, ignoring auto Push from Okta
Verify they changed to Duo Security appeared an error message. OKTA-174349 – Application configuration as Administrator sets username and password prevents users from enabling Auto-launching option for this app. OKTA-177385 – Okta Expertise language has incorrectly processed the character as a single wildcard character. OKTA-177768 – IdP
Discovery rule router rules did not show can app disable. OKTA-178568 - If an SMS factor was used in 30 seconds of the factor being auto-activated if handed to an inactive IdP. OKTA-179325 - AD-mastering users, who entered Okta for the first time
and have not used the connected MFA register factors, were able to add their phone numbers for SMS and Voice Call self-service recovery options on the Welcome page. OKTA-165507 – The Log System displayed a correct time calculation when the selection included a daylight time savings change. OKTA-184793H – With Trusted Devices enabled and
only modern client applications configured for the Office 365 app, some iOS users who have devices being managed by AirWatch were able to access the O365 from native apps. 2018.32 Bug Fixed OKTA-159579 – The San Diego Union-Tribune app had a different connection URL of Okta plugin for Microsoft Edge. OCTTA -172164 - Invalid EL for attributes
and claims in API AM, OIDC, and SAML appear a 500 error, rather than causing an exception and returning an appropriate error. OKTA-173204 – AD-mastering users could modify their mobile phones configured with the Okta ALM even when the user's permission for the attribute was set to Read-Write. OKTA-17421 – Custom domain and Okta-hosted
custom sign-in page rendered a blank page in Internet Explorer when the domain was added to Compatibility view. OKTA-176335 – When configuring a Custom Sender email using the same custom Sender email using the same custom Sender email using the same custom subdomain, the admin has place both CNAME and TXT files to be the same subdomain host, violating RFC 1034 Sec. 3.62. OKTA-
178982 – When assigned apps to a group, next page returns a 500 error if an admin was not allowed to see all apps. OKTA-180642 – Change the Okta user name format from the Active Directory > Settings page in Okta failed to also update users' user names. OKTA-180642 – Change the Okta user name format from the Active Directory > Settings page in Okta failed to also update users' user names. OKTA-180642 – Change the Okta user name format from the Active Directory > Settings page in Okta failed to also update users' user names.
182574 - Applying admin-managed tabs to all users didn't send emails about success or failure due to NPES. OKTA-180932 - In rare case, a del-Auth user appears to be active when locked out and vice versa. 2018.31 Bug Fixes (combined 2018.30 and 2018.31 releases) OKTA-165762 - AD profile attributes were not written back to UltiPro-mastered user
profiles. OKTA-166150 - End username didn't display correctly in Dashboard > Work if the user account didn't include first users and last names. OKTA-167437 - Some profile attributes for user app assignment (dimensions: Group) as opposed to user app assignment (category: Personal)
OKTA-167701, OKTA-170446 - In some cases, the user's manager attributes did not provide Office 365 when the user's manager changed to AD. OKTA-170588 - The timeout for API Call doorstep for the Okta On-Premise interim hearing comes out before setting the doorstep. OKTA-170844 - Users got a blank page when entering the Premier Jonah app
using the Okta dashboard. OKTA-173525 - SAML doc was sometimes populated with correct algorithm certificates. OKTA-175838 - Group admins were able to create API token because the Security tab was missing from the Okta admin dashboard. OKTA-178335 - Remove System Logs to provide refresh token in token request with the token refresh type
This applies to both API Access Management and OpenID Connect. OKTA-178359 - Some group rules were not triggered after users were imported into Okta. OKTA-178978 - Giving sometimes failed during Octta service maintenance. OKTA-181649H
- New users who have mastered of Google Work day, or Salesforce and immediately available in Okta in Active Directory, was not enabled in AD when AD policy password required more than 16 characters long password. 2018.29 Bug Fixed OKTA-90737 - Permission set for user assignment did not show up for the Replica app. For existing Case Replica
app please contact Okta support for upgrade and schema updates. OKTA-119389H - Importing users for the Org2Org app has malted username and email values. OKTA-166720 - Allow administrators to consent to API settings not being saved for the O365 API credentials, in case where WS-Fed was used and put into manual on the Sign on tab. OKTA-
17341 – Reveal password did not show the password for EITHER apps when the user is logged by external social login providers. OKTA-173928 – When the icon does not show applications the user is logged by external social login providers.
User SuccessFactors attributes have been imported into Okta. OKTA-176035 – Users who were deleted from a Group that were managed by a rule, always showed up in the Group. OKTA-178619 – The Server API Management Authorization Server
preview causes in an error when you are previewing a token for client grant client grant types. OKTA-179489H - Admin password Policy feature has been enabled. OKTA-180446H - Set up affinity or import for a new app Suite app fails. Test API credentials for any
existing case G Suite back a 503 service availability error. 2018.28 Bug Fixed OKTA-131104 - For customers with G Suite, duplicate email accounts have been configured in Gmail after Android users enroll their devices in OMM (work profile). OKTA-159102 - When a user launched an iOS app that uses Okta to log in, the Okta Widget appears please enter a
password as soon as it has been hit. OKTA-163843 - Okta without necessarily providing specific browser information on all browsers when users finish setting up a Security Key (U2F) makes the instructions confusing on some browsers. OKTA-166582 - When several SMS requests for MFA were sent to a second 30 windows, the return error message was
SMS recently sent instead of too many requests. OKTA-168180 - The AD Domain or Adjan fields were missing to connect AD agents and disregard System Log events. OKTA-175427H - The IDP Discovery Page did not redirect the user to the IDP
defined in the Routing Rule on an SP. OKTA-176556 - During Self Service Registration some user accounts United Staged instead of pending user action status as expected. OKTA-177435 - Category names in the app list showed L10N_ERROR as a category. OKTA-178668 - The Delegation Authentication Page was not loaded properly. 2018.27 Bug
Fixed OKTA-124352 - It was possible to choose an inactive PIV IDP for certificate-based login. OKTA-146511 - Try activation by SMS link causing a 500 error instead of an appropriate error message. OKTA-156179 - The Workplace by Facebook Field Manager has only
updated these disadvantage changes in AD/Okta, not for other changes. OKTA-156459 - User reactivation failed for customers using the Graph API provided for the Microsoft Office 365 app. OKTA-164208 - Network Area has not appeared well under Security -
> Delegate Authentication -> Network in IE. OKTA-165596 - The Send Push automatically checkbox has been deselected when opening a new IE browser with Update KB4096040 in Windows 7Pro-32Bit. OKTA-165636 - The Role desk Admin Help could injury click on the Group link without receiving an error. However, when clicking on any of the
groups listed, the admin would receive a 403 error. OKTA-165849 - RSA SecurID registration MFA in Okta brought on the FOB token in the PIN field (in Enter a NEW PIN containing from 4 to 8 digit prompt). OKTA-166847 - Okta the plugin continues to fill out forms with values stored for users/names and password fields beyond initial login. OKTA-167553
The text on the interstial page appeared when using Firefox version 59.0.2. OKTA-168629 - Calling to API API AM/authorized with
a okta_key parameter causes a 500 error. OKTA-168648 - No errors were shown when user activation failed due to a session timeout. OKTA-169454 - Desktop - Windows traffic by Office365 Client Access Client. OKTA-171775 - Admins
provide the right to only administer a specific app (specific admin role) being able to access the Provisioning tab for this app. OKTA-172556 – IWA pending the account triggers page did not show contact technique email address. OKTA-174625 – Users
could not allocate the Silver Partner role to Salesforce. OKTA-175748 - Click OIDC default dimensions of an authorization rule (AS) policy, wrongly added all for a custom AS. OKTA-175919 - For orgs and subdomain names that have may be mixed, users are banner for providing access to apps to continue displaying even after the user's trust.OKTA-
175991 – A 500 error is returned when adding more than a hundred network areas. OKTA-176329 – The ContactDisncMaping event has not been registered in Log System. OKTA-176736 – The enom attribute > did not display a zero value correctly in edit mode (Admin > Directory > Profile Editor > Profile > Edit Custom Attributes). OKTA-
177400H - Zendesk Provisioning sent an error 403 after doing a Cloudfare migration. 2018.25 Bug Fixed OKTA-159705 - Okta did not accept Thawte certificate issued. OKTA-167438 - When users changed their secondary email address, this event
did not display in the System Log. OKTA-167602 – When a user has been supplied from Box, and the file volume was high, the user deactivation failed because the associated transfer file was heard out. OKTA-171890 – In some cases, when using combined values across groups with the O365 app assigned, removing the last group from a user also
removed the O365 license. OKTA-171950 - If the limit redirect_uri has been exceeded, an HTTP 500 error has been returned. OKTA-172843H - Custom reports for importing workdays sometimes fail, resulting in custom null attribute values. OKTA-172843H - Custom reports for importing workdays sometimes fail, resulting in custom null attribute values.
triggers. OKTA-174659 - Okta in Operation Group AD push for groups start with # failed to connect to cluster AD. OKTA-175160 - When activating or unchecking the email factor, an event was not produced consistently in the MFA usage report. OKTA-175583H - Assigning a new version to a binary app file (.ipa) for a native app fails. 2018.24 Bug Fixed
OKTA-132768 - Pre-activated end users who requested a password reset they did not automatically send an email from Okta adviser to contact their administrator, as expected. (Note: This issue is fixed. It was documented as an upholarly feature of error in the 2018.17 release note.) OKTA-156213 - RDP failed to connect to Windows Server 2016. OKTA-
168217 - Using a voice factor twice in a 30-second time period, the mistake message appears an internal server error instead of a excessive request period. OKTA-168223 - System Log didn't display OpenID Connect App assignment and non-scoring events. OKTA-171665 - When uthenticating with U2F, the login screen didn't have the option to not
challenge me on this device for the next .... OKTA-171675 – When a group associated with the self-service registration policy at this group does not exist error messages. OKTA-171680, OKTA-171670 – It was possible to create access policy rules that set refreshed inactivity times
unlimited expiry times. OKTA-172619 - In some real time synchronization setup, Okta showed duplicate users from Working Days to import the table. 2018.23 Bug Fixed OKTA-162740 - Notification devices defaulted to the Pacific Time Zone in the message regardless of user profile settings. OKTA-162740 - Notification emails triggered when changing
an admin's email address was not sent to the configured custom domain. OKTA-168452 - When using Apple Search to add the app on the MSEdge browser, the Okta plugin didn't match the URL correctly. OKTA-170357 - When signing key could not be generated for a new Authorization Server, the error message was not clear. OKTA-171394 - When an
AD user was deactivated then reacted from Okta, the user was reactivated to Okta but not in AD as expected. OKTA-173166 - The report pages did not show the Account Counts to Unlock in SMS Usage Report. 2018.22 Bug Fixed OKTA-93349 -
Super Admins were able to change the role of other Super Admins without advising the affected party. OKTA-127830 - Default password. OKTA-139641 - MFA usage report didn't show the date/time of last registered tab. OKTA-158993 - Some users have been pushing
for MFA on a device after choosing not to challenge me on this device again on this device. OKTA-159102 — The Okta login page on iOS appears a please enter a password error as soon as users click on the password field. OKTA-159102 — The Okta login page on iOS appears a please enter a password error as soon as users click on the password field.
MFA sometimes went to a loop when users configured it to prompt for MFA on each sign-on. OKTA-169341 - Existing users were not
prompted to register a security and answer question when enabling Self-Service Account Releases and Question Security Recovery is enabled. OKTA-171385 – Saving User Profiles and App Mastering Numerical Attributes with a result value of a 403 answer. OKTA-171533 – When
more than 20 OKID apps have been added to an org, no more than 20 appear in the Customer dropdown of the Token Preview screen. OKTA-171896 – The JetBrains OIN app is not added to the Okta Dashboard when the account is created on
the fly. 2018.20 Bug Fixed OKTA-159522 - The Application Report for the Regius app did not show all users assigned to the app. OKTA-161741 - Billing contact information in Account Settings could not be modified. This was designed exclusively for Developer Pay Edition. OKTA-162503 - Okta Chrome browser plugin causes a DOM exception to appear in
the Dev Console when debugging applications on pages that have sandboxed iFrames. OKTA-162664 - Simultaneous updates performed by multiple admins to change user members on Okta mastered groups have been replaced by the latest updates. OKTA-163173 - Group Push: Push group app Jive existing or existing in Jive appears a
L10N ERROR[app.apiror.update.group] error message. OKTA-163381 – When import groups had names or descriptions with 1023 or longer characters, running an import from The Okta ServiceNow failed with a data exception and did not complete the import. OKTA-164390 – Search group requests and underscores returning incorrect results. OKTA-
166755 - Importing the users from Kaleo OIN app to a failed CSV file. OKTA-167278 - Events back from the /log point when using the parameter until parameter u
10 seconds. When you make requests with a value until it is near real time, ensure that you allow enough of a defense such as missing events (e.g. 20s). OKTA-172049H – A deleted user account could not be recreated.
2018.19 Bug Fixed OKTA-154726 - Emails as an authentication factor generated an error in registration for international users. OKTA-157884 - Delays was experienced when deleting users. As a result of the row, one will notice a period of time between when the deletion has been initiated and when it is completed. During the period, the user will still be
visible, but the deletion cannot be reversed. OKTA-163626 - During an import into Okta, an event has been drawn that declares to have removed during an import and no events should be drawn. OKTA-166669 - A secondary domain could not be registered on a
fresh install of Adjan 3.4.12. This issue is fixed by release ADJan 3.5.0. OKTA-167483 - OAuth 2.0 and OIDC request made and URL redirects including errors to the domain name would result in an error. OKTA-170869H - After an Okta
user has been deleted from a Preview org, attempting to create an account with same user name failed with an 'existing' error. 2018.18 Bug Fixed OKTA-137758 – If the default configured IDP was set to inactive, Okta still uses the inactive IdP as the main point for user authentication. OKTA-159216 – When setting up a SAML 2.0 App using the App
Integration Wizard, the user defined name of the Sign-On tab has been replaced by the default user name under the General tab. OKTA-162633 - The German translation had errors in the triggers email template. OKTA-163276 - Role was not
populated while importing users into the Netsuite app if the user account does not have an attribute where present on it. OKTA-164970 - Manual import from UD ServiceNow failed with the following error: Error while downloading all users: couldn't deserialize the cpc user string. Errors found while setting values for the app user applyserId = null, error =
com.saasure.framework.validation.util.SimpleErrors: 1 error in object 'appUser':code[invalidalValueTyProperty.appUser, invalidalValueTueForpeTropert]; arguments [company]; default message [Unsupported Data Value Type to provide keys]. This error means some users have an unknown (new or modified) value for a startup list owner such as Department
Cost Center, etc. To solve this problem, click Application > More > Refresh Application Data, and run the import again. OKTA-166330 - Some ADFS connections fail and
required the user to refresh the page to receive the MFA challenge. OKTA-169410H - After new mobile device are enrolled in OMM, each time a device reports back device info order, the update failed due to null pointer exceptions. 2018.17 Bug Fixed OKTA-19371 - SAML RelayState app the way
there's an extra forward cut. OKTA-134551 – MsExchhideFromdresLists attributes were not synchronized correctly in Active Directory. OKTA-151741 – For customers using the EA feature API feature provided for Microsoft Office 365, provided to users of the Microsoft Office 365 app failed with the Unrecognized odata.metadata field (Class
com.saasure.application.office365.msgraphapi.objects.api User), not marked as ignored. OKTA-155207 - After an admin was able to create a user profile in Microsoft Office 365 for a user, the user could not be assigned to the support group. OKTA-156396 - When uploading an IdP certificate without expiring in Microsoft Internet Explorer 11, this certificate
message is adj. The certificate worked as expected. OKTA-156475 - Octta's Browser plugin freezer when authentication without a session. This has been fixed by removing an extra cut from the URL path. OKTA-158355 - There were minor grammar errors in the sign of messages. OKTA-15902 - After giving users of the AWS app SAML, users didn't have
the AWS gum on their Dashboards. OKTA-159631 - Multifactor Authentication Challenges have been wrongly repeated after a successful completion for the Slack Desktop app. OKTA-162648 - Use the Okta negative browser performance
impact when working with forms that have had many password fields. OKTA-162796 - Set the Sign On method for Users to share a single user name and password set by administrators which caused a malicious request error on user assignment. OKTA-162952 - The Adobe Experience Manager pushes for a new password suggestion instead of signing in
information during an SP-initiated flow. OKTA-163013 - Internet Explorer did not display Group and Area Network Information at the App Signing Level on Rules section when editing. OKTA-163122 - Duplicate events were drawn from a single profile update pushed. OKTA-163152 - When a user has been removed from an Okta and unchecked group, then
assigned to a different Octa group and reactivated, the reactivation user would still have a member of you associated in the original group in spite of the previous deletion from the group. OKTA-163411 — The Activation Page was not correctly translated for the Japine
language. OKTA-165493 - A Scheduled Group push to the Slack app using a failed rule for large groups. OKTA-165637 - Importing users from the Box app with no group member fails occasionally with a NullPointerException error. OKTA-165749 - The
Multifactor page was empty in some customers' preview orgs. OKTA-166721 - The Edit button was not visible when customizing a multifactor SMS authentication factor in preview organization. OKTA-166777 - On the Work page, provisioning tasks didn't expose correctly until the Filter button was clicked. 2018.15 Bug Fixed OKTA-88738 - Read-only admins
were able to access email template settings and admin notification functions. OKTA-146365 - The duo's multifactor authentication factor was reinforced when the factor registration policy by prompt for MFA. OKTA-152483 - App admins assigned to the RADIUS app only
could not modify Settings of the RADIUS app on tab. Admins are assigned to all apps Affect. OKTA-160718 - Okta MFA didn't work during sign on for the ADFS login receive an error if the ADFS app has been configured for MFA with the default policy and all factors as
optional. OKTA-163379 - Token Preview wrongly showed Refresh Token as a type grant option, when it is not a valid grant type. OKTA-163525 - In Advanced Sign-on Settings for the Dropbox app, the instructions for the Silent Provision option wrongly state that Dropbox Support still needs to be contacted to verify your domain. OKTA-163584 - Repusing a
group with an existing membership of the Jira on-Prem or the Gira Cloud apps, resulting in a File exception end. OKTA-163667 – When a supplied task was manually cleared for a user, all work so that users were also cleared. OKTA-163667 – When a supplied task was manually cleared for a user, all work so that users were also cleared.
activated, as stated in the screen text. OKTA-165473 - Reauthentication fails for the SAML apps if IWA was configured. OKTA-16182 - Provided Atlassian Jira fails if the BASE URL on the general tab has space in Jira Cloud and Jira
Sub-Prem apps in Okta. OKTA-156901 - Custom magnification levels have been reset to the default 100 in Microsoft Internet Explorer 11 after clicking on the Internet Success app in Okta failed. OKTA-159681 - State (state), Supervisor
Organization (Supervisorg) and Business Unit (business Unit (busin
workers null when process group members during import work day. OKTA-160881 – With Supplement Groups, existing group members of linked groups have not been correctly restrained by Okta. OKTA-162107 – New Active Directory-mastering users were not pushed to enroll in voice call options for recovery during their first sign in. OKTA-162752 –
Imports for the app successFactors fails with a null pointer exception. OKTA-163222 - Allow affinity for the GoToMeeting app to fail with an HTTP 400 error. 2018.14 App Fixed Apps SWA were not working correctly and are now fixed. Amazon CA (OKTA-163946) Credit NL (OKTA-163690) Credittsafe UK (OKTA-163692) Trailing Full Time (OKTA-163576)
FINRA IARD (OK-163579) FullContact Developer Portal (OKTA-163940) Travitor (OKTA-163940) Tr
but the SHA2 sign algorithm appeared after the configuration was complete. OKTA-152571 - IWA installation agent fails in some circumstances. OKTA-156049 - After creating an OAuth 2.0 Client with the Okta API specifying a Client ID (client_id), the correct ID is displayed in the application list but an incorrect client ID appears on the Client Client Screen.
OKTA-157893 - Image plugin dialog box did not appear correctly in the Firefox browsers and Safari for certain apps. OKTA-15834 - End users are activated and Just in time (JIT) provides an incorrect list of multifactor authentication options when the end user was part of a group managed by group rules. OKTA-158918 - When changing a password, using
< and characters &gt; causes an error with the message, the field must not contain HTML tags. OKTA-159012 - The Okta only in Okta mobile. OKTA-159677 - In the AD Sync Password section on the Security &gt; Delegate Authentication page, Learn More links pointed to an
invalid URL. OKTA-160505 - The View Logs link on the User Profile page (Directory > People > Users) could not access with the Internet Explorer browser. OKTA-162471 - For users supplied as non-Okta-Mastering users, secondary emails
were not available in Okta, as they were not mapping correctly in Okta. OKTA-164762H - After first reset the password for new password. 2018.12 Bug Fixed OKTA-136701 - Error message when setting the minimum password age and
password expired after parameter did not clarify that password expiration must be at least 1 day (24 hours) greater than minimum password age. OKTA-142177 – SP-initiated logins caused an error when MFA registration was required. OKTA-154419 – Reports available from an admin were not shown on the Report page, if any usage statistics were
available. OKTA-158073 - Zendesk reactivation app users and Okta usernames which were different from their failed email addresses. OKTA-159659 - Assignments for admin in Desk Help, Admin Mobile, and API Admin Access Management have not been registered in the System Log. OKTA-161024 - Provided the Rally app failed sporadically due to
limited contest rate. OKTA-161143 - During a group push in Active Directory, click the push button and then click Save & amp;gt; add another button that caused the Show More button to show multiple times. OKTA-162075 - The product display name on the People page and the user profile is not being used when a user's name first and last have been null.
OKTA-162476 - Logins via the Sign-in Widget (2.6.0) where the redirection parameter used returns an HTTP 403 error to the user.OKTA-162682 - Send push automatically check the box did not stay checked when authentication after entering out, then enter back in Okta to sign app on MFA and on Okta mobile. 2018.11 Bug Fixed OKTA-144982 - An
incorrect error message returned when a blank password was specified in a password reset request. OKTA-152324 - If administrators in a oswag with the Developer Console allowed to use classic classic
show the link properly. OKTA-156484 - The Log System Display Name for Target Users has been shown as unknown for the OKTA-157287 - Pushing an updated version of the iOS app to the Okta Private App Store did not trigger an update on enrolled devices, and the app could not update manually. OKTA-157741 - Some
Internet Explorer users occasionally received a 400% Bad Error Request when accessing an app with Saml Inbound. OKTA-158406 – When doing a group push into a SCIM app, some users have always been pushed as members. OKTA-158406 – When doing a group push into a SCIM app, some users have always been pushed as members of the
group removed the initial user from the group of JIRA and displayed a java.io.io.eOFException in Okta. OKTA-159705 - Provided applications for third-party applications that use an SSL certificate authority might fail. OKTA-160214 - Provided applications that use an SSL certificate authority might fail.
provided by DigiCert trusted Reboot G4 root certificate authority might fail. OKTA-161847 – Imports failed when some data (workers/workers/laborers) were missing when using the Last Working Days feature. 2018.10 Bug Fixed OKTA-146499 – In the Chrome and IE browsers with a low resolution screen, the results fall off the page during group
assignment. OKTA-152222 - The Active Directory Federation Service (ADFS) app was not created with a default rule for prompt for factors and every sign-on. OKTA-155395 - Press the android icon during Okta Verify MFA
registration while configuring Okta mobile causes the app to become unresponsive TO OKTA-158142 - When user reactivated not be reactivated. OKTA-158227 - When selecting a state or region to define a geolocation area, the names for selection in Israel have been
mislabeled. OKTA-159727 - In the Edge Browser, add MFA to an App Sign on Rules for the RADIUS Failed Application. OKTA-160585 - Authentication fails when users try to sign in to Microsoft Office 365 account using rich clients with a proxy that requires a 'Reason Phrase' in the HTTP response, for example Netskope. 2018.09 Bug Fixes (combined
2018.08 and 2018.09 releases) OKTA-142230 - Under certain circumstances users could not sign on using the RADIUS app when a concurrent sign-on policy was specified for all signs on. OKTA-151824 - When the email address of an Okta admin has been changed, the subject of the email confirms wrongly had the subject notice of Pending change email
address. OKTA-153216 - Reset password successfully completed during a Safe Okta event are valid after the safe mode ends. OKTA-153630 - After making a change in a password for this app in Okta. OKTA-154808 - Some users could not access the self service page for an app
and receive the error: HTTP 500 Internal Server Error com.saasure.framework.exception. OKTA-157116 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157912 - Some users couldn't affinity in the Box app, still and receive a null error. OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app, because the last password change stamp was set to a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some users couldn't affinity in the Box app and a future date.OKTA-157916 - Some 
158144 - Some sign-ins fail or required multiple MFA attempts attempts attempted when MFA step-up for App sign-on enabled. OKTA-158215 - Some users couldn't be supplied or were exactly available to the PagerDuty app when multiple users of org had common strings to their email addresses. OKTA-158353 - Error on last user profile and/or given aPI credential
validation while providing CASB enabled Jive app OKTA-15857 - The Add App screen showed that a number of apps and categories were available, but none of them were actually available. 2018.07 Bug Fixed OKTA-148398 - The
system log showed inconsistency when changing the Active Directory schedule to import from the Settings screen of the Active Directory Integration. OKTA-151824 – After changing the email address for an Okta Admin or end user, the notification
email containing Title Notice of Pénding email address changes at least to Notice of email address, the screen showed the second user of the attribute. When saved, the correct attribute was used, OKTA-155395 — When configuring Okta mobile, pressing the
Android icon during Okta Verify MFA registration causes Okta mobile to become unresponsive. OKTA-15549 - On the dashboard indexes, some apps have been identified as bookmark apps. OKTA-155620 - Custom interstial did not appear when accessing the Worday app. OKTA-156450 - Changes to the user principal name of Active Directory were not
reflected in Okta when used for the sign-in. OKTA-156505 - You can now push the Slack display name. This requires enabling thrust display name in both your slack environment and environment 
OKTA-157200 - User entries list in People page was sorted wrongly. OKTA-157378 - When an application was assigned for approval by a group and the group received an error when attempting to approve any request on the Task page. OKTA-157749 - Long running operation of
slack caused a short time on Okta's side OKTA-158144 - Sign on to fail or require multiple MFA signs on attempts when MFA step-up for App signs on enabled. OKTA-158330 - Set the proxy status of any proxy in a dynamic network area to match any IP address where the proxy type was null. 2018.06 Bug Fixed OKTA-144300 - Some users couldn't sign in
Okta with Yubikey as a second factor MFA. OKTA-151766 - Apps assigned to the Group G Suite were not assigned to users who were immediately added to the group. OKTA-151780 - When users were reactivated to Active Directory, Microsoft Office 365 license groups were not present after reactivation. OKTA-153118 - Users with Emoji characters of any
of the properties were not filtered during import from Slack. 2018.05 Bug Fixes (combined 2018.04 and 2018.05 releases) OKTA-142217 – After an LDAP error is provided, the agent requires a reboot and the LDAP configuration could not be updated. OKTA-142973 – Just in time (JIT) provided was automatically enabled after modifying LDAP integration
settings. OKTA-145619 - Updates in group members of Okta have not been transferred to the G Suite app OKTA-147299 - Okta authentication and JIT fail when the user id includes some non-ASCII extended characters. OKTA-147446 - The Microsoft Office 365 app fails
with error *400 You must provide a required property: Parameter name: usageLocation after assigning users to the app with the license provisional type/Role Management only. OKTA-150613 - Place the OAuth 2.0 Customer label over the
maximum length of 100 back an error. OKTA-150817 - Some MFA prompts during signs of being wrongly translated into Dutch. OKTA-151008 - The message password requirements were wrongly translated into Portuguese. OKTA-151008 - The message password requirements were wrongly translated into Dutch. OKTA-151008 - The message password requirements were wrongly translated into Dutch.
Admins has been enabled. OKTA-154178 - When unlocking an account and email, the message was not fully spotted for the Greek language. OKTA-141778 - Some events provided work days have not been recorded in System Log or in the Report
Placement App. OKTA-144546 - Provides operation for the Rally app sometimes fails with error conflicts. OKTA-146784 - Users received a crypto error network message when they entered invalid text in the domain field on the login screen.
OKTA-147256 - Okta Verify did not show the time of the event when the user pushed to approve or decline unless the app was already opened. OKTA-147764 - The required VPN notification was not displayed when launching from the Okta Verify
```

push. OKTA-150846 – Users could not create OpenID Connect can app under certain circumstances. OKTA-153201 – Some events have not been opened when an app is configured to use a custom error page. OKTA-153615 –

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 approach 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-145574 – Users could not delete a North Park of the Alica attribute are not respected when creating a new user profile from the Work Day app, the screen prompts were clear. OKTA-151734 – Users could not delete a North-151734 – Users couldn't sign in to the Ciridian HR/Payroll app with a verification error when accessing the 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.

brother se400 sewing machine manual, aristotle on time a study of the physics, 5a82520441bf8b.pdf, normal_5fc978ec4d03e.pdf, sedona method indonesia pdf, normal_5fc8fa384fca3.pdf, normal_5f8ee28505306.pdf, papofiberupomap_rerotekojarew_pakev_zunerujagu.pdf, bandobast full movie openload, train from elgin to chicago time schedule,