Oracle® Cloud

What's New for Oracle Identity Cloud Service

Release 22.4.92

E81008-76

March 2025

What's New for Oracle Identity Cloud Service

When new and changed features become available, Oracle Identity Cloud Service instances are upgraded in the data centers where Oracle Cloud services are hosted. Here's an overview of new features and enhancements added recently to improve your Oracle Identity Cloud Service experience.

This guide documents the complete set of new and changed features for Oracle Identity Cloud Service. Your localized version of Oracle Identity Cloud Service might contain a subset of these features. Therefore, you might find features in this documentation that are not available in your localized version of Oracle Identity Cloud Service.

Service Change Announcement

Service Change	The Oracle Identity Cloud Service **Audit Events APIs** are deprecated and some report templates will return data for up to 14 days.
Date Announced	May 24, 2023
Date in Effect	May 2025
Details	Starting May 2025, the Oracle Identity Cloud Service Audit Events APIs will no longer be available. Out of the box reports will continue to be available, but they will be limited to the last 14 days of data. The following AuditEvents APIs are deprecated: • AuditEvents The following Oracle Identity Cloud Service report templates in the reports APIs will continue to be supported with limited data (14 days):

	• User Login • System Log • Sync Failure • Suspicious Events • AppRole Assignment • Application Access
Does this impact me?	If you are currently using Oracle Identity Cloud Service APIs for AuditEvents, continue to do so until your Identity Cloud Service instances are migrated to be identity domains.
What do I need to do?	After migration to identity domains, use the OCI Audit APIs.

Application Integration

To find out about the new applications and features that have been added to the Oracle Identity Cloud Service Application Catalog, see the *What's New* section of the *Oracle Identity Cloud Service - Application Catalog*.

Topics:

October 2024

Category	Feature	Description
E-Business Suite Asserter	Certified Components	The supported WebLogic Service versions are now: Oracle WebLogic Server 12c (12.1.3 and 12.2) Oracle WebLogic Server 14c (14.1.1)

Release 24.2.174 — May 2024

Category	Feature	Description
Security	MFA Access for Identity Cloud Service Consoles	**Default MFA Security for Identity Domains My Profile and My Apps Pages** MFA enrollment and authentication is enabled by default for My Profile and My Apps access for all users. Default MFA security means that: • The following phishing resistant MFA factors are enabled in the **Default Sign-On Policy**: – Mobile app push notification – Mobile app passcode – Fast ID Online (FIDO) **Important**: At least one of these phishing resistant factors must be enabled. • Users accessing My Profile and My Apps pages will be challenged for MFA, even if they've already authenticated with MFA during their current session. • Any users who aren't enrolled in MFA, will be forced to enroll. My Profile and My Apps example URL: `<domain_URL>/ui/v1/myconsole` **Disabling Default MFA Access** We don't recommend that you disable the default MFA security feature. If you want to disable this feature, then Oracle support must disable it for you. See Getting Help and Contacting Support to contact Oracle support.

Release 23.4.146 — December 2023

Category	Feature	Description
Security	MFA Access for Identity Cloud Service Consoles	MFA access to the My Profile, My Apps, and the Identity Cloud Service console is now enforced by default when all the below criteria are met: • The **Default Sign-On Policy** is NOT configured for MFA • The user is enrolled in at-least one MFA factor • The user is trying to access the My Profile, My Apps, or the Identity Cloud Service console Example URLs: • My Profile and My Apps: `idcs-xxx/ui/v1/myconsole` • Identity Cloud Service Admin console: `idcs-xxx/ui/v1/adminconsole` Where `idcs-xxx` is equal to your identity domain URL or Identity Cloud Service stripe base URL. If a user is already enrolled in MFA and tries to access the My Profile, My Apps, or the Identity Cloud Service console even if the **Default Sign-On Policy** is not configured for MFA, the user will be prompted for MFA. **Note:** This security posture doesn't enforce new MFA enrollment. **Disabling Default MFA Access** We don’t recommend that you disable this default security feature. To disable this feature, update an SSO setting using the API. Use the following high-level steps as a guide. 1. Using cURL, GET `idcs-xxx/admin/v1/SsoSettings/SsoSettings` using the IDA-scoped token. 2. Backup your instance in case rollback is required. 3. Find the `idcsConsoleMfaEnforcementEnabled` attribute (in the payload from step 1). Set `idcsConsoleMfaEnforcementEnabled=false` and users aren't prompted for MFA unless the **Default Sign-On Policy** is configured for MFA. 4. Using cURL, PUT `idcs-xxx/admin/v1/SsoSettings/SsoSettings` to update the attribute using the payload from step 3 with the IDA-scoped token.

Release 22.4.96 — May 2023

Service Change Announcement- Deprecated Endpoints

Category	Feature	Description
REST API	Deprecated Endpoints	Starting **May 24, 2024**, the Identity Cloud Service APIs for **AuditEvents** and certain reports templates in the **Reports APIs** no longer work with Identity Cloud Service. See Service Change Announcement.

Release 22.4.92 — January 2023

Generally Available Features

Category	Feature	Description
Security	App Gateway	New RFC limits could cause errors. These response error messages will contain a message similar to: `400 Bad Request: invalid header value`. See My Response Error Message Contains: 400 Bad Request: invalid header value.
Authentication	Linux Authentication	We now support Oracle Enterprise Linux 8 for the Linux Pluggable Authentication Module (PAM). See Certified Components.

Release 22.3.77 — November 2022

Generally Available Features

Category	Feature	Description
Getting Started	API rate limits	Information about the API rate limits for Foundation license types and Standard license types (Enterprise users and Consumer users). See API Rate Limits.
Important: Explicit Trust Scopes	Correction to the scope parameter.	The scope to use when specifying multiple scopes belonging to different resources in a single Authorization request or token request was previously documented as: `urn:opc:resource:multiscopes`. This is incorrect. Use `urn:opc:resource:multiresourcescope` instead.

Release 22.3.77 — September 2022

Generally Available Features

Category	Feature	Description
Security	Cross-Origin Resource Sharing (CORS) settings for Cloud Gate	Cross-Origin Resource Sharing (CORS) is a header-based protocol that allows JavaScript to make requests on your behalf to access resources in another domain. Configure Cloud Gate so that it enables CORS and enforces CORS settings for Cloud Gate running in App Gateway. If you need to configure Cloud Gate CORS settings in Oracle Identity Cloud Service, then you use the Oracle Identity Cloud Service REST API. See Configuring Cloud Gate CORS Settings in Oracle Identity Cloud Service.

Release 22.3.77 — August 2022

Generally Available Features

Category	Feature	Description
JIT Provisioning	Group Mappings	Two new properties have been added for group mappings: • `jitUserProvGroupMappingMode` - String property that controls how the groups in the IdP are mapped to those in the Identity Cloud Service tenant. Valid values are: – `explicit` - IdP groups are explicitly mapped to the groups in the Identity Cloud Service tenant via the configuration property `jitUserProvGroupMappings`. – `implicit` - Group names in the SAML assertion must match group names in the Identity Cloud Service tenant. `"jitUserProvGroupMappingMode": "explicit",` • `jitUserProvGroupMappings` - Array of mappings between groups in the IdP assertion and groups in the Identity Cloud Service tenant. Every object in the array represents a mapping between an IdP group and an Oracle Identity Cloud Service group.

Category	Feature	Description
REST API	New REST API attribute for users to change their own profile attributes.	Users can now use the API to change their profile attributes (for example, an email address or a password) by setting the `allowSelfChange` attribute to `true` in the request payload or URL query string parameter. By default, this attribute is set to `false`. Set `"allowSelfChange": true` in the request payload for the following operations: • Users (PATCH, REPLACE) • UserCapabilityChanger (REPLACE) • UserLockedStateChanger (CREATE) • UserPasswordChanger (REPLACE) • UserPasswordResetter (REPLACE) • UserStateChanger (PATCH) • UserStatusChanger (REPLACE) • UserDbCredentials (CREATE) • ApiKeys (CREATE, UPDATE) • AuthTokens (CREATE, UPDATE) • CustomerSecretKeys (CREATE, UPDATE) • OAuth2ClientCredentials (CREATE, UPDATE) • SmtpCredentials (CREATE, UPDATE) • SupportAccounts (CREATE) Example PUT on `/UserCapabilitiesChanger/<id>{ "canUseApiKeys": true, "canUseAuthTokens": false, "canUseConsolePassword": true, "canUseCustomerSecretKeys": true, "canUseOAuth2ClientCredentials": true, "canUseSmtpCredentials": true, "canUseDbCredentials": true, "urn:ietf:params:scim:schemas:oracle:idcs:extension:selfChange:User:allowSelfChange": true, "schemas": ["urn:ietf:params:scim:schemas:oracle:idcs:UserCapabilitiesChanger"] }` Set `"allowSelfChange=true"` as a URL query string parameter for the DELETE operation on the following APIs. **Note:** You must set `allowSelfChange=true` as a URL query string parameter for DELETE operations. • UserDbCredentials (DELETE) • ApiKeys (DELETE) • AuthTokens (DELETE) • CustomerSecretKeys (DELETE) • OAuth2ClientCredentials (DELETE) • SmtpCredentials (DELETE)

Category	Feature	Description
		• SupportAccounts (DELETE) Example POST on / `CustomerSecretKeys{ "diplayName": "Alice Customer Secret Key", "description": "Alice's Customer Secret Key", "user": { "value": "9d7e8d1a4f224fcdae6ac550d0cbdc47" } , "urn:ietf:params:scim:schemas:oracle:idcs:extension:selfChange:User:allowSelfChange": true, "schemas": ["urn:ietf:params:scim:schemas:oracle:idcs:customerSecretKey"] }`

Category	Feature	Description
Explicit Trust Scopes	A new option is available for using the Explicit trust scopes from multiple resources.	The `Explicit` trust scope defines trust scope for only those services where an explicit association between the client and the target service exists. You can specify multiple scopes belonging to different resources in a single Authorization request or token request and obtain multiple access tokens in return with each of them containing the scopes for each resource. To use this feature: • You must specify the newly defined scope, `urn:opc:resource:multiresourcescope` in the Authorization request or token request. Token requests will fail if multiple scopes belonging to different resources are specified without this scope. • The OAuth Client must be able to parse the token response that includes multiple access tokens and use each token to access each resource service. **Note:** You can use this feature with all the grant types except for the Implicit flow. See Implicit Grant Type. See Using the Explicit (Specific) Trust Scope for more information about the explicit trust scopes. **Request and Response Examples** The request and response examples show the client credentials flow using a fully-qualified scope. **Request Example** `https://yourtenant.identity.oraclecloud.com/oauth2/v1/authorize?client_id=<client-id>&response_type=code&redirect_uri=<redirect-url>&`

Category	Feature	Description
		scope=http://abccorp.com/scope1 http://123corp.com/scope1 openid urn:opc:resource:multiresourcescope curl -i -H 'Authorization: Basic MzgzZTU4Z….NTM3YjFm' \ --request POST 'https://yourtenant.identity.oraclecloud.com/oauth2/v1/token' \ -d 'grant_type=authorization_code' \ -d 'code=AgAgYjc1MzgzNWM2NGQxNDA5… YcxU_XdtfLWXUp1Vn4a5uIHiOn4=' curl -i -H 'Authorization: Basic MzgzZTU4Z….NTM3YjFm' \ --request POST 'https://yourtenant.identity.oraclecloud.com/oauth2/v1/token' \ -d 'grant_type=client_credentials' \ -d 'scope=http://abccorp.com/scope1 http://123corp.com/scope1 urn:opc:resource:multiresourcescope**Response Example** { "tokenResponses": [{ "access_token": "eyJ4NXQjUzI1NiI6InZBV3RzNEo1clE1Z.. ...1iZDc2NjFjMWJiZjA0OGNhOTkyMWNlN2Q 4MThkNDY0YSIsImp0aSI6Ijg53ZFOT2FxyZY jocCnm1b1w", "token_type": "Bearer", "expires_in": 3600 }, { "access_token": "eyJ4NXQjUzI1NiI6InZBV3RzNEo1clE1Z.. ...HplcmtUNjdsU19SjZlYjc5ZDgzMTVhYjQ 0ODBiNDlkMjU3NzdkZWMzMDE2In0.k4QShMb O5aPGmYyKo", "token_type": "Bearer", "expires_in": 3000 }], "id_token": "eyJ4NXQjUzI1NiI6InZBV3RzNEo1clE1ZHp lc.....mtUNjdsU19SYjhQTWoYDSVhTUmDl8 zK3a9vk7cowIW2hr3smwtcsvfsbrewwtbnCr Gerp7v4CUcVYlSw" }

Release 22.2.68 — June 2022

Generally Available Features

Category	Feature	Description
Patch for high availability users of App Gateway	Cloud Gate has updated Block Cipher, which changes how data is encrypted by Cloud Gate.	To ensure that you can upgrade without service interruptions, the change is being rolled out over three patch releases. See Upgrade Path for High Availability Deployments.

Release 22.1.49 — January 2022

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
Identity Providers	Configuration change for the `redirectUrl` for social identity providers. **Note:** Each social identity provider calls redirect URLs by a different name. For example, Twitter calls them "callback URLs."	For social identity providers created before release 22.1.49, ensure that the `redirectUrl` doesn't contain port number `:443`. If it does, update the existing URL to remove the port number or add a new URL without the port number to the identity provider application using the external provider developers' website. For example, if your configuration looks like the following: `https://<IDCS tenant base URL>:443/oauth2/v1/social/callback` change it to: `https://<IDCS tenant base URL>/oauth2/v1/social/callback`. See the *Prerequisites* section for Adding a Social Identity Provider.
REST API	SAML Just-In-Time Provisioning	An new Boolean property has been added: `jitUserProvIgnoreErrorOnAbsentGroups` This new property determines the action to take when the incoming assertion attribute specifies a group that does not exist in the Oracle Identity Cloud Service tenant. If this property is `true`, then the missing group is ignored, and the user is created. If this property is `false`, and a nonexistent group is specified, user creation will fail. See Configuring SAML JIT Provisioning.

Release 21.4.38 — December 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
REST API	SAML Assertion Grant type.	Added new instruction regarding the recipient value in SAML assertions. See Example Authorization Flow for the Assertion Grant Type.
REST API	Requesting group memberships.	There is a new upper threshold limit when requesting group memberships. See the *Example* sections of the following operations for instructions regarding the new limit. • POST/.search on Group • GET on Groups
REST API	Client and user assertions.	New instructions added for generating user and client assertions using a signing key and sample output and sample decoding examples from the assertion java code. See Client/User JWT Assertion.
Pricing Models	Linux-PAM Module was added as a Standard feature.	See About Oracle Identity Cloud Service Pricing Models .

Release 21.4.38 — October 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description

Security	SAML Just-In-Time Provisioning	The REST API instructions for Configuring SAML JIT Provisioning have been updated to include instructions regarding the default behavior for the `jitUserProvCreateUserEnabled` attribute.
		The JSON Example for the `attributeMappings` configuration was also updated:
		`{ "idcsAttributeName": "urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:isFederatedUser", "managedObjectAttributeName": "#toBoolean(\"true\")" },`
		has been changed to
		`{ "idcsAttributeName": "urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:isFederatedUser", "managedObjectAttributeName": "#toBoolean(\"false\")" },`
		See Configuring SAML JIT Provisioning.

REST API	Header parameters	The `x-resource-identity-domain-name` header parameter has been deprecated. References to it have been removed.
Integrations	AD Bridge	A new troubleshooting and FAQs section was added for Active Directory (AD) Bridge. See Troubleshooting and FAQ for Active Directory (AD) Bridge.

Release 21.4.33 — October 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
Security	Delegated Authentication	Updated descriptions for the password options available when deactivating Delegated Authentication. • Send a Password Reset Notification (recommended) • Create a Password See Deactivate Delegated Authentication.

Category	Feature	Description
Security	Revoke Refresh Token	The following new request examples for revoking a refresh token were added. • Basic `<client_id:client_secret>` and payload is `token=<refresh_token>` • Basic `<client_id:client_secret>` and payload is `user_id=<user guid>` • Bearer `<administrator access token>` and payload is `user_id=<user guid>` See Revoke Refresh Token.
Security	Custom Sign-In application	New instructions explaining how to configure the Custom Sign-In application for FIDO integration. See section *Configure the Custom Sign-In Application for FIDO Integration* in `idm-samples/idcs-authn-api-signin-app/README.md`.
Auditing	Reports	Reporting documentation updated to reflect that the System Log report has been renamed the Audit Log report. A list of Audit Log events and examples of using the Audit Log were also added. See Audit Log Report.
Licensing	User and Group Management - Specifically, granting user access to various applications by assigning users to the applications directly, or by assigning users to groups and groups to applications.	This User and Group Management feature was not listed in the Foundation tier. That has been corrected. See About Oracle Identity Cloud Service Pricing Models .
Licensing	Linux-PAM Module	Linux-PAM Module has been added to the pricing models. Linux-PAM Module is a Standard tier feature. See About Oracle Identity Cloud Service Pricing Models .

Release 21.3.2 — August 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
Security	New algorithm for FIDO authentication	In addition to the ES256 (default) algorithm, Oracle Identity Cloud Service now certifies the RS256 algorithm as well. **Note:** The RS256 algorithm is mandatory for Windows Hello FIDO authentication. See Configure FIDO Security.
Audit Logs	Device fingerprinting	Enhancements to device fingerprints: • UserDevices REST API endpoint returns details about the devices with unique device fingerprints have been used to login by a user. • You can search for device fingerprints in audit logs. • The device fingerprint is available as a claim in ID tokens and Access tokens. See Use Device Fingerprints.

Release 21.3.1 — July 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
App Gateway	App Gateway Server	A new step has been added to check the OVA version being installed when configuring the App Gateway Server. See Configure the App Gateway Server.
Licensing	SSO and user sync	The "SSO for Oracle Cloud Services" and "Generic SCIM APP Template" pricing model descriptions were updated to specify that SSO and syncing users between two Oracle Identity Cloud Service instances is included in the Foundation pricing tier. See About Oracle Identity Cloud Service Pricing Models .
Migrating users	Creating the CSV import file	The task did not specify the required column headers for CSV import. Required headers were added to the documentation. See Migrate Users.

Category	Feature	Description
Applications	Application roles membership import	Text was added to clarify that importing application roles imports application role memberships only. The application roles must already exist in Oracle Identity Cloud Service. If the application roles don't exist, you will receive an error for the membership import for that application role. See Import Users and Groups for Oracle Application Roles and Create and Prepare a Comma-Separated Value File.
Authentication	TLS Client Authentication grant type	The TLS Client Authentication grant type documentation was in the Add a Mobile Application topic. This was incorrect. TLS Client Authentication" grant type was added to the correct topic, Add a Confidential Application. See Add a Confidential Application.
App Catalog	FA Rel. 13	Updated configuration steps for the new template. See Oracle Fusion Applications Release 13.
MS AD Bridge	AD Credentials	Use the AD Bridge client to change administrator credentials or change to a different administrator. See Change Administrator Account Credentials for AD Bridge.
Reports	Diagnostics data	There's a new option to identify the resources returned in the diagnostic log. See Run the Diagnostic Data Report.

Release 21.2.2 — May 2021

Standard License Tier Features

To learn more about Standard License Tier features, see Standard License Tier Features for Oracle Identity Cloud Service.

Generally Available Features

Category	Feature	Description
Security	Network Perimeters/ Sign-on Policies	For applications on OCI-C, where Oracle Identity Cloud Service is the Identity Provider, the following OCI Service Gateway IP range must be added to the network perimeter used by Sign-On policy: OCI Service Gateway IP CIDR 240.0.0.0/4. See Add a Sign-On Policy.

Category	Feature	Description
App Gateway	Updated OVA instructions	Added updated steps for App Gateway OVA 20.4.1-4.0.0 and higher. See • Configure the App Gateway Server (in SSL Mode on Port 1024 or Lower) • Configure the App Gateway Server (in the user interface)
Licensing	Standard Tier License features	You no longer need to file a Service Request to enable features for the Standard Tier License. See Standard License Tier Features for Oracle Identity Cloud Service.

Release 21.2.1 — April 2021

Service Request Features

Service Request features must be enabled by Oracle. To learn about the features that Oracle must enable for you and how to enable them, see Service Request Features for Oracle Identity Cloud Service.

Category	Feature	Description
Audit Logs	Device fingerprinting	Enable device fingerprinting using cookies to uniquely identify user systems. See Use Device Fingerprints.

Generally Available Features

Category	Feature	Description
Active Directory (AD) Bridge	New option to quit an unresponsive AD Bridge	You can now quit an AD Bridge sync that is taking longer than expected. After you have quit your current AD Bridge sync, you can then start another AD Bridge sync. See Quit an Unresponsive Microsoft Active Directory (AD) Bridge Sync.
Active Directory (AD) Bridge	Locate a new Domain Controller	If the domain controller you have configured changes or you're having domain controller connectivity issues (for example, an LDAP Server Unavailable error), use the AD Bridge client to locate another domain controller to use. See Locate a New Domain Controller.

Category	Feature	Description
Active Directory (AD) Bridge	New administrator notifications	You can now send an administrator a notification when an AD Bridge sync has succeeded as well as when an AD Bridge sync has failed. See About Administrator Notifications.

Other Documentation Changes

Feature	Link
Accessing SAML metadata. Added instructions explaining how to download the SAML metadata for Active Directory Federation Services (ADFS) using a URL.	See Access SAML Metadata.
Corrected the NameID Value field description. The description incorrectly referenced using a "regular expression" when specifying a NameID value. Instead you must use an Oracle Identity Cloud Service Policy Engine Path Expression. The description was updated with examples.	See Add a SAML Application.
Updates to the Generic Scripting Connector app catalog instructions. The instructions for setting up for LCM changes for dynamic attributes have been updated including the example request body.	See Setup for LCM Changes for Dynamic Attribute.
Added a section that describes the RADIUS Proxy mapping requirements when setting up RADIUS Proxy.	See Setup RADIUS Proxy.
Added more details to the instructions for configuring passwordless authentication.	See Configure Passwordless Authentication for User Accounts.

Release 21.1.3 — March 2021

Service Request Features

Service Request features must be enabled by Oracle. To learn about the features that Oracle must enable for you and how to enable them, see Service Request Features for Oracle Identity Cloud Service.

Category	Feature	Description
Security	ID Token Encryption	Use content encryption algorithms so that id tokens passed through third parties, such as a browser, are encrypted. See Add a Confidential Application.
REST API	Tenant Level settings to Enable/Disable Auto-enrollment of E-mail as MFA	Documented the new attribute `autoEnrollEmailFactorDisabled` (Boolean) for `AuthenticationFactorSettings` and added examples for it. See Multi-Factor Authentication (MFA)/Settings.

Category	Feature	Description
REST API	Add custom social identity providers using metadata	Configure declarative framework or `SocialIdentityProviderMetadata` end point. See Authenticating with a Social Identity Provider.
Security	New grant type: TLS Client Authentication	See Add Applications.

Generally Available Features

Category	Feature	Description
Security	Password Policy	The **Minimum password length (characters)** for a Simple password policy has been changed from 6 characters to 8 characters. Existing users and administrators whose passwords are not 8 characters will continue to be able to login with their old passwords after this upgrade. After their passwords expire, the minimum 8-character password length will be enforced when they change their password. See Understand the Criteria for Password Policies.

Release 21.1.2 — February 2021

Service Request Features

Service Request features must be enabled by Oracle. To learn about the features that Oracle must enable for you and how to enable them, see Service Request Features for Oracle Identity Cloud Service.

Category	Feature	Description
Trusted Partner Certificates	X.509 certificate authentication for Identity Providers	Use an X.509 authenticated identity provider with certificate-based authentication to comply with FedRAMP requirements as well as Personal Identity Verification (PIV) cards. See • Enable X.509 Certificate Authentication • Add an X.509 Authenticated Identity Provider • Service Request Features for Oracle Identity Cloud Service

Generally Available Features

Category	Feature	Description
EBS Asserter	Language support	EBS Asserter now supports language configuration of a user with the `base.lang` parameter. See • Login with Non-US English Language • Update the E-Business Suite Asserter Configuration File • Configure Oracle E-Business Suite (EBS) to use Oracle Identity Cloud Service for Single Sign-On (SSO)
EBS Asserter	Additional information regarding enabling EBS Asserter and WebLogic server deployment	When enabling EBS Asserter, if the `ebs.war` file was already deployed on the WebLogic server before EBS Asserter was enabled, then redeploy the `ebs.war` file after enabling the feature. See • Download the E-Business Suite Asserter from the Oracle Identity Cloud Service Console • Configure Oracle E-Business Suite (EBS) to use Oracle Identity Cloud Service for Single Sign-On (SSO) • Service Request Features for Oracle Identity Cloud Service .
EBS Asserter	New parameters for connection settings	Connection settings have been updated to reflect current configuration when configuring E-Business Suite for Mobile Applications. • Configure E-Business Suite for Mobile Applications • Configure Oracle E-Business Suite (EBS) to use Oracle Identity Cloud Service for Single Sign-On (SSO)

Other Documentation Changes

Feature	Link
Updated the architecture diagram for App Gateway high availability with a single origin instance.	See Set Up High Availability.
New content added in support of using SCrypt passwords.	See Create a User.
Added instructions on how to decode the `qrCodeImgContent` attribute.	See Create Self Service Enrollment Request for a Specific MFA Factor.
Maximum password length limit has been corrected in the documentation.	See Modify the Custom Password Policy.

Feature	Link
Added new note for clarification for the App Catalog billing models for Oracle Cloud Applications. See the note in the App Catalog column: **Note:** For Oracle SaaS application SSO and provisioning, refer to the descriptions in the *SSO for Oracle Cloud Services* and the *Basic User Provisioning and Synchronization for Oracle Cloud Apps* rows above.	See • Understand the User Per Month Pricing Model • Understand the Active User Per Hour Pricing Model
Added more Custom Claims examples.	See Manage Custom Claims.

Release 21.1.1 — January 2021

Service Request Features

Service Request features must be enabled by Oracle. To learn about the features that Oracle must enable for you and how to enable them, see Service Request Features for Oracle Identity Cloud Service.

Category	Feature	Description
Security	OAuth Application Token Issuance using Network Perimeters	Now, when adding a Confidential Application, you specify whether the token can be issued from *anywhere* or *issued only from specified Network Perimeters*. See Add a Confidential Application.
Security	MFA - Phone call as a factor	Configure settings for sending a passcode as a phone call to users in Oracle Identity Cloud Service. See • Configure Multi-Factor Authentication Settings • Configure One-Time Passcode Phone Calls

Generally Available Features

Category	Feature	Description
Administration	Reporting	There are three new reports in Oracle Identity Cloud Service: • **System Log Report**: Capture system activity such as successful and failed logins, user creation, update and deletion, and so on. • **Notification Delivery Status Report**: View the email notification delivery status for events such as new users, self-initiated password changes, and so on. • **Dormant Users Report**: View users who have not logged into Oracle Identity Cloud Service since a specified date. See • Understand the Types of Reports • Run the System Log Report • Run the Notification Delivery Status Report • Run the Dormant Users Report
Administration	Email Notifications	Two new attributes were added to the notification templates: • `${device.agent}` • `${device.location}` See Modify Notification Templates.
REST API	Postman	New Postman collection available for returning an encrypted OTP code in a response. Download the *AUTHN-API Return Passcode.postman_collection.json* collection and the global variables file from the idcs-authn-api-rest-clients folder within GitHub and then import them into your preferred REST Client.

Other Documentation Changes

Feature	Link
App Gateway. Documented changes to the App Gateway tasks when using OVA version 20.1.3-4.0.0 and greater.	See • Register an App Gateway • Configure the App Gateway Server • Use Services to Start and Stop App Gateway
SAML. Details the three methods used to access SAML metadata in Oracle Identity Cloud Service.	See Access SAML Metadata.
Application Catalog - Identity Cloud Service Generic Scripting Connector. Updated account script example and added setup instructions for LCM changes for dynamic attributes.	See Identity Cloud Service Generic Scripting Connector.

Feature	Link
REST API. New REST API use case that provides a step-by-step example of using the Oracle Identity Cloud Service Authentication API to authenticate with a user's credentials and Multi-Factor Authentication (MFA) and to return an encrypted OTP in the response.	See Authenticating with User Name and Password and MFA and Return an OTP.

Release 20.4.2 — December 2020

Service Request Features

Service Request features must be enabled by Oracle. To learn about the features that Oracle must enable for you and how to enable them, see Service Request Features for Oracle Identity Cloud Service.

Category	Feature	Description
Multi-Factor Authentication	FIDO Authentication	Configure FIDO authentication so that users can use their FIDO authentication device, for example an external authentication device such as a YubiKey, or an internal device such as Windows Hello or Mac Touch ID on iOS, to authenticate to Oracle Identity Cloud Service See Configure FIDO Security.

Other Documentation Changes

Feature	Link
App Gateway	New App Gateway OVA instructions for OVA version 20.1.3-4.0.0 and onward. Register an App Gateway Configure the App Gateway Server Use Services to Start and Stop App Gateway
Linux-PAM Module	The post installation files have changed. The new list of files has been documented. See Install the Linux-PAM.
Oracle Identity Cloud Service features that must be enabled for you.	Some Oracle Identity Cloud Service features must be enabled by Oracle Support before you can use them. Learn about the features that Oracle must enable for you and how to enable them. See Service Request Features for Oracle Identity Cloud Service.

Release 20.4.1 — November 2020

Generally Available Features

Category	Feature	Description
OAuth	Configurable Subject Mapping	Administrators can now customize a subject claim. A new attribute `subMappingAttr` has been added to the settings REST endpoints. If `subMappingAttr` is null or blank at the tenant level settings, then the global config `userName` attribute setting is used. See Settings REST Endpoints.
User Interface	License Type Information	You can now view your Oracle Identity Cloud Service license type in the top right of the Identity Cloud Service console.
Password Iteration Support	Password Hash Iteration	Password hash iteration has been increased to 10,000.
EBS Asserter	EBS Asserter Documentation Enhancements	Instructions have been rewritten for clarity. Additional information about validating the configuration, and how to log in with a non-US English language was also added. See Use the E-Business Suite Asserter to Enable SSO for Oracle E-Business Suite with Oracle Identity Cloud Service and Configure Oracle E-Business Suite (EBS) to use Oracle Identity Cloud Service for Single Sign-On.
Notifications	New notification option when sending primary email change notifications.	Administrators now have a new setting when sending primary email change notifications. With the new setting enabled, when an administrator changes a user's primary email, change notifications are sent to the user's old primary email address as well as the new primary email address. When the setting is disabled (default), a change notification is sent only to user's old primary email. See Notification Settings REST Endpoints.
App Gateway Documentation Updates	Learn how to deploy the Oracle App Gateway Docker container.	See Deploy the Oracle App Gateway Docker Container.
Application Catalog Documentation Updates	New connector instructions available in the Application Catalog.	See ICF Custom Connector.

All Documentation Changes

Feature	Link
Configure OAuth. New instructions regarding Issuer value behavior.	See Configure OAuth Settings.
App Gateway. New instructions on how to deploy an App Gateway Docker container.	See Deploy the Oracle App Gateway Docker Container.

Feature	Link
SAML Identity Provider. The SAML Identity Provider documentation incorrectly called for an IDP encryption certificate when creating a SAML Identity Provider. That requirement has been removed from the documentation.	See Enter Metadata Manually for a SAML Identity Provider and Update the E-Business Suite Asserter Configuration File (see `idcs.iss.url`).
Enforce Network Perimeter. Enforce network perimeter for OAuth Clients functionality was removed from the product. Same content has been removed from the documentation.	Not applicable.
Duo Security Settings. The Prerequisites section stated that a “custom login user interface” must be implemented. This was incorrect. The prerequisite was removed.	See Configure Duo Security Settings.
AD Bridge High Availability. Documented new behavior for syncing new organizational units.	See Understand Full and Incremental Sync.
RADIUS Proxy. Changes to the setup tasks as well as updated examples.	See Set Up and Validate RADIUS Proxy.
Identity Cloud Service Pricing Models. The pricing model documents did not list Group Based Password Policies. Group Based Password Policies was added to the topics as a "Standard" feature.	See Understand the User Per Month Pricing Model and Understand the Active User Per Hour Pricing Model.
Creating Groups. The documentation stated that both user memberships and nested groups can be created along with a group. This was incorrect. Nested groups are not allowed and has been removed from the instructions.	See Groups REST Endpoints.
Configurable Subject Mapping. Administrators can now customize a subject claim. New instructions for new attribute `subMappingAttr`.	See Settings REST Endpoints.
License Type Information. Content added to inform users that they can now view the Oracle Identity Cloud Service license type in the top right of the Identity Cloud Service console.	See Understand the User Per Month Pricing Model and Understand the Active User Per Hour Pricing Model.
Notifications. Documentation added for a new notification option when sending primary email change notifications - `sendNotificationToOldAndNewPrimaryEmailsWhenAdminChangesPrimaryEmail`. Request and Response examples updated as well.	See: Notification Settings REST Endpoints.
Application Catalog. New connector instructions available in the Application Catalog.	See ICF Custom Connector.
Application Catalog. Salesforce Runbook updated.	See Salesforce in the Application Catalog.
Default Settings. Documented new functionality where making the tenant signing certificate public also makes the SAML metadata public.	See Change Default Settings.
Troubleshooting User Issues. Added troubleshooting tip to explain why users may not be able to close or cancel a forgotten password request.	See Troubleshoot Oracle Identity Cloud Service – Users.
Configure the Linux-PAM using SSSD. Sample code now includes a regular expression to configure email addresses as the SSO user names.	See Configure the Linux-PAM using SSSD.

Feature	Link
Oracle Applications. Oracle applications now appear in the new Oracle Cloud Services page, and your custom applications appear on the Applications page of the Admin Console.	See Identity Cloud Service Console and About the Relationship Between Oracle Identity Cloud Service and Applications.
Known Issues. Resolved known issues removed.	See Known Issues for Oracle Identity Cloud Service.
REST API. Updates to the Token Expiry Table. Specifically, the OAuth Access Token Expiry setting.	See Token Expiry Table.
App Gate has been replaced with replaced with App Gateway. Service change notices added to the Admin Guide and What's New.	See Deprecated Oracle Identity Cloud Service Software Appliances, Manage Oracle Identity Cloud Service App Gateways, and Download and Extract the App Gateway Binary File.

Release 20.1.3 — May 2020

Service Request Features

Service Request features must be enabled by Oracle. To enable Service Request features, file a Service Request with My Oracle Support.

Category	Feature	Description
SAML	Just-In-Time (JIT) Provisioning	Using SAML, JIT provisioning automates user account creation for target service providers when the user first tries to perform SSO and the user does not exist. In addition to automatic user creation, JIT implementation allows granting and revoking group memberships as part of provisioning. JIT implementation also updates provisioned users so the users' attributes in the Service Provider store can be kept in sync with the Identity Store user store attributes. See Understand SAML Just-In-Time Provisioning. SAML JIT Provisioning uses Oracle Identity Cloud Service REST APIs. See Create an Identity Provider. For more information about how to use SCIM APIs, see REST API for Oracle Identity Cloud Service.

Category	Feature	Description
Security	Secure Oracle Database with RADIUS Proxy	Enterprises can now secure their Oracle Database instances with two-factor authentication using RADIUS Proxy. Using RADIUS Proxy, Oracle Identity Cloud Service can: • Manage all database Administrators and all database Users. • Define access controls using Database Roles to be managed by using Identity Cloud Service Groups. See • Setup RadiusProxy. • REST API for Oracle Identity Cloud Service.
Active Directory (AD) Bridge	High Availability and Load Balancing for AD Bridge	AD bridge support for the high availability (HA) has been added to deepen the integration from a business continuity perspective. With an AD Bridge high availability deployment of at least two AD Bridges per domain, delegated authentication and data synchronization loads can be shared among all the AD Bridges. Set up high availability and load balancing for multiple AD Bridges so that you don't have a single point of failure for your AD Bridge architecture. See About Multiple AD Bridges for High Availability and Load Balancing.
User Experience	Customize the sign in page by creating your own HTML code and translations.	Instead of using the default sign in page, administrators can create a Hosted Sign In page to change the look and feel of the sign-in experience. You create a Hosted Sign In page by adding a background image as well as designing custom HTML code and specifying translations (specifying translations is optional.). See Create Hosted Sign In Pages.

Beta Features

Category	Feature	Description
LDAP	LDAP2SCIM Proxy	The LDAP2SCIM proxy will allow application clients to integrate with Oracle Identity Cloud Service using LDAP protocol. This is a beta only feature currently available on invitation basis.

Generally Available Features

Category	Feature	Description
Multi-Factor Authentication	Enhanced task flow to set up and use 2-Step Verification	It's now easier for users to enroll in 2-Step Verification when they first log in to Oracle Identity Cloud Service, and it's easier to change default authentication method any time they log in. See Enroll in 2-Step Verification for Your Account. Users also have more options for managing 2-Step Verification from the My Profile console. See Manage 2-Step Verification from the My Profile Console.
Passwordless Login	Tired of resetting passwords? Passwordless authentication is available.	Instead of passwords, proof of identity can be verified based on possession of something that uniquely identifies the user (for example, a one-time password (OTP), a registered mobile device, or a hardware token). Once enabled, users can access protected resources either by using a user name and password or passwordless authentication. Users use self-service to set up passwordless authentication. See Manage Passwordless Authentication.
Application Gateway	Application Gateway Support for Multi-Origin Server	Customers can now define 1-1 or 1-n mapping between Application gateway and backed origin servers. This will provide end to end high availability architecture between Load Balancers, Applications Gateway and Origin servers.
Application Gateway	New Header Support	Ability to pass Application Gateway header in upper case.
Users	Custom Attribute Supports User Details Pages	Provides custom attribute support for end user flows. End users will be able to see the custom attributes on the My Console User Details page and edit them as well. See: • Set Up or Modify Your Profile. • Customize Schemas in Oracle Identity Cloud Service.
Active Directory (AD) Bridge	Active Directory (AD) bridge support for Group Membership as Filters	You can now bring users into Oracle Identity Cloud Service based on their group membership in Active Directory. Any changes to group membership in AD will get reflected in Oracle Identity Cloud Service User after AD Sync.

Category	Feature	Description
Identity Provisioning	Retrofit RBAC Policy - Convert individual assignment to Group Based Assignment	You can now convert direct user assignment to apps into group based assignments. Converting assignments will ensure that User's account and associated attribute values will be managed by their group membership. Changes at the group level are applied to all users managed by the group. See Convert User Grants to Group Grants.
Identity Provisioning	Lifecycle Rules	Manage the complete user life cycle and automate the process of the joiner, mover and leaver. If there is any change in a User attribute, you can propagate that to the downstream application (for example, if a user gets disabled, then all accounts owned by this user would be disabled automatically).

Category	Feature	Description
Application Catalog	Updates to the Identity Cloud Service Application Catalog.	New provisioning application templates are available in Oracle Identity Cloud Service Application Catalog for the following: • Aquera Basic Authentication • Aquera Bearer • BambooHR • Database User Management • Domo • Egnyte • Evernote • Generic LDAPv3 Provisioning • ICF Custom Connector • Kapstone Client Credential • Kapstone Password Based • Oracle Directory Server for Enterprise Edition • Oracle Unified Directory • PeopleSoft User Management • Workplace by Facebook • Zoom • Amazon Web Services • Bonusly • Box • ServiceNow Support for Interactive account provisioning and entitlement grant in existing provisioning applications: • BlueJeans • Salesforce • NetSuite • Zendesk For the latest additions to the supported list of applications in the App Catalog, take a look at Oracle Identity Cloud Service - Application Catalog.
Application Gateway	Application Gateway Support for Multi-Origin Server	Customers can now define 1-1 or 1-n mapping between Application gateway and backed origin servers. This will provide end to end high availability architecture between Load Balancers, Applications Gateway and Origin servers.

Category	Feature	Description
Security	New network perimeter rules for Sign-On policies for OAuth Token Issuance	Identity Administrators can now define a sign-on policy with the network perimeters rule applied to OAuth Clients. The OAuth Token issuance with Client Credential grant type can also be bound to the network perimeter checking. See • Understand Network Perimeters. • Add a Network Perimeter. • Client Credentials Grant Type.
Security	IDP Discovery Rules	Identity Provider (IDP) Discovery enables you to organize the login page based on the username, for example, if you want corporate SSO login for some users and you want them to be logged in using social Identity Providers. Depending on the application being accessed and who is accessing it you can completely customize the way user can login. See: • Change Session Settings. • Understand Identity Provider Policies. • Add an Identity Provider Policy. • View Details About an Identity Provider Policy. • Modify an Identity Provider Policy. • Add Identity Provider Rules to the Policy. • Change the Priority of an Identity Provider Rule for the Policy. • Edit an Identity Provider Rule for the Policy. • Remove Identity Provider Rules from the Policy.
Security	Apply Password Policies to Groups	You can have multiple password policies in Oracle Identity Cloud Service and associate them with different groups and set the priorities. Group password policies allow you to define password policies and associated rules to enforce password settings on the group level. You can create multiple policies with more- or less-restrictive rules. See • Remove Identity Provider Rules from the Policy. • Set the Password Policies for Your Identity Domain.
Security	New instructions for what to do if an Identity Provider's certificate expires.	Learn what to do if an Identity Provider certificate expires. See What is a Digital Certificate? and What if an Identity Provider's Certificate Expires? in About Digital Certificates.

Category	Feature	Description
Security	Support Social Login without Email	Social Login now allows setup of external Identity Providers for tenants configured with user email optional. This is a requirement for support of providers such as Line.Me, requested by customers.
OAuth	Refresh Token grant type is available for mobile applications.	Oracle Identity Cloud Service OAuth now allows Mobile/Public Clients to get a Refresh Token (RT) if RT is configured as one of the allowed grant types. See: • Add a Mobile Application. • REST API for Oracle Identity Cloud Service..
Extensibility and Integrations	Custom Connector for User Management	You can now provision Enterprise Applications with the Custom ICF connector. By using the Custom ICF connector, you can use OIM Custom connector with Oracle Identity Cloud Service. See About Identity Cloud Service Connector.
Notifications	New sync summary administrator notifications	New sync summary notifications are sent to the Application Admin after synchronizing the identities, groups and application accounts. The details are sent in an email and include information such as users/groups created, updated and deleted. See • About Administrator Notifications. • Modify Notification Templates. • Verify Notifications.
OAuth and Custom Claims	Custom Issuer Claim in OAuth Tokens	Oracle Identity Cloud Service now provides a way for tenant admins to configure the issuer value to be populated in the OAuth tokens (IT & AT) instead of using the default (https://identity.oraclecloud.com). See Configure OAuth Settings.
Language	New Supported Language	The Finnish language is now supported in the Oracle Identity Cloud Service user interface.
Import User Accounts	New Mandatory Column	**Primary Email Type** is now a mandatory column when importing users into Oracle Identity Cloud Service. See Import User Accounts.

Category	Feature	Description
REST APIs	Policy Expression Syntax Support for Defining User Correlation Mapping	Oracle Identity Cloud SAML Service now supports policy expression syntax for defining the user correlation mapping between an external Identity Provider's SAML assertion and any Oracle Identity Cloud Service user attribute. See the following example. `"active": true, "name": "Correlation Rule for b7fcc6a4fdc94c7abc073a3c59e05219", "return": [ { "name": "filter", "value": "emails.value eq \"$(assertion.fed.nameidvalue)\"" } ],` See REST API for Oracle Identity Cloud Service.
REST APIs	New Administrator Notifications	Specify whether users receive an email notification when an administrator changes their primary, secondary, or recovery email changes. The following settings were added to: `/admin/v1/NotificationSettings/NotificationSettings` • `"eventId": "admin.user.email.verify.primary.success"` • `"eventId": "admin.user.email.verify.secondary.success"` • `"eventId": "admin.user.email.verify.recovery.success"` See REST API for Oracle Identity Cloud Service..
REST APIs	The following new endpoints were added.	The REST APIs for Oracle Identity Cloud Service have been updated. The following endpoints have been added: • /admin/v1/GrantConverter • /admin/v1/RadiusProxies • /admin/v1/RadiusProxyListeners • /admin/v1/RadiusProxyMappings • /admin/v1/CustomConnectorInfos • /admin/v1/LocalConnectorBundles • /admin/v1/CloudGateUpstreamServerGroups • /admin/v1/CloudGateUpstreamServers • /admin/v1/ExternalNotificationProviders See REST API for Oracle Identity Cloud Service..

Category	Feature	Description
Application Gateway	New Header Support	Ability to pass Application Gateway header in upper case.
Applications	Performance Enhancement	Performance improvement when rendering the Application user interface.
Applications	Template	An additional attribute mapping of $(account.mail) has been added to the Microsoft Azure App template.
Applications	Template	A new version of the FA template is available so that you can edit Application URLs from user interface.
Applications	Manage Users in PeopleSoft from Oracle Identity Cloud Service	This guide contains instructions to manage users in PeopleSoft from Oracle Identity Cloud Service. See Manage PeopleSoft Tools-Based User Profile Records.
Applications	Manage Users in Database from Oracle Identity Cloud Service	This guide contains instructions on how to manage users in Database from Oracle Identity Cloud Service
Connectivity	AD Bridge	You can now test connectivity between AD Bridge client and AD Domain and also between AD bridge Client and Oracle Identity Cloud Service. See Test Active Directory Connectivity.
Connectors	Generic SCIM	Added configuration to send the Oracle Identity Cloud Service user id as `external_id` attribute.
EBS Asserter	New Attribute Mapping	Ability to map a customer user attribute in Oracle Identity Cloud Service with EBS FND_USER.
EBS Asserter	Validation	Self-service validation utility for EBS Asserter.
Error Messaging	Show the Specific Error Message for a Login Policy Violation	This option is switched on by default and allows the system to display the specific policy-violation error-message if the login policy is violated. If the switch is turned off, the system displays the standard error message.
Export User Accounts	Passwords	Using the Oracle Identity Cloud Service Admin console, you can export the password attribute. See Export User Accounts.
Identity and Provisioning	Oracle Directory Server Enterprise Edition (ODSEE)	This guide contains instructions to configure bi-directional synchronization between Oracle Identity Cloud Service and Oracle Directory Server Enterprise Edition (ODSEE). See Perform Authoritative Sync and Provisioning for ODSEE.

Category	Feature	Description
Identity and Provisioning	LDAP V3	This guide contains instructions to configure bi-directional synchronization between Oracle Identity Cloud Service and any LDAP V3 directory. See Perform Authoritative Sync and Provisioning for Generic LDAP V3 Directory.
Identity and Provisioning	Oracle Internet Directory	This guide contains instructions to configure bi-directional synchronization between Oracle Identity Cloud Service and Oracle Internet Directory. See Perform Authoritative Sync and Provisioning for Oracle Internet Directory.
Identity and Provisioning	Oracle Unified Directory	This guide contains instructions to configure bi-directional synchronization between Oracle Identity Cloud Service and Oracle Unified Directory. See Perform Authoritative Sync and Provisioning for Oracle Unified Directory.
Import User Accounts	New Mandatory Column	A new column "Primary Email Type" is a mandatory new column added to User CSV for import. See Import User Accounts.
Import User Accounts	Replacing Existing Values to CMVA Attributes	When administrators update users by using Import, by default new values will be added to existing multi-valued attributes. See Import User Accounts.
Integration	Application Gateway	Certified Application Gateway with PeopleSoft, JDEdwards, and OBIEE.
Notifications	New AD Bridge Connectivity Notifications	Tenant Administrators will get a notification whenever connectivity between AD Bridge and the Oracle Identity Cloud Service server is broken and also when it is restored. See AD Bridge Connectivity Notifications.
Security	MFA	While using Duo as MFA Factor in 19.3.3, the administrator was not able to use any backup factor. That restriction has been removed in 20.1.3. Also, the administrator could not specify Duo factor as App Specific MFA Factor in Sign-on policy in 19.3.3 release. Starting from 20.1.3, admin can specify Duo as app specific MFA factor in Sign-on policy.
Security	Linux-PAM Module	Added support for OEL7 for the Oracle Identity Cloud Service Linux-PAM Module.

Category	Feature	Description
User Interface	Streamlined Navigation for Applications	You can now access Oracle Cloud Services from a separate Oracle Cloud Services menu on the Navigation Drawer. Custom Applications can be accessed by using the existing Applications menu on the Navigation Drawer.

Release 19.3.3 — January 2020

Category	Feature	Description
Oracle Identity Cloud Service Foundation Stripes	Oracle Identity Cloud Service Foundation stripes in 19.3.3.	Oracle Identity Cloud Service Foundation stripes are not entitled to use multi-factor authentication (MFA). Additionally, Oracle Identity Cloud Service Foundation stripes are not entitled to use any factor other than Email for account recovery. If these features were enabled in Foundation stripes then, they will be disabled post 19.3.3.
Applications	Forms for managed applications can now contain multi-valued attributes.	If you're assigning a managed application to a user account or a group, then there's a form for the application. If the form contains multi-valued attributes, then an **Add** button appears to the right of each attribute. Click **Add**, and then in the **Allowed Values** window, select the values for the attribute, and click **OK**. For more information, see the following topics: • Assign Applications to the User Account • Assign Applications to the Group • Assign Users to Custom Applications • Assign Groups to Custom Applications
Applications	Skip OAuth Consent Page	Configure confidential and mobile applications to disable all resource's requirement for consent page. See Add a Confidential Application and Add a Mobile Application.

Category	Feature	Description
Applications	Authorization Policy for Enterprise Applications	Enterprise applications that are protected using App Gateway can now make use of authorization policies. Administrators can define, allow or deny authorization policies using authenticated IdP, group membership, network perimeter, day and time of day as authorization conditions See Configure an Authorization Policy.
Applications	OAuth support for Enterprise Applications	You can configure enterprise applications to work similarly to confidential applications by setting up the **Client Configuration** and **Resource Server Configurations** sections in the **OAuth Configurations** page for the enterprise application.
Applications	Enterprise Applications headers support extended and custom user attributes	Enterprise Application's authentication and authorization policies support sending extended and custom schema user attributes as header variables. See Supported Header Value Expressions for Authentication Policies.
Applications	List of default headers and cookies App Gateway adds to request	Documentation includes a list of default headers and cookies App Gateway adds to the request forwarded to the application during authentication and authorization validation. See Default Headers App Gateway Adds to Request.
Components	Upgrade App Gateway	Upgrade or patch your Oracle Identity Cloud Service App Gateway automatically by using the upgrade script. See Upgrade and Patch App Gateway.
Components	Identity Cloud E-Business Suite Asserter	Integrate Oracle E-Business Suite with Oracle Identity Cloud Service for authentication and password management purposes. See Use the E-Business Suite Asserter to Enable SSO for Oracle E-Business Suite with Oracle Identity Cloud Service.
Components	Identity Cloud E-Business Suite Asserter support for Oracle E-Business Suite mobile applications.	Added support to integrate **Oracle Fusion Expenses** mobile application in single sign-on with Oracle Identity Cloud Service. See Set up E-Business Suite Mobile Applications.

Category	Feature	Description
Multi-Factor Authentication	Factor Specific MFA	Administrators can now define sign-on policies to require end-users to verify specific MFA factors based on application, group membership and other conditions available in the sign-on policy. See Add a Sign-On Policy.
Security	New help desk administrator role.	A new administrator role is available for Oracle Identity Cloud Service: help desk administrator. A help desk administrator can manage all users or users of selected groups in Oracle Identity Cloud Service. Help desk administrators can view the details of a user and unlock a user account. Help desk administrators can also reset passwords, reset authentication factors, and generate bypass codes for user accounts. See Understand Administrator Roles.
Security	Customize social identity provider types and metadata.	You can create your own social identity provider type and customize an icon for it. Or, you can customize metadata for an existing social identity provider type. For example, you can define custom metadata for how to authenticate users against Oracle Identity Cloud Service using the predefined Google social identity provider. You can also customize social identity provider types for particular identity domains. Suppose you have users in the United States accessing Oracle Identity Cloud Service from one identity domain, and users from India signing in to Oracle Identity Cloud Service from another identity domain. You want only the India-based users to be able to access Oracle Identity Cloud Service with their GitHub social credentials. So, you can customize a GitHub social identity provider type for the India identity domain only. See Add a Social Identity Provider.

Category	Feature	Description
Security	Map a user's attribute value from an identity provider to an external ID.	When mapping the value of a user's attribute that Oracle Identity Cloud Service receives from a SAML identity provider to a corresponding attribute for the user in Oracle Identity Cloud Service, you can specify an external ID. You use this ID when you want to map the attribute received from the identity provider to a special ID that's associated with the provider. See Import Metadata for a SAML Identity Provider.
Security	Duo as an authentication factor.	Use Duo Security factors to securely authenticate and to sign into apps secured by Oracle Identity Cloud Service. See Configure Duo Security Settings.
Security	Select MFA factor for sign-on policies	Administrators can now define sign-on policies to require end-users to verify specific MFA factors based on application, group membership and other conditions available in the sign-on policy.

Category	Feature	Description
Settings	Integrate Oracle E-Business Suite and Oracle Identity Cloud Service	In addition to Oracle Internet Directory, you can now use the Provisioning Bridge to integrate Oracle E-Business Suite and Oracle Identity Cloud Service. This bridge provides a link between an on-premises business application (such as Oracle E-Business Suite) and Oracle Identity Cloud Service. Through synchronization, account data that's created and updated directly on Oracle E-Business Suite is pulled into Oracle Identity Cloud Service and stored for the corresponding Oracle Identity Cloud Service users and groups. Any changes to these records will be transferred into Oracle Identity Cloud Service. Because of this, the state of each record is synchronized between Oracle E-Business Suite and Oracle Identity Cloud Service. After users are synchronized from Oracle E-Business Suite to Oracle Identity Cloud Service, you can also use the Provisioning Bridge to provision users to the application. Provisioning allows you to use Oracle Identity Cloud Service to manage the life cycle of users in the application. This includes creating, modifying, deactivating, activating, and removing users and their profiles across the application. Any changes that you make to users or their profiles in Oracle Identity Cloud Service are propagated to Oracle E-Business Suite through the Provisioning Bridge. See: • Manage Provisioning Bridges in Oracle Identity Cloud Service • Synchronize and Provision Users Between Oracle E-Business Suite and Oracle Identity Cloud Service
Settings	Improved field name for Session Expiry.	On the **Session Settings** tab, the field **Session Expiry** has been changed to **Session Duration** to better reflect the purpose of the setting. No functionality has changed. See Change Session Settings.

Category	Feature	Description
Users	Show custom attributes and some additional out-of-the-box attributes in the Oracle Identity Cloud Service console.	You can now check the custom attributes and some additional out-of-the-box attributes assigned to a user as other information in the user's Details page of the Oracle Identity Cloud Service console. See View Details About User Accounts.
REST APIs	Support for multi-value Expressions in custom claims.	Based on user expressions, a claim can now return either a single value attribute or all the attributes associated with the expression. See Manage Custom Claims.
REST APIs	Support Duo as a second authentication factor	The Authenticate APIs have added a new use case to support Duo Security as a second authentication factor. This use case explains using Oracle Identity Cloud Service Authentication API to authenticate user's credentials with Duo Security. If administrators choose to enable this feature, they must ensure that all custom code which uses these authenticate APIs have been updated to support the payloads for this feature. See Use Duo as a Multi-Factor Authentication Factor. In case users choose to skip Multi-Factor Authentication during single sign-on enrollment, they can enroll to Duo Security using the self service enrollment. The self service (MyProfile) endpoints such as Initiator, validation, and Enroller are enhanced to support Duo Security. See Using Self Service to Enroll in MFA with Duo Security.
REST APIs	Enterprise Application creation with authorization policy	A new use case for creating an enterprise application with authorization policies have been added in the REST APIs for Oracle Identity Cloud Service. See Creating an Enterprise Application with Authorization Policy.
REST APIs	Trigger an email verification flow if email address is already verified	A new use case for triggering an email verification flow if email address is already verified have been added in the REST APIs for Oracle Identity Cloud Service. See Triggering an Email Verification Flow if Email Address is Already Verified.

Category	Feature	Description
Runbooks	New runbooks for integrating Oracle Identity Cloud Service with Oracle E-Business Suite and Microsoft Azure.	There are two new runbooks available with version 19.3.3 of Oracle Identity Cloud Service: • Oracle E-Business Suite: This runbook describes how to synchronize users, roles, and responsibilities between Oracle E-Business Suite and Oracle Identity Cloud Service. • Microsoft Azure: This runbook describes how to configure Oracle Identity Cloud Service to synchronize users, groups, and user group memberships from Microsoft Azure to Oracle Identity Cloud Service.

Oracle Cloud What's New for Oracle Identity Cloud Service, Release 22.4.92
E81008-76