Okta Features Cheat Sheet

by emartinez via cheatography.com/100849/cs/21137/

SINGLE SIGN ON (SSO)

About SSO	SSO refers to the ability to access multiple systems by only logging in once into one system known as the Identity Provider
Okta Integration Network (OIN)	Over 6000 pre integrated apps ready for SSO through SAML, OIDC and WS FED
Desktop SSO	Logging in to your computer automatically logs you into Okta
Mobile SSO	Using the Okta mobile app to access your work apps right from your phone without the need to sign into each app individually
MFA & SSO	Prompt for MFA per application, recommended for applications with access to sensitive information
Radius Authentication	Okta supports the ability to handle Radius authentication requests from various Radius apps such as Cisco VPN
PIV card auth	Use Personal Identity Verification (PIV) Credentials to enable Passwordless Authentication
Custom URLs	Ability to set up vanity URLs for your Okta tenant
Active Directory / LDAP Integration	Use your AD credentials to login to Okta with password synchronization or password delegation to your directory
SIEM Integrations	Robust data logs that allows for seamless integration to Security Information and Event Management systems

ADAPTIVE SINGLE SIGN ON

Adaptive SSO includes all SSO features plus the following:

Location context	Restrict or allow access to applications based on location
Device context	Restrict or allow access to applications based on device, for example deny mobile logins
Network context	Restrict or allow access to applications based on defined network zones
Risk-based Authentication	Restrict or allow access to applications based on the calculated risk a user poses

LIFECYCLE MANAGEMENT (LCM)

About LCM	LCM is the ability to manage a user from start to finish. This means creating, updating and deleting/deactivating users at the right time in an automated fashion.
Auto Provisioning/Deprovisioning for OIN Apps	Manage accounts in external applications entirely, Creation, Update and Deletion all automated
Active Directory/LDAP Integrations	Robust integration with Active Directory or LDAP Directory for Lifecycle management: complete ability to Create, Read, Update, Delete (CRUD) users in both directions all automated
Office 365	Manage accounts in Office 365 applications entirely, including license management all within Okta as an automated process
Lifecycle States	Lifecycle states make it possible to automate the process, when a user changes lifecycle state, access to other apps can be granted/revoked, accounts can be created/deleted or updated, all as an automated process

LIFECYCLE MANAGEMENT (LCM) (cont)

Group Management	Manage application groups within Okta by matching, creating or updating groups in your applications, all as an automated process
Access Request Workflows	Take the burden off of IT by allowing users to request access to applications on their own and setting who approves the access
Real time Reporting	See system tasks such as creation, update, deletion of users in Okta and connected applications in real time
Attribute Mapping and Transforms	Select exactly what data flows in both Directions between Okta and your connected Applications, need to format the data in a specific format? All doable in Okta
Mastering from a System of Records	Ability to select one or multiple authoritative sources of data, for example Active Directory or an HR system such as Workday

Advanced Lifecycle Management

Advanced LCM includes everything from LCM plus the following:

Automations	Policy for automatically suspending, deactivating or deleting users based on date based conditions and triggers. For example a contract expiration date
Built-in standards-based provisioning (SCIM)	Connect to applications through a SCIM based connector
On-prem provisioning SDK	Software Dev Kit to manage users in on-prem applications not in the OIN

INBOUND FEDERATION

Inbound SAML	Ability to have an external identity provider
Just-in-time provisioning	Okta automatically creates users on the fly when they first attempt to login and an account doesn't exist

MULTIFACTOR AUTHENTICATION (MFA)

About MFA	MFA is a secured 2nd factor of authentication on top of the standard method of username and password
Security Questions	Predefined set of questions that the user knows the answer to used as a second factor of authentication
Okta Verify OTP	Mobile app (iOS and Android) that generates a One Time Password (OTP) used as a second factor of authentication
Okta Verify with Push	Mobile app (iOS and Android) that sends a push notification to your phone to approve/deny the login attempt, used as a second factor of authentication
Email as a Factor	Email sent out containing a One Time Password (OTP) used as a second factor of authentication
SMS	One Time Password (OTP) sent your phone as an SMS message used as a second factor of authentication
Voice	Receive a One Time Password (OTP) through a phone call used as a second factor of authentication
U2F	Physical device that is inserted into the computer used as a second factor of authorization
3rd Party Factors	Google Authenticator, DUO, Symantic VIP, RSA Token and YubiKey
Windows Hello	Windows Hello allows for passwordless 2nd factor authentication by simply authenticating using windows device with your fingerprint, iris scan or facial recognition

MULTIFACTOR AUTHENTICATION (MFA) (cont)

Apple Touch ID	Passwordless 2nd factor authentication using your fingerprint to approve push notifications right from your lockscreen

ADAPTIVE MULTIFACTOR AUTHENTICATION

Adaptive MFA includes all MFA features plus the following:

Specified IP Address	Ability to configure MFA for logins only from trusted network zones defined by you
Location Context	Ability to configure MFA when a user logs in in a new city, state, or country
New geolocation	Ability to configure MFA when a user logs in from an entirely new location
Impossible travel patterns	Ability to configure MFA if the calculated velocity between login locations and times exceeds a defined limit
New device	Ability to configure MFA when a user logs in from a new device, such as a laptop or cellphone
Managed device	Ability to configure MFA when a user logs in from a pre registered managed device through solutions such as mobileIron
New IP	Ability to configure MFA when a user logs in from a new IP address
Network Anonymizers	Ability to configure MFA when a login originates from a proxy or tor connection

UNIVERSAL DIRECTORY

Cloud Directory	Manage your users entirely from the cloud by having Okta be the authoritative source of data where a user’s lifecycle starts and ends
Active Directory/LDAP Integrations	Robust integration with Active Directory/LDAP to import and manage users in both directions

UNIVERSAL DIRECTORY (cont)

Custom Attributes/Fields	Customize the schema of attributes users have to have data rich users
Custom Mapping and Transforms	Ability to transform data to be in an specific format for provisioning accounts or federation
Cloud based LDAP authentication	Delegate authentication to your directory, users only need to know one password

API ACCESS MANAGEMENT

Okta ThreatInsight	Adaptive tool that learns about login behavior and provides information on potential security risks
OAuth 2.0 and OIDC compliant	Okta is a certified OIDC and OAuth 2.0 provider
Central access and authorization management	Allows your custom applications to use Okta as an Authorization Server shifting the workload to Okta instead of your custom applications