ONE IDENTITY
PRODUCT GUIDE

This Product Guide states the usage rights and other terms associated with each One Identity Product that you ("You" or "Customer" or "Licensee") have purchased (the "Product Terms"). If You have an agreement with One Identity LLC that references the Licensing Guide, this Product Guide shall be deemed to be the Licensing Guide for that agreement.

The Product Guide is in three parts: License Types, Product Specific Terms, and Other Terms. While every One Identity Product has a License Type, only some are subject to Product Specific Terms. Any capitalized terms within a License Type definition shall be as defined elsewhere in the Product Guide.

PART 1 - LICENSE TYPES	
Active Roles Managed User Accounts	Active Roles Managed User Accounts are all enabled user account objects within any production directory(s), including but not limited to Microsoft® Active Directory and Microsoft® EntraID, within the scope of the product. A hybrid account with a system link to an already licensed account does not require an additional license. Microsoft Entra Guest (B2B) Accounts do not require licensing under this license metric. This license type excludes directory services hosted in Microsoft® Azure Government. The license quantity for Software licensed by this License Type must be at least the total number of accounts (regardless of account type) in the domain(s) or other logical group of accounts with which the Software is to be used.
Active Roles Managed User Accounts Government	Active Roles Managed User Accounts Government are all enabled user account objects within any production directory(s), including but not limited to Microsoft® Active Directory and Microsoft® EntraID, within the scope of the product. A hybrid account with a system link to an already licensed account does not require an additional license. Microsoft Entra Guest (B2B) Accounts do not require licensing under this license metric. This license is required for managing directory services hosted in Microsoft® Azure Government. The license quantity for Software licensed by this License Type must be at least the total number of accounts (regardless of account type) in the domain(s) or other logical group of accounts with which the Software is to be used.
Appliance	An Appliance is the computer on which the Software is delivered or on which the Software is used. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
ARS Enabled Accounts	ARS Enabled Accounts are the total number of unique enabled accounts in the domain(s) and cloud managed or configured using the Software, including but not limited to users' logon accounts, secondary accounts tied to users, administrative accounts, service principals, non-human accounts, service accounts, test accounts, person, user and inetOrgPerson objects. Enabled accounts includes all accounts that are active, functional, and available for use in authentication. The combined total of your ARS Enabled Accounts and ARS Disabled Accounts licenses must be at least the number of accounts managed or configured using the Software.
ARS Disabled Accounts	ARS Disabled Accounts are the total number of unique disabled accounts in the domain(s) and cloud managed or configured using the Software, including but not limited to users' logon accounts, secondary accounts tied to users, administrative accounts, service principals, non-human accounts, service accounts, test accounts, person, user and inetOrgPerson objects. Disabled accounts includes all accounts that are not active, non-functional, and not available for use in authentication. The combined total of your ARS Enabled Accounts and ARS Disabled Accounts licenses must be at least the number of accounts managed or configured using the Software.

Boomi Connection	A Boomi Connection is an integration between a component of the Software and another database, application, or API.
Cached Account	Cached Account is an account credential cached by the Software on one or more Virtual Appliance(s).
Connector	A Connector is software allowing one way, or bi-directional, alert / event synchronization between two designated third party management platforms / frameworks.
Customer	A Customer is the legal entity which purchased the license for the Software.
Desktop	A Desktop is one instance of a single user operating system on a single user computer.
Device	A Device is any physical or virtual machine or peripheral equipment connected to a network, including, but not limited to those which store, process, transmit, capture, or display data. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
Enabled User Account	Enabled User Accounts are all the user accounts in the domain(s) to be managed by the Software, including, but not limited to, users' logon accounts, secondary accounts tied to users, administrative accounts, service accounts, test accounts, and iNetOrgPerson objects. The license quantity for Software licensed by this License Type must be at least the total number of accounts (regardless of account type) in the domain(s) or other logical group of accounts with which the Software is to be used.
EPIC User	An EPIC User is a User with access and use rights to software separately licensed by Epic Systems Corp. Software licensed by this License Type is sold on a tiered basis. Customer must purchase the license tier associated with the total number of EPIC Users in their environment (e.g. 1-10000 EPIC USERs, 10001-50000 EPIC USERs, or 50001+ EPIC USERs). Software licensed by this License Type may only be used in conjunction with One Identity's Identity Manager Product and is subject to Product Specific Terms in Part 2 of the Product Guide.
External User	An External User is any User that is not an Internal User or IDM User, such as business partners, service providers, and customers.
IDM Concurrent Session	An IDM Concurrent Session is created and exists for the duration of a user's connection, created by the Software, to a remote computer or Device.
IDM User	An IDM User is a person's account or a Service Account that uses or accesses the Software. A Service Account is an account used to provide access between application software and data. The license quantity for Software licensed by this License Type must be at least the total number of accounts (regardless of account type) in the domain(s) or other logical group of accounts with which the Software is to be used unless such accounts are otherwise licensed as an External User.
Inactive User	An Inactive User means a User who is marked in the Software as being inactive (e.g., Person table, "IsInActive" flag is set to True), and remains in the inactive state for the duration of the applicable license term. If the User is partially active for any portion of the license term, that User is counted as active and is not an Inactive User. If the Software does not have built-in functionality to mark a User as inactive, this License Type will not be valid for such Software and Users will be counted as active.
Internal User	An Internal User is any full-time, part-time, contract employee, or contractor of Customer. Software licensed by this License Type may be used by one User on an individual computer, on a network storage device, or in a virtualized or shared environment (such as a Citrix server).

Limited Privileged User	Limited Privileged User is a Privileged User restricted to a maximum combined use of 10 sessions per calendar month. Any unused sessions will not roll over to the next calendar month. A session is a single discrete instance of access initiated through the Software to a target asset. A session begins when access is granted and ends when the connection is terminated or the credential is checked back in.

Lite Managed Person	A Lite Managed Person is a Managed Person that is considered to be a limited use user (which may include retail location employees, manufacturing line workers, etc.) and have assigned "X" or fewer user accounts being managed by the Software. "X" will be the number of user accounts stated in the product description in the Order; and if no number is so stated, X will default to three (3). A Lite Managed Person cannot be a Managed External Person. If the Software does not have built-in functionality to count the number of user accounts that the employee or contractor has access to, this License Type will not be valid for such Software and all applicable employees and/or contractors will be counted as a standard Managed Persons. Also, if any employee or contractor has assigned more than "X" user accounts, as of the date of that assignment Customer must purchase or use a Managed Person license for that employee or contractor and that employee or contractor will no longer be counted as a Lite Managed Person.
Log Source Host ("LSH")	A Log Source Host ("LSH") is any host, server, or device (including virtual machines, active or passive networking devices, syslog-ng clients and relays, and so on) that is capable of sending log messages. Log Source Hosts are identified by their IP addresses, so virtual machines and vhosts are separately counted.
Managed External Person	A Managed External Person is a person who is not a full-time, part-time, or contract employee, or contractor of Customer but who has one or more LAN, WAN, Cloud, or on-premises based account capable of being managed by the Software.
Managed Identity	A Managed Identity is a unique digital representation of a person or thing that is maintained in an identity repository.
Managed Non-Human Identity (NHI)	A Managed Non-Human Identity is a digital credential or identity - used by machines, applications, service agents, or automated processes or other non-human process to execute tasks and activities - that is managed by the Software. A Managed Non-Human Identity is not tied to an individual, but rather serves roles like accessing resources, data transfer, or performing automated workflows or operations.
Managed Person	A Managed Person is any full-time, part-time, or contract employee, or contractor of Customer with one or more LAN, WAN, Cloud, or on-premises based accounts capable of being managed by the Software.
Managed Secret	A Managed Secret is a secret managed by the Software.
Managed User	A Managed User is a person with defined access on the source or target environment. Software licensed by this License Type may only be used for one migration project (from one environment to another environment).
Managed Workstation	A Managed Workstation is any computer running a workstation version of a Microsoft or other operating system. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
MIPS Based Licensing	MIPS (millions of instructions per second) is the speed of the processor on the mainframe on which the Software is installed. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
Non-Privileged User	A Non-Privileged User is a named individual (including employees, contractors, and authorized third parties) or unique login identity authorized to use the Software for standard credential vaulting, retrieval, and sharing of everyday business applications and web services and who does not hold elevated rights, administrative access, or ability to administer, configure, operate, support, or secure Customer systems, applications, platforms, or infrastructure.
OL Adaptive Rate Multiplier	Each OL Adaptive Rate Multiplier license shall increase, by a multiple of 1, the default rate limit for an endpoint for purposes of increasing capacity for calls to the Software platform within the stated time period in the rate limit.

OL Connector	An OL Connector is a data transfer mechanism between the Software platform and an application or directory.
OL Delegated Admin User	An OL Delegated Admin User is a unique User who has been granted an elevated privilege create by the Software's Delegated Admin feature.

OL Monthly Active User	OL Monthly Active User measures the number of Active Users for a calendar month. An Active User is an identity in the Software directory that performs an action in the Software or performs an action on a third party service which triggers an activity in the Software. An Active User is only counted once during a calendar month.
OL On Premises Connection	An OL On Premises Connection is an on-premises application or directory that is to be connected to the Software platform.
OL Server Accessed via RDG	An OL Server Accessed via RDG is a single physical computer or virtual machine used to provide services or resources to one or more users, where the access to the server is managed by Microsoft RD Gateway.
OL Service Accounts	An OL Service Account is a non-User account that is monitored by or used with the Software.
OL Student User	An OL Student User is any full-time or part-time student of an educational institution.
OL Telephony Credit	The purchased quantity of OL Telephony Credits is equal to the price paid by Customer for that quantity, and OL Telephony Credits are consumed each time a customer opts to use telephony services for multi-factor authentication purposes, including SMS message sends or voice calls. The quantity of consumed OL Telephony Credits are calculated based on then-current telephony services pricing for such services.
OL Tenant	Each Customer environment within the Software portal with a unique tenant ID number.
OS Instance	An OS Instance is an instance of an operating system whether installed on a physical or virtual machine.
Privileged User	Privileged User is a named individual (including employees, contractors, and authorized third parties) or unique login identity authorized to use the Software to request, receive, approve, broker, initiate, monitor, or perform privileged access of any kind. Privileged access can include (but is not limited to) holding elevated rights, administrative access, or ability to administer, configure, operate, support, or secure Customer systems, applications, platforms, or infrastructure. Each unique individual accessing an administrative account shall count as a single Privileged User, even where the administrative account is shared with other users. This definition shall not include “Managed Non-Humans” which are defined under the heading “Safeguard Managed Non-Human Identity (NHI)”.
QAS-Enabled Cluster System	A QAS-Enabled Cluster System is a computer configured with a master administrative system image that utilizes the QAS client software while also controlling access to and authentication for any number of slave processing images.
QAS-Enabled Mainframe Partition	A QAS-Enabled Mainframe Partition is an IBM s/390 or zSeries Logical Partition (LPAR) that utilizes QAS client software in multiple virtual computer images.
QAS Server	A QAS Server is a physical or virtual computer (or an OS instance, a domain, or a partition on a physical or virtual computer) on which the QAS Software is installed and which is used to provide an application or service to multiple users. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
QAS User Account	A QAS User Account is a Unix-enabled user account within Microsoft® Active Directory that is used by one person and is managed by the QAS Software. Software licensed by this License Type may be used by one User on an individual computer, on a network storage device, or in a virtualized or shared environment (such as a Citrix server).

QAS Workstation	A QAS Workstation is a physical or virtual computer (or an OS instance, a domain, or a partition on a physical or virtual computer) on which the QAS Software is installed and which is used by only one user at any time. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
QSJ Server	A QSJ Server is any machine, physical or virtual, running a software application that employs QSJ Single Sign-on for Java server-side components to authenticate users in Microsoft Active Directory. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.

QSJ User Account	A QSJ User Account is a user account within Microsoft® Active Directory (use limited to one person) which uses the QSJ Single Sign-on for Java Server software to authenticate a network connection. The license quantity for Software licensed by this License Type must be at least the total number of accounts (regardless of account type) in the domain(s) or other logical group of accounts with which the Software is to be used.
Safeguard Managed Non-Human Identity (NHI)	Means a Managed Non-Human managed by Safeguard, subject to the following additional conditions: A Safeguard Managed Non-Human Identity (NHI) is an active, unique logical digital identity used by machines, applications, service agents, or automated processes to authenticate and interact with target systems. This includes usage for machine-to-machine authentication, credential retrieval, secret consumption, credential rotation, or trust brokering. An NHI is considered managed by Safeguard when it meets the following criteria: - It is represented within the Software with a non-human identity type (such as Service, Machine, Shared, or equivalent); - It is active in the system; and - It has assigned access, including but not limited to accounts, credentials, secrets, or system permissions. - Each managed NHI requires exactly one license and is counted once, regardless of the number of associated accounts, secrets, certificates, keys, credentials, entitlements, containers, workloads, transactions, or runtime instances it utilizes. - This license type strictly excludes standard human administrators, applications without an associated identity, and technical objects not represented as logical identities within the Software.
Server	A Server is a single physical computer or virtual machine used to provide services or resources to more than one user. Software licensed by this License Type which is registered to a specific Device (e.g., node-locked) may only be transferred to a Device other than that on which it was initially installed if (a) the new Device replaces the original Device and is used for the same purpose as the replaced Device or (b) One Identity provides its written consent.
System	A System is one application, operating system, or database with a unique account management structure to be managed by the Software.
Token	A Token is a software object used to authenticate one person.
User	A User is a named individual or unique login identity. Software licensed by this License Type may be used by one User on an individual computer, on a network storage device, or in a virtualized or shared environment (such as a Citrix server).
Virtual Appliance	A Virtual Appliance is a virtual machine image designed to run on a virtualization platform.
Workflow Task	A Workflow Task is a unit of work associated with an action that requires compute resources, including a connector's action, and a Workflow Task is consumed each time such unit of work is performed.

Workforce User	Workforce User is a named individual or unique login identity (including any Privileged User, Limited Privileged User and Non-Privileged User) authorized to access the software.

PART 2 - PRODUCT SPECIFIC TERMS

Designated Support Engineer	The Designated Support Engineer ("DSE") shall be Customer's first point of contact and coordinator for Maintenance Services involving the Software for which the DSE's services were purchased (the "Covered Software"). The DSE's services will be provided remotely during the standard business hours of the region of the "Ship-to" location stated on the Quotation or Order for the Covered Software. One Identity shall assign the person to be the DSE and may change such person in its sole discretion. If the DSE is unavailable (e.g., illness, vacation), One Identity will assign another person to temporarily fulfill the DSE role. The DSE is provided as part of Maintenance Services under the terms and conditions governing the Covered Software.
Freeware	⁘ Foglight Network Management Freeware. The terms and conditions that govern the use of the Freeware version of Foglight Network Management Server are located at http://communities.oneidentity.com/community/foglight/nms. ⁘ Privilege Manager for Sudo Freeware. The Privilege Manager for Sudo Freeware may only be used with ten (10) Managed OS Instances. Limitation of Liability and Damages. IN NO EVENT WILL ONE IDENITYT, ITS SUBSIDIARIES OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF ANY OF THE FOREGOING BE LIABLE TO LICENSEE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND DATA AND THE LIKE), WHETHER FORESEEABLE OR UNFORESEEABLE, OR FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES, REGARDLESS OF THE BASIS OF THE CLAIM AND EVEN IF One Identity OR A ONE IDENTITY REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ONE IDENTITY'S CUMULATIVE LIABILITY FOR DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO $500.00. ⁘ All Other Freeware Products. The following provisions shall apply to Customer's use of all other Freeware products. The terms outlined herein shall supersede any conflicting terms set forth in the Agreement. Capitalized terms not defined herein shall have the same meaning as those set forth in the Agreement. ‖ License. One Identity hereby grants Licensee a non-exclusive and non-transferable, license to use the Freeware, in executable object code form only, for personal or internal business purposes, for the duration specified by One Identity. Licensees who are partners of One Identity may use the Freeware on their customer sites for promotional purposes only, provided, however, that if their customer wishes to obtain their own copy of the Freeware, Licensee must direct their customer to One Identity's download site to obtain a copy of the Freeware. One Identity may change the scope of use restrictions set forth herein at any time in its sole discretion. This license does not entitle Licensee to receive from One Identity hard-copy Documentation, technical support, telephone assistance, or enhancements or updates to the Freeware. If One Identity releases a commercial version of the Freeware, the parties shall agree upon the fees and terms of such use in a separate signed agreement. ‖ Disclaimer of Warranty. THE FREEWARE IS PROVIDED FREE OF CHARGE, AND, THEREFORE, ON AN "AS IS" AND UNSUPPORTED BASIS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES THAT IT IS FREE OF DEFECTS, VIRUS FREE, ABLE TO OPERATE ON AN UNINTERRUPTED BASIS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT. NO USE OF THE FREEWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER. ‖ Fees and Taxes. There is no fee for Licensee's use of the Freeware in accordance with the Agreement, however, Licensee is responsible for any applicable shipping charges or taxes which may be incurred under the Agreement, and any fees which may be associated with usage beyond the scope permitted herein.

Freeware (Continued)	Limitation of Liability and Damages. WITH RESPECT TO FREEWARE, IN NO EVENT WILL ONE IDENTITY, ITS SUBSIDIARIES OR ANY OF THE LICENSORS, DIRECTORS, OFFICERS, EMPLOYEES OR AFFILIATES OF ANY OF THE FOREGOING BE LIABLE TO LICENSEE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND DATA AND THE LIKE), WHETHER FORESEEABLE OR UNFORESEEABLE, OR FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES, REGARDLESS OF THE BASIS OF THE CLAIM AND EVEN IF ONE IDENTITY OR A ONE IDENTIY REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ONE IDENTITY'S CUMULATIVE LIABILITY FOR DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO $500.00.
Hardware (including Dell Hardware)	In the event Customer acquires Hardware under the Agreement, title to such Hardware shall pass to Customer upon shipment (unless such Hardware is rented, leased or loaned to Customer). Unless otherwise stated herein, Hardware shall be warranted in accordance with the warranty document delivered with the Hardware. In the event Customer acquires Hardware that is delivered with a third party warranty ("Third Party Warranty"), Customer will rely solely on the applicable third party for all Third Party Warranty obligations.

Identity Manager Healthcare Integration for Epic	The terms and conditions of use of the Software are governed by the Agreement between One Identity and the Customer. Epic Systems Corporation (“Epic”) is not a party to the Agreement between One Identity and Customer, and the Agreement does not bind Epic in any manner. One Identity and Customer agree that; 1) Epic makes no warranty or representation about the Software; 2) Epic is not responsible for any third party or Customer claims arising out of or related to the use of the Software; 3) One Identity shall have the right to disclose or share the portion of the Agreement between One Identity and Customer specific to the Software with Epic upon Epic’s request; and 4) Epic is not responsible for providing any level of support for the Software. If Epic should choose to provide any support services related to the Software, Epic may charge the Customer for such services under the terms and conditions of a separate agreement with Epic. Customer agrees that Epic and any Epic owned entities are third party beneficiaries of the confidentiality and data protection portions of the Agreement between Customer and One Identity Customer may conduct an inspection of One Identity's records through the use of a third party auditor mutually acceptable to Customer and One Identity to verify One Identity's compliance with the Epic App Orchard program terms, and One Identity will reasonably cooperate with such inspection, This inspection will be at Customer’s expense unless material non-compliance is discovered as a result of the inspection, in which case One Identity will pay for the cost of such inspection. The Software is licensed for use in conjunction with Identity Manager only. When the Software is deployed to an Identity Manager Job Server, log files are generated based on the configuration of the Software by the Customer. The log files at this location log the Epic users’ Community ID and Internal ID and any errors or exceptions returned by the Epic web services. These log files include; 1) JobService.log; 2) Synchronization Editor.log; 3) StdioProcessor.log and 4) HSCEpic.log. Epic data, the Epic Credentials, and ClientID that is accessed thru the Epic App Orchard program are stored in the Identity Manager database. The Software itself does not store any Epic related information or data and only facilitates the transfer of data between Identity Manager and the Epic web service. The duration of the transfer will depend on the type of attributes and quantity of data chosen by Customer’s Identity Manager administrator for transfer between Identity Manager and the Epic web service. The Software supports the following Epic web services: 1) Epic Personnel Management (Category Security); CreateUser; UpdateUser; DeleteUser; ActivateUser; InactivateUser; ViewUser; ForcePasswordChange; SetUserExternalPasswords; SetUserPassword; 2) Epic Demographics (Category Common) UpdateUserDemographics; 3) Epic Interconnect; GetRecords and 4) EPIC Core; GetEnvironmentInformation, GetConnectivityInformation.

	The following information is stored in Identity Manager for synchronization purposes and will reside in the Identity Manager database until the user is deleted from Identity Manager by an Identity Manager administrator: UserInternalID, UserCommunityID, UserExternalID, Name, UserComplexName, ContactDate, ContactComment SystemLoginID, LDAPOverrideID, AuthenticationConfigurationID, BlockStatus, IsActive, StartDate, EndDate UserAlias, UserPhotoPath, LinkedTemplatesConfig, UserSubtemplateIDs, Sex, EmployeeDemographics, ReportGrouper1, ReportGrouper2, ReportGrouper3, CategoryReportGrouper1, CategoryReportGrouper2, CategoryReportGrouper3, CategoryReportGrouper4, CategoryReportGrouper5, CategoryReportGrouper6, Notes, InBasketClassifications, PrimaryManager, UsersManagers, UserRoleIDs, DefaultLoginDepartmentID, CustomUserDictionaries, UserDictionaryPath, LinkedProviderID, ProviderAtLoginOption, IdentityIDs, ExternalIdentifiers, AuditUserID, AuditUserIDType, AuditUserPassword, EmailAddress, PhoneNumber, FaxNumber, Address, City, Country, County, District, HouseNumber, Lines, State, ZipCode. A copy of One Identity's Privacy Policy is located here: https://www.oneidentity.com/legal/privacy.aspx
Identity Manager on Demand (IMOD)	Identity Manager on Demand (IMOD) includes a default data storage allocation which is detailed in in the IMOD Product Documentation. Customers who exceed this allocation may experience limitations in system performance or functionality. Additional storage capacity may be available subject to applicable fees and terms. Customers will be notified – as a notification in IMOD, via automated email notifications, through their designated account representative, or other method – when usage approaches the allocated threshold.
Instant Messaging Network Terms of Use	Customer understands and agrees that the Agreement does not modify or discharge Customer from compliance with the terms and conditions governing Customer's use of any third party instant messaging service ("Instant Messaging Agreement"). Customer hereby agrees to comply with all applicable Instant Messaging Agreements, (ii) that One Identity shall not be liable for Customer's violation of an Instant Messaging Agreement, and (iii) to indemnify and hold One Identity harmless from any liability related to Customer's violation of an Instant Messaging Agreement. In addition, Customer understands and agrees that the Agreement does not guarantee the availability of any instant messaging networks and that One Identity shall not be liable for any outages, discontinued services or termination of service by such third-party instant messaging providers.
One Identity Manager On Demand	The Documentation for One Identity Manager On Demand includes restrictions on customizations. Ignoring these restrictions may cause the One Identity Manager On Demand Cloud components to become in an un-upgradable state. If this happens, additional professional services may be required at Customer's expenses to revert the One Identity Manager On Demand components to the original state or to install upgrades to the One Identity Manager On Demand components.

OneLogin Software	For OneLogin Software licensed by Internal User, External User, OL Student User, and/or OL Delegated Admin User, the number of licenses is the maximum number of such Users that can be assigned that role in Customer's systems that are tracked and/or managed by the Software. For OneLogin Software licensed by OL Monthly Active User, the number of licenses multiplied by 12 equals the maximum aggregate number of Active Users through the twelve-month period who may perform an action on the Software or may perform an action on a third party service which triggers an activity in the Software. In the event Customer exceeds the maximum aggregate number of Active Users licensed under this metric, Customer must pay for each additional Active User for the remainder of the subscription term. For OneLogin Software licensed by OL Monthly Active User, the number of licenses multiplied by 12 equals the maximum aggregate number of Active Users through the twelve-month period who may perform an action on the Software or may perform an action on a third party service which triggers an activity in the Software. In the event Customer exceeds the maximum aggregate number of Active Users licensed under this metric, Customer must pay for each additional Active User for the remainder of the subscription term.
Premier Plus Support	Premier Plus Support includes all aspects of Premier Support, plus an Advanced Support Engineer ("ASE"). Premier Support Plus for One Identity is limited to specific product lines (Active Roles, Log Management, Identity Governance, or Privilege Management). The applicable product line will be stated on your Order. Premier Plus Support for One Identity is available in three levels, Business, Enterprise, or Elite. The applicable level will be stated on your Order. The ASE is a semi-dedicated support engineer that provides oversight for all suppor requests, conducts knowledge sharing sessions, engages in application monitoring of the software covered by Premier Support Plus, provides upgrade assistance, and engages in quarterly health checks of the software covered by Premier Support Plus as furthered detailed in the Support Guide. Premier Support Plus includes the following percetage of an ASE's time depending on the level purchase: Business = 20% of an ASE's time; Enterprise = 50% of an ASE's time; Elite = 100% of a dedicated ASE's time.
Premier Support	Premier Support includes accelerated response times as stated the Support Guide and provides a shared, named Customer Success Manager (“CSM”) as a single point of contact. The CSM shall provide introductory training in the use of the Maintenance Services, manage the escalation and resolution of Service Requests, to provide monthly Service Request reports, and to attend monthly calls with Customer to review priorities. Additionally, the CSM will communicate Customer priorities to the One Identity support team, review and document Customer’s Software assets, gain an understanding of Customer’s environment and future plans, provide proactive notification of Software patches and fixes.

Privileged Account Products: Warranty Appliance Replacement Program	"PA Software" is a One Identity Software product from its "Privileged Account" family of software products. "PA Appliance" is an Appliance on which PA Software is delivered. Warranty. One Identity warrants that for one (1) year following the initial delivery of the PA Appliance, the PA Appliance will operate in a manner which allows the PA Software to be used in substantial conformance with the Documentation (the "PA Appliance Warranty"). As Customer's sole and exclusive remedy and One Identity's sole obligation in the event of a breach of the PA Appliance Warranty, One Identity shall fulfill its obligations under the Appliance Replacement Program (as described below). Any breach of the PA Appliance Warranty must be reported by Customer to One Identity during the applicable Warranty Period. Appliance Replacement Program. If Customer has purchased a License to use PA Software and has purchased Maintenance Services for the PA Software continuously since the purchase of such License, One Identity shall make available to Customer an Appliance Replacement Program (as defined below) for the PA Appliance. The "Appliance Replacement Program" is as follows: on the business day following One Identity's determination that a replacement Appliance is required, One Identity will either ship a replacement for the Appliance (a "Replacement Appliance") or, at its discretion, ship a replacement part for the Appliance to be installed by Customer (a "Replacement Part"). Any Replacement Parts shall be externally replaceable, not requiring the Appliance case to be opened. Replacement Appliances or Replacement Parts may be previously used, but shall not be of lesser capacity or specification than the Appliance or part being replaced. If Customer cannot permanently delete the data from the Appliance's data storage device and Customer's information security policy does not permit return of the Appliance with the sensitive data on it, Customer may remove any data storage device that does not require the Appliance case to be opened and return the Appliance without the device, provided, however, that Customer shall be required to purchase a replacement data storage device from One Identity. Customer agrees to return the replaced Appliance or part within forty-five (45) days after receiving the Replacement Appliance or Replacement Part.
QAS or QSJ	For the purposes of this paragraph, "you" means Licensee. If you obtain services, including logon, authentication, authorization and group policy services from Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire. If you have already purchased the licenses required by Microsoft to use the Microsoft operating system products, this clause does not require you to purchase additional licenses.
QMX for SMS, or QMX for Configuration Manager 2007 or QMX Additional Microsoft License Requirements	For the purposes of this paragraph, "you" means Licensee. If you obtain services, including systems management services, from Microsoft Systems Management Server or Microsoft Configuration Manager 2007 products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft Systems Management Server or Microsoft Configuration Manager 2007products you are using to determine which licenses you must acquire. If you have already purchased the licenses required by Microsoft to use the Microsoft Server products, this clause does not require you to purchase additional licenses.

QMX for SCOM, and QMX for SCCM Additional Microsoft License Requirements	Customer understands and agrees that QMX for SCOM and QMX for SCCM may contain the following Microsoft products: System Center Operations Manager and System Center Configuration Manager (the "Microsoft Products"). The rights and restrictions set forth in the Agreement that apply to the One Identity Products shall apply in the same manner to the Microsoft Products. In addition, high risk use of the Microsoft Products is not permitted, including but not limited to, use in or in conjunction with aircraft or other modes of human transportation, nuclear or chemical facilities, and Class III medical devices under the Federal Food, Drug and Cosmetic Act. Customer hereby consents to the disclosure of Customer information from One Identity to Microsoft for the purpose of reporting to Microsoft that Customer has licensed a product containing the Microsoft Products from One Identity. To the extent permitted under applicable law, all warranties and liability of Microsoft with respect to the Microsoft Products shall be disclaimed, including but not limited to (i) warranties of title, non-infringement, merchantability and fitness for a particular purpose, (ii) any implied warranty arising from course of dealing or usage of trade, (iii) any common law duties relating to accuracy or lack of negligence, (iv) any warranty that the Microsoft Products will operate in connection with the applicable One Identity Product or on any Customer system, and (v) any liability for damages, whether direct, indirect, incidental or consequential, as a result of the use and/or installation of the Microsoft Products. Customer represents and warrants that (i) it is not licensing Microsoft Products separate and apart from the applicable One Identity Product, (ii) that the copies of the Microsoft Products that it receives from One Identity do not entitle Customer to maintain on its computer systems any more copies of the Microsoft Products than it previously licensed from One Identity or Microsoft, and (iii) it possesses and will maintain sufficient quantities of fully valid Microsoft licenses to support the maximum number of users and devices that may access or use the applicable One Identity Product under the terms of the Agreement. For purposes of the Microsoft Products, Microsoft shall be an intended third party beneficiary of the Agreement with the right to enforce warranties and any other provisions of the Agreement and to verify the compliance of the Customer with the same.
QMX SMSE Managed Server	For each QMX SMSE Managed Server license granted by One Identity Customer may use defined QMX products for management of a licensed physical server, or up to the licensed numbers of OSEs running on a single physical server or device.
QMX SMSD Managed CPU	For each CPU running on a physical server or device, Customer must purchase the corresponding number of QMX-SMSD Managed CPU licenses and may use such licenses to manage an unlimited number of OSE running on such physical servers or devices.

Token Hardware	The sole and exclusive warranty for the Tokens is as set forth in this paragraph. All other warranties, express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose are hereby disclaimed. One Identity warrants that for a period of 12 (twelve) months (or, with regard to Go-3, Go-6, Go-7 and Slim Tokens, 36 (thirty six) months) following delivery by One Identity (the "Warranty Period") the tokens are free from faults in manufacture and materials where such faults materially affect the use of the Tokens (the "Token Warranty"). One Identity shall not be liable for defects in Tokens which are notified by Licensee after expiration of the Warranty Period, nor for any minor cosmetic faults where use of the token is still possible. This limited warranty does not apply to malfunctions attributable to (i) extrinsic causes such as natural disasters including fire, smoke, water, earthquakes or lighting, (ii) electrical power fluctuations or failures, (iii) abuse, misuse, accident, alteration, neglect or unauthorized repair or installation, or (iv) storage outside of +10 °C to +30 °C with 85% relative humidity in non-condensing conditions. One Identity does not warrant that the Tokens operate without interruption or without error. Customer's exclusive remedy and One Identity's sole obligation for any breach of the Token Warranty shall be for One Identity to replace defective Tokens within a reasonable time or, where replacement is not reasonably possible, to refund the fees paid for the non-confirming tokens. Customer must return to One Identity the non-conforming Tokens no later than fourteen (14) days after its receipt of the replacement Tokens.
VAS, VSJ, VMX	These products have been re-branded to QAS, QSJ, and QMX respectively

PART III - OTHER TERMS

Notwithstanding anything otherwise set forth in the Agreement, the terms and restrictions set forth in the Agreement shall not prevent or restrict Customer from exercising additional or different rights to any source software that may be contained in or provided with the Products in accordance with the applicable open source licenses.

Certain Products may include Java software from Oracle. The Java software components included in such Products are subject to the terms and conditions set forth in the Software License.txt and THIRDPARTYLICENSEREADME.txt files that are included in the Java software.

Customer is hereby notified that the Software may, with the user's consent, collect certain information from the Customer and transmit such information back to One Identity or its sub-processors. Such information may include statistics relating to how often the Software and tools are started and completed, the duration of use of the Software, performance metrics relating to the Software, and Software configuration settings. These usage statistics are gathered, transmitted, and analyzed for the purpose of improving the Software. In addition, Customer is hereby notified that (1) the Software may require a registration process whereby machine specific identifiers (that have been encrypted and are unique) and the username and user's email address are transmitted to One Identity's licensing server to allow One Identity to generate a unique key that is bound to the specific computer on which the Software may be used in order to limit the use of the Software to authoirzed systems owned by licensed customers, (2) the Software may communicate with One Identity's patching server and allow Customer to download patches when they are available, to enable Customer to receive the newest enhancements promptly, (3) the Software may provide a 'Feedback' facility that allows Customer to send suggestions and ideas for improving the Software ("Feedback"), (4) the Software may include a mechanism to transmit information to One Identity regarding unhandled exceptions to allow One Identity's engineers to identify otherwise unreported issues to be addressed to improve the Software, and (5) the Software may make connections to One Identity servers to verify license validity to ensure One Identity Software is being operated only on authorized systems owned by licensed customers. By using the Software and opting-in, Customer hereby consents to the collection of such information by the Software, the transmission of such information to One Identity or its sub-processors, and the use of such information by One Identity or its sub-processors for the purposes specified here and any additional purposes specified in the Software at the time the user is prompted to opt-in.

This Product Guide may be amended from time to time by One Identity, provided, however, that the terms and conditions of this Product Guide that are in existence as of the date One Identity accepts an order placed by Licensee or Customer shall apply to the first purchase of specific Software referenced in such order regardless of any changes that are subsequently made to this Product Guide. For clarification, all of Licensee's or Customer's licenses for specific Software, regardless of license date, will be governed by the version of the applicable Product Terms in effect on the date of the most recent license purchase.