

5. $\frac{1}{2} \times \frac{3}{4} \times \frac{5}{6} \times \frac{7}{8} \times \frac{9}{10}$

[illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible]

۱۰۰. (مَوْجِدُ مَوْجِدَانِ رُؤُوسَ دَر) ۱۰۰

[illegible]

7. في سائر النسخ التي في المخطوطات والتي في المطبوعات

7.1. $500,000/-$ (پانچ سو روپيا) جي رقم جو سود جو تناسب 0.05% جي شرح تي ٿيندو.

[illegible][illegible]

7.4. ۋە ئاجايىدە ئەمەلىيەتچى، ۋە ئاجايىدە سۆز ۋەكىلى، ئانىسىنىڭ قىممىتىنى بىر نەرسىگە سېتىپ، سىرتقى دۇنيادىن 07 تۈرۈندە قوشۇلدى، ۋە ئاجايىدە سۆز ۋەكىلى، جەنسەنەمنىڭ ئىززەت-قۇدرىتى ۋە شەخسەنەمنىڭ رەھبەرلىك قىلىشى.

[illegible]

8. مَرِّضَ مَرْصُومًا وَفَرَسًا:

[illegible]

8.2. دِهَ اِيسُوْدِي دَسَرِنَمو سِدْمُو 6 (رَنه) دَوْتِرُو دَوْتِر مَحْسُوسُو زَرْبُو دِمْدِي هَرَجَزَرُو زَرْبُو رَسَدُم خَوُسَرُو.

8.3. $\Delta_{\text{H}}^{\text{H}}$ သို့မဟုတ် $\Delta_{\text{H}}^{\text{H}}$ မှတစ်ဆင့်၊ အသံအချိန် (စက်မှုနှုန်း) ကို တွေ့ရှိရသော အချိန်ကို

မှန်ကန်စွာ ဖော်ပြနိုင်သည်။ အသံအချိန်ကို တွေ့ရှိရသော အချိန်ကို

9. $\frac{1}{2} \log 2$

[illegible]

9.2. $\frac{d}{dt} \left(\frac{1}{2} m v^2 \right) = \frac{d}{dt} \left(\frac{1}{2} m \left(\frac{dx}{dt} \right)^2 \right) = m \frac{dx}{dt} \frac{d^2x}{dt^2} = m v a$

دَدَسَاوَنَیوَسَ وَاِنِیْکُمُ سَدَ هُوَ لَکُمُ سَیِّئٌ وَاِنِیْکُمُ سَدَ هُوَ لَکُمُ سَیِّئٌ وَاِنِیْکُمُ سَدَ هُوَ لَکُمُ سَیِّئٌ
 رَوَیْکُمُ سَدَ هُوَ لَکُمُ سَیِّئٌ

10. $\frac{1}{x^2} = x^{-2}$ $\frac{d}{dx} x^{-2} = -2x^{-3} = -\frac{2}{x^3}$

10.1. $\frac{1}{n} \sum_{j=1}^n x_j = \bar{x}$

[illegible]

10.2. $\frac{1}{x^2} = x^{-2}$, $\frac{d}{dx} x^{-2} = -2x^{-3} = -\frac{2}{x^3}$.

[illegible][illegible]

ا ل ر د ا و ح خ ص ط ز س ش ه و ع ف ق ك غ

11. دُرُفَرْمُورْ دَسْمِزْ نَمُ سُرْمُورْ دِجْ سَرَوَ اَرِزْ سُرْ نَسْرُورْ سُرْ اَرِزْ سُرْ

11.1. $\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{x}} \right) = \frac{\partial L}{\partial x}$, $\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{y}} \right) = \frac{\partial L}{\partial y}$, $\frac{d}{dt} \left(\frac{\partial L}{\partial \dot{z}} \right) = \frac{\partial L}{\partial z}$

سرسر سسر سسر، ار سسر سسر، سر سسر سسر، سر سسر سسر، سر سسر سسر، سر سسر سسر، سر سسر سسر، سر سسر سسر

[illegible]

כִּדְרֵי־סוּרִים תִּשְׁחַדְנָם מִשְׁחָלֵם וּמִסְרָדָם.

11.2. دسټوانو، خوږوڅي اوسر ترمنځ روڼ سړومو، وړانديز، داختم اوسرو، قريه سرسره، ډېر ښه خبره، 15% اوسر-اوسر اوسرو

[illegible][illegible]

٤٢٤ (٥) دسمبر ۱۹۷۱ء کو کراچی میں منعقد ہونے والے پاکستان مسلم لیگ ق کے جلسے میں قائد اعظم کی پوری تصویر دکھائی گئی۔

[illegible]

اَلْحَمْدُ لِلّٰهِ الَّذِي هَدَانَا لِهٰذَا وَمَا كُنَّا لِهٰذَا لَٰئِقِيْنَ

(CP*0.005*LD)

CP (نِسْرَجْ مَرْنَجْ نِسْرَجْ مَرْنَجْ) : نِسْرَجْ مَرْنَجْ نِسْرَجْ مَرْنَجْ نِسْرَجْ مَرْنَجْ نِسْرَجْ مَرْنَجْ

LD • (مَوْجِدٌ ۚ تَرْتَمُّونَ) : تَرْتَمُّونَ تَرْتَمُّونَ تَرْتَمُّونَ تَرْتَمُّونَ تَرْتَمُّونَ

12. $\frac{1}{x^2} = x^{-2}$, $\frac{d}{dx} x^{-2} = -2x^{-3} = -\frac{2}{x^3}$

12.1. جَدَّسَ لِمَا سَمِعْتُمْ دَرَّ هَؤُلَاءِ رُسُلُكُمْ قَدْ كَذَبُوا بِكُفْرِهِمْ وَأَسَاءَ أَعْيُنُكُمْ أَلَيْسَ لَكُمْ رَسُولٌ أُرْسِلَ؟

12.2. $\frac{d}{dt} \left(\frac{1}{2} m v^2 \right) = \frac{1}{2} m \frac{d}{dt} (v^2) = m v \frac{dv}{dt} = m v a = m v \frac{dv}{dr} \frac{dr}{dt} = m v \frac{dv}{dr} v = m v^2 \frac{dv}{dr}$

[illegible][illegible]

سر. قسٹ نامہ لاگو ہوئے ہوئے کی قیمت پر دس روپے - خرچہ گرانٹوں %00 دھونس کے ساتھ.

[illegible][illegible]

دې ژبې د غږونو او لفظونو په واسطه خپل پیاوړتيا ته رسوي.

[illegible]

Annex 1

Bid Submission Form

Iulaan No: (IUL)94-Q/94/2025/52

IMPORTANT: This sheet should serve as the front page of the proposal. If any bidder fails to submit the relevant information and bid documents stated in information sheet section 5, the bid will be rejected at the bid opening stage.

Bid Title: Supplying ManageEngine Endpoint Central UEM Edition

Qty	Description	Price
01	ManageEngine Endpoint Central UEM Edition	
GST (8%)		
TOTAL (MVR)		
Total in Words:		

Duration	Calendar days	
Proposed Period		days

Bidders Information:

Business Name: _____

Registration Number: _____

Address: _____

Contact Person: _____

Designation: _____

Contact No.: _____

Mail Address: _____

Bid Checklist (this sheet should be attached with bid submission form)

		Yes (✓)	No (x)
1	Bid Submission Form Completed & Signed (Annex 1)		
2	Quotation		
3	Business Information Sheet – Issued via the Business Portal of the Ministry of Economic Development and Trade.		
4	Business Activity Registry (must be registered under an activity related to the scope of work)		
5	S.M.E Registration		
6	G.S.T Registry / GST Document		
7	Tax Clearance Form		
8	Bid Security (If the bid amount is greater than 500,000.00)		
9	Past Experience Documents (Related to the bid)		
10	Bank Statement		

Annex 2

Technical Requirement

<i>Endpoint Management solution</i>			
<i>General Requirements</i>		Compliance (Yes/NO)	Remarks
1	The solution should support patching for various operating systems (Windows, Linux, MAC etc) for desktops, laptops & servers centrally using a single solution user Interface.		
2	The solution must support users connecting through VPN and internet-connected users.		
3	The solution shall operate without requiring computers to belong to a Domain or Active Directory. The solution shall be capable of integrating with one or more Active Directory structures if present.		
4	Patching for all remote locations needs to be managed centrally using a central management server.		
5	The solution should work over low-speed connections at remote sites.		
6	The solution should also help in bandwidth throttling without depending on OS capabilities.		
7	In an event of any critical Zero-day vulnerability, the solutions should support to implement security work around recommended by OEMs across the enterprise rapidly.		
8	The solution should also maintain the asset inventory. Thus, all the asset information will be available centrally at Customer HQ locations.		
9	The solution should support remote imaging and deployment for windows Operating Systems		
10	The solution should also support software distribution for Windows, Mac, and Linux.		
11	The solution must be capable of proactively reporting changes to managed desktops within a few minutes of detecting change or upon executing any action deployed from the server.		
12	The solution must include agent software that is deployed on all managed desktops.		
13	If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from the internet, then the integrity of all such content must be verified by the solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the file is downloaded intact and unchanged		
14	The solution must have fully documented APIs for integration into other complementing tools. The eligibility to use all such APIs must be included in the solution proposed.		
15	The solution should provide ready-to-use patch management policies so that patch administrators can readily start patching the supported OS platforms using policy-based patching & customization.		

Architecture Requirements			
1	The solution must support distributed environment including Hub and Spoke sites connected by variety network links varying from less than 1Mbps to 2Mbps or more.		
2	The solution must be capable of using existing client computers as distribution points at remote sites without the need for allocating dedicated servers.		
3	The solution must have a native in-built ability to throttle bandwidth, either statically or dynamically. The throttling capability must support up and downstream throttling for both the server and agents.		
4	The solution must support the ability to cache content on the remote office distribution point as required by the computers.		
5	The solution must be capable of downloading and caching payload at the remote distribution points before the scheduled time of an action. This will ensure timely completion of activities within the scheduled window without having to wait for downloads to complete during the scheduled window over slower WAN links.		
6	The solution must operate using a few configurable ports for all communications between Agents, Distribution Points, and Servers. etc.		
7	Does the solution ensure continuous compliance by assessing for devices outside the company network, while managing roaming devices using IP scope and agents?		
8	Can the agent remain idle until tasks are scheduled, while still regularly checking for instructions from the server?		
9	The Desktop Management software must support the following OS platforms with agent and functionality coverage: a. Windows, Linux, MAC.		
10	The solution must provide a remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory, NT Domains, or Local Administrator Authentication for deploying agents to remote computers.		
11	The bidder's agent deployment strategy should also consider the use of the following agent deployment methods:		
	a. Active Directory Group Policies to deploy agents at domain login		
	b. login scripts to deploy agents at domain login		
	c. Email installation instructions to remote users for unreachable users.		
	d. Use of existing 3rd party software distribution tools as available.		
	e. Manually installing the agent where no other methods succeed. The multiple method approach is necessary for a complete desktop coverage as part of the implementation project		
12	The solution must support documented procedures for including the agent as part of a 'gold' OS image.		
13	The solution must provide easy-to-use in-place upgrade procedures for all components through the console.		
14	The solution should use a Single management UI for of all features/functions and components.		

15	The solution must have native support for a high level of encrypted communications without any dependency on additional software, hardware, third-party Certificates, or Certificate Authority.		
16	The solution must include failover capability to cater to scenarios such as hardware failure or site disaster.		
17	The solution should support the air-gap network.		
Management of Agents			
1	The solution should enable the management of all computers from a central console.		
2	The Administrator shall be able to perform the basic management tasks from the central console:		
	a. Configure all agent settings centrally		
	b. Create Dynamic computer groups		
	c. Create Users with Role Based Access Control		
	d. Assign agents to Distribution points		
	e. Setup bandwidth Throttling		
	f. Perform agents upgrade remotely without manual intervention in agent machines		
3	The solution should enable monitoring of the status of all agents from a central console.		
4	The User Interface for Administration i.e. Console should provide flexibility to allow users to customize the console to fit their individual requirements by adding, and removing column headers/functions based on the role of the user.		
5	The solution should enable console operators to instantly query and collect information results for a custom inventory query from the database.		
6	The solution should enable console operators to group computers statically by selecting computers and adding to the group or dynamically based on the result of inventory properties such as e.g. Active Directory groups, OS, IP address etc.		
7	Solution Agent should provide an end user Information interface that allows the user interacts with the agent for interactive actions		
8	The solution should enable administrators to prevent the end user from uninstalling the agent, using the central management console.		
9	Information stored in the solution's central database shall always be accurate and up-to-date based on scheduled time.		
10	If the agent fails to communicate to the server within a specified interval, the central console shall automatically mark the agents as offline.		
11	The solution should enable the assignment of agents to console users for management purposes.		
Patch Management Requirements			
Patch Detection			
1	The solution should provide out-of-box patch assessment without the need to schedule and maintain the patch or inventory scan process.		
2	The agent should report the assessment automatically within minutes once the server has distributed the new patch metadata/signatures.		

3	The solution shall use all of the following methods to determine if a patch has been installed on the client:		
	a. Inspecting the registry.		
	b. Examining if the required files exist.		
	c. Inspecting the version number of existing files on the agent. OR		
	d. Any proprietary method (in addition to the patched OEM's specified method) to check the installation of the patch		
4	The solution should be able to determine patch dependencies prior to the deployment of patches to the desktop.		
5	The solution should be able to determine if a patch has already been installed on a desktop.		
6	The solution should be able to determine if a newer patch has been installed on the desktop and if so, the system shall treat the desktop as patched.		
Patch Deployment			
1	The solution must provide the ability to group computers manually and dynamically based on asset and software information.		
2	Descriptions and severity levels of the patches shall be available within the Solution. A hyperlink to the patch information on software vendors' websites shall be provided.		
3	All patches shall be tested based on standard practices before the patch information is made available and notifications shall be informed of any problems encountered during testing.		
4	The solution must allow the console operator to deploy patches to all computers or target specific computers to deploy the patches via a central console.		
5	The solution must allow the console operator to deploy patches without intervention from the users.		
6	The solution must allow the console operator to define different patch deployment policies & create custom policies.		
7	The solution must be able to provide real-time (within minutes) patch deployment status monitoring.		
8	The solution must allow console operators to deploy multiple patches at one time without the need to restart the computers.		
9	The solution must allow console operators to spread the patch deployment over a pre-defined period of time to reduce the overall impact on network bandwidth.		
10	Allow console operators to customize the message displayed in a pop-up message box to all users before the installation of any patch.		
11	Allow admin users to postpone the deployment of a patch for a period of time determined by the console operator.		
12	Allow admin users to postpone the restarting of their computers for a period of time determined by the console operator		
13	Able to re-deploy the patch on a computer automatically if the initial deployment is not successful or uninstalled by the user.		
14	The solution should support patching for a range of standard desktop applications from various vendors e.g. Microsoft, Google, Mozilla, Real Networks, Apple, Sun, Oracle, etc.		
15	Able to cache the patches in the various Distribution points.		

16	Able to install all previously deployed patches automatically to computers that are subsequently added to the network.		
17	Able to delete the patch installation files from the computers' hard disk automatically once the patch has been successfully applied.		
18	The administrator must be able to target the particular patch on all the machines with any specific properties.		
19	The system must be intelligent to check the relevance of the computer before deploying a patch after downloading on the endpoint.		
20	Solution shall support Out of window deployment for patching		
21	Solution shall identify the EOL of Windows OS machines among the managed devices.		
22	Solution shall provide option to shutdown databases and/or specific services.		
Patch Rollback			
1	Solution shall identify computers needing a patch rollback and console operators monitor the process, and able to report if the rollback is successful.		
Asset Inventory Requirements Asset Discovery			
1	The solution should provide a method to install the agent where applicable.		
2	Provide a wizard for console operators to configure and schedule scans.		
3	The 'scan point' should only upload the differences from the last scan.		
Hardware Inventory Management			
1	Able to retrieve hardware asset information from the systems which have the agents installed without the need of scheduling an inventory scan.		
2	Inventory changes should be automatically processed at the agent and sent to the server without operator intervention.		
3	All hardware asset information shall be recorded in the management server and some of the basic information shall include but not limited to:		
	· CPU speed and type		
	· Hard disk space		
	· Computer name		
	· Computer model		
	· IP address		
	· Operating System		
	· Attached peripherals		
4	Allow the console operator to create custom queries on hardware asset information retrieved by the agents.		
5	Able to dynamically group computers based on the hardware asset information.		
Software Inventory Management			
1	Able to list all software and applications, including version numbers, which are installed on the agent.		
2	Inventory changes are automatically processed at the agent and sent to the server without operator intervention.		

3	Able to list all software and applications installed for a group of computers, including the number of installations for each software and application.		
4	Able to list all services running on a particular agent.		
5	Allow console operators to edit the registry entries of selected computers via the central console.		
6	Allow console operators to create custom queries on software inventory information retrieved by the agents.		
7	Allow console operators to create custom actions to be performed on computers (e.g. Stopping a service)		
8	The Analysis should include the following information (but not limited to) with the ability to drill down for more detailed views:		
	a. Publisher name		
	b. Software title name		
	c. Software title version		
	d. Total computers Count		
9	Web UI should allow Role Based access to allow or restrict users' privileges by their role.		
10	Web UI should have the ability to view, filter, and sort upon user input to create custom reports.		
11	Ability to view all properties & raw data gathered from the agent during the inventory process.		
12	Ability to create groups based on inventory properties like (but not limited to):		
	a. Subnet Address		
	b. Operating System		
Software Distribution Requirements			
1	The solution supports the deployment of multiple packaging formats including but not limited to EXE, MSI.		
2	Allow console operators to distribute third-party or in-house software to targeted computers.		
3	The solution should provide a wizard-driven approach that allows console operators the ability to configure package information and target the applicability of the software distribution packages.		
4	Ability to add the software to portal that allows the end user to install any/all pre-defined software packages assigned to the device.		
5	The software distribution solution shall not require the installation of a separate agent on the system.		
6	Allow console operators to specify the deployment success criteria.		
OS Deployment			
1	The solution should be able to perform online and offline image creations		
2	The solution should be able to perform user profile backups on target machines		
3	The solution should be able to create multiple deployment templates for deployments		

4	The solution should support post deployment activities like 1. Computer name change 2. Generate new SID 3. Add machines to Domain and OU 4. Create new Local and Domain user accounts 5. Restore User profiles		
5	The solution should support installing various drivers and applications during post deployment process		
6	The solution should support multiple bootable media like PXE, USB and ISO		
7	The solution should support remote office with Distribution Servers to replicate images and drivers		
8	Ability to perform zero touch deployment without manual intervention		
9	Ability to perform standalone deployment to WFH users		
10	Ability to perform deployments using passcode and template selection		
11	The solution must have effective driver management to automatically collect drivers from target machines and install required drivers during deployment process		
Remote Control			
1	This module is expected to take complete desktop control of Windows desktops/servers from a central location.		
2	It shall support security-related features for taking the control of remote PCs, based on predefined policy and authorization.		
3	The solution should support 256-bit Advanced Encryption Standard (AES) encryption protocols during remote access operations.		
4	It shall provide flexibility with respect to the type and capability of the remote control session like:		
	(a) Full control of the remote PC not only in client server mode but also over the Web		
	(b) Monitor-only-mode.		
	(c) It shall support locking of keyboard and mouse of the remote PC.		
	(d) It shall support interactive chat facility and should log the chat session		
	(e) It shall support file transfers		
5	The Remote Control should be a policy-based remote management solution to facilitate the use of a set of rules to manage IT resources. The Remote Control should also allow IT managers to set policies that are centrally defined, managed, and stored; and determine who will be allowed to access which targets in what manner.		
6	Roles should be used to restrict the level of operations an administrator can perform. The Remote Control should offer the least the following four roles:		
	i) Control - Take control of the remote machine; execute commands and applications (active state)		
	ii) Monitor - View the display of the remote workstation and monitor activities (monitor state)		
	iii) Reboot - Reboot the remote workstation		

	iv) File transfer - lets you transfer files and directories from endpoint to endpoint		
7	To further protect against abuse, end users should be prompted to relinquish control, and should be able to regain control of their system at any time. Encryption technology should be used to ensure that the controller could be launched only from the Enterprise Management environment. The enterprise-scale remote control solution must enable rapid connection to the right target with the help of an automatically updated searchable list of target system names, enabling the administrator to establish a remote control session by simply clicking the target.		
8	The Remote Control should also be able to create target lists/groups. Lists/groups restrict administrator access to a specific group of machines, increasing security and performance.		
9	Web Browser Interface - Solution should provide a web interface with below mentioned capabilities		
	a. The Remote control module should provide an authorization-based Web Interface for Administrators to facilitate Remote control using a browser. It should support all the functions i.e. Remote Control, Chat, Files Transfer, etc. through the Web Browser Interface.		
	b. It should provide enhanced central logging to track session information including controller ID, target host name, session policies, and auditable events such as user acceptance, file transfer operations, session mode changes, and chat transcripts.		
	c. It should provide collaboration facilitates for improved problem resolution.		
	d. It should provide Active Directory authentication and data synchronization.		
	e. It should provide full data stream encryption for all communications and file transfers between controllers and targets.		
	f. It should provide automatic session lock due to administrative inactivity.		
	g. Help desk agents/persons taking the remote control should be able to give control of a problem to another agent or revoke control as necessary. This hand-over should be done without reopening the session, expediting problem resolution.		
	h. It should allow multiple help desk agents to use built-in collaboration capabilities to resolve complex problems that require input from multiple sources, providing the user with a seamless problem-resolution experience.		
	i. It should terminate the remote connections if they are idle for a specific duration.		
10	Does the solution support Wake on LAN functionality to power on devices remotely, even if they are powered off?		
11	Can administrators configure Wake on LAN across different subnets in the network?		
12	Solution shall Kill or stop currently running process in the device.		
13	Announcement shall be deployed to bulk number of users or computers simultaneously		

14	Can the Windows System Tools in Endpoint Central remotely manage processes, services, and software on endpoints without requiring user intervention?		
Software Usage and License usage reporting			
1	Ability to track installed applications on each agent, i.e. Applications that will run only if Installed on the computer		
2	Ability to create License contracts based upon Software Titles that includes		
	a. License cost		
	b. License count		
	c. Purchase and expiration dates		
3	Ability to create License Compliance reports based on the details specified in License Contracts that were created.		
4	The product must be capable of generating software usage metering reports for Windows.		
5	The product must be capable of generating license compliance reports for Windows /Linux and Other Major OS platforms available in the market.		
8	The solution shall discover the computers' compliance status with security configurations and achieve 100% compliance.		
Reporting Requirements			
1	The solution shall include a web-based reporting module.		
2	Information reported shall not be more than 1 day old for devices that are active on the network.		
3	Access to reporting function shall be controlled based on rights assigned by the Master Administrator.		
4	The reporting module shall contain, but not be limited to, the following reports: Progress of all patches applied:		
	i. Number of vulnerabilities detected by month		
	i. Total number of computers managed and the distribution of these computers		
	ii. Top 10 most common vulnerabilities detected		
	iii. List of software installed on each agent		
5	Allows console operators to create and save reports from a list of built-in default reporting templates as well as the flexibility of creating & generating custom reports.		
6	Allow console operators to customize and save the reports without the use of third-party reporting tools.		
7	Able to generate reports on Hardware and Software inventory information.		
8	Allow console operators to generate customized reports on Hardware and Software inventory information.		
9	Able to generate reports on asset properties that are fetched by the agent.		
10	Allow console operators to create filters to include or exclude certain categories of information from the reports.		
11	Allow console operators to drill-down from the report to the specific computers.		
12	Allow console operators to schedule report generation.		
13	The Tool should be able to provide/maintain report data from the implementation date		

14	Solution shall have the ability to retrieve the required information from the database using the Query.		
Mobile device management			
1	Supported Operating System - iOS / iPadOS, Android, MacOS, Windows 10 & 11, tvOS, Chrome OS		
2	Configurations - Passcode, WiFi , VPN, Per-App VPN, Web content filtering, Wallpaper, Web shortcuts, Certificate management, Restrictions, Shared device configuration, Filevault encryption, Firmware password, Custom configuration		
3	Application management - Apple VPP (ABM), Google Play for Work, Chrome Web Store, Windows Business Store, Silently install/uninstall applications, Blocklist applications, Manage enterprise/in-house mobile apps, Schedule & automate app updates		
4	App lockdown - Single app kiosk, Multi-app Kiosk, Home screen layout - supported for mobile devices		
5	Inventory Tracking - Comprehensive insights on hardware and software inventory, Detect and remove jailbroken and rooted devices, Geo location tracking, Procurement of location history for mobile devices.		
6	Asset Management - Corporate data wipe and complete data wipe, Remote alarm, Remote lock, Lost mode, Reset/clear passcode, Remote restart/shutdown, Scan		
7	Update management - Automate OS updates for mobile devices		
8	Device Enrollment(BYOD) - Self Enrollment, Enrollment via E-mail & SMS, Bulk Enrollment, OS independent invites Other device onboarding methods - Apple - DEP (ABM), Apple Configurator, Android - EMM Token (QR) Enrollment, Zero Touch Enrollment, Samsung Knox Enrollment, NFC Enrollment Windows - Azure AD Enrollment, AutoPilot Enrollment, Windows ICD Enrollment, Chrome enrollment		
9	Email Management - Configure enterprise E-mail accounts, Microsoft Exchange ActiveSync, Conditional access to Exchange, Conditional O365 access, Conditional O365 MAM policy Conditional access using Azure AD CBA		
10	Tools - Announcement, Alerts, Battery level tracking, Remote view/control		
11	Content Management - Distribute corporate files, Document viewer		
12	Telecom expensment - Track mobile data usage on the mobile devices		
13	Shared device management - iPads, Android and Windows PC		
14	Self service app for mobile devices		
15	Geofencing - Geo fencing for mobile devices		

Integrations			
1	Solution shall integrate with ITSM solutions for capabilities to streamline the process, including ticketing, assignment, tracking, Asset life cycle management and verification.		
2	Users need to adjust the integration settings in the ITSM solution to meet their specific operational needs, such as mapping fields, defining workflows, and automating data synchronization.		
3	SIEM integration shall supports Event log management, compliance tracking, and reporting .		
4	Vulnerability assessment Integration shall supports vulnerability management, including the synchronization of vulnerability data and the automation of remediation tasks.		
5	Solution shall facilitates easy integration with infrastructure using REST APIs.		
Product accessibility			
1	Web interface - Access the Solution's console from a web browser.		
2	Mobile interface - Access the Solution from a mobile device.		
3	Customizable feature accessibility - Enable the products features for users belonging to specific Remote Office, Static unique Custom groups and all computers.		
4	Multiple access media for Solution - Shall access Solution via Web app, Mobile apps, API access.		
5	Multi-language support: The product is available in the following languages: English Japanese Turkish Swedish Spanish Russian Polish Italian German French Finnish Dutch Danish Chinese Brazilian Portuguese Norwegian Portuguese Traditional Chinese Korean Hungarian Czech		
Training			
1	Instructor led certified training session for 5 users		
Required Document			
1	Vendor should be provided the manufacture Authorization letter from principle		

Annex 3

"قَوِّمُوا 5 اَلْاَشْهُوَرِ فِى اَلْاَسْهُوَرِ فِى اَلْاَسْهُوَرِ فِى اَلْاَسْهُوَرِ فِى اَلْاَسْهُوَرِ 10 وَسُورَةُ"

#	دستورالعملی که خوانم	دستورالعملی که میخوانم	دستورالعملی که میخوانم
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

[illegible]

		٢٠٢٤ ٢٠٢٣ ٢٠٢٢	
		٢٠٢٤ ٢٠٢٣ ٢٠٢٢	٢٠٢٤ ٢٠٢٣ ٢٠٢٢