

Max Secure Cloud Site Administrator Guide



AI Powered Cloud / On Premises Anti-Virus for End Point Protection

Version 10.0.019 May 2022

Deliver layered security services to multiple offices, networks and devices, with a single Cloud-based centralized Management platform offered as a service or On-premises

For Windows, Mac, Linux and Android

Privacy and Data Collection Disclosure

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. If you have questions, comments, or suggestions about this or any Max Secure Software document, please contact us at tech@maxpcsecure.com.

For online installations, Max Secure Threat community, Threat Intelligence, Sandboxing and Artificial Intelligence models collect and send probable malicious data and detection information to Max Secure. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Max Secure to collect personal data, you must ensure that you disable the related features from Policies on the Cloud Security dashboard after installation. To do this Go to Manage → Policy → Click on any existing Policy → uncheck Threat community and Threat Intelligence.

Live update downloads updates on malware definitions and product upgrades from our servers and CDN. This data is malicious code free as to the best of our knowledge and understanding. We will not bring malicious content to your PC or servers.

For offline installation, on your premises we do not collect or send any data outside your network. You download updates on any external windows or Linux PC, using our live update tool and copy the updates to the Update folder on the PC where Max Cloud Security is installed. Similarly, Windows Patch management tool downloads updates on external PC having Internet. After download updates are copied on the Cloud Security server. Server pushes these updates to client agents using web APIs and client agent installs and updates the client's devices. This data is malicious code free as to the best of our knowledge and understanding.

The following link outlines the types of data that Max Secure collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://www.maxpcsecure.com/privacypolicy-EndpointSecurity.htm>

Document Update Date

May 12, 2022

Table of Contents

Cloud Security Portal Registration	6
Sign-In to the Admin Portal	9
Enabling 2-factor authentication (2FA)	9
Dashboard	10
Profile picture and Logo	11
Notification Alerts	12
Most recent Alerts on Dashboard	13
Detail Dashboard	13
Monitor	15
Detection	15
Alerts Management and Notifications	23
Reports	24
Manage	25
Endpoints	25
Add Devices	26
Key Generation and Active Directory	42
Actions	56
Zero Trust	70
Policy	72
Scan Settings	75
USB Manager	77
Firewall Policy	78
Configurations	81
Application Whitelist	82
Back-up & Restore	83
Exclude Folder	86
File Block	86
Folder Vault	87
Hash Block	88

Instant Remediation.....	89
Ransomware	90
Scheduler	92
USB Whitelist	93
Wi-Fi Whitelist	94
Tasks	95
Content Search	95
Broadcast Message	99
Share Files.....	100
Send Command.....	100
Groups	101
Data Loss Prevention (DLP).....	103
Update Management.....	106
Vulnerability Scan	106
Software Updates	107
Full Disk Encryption.....	110
Inventory Management.....	111
Hardware Inventory	111
Software Inventory	114
Device Control.....	115
File Integrity Monitor.....	116
FIM Policy.....	116
FIM Rule	117
FIM Details	118
Endpoint Forensic	119
Endpoint Security Posture	121
Setup	123
Uninstallation Protection.....	123
License Management	123
Manage Registration Keys.....	123
About Registration Keys	124

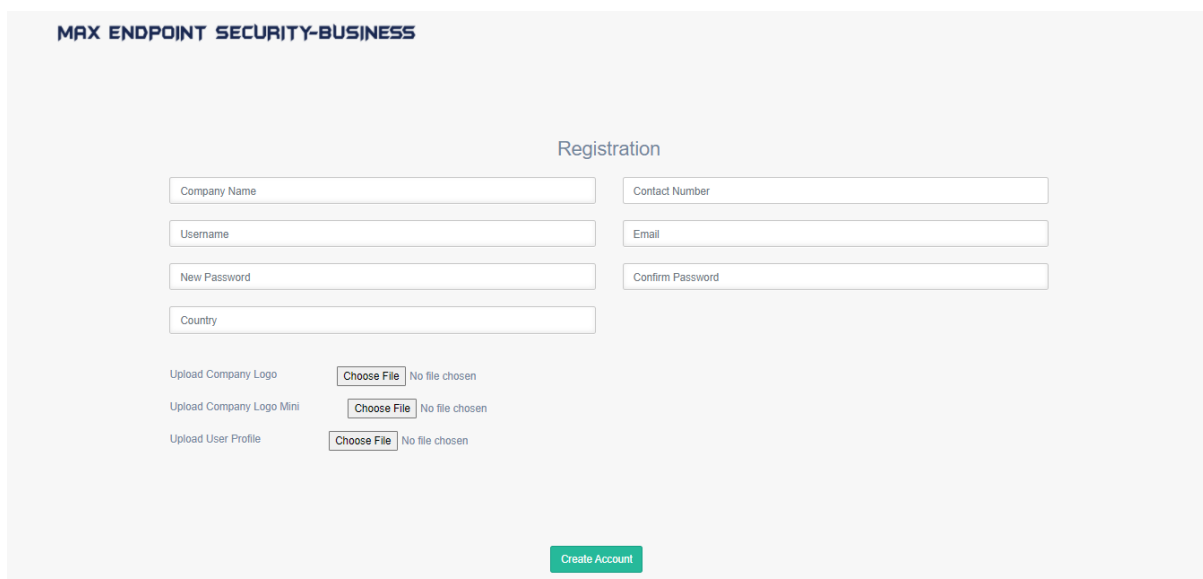
Client Agent Installation Token Information.....	127
Email Settings	128
User Management.....	129
Distribution Packages	133
Contact Us	133

Cloud Security Portal Registration

This Portal is a web-console available on our Cloud servers offered as SaaS. You can also choose to install it on local network for total privacy, for specific requirements such as Defence or Government organizations who prefer to keep their data away from any internet. On-Premises installation provides all of the features as on our On-line server Portal. Use it the way you prefer it. On-Premises server can be installed on any operating system starting from windows 10 onwards, requires IIS. For up to 1000 clients no SQL server license is required on Client site.

Getting started

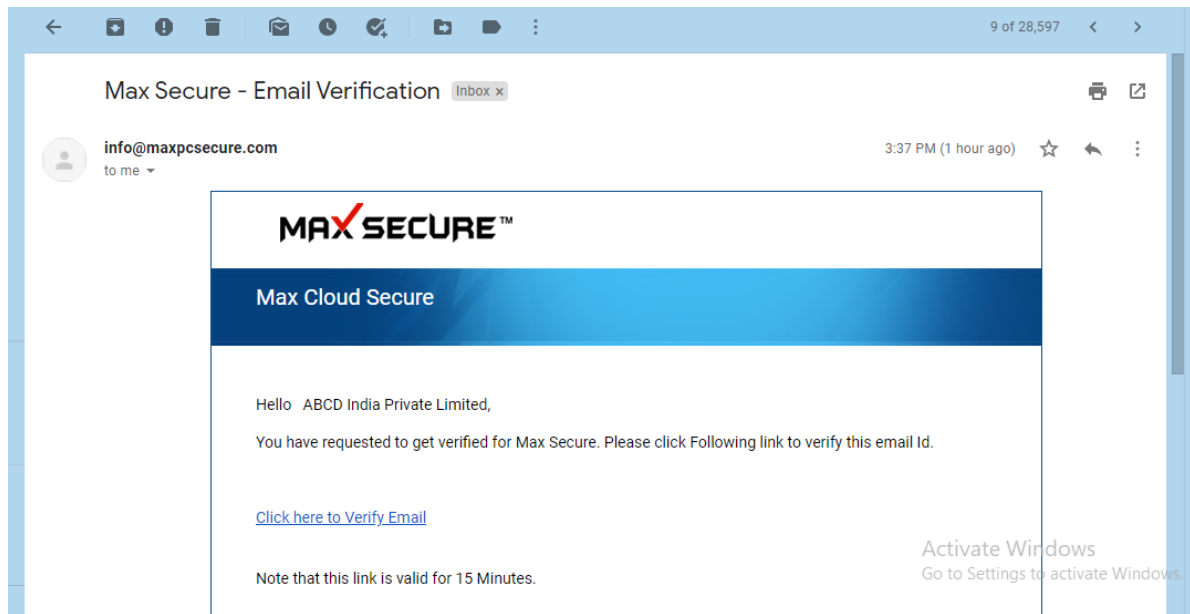
1. If this is your first time coming to this site, you need to do register your company first.
2. Browse <https://maxsecurecloud.com> and click on 'Register For Free'.
3. To create an account you need to fill up the form, follow the instructions, and create user name and password to login to the Dashboard.



The screenshot shows the registration page for MAX ENDPOINT SECURITY-BUSINESS. The page has a light gray background with the product name in the top left. The registration form is centered and includes the following fields and options:

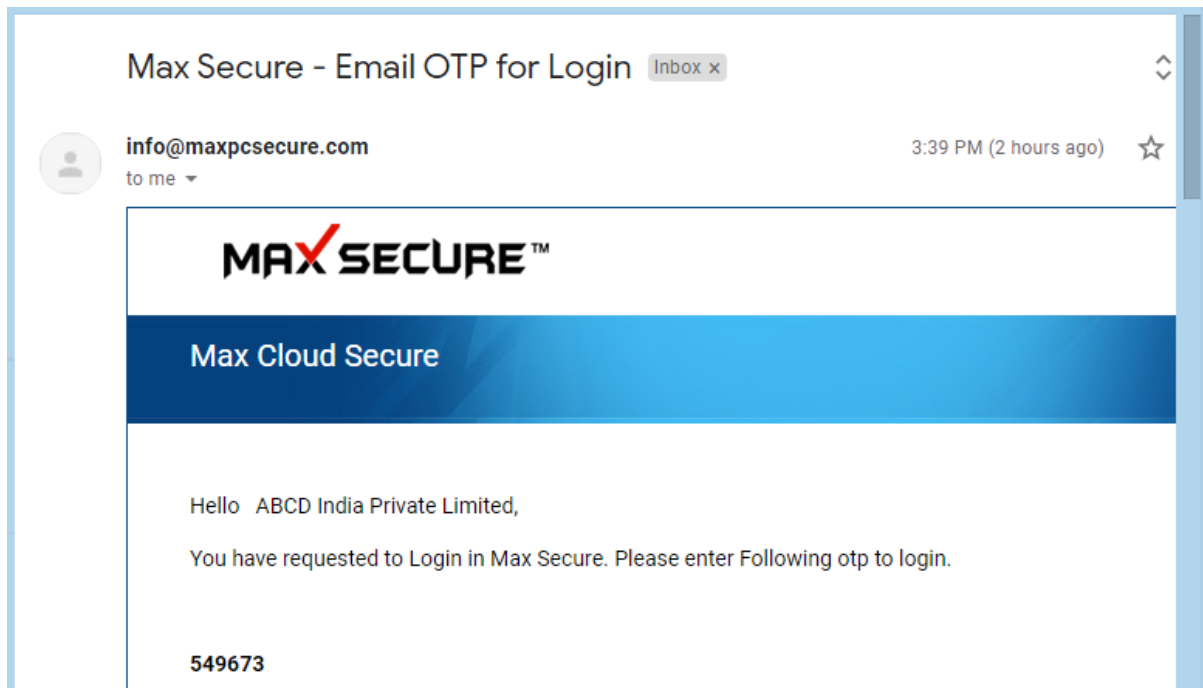
- Registration** (Section Header)
- Company Name** (Text input)
- Contact Number** (Text input)
- Username** (Text input)
- Email** (Text input)
- New Password** (Text input)
- Confirm Password** (Text input)
- Country** (Text input)
- Upload Company Logo** (Text label) with a **Choose File** button and "No file chosen" text.
- Upload Company Logo Mini** (Text label) with a **Choose File** button and "No file chosen" text.
- Upload User Profile** (Text label) with a **Choose File** button and "No file chosen" text.
- Create Account** (Green button at the bottom right).

4. You can customize web experience by uploading your company logo, small logo and your photo now or choose to do it later after you have logged in.
5. After creating an account, you will receive an email which you need to verify by clicking into the provided link.

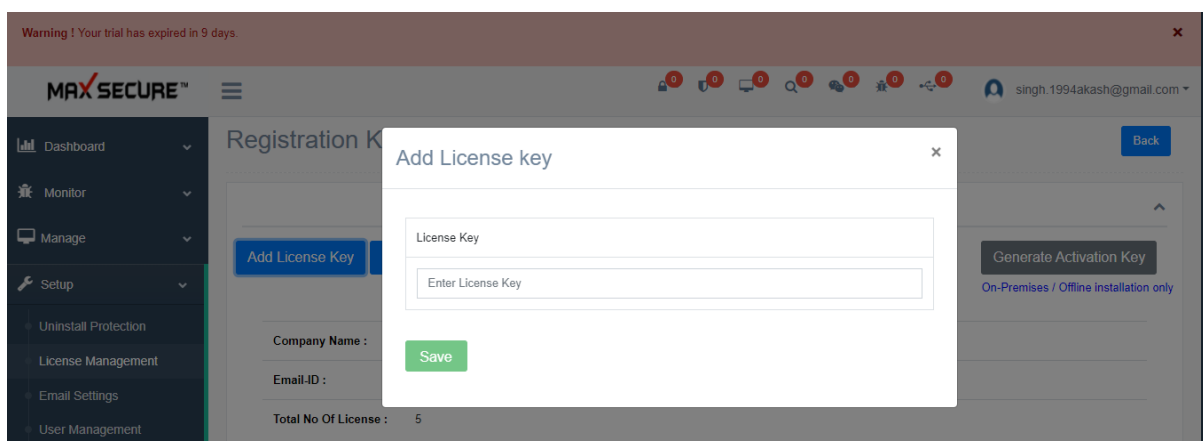


6. Just after clicking on the link, you will receive an email which contains your login OTP to verify for authentication which you need to enter within 30 seconds.

7. Click on the 'Click to Login' button after entering valid OTP, then will redirected into the Login Page.



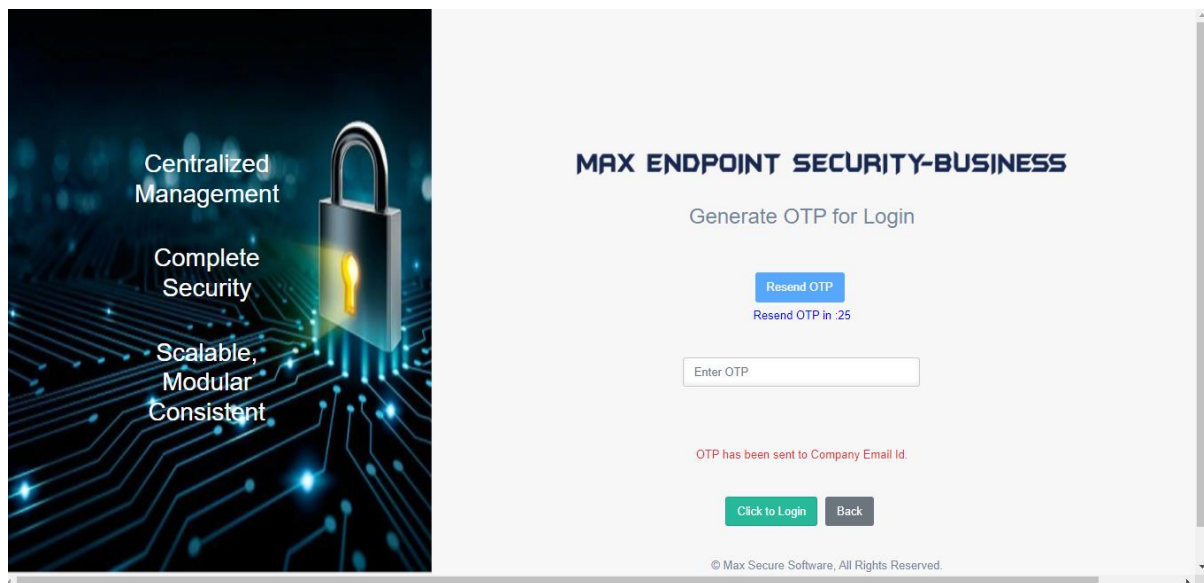
8. Now you can log in to the portal, enter valid username and password that you entered at the time of registration for successful login.
9. By default you will get 10 days free trial period for 5 Clients.
10. You will also need a 'License Key' for successful registration. You can get this key after purchasing a license from Max Secure Software.
11. When you buy a new license, you need to activate. To activate a license, do as follows.
 - A. Ensure you have the license key from Max Secure Software only.
 - B. Now Admin needs to sign in to the portal.
 - C. Go to right side tab click on *Setup*→ *License Management*→ click on 'Manage License' button→ click on 'Add License Key' button.
 - D. Enter valid key now to get the registration process completed. Copy and paste the Registration Number to ensure exact data entry, do not try to type it in.



Sign-In to the Admin Portal

Max Secure provides 2FA stands for Two Factor Authentication

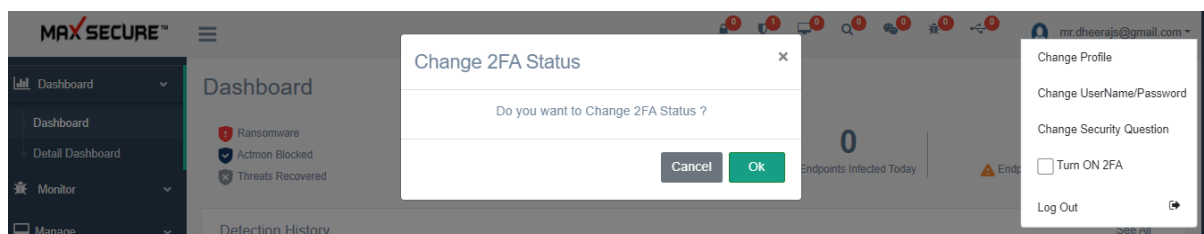
When two-factor authentication is enabled, you must provide a unique, one-time verification code as well as a password when you log on to Max Endpoint Security-Business Portal. You will receive an email which contains your login OTP to verify for authentication which you need to enter this OTP into the portal within 30 seconds.

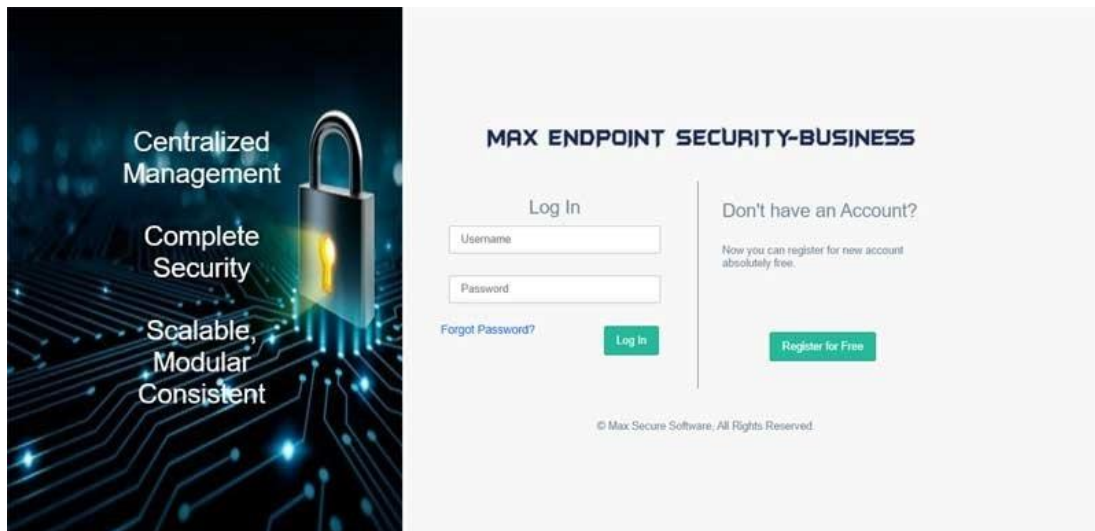


Enabling 2-factor authentication (2FA)

Step to enable 2-Factor Authentication:

1. Login to the Cloud Security Dashboard
2. Click on the profile tab present at top right corner of the page.
3. Click on Turn ON 2FA
4. Click on OK into the alert pop-up





Dashboard

Once you have logged in, you will be presented with a graphical chart, which would give you birds-eye view of all-important events happening on the Client devices.

This chart will populate data once you have added Devices and scanned them or performed other Actions. Even if you do not apply any policy, several features would start working as soon as you have installed client agent such as Malware scanning, Inventory management, Data back and Restore, Vulnerability scan right after installation and at default scheduler of 11 AM. You have options to change the scan schedule from Configuration menu.

You have option to search on dates for which you would like to see summary on the chart, by default it shows last 10 days data. On the top of the chart, you would see today's summary of important report blocks such as Total endpoints, Malware found today, Endpoint infected today and Endpoints scanned today.

All the results, such Total Endpoints=9, is clickable and open in a new tab to show you further details. Clicking on any alert icon opens reports in a new tab, where you can see full details on that alert.



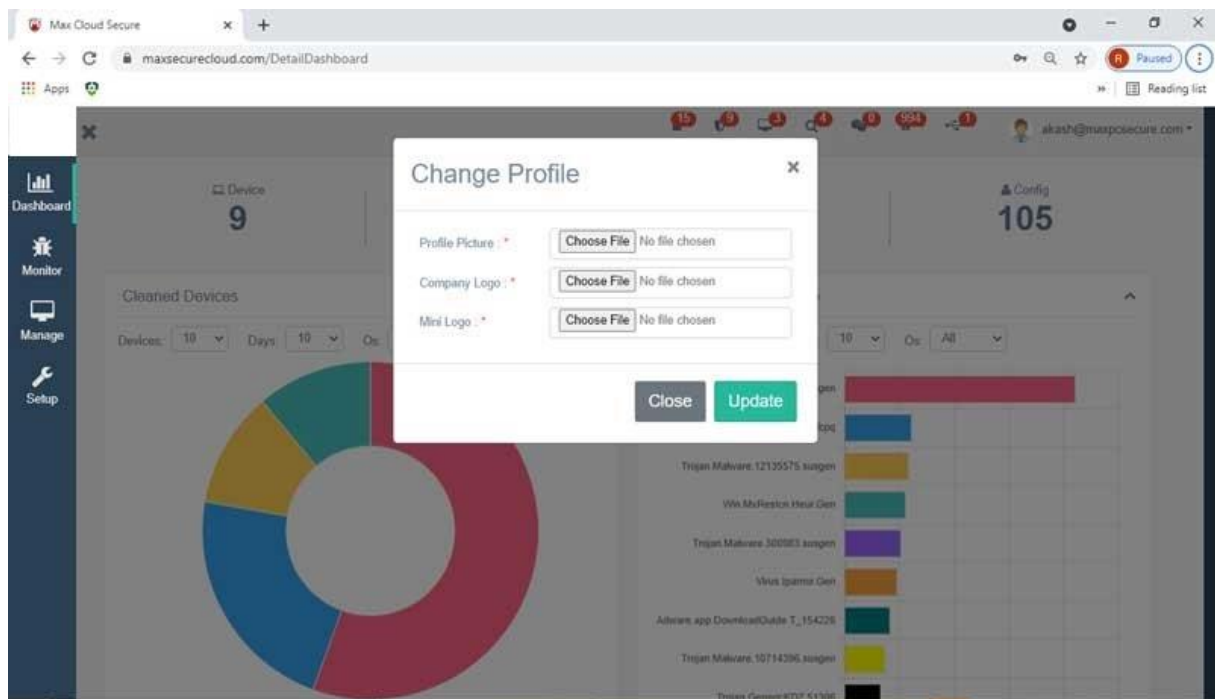
Profile picture and Logo

Clicking on Admin picture on the top right corner → Select Change Profile will allow you to customize the portal and make it friendlier by adding your company logo and admin picture.

Choose this option anytime to change the images whenever you need it.

Clicking on hamburger button (3 horizontal parallel lines) on the top left menu bar, next to company logo, Max Secure in this picture, shrinks the left menu bar and allows you the full screen view of the Dashboard.

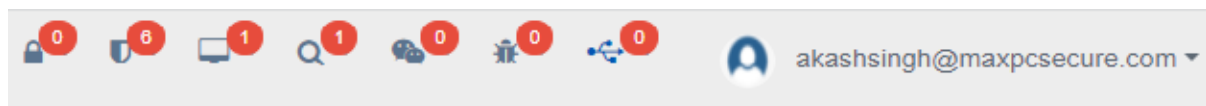
Here you can only see your company mini logo that you provided at the time of registration or you can change by clicking on profile on the top right hand corner of the Dashboard.



Notification Alerts

You would see important notification alert icons in red colour on the top bar of the Dashboard.

Hover over any icon you can see what information it has. Following alerts are provided on the top menu:

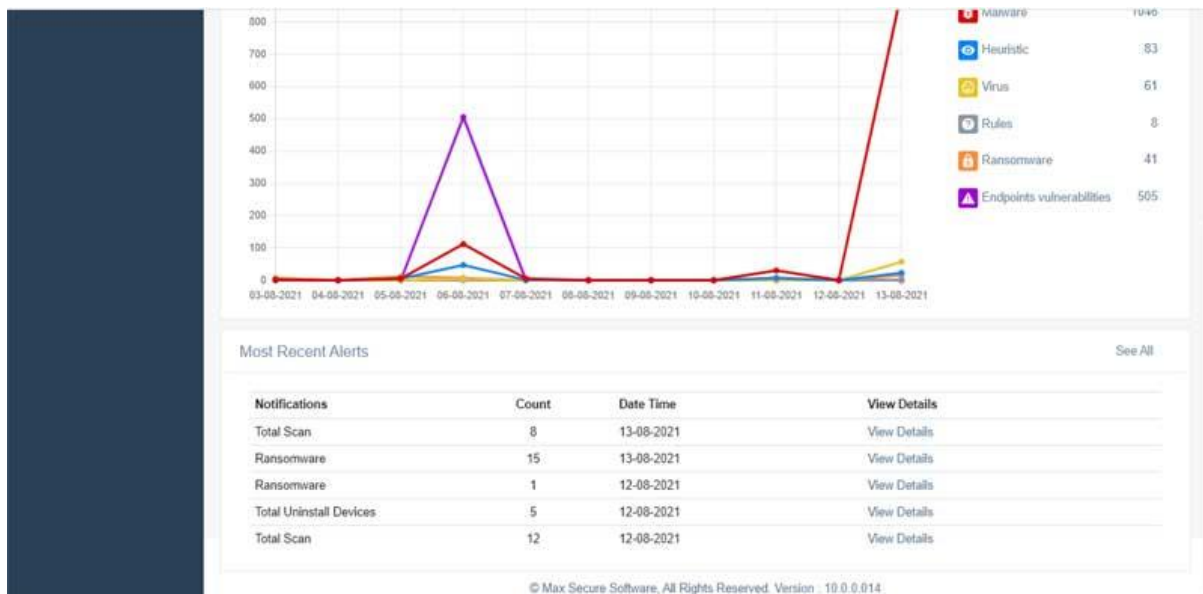


No.	Description
1	Ransomware found today
2	Real-time Protection Off Alert
3	Devices which are online
4	Total devices scanned today

5	Total messages received today
6	Total Malware found today
7	Total USB device attached today

Most recent Alerts on Dashboard

You would see 'Most recent Alerts', at the bottom of this master chart as you scroll down. Each alert is clickable and opens in a new tab to show you full details of that alert. Alerts are managed for total Devices scanned, Ransomware found, total uninstalled devices, Vulnerabilities found and total messages sent or received and total DLP violations found today.

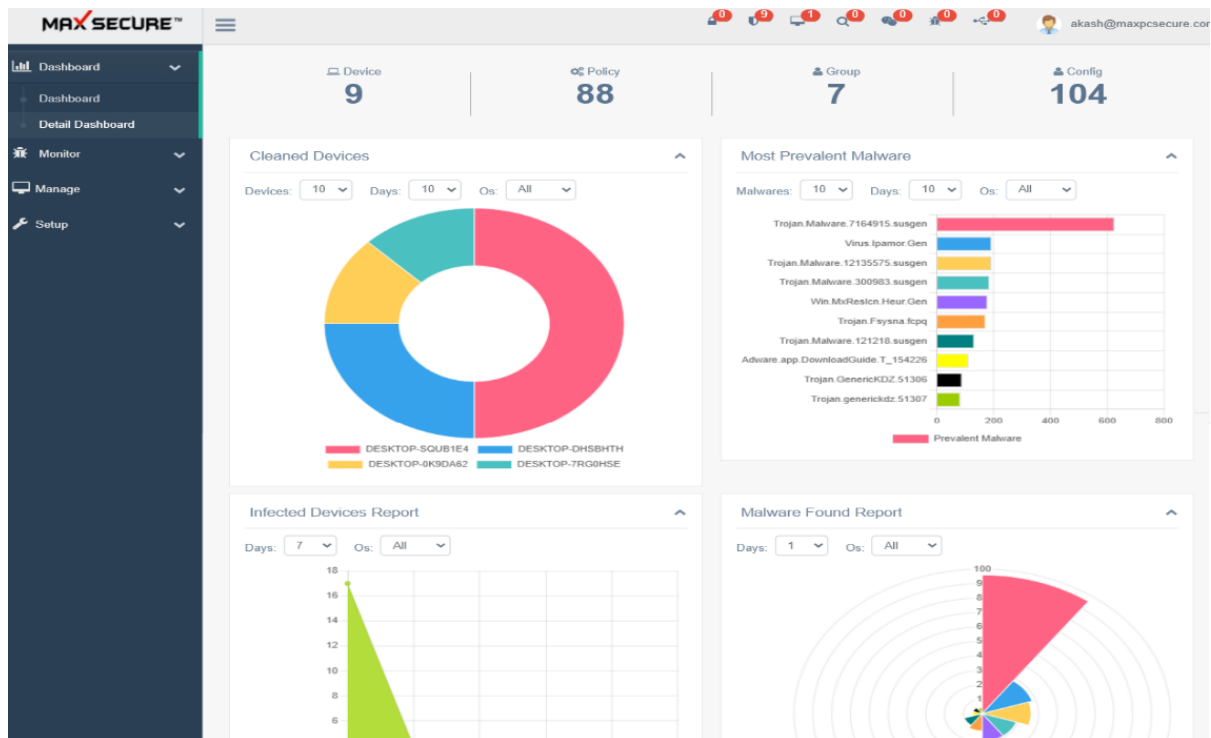


Detail Dashboard

There is yet another group of charts provided to help admin get birds-eye view of various security parameters in one place quickly.

You can see following parameter Charts here:

No.	Parameters	Description
1	Cleaned Devices	Devices, which were found to have malware presence and now clean after scan and quarantine of malware. You have drop down selection to choose count of devices or No of Days reports here.
2	Most Prevalent Malware	You could select how many malware or days report you would like to see here
3	Infected Device Report	By default, we show you this Chart for the last 7 days but you could choose no. of days to see different report.
4	Malware found	Count of total malware found in the last 30 days. You could see different Chart by selecting no of days from the drop down from 1-150 days
5	Online vs. Offline devices:	You can see how many Devices at this time are Online or Offline.
6	Clean vs. Infected Device	This Chart shows, in the last scan how many devices were found to have no malware vs. how many devices were found to have presence of Malware.



Monitor

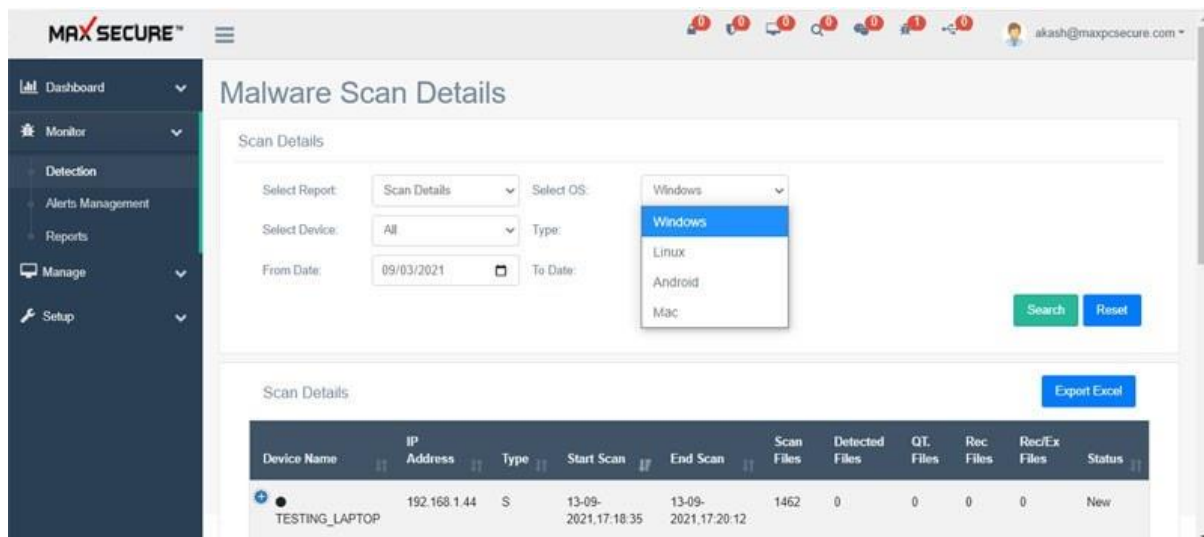
From this menu, you can view all the activities that have happened on the client devices. Easy and quick searches will give insight into different scan details.

Detection

Note: Main difference between Detection and Reports is that, for searches under 'Detection' Admin can apply Actions such as Get File, Recover etc. whereas 'Reports' results are only for viewing purpose.

Here you will see in detail all the malware related scan results and be able to Recover/Exclude/Get File to the server etc. You can choose which OS results you would like to see from the drop down list of "Select OS".

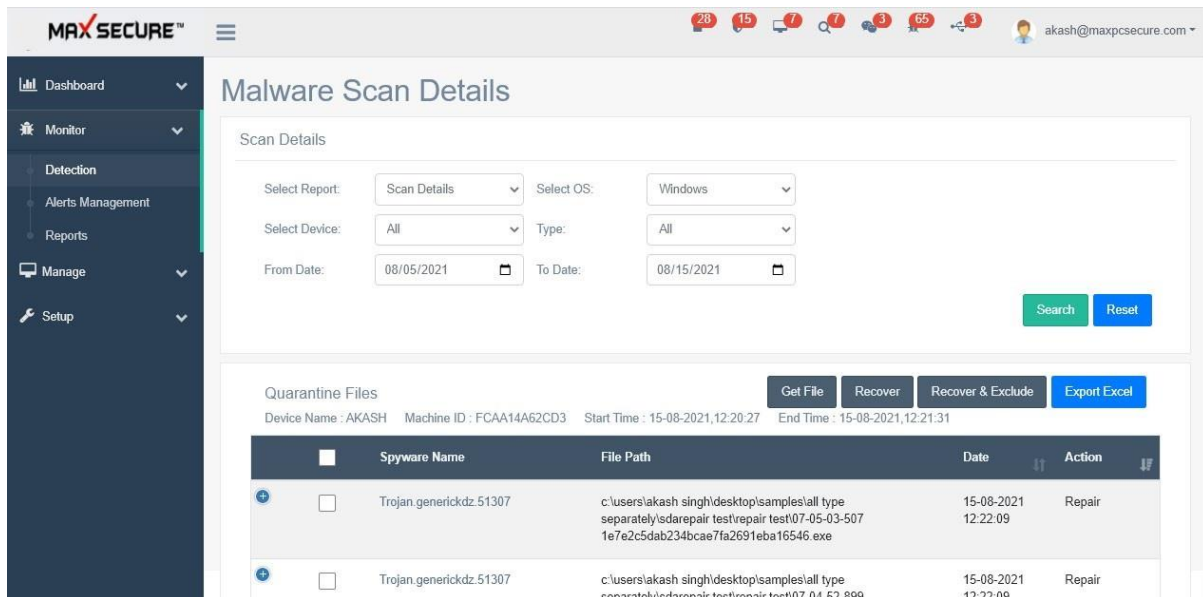
1. Scan Details provide full information on Devices by device name, IP address, Start Scan, End Scan time, total files scanned, total files detected by Anti-virus scanner, quarantined files, recovered files or recover/Exclude files (This can be done by Admin from here. He can click on quarantined files count for any device and select Action such as Get File/Recover/Exclude etc.) and Status such as deleted, repaired or failed to delete.



- 1.1 In any type of search here, you can click on QT. Files (quarantined or deleted files) count or detected files count shown in blue.

DESKTOP-BJ0B94R			2021,12:32:33							
AKASH	FCAA14A62CD3	S	15-08-2021,12:20:27	15-08-2021,12:21:31	15	15	15	0	0	New
MIRAJ_MR	BTNL82100BT1	S	15-08-2021,12:19:23	15-08-2021,12:21:40	9	9	9	0	0	New

- 2.1 Clicking on any of them opens another page with more details on file path, Action taken by scanner and malware name.



- 3.1 This is the Action page and you can use the following features:

No.	Description	Monitor→ Detection
1	Get File	Select one or more check boxes on the left and click Get file to upload the files from the device to the End Point server.
	<i>Use case for Get File</i>	Now admin can download the file and study if he has any doubt about that the file is malicious or not. He may want to do this for example if he suspects any false positive.
2	Recover	Select any check box and click Recover. By doing this device will get this file back on his file system from our quarantine vault. Note: Recovered file will again be detected by active monitor or Scan. IF you do not ever want to scan this file then select Exclude/Recover option

	<i>Use case for Recover</i>	If file is false positive (a white file detected as Malware) or it is a malicious file but for any reason device user wants the file back.
3	Recover / Exclude	Admin can select one or more check boxes and select this option. Excluded files will not be scanned by our scanner, if you perform this action on any file. Not recommended, use this option judiciously, as a malware file will spread infection and our scanner will not detect it as Admin has chosen to exclude it.

Here you can find all the details on the Devices scanned, Malware found, search by Malware name or Family name or PE Hash signature of the Malware.

Use our PE creator tool to create PE Hash signature of any file or grab PE signature from any Malware file already scanned and reported to the dashboard.

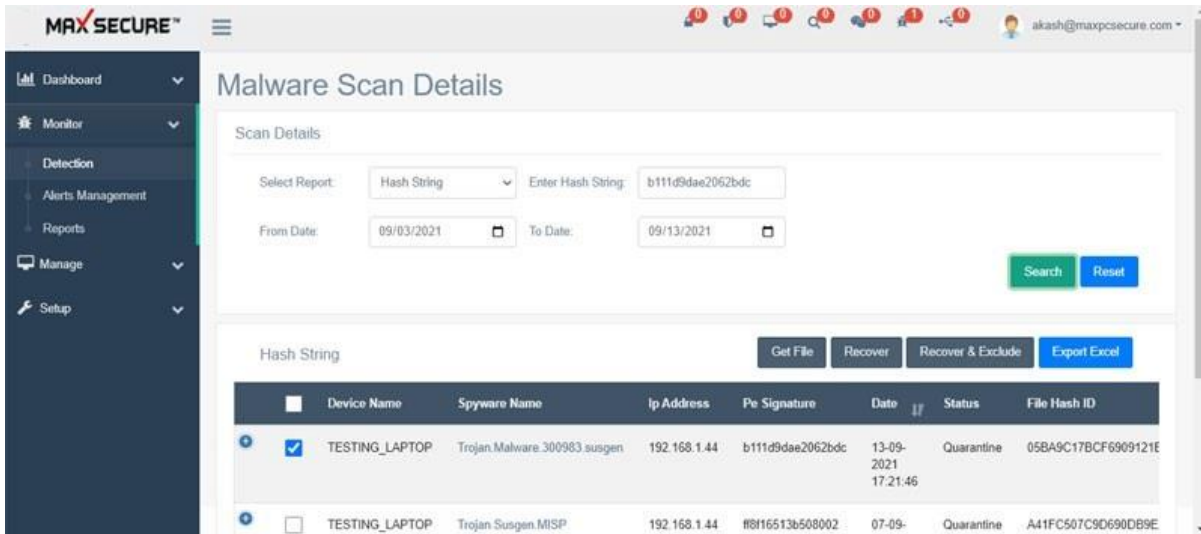
- Scan Details
 - Search on Malware found and view their information on Encyclopaedia.
 - Find which Malware were found on which device and action taken.
 - You can also Recover that file if you think that it was false detection
 - After search on any file, you can also click on Exclude/Recover button on the bottom of the page so that from now onwards that file will not be scanned by scanner and will be whitelisted
2. Drop down option under “Select Report” gives you flexibility to search data on different parameters:

Device Name	IP Address	Type	Start Scan	End Scan	Scan Files	Detected Files	QL Files	Rec Files	Rec/Ex Files	Status
TESTING_LAPTOP	192.168.1.44	S	13-09-2021, 17:18:35	13-09-2021, 17:20:12	1462	0	0	0	0	New

3. Malware search: Similar to Scan Details, you can search for Malware found by name or partial name and perform similar actions by clicking on the Malware search result.

Device Name	Spyware Name	Ip Address	Pe Signature	Date	Status
TESTING_LAPTOP	Trojan.Malware.300983.susgen	192.168.1.44	b111d9dae2052bdc	13-09-2021 17:21:46	Quarantine
TESTING_LAPTOP	Trojan.Susgen.MISP	192.168.1.44	#916513b508002	07-09-...	Quarantine

4. Hash String Search : You can search for any Malware by its Hash and take similar actions as in "Scan Details"



Malware Scan Details

Scan Details

Select Report: Hash String Enter Hash String: b111d9dae2062bdc

From Date: 09/03/2021 To Date: 09/13/2021

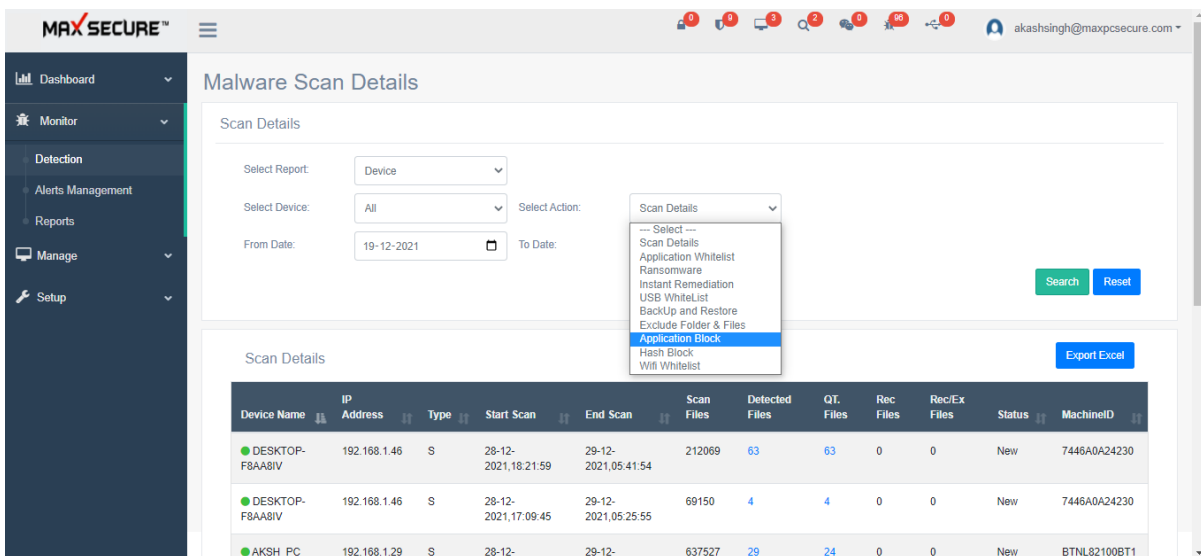
Search Reset

Hash String

Get File Recover Recover & Exclude Export Excel

Device Name	Spyware Name	Ip Address	Pe Signature	Date	Status	File Hash ID
TESTING_LAPTOP	Trojan.Malware.300983.susgen	192.168.1.44	b111d9dae2062bdc	13-09-2021 17:21:46	Quarantine	05BA9C17BCF6909121E
TESTING_LAPTOP	Trojan.Susgen.MISP	192.168.1.44	#8f16513b508002	07-09-	Quarantine	A41FC507C9D690DB9E

5. Under Device option several Actions are available such as Scan Details, Application Whitelist report, Ransomware report, Instant Remediation report, USB Whitelist, Backup and Restore, Excluded Files & Folders report, Application Block report, Hash Block and Wi-Fi Whitelist



Malware Scan Details

Scan Details

Select Report: Device

Select Device: All Select Action: Scan Details

From Date: 19-12-2021 To Date:

Search Reset

Scan Details

Export Excel

Device Name	IP Address	Type	Start Scan	End Scan	Scan Files	Detected Files	Q.T. Files	Rec Files	RecEx Files	Status	MachineID
DESKTOP-F8AA8IV	192.168.1.46	S	28-12-2021, 18:21:59	29-12-2021, 05:41:54	212069	63	63	0	0	New	7446A0A24230
DESKTOP-F8AA8IV	192.168.1.46	S	28-12-2021, 17:09:45	29-12-2021, 05:25:55	69150	4	4	0	0	New	7446A0A24230
AKSH_PC	192.168.1.29	S	28-12-	29-12-	637527	29	24	0	0	New	BTNL82100BT1

6. Device→ Backup and Restore shows you all the devices and their backups by date. Click on Apply can restore the backed up data in the folder and location on the device. By default it runs & admin can also set schedule on demand from Manage→ Configuration→ Add Configuration→ Backup & Restore

The screenshot shows the 'Malware Scan Details' page in the MAXSECURE portal. The left sidebar contains navigation links: Dashboard, Monitor, Detection, Alerts Management, Reports, Manage, and Setup. The main content area has a 'Scan Details' section with filters: 'Select Report' (Device), 'Select Device' (All), 'Select Action' (BackUp and Restore), 'From Date' (06/01/2021), and 'To Date' (09/13/2021). There are 'Search' and 'Reset' buttons. Below this is a table titled 'Device' with an 'Export Excel' button. The table has columns: Device Name, Ip Address, Folder Name, Date, Total Count, Status, and Apply Restore.

Device Name	Ip Address	Folder Name	Date	Total Count	Status	Apply Restore
DESKTOP-0K9DA62	192.168.1.68	29-08-2021 13-01-17_auto	29-08-2021	37	Not Restore	Apply
DESKTOP-0K9DA62	192.168.1.68	29-08-2021 13-01-17_auto	29-08-2021	37	Not Restore	Apply

7. Device→ Exclude Folder/Files: Shows list of files/folders excluded from our scanner. You have an option to choose delete to remove the exclusion from here. Admin can add file/folder exclusions from Manage→ Configuration→ Add configuration→ Exclude Folder

The screenshot shows the 'Malware Scan Details' page in the MAXSECURE portal. The left sidebar contains navigation links: Dashboard, Monitor, Detection, Alerts Management, Reports, Manage, and Setup. The main content area has a 'Scan Details' section with filters: 'Select Report' (Device), 'Select Device' (All), 'Select Action' (Exclude Folder & File), 'From Date' (04/01/2021), and 'To Date' (09/13/2021). There are 'Search' and 'Reset' buttons. Below this is a table titled 'Device' with 'Delete' and 'Export Excel' buttons. The table has columns: Device Name, File Path, Insert Date, and Action.

Device Name	File Path	Insert Date	Action
DESKTOP-OKSKNSQ	e:\deep freeze\faronics deep freeze standardenterpriseserver 8.60.020.5592\faronics_deep_freeze_8.60.020.5592_standard\faronics deep freeze 8.60.020.5592 standard\crack\patch.exe	20-08-2021 13.24.25	Exclude

All the available options of Detection are explained in the table below for your reference:

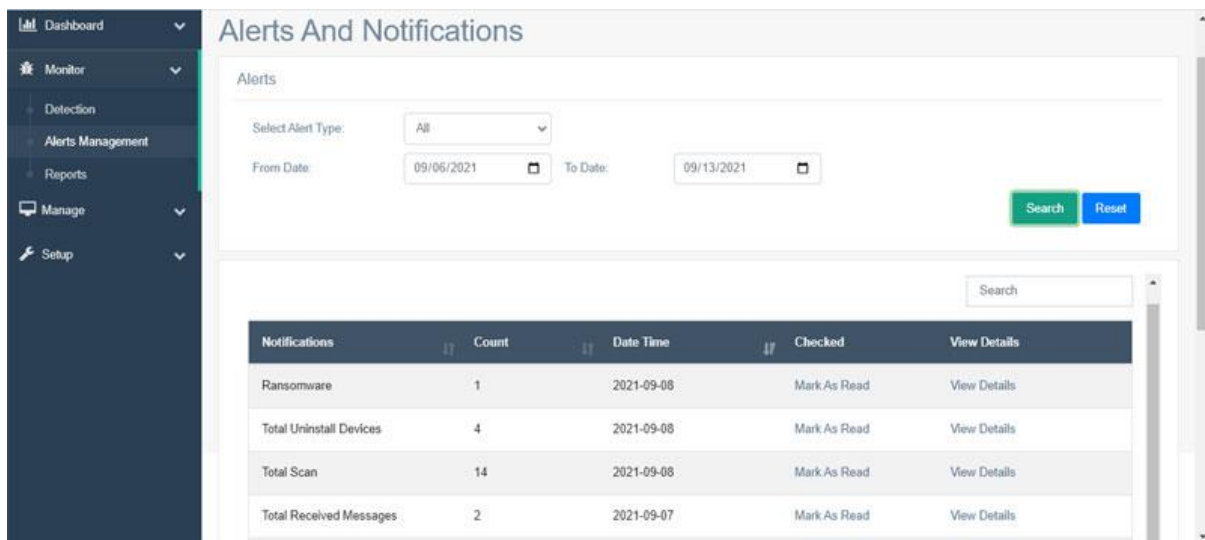
No.	Option	Description
1	Scan Details	Choose Windows, Linux, Android or Mac device from drop down. Select Date for searches. Select all devices or a specific device from the drop down. From Type select →malware found in Scan or Active monitor
	Scan Details→ Windows Scan Details→ Linux Scan Details→ Mac Scan Details→ Android	
2	Malware	This option allows you to search for detected malware by name (full name not required to search) or type of scan detection.
3	Hash String	You can search for any detected Malware by copying the hash value here
4	Device	Search for scan results for a device or All device. Search by selection of Date available.
	Device→Scan Details	Select Date range and find a list of all malware scanned. You can select to get any of these files on the server for analysis or export results in Excel
	Device→Application whitelist	If you white-list any application for a device then only that application (other than Microsoft files) will be allowed to be launched, rest will be blocked from execution. Note: Admin can whitelist Applications from Configurations tab→Application White-list

	Device→Ransomware	Search for all Ransomware found on all devices and Admin can click on Delete to recover them back on the device, if Admin finds that they were legitimate files. Results can also be exported to Excel.
	Device→Instant Remediation	These files have been quarantined by our Ransomware behavior scanner or Pattern scanner or manually added as malware for immediate detection by our scanner by Admin. Note: You can manually add signatures of any malware file from Configuration→Instant Remediation. You need to add PE signature for which we have provided a PE signature creator tool. You can download that from Setup→License Management→Manage License...scroll down to item 7 "creating PE hash signature of any file" under windows installation instructions.
	Device→USB Whitelist	Here you see the list of USB devices which are white-listed. Only these devices will be allowed to be used. You can white list USB from Configuration→Add configuration→choose USB whitelist in the drop down list
	Device→Backup and Restore	See a list of backup done in the past on all the devices. You can recover backed-up data in case you need that. By default data backup is done on selected extension files on the devices. Admin can also choose to add his extension and schedule and back up data storage space and location on his device or network drive from Configuration→Add new configuration→Choose Backup and Restore from the drop down list and modify. Save and then choose "Apply" on selected devices.
	Device→Exclude Folder and Files	You can exclude folders and files which you do not want to be scanned by our Anti-Virus scanner
	Device→Application block	Shows which applications are manually blocked by Admin from execution on selected devices. Applications can be blocked from Policy→Firewall→Application Rule. Once you add applications by name here and apply this policy on selected devices then these application cannot execute on the devices.
	Device→Hash Block	You can block any Malware by giving your own value of 256 Hash. Here you see a report of all Malware detected by Hash value added by you. Note: SHA256 Hash values can be added from Configuration→Hash Block. You can also upload using an excel file or one value at a time.

	Device→Wi-Fi Whitelist	View list of all white-listed Wi-Fi network. Note: Whitelisting is done from Configuration tab→Wi-Fi Whitelist
5.	File Name/Path	Search on any malware detected file name or path

Alerts Management and Notifications

Here you can see reports of all alerts received in details today or search on date. To avoid seeing the same alerts you can click “Mark as Read” so it does not show you again in Alert grid. To view details of any Alert click on “View Details” and it opens details in a new page:



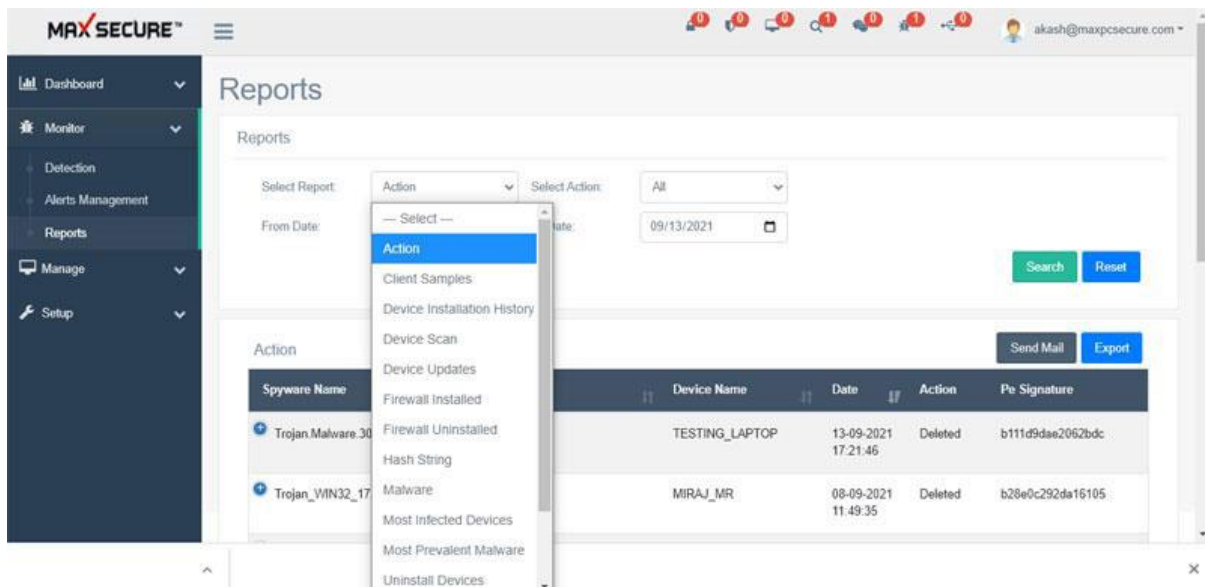
Here is the list of Alerts and Notifications received. These alerts are also mailed to Admin email id as soon as they happen:

No.	Description	Monitor→Alerts management
1	Total DLP violation	All events where DLP violation has been found such as writing to USB, network share or sending by Email attachment.
2	Ransomware found	If Ransomware is found on any device
3	Total Scan	Count of total devices scanned by Anti-virus scanner today
4	Total Uninstalled devices	If any devices are uninstalled. <i>Note: All windows and Android devices need an uninstall password to uninstall</i>

5	Total Sent/Received Messages	From Task → Broadcast Messages Admin can send and receive messages to / from devices
---	------------------------------	--

Reports

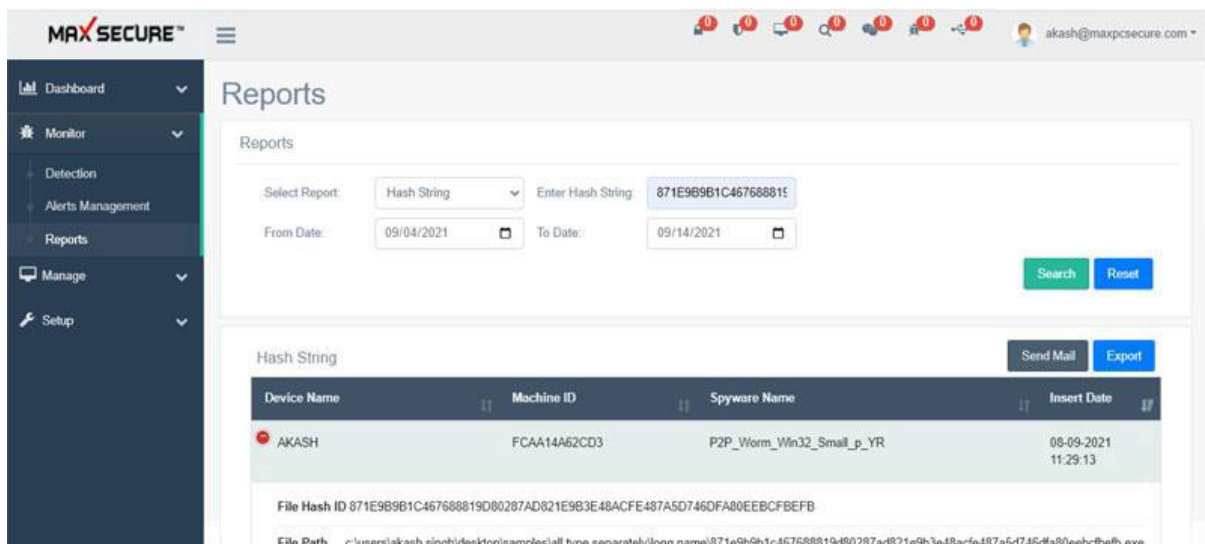
Very exhaustive reports are available, you can export them to Excel or mail.



The screenshot shows the MAX SECURE Reports page. A dropdown menu is open for the 'Action' column, listing various actions such as Client Samples, Device Installation History, Device Scan, Device Updates, Firewall Installed, Firewall Uninstalled, Hash String, Malware, Most Infected Devices, Most Prevalent Malware, and Uninstall Devices. The main table displays data for two devices: TESTING_LAPTOP and MIRAJ_MR, both marked as Deleted.

Device Name	Date	Action	Pe Signature
TESTING_LAPTOP	13-09-2021 17:21:46	Deleted	b111d9dae2062bdc
MIRAJ_MR	08-09-2021 11:49:35	Deleted	b28e0c292da16105

For example, you can search on sha256 Hash string of Malware:




The screenshot shows the MAX SECURE Reports page with the 'Hash String' report selected. The search criteria are set to 'Hash String' with the value '871E9B9B1C46768819D0287AD821E9B3E48ACFE487A5D746DFA80EEBCFBEBF'. The results table shows a single entry for device 'AKASH' with Machine ID 'FCAA14A62CD3' and Spyware Name 'P2P_Worm_Win32_Smail_p_YR'. Below the table, the File Hash ID and File Path are displayed.

Device Name	Machine ID	Spyware Name	Insert Date
AKASH	FCAA14A62CD3	P2P_Worm_Win32_Smail_p_YR	08-09-2021 11:29:13

File Hash ID 871E9B9B1C46768819D0287AD821E9B3E48ACFE487A5D746DFA80EEBCFBEBF
File Path c:\users\akash singh\desktop\samples\all type separately\long name\871e9b9b1c46768819d0287ad821e9b3e48acfe487a5d746dfa80eebcfbefb.exe

Report features:

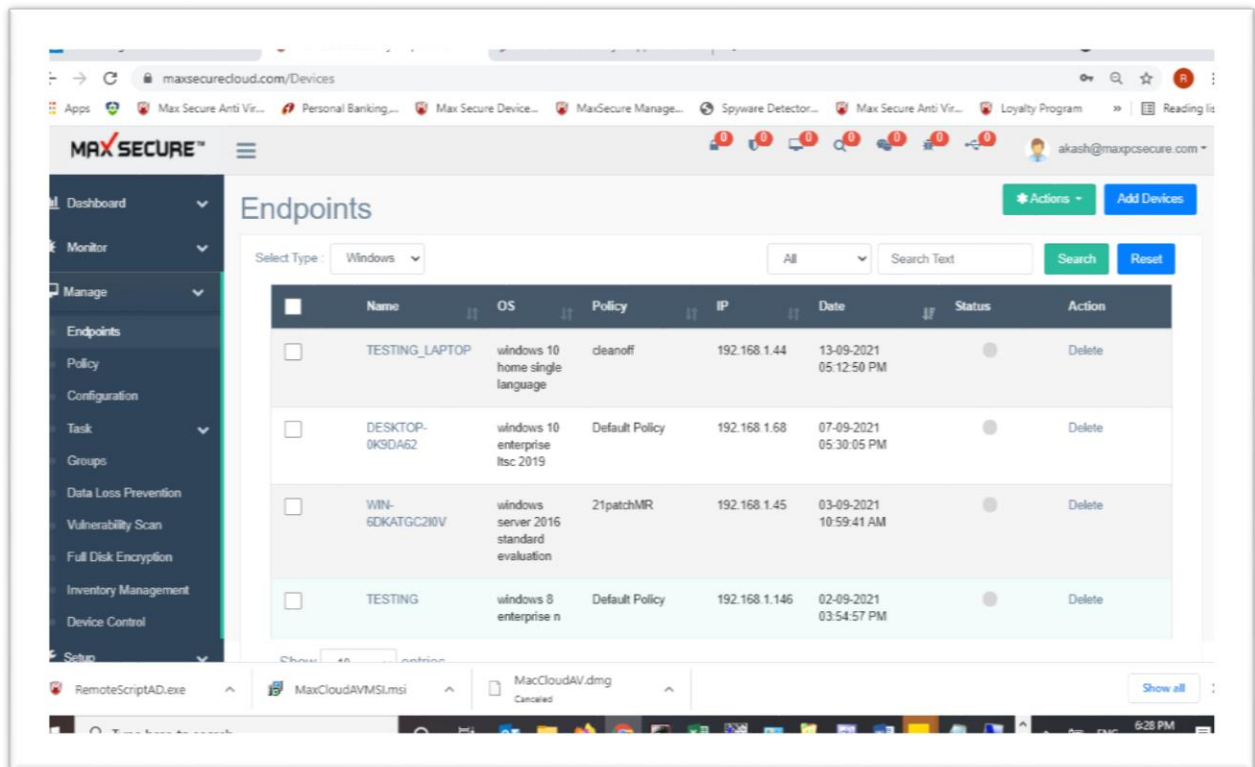
No.	Description	Monitor→Reports
1	Actions	Search on date malware found, device name, date, Action taken on detected malware and its PE signature. <i>Note:</i> PE signature is our proprietary signature mechanism, we have provided a tool to create PE signature of any file to find sha256 hash of the same file, click on  sign next to device name
2	Ransomware found	If Ransomware is found on any device
3	Total Scan	Count of total devices scanned by Anti-virus scanner today
4	Total Uninstalled devices	If any devices are uninstalled. <i>Note: All windows and Android devices need an uninstall password to uninstall</i>
5	Total Sent/Received Messages	From Task → Broadcast Messages Admin can send and receive messages to /from devices

Manage

You can find Endpoints, Policy, Configuration, Tasks-Content search, Broadcast message, Share Files, Groups, Data loss prevention, Vulnerability scan, Full disk encryption and Inventory Management and Device control settings.

Endpoints

You will get a quick overview of devices installed, their device name, operating system, policy applied on them, date installed, status (online or offline) and action.



Add Devices

You can add devices and attach them to this Portal in 3 ways:

Method 1: For manually installing and registering device, click on Add devices → choose which license key you would like to use (if you have more than one) and generate registration token for number of device that you are ready to install.

Registration tokens can be viewed from **Setup → License Management →**

Windows Client setup can be downloaded manually from the following links. After installation, use the registration token generated above on client setup user interface:

For 64 bit OS:

<https://maxsecure.b-cdn.net/maxcloudav/MaxCloudAVx64.exe>

For 32bit OS:

<https://maxsecure.b-cdn.net/maxcloudav/MaxCloudAV.exe>

Steps to install:

1. Double click on the downloaded executable
2. User interface will open, click on Register Now

Linux set up can be downloaded from:

For 64 bit:

https://cloud.maxpcsecure.com/MaxAVLinux_x64.zip

For 32 bit:

https://cloud.maxpcsecure.com/MaxAVLinux_x86.zip

Steps to Run:

1. Extract the Zip File
2. Open the Extracted folder
3. Inside folder Right Click and Open "Terminal".
4. Type "sudo chmod +x Setup"
5. Enter the User Password and Press Enter
6. Then Type "./Setup"
7. After Installation Close Terminal
8. Search for Maxav or Open terminal and type "maxav"

Mac set up can be downloaded from Setup → License Management → Mac installation instructions section or link below:

<https://cloud.maxpcsecure.com/InstallerExes/Mac/MacCloudAV.dmg>

Step to install:

1. Double click on DMG file
2. Drag and drop cloud security into application folder
3. Go to application and launch cloud security application
4. Enter Id and Installation key

Android set up can be downloaded from Setup → License Management → Android installation instructions section or link below:

https://play.google.com/store/apps/details?id=com.max.maxcloudsecurity&hl=en_IN&gl=US

Step to install App:

1. Install App
2. After installation, App launches and asks for permissions, allow them.
3. Then login page opens. Enter email id and registration token.
4. App will get registered and can be viewed on the Portal under
5. Manage → Endpoints → choose type of devices from the drop down → Android

Method 2: Dynamic package installer can be generated (for Windows and Mac Only), where you need not use any code to register and client devices will automatically connect to the dashboard right after installation.

Get them from Setup → Distribution Packages → Distribution Package for Windows or Mac → Click on 'Generate' button then copy that link and hit on the browser.

For Windows devices choose Distribution Package with Download Manager.

For Mac devices choose Distribution Package for MAC.

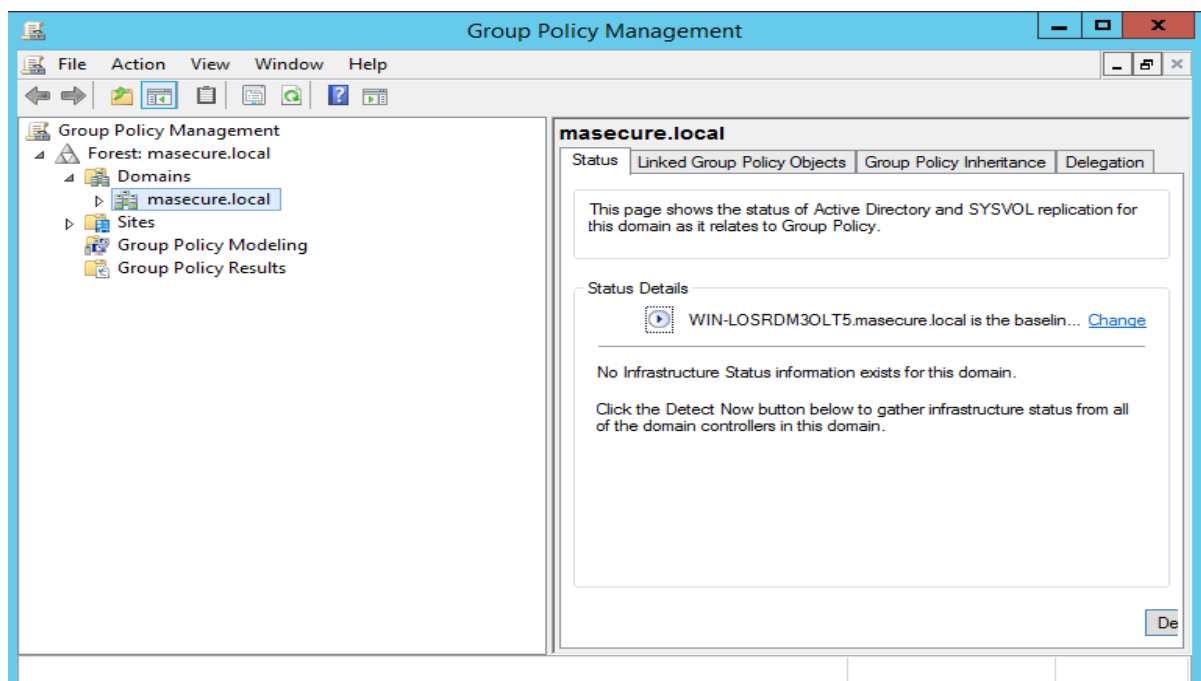
Method 3: Using Active directory. If your organisation has Active directory installed on your network then use that to very quickly install client setups. (For windows devices only).

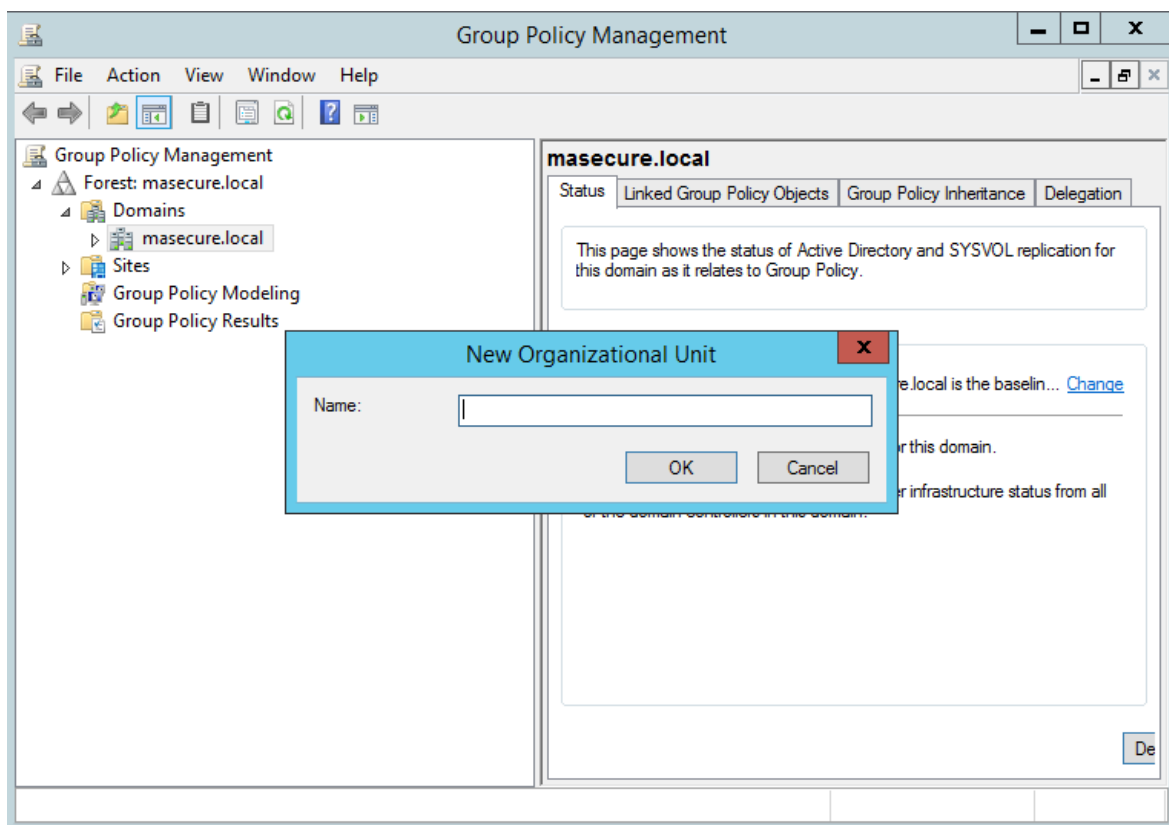
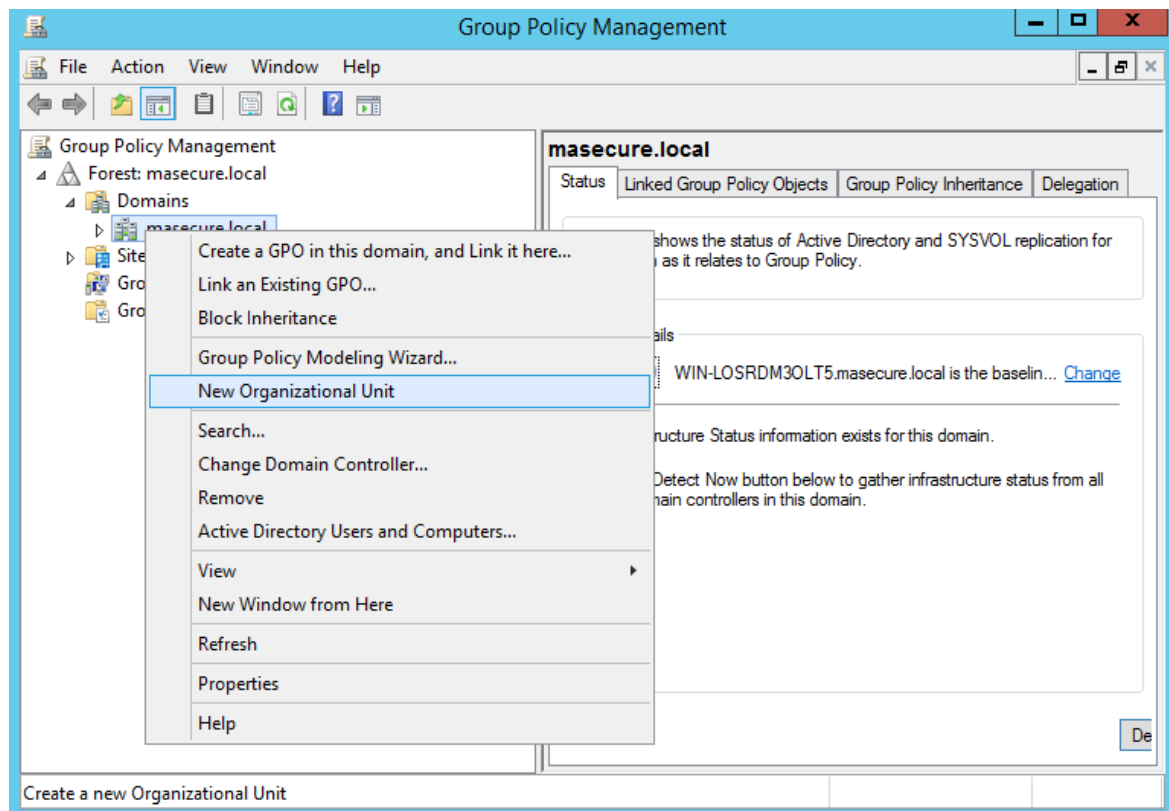
Scroll down to Setup → Distribution Packages → Windows installation instructions → item 5→ for Active Directory msi file.

Instructions to use Active Directory through msi installation:

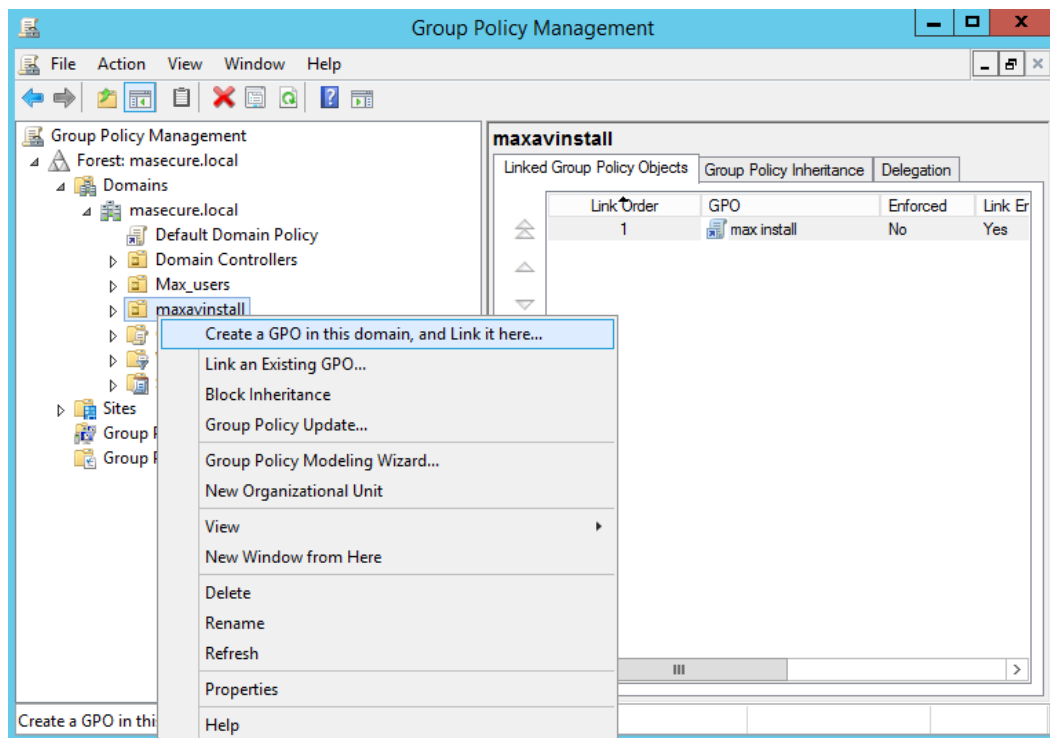
Step 1:- Create a folder at any drive and put the Max AV Cloud Setup 32 & 64-bit and also MaxCloudAVMSI.msi in that folder and share that folder.

Step 2:- Go to tools and click on Group policy management then right click on domain and again click on new organization unit and provide the name to organization.

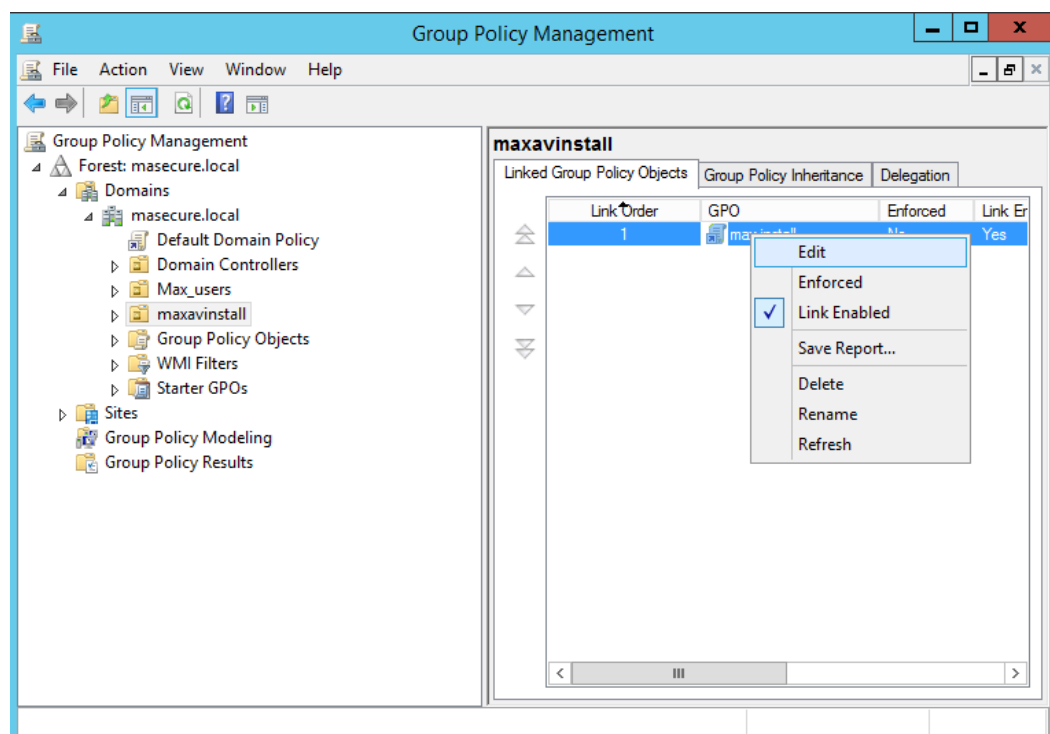




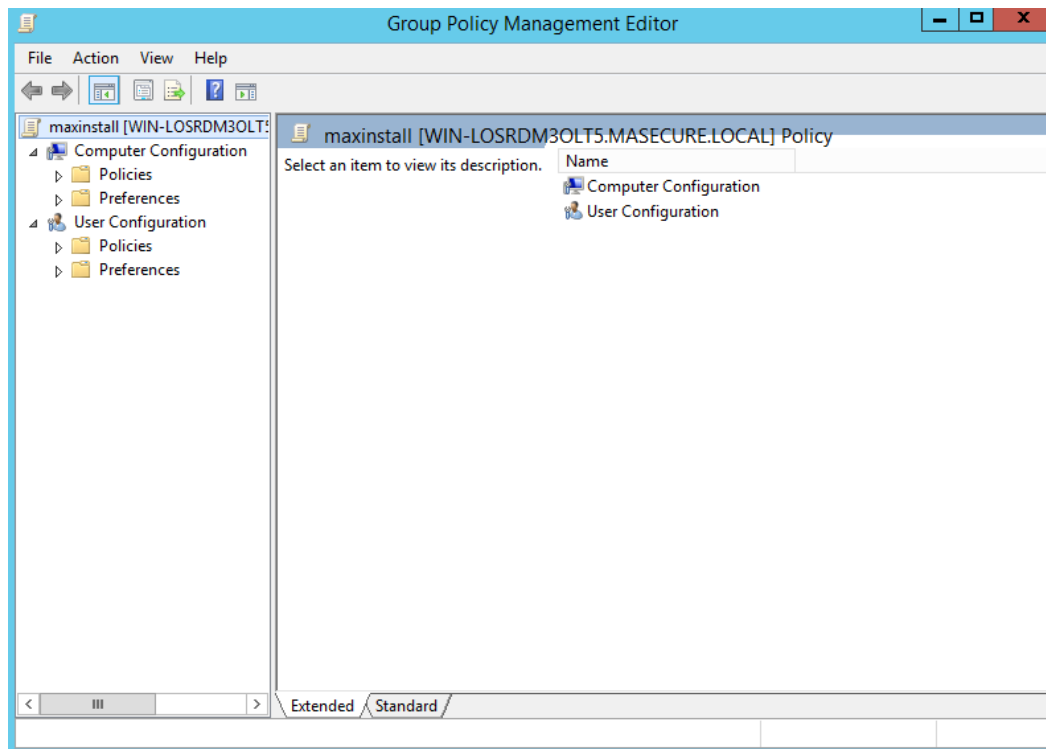
Step 3:- Folder which is created for new organization unit. Right click on that and create a GPO.



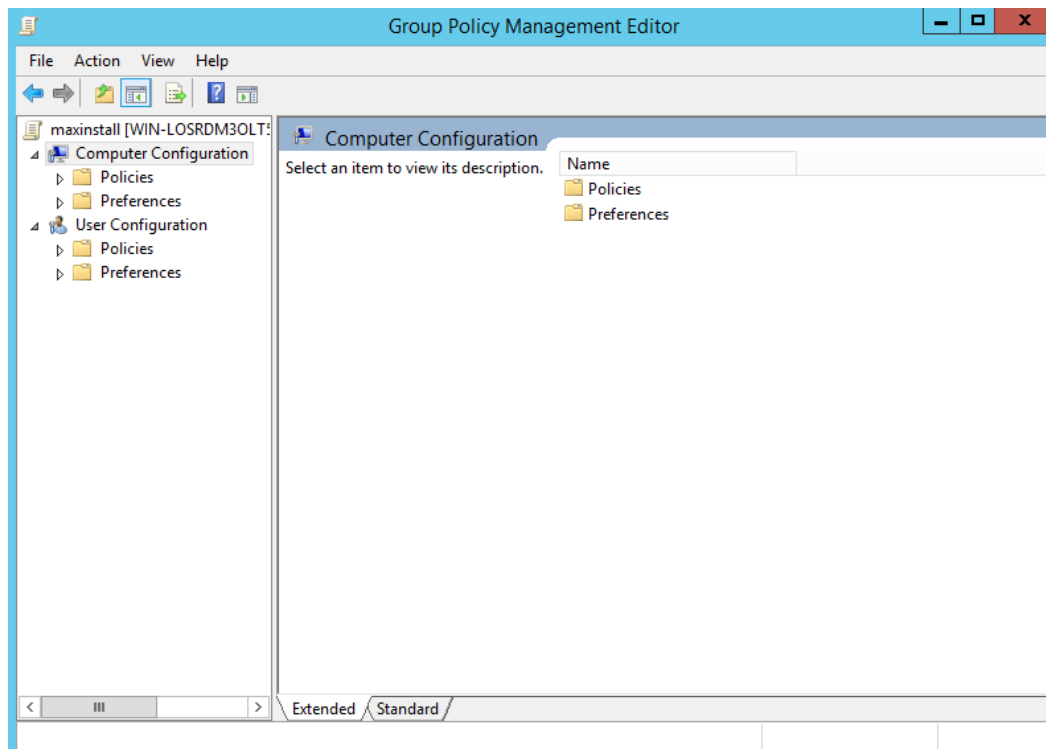
Step 4:- Right click on GPO and go to edit option.

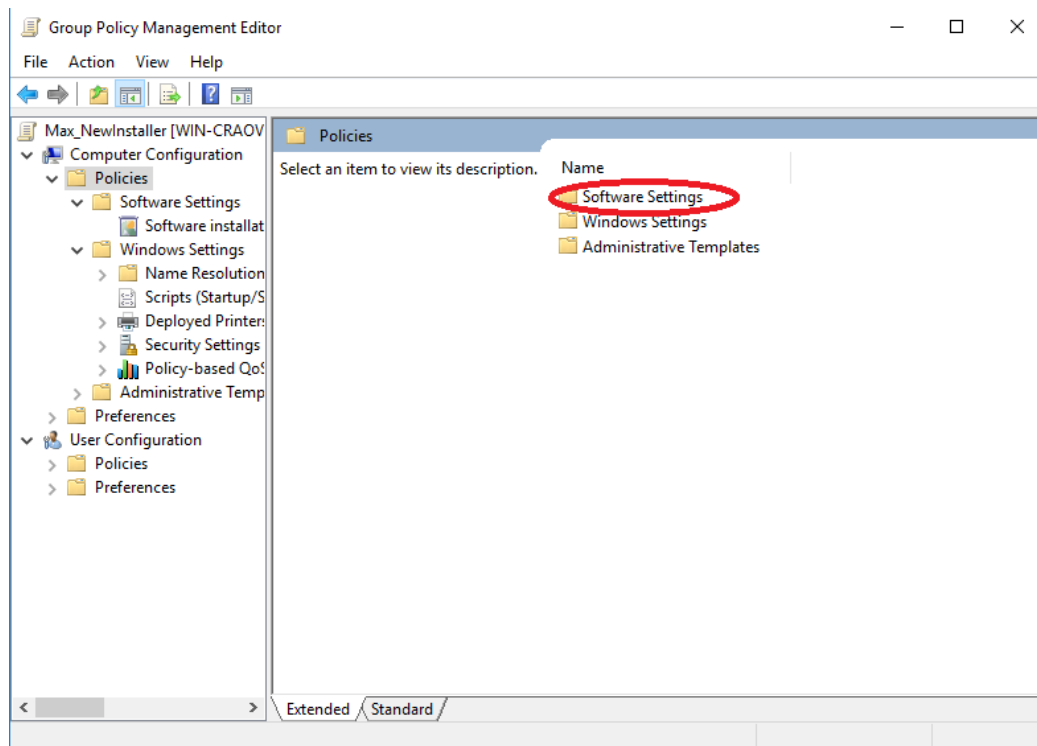
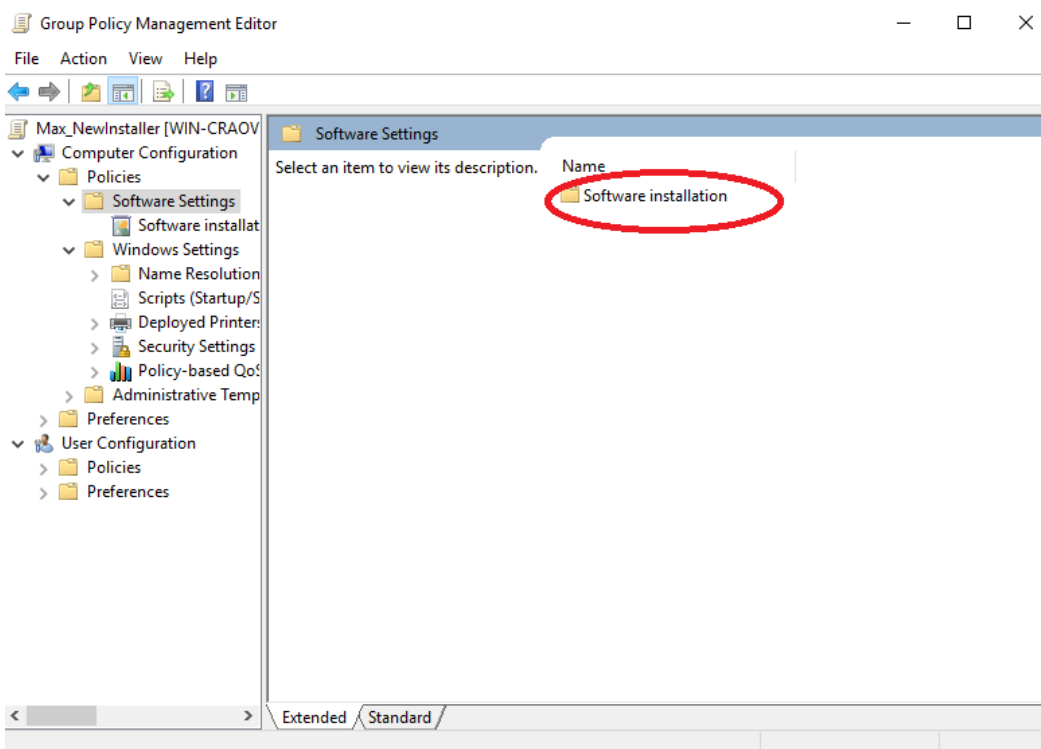


Step 5:- Click on Computer Management.

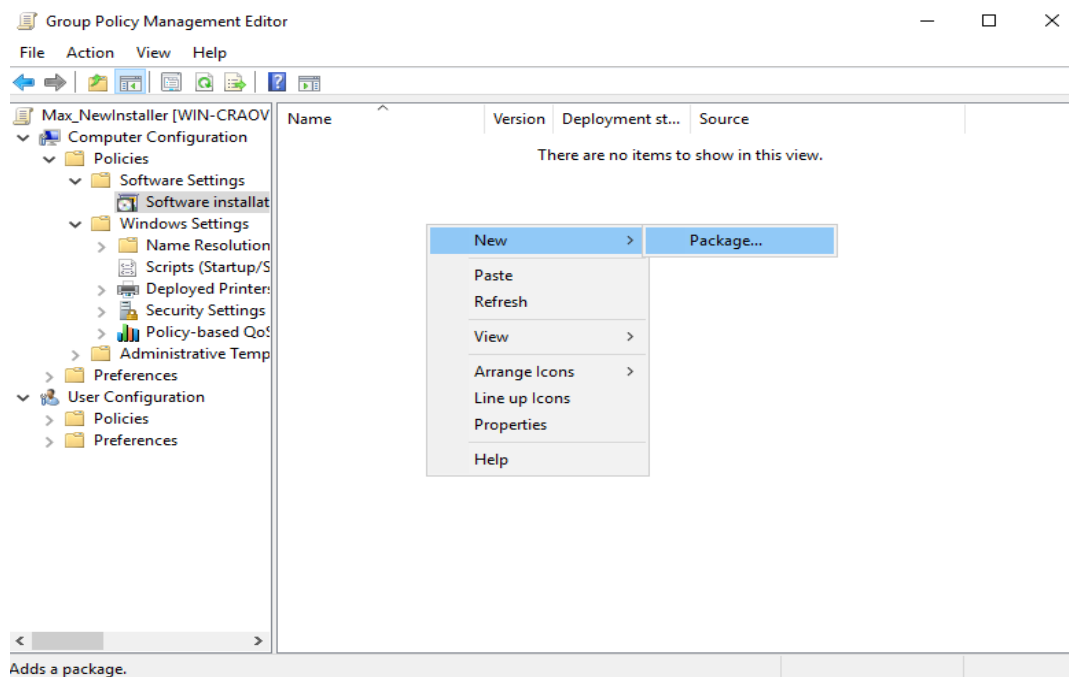


Step 6:- Click on Policies.

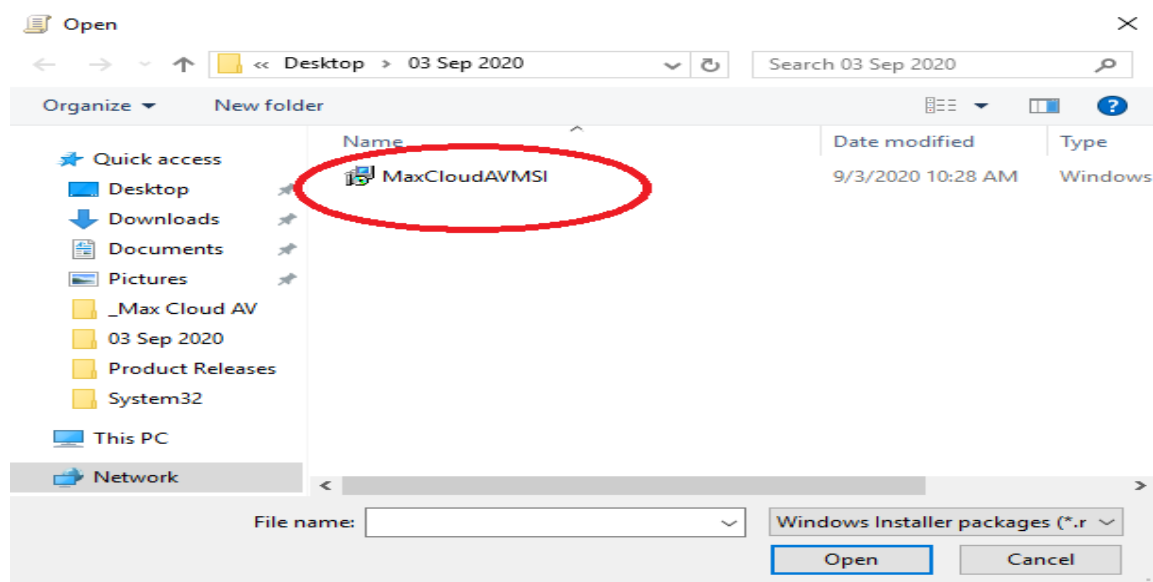


Step 7:- Click on Software Setting.**Step 8:- Click on Software Installation.**

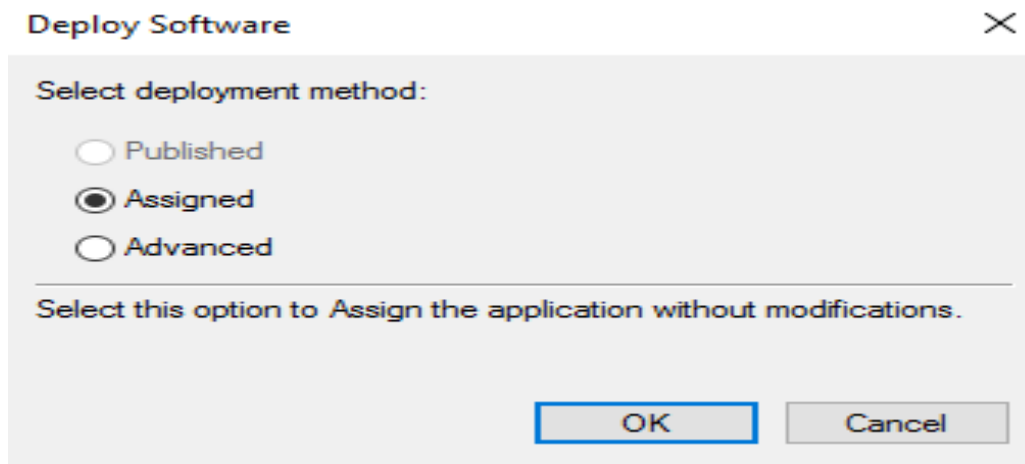
Step 9:- Please Right Click in that new select Packages.



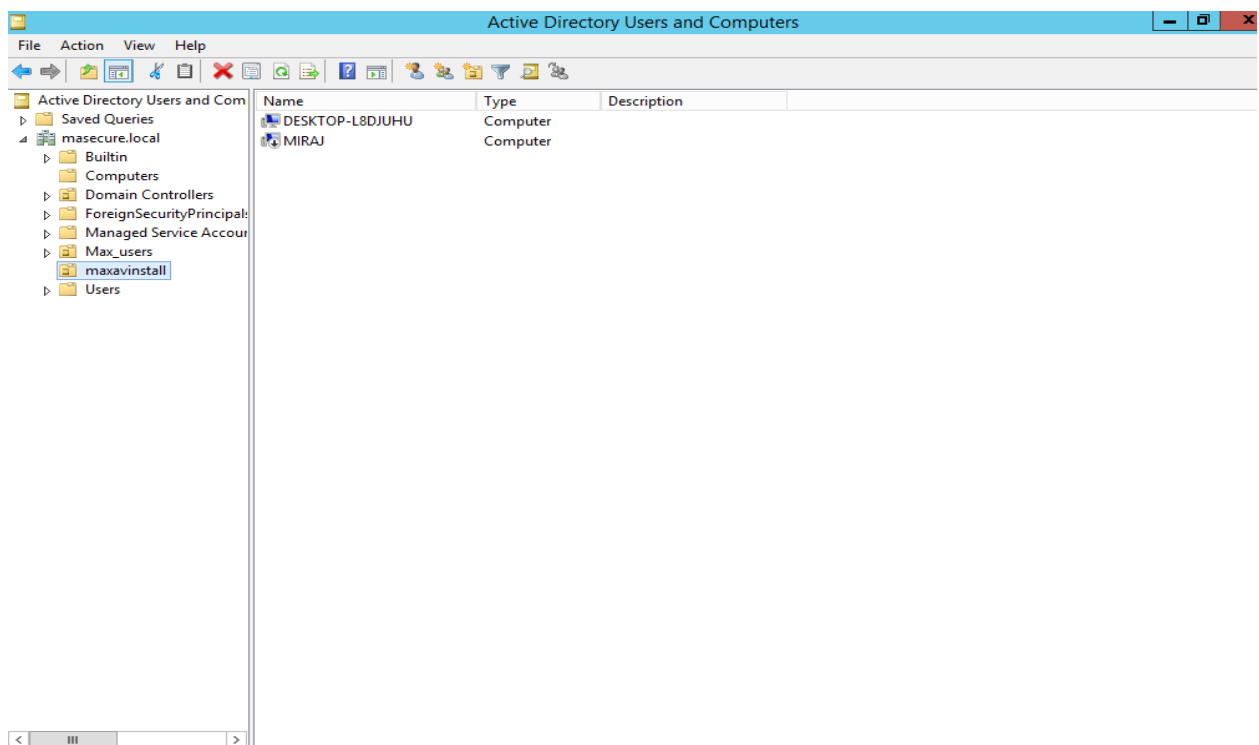
Step 10:- Select the MaxCloudAVMSI.msi where you are kept and click on OK button.



Step 11:- Select the assigned option and click on OK button.



Step 12:- Go to Active Directory Users and Computer then add those computer in organization Folder on which you have to install and then open the command prompt and enter gpupdate/force.



Note: - Setup should install when the machine gets start. If the machine is on then setup is not install because it required restart.

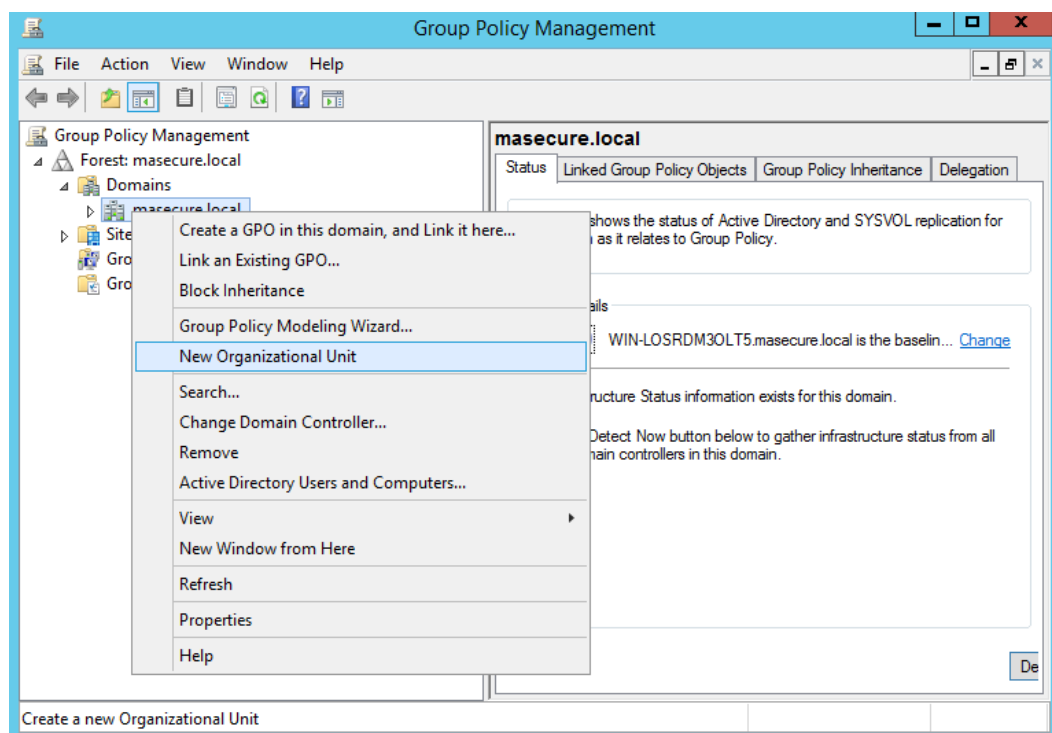
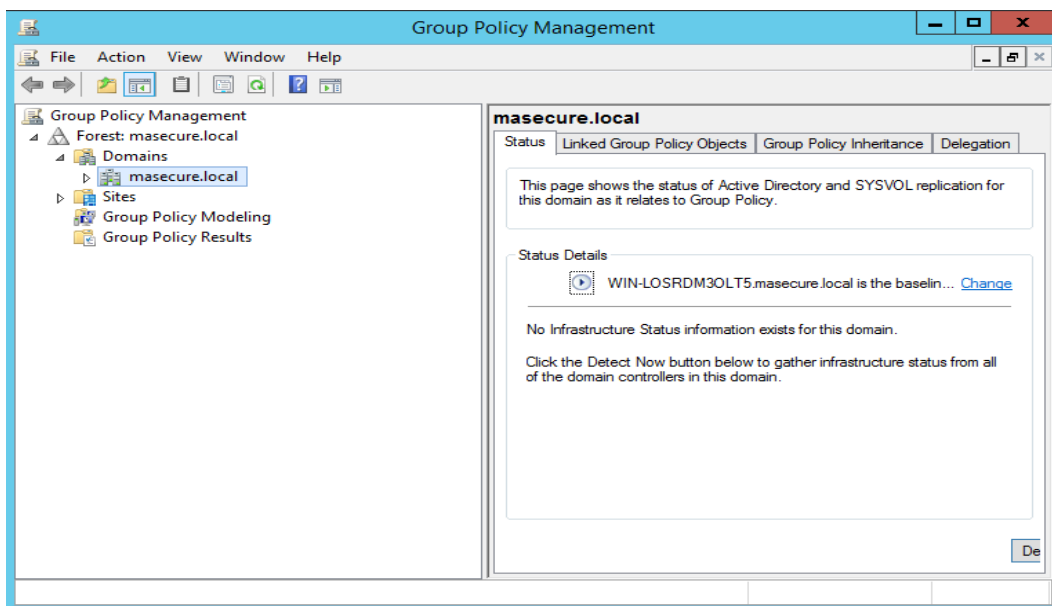
Method 4: Using Group Policy. Use group policies to very quickly install client setups. (For windows devices only).

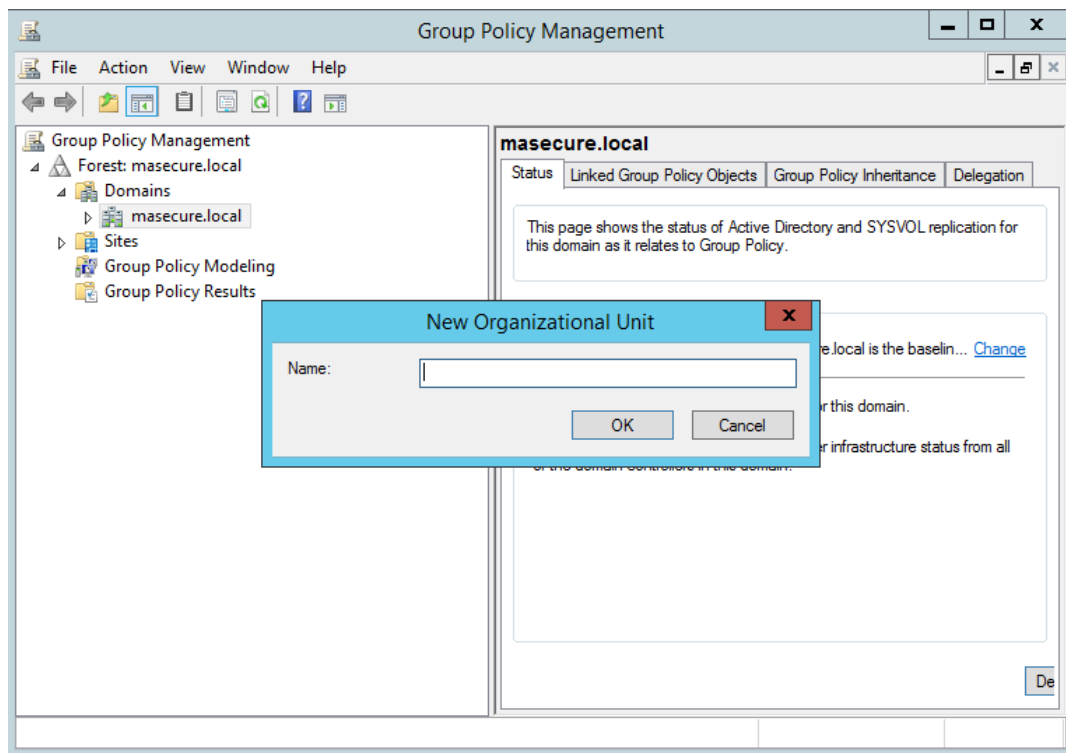
Scroll down to Setup → License Management → Manage License → windows installation instructions → for Group policy RemotescriptAD.exe

Instructions to use Group Policy:

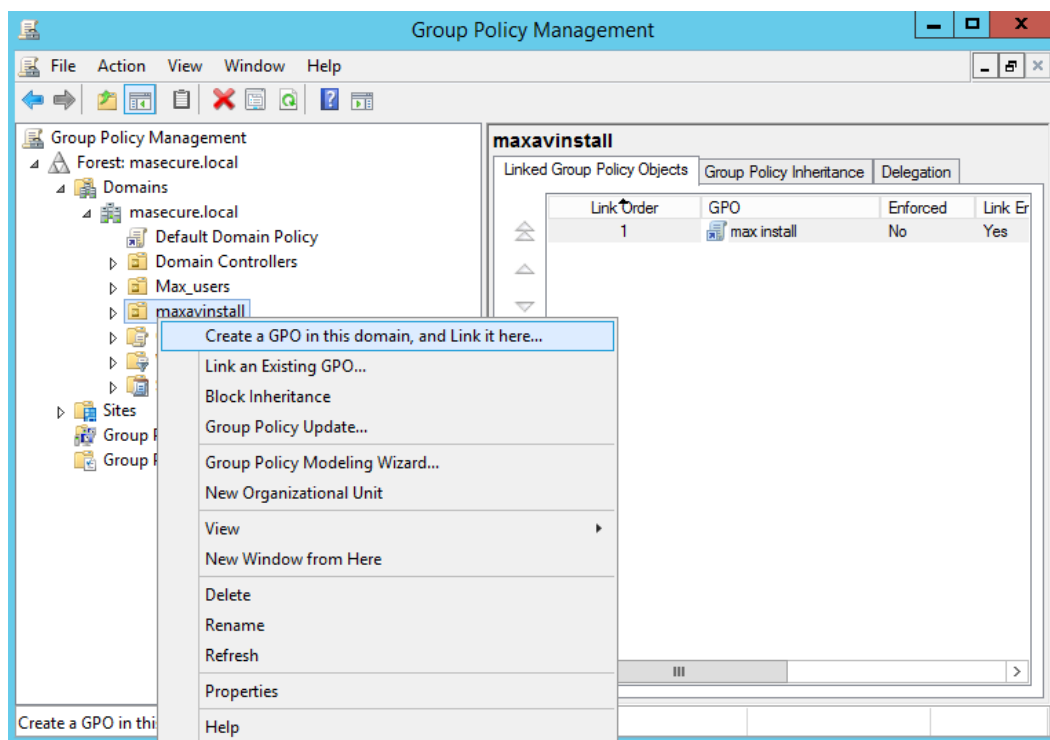
Step 1:- Create a folder at any drive and put the Max AV Cloud Setup 32 & 64-bit and also RemoteScriptAD.exe in that folder and share that folder.

Step 2:- Go to tools and click on Group policy management then right click on domain and again click on new organization unit and provide the name to organization.

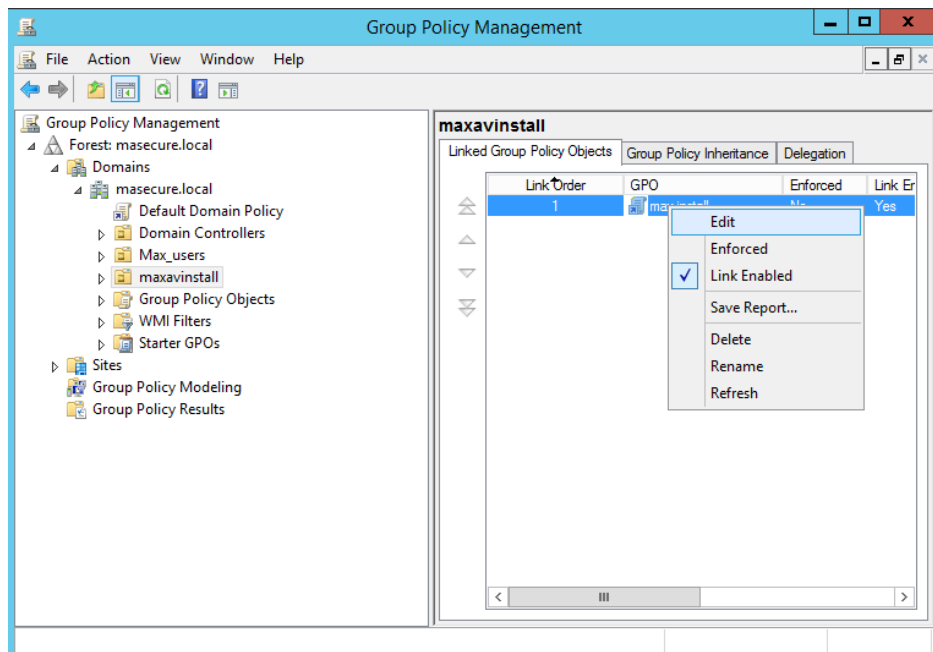




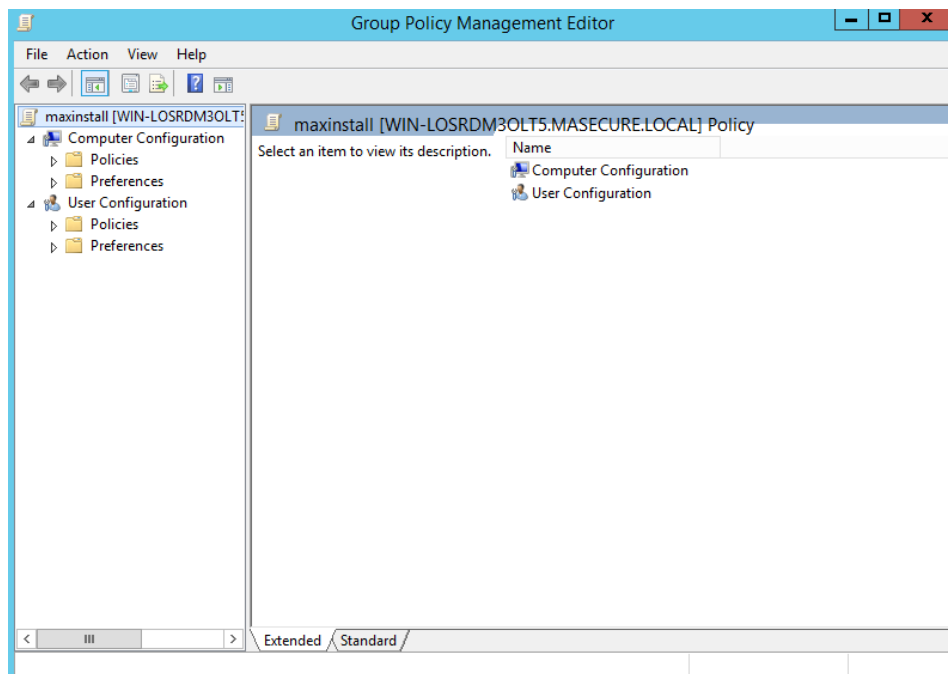
Step 3:- Folder which is created for new organization unit. Right click on that and create a GPO.



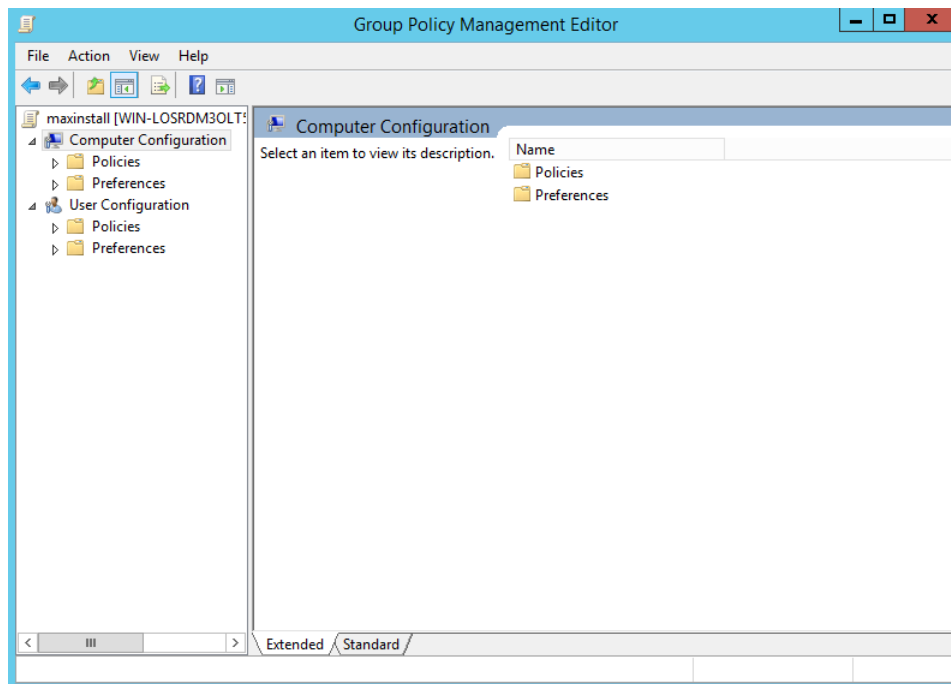
Step 4:- Right click on GPO and go to edit option.



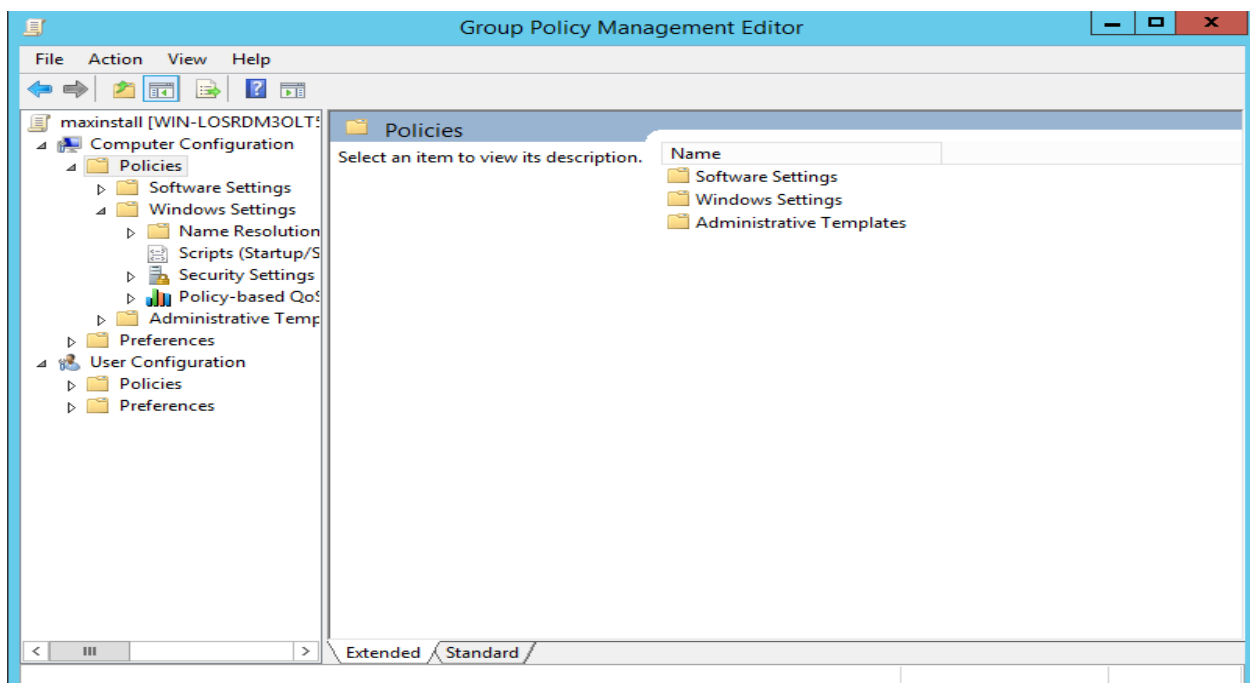
Step 5:- Click on Computer Management.



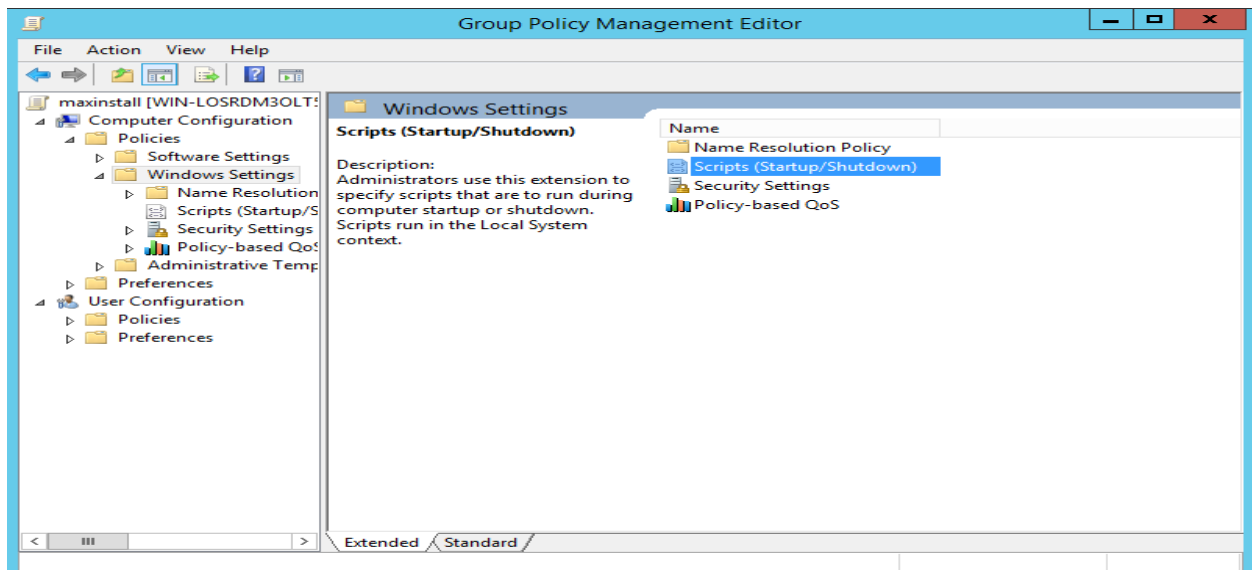
Step 6:- Click on Policies.



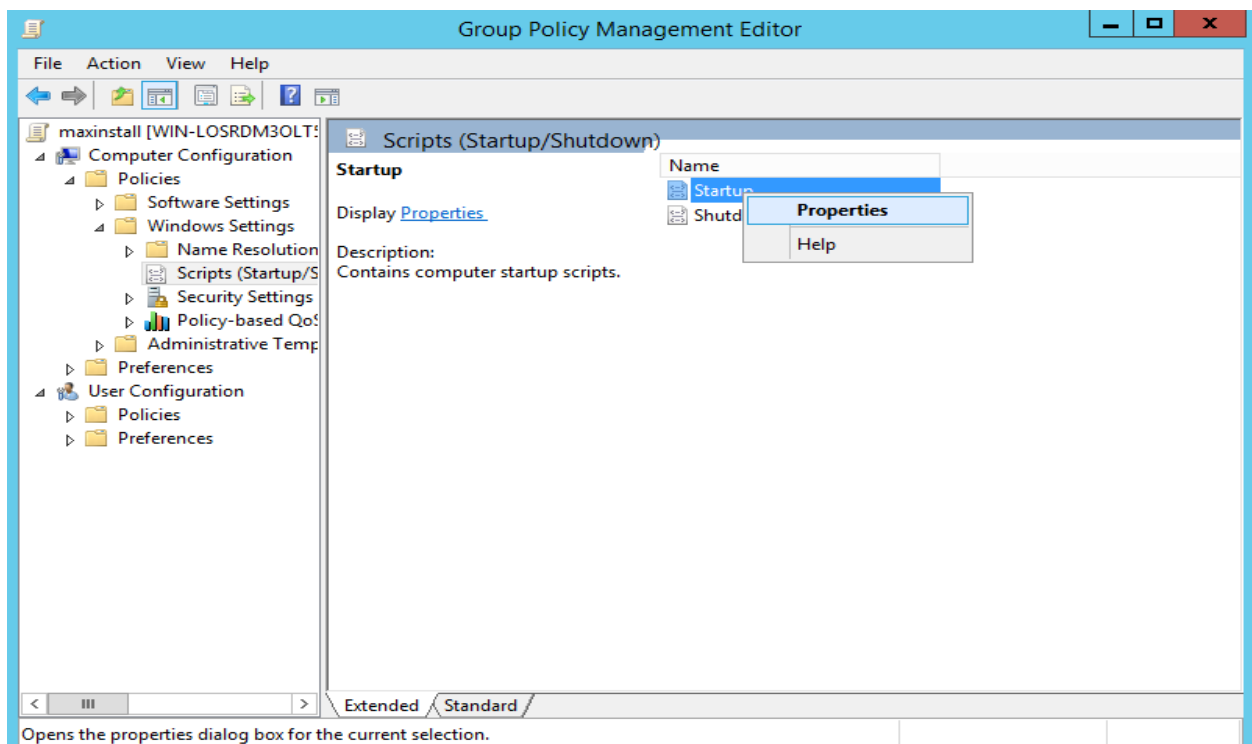
Step 7:- Click on Window setting.



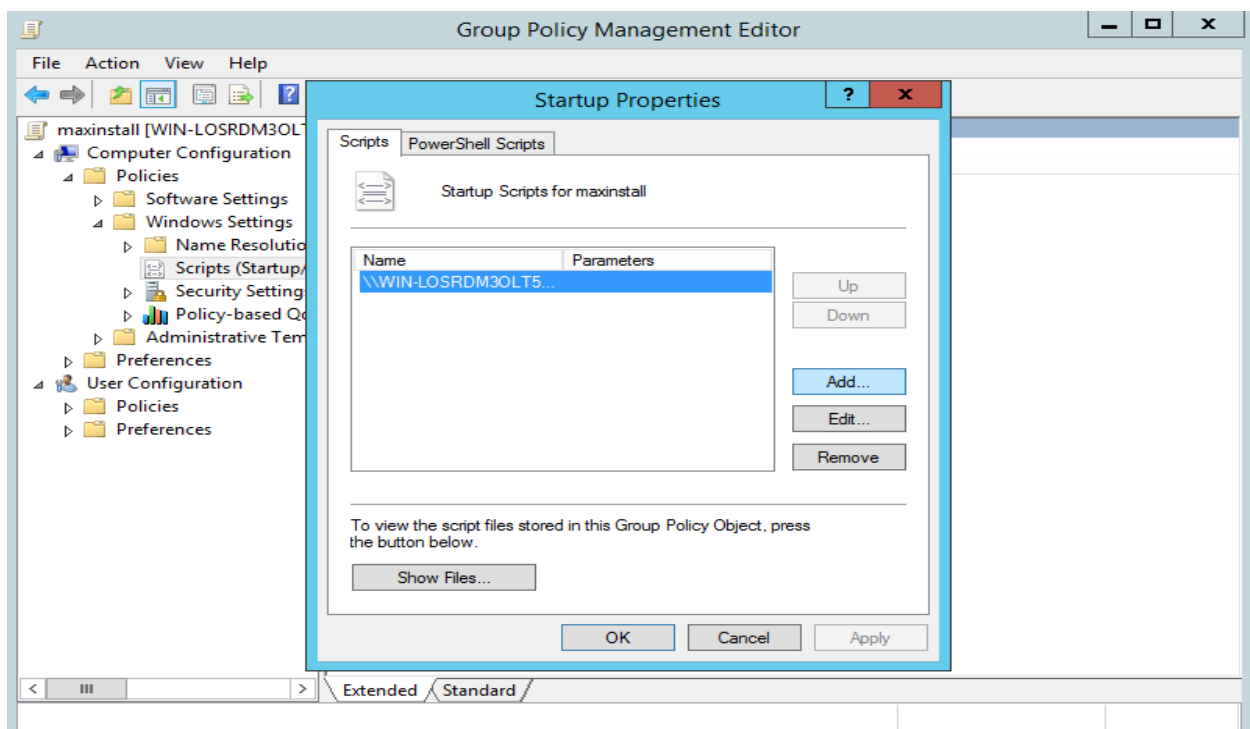
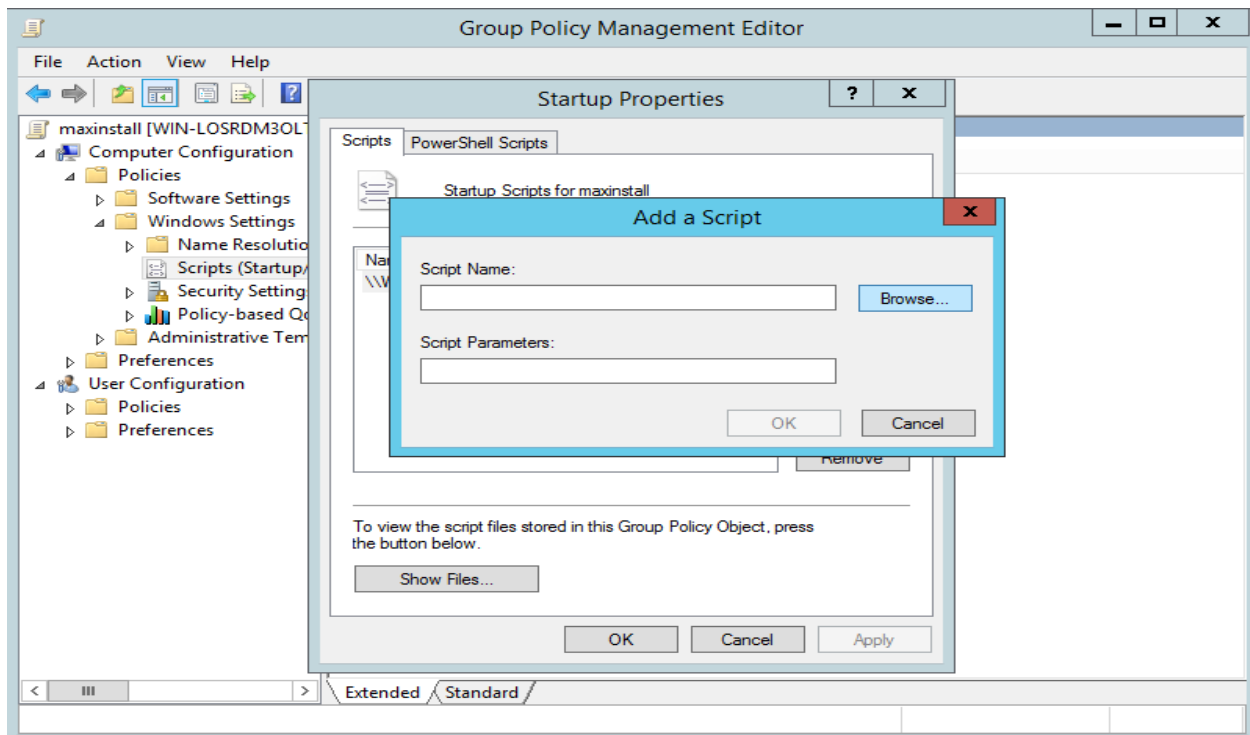
Step 8:- Click on Script Start-up/Shutdown.



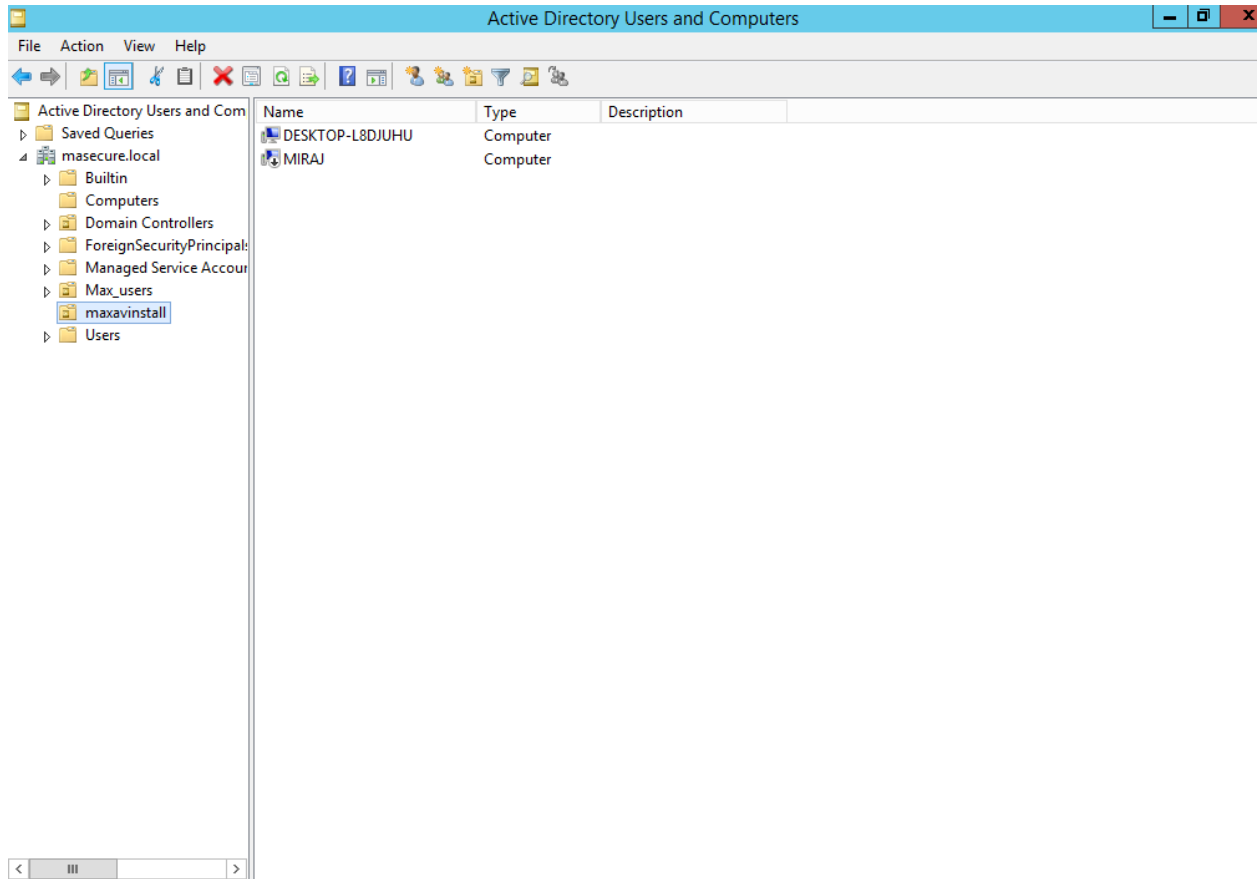
Step 9:- Right Click on Start-up properties.



Step 10:- Click on Add Script and select the Share location path.



Step 11:- Go to Active Directory Users and Computer then add those computer in organization Folder on which you have to install and then open the command prompt and enter gpupdate /force



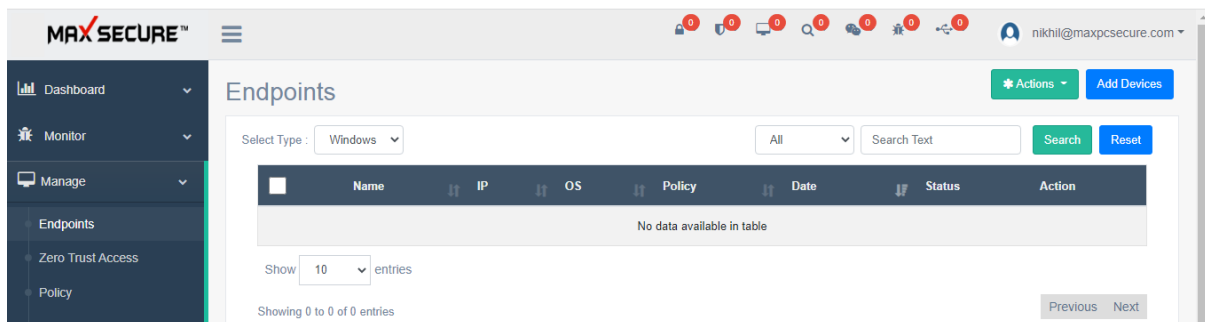
Note: - Setup should install when the machine gets start. If the machine is on then setup is not install because it required restart.

Key Generation and Active Directory

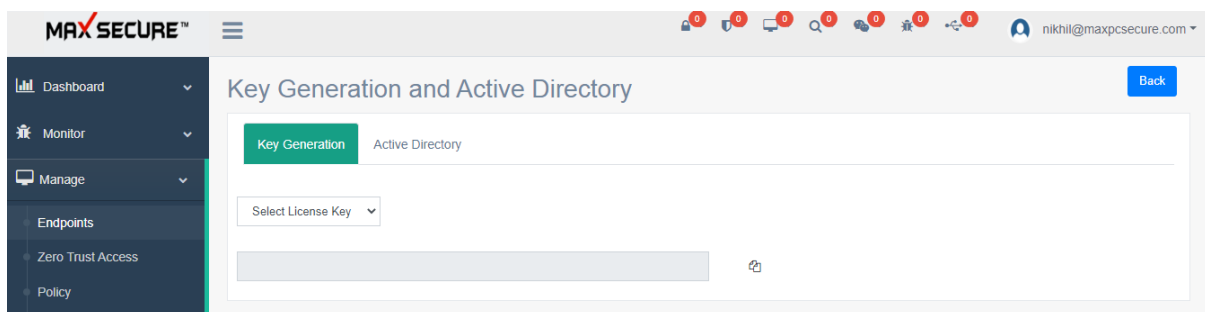
Active Directory

Users can obtain network resources through Active Directory (AD), which provides a database and a set of services.

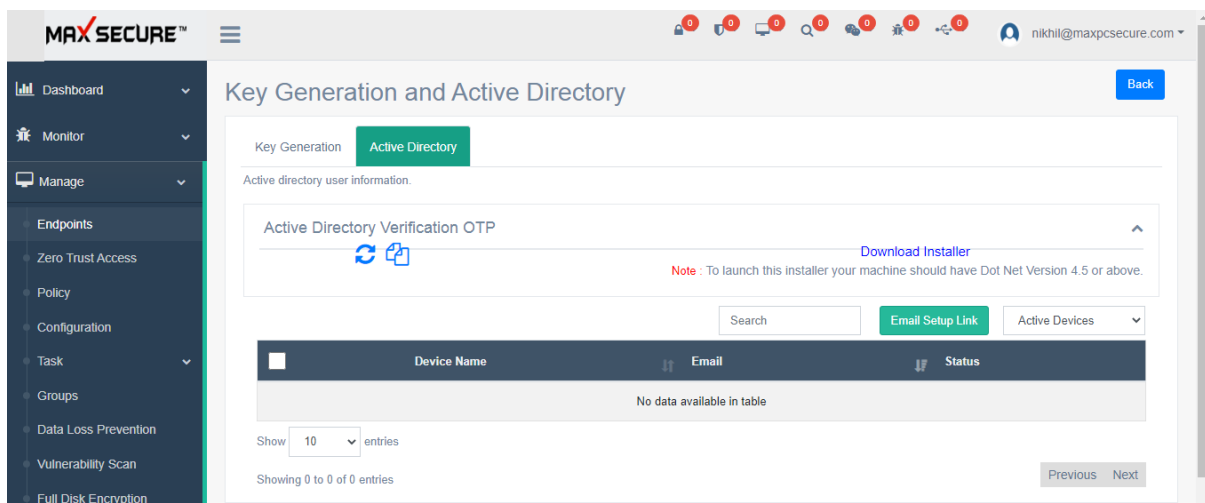
1. Open **Manage** and Click on **Endpoints**.



2. Click On **Add Devices**.



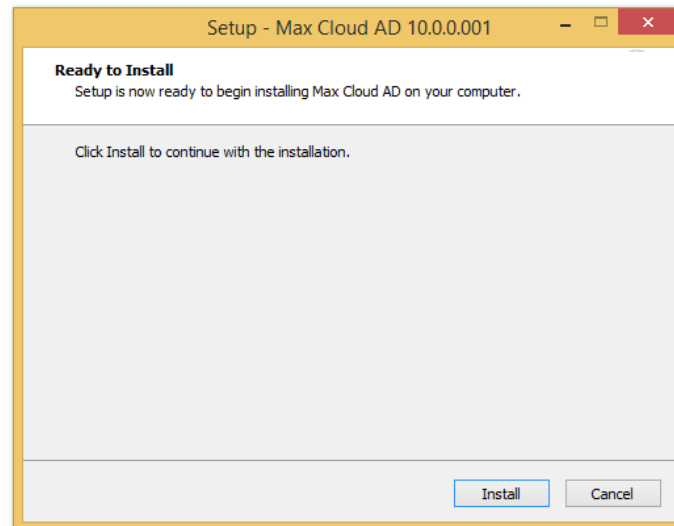
3. Click On **Active Directory**.



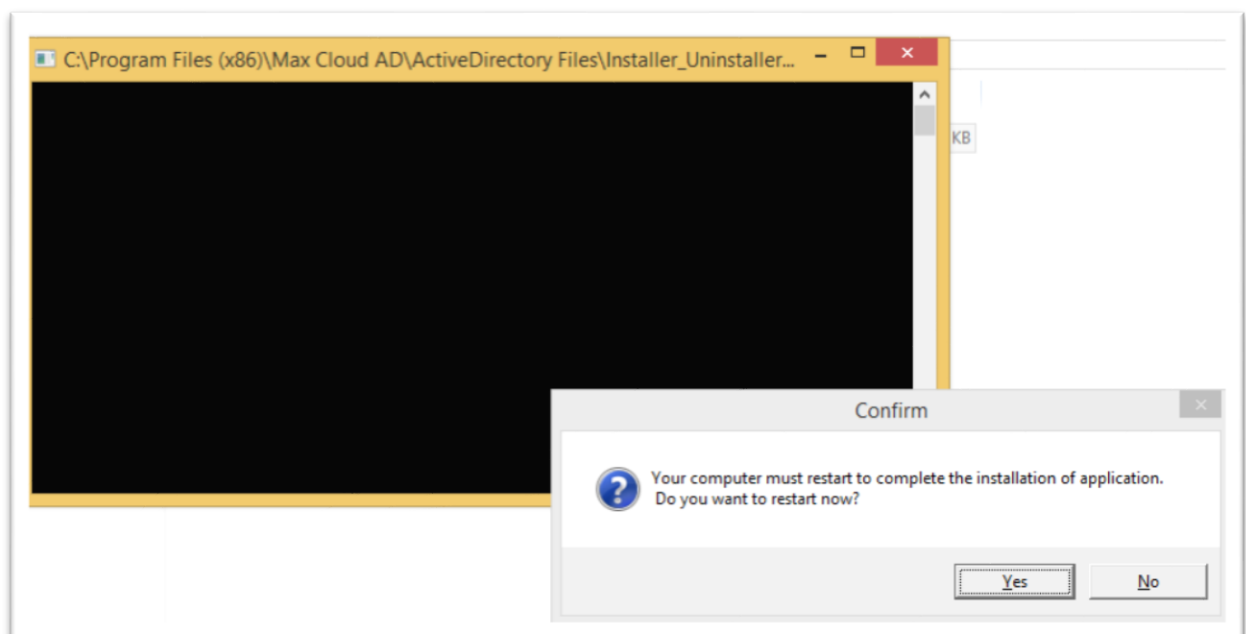
4. Click On **Download Installer**. Max Cloud AD.exe File Start Downloading.

5. Click on file and its start the Installation Process.

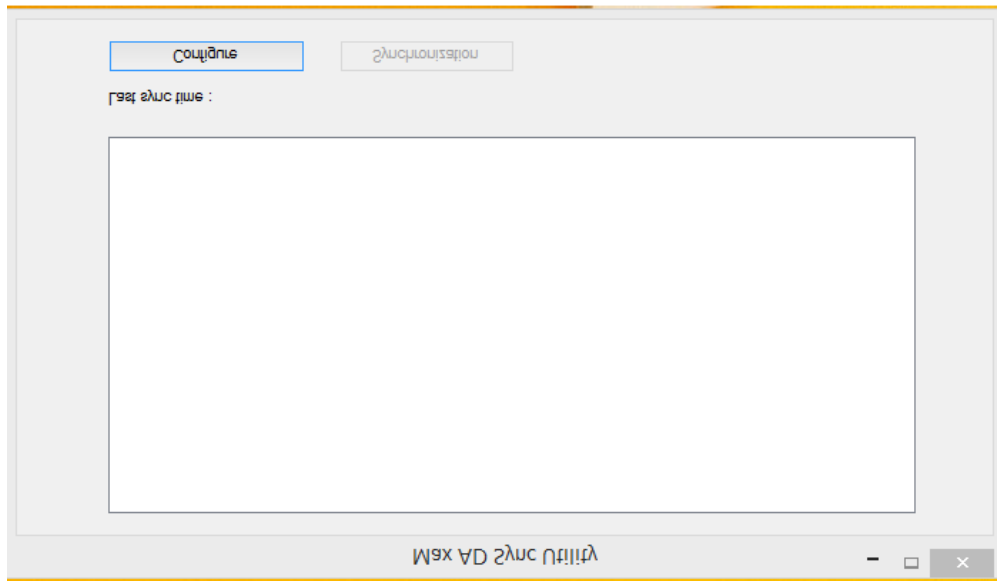
Name	Date modified	Type	Size
MaxCloudAD	3/10/2022 2:06 PM	Application	1,908 KB



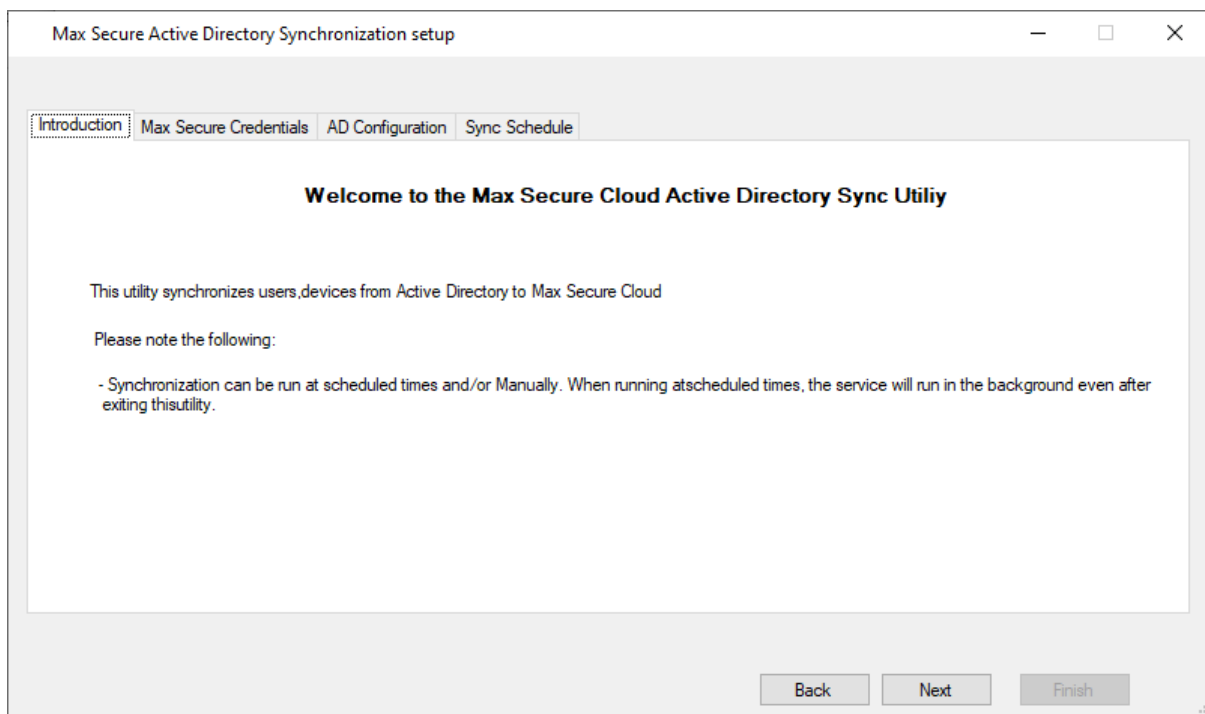
6. After Click on Install, cmd will launch and successfully installed a New Popup Comes of **Do you want to restart now?** With yes or no option.



7. Click on Yes Restart will Start and After Restarting Max Cloud AD.exe Shortcut Created On Desktop.
8. Open the Max Cloud AD Application and Start the Configuration Process.



9. Now Click On **Configure**. New popup Window comes up i.e. **Introduction** Page.



10. Click on Next then User want to Setup the Credentials Part.

The screenshot shows the 'Max Secure Active Directory Synchronization setup' window. The 'Max Secure Credentials' tab is selected. The 'Max Secure Portal Credentials' section contains the following fields and controls:

- ☐ On Premises: A checkbox that is currently unchecked.
- Enter On Premises IP address below: A text input field.
- User Name: A text input field.
- Password: A text input field.
- Validate: A button.

At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Finish'.

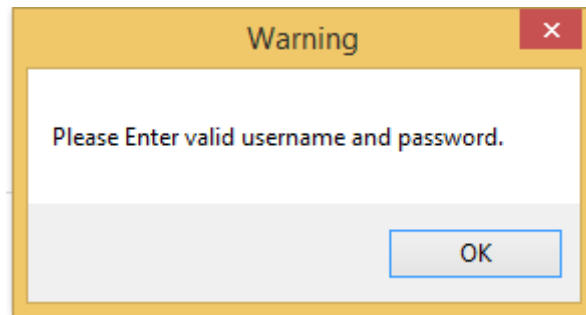
10.1 If Offline User Need to Click in On Premises Check box and Put the IP of Portal and username and password of Portal Login and Click on Validate.

The screenshot shows the 'Max Secure Active Directory Synchronization setup' window with the 'Max Secure Credentials' tab selected. The 'Max Secure Portal Credentials' section is now filled with the following data:

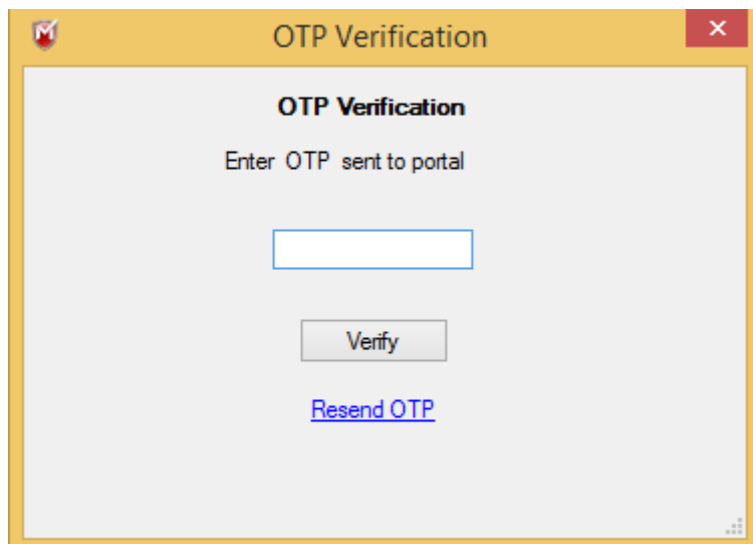
- ☒ On Premises: The checkbox is now checked.
- Enter On Premises IP address below: The text input field contains '192.168.1.11'.
- User Name: The text input field contains 'maxsupport'.
- Password: The text input field contains '*****'.
- Validate: A button.

At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Finish'.

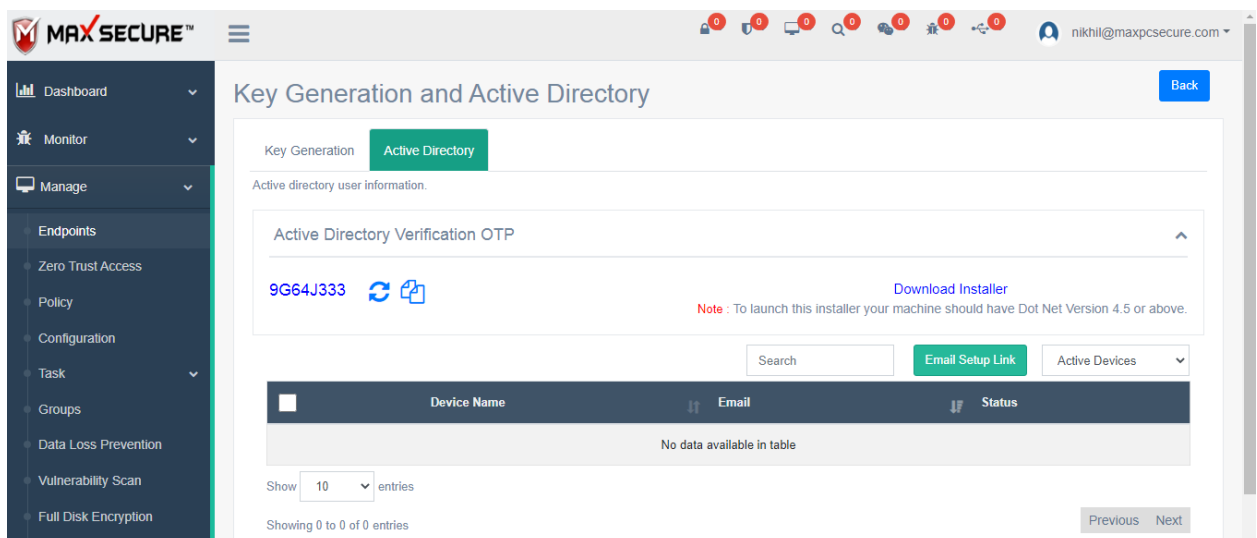
10.2 If Credentials Gone Wrong Enter valid Username and Password Popup Comes.



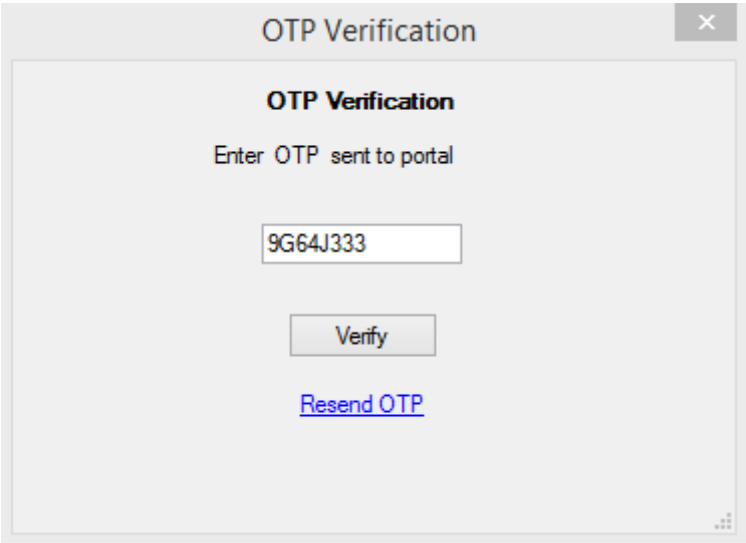
11. New Popup Comes of **OTP Verification**.



12. For OTP Verification User Need To Check the Portal For OTP Comes In **Manage>Endpoints>Add Devices>Active Directory**.

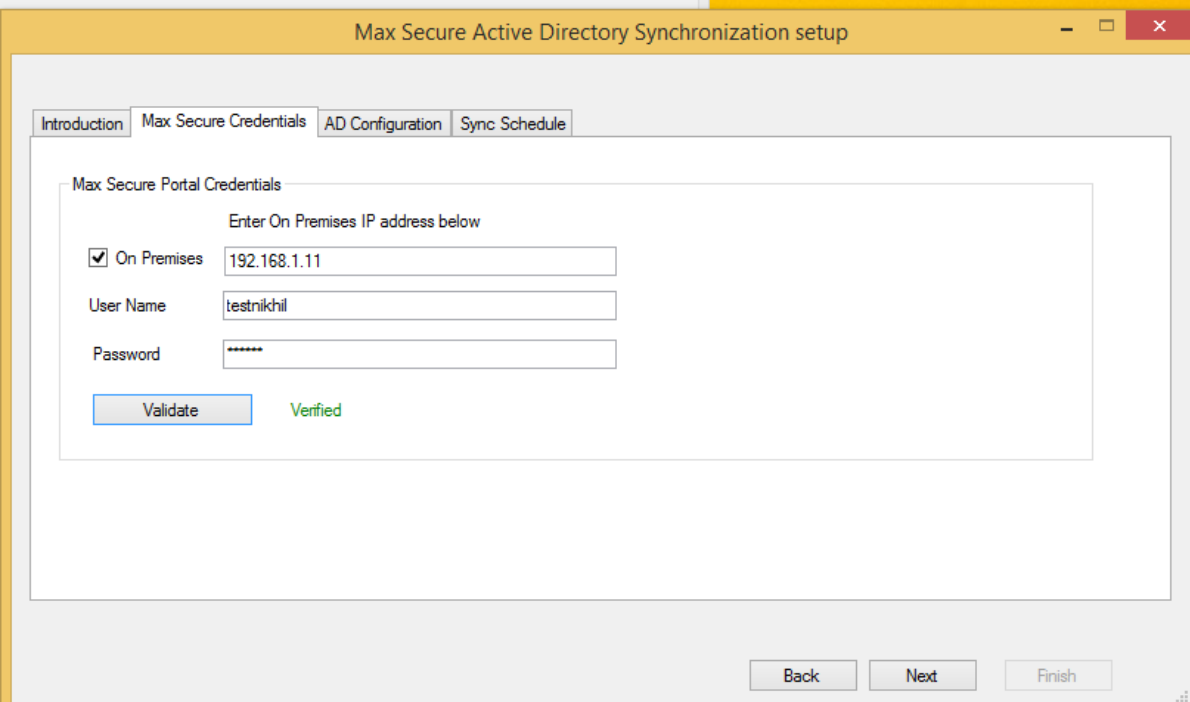


13. Copy the OTP and Paste On **OTP Verification** Window.



The image shows a window titled "OTP Verification" with a close button in the top right corner. Inside the window, the text "OTP Verification" is displayed in bold. Below it, the instruction "Enter OTP sent to portal" is shown. A text input field contains the alphanumeric code "9G64J333". Below the input field is a button labeled "Verify". At the bottom of the window, there is a blue hyperlink labeled "Resend OTP".

14. On the Credentials window, click on Verify if OTP is Valid and it will show Verified next to the Validate button.

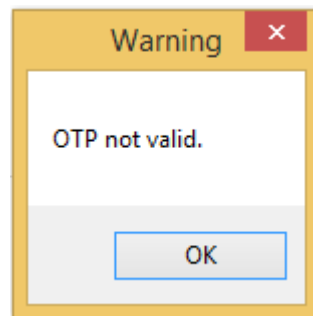


The image shows the "Max Secure Active Directory Synchronization setup" window with the "Max Secure Credentials" tab selected. The "Max Secure Portal Credentials" section contains the following fields and controls:

- A checkbox labeled "On Premises" is checked.
- A text input field for "Enter On Premises IP address below" contains the value "192.168.1.11".
- A text input field for "User Name" contains the value "testnikhil".
- A text input field for "Password" contains six asterisks "*****".
- A button labeled "Validate" is present.
- To the right of the "Validate" button, the word "Verified" is displayed in green text.

At the bottom of the window, there are three buttons: "Back", "Next", and "Finish".

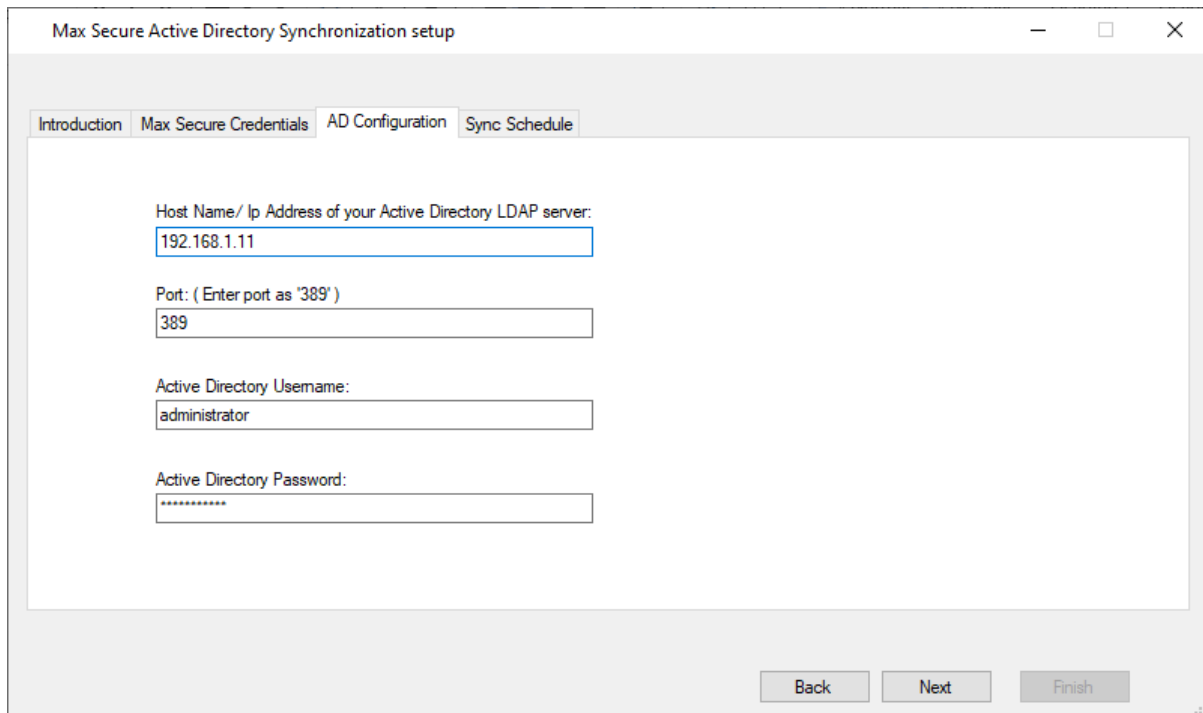
14.1 If User put Wrong OTP Warning Comes up OTP not Valid.



15. After Verified Credentials Parts User Click on Next and Active Directory Configuration Window will open.

A screenshot of the "Max Secure Active Directory Synchronization setup" window. The window has a yellow title bar and a tabbed interface with four tabs: "Introduction", "Max Secure Credentials", "AD Configuration" (which is selected), and "Sync Schedule". The "AD Configuration" tab contains four input fields: "Host Name/ Ip Address of your Active Directory LDAP server:" (with a blue border), "Port: (Enter port as '389')", "Active Directory Username:", and "Active Directory Password:". At the bottom right of the window are three buttons: "Back", "Next", and "Finish".

16. User need to fill Hostname/ IP address of AD Server, Port should be 389, Active Directory Username and password which Set on the Time of Creation of AD Server.
- 16.1 If User Want to Validate the AD Server with IP Address.



The screenshot shows the 'Max Secure Active Directory Synchronization setup' window. It has a title bar with standard window controls. Below the title bar is a tabbed interface with four tabs: 'Introduction', 'Max Secure Credentials', 'AD Configuration', and 'Sync Schedule'. The 'AD Configuration' tab is selected. The main content area contains four input fields: 'Host Name/ Ip Address of your Active Directory LDAP server:' with the value '192.168.1.11', 'Port: (Enter port as '389')' with the value '389', 'Active Directory Username:' with the value 'administrator', and 'Active Directory Password:' with a masked password '*****'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Finish'.

Max Secure Active Directory Synchronization setup

Introduction Max Secure Credentials AD Configuration Sync Schedule

Host Name/ Ip Address of your Active Directory LDAP server:
192.168.1.11

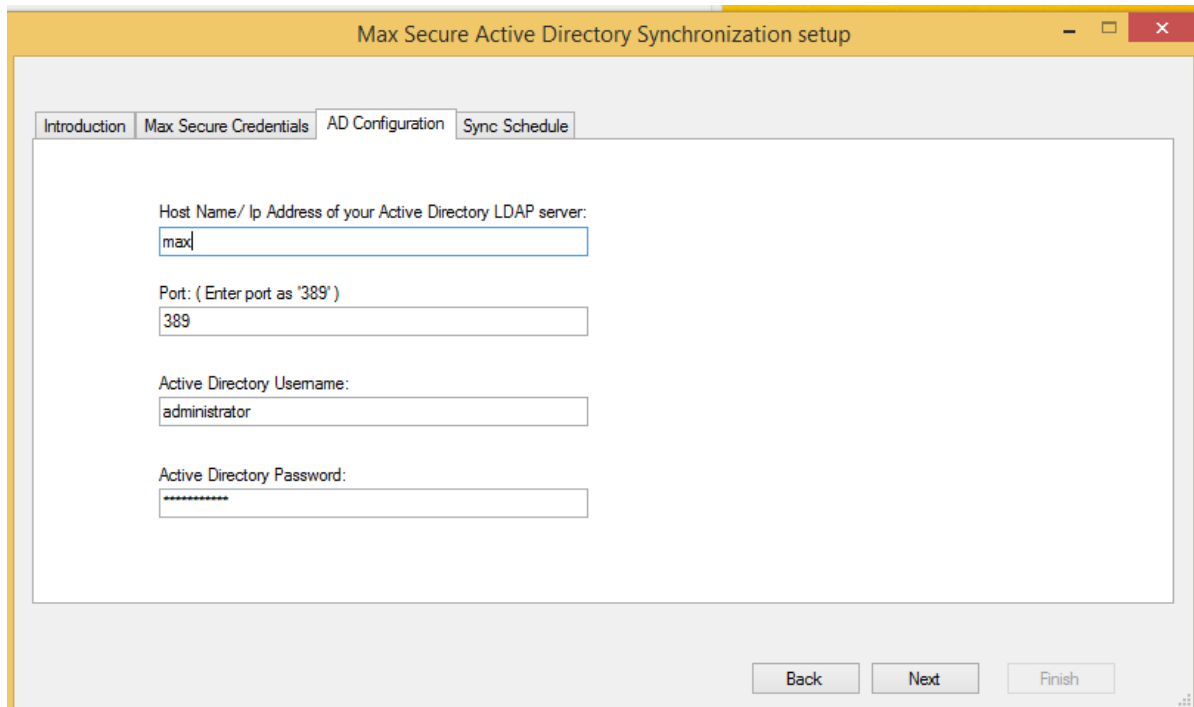
Port: (Enter port as '389')
389

Active Directory Username:
administrator

Active Directory Password:

Back Next Finish

16.2 If User Want to Validate the AD Server with IP Address.



This screenshot is identical to the previous one, showing the 'Max Secure Active Directory Synchronization setup' window with the 'AD Configuration' tab selected. The input fields are the same, but the 'Host Name/ Ip Address of your Active Directory LDAP server:' field now contains the text 'max' instead of an IP address. The 'Port', 'Username', and 'Password' fields remain unchanged. The 'Back', 'Next', and 'Finish' buttons are still present at the bottom right.

Max Secure Active Directory Synchronization setup

Introduction Max Secure Credentials AD Configuration Sync Schedule

Host Name/ Ip Address of your Active Directory LDAP server:
max

Port: (Enter port as '389')
389

Active Directory Username:
administrator

Active Directory Password:

Back Next Finish

17. Now User Click On Next and Sync Schedule Window Comes.

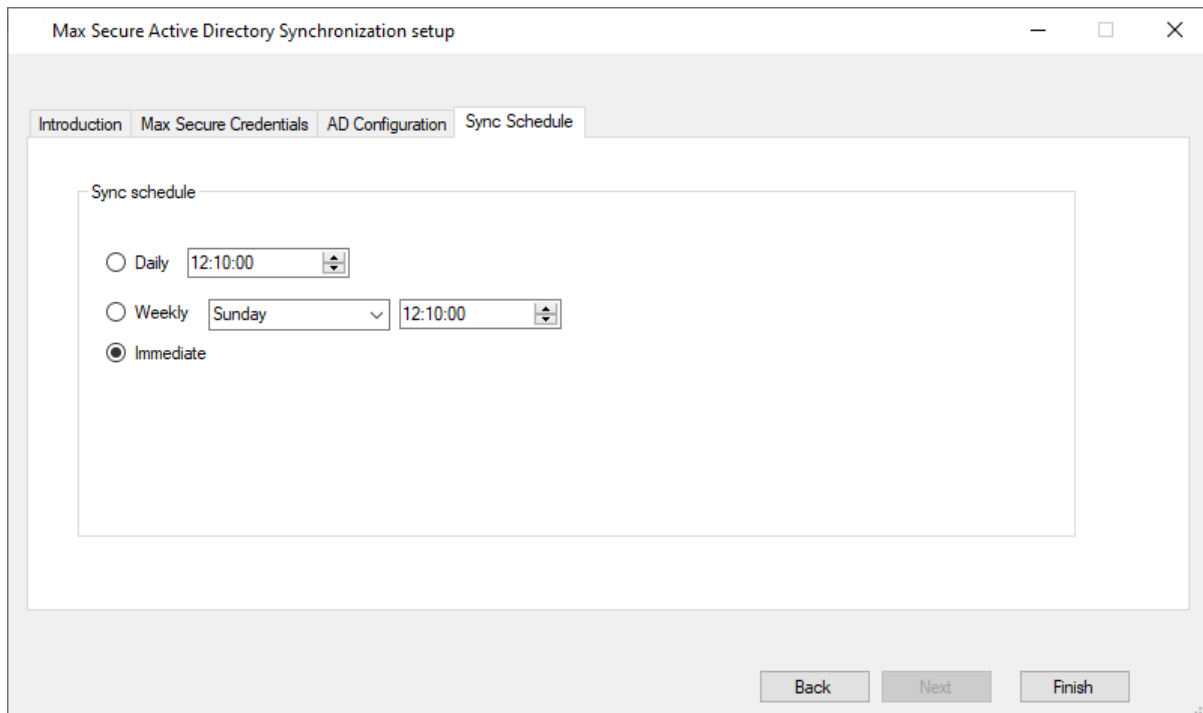
17.1 If User Want to Set Sync Schedule Daily on what time.

The screenshot shows the 'Max Secure Active Directory Synchronization setup' window with the 'Sync Schedule' tab selected. The 'Sync schedule' section contains three radio button options: 'Daily' (selected), 'Weekly', and 'Immediate'. The 'Daily' option is accompanied by a time dropdown menu set to '12:10:00'. The 'Weekly' option is accompanied by a day dropdown menu set to 'Sunday' and a time dropdown menu set to '12:10:00'. The 'Immediate' option has no associated fields. At the bottom right, there are three buttons: 'Back', 'Next', and 'Finish'.

17.2 If User Want to Set Sync Schedule Weekly on which day and time.

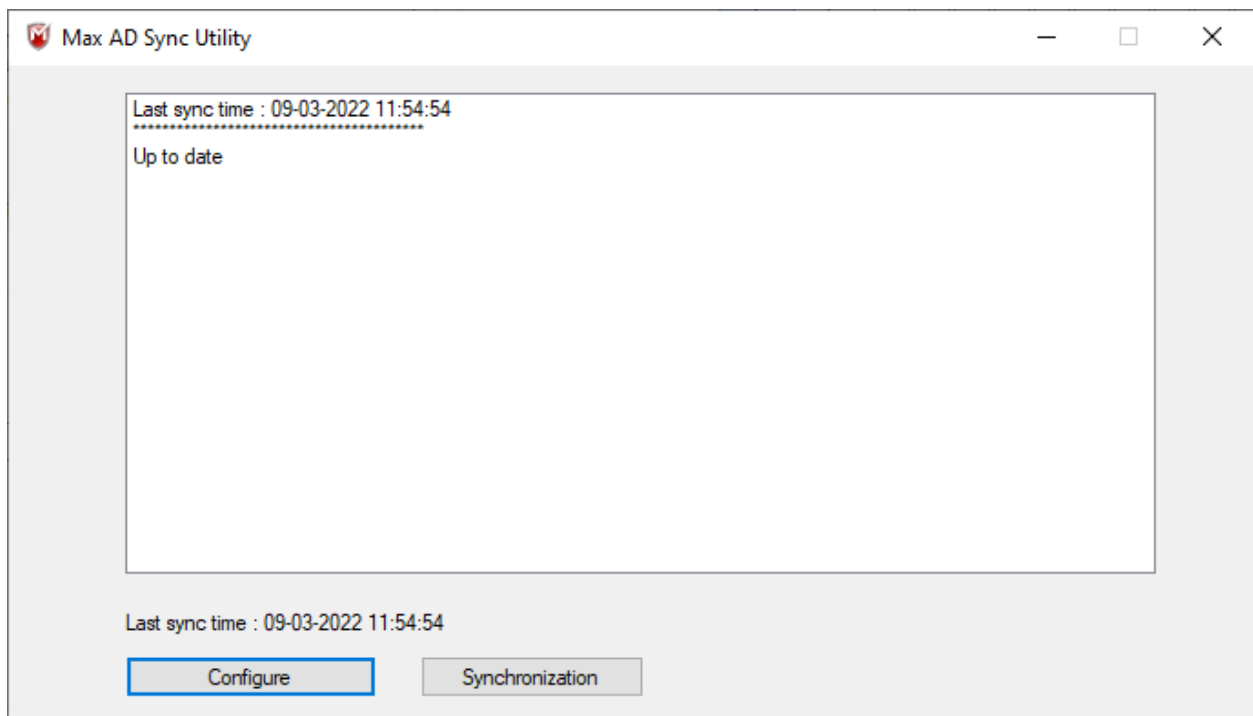
The screenshot shows the 'Max Secure Active Directory Synchronization setup' window with the 'Sync Schedule' tab selected. The 'Sync schedule' section contains three radio button options: 'Daily', 'Weekly' (selected), and 'Immediate'. The 'Daily' option is accompanied by a time dropdown menu set to '12:10:00'. The 'Weekly' option is accompanied by a day dropdown menu set to 'Sunday' and a time dropdown menu set to '12:10:00'. The 'Immediate' option has no associated fields. At the bottom right, there are three buttons: 'Back', 'Next', and 'Finish'.

17.3 If User Want to Set Sync Schedule Immediate.



The screenshot shows the 'Max Secure Active Directory Synchronization setup' window. It has four tabs: 'Introduction', 'Max Secure Credentials', 'AD Configuration', and 'Sync Schedule'. The 'Sync Schedule' tab is active. Inside the tab, there is a 'Sync schedule' section with three radio button options: 'Daily' (selected with a time of 12:10:00), 'Weekly' (selected with a day of Sunday and a time of 12:10:00), and 'Immediate' (which is selected with a filled radio button). At the bottom of the window, there are three buttons: 'Back', 'Next', and 'Finish'.

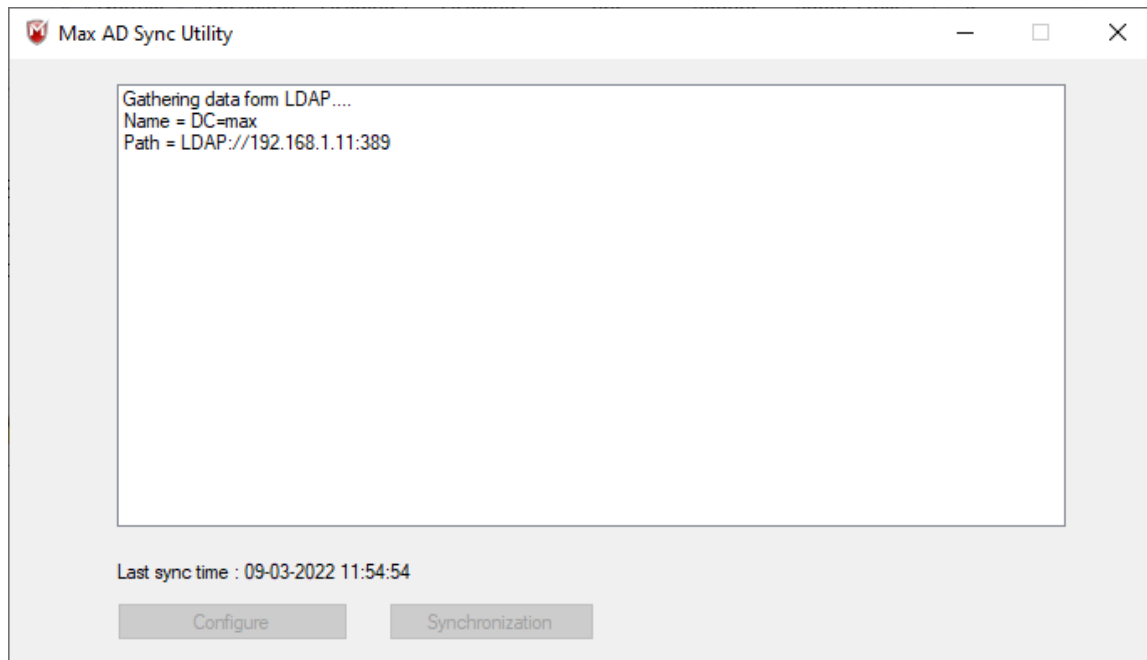
18. After that Click On Finish then Synchronization Option Enable.



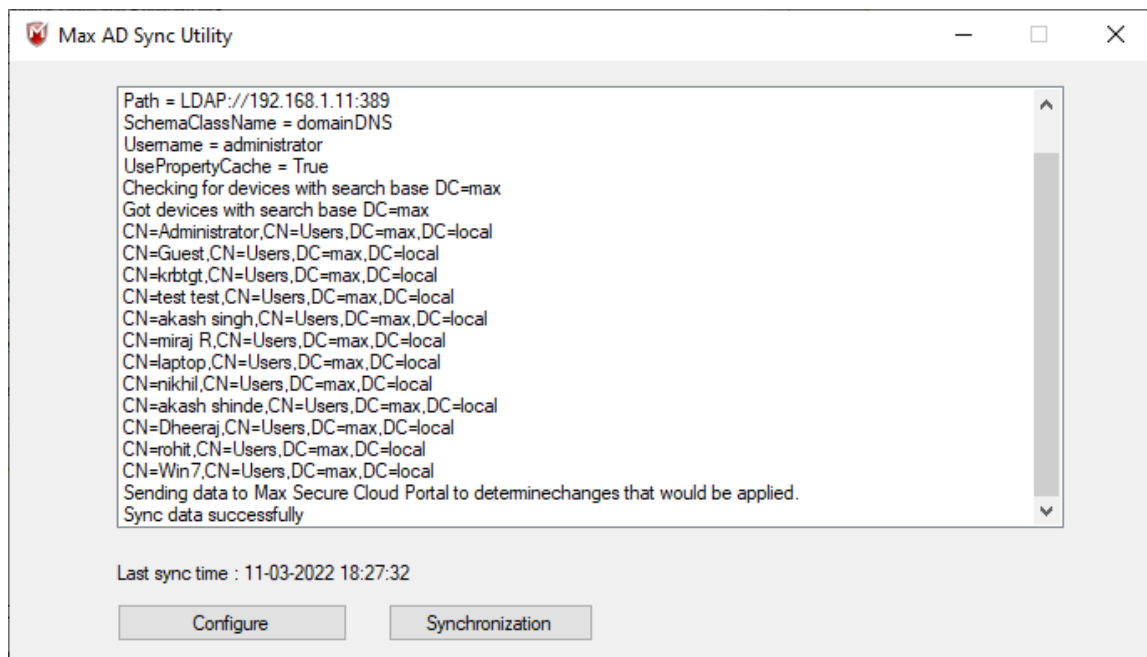
The screenshot shows the 'Max AD Sync Utility' window. It displays the 'Last sync time : 09-03-2022 11:54:54' and the status 'Up to date'. At the bottom, there are two buttons: 'Configure' and 'Synchronization'. The 'Configure' button is highlighted with a blue border.

19. If you want to start Immediate Sync then Click on Synchronization Option or if you set timer for Synchronization then close the application and open after the set time then last sync time will be updated to your set time and sync up to date.

19.1 Sync Start.



19.2 Sync Finish.



20. Now all data fetch Will be Shown in Portal i.e. Device Name, Email, Status.

Active Directory Verification OTP

9G64J333 [Download Installer](#)

Note : To launch this installer your machine should have Dot Net Version 4.5 or above.

Search [Email Setup Link](#) Active Devices

<input type="checkbox"/>	Device Name	Email	Status
<input type="checkbox"/>	Win7	s@gn	Enable
<input type="checkbox"/>	nikhil	nikhil@maxpcsecure.com	Enable
<input type="checkbox"/>	miraj R	miraj@maxpcsecure.com	Enable
<input type="checkbox"/>	Dheeraj	Dheeraj@maxpcsecure.com	Enable
<input type="checkbox"/>	akash singh	akashsingh@maxpcsecure.com	Enable
<input type="checkbox"/>	test test	akashs@maxpcsecure.com	Enable
<input type="checkbox"/>	akash shinde	akashs@maxpcsecure.com	Enable
<input type="checkbox"/>	Administrator		Enable

Show 10 entries

20.1 Active Devices are those devices which Status is Enable in AD Server.

Active Directory Verification OTP

9G64J333 [Download Installer](#)

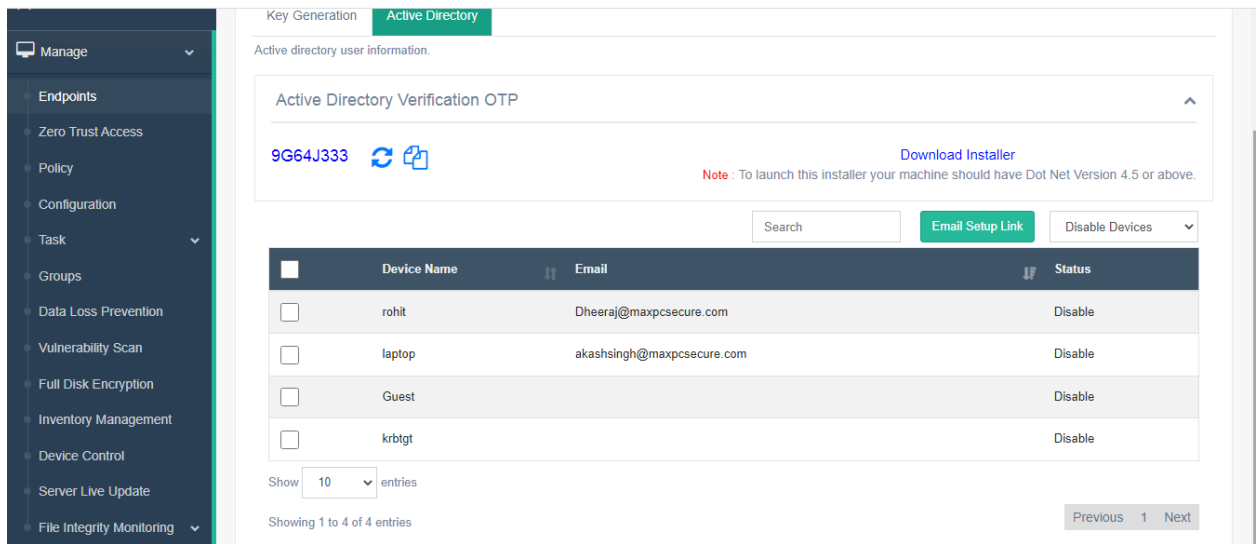
Note : To launch this installer your machine should have Dot Net Version 4.5 or above.

Search [Email Setup Link](#) Active Devices

<input type="checkbox"/>	Device Name	Email	Status
<input type="checkbox"/>	Win7	s@gn	Enable
<input type="checkbox"/>	nikhil	nikhil@maxpcsecure.com	Enable
<input type="checkbox"/>	miraj R	miraj@maxpcsecure.com	Enable
<input type="checkbox"/>	Dheeraj	Dheeraj@maxpcsecure.com	Enable
<input type="checkbox"/>	akash singh	akashsingh@maxpcsecure.com	Enable
<input type="checkbox"/>	test test	akashs@maxpcsecure.com	Enable
<input type="checkbox"/>	akash shinde	akashs@maxpcsecure.com	Enable
<input type="checkbox"/>	Administrator		Enable

Show 10 entries



20.2 Disable Devices are those devices which Status is Disable in AD Server.



Key Generation **Active Directory**

Active directory user information.

Active Directory Verification OTP

9G64J333  

[Download Installer](#)

Note : To launch this installer your machine should have Dot Net Version 4.5 or above.

Search [Email Setup Link](#) [Disable Devices](#)

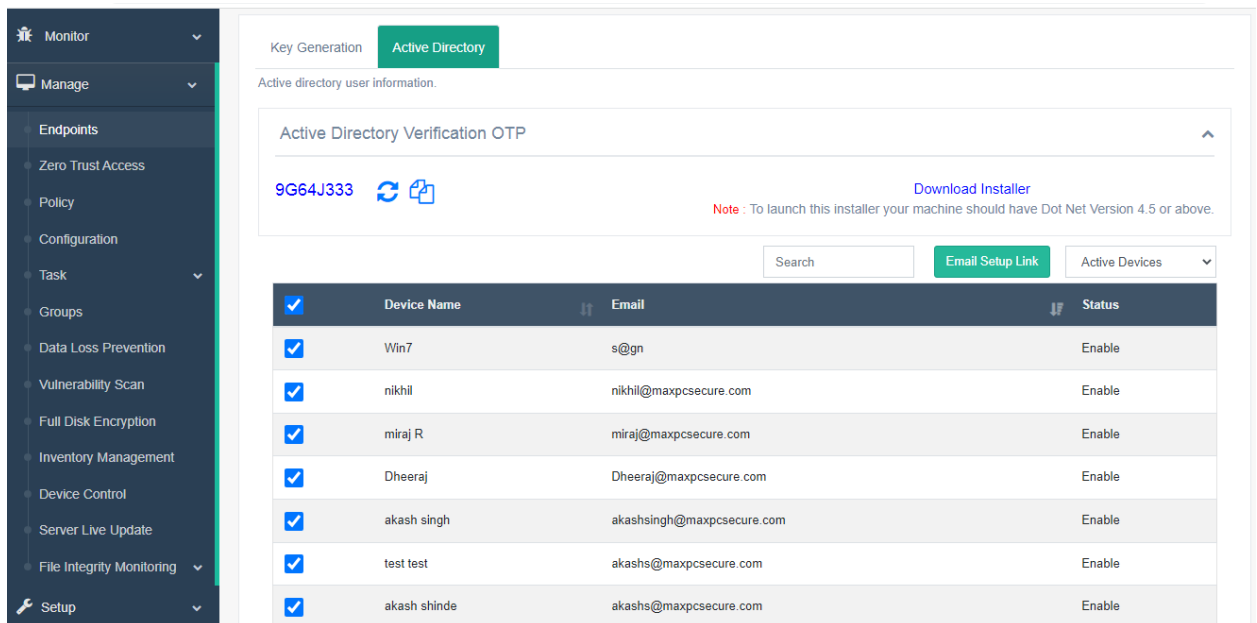
<input type="checkbox"/>	Device Name	Email	Status
<input type="checkbox"/>	rohit	Dheeraj@maxpcsecure.com	Disable
<input type="checkbox"/>	laptop	akashsingh@maxpcsecure.com	Disable
<input type="checkbox"/>	Guest		Disable
<input type="checkbox"/>	krbtgt		Disable

Show 10 entries

Showing 1 to 4 of 4 entries

Previous 1 Next



21. From Portal Admin Can Send Setup Link to Clients Which are active or Disable in AD by their Email Address. Email Setup Link can be send one to one or multiple users also.



Key Generation **Active Directory**

Active directory user information.

Active Directory Verification OTP

9G64J333  

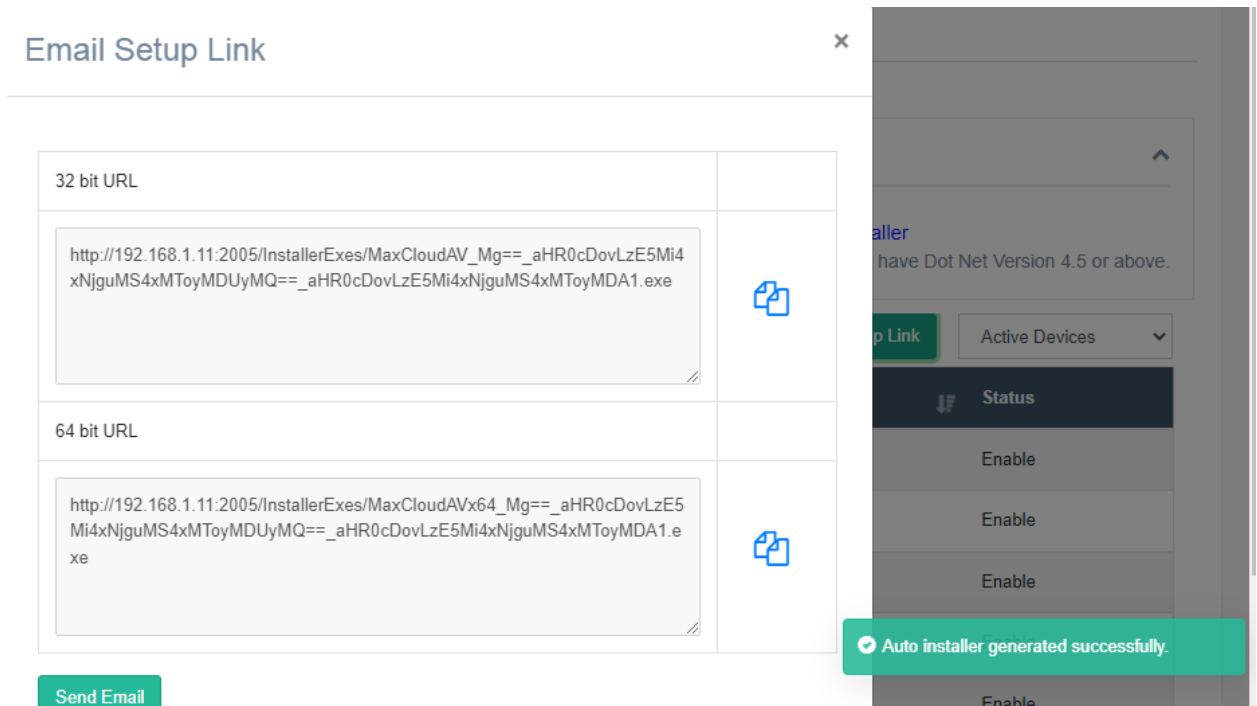
[Download Installer](#)

Note : To launch this installer your machine should have Dot Net Version 4.5 or above.

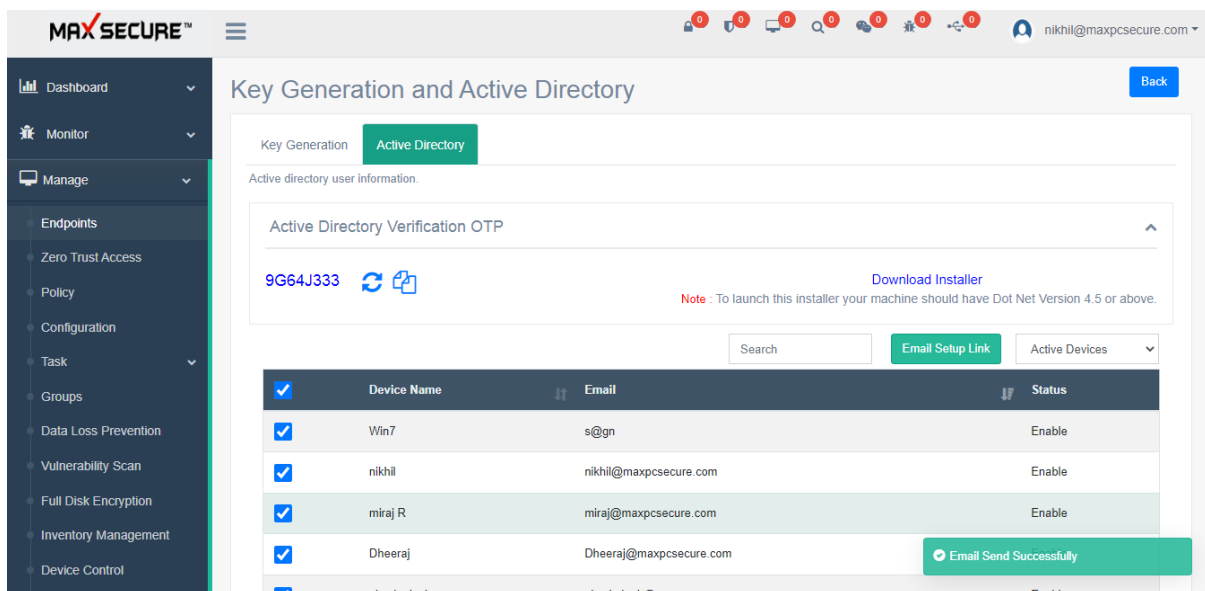
Search [Email Setup Link](#) [Active Devices](#)

<input checked="" type="checkbox"/>	Device Name	Email	Status
<input checked="" type="checkbox"/>	Win7	s@gn	Enable
<input checked="" type="checkbox"/>	nikhil	nikhil@maxpcsecure.com	Enable
<input checked="" type="checkbox"/>	miraj R	miraj@maxpcsecure.com	Enable
<input checked="" type="checkbox"/>	Dheeraj	Dheeraj@maxpcsecure.com	Enable
<input checked="" type="checkbox"/>	akash singh	akashsingh@maxpcsecure.com	Enable
<input checked="" type="checkbox"/>	test test	akashs@maxpcsecure.com	Enable
<input checked="" type="checkbox"/>	akash shinde	akashs@maxpcsecure.com	Enable

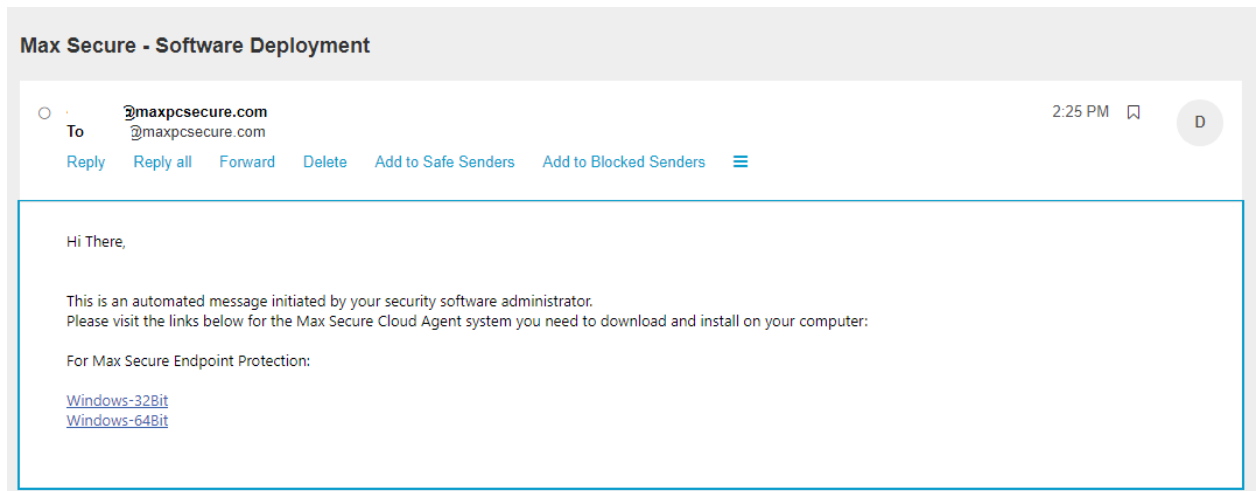
22. After Select all the Users and Click on Email Setup Link new Window popup comes up.



23. After that Admin Need to Click on Send Email, message of Email sent successfully comes in bottom of page.



24. Email which Users Received looks like this.



Actions

Manage → Endpoints → Actions

Right after installing client setups on device, you can start applying various action items.

Actions for Windows Devices

MAXSECURE™

Endpoints

Select Type: Windows

Name	IP	OS	Policy	Date	Status
DESKTOP-2F0UOB2	192.168.1.7	windows 10 pro	Default Policy	11-01-2022 12:36:40 PM	Active
AKASH	192.168.1.6	windows 10 pro n	newone	07-01-2022 11:08:31 AM	Active
WIN-3L25PHS4FBB	192.168.1.25	windows server 2019 standard evaluation	server20219	29-12-2021 10:29:45 AM	Inactive
DESKTOP-A8NSVJ8	192.168.1.11	windows 10 pro	Check	10-12-2021 02:43:56 PM	Inactive
TUSHARWIN10	193.168.0.130	windows 10 enterprise Itsc 2019	Tushar	09-12-2021 03:16:36 PM	Inactive

- Antitheft
- Disable Network
- Firewall
- Full Disk Encryption
- Live Update Now
- Log Off
- Offline Live Update
- RollBack
- Scan Device
- Shutdown PC
- USB Protection Disable
- Uninstall Device
- Vulnerability Scan
- FIM Scan

No.	Description	Manage → Endpoints → Action
1	Anti-Theft	<p>Once you select a device → you have several options in case your laptop is stolen. Location service will start sending the current location of the device to the portal.</p> <ul style="list-style-type: none"> • Mark it as 'Lost' • Select 'Lock my Device' and type message in the Display field. • <i>Use Case:</i> You can display your phone no. on locked screen of laptop so that person who found it can call you and return the laptop. • Wipe Data • Take Snapshot: If enabled, laptop will start taking pictures and send it to the dashboard. This may help you identify the location or the photos of the person or place <p><i>Note: If a device is stolen, click on Manage → Endpoints → Device Name and it will open Device details page where you can see the location and snapshots of the place and person</i></p>
2	Disable Network	Admin can remove any selected device from the network
3	Firewall	Install/Uninstall Firewall from here on selected devices (Windows)
4	Full Disk Encryption	<p>Enable full disk encryption module on the selected devices. Any folder on PC or USB/external hard disk drive folder can be encrypted using this option on the devices where this module is enabled. <i>Note: Only on these devices one can decrypt data with password.</i></p>
5	Live-update	<p><i>On demand Admin can immediately update selected client agents.</i></p> <p>Client agents have a default update schedule and Admin can change it from Manage → Configuration → Scheduler.</p>
6	Logoff	Logoff selected devices
7	Offline Live update	Allow Client agents to take update locally from On-premises server. Turning off will allow you to take update globally.

8	Roll Back	In case there are any issue with Client update, you can roll back to previous versions
9	Scan Device	Client agents can be scanned for Anti-virus scan immediately by selecting the devices. By default Client agent does background scan (without user interface opening up on devices) on scheduled time.
10	Shut down PC	Remotely shutdown any device
11	USB protection disable	Even if you have USB protection on all devices, by selecting this option USB protection can be disabled temporarily.
12	Uninstall Device	Selecting this will uninstall client agent from that device.
13	Vulnerability scan	Immediately do vulnerability scan on the selected devices
14	FIM Scan	On demand Admin can run FIM (File Integrity Monitor) scan.

1. Antitheft

Click on Endpoints name to view Anti-Theft information collected from client device such as lost device location and stolen pics

Follow these steps for 'Antitheft':

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. *Select Antitheft*
5. *Select option to Lock My Device, Wipe Data or Take Snapshot, you can also enter message to display it on lost device.*
6. Click on Apply button

Anti-Theft Settings



☒ Lost ☒ Lock My Device ☒ Wipe Data ☒ Take Snapshot

Username : akash

Password :

Display Message on Laptop:

Return it immediately

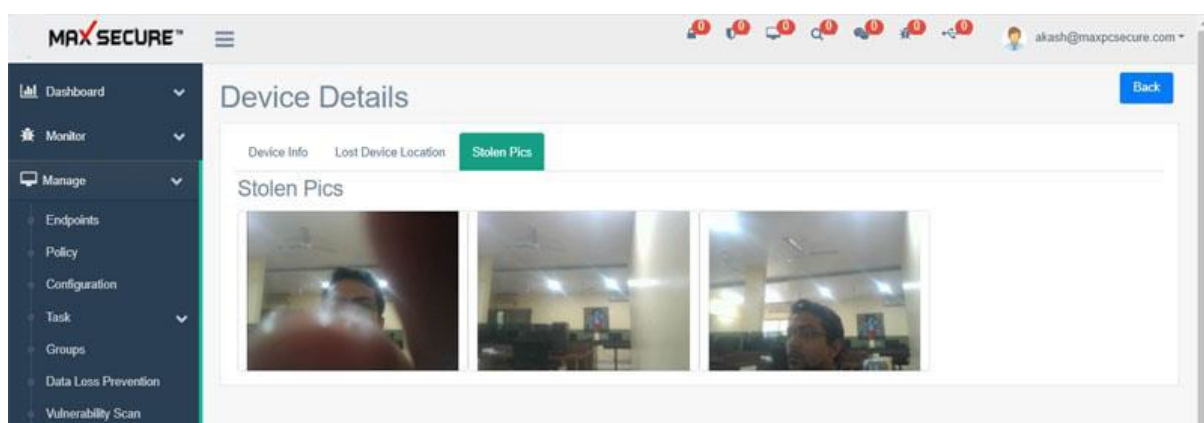
Close

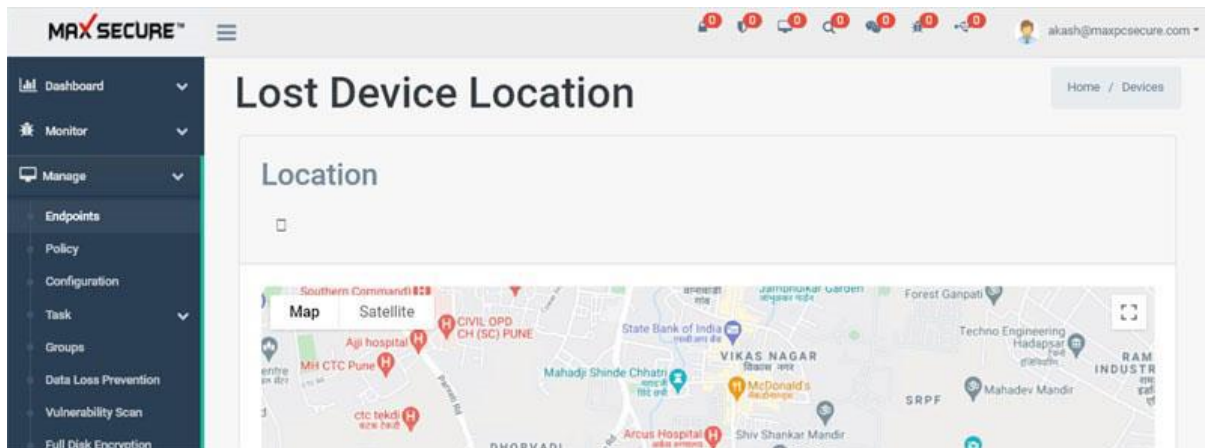
Apply

How can we see lost device report?

Here you can see lost device report:

1. Go to Manage > Endpoints
2. Click on device name
3. Device lost details will be showing.



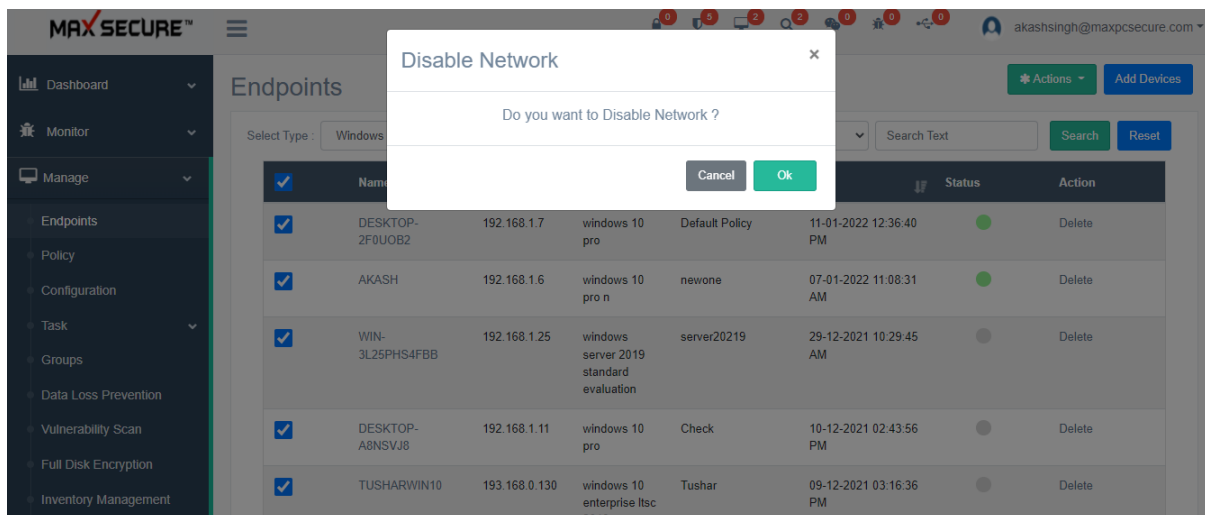


2. Disable Network

To disable your network. Disconnect Client's PC from LAN & Internet both. This will disconnect your client's PC from a network. It can be helpful when there is any infected PC in a network.

Follow these steps for 'Disable Network':

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select *Disable Network*
5. Click on 'OK' button for confirmation

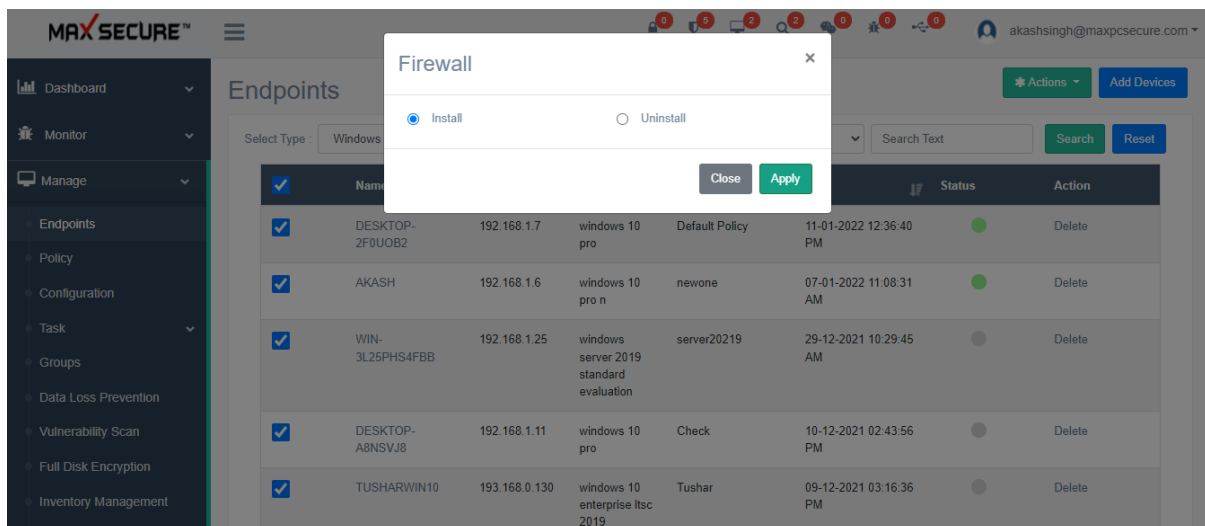


3. Firewall

To monitor network traffic. To restrict internet usage, prevent malicious behaviour, protect running processes and filter web content.

Follow these steps to install/uninstall firewall on client agent machine:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select Firewall
5. Select Install/Uninstall
6. Click on 'Apply' button.

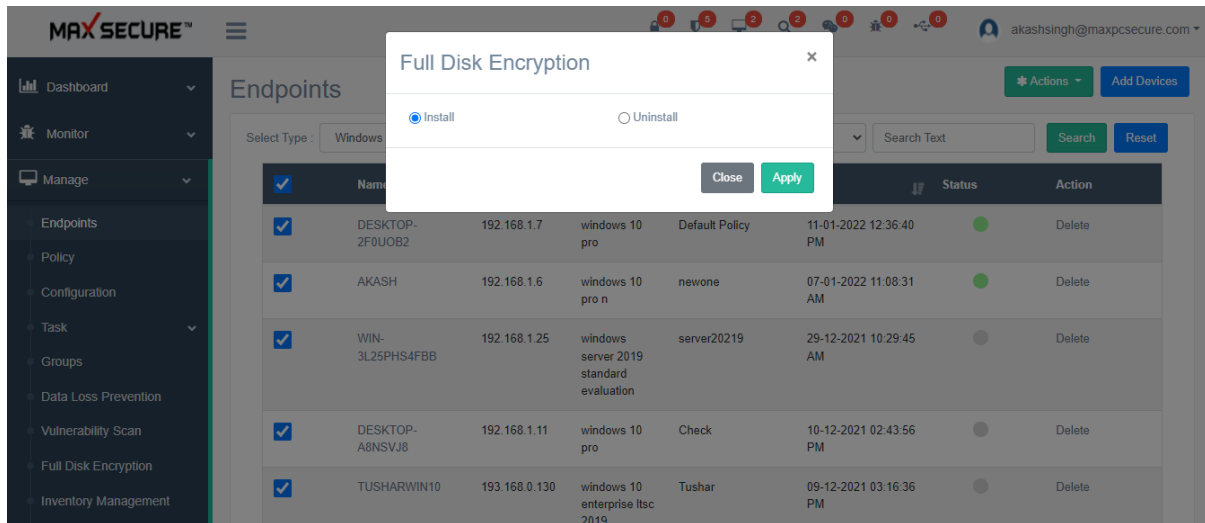


4. Full Disk Encryption

Enable/Disable full disk encryption module on the selected devices. Any folder on PC or USB/external hard disk drive folder can be encrypted using this option on the devices where this module is enabled. *Note: Only on these devices one can decrypt data with password.*

Follow these steps to update client agent remotely:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select Live Update Now
5. Click on 'Apply' button for confirmation

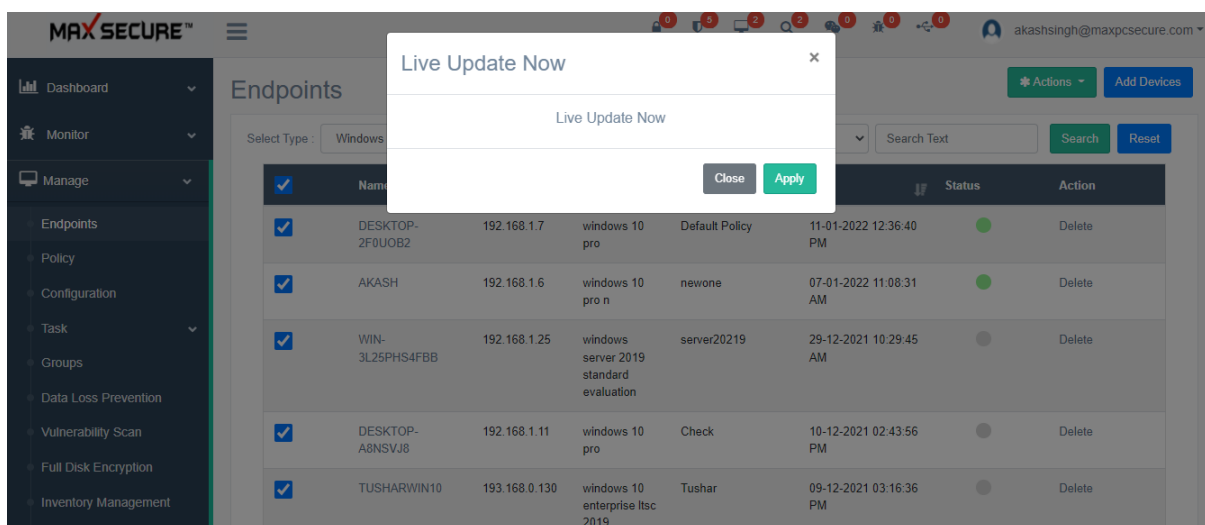


5. Live-update

On demand Admin can immediately update selected client agents. Client agents have a default update schedule and Admin can change it from Manage → Configuration → Scheduler.

Follow these steps to update client agent remotely:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. *Select Live Update Now*
5. Click on 'Apply' button for confirmation

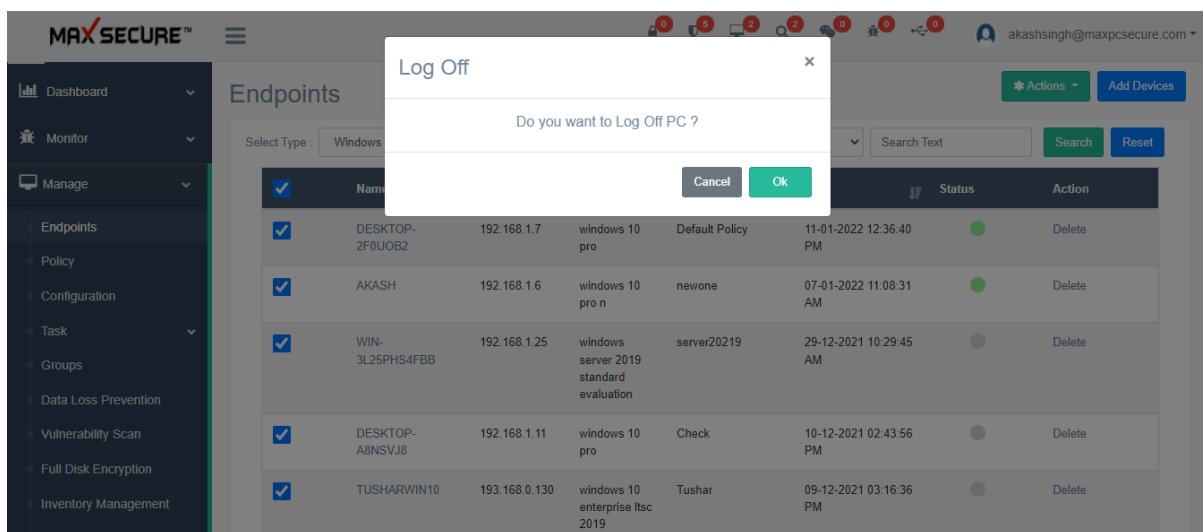


6. Log Off

Sign-out from your existing user.

Follow these steps to log off client agent PC:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. *Select Log Off*
5. Click on 'OK' button for confirmation

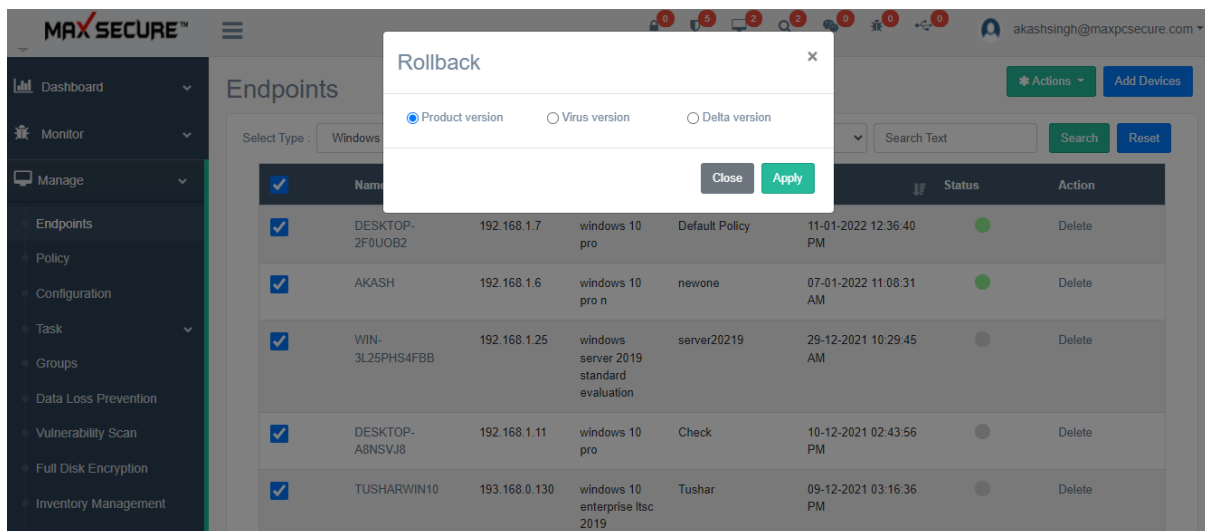


7. Rollback

In case there are any issue with client **updates**, you can roll back to previous versions, there is an option to rollback Product Version, Virus Version & Delta Version.

Follow these steps to rollback client agent's updates:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. *Select Rollback*
5. *Select option to choose rollback for product version, virus version or delta version*
6. Click on 'Apply' button

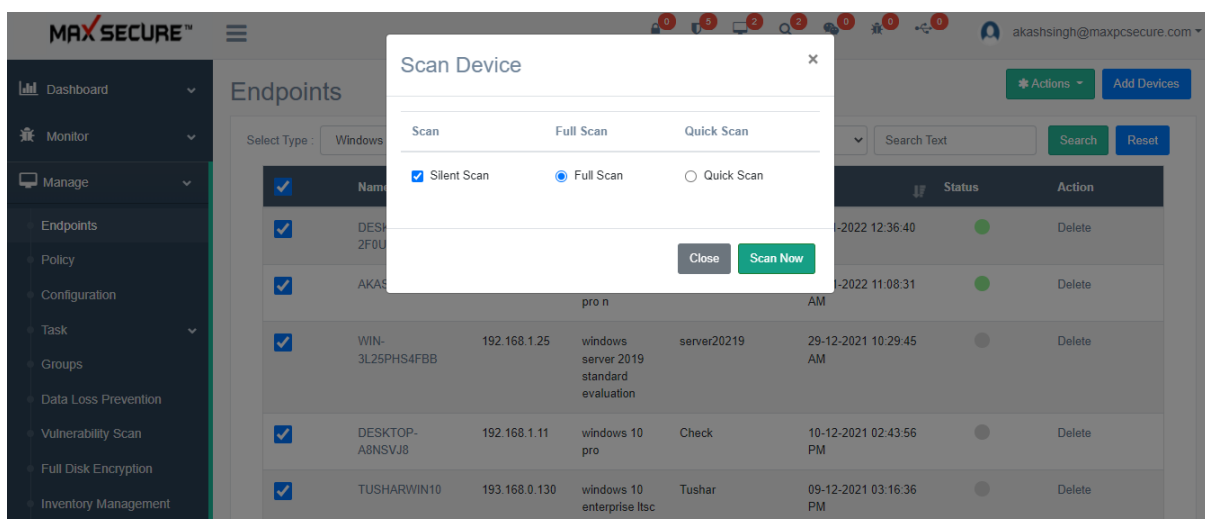


8. Scan Device

To run on demand scan for malicious files on your Client's PC which keeps their device protected.

Follow these step to scan client agent on demand:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. *Select Scan Device*
5. Select 'Silence scan' in order to perform scanning silently in background without knowing and affecting the client's work. You can uncheck silence scan checkbox which will open UI and scan client's PC.
6. Select option for Full System Scan or Quick Scan; select Radio-button accordingly.
7. Click on 'Scan Now' button for confirmation.

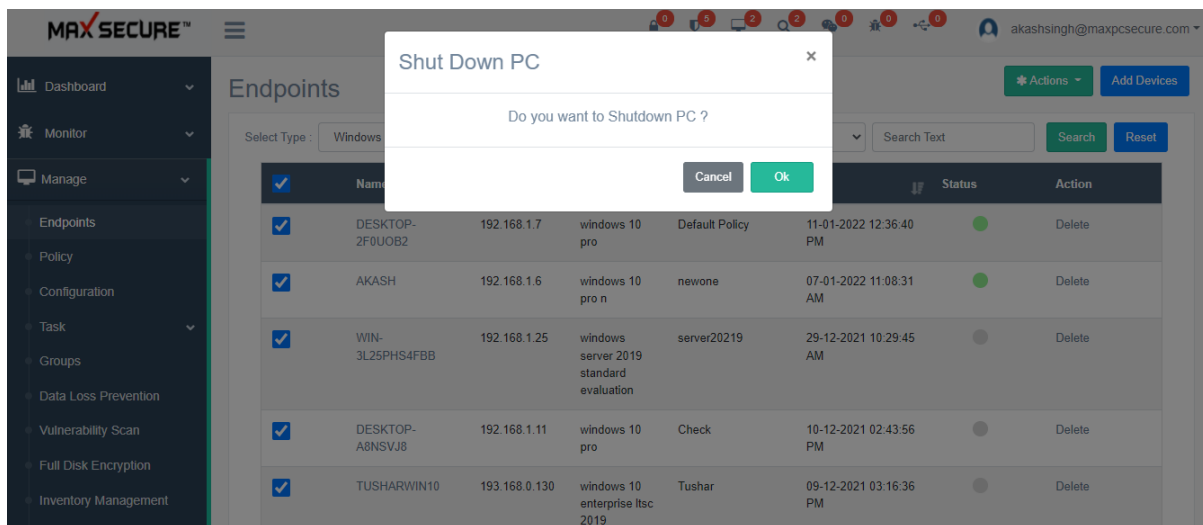


9. Shutdown PC

To shut down client's PC.

Follow these step to shut down client agent:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select Shutdown PC
5. Click on 'OK' button for confirmation

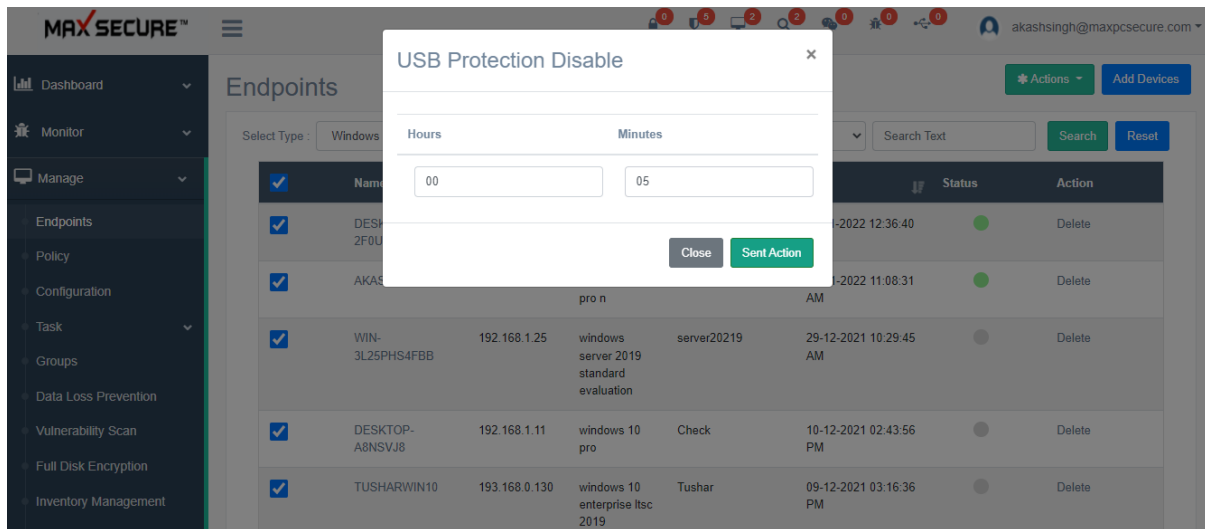


10.USB Protection

To uninstall Max Cloud AV product from client's PC but this leads to client's PC unprotected. This will remove all control to client's PC from server portal and makes client's PC unprotected.

Follow these step to uninstall client agent remotely:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select Uninstall Device
5. Click on 'Uninstall' button for confirmation

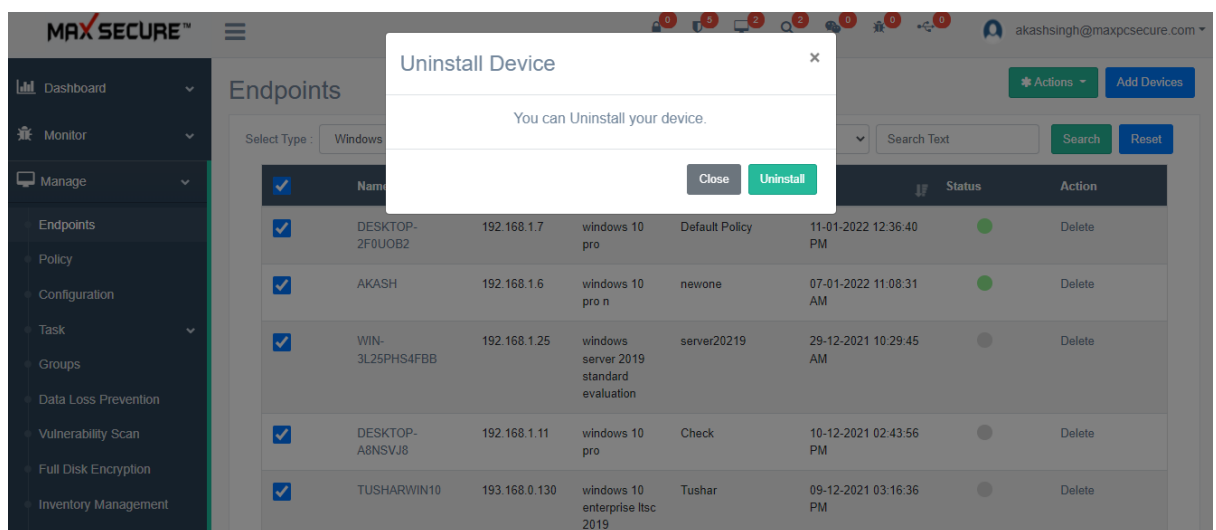


11. Uninstall Device

To uninstall Max Cloud AV product from client's PC but this leads to client's PC unprotected. This will remove all control to client's PC from server portal and makes client's PC unprotected.

Follow these step to uninstall client agent remotely:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select *Uninstall Device*
5. Click on 'Uninstall' button for confirmation

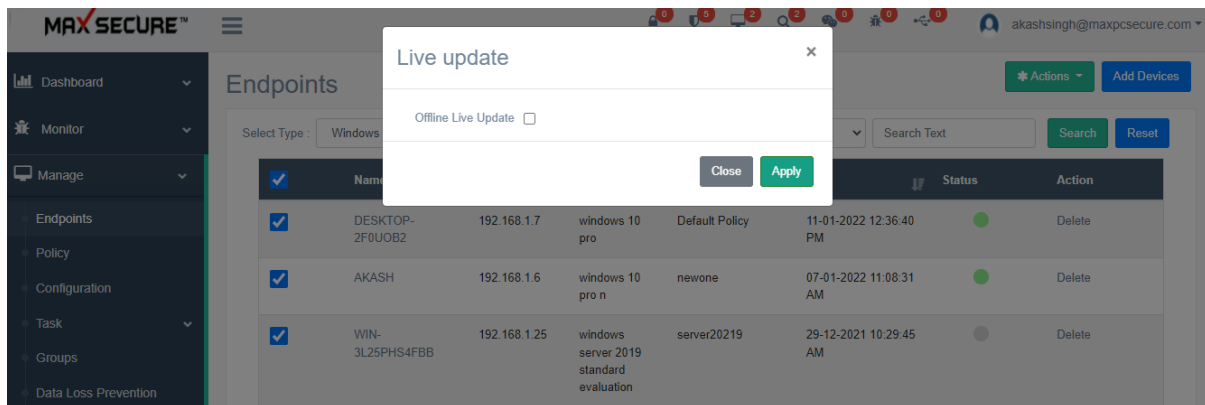


12. Offline Live Update

This action is for local live update, by default this option is unchecked but you can turn it ON in order to update client agent locally.

Follow these step to uninstall client agent remotely:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Click on 'Actions' button.
4. Select *Offline Live Update*
5. Check/Uncheck *Offline Live Update*
6. Click on 'Apply' button

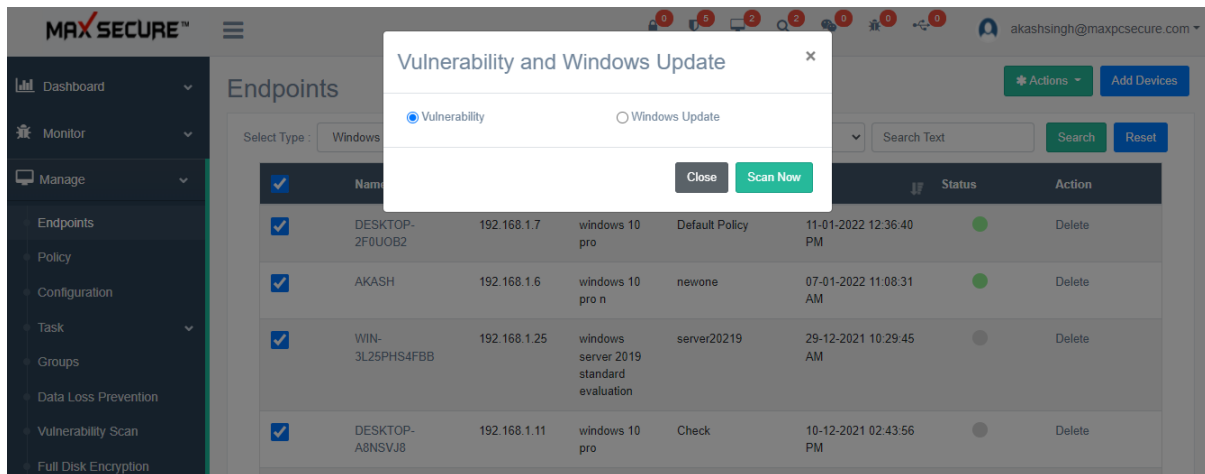


13. Vulnerability Scan

This action will provide the information about Client's PC remaining security and Windows Update; it can be used to download all windows security updates.

Follow these step to run vulnerability scan on client agent side:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Go to 'Actions' button
4. Select Vulnerability Scan
5. Select Vulnerability for showing only security updates or select Windows update for showing windows update.
6. Click on 'Scan Now' button.

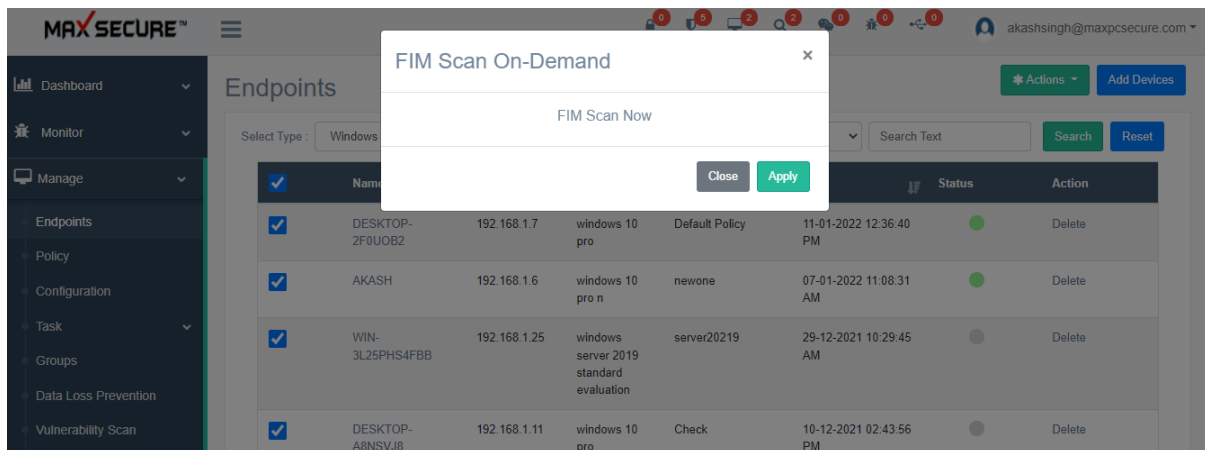


14.FIM Scan

This action will launch file integrity monitor scan on demand in order to check the integrity of file/directory as per the applied rule.

Follow these step to run vulnerability scan on client agent side:

1. Go to left side menu bar Manage → Endpoints
2. Select client agents.
3. Go to 'Actions' button
4. Select FIM Scan
5. Click on 'Apply' button.



Action for MAC Devices

In the Endpoint you can find way to Add Mac devices to this Portal, Scan them, apply policies and get reports.

For MAC devices, client agent list, follow below steps:

1. Go to Manage → Endpoints
2. Select 'Mac' from Select Type dropdown options.

Below is the action that we can apply on MAC devices remotely:

1. Scan Device

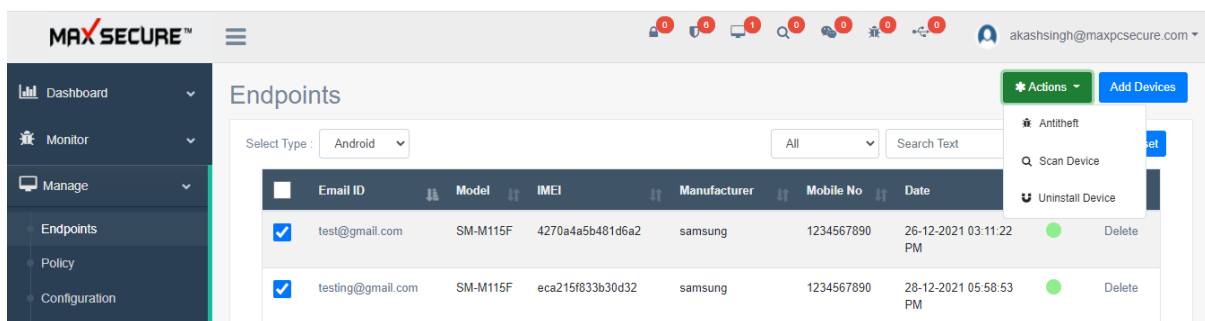


Action for Android Devices

Actions will let admin to run scan, turn on antitheft in case of stolen device on android devices remotely.

For MAC devices, client agent list, follow below steps:

1. Go to Manage → Endpoints
2. Select 'Android' from Select Type dropdown options.



Following are the actions that we can apply on android devices remotely:

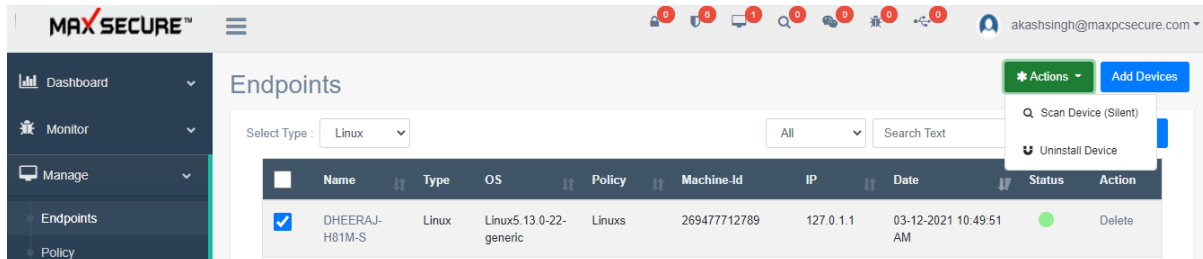
1. Antitheft
2. Scan Device
3. Uninstall Device

Action for Linux Devices

Actions will let admin to run scan and uninstall android devices remotely.

For Linux devices, client agent list, follow below steps:

1. Go to Manage → Endpoints
2. Select 'Linux' from Select Type dropdown options.



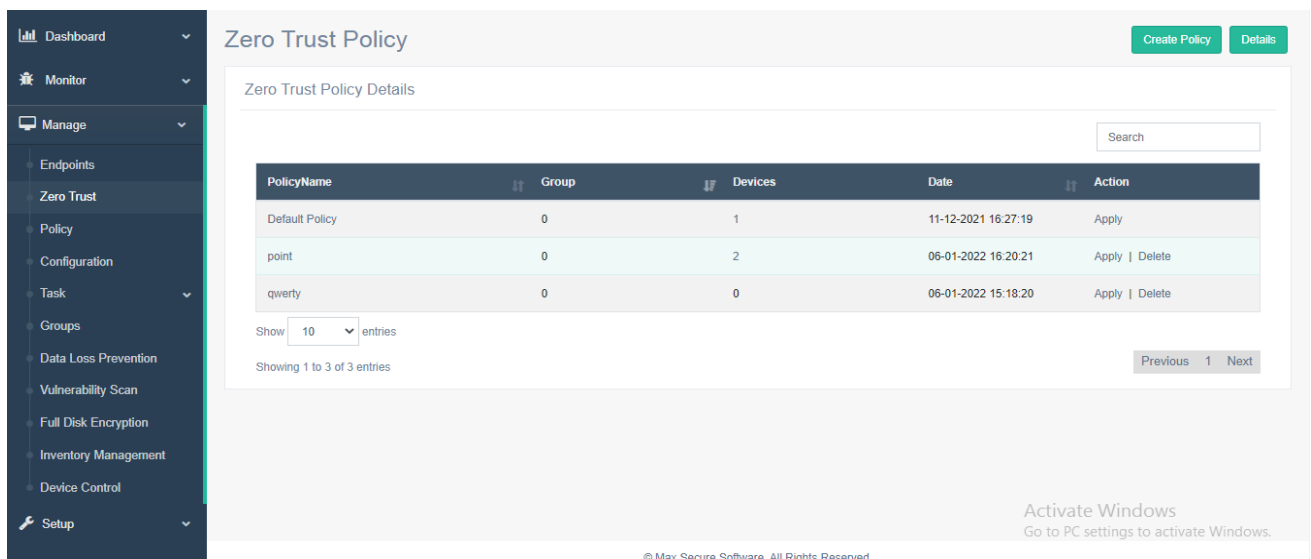
Following are the actions that we can apply on Linux devices remotely:

1. Scan Device
2. Uninstall Device

Zero Trust

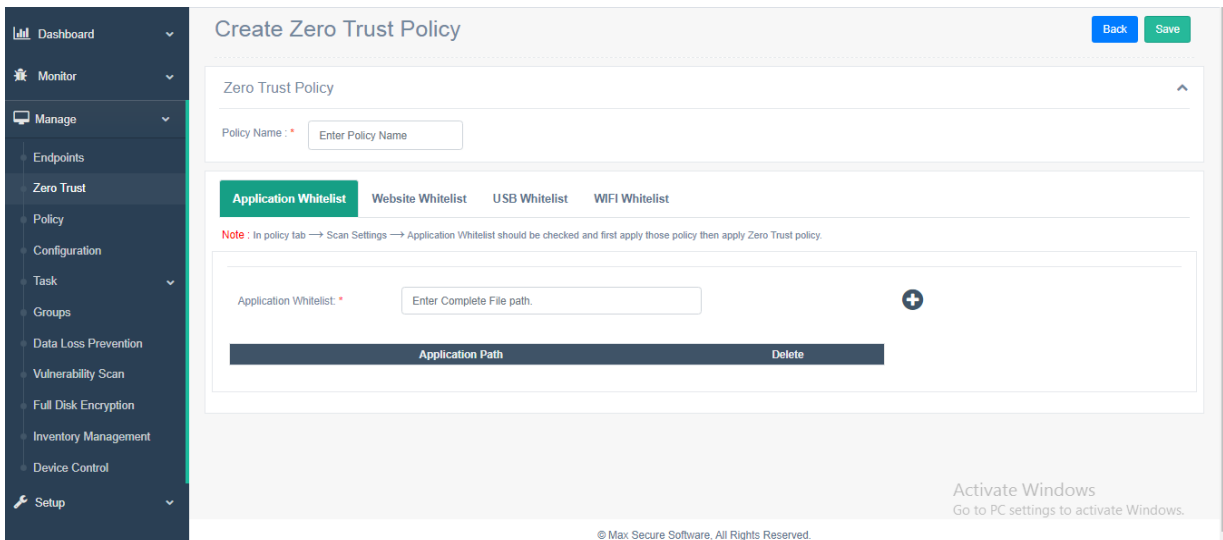
Zero Trust:- Zero Trust has high Priority comparing by another policy if user has to apply Zero Trust Policy then user cannot apply any other policy which are added in Zero Trust Policy.

Zero trust tab: - On Zero trust Tab you can see Create Policy Button, Details Button & Zero trust Policy Details.



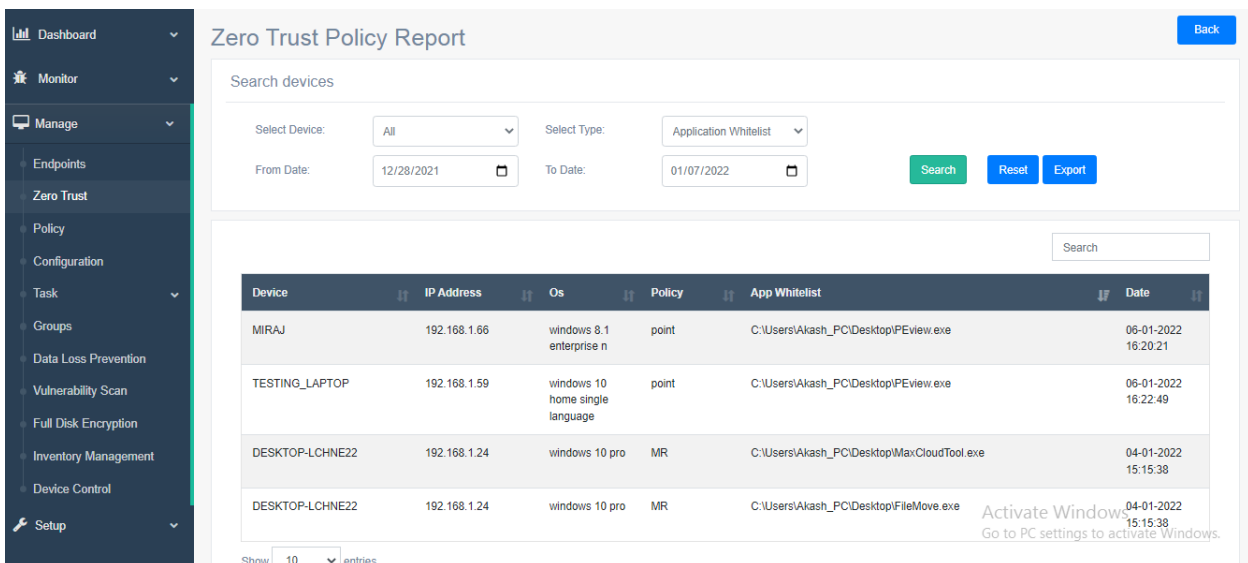
How to Create Policy for Zero Trust: - In this tab you can create policy For Application White list, Website White List, USB Whitelist & Wi-Fi Whitelist.

- Create one policy which you want and give name to the policy and save this policy. After policy get saved you can apply to client.
- If user can delete zero trust policy then policy is getting removed from client side & set default policy.



Details tab: - user can see the report on Details tab for which policy is apply to client and details what are added to policy. You can also export the report.

- You can select device and report type & Set a date for a specific report.
- There are option for select report like application whitelist, website whitelist, USB whitelist, Wi-Fi Whitelist.

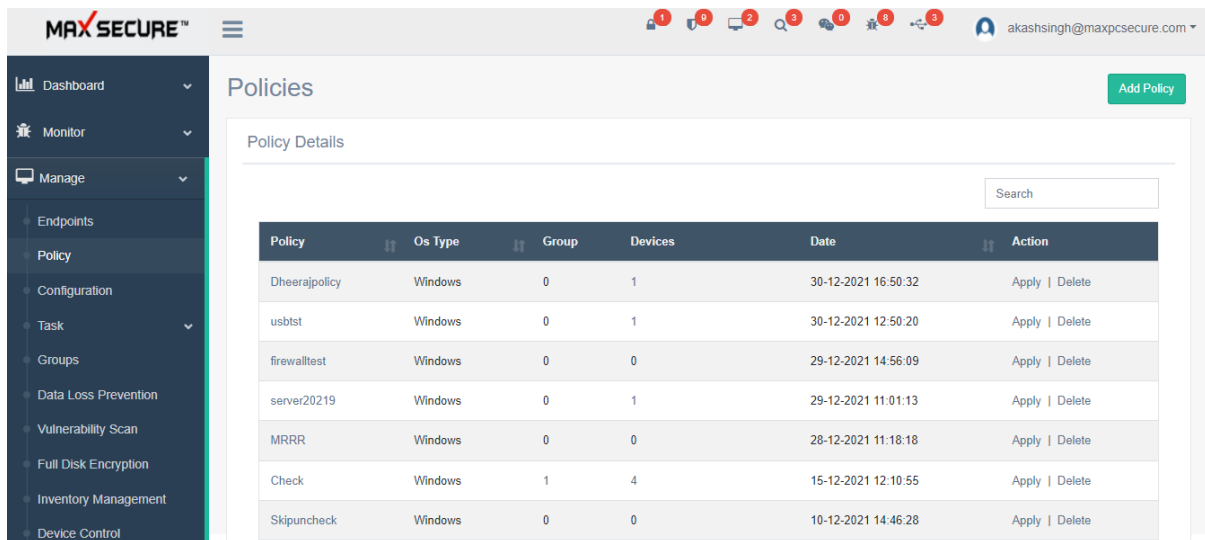


Device	IP Address	Os	Policy	App Whitelist	Date
MIRAJ	192.168.1.66	windows 8.1 enterprise n	point	C:\Users\Akash_PC\Desktop\PEview.exe	06-01-2022 16:20:21
TESTING_LAPTOP	192.168.1.59	windows 10 home single language	point	C:\Users\Akash_PC\Desktop\PEview.exe	06-01-2022 16:22:49
DESKTOP-LCHNE22	192.168.1.24	windows 10 pro	MIR	C:\Users\Akash_PC\Desktop\MaxCloudTool.exe	04-01-2022 15:15:38
DESKTOP-LCHNE22	192.168.1.24	windows 10 pro	MIR	C:\Users\Akash_PC\Desktop\FileMove.exe	04-01-2022 15:15:38

Policy

All client agents come with a default policy configuration so even if nothing is applied from the portal, clients will perform malware scan, vulnerability scan, report their hardware and software inventory to the portal, do backup and Restore of default extension files and update new malware definitions centrally from the portal at default schedule, every day.

However, Admin has full control over client application and can apply customized settings from here.



The screenshot shows the MAXSECURE™ web interface. The left sidebar has a 'Manage' dropdown menu with 'Policy' selected. The main content area is titled 'Policies' and contains a table of policy details. A search bar is located at the top right of the table.

Policy	Os Type	Group	Devices	Date	Action
Dheerajpolicy	Windows	0	1	30-12-2021 16:50:32	Apply Delete
usbtst	Windows	0	1	30-12-2021 12:50:20	Apply Delete
firewalltest	Windows	0	0	29-12-2021 14:56:09	Apply Delete
server20219	Windows	0	1	29-12-2021 11:01:13	Apply Delete
MRRR	Windows	0	0	28-12-2021 11:18:18	Apply Delete
Check	Windows	1	4	15-12-2021 12:10:55	Apply Delete
Skipunchcheck	Windows	0	0	10-12-2021 14:46:28	Apply Delete

Go on the left menu bar Manage → Policy → Add Policy allows you to customize features to manage **MAC Devices**.

Note: For the creation of MAC policy choose 'Select OS 'to Mac from given dropdown.

1. Auto Quarantine: If check box is selected then if any malware are found during scan then those files will be quarantined (deleted or repaired in case of virus) This option is used turn auto-clean On/Off.
2. Switch off Real-time Protection: If you would like to turn off Active Protection then uncheck this option.

The screenshot shows the 'Create Policy' page in the MAXSECURE portal. The left sidebar has a 'Manage' menu with 'Policy' selected. The main area has a 'Policy' header with a 'Back' button and a 'Save' button. Below the header, there is a 'Policy Name' field with a red asterisk and a 'Select OS' dropdown menu set to 'Mac'. A 'General Settings' tab is active, showing checkboxes for 'Auto Quarantine' and 'Realtime Protection', both of which are checked. The text 'Select/unselect checkboxes to enable/disable appropriate scan settings' is displayed above the checkboxes.

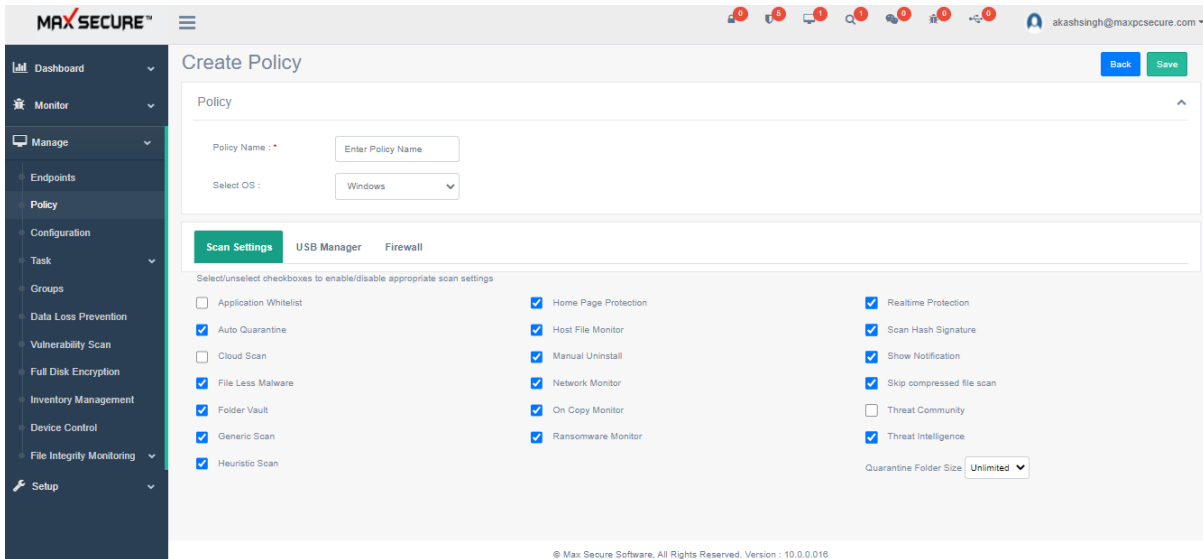
Go on the left menu bar Manage → Policy → Add Policy allows you to customize features to manage **Linux Devices**.

Note: For the creation of Linux policy choose 'Select OS 'to Linux from given dropdown.

1. Auto Quarantine: If check box is selected then if any malware are found during scan then those files will be quarantined (deleted or repaired in case of virus) This option is used turn auto-clean On/Off.
2. Manual Uninstall: If you would like to turn on protection then while uninstalling client agent it will ask password, if you give right valid password then only it will allow uninstallation of client.

The screenshot shows the 'Create Policy' page in the MAXSECURE portal, similar to the previous one but with 'Linux' selected in the 'Select OS' dropdown menu. The 'General Settings' tab is active, showing checkboxes for 'Auto Quarantine' (unchecked) and 'Manual Uninstall' (checked). The text 'Select/unselect checkboxes to enable/disable appropriate scan settings' is displayed above the checkboxes.

Go on the left menu bar Manage → Policy → Add Policies allows you to customize features to manage **Windows Devices**.



No.	Description	Functionality
1	Policy Details	Here you will see all the policies that you have applied by Policy name, date and operating system. Clicking on Policy name, you can see what options were selected for this policy. You can change any options and save and this policy will be update don all the client where this was previously applied. To apply this existing policy to new device, click on Apply. Choose delete to remove this policy from the portal as well from devices.
2	Add Policy	Three tabs allows you to configure Scan Settings, USB Manager and Firewall settings.
2.1	Scan Settings	Diverse settings applicable to scan such as if you want to scan for File-less Malware, Real-time protection , Threat community and Threat Intelligence etc. allow Admin to manage client agents scanner.
2.2	USB Manager	Admin can choose to completely block USB or selectively block CD/Camera, block Read only, Write only, complete block, execution block, password protect USB devices, skip or allow USB drive scan when connected and enable USB activity monitor (like what was copied to USB or from USB to PC, deleted etc.). Note: USB activity monitoring can be viewed (if enabled) from Monitor → Reports → USB Activity log

2.3	Firewall	A complete software firewall can allow you to block websites, applications, ip address and protocols, email Anti-virus scan, Anti-Spam and Anti-Phishing
2.3.1	Network Filter	Enable this option and select default protocols that you would like to block like DHCP or add your own IP address and port that you would like to block
2.3.2	Application Rule	Select 'Enable Application Rule' allow you to block internet access of that application. <i>For ex. You can block internet access of Anydesk on all client pcs if you put anydesk.exe here.</i>
2.3.3	Internet Filter	This options lets you manage web browsing experience by enabling blacklist. So if you any url here then that will be blocked from being browsed on the selected client devices. Enable anti-Phishing to block phishing urls. Enable content search goes one step ahead and also find these url if they occur in any documents such as pdf or word or txt files and block opening such files.
2.3.4	Client Control	This option is very good for safe browsing as it comes with it's our own researched default list of websites, category-wise. <i>Note: For example, if you want to block social networking sites then select 'Block Categories'→Select 'Social Network'.</i> You can add your own websites as well by full name or keywords, if keyword is found in domain, sub domain or even body of the page then that website is blocked. Internet and computer usage can be regularized from here. PC will logoff beyond the set day and time settings.
2.3.5	Email Scan	Completely manage your Outlook mail box with options such as block attachment or scan attachment for malware, enable Anti-Spam, stamp strings on the emails and many other options

Scan Settings

Go to *Manage*→ *Policy*→ *Add Policy*→ *Scan Settings for windows*

Selectively disable or enable scanner features.

1. **Application Whitelist:** This allows admin to control execution of applications on client agents. You can decide to Block all applications and only let whitelist applications to launch. From here admin can enable & disable application whitelisting, adding application into the whitelist require you to create application whitelisting configuration from Configuration.

2. **Auto Quarantine:** If check box is selected then if any malware are found during scan then those files will be quarantined (deleted or repaired in case of virus)
3. **Cloud Scan:** Disable this to turn off Cloud scan.
4. **File less Malware:** Scanners are also looking out for malicious software that uses legitimate programs to infect a computer. Such Malware not rely on files and leaves no footprint, making it challenging to detect and remove.
5. **Folder Vault:** Secure important data folder. Once a folder is protected no one can open that folder and read/write/modify its contents, not even Ransomware. Protected with kernel drivers.
6. **Generic Scan:** We use several algorithms to find malicious files such Artificial Intelligence with supervised learning. They fall under this category and if check ON generic scanner works along with the other scanners.
7. **Heuristic Scan:** Some malware are detected by using pattern, logic, behaviour or logic. If this check is ON then heuristic scan takes place.
8. **Home Page protection:** Monitors if any malware tries to change home page of browser.
9. **Host File Monitor:** Alerts if any malware tries to change home page of browser.
10. **Manual Uninstall:** If this check is OFF then client agents cannot remove the Cloud AV software from their devices manually. Admin can only remove the software by going to Windows → Device and selecting Action to uninstall if he wants to delete it.
11. **Network Monitor:** This will guard your PC from malware coming through network share. For this feature to work Real time protection should be ON.
12. **On copy monitor:** Active protection monitors when files are copied on the file system
13. **Ransomware Monitor:** A special Service and Driver is dedicated to managing any outbreak of Ransomware using decoy files and process inspection.
14. **Real-time Protection:** If you would like to turn off Active Protection then uncheck this option.
15. **Scan Hash Signatures:** Scan for hashes on Amazon AWS.

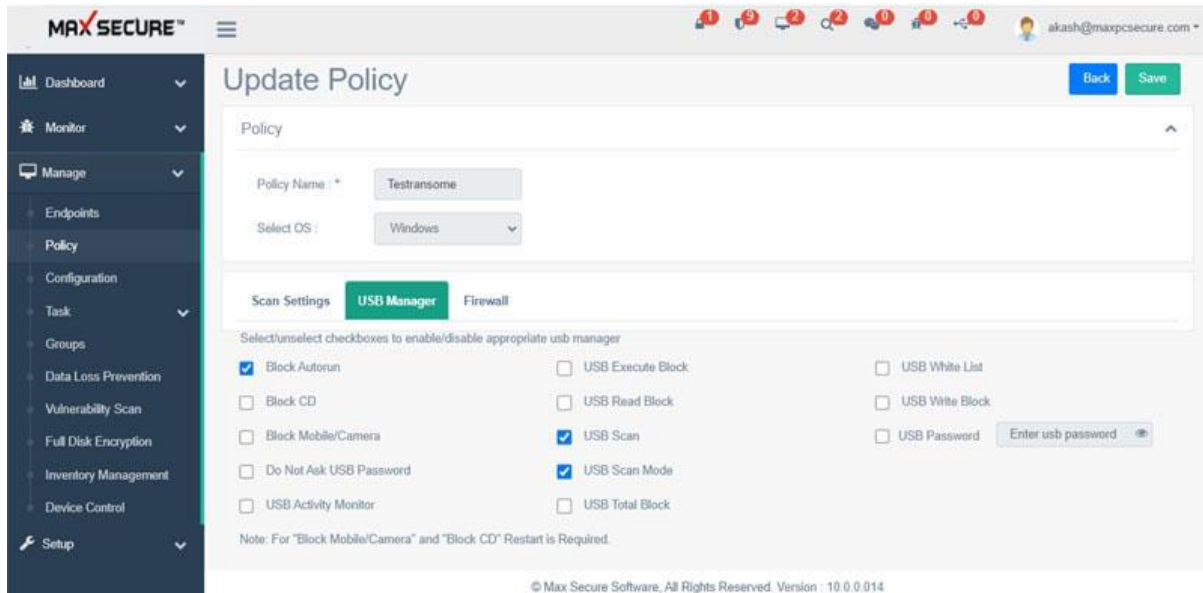
16. **Show Notifications:** If any malware are detected, tray notification is given on client devices. You can decide to turn it off.
17. **Skip Compressed File:** If this option is checked ON then compressed files like zip, rar will be skipped from scan
18. **Threat Community:** Suspected malware samples based on heuristic and AI/ML detection are sent to our server for further analysis, which helps community. If you do not want any files to go out of your PC then to turn this feature off.
19. **Threat Intelligence:** Metadata of suspected files are sent to Max Secure Threat Intelligence server and malicious files are identified.
20. **Quarantine Folder size:** Selecting this will help admin to manage how much space quarantine folder on client agents. So if you, for example, put size of 500MB then as soon as Quarantine folder reaches this size it is automatically deleted.

USB Manager

For managing USB settings go to *Manage→Policy→Add Policy→USB Manager*

1. Complete control over USB devices, Read/Write/Execute, Monitor activity, and Scan.
2. **USB Scan:** If unchecked, USB devices when connected will not be scanned with malware scanner. Scan will be skipped. By default check is ON.
3. **USB Scan mode:** If check box is selected then USB devices scan will be in the automatic mode and user will not be asked if he wants to allow that. If unchecked, user will be asked-"Do you want to scan". It is recommended to leave the check ON
4. **USB White List:** If this option is checked ON then only white listed USB device with their device id (Use the tool to get id) will be able to connect to your main devices. You can only Read/Write data from the white listed devices, rest all USB devices will be blacklisted.
5. **Block Mobile devices:** If this option is checked Mobile devices cannot be connected to your main device.
6. **Block Auto run:** We use several algorithms to find malicious files such Artificial Intelligence with supervised learning. They fall under this category and if check ON generic scanner works along with the other scanners.

7. **Do not ask USB Password:** If this check is on, then password will not be asked for USBs present in the USB Whitelist.



Firewall Policy

Once you have installed Firewall from the Devices → Action → Firewall, you can Enable or disable from the check box. Firewall has many options which can be configured from here. For managing firewall policy go to *Manage → Policy → Add Policy → Firewall*

Enable Firewall: Unchecking this option will disable Firewall and all its settings from the client agents.

1. **Network Filter:** Add Network Filter from here to Allow or Block based on protocols such as DHCP, DNS, IGMP, Kerberos, LDAP, NetBIOS, ICMP, VPN and FTP.

There is also an option to block specified IP Address Range and their specific or all ports.



Network Filter Application Rule Internet Filter Client Control Email Scan Max IDS

Note : Block any network by a combination of IP address and /or Port
Select/unselect checkboxes to enable/disable appropriate Network filter

☒ **ENABLE NETWORK FILTER**

Rule Name	Actions
DHCP	ALLOW
DNS	ALLOW
IGMP	ALLOW
KERBEROS	ALLOW
LDAP	ALLOW
NETBIOS	ALLOW
ICMP	ALLOW
VPN	ALLOW
FTP	ALLOW

☐ **ENABLE NETWORK MONITOR**

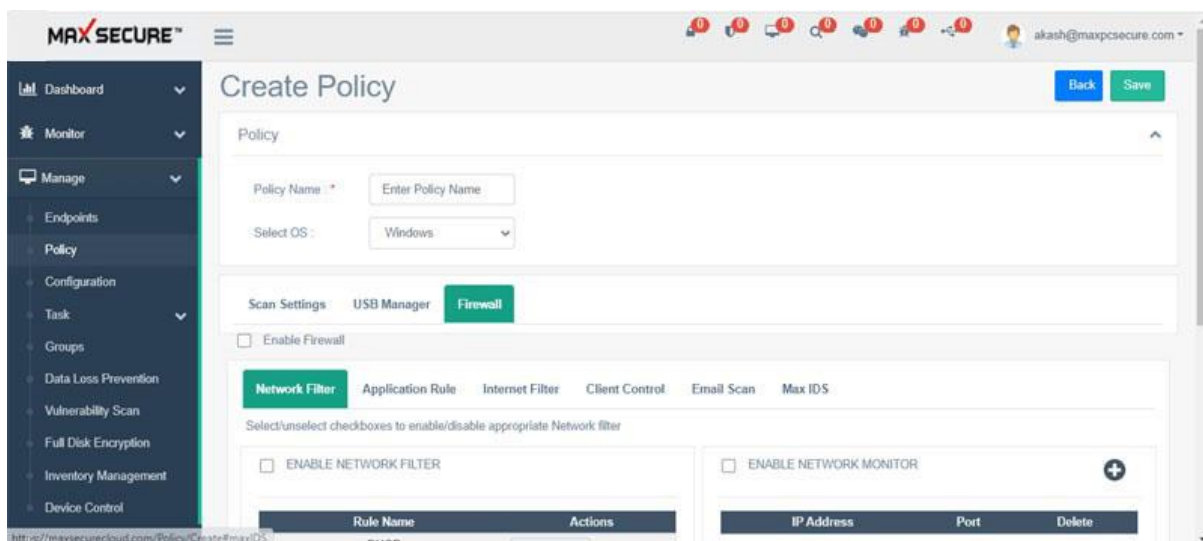
IP Address	Port	Delete
------------	------	--------

☒ **ENABLE IP ADDRESS RANGE**

From Ip Address	To Ip Address	Port	Delete
192.168.1.200	192.168.1.201	20	

- 2. Network Monitor:** You can also block incoming and outgoing connections to and from a particular IP address and port
- 3. Application Rule:** Enable this rule and Applications that are added here will only not be allowed internet access. For example, if you add skype.exe then the device where you apply this policy, cannot use Skype to chat or if you add chrome.exe browser and users cannot browse any websites using Chrome.
- 4. Internet Filter:** Allow all option will allow users to browse all the websites except the ones added in the black list here.
- 5. Add Black List:** Click on Add Blacklist to add any websites and they will be blocked from browsing.
- 6. Enable Anti-Phishing:** Selecting this option will block phishing websites as listed in our Anti-Phishing database.
- 7. Block All:** If this radio button is selected, then no websites can be browsed except the ones in the allowed White list.
- 8. Add White list:** Add any web site urls here to allow them to be browsed.
- 9. Save Data:** To apply all the changes click Save Data
- 10. Client Control:** Here Admin has full access over the computer and Internet usage of devices.
- 11. Restrict usage based on categories.** These are pre-defined list under these categories and all of them will be blocked from browsing

12. Block access to particular websites by adding them here.
13. Schedule Internet Usage: Enable or Block Internet usage on weekends, weekdays, and hour of the day.
14. Schedule Computer usage: User will only be allowed to use the PC during the allowed time and will be logged off after that
15. Set Password: Client Control can be overridden if user is given the password access. Add password here.
16. **Email Scan:** Several email scan related features can be added here.
17. **E-mail Protection:** Turn On and Off email protection and scan of outgoing and incoming emails
18. **Scan Attachment:** If this option is ON then all the incoming and outgoing emails will be scanned.
19. **Block Attachment:** Selecting this will block email attachment if they are found infected with Malware.
20. **Enable Anti-Spam:** Several settings are provided to customize what to do with the email if it is found to be Spam.
21. **Body Text Label:** What label to put on the email body, such As: This email was scanned by Max Total Security" etc.
22. **Microsoft outlook plugin:** Specify a folder where you want to move your Spam emails.



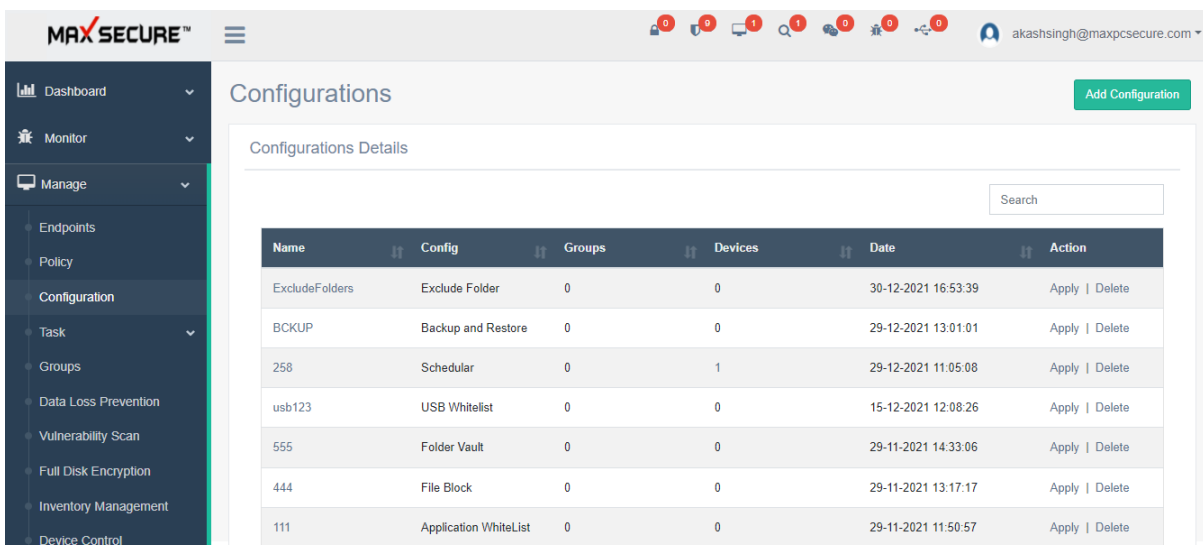
Configurations

Similar to Policies, configuration allow you to apply advance settings on the selected client agent devices for advanced management. In the main grid you see name of the configuration, type of the configuration, Group count if configuration applied to groups, Device count, clicking on Devices count, you can see which devices, creation date of this configuration and Action. From Action you can add more devices to which this configuration can be applied.

Configuration grid shows the following details:

1. Add: Select the Settings that you would like to apply and save. Once Settings is created , you will use Apply button to add Devices/ Groups who will use these Settings
2. Policy Name
3. Group: Count of Groups using this policy
4. Devices: Count of devices in this group
5. Edit: Allows you to edit the features of this policy
6. Delete: Deletes Policy. All the devices and Groups using this policy will be assigned the default policy once this policy is deleted
7. Apply: Allows you to add Devices and Groups who will use this policy.

Manage → Configuration



Configurations

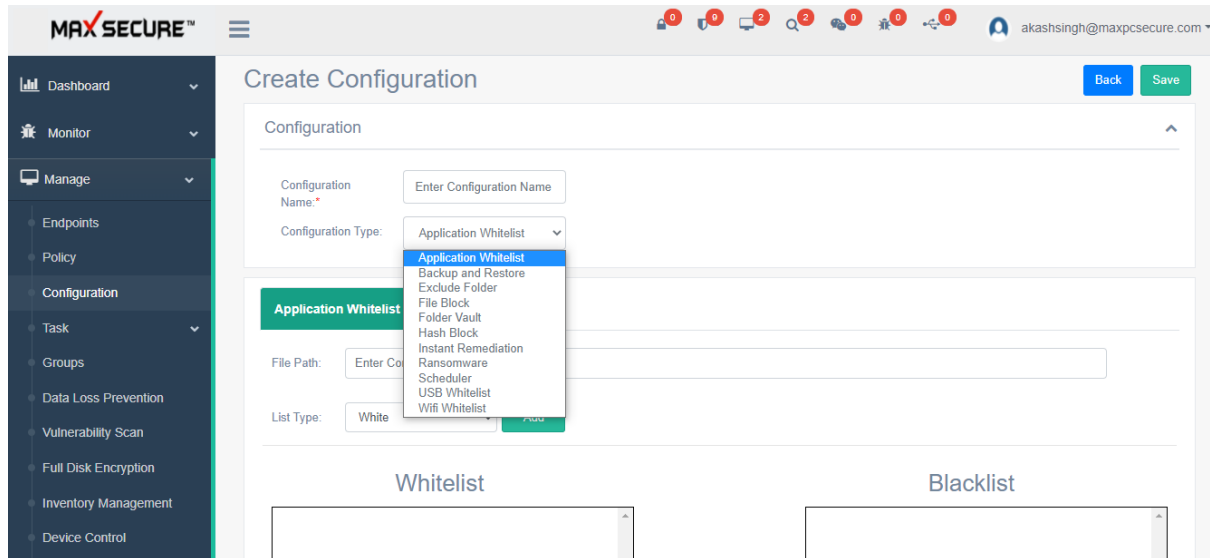
Configurations Details

Name	Config	Groups	Devices	Date	Action
ExcludeFolders	Exclude Folder	0	0	30-12-2021 16:53:39	Apply Delete
BCKUP	Backup and Restore	0	0	29-12-2021 13:01:01	Apply Delete
258	Scheduler	0	1	29-12-2021 11:05:08	Apply Delete
usb123	USB Whitelist	0	0	15-12-2021 12:08:26	Apply Delete
555	Folder Vault	0	0	29-11-2021 14:33:06	Apply Delete
444	File Block	0	0	29-11-2021 13:17:17	Apply Delete
111	Application WhiteList	0	0	29-11-2021 11:50:57	Apply Delete

How to create Configuration?

Click on Add configuration, in the drop down you can see multiple configurations that you can create and apply to selected clients.

Manage → Configuration → Add configuration



Application Whitelist

This feature helps to control execution of unwanted application in back ground.

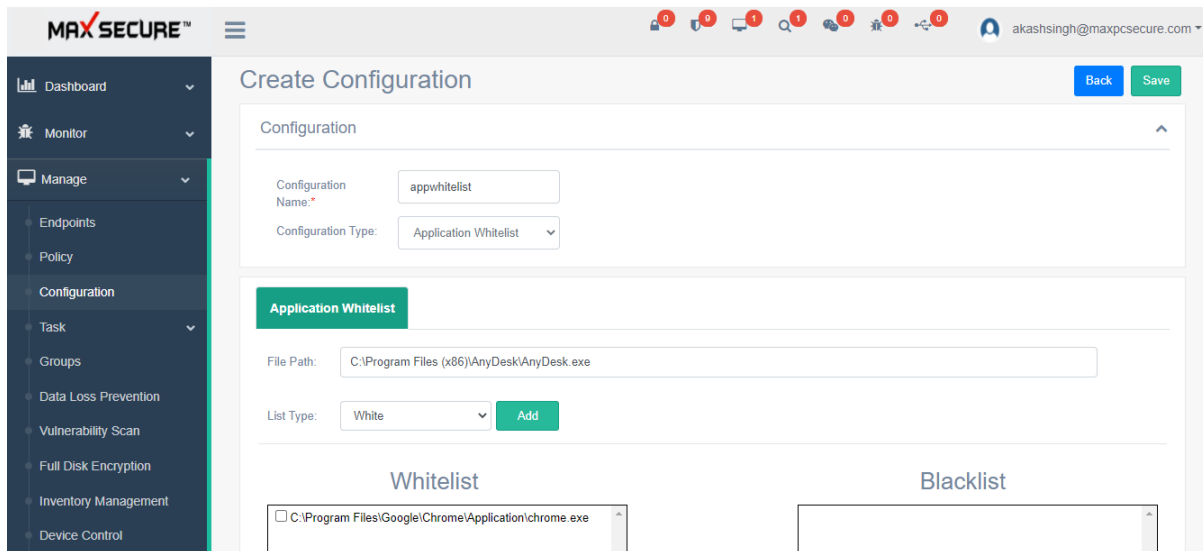
This will allow user to control execution of applications. By default it will block every application except windows essential processes & Microsoft processes. User can allow needed application by adding it into application white list.

User can also remove or add new application from white list or block list.

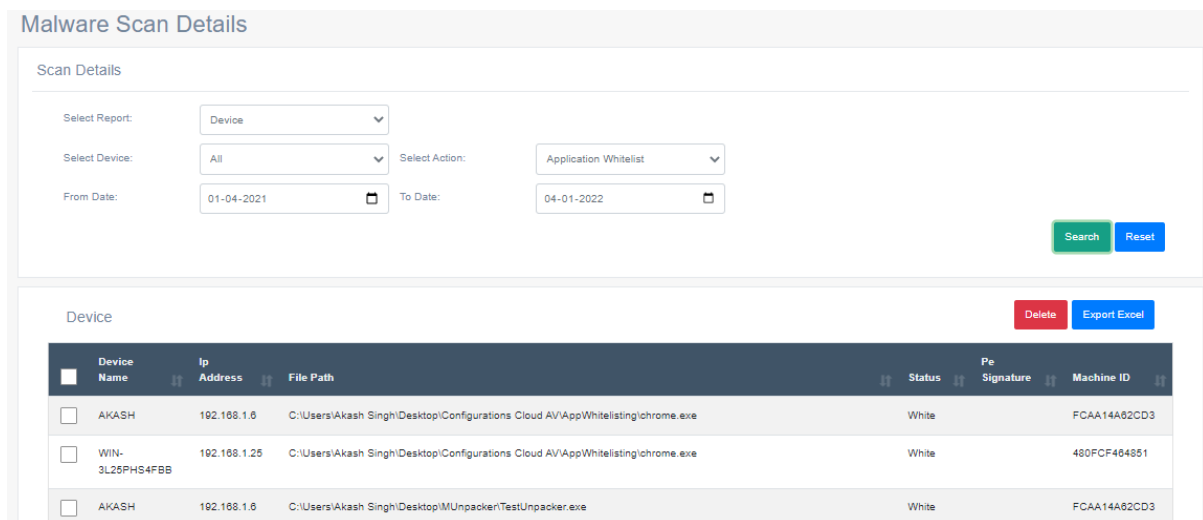
How can we create Application Whitelist Configuration?

Follow below step to add whitelist:

1. Go to Manage → Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'Application Whitelist' from drop down(which is selected by-default)
5. Now enter file path in File Path textbox (File Path of an application should be exact and proper).
6. Click on 'Add' Button to add application on whitelist.
7. Now click on 'Save' button to save this configuration.



Note: Admin can remove the added whitelisted application on Client Agent side from portal only present under *Monitor* → *Detection* → *Select Report: Device* → *Select Action: Application Whitelist*.



Device Name	Ip Address	File Path	Status	Pe Signature	Machine ID
AKASH	192.168.1.6	C:\Users\Akash Singh\Desktop\Configurations Cloud AV\AppWhitelisting\chrome.exe	White		FCAA14A82CD3
WIN-3L25PHS4FBB	192.168.1.25	C:\Users\Akash Singh\Desktop\Configurations Cloud AV\AppWhitelisting\chrome.exe	White		480FCF464851
AKASH	192.168.1.6	C:\Users\Akash Singh\Desktop\Unpacker\TestUnpacker.exe	White		FCAA14A82CD3

Back-up & Restore

This configuration allows to take backup of Client Agent's document files automatically by using max backup scheduler. These files can be later restored in case they have accidentally removed some or all of them or they have been infected by some malware. Backup file are protected in a vault called "MaxSecureDataBackupTask" on Client Agent's machine and

cannot be deleted from explorer view or infected by any malware. These files are compressed and intelligently backed up to optimize the space used by them on Client Agent's machine.

By default few extensions files will be backed up but Admin has full control over what to back up and schedule the backup and view Reports

Admin also has control over what to restore in case of any data loss on users PC due to any reason. Data on Client Agent PC is completely protected by our kernel drivers so even Ransomware cannot infect it.

Manage Data: Documents, text, images, word, excel, ppt, finance documents, etc. Admin can also protect any files (select by file extensions given in the list or add your own file extensions).

Admin can select from given choice of minimum required file extensions but can also select more extension from the given list and can also add more extensions if do not find them in the given list.

Data backup interface consists of file backup setting Max Backup size allowed (MB), File Modified within (Days), Max file size allowed (MB), Source Backup Drive, change backup drive, etc.

How can we create Backup & Restore Configuration?

Follow below steps to create Backup & Restore configuration:

1. Go to Manage→ Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'Backup and Restore' from drop down.
5. Now from configuration you can choose File Extension to take back up from the given list or can add more extension also.
For adding new extensions enter extension and click on 'Add' button.
For deleting any extension select extension given in the list by checkbox & click on 'Delete' button.
6. Select file settings to take backup
 1. Max Backup size allowed (MB): You can limit the backup size on Client Agent machine from here only. Backup size is in MB.
 2. File Modified within (Days): You can set backup to take for the file as per last modified days.
 3. Max file size allowed (MB): One can select the maximum size of the file to take backup, file size is in MB.
 4. Source Backup Drive: This will allow admin to enter the specific drive path for which backup will take place in future. By default it will take the backup of all available drive on the Client Agent's system.

5. Change Backup Drive: This will allow admin to select any specific backup store location drive. By default it will take backup on the drive where maximum free space available.
7. Now set the time for scheduling backup
8. Click on 'Save' button to save this configuration.

Backup And Restore

File Extension To Take Backup

☐ Select All

☐ .3FR

☒ .ACCCDB

☒ .ACCDE

☐ .AI

☐ .ARW

☐ .BAY

☐ .BMP

☐ .CDR

☐ .CER

☐ .CR2

☐ .CRT

☐ .CRW

☐ .CPP

☐ .DBF

☐ .DCR

☐ .DER

☐ .DNG

☒ .DOC

Add
Delete

File Settings To Take Backup

Max Backup size allowed(MB):

File Modified within(Days):

Max file size allowed(MB):

Source Backup Drive:

☐ Change Backup drive:

☐ Network Path:

Backup Scheduler

☐ Daily

☒ Weekly

☐ Monthly

Note: Admin can restore created backup on Client Agent side from portal only present under *Monitor* → *Detection* → *Select Report: Device* → *Select Action: Backup and Restore*.

Malware Scan Details

Scan Details

Select Report:

Select Device:

Select Action:

From Date:

To Date:

Search
Reset

Device
Export Excel

Device Name	Ip Address	Folder Name	Date	Total Count	Status	Apply Restore
WIN-3L25PHS4FBB	192.168.1.25	31-10-2021 13-01-12_auto	31-10-2021	418	Restore	Apply
DESKTOP-0K9DA62	192.168.1.88	29-08-2021 13-01-17_auto	29-08-2021	37	Not Restore	Apply
DESKTOP-2F0UOB2	192.168.1.138	25-08-2021 13-23-25_auto	25-08-2021	77	Not Restore	Apply
AKASH	192.168.1.6	24-10-2021 13-01-26_auto	24-10-2021	873	Restore	Apply
DHEERAJ-PC	192.168.1.15	24-08-2021 16-38-43_auto	24-08-2021	299	Not Restore	Apply

Exclude Folder

This option will allow portal admin to completely exclude scanning of the folder or file so that data that you do not want to be scanned in future by Client Agent can be added from here.

How can we create Exclude Folder Configuration?

Follow below steps to create Exclude Folder configuration:

1. Go to Manage → Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name.
4. Select Configuration Type as 'Exclude Folder' from drop down.
5. Enter the folder/file path which you want to exclude from malware scan.
6. Click on 'Add' button.
7. Click on 'Save' button to save configuration.

MAXSECURE™ | akashsingh@maxpcsecure.com

Create Configuration

Configuration

Configuration Name:

Configuration Type:

Exclude Folder/Files

Folder/File Path:

Add

File Path	Delete
C:\Users\Akash Singh\Desktop\exclude folder	<input type="button" value="Delete"/>

Note: To start scan again of excluded folder/file you need to remove it from portal present under *Monitor → Detection → Select Report: Device → Select Action: Exclude Folder & File*.

File Block

Application control policy: Max Endpoint Security-Business Console enables you to block 'application' that is, legitimate applications that are not a security threat, but that you decide are unsuitable for use in your office environment. Such applications may include instant messaging (IM) clients, digital imaging software, media players, etc. you can add its application name in application block list to block its execution on Client Agent's machine.

After blocking an application, you can also unblock it from portal only. Blocking/Unblocking an application depends on the status you gave during creation of configuration.

Suppose you want to block remote desktop or chrome on Client Agent side then you can add 'mstsc.exe' or chrome in its block list, now in order to remove the block list from Client Agent side you can create new or modify the same configuration and change its status to Delete.

How can we create File Block Configuration?

Follow below steps to create File Block configuration:

1. Go to Manage → Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'File Block' from drop down.
5. Enter the application name on File Text textbox.
6. Select the status from dropdown whether you want to block or unblock (after blocking) application.
7. Click on 'Add' button.
8. Click on 'Save' button to save this configuration.

File Name	Status	Delete
mstsc.exe	ADD	⊖
saplogon.exe	Delete	⊖

Folder Vault

Admin or Clients can protect any folder by adding them in the list here. This will give security to folders which user does not want to be modified by any source. These folders will not be accessible & deny permission to any application in case of read or write data in this folder. These folders are protected by kernel drivers and unbreakable even on Ransomware attack.

How can we create Folder Vault Configuration?

Follow below steps to create Folder Vault configuration:

1. Go to Manage→ Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'Folder Vault' from drop down
5. Enter the path of folder that needs to be protected.
6. Click on 'Add' button.
7. Click on 'Save' button to save this configuration.

The screenshot shows the 'Create Configuration' page in the Max Secure portal. The left sidebar has a menu with 'Dashboard', 'Monitor', 'Manage', 'Endpoints', 'Policy', 'Configuration', 'Task', 'Groups', 'Data Loss Prevention', 'Vulnerability Scan', 'Full Disk Encryption', and 'Inventory Management'. The 'Manage' section is expanded. The main content area is titled 'Create Configuration' and has 'Back' and 'Save' buttons. Under the 'Configuration' section, there are two fields: 'Configuration Name' with the value 'foldervault' and 'Configuration Type' with a dropdown menu showing 'Folder Vault'. Below this, there's a 'Folder Vaults' section with a 'Folder Path' input field containing the placeholder text 'Enter Complete File Path' and an 'Add' button. At the bottom, there's a table with two columns: 'Folder Path' and 'Delete'. The table contains one row with the value 'E:\important' and a delete button.

Note: Admin can unlock the folder available on Client Agent side from portal only by applying policy present under *Manage→ Policy→ Add Policy: Scan Settings> Folder Vault, uncheck it.*

Hash Block

The most common method for blocking unauthorized software is to block the primary program executable. To ensure that the correct file is blocked, Max Secure recommends that you calculate the hash signature of the file or for generating SHA-256 signature of file we are also providing a tool.

Note: When an update for a program is available and its executable modified, you need to create and add a new hash signature.

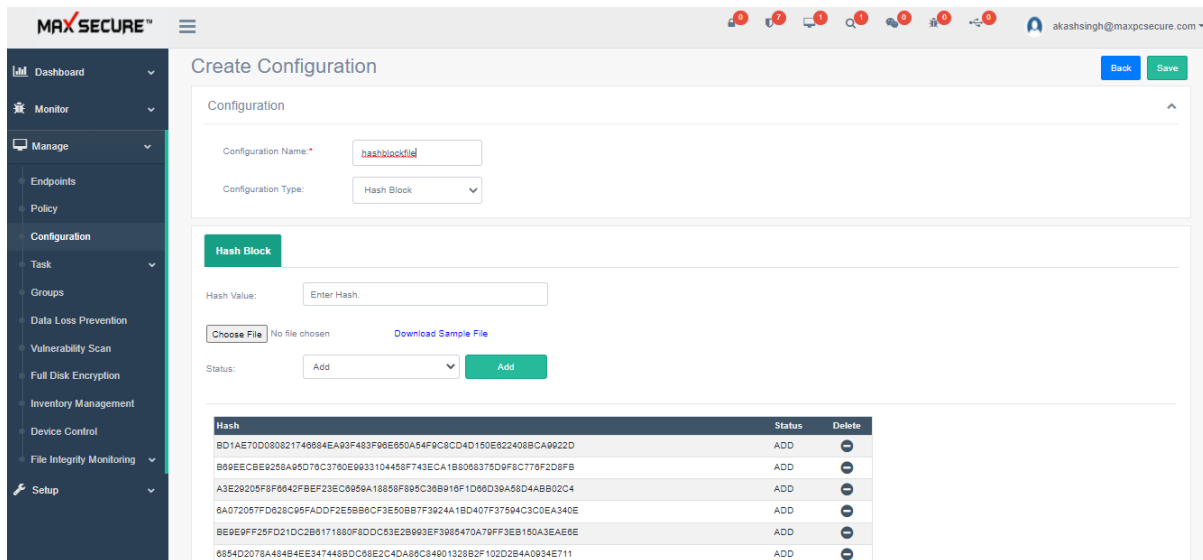
During scan or our real time protection will detect these files present under hash block list. There is also an import option for adding 4000 files hashes at once in the format of .xls.

How can we create Hash Block Configuration?

Follow below steps to create Hash Block configuration:

1. Go to Manage→ Configuration

2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'Hash Block' from drop down.
5. Enter the hash (SHA-256) signature of the file.
Or
You can also import hashes from .xls file (If you want to add multiple file hashes at once).
6. For detecting any file status should be 'Add' which is selected by default, but if you want to remove any file already added on block list you can simply change its status to delete.
7. Click on 'Add' button.
8. Click on 'Save' button to save this configuration.



Hash	Status	Delete
BD1AE70D080821749684EA93F483F8E650A54F9C8CD4D150E8224088CA9922D	ADD	🗑️
B69EECEB6258A95D76C3780E9933104458F743ECA1B806837509F8C776F2D8FB	ADD	🗑️
A3E26205F8F9642FBEF23EC6699A18858F895C36B918F1D66D39A58D4ABB02C4	ADD	🗑️
6A072057FD628C95FADF2E58B6CF3E50BB7F3924A1BD407F37594C3C0EA340E	ADD	🗑️
BE9E9FF28FD21DC2B0171880F8DDC53E2B093EF3665470A76FF3EB150A3EAE6E	ADD	🗑️
6854D2078A4848EE347448BD0C68E2C4DA86C84901328B2F102D2B4AD934E711	ADD	🗑️

Note: In order to remove hash signature on client agent side admin can change the status to 'delete'.

Instant Remediation

Custom malware scan

Admin has full control over malware detection and can add his own malware file signatures to all or selected devices. So this option gives you custom malware detection beyond Max Cloud AV detection.

Use case would be, if any malware has come in the wild through some research paper or website that he just read; now Admin wants to make sure that this malware gets detected. He can stay ahead of this malware and add his own detection using the hash tool provided.

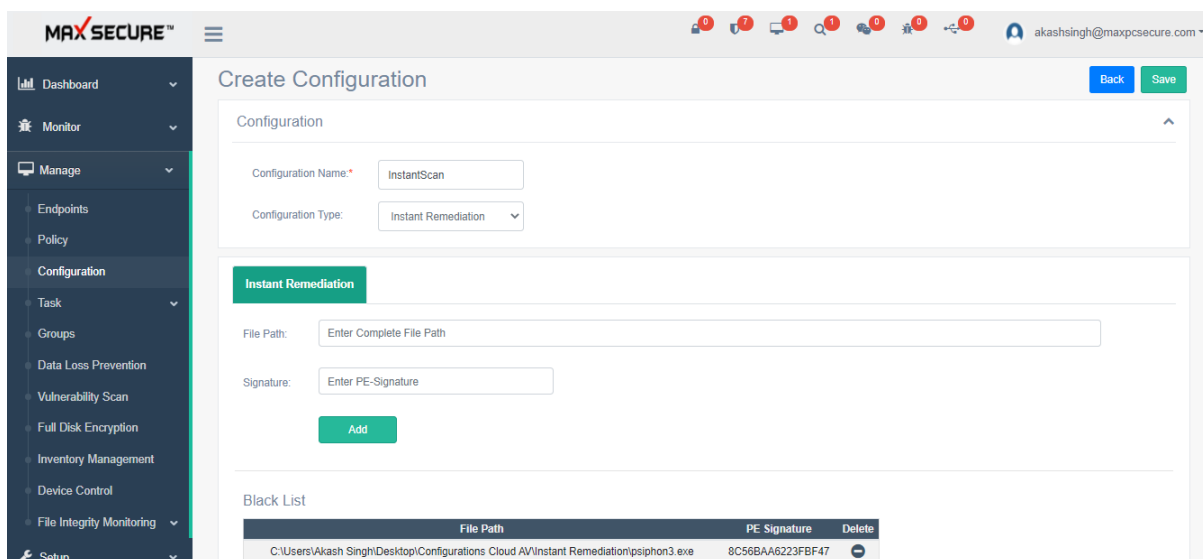
Please note here that the path option is not stringent and any path can be added as well as we does not scan by path. Hash should be added and that will be used to find malware file no matter in whichever location it is hiding.


How can we create Instant Remediation Configuration?

Follow below steps to create Instant Remediation configuration:

1. Go to Manage→ Configuration
2. Click on 'Add Configuration' button
3. Enter Configuration Name
4. Select Configuration Type as 'Instant Remediation' from drop down.
5. Enter the path of folder where file exist although file detection are not on file path dependent, it will detect file present anywhere on the system.
6. Enter signature of the file.
7. Click on 'Add' button.
8. Click on 'Save' button to save this configuration.

Note: Admin can also remove file from instant remediation list present under *Monitor→ Detection→ Select Report: Device→ Select Action: Instant Remediation*.



File Path	PE Signature	Delete
C:\Users\Akash Singh\Desktop\Configurations Cloud AV\Instant Remediation\psiphon3.exe	8C56BAA6223FBF47	

Ransomware

Update client agents with any known malware/ Ransomware signature instantly.

If any of the client agents PC gets attacked by some Ransomware then Cloud AV detects it, based on its behaviour and blocks it. At the same time it sends the hash of that Ransomware to the portal.

Admin gets an alert from notification icon on the top menu of the portal as well as he can

schedule such incident reports to be emailed to him.

As soon as he discovers such an incident, he can send this signature to all other client agents and they get protected early on from this Ransomware.

Admin can also add hash of any known malware file using tool provided to create hash and send this signature to all PCs to protect them.

Although, even if Admin has not added this signature in the instant remediation and pushed to his client agents, we immediately update our Cloud server (if Cloud Scan is ON).

Admin also has an option to remove that Ransomware infected PC from network from Dashboard→ Windows→ Devices→ select that Device→ Action→ Disable Network

How can we create Ransomware?

Follow below steps to create Ransomware configuration

1. Go to Manage→ Configuration
2. Click on 'Ransomware' button
3. Enter Configuration Name
4. Select Configuration Type as 'Ransomware' from drop down.
5. Enter the file path although detection are not on file path dependent, it will block its execution irrespective of the path, anywhere on the PC.
6. Enter signature of the file, for this tool is provided.
7. Click on 'Add' button.
8. Click on 'Save' button to save this configuration.

Note: To check its report or to remove blacklisted file admin can do that from portal only available under *Monitor→ Detection→ Select Report: Device→ Select Action: Ransomware*. To completely remove file from blacklist remove it from instant remediation list also present under *Monitor→ Detection→ Select Report: Device→ Select Action: Instant Remediation*.

The screenshot shows the 'Create Configuration' interface in the MAXSECURE Cloud Portal. The sidebar on the left contains navigation links: Dashboard, Monitor, Manage, Endpoints, Policy, Configuration, Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, and File Integrity Monitoring. The main panel is titled 'Create Configuration' and includes a 'Configuration' section with the following fields:

- Configuration Name: * Ransomwareadd
- Configuration Type: Ransomware

Below the configuration fields is a 'Ransomware' section with the following fields:

- File Path: Enter Complete File Path
- PE Signature: Enter PE-Signature
- List Type: Black (with an 'Add' button)

At the bottom, there are two sections: 'Whitelist' and 'Blacklist'. The 'Blacklist' section shows a file path: C:\Users\Akash Singh\Desktop\Configurations Cloud AV\Ransomware\N w folder(8C56BA6223FBF47).

Scheduler

Schedule to run live updates, Scan remote client agent PC's when you like it.

Highly configurable scheduler lets Admin have full freedom on remote PCs scan time, scan type, scan action and live update to get latest malware definition and upgrades.

Admin can also choose the option to shut down or Logoff PCs after scheduled scan is complete.

How can we create Scheduler?

Follow below steps to create Scheduler configuration

1. Go to Manage → Configuration
2. Click on 'Scheduler' button
3. Enter Configuration Name
4. Select Configuration Type as 'Scheduler' from drop down.
5. Check 'Scan Scheduler' to turn on scan scheduler.
6. Select Scan Option whether you want to turn Quick Scan or Full Scan.
7. Select 'Silence Scan' option if you want the scan to launch it in the background without knowing/disturbing Client Agent.
8. Select 'After Scan is Complete' option whether you want to shutdown, logoff Client Agent machine or take No Action after scan gets completed.
9. Set the scan time for daily or weekly basis.
10. Check 'Live Update Scheduler' to turn on live update scheduler.
11. Set time for live update.
12. Click on 'Save' button to save this configuration.

Create Configuration

Configuration

Configuration Name:

Configuration Type:

Scheduler

☒ Scan Scheduler

Scan Option: ☒ Quick Scan ☐ Full Scan ☐ Silence Scan

On Detection: ☐ Log Only ☒ Clean

After Scan is Complete: ☐ Shut Down PC ☐ Log Off PC ☒ No Action

Scan Time: ☒ Daily ☐ Weekly ☐ Hourly ☐ Minutely

Daily:

Weekly:

Hourly:

Minutely:

☒ Live Update Scheduler

Live Update Scheduler: ☒ Daily ☐ Weekly

Daily:

Weekly:

USB Whitelist

Complete control over USB devices like Pen drives or external hard disk

If Admin would like that only designated external devices are allowed to copy any data then this White-list feature can be used. It is a very useful feature for Data theft protection.

We have provided a tool to identify the device ID then add that ID here as white list. Only these white-listed Devices will be able to copy data on PCs where Cloud AV is installed and registered.

How can we create USB Whitelist?

Follow below steps to create USB Whitelist configuration

1. Go to Manage → Configuration
2. Click on 'Scheduler' button
3. Enter Configuration Name
4. Select Configuration Type as 'USB Whitelist' from drop down.
5. Enter the USB serial number that has been generated from given tool on 'Serial No'.
6. Enter 'USB Name' as per your understand
7. Check 'Scan Scheduler' to turn on scan scheduler.
8. Select Scan Option whether you want to turn Quick Scan or Full Scan.
9. Select 'Silence Scan' option if you want the scan to launch it in the background without knowing/disturbing Client Agent.
10. Select 'After Scan is Complete' option whether you want to shutdown, logoff Client Agent machine or take no action after scan gets completed.
11. Set the scan time for daily or weekly basis.
12. Check 'Live Update Scheduler' to turn on live update scheduler.
13. Set time for live update.
14. Click on 'Save' button to save this configuration.

The screenshot shows the 'Create Configuration' page in the Max Secure Cloud Portal. The left sidebar contains navigation options: Dashboard, Monitor, Manage (selected), Endpoints, Policy, Configuration (selected), Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, and File Integrity Monitoring. The main content area is titled 'Create Configuration' and has 'Back' and 'Save' buttons. Under the 'Configuration' section, the 'Configuration Name' is 'USBwhitel' and the 'Configuration Type' is 'USB Whitelist'. Below this, there is a 'USB Whitelist' section with input fields for 'Serial No.' (placeholder: 'Enter USB Serial Number') and 'USB Name' (placeholder: 'Enter USB Name'), and an 'Add' button. At the bottom, a table lists existing USBs in the whitelist.

USB Serial No	USB Name	Delete
20054963930C93831C1C	HP1	
hryui1bdcd	Transcent	

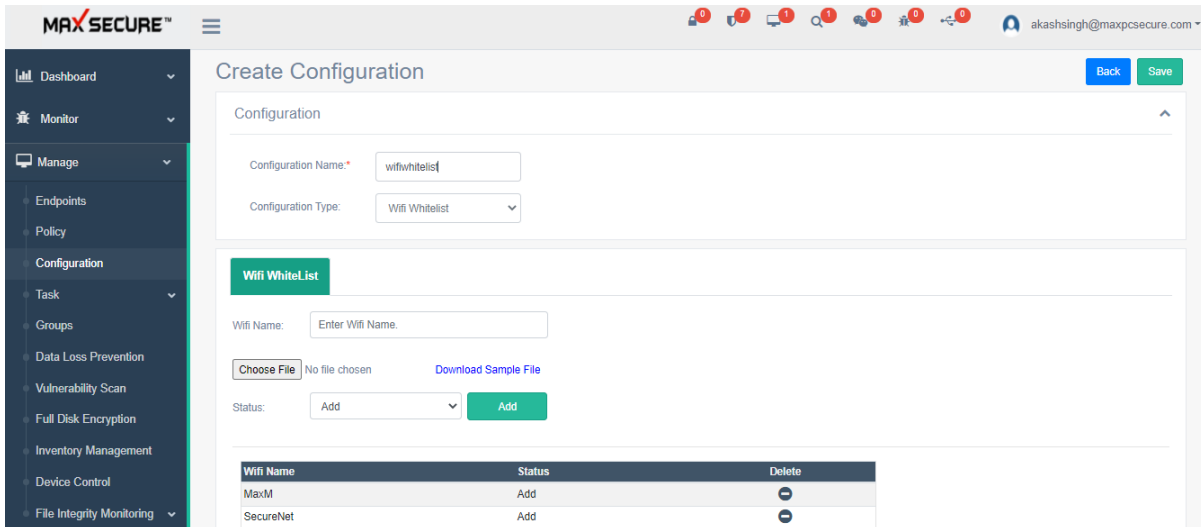
Wi-Fi Whitelist

This configuration is for adding a Wi-Fi network to the trusted list. You can allow users connect to Wi-Fi networks that you consider to be secure, such as a corporate Wi-Fi network. To do so, you must add the network to the list of trusted Wi-Fi networks. It will block access to all Wi-Fi networks except those specified in the trusted list on Client Agent side.

How can we create Wi-Fi Whitelist?

Follow below steps to create Wi-Fi Whitelist configuration

1. Go to Manage→ Configuration
2. Click on 'Wifi Whitelist' button
3. Enter Configuration Name
4. Select Configuration Type as 'Wi-Fi Whitelist' from drop down.
5. Enter the Wi-Fi Name on the Wi-Fi name text box.
6. Select the status as 'Add' (which is selected by default) when we want to add it on Whitelist. Status Remove is for removing it from whitelist.
7. Click on 'Save' button to save this configuration.



MAX SECURE™

akashsingh@maxpcsecure.com

Create Configuration

Configuration

Configuration Name:

Configuration Type:

Wifi WhiteList

Wifi Name:

Choose File No file chosen Download Sample File

Status:

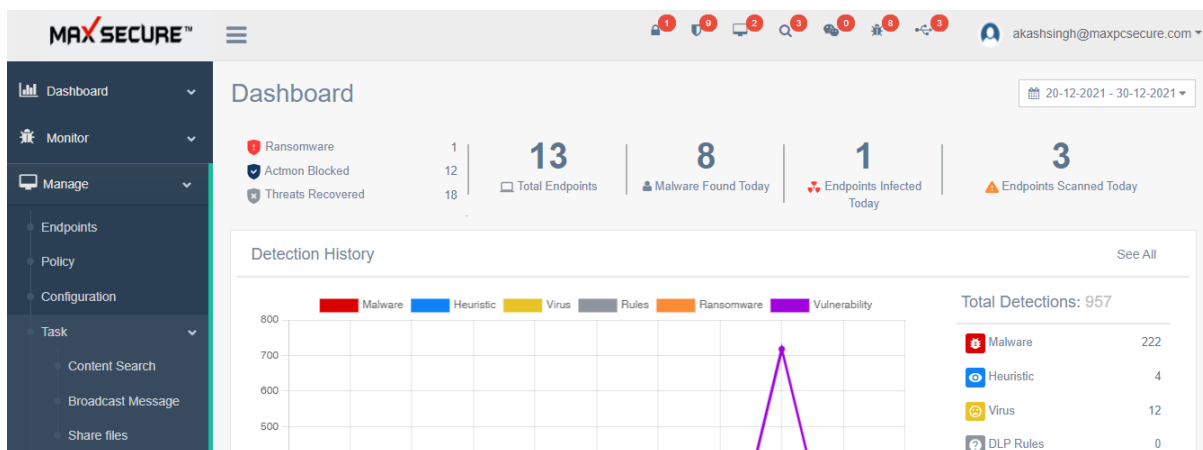
Wifi Name	Status	Delete
MaxM	Add	<input type="button" value="Remove"/>
SecureNet	Add	<input type="button" value="Remove"/>

Note: In order to remove Wi-Fi whitelist, admin can change its status to 'Remove'.

Tasks

Left menu bar Manage → Tasks → gives you several additional features to perform execution remotely or like:

- Content Search
- Broadcast Message
- Share Files
- Send Command



Content Search

Left menu bar → Manage → Task → Content Search allows Admin to do searches on the Client Devices documents files like office, logs, text, pdf files with any keywords, sentences if any Audit compliance requirement is there.

The screenshot displays the MAXSECURE Content Search interface. The left sidebar contains navigation links: Dashboard, Monitor, Manage (with sub-links: Endpoints, Policy, Configuration, Task), and Task (with sub-links: Content Search, Broadcast Message, Share files). The main content area is titled 'Content Search' and includes 'Content Search Policy Details'. A search bar is present. Below it is a table with the following data:

Rule	Date	Action
ContentSearchss	29-11-2021 15:41:29	Apply Delete
second	24-11-2021 12:14:50	Apply Delete
one	23-11-2021 16:21:59	Apply Delete

Below the table, there is a 'Show 10 entries' dropdown and a 'Showing 1 to 3 of 3 entries' status. At the bottom right, there are 'Previous', '1', and 'Next' pagination links.

Admin can also remotely replace found keywords with any other keywords if they are not acceptable for a corporate reputation.

How can we create Content Search Rule?

1. Go to → *Manage* → *Task* → *Content Search*
2. Click on 'Add Rule' button
3. Select rule as per need, rule detail given below:

Search/Audit/Replace phrases, sentences in documents

1. Search in whole drive or selected Path
2. Search should include File name
3. Recursively search in sub-directories
4. Search should be case sensitive or not
5. Do you want to include Unicode search
6. Debit Card: This will monitor for debit card on Client Agent side.
7. Driving License: This will monitor for driving license.
8. Enter the keywords or phrases that you want to search
9. You can also Replace these keywords with another keyword
10. File Mask: Select which file extensions you want to search for these keywords or by default it is selected on all *.* extensions.
11. Exclude Mask: Select which file extensions you want to exclude for content audit.

4. Click on 'Save' button.

The screenshot shows the 'Create Policy' page in the MAXSECURE portal. The left sidebar contains navigation options: Dashboard, Monitor, Manage (expanded), Endpoints, Policy, Configuration, Task (expanded), Content Search, Broadcast Message, Share files, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, and File Integrity Monitoring. The main content area is titled 'Create Policy' and shows a 'Content Audit Policy' configuration. The 'Policy Name' field is set to 'Contentsearch'. Under 'Content Search', 'Custom Search' is selected. A search criteria table is displayed with the following settings:

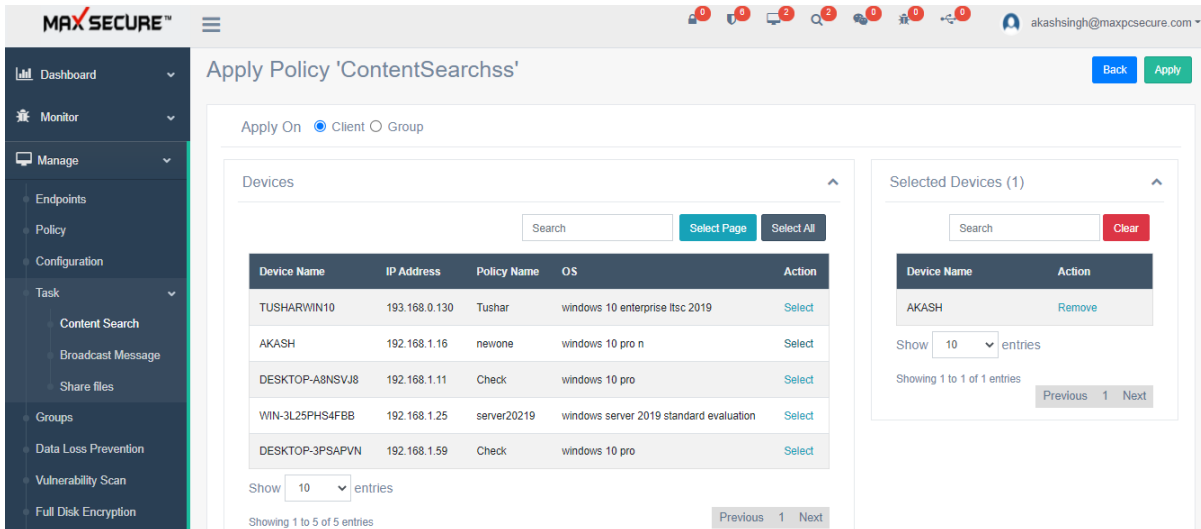
Search Includes	Search Includes Sub Dir.	Case Sensitive	Unicode Search
<input checked="" type="checkbox"/> Search includes File Names	<input checked="" type="checkbox"/> Search includes Sub Dir.	<input checked="" type="checkbox"/> Case Sensitive	<input checked="" type="checkbox"/> Unicode Search
<input checked="" type="checkbox"/> Credit/Debit card	<input type="checkbox"/> Driving License		

Below the table, 'Find Text' is checked with a note '* Keyword should be exact match'. An 'Add Find Text' field contains 'ex. maxsecure'. At the bottom, a table lists the find text entries:

Find Text	Delete
testkeyword	

How can we apply Content Search Rule to Client Agents?

1. Go to → *Manage* → *Task* → *Content Search*
2. Select rule which you want to apply.
3. Click on 'Apply' link.
4. Select below fields:
 - Apply On: There is option for admin to select '**Client**' or '**Group**' for applying content search rule.
 - Devices: You can select client from '**Select**'/'**Reselect**' button. '**Select Page**' button is available to select all client available in the current page. '**Select All**' button is available to select all clients connected.
 - Selected Devices: It will show the list of applied or to be applied client(s)/group(s).
 - You can also remove the recently added client by '**Remove**' button present on the Selected Devices side.
5. Click on 'Apply' button.



MAX SECURE™

Apply Policy 'ContentSearchss'

Apply On ☒ Client ☐ Group

Devices

Device Name	IP Address	Policy Name	OS	Action
TUSHARWIN10	193.168.0.130	Tushar	windows 10 enterprise ltsc 2019	Select
AKASH	192.168.1.16	newone	windows 10 pro n	Select
DESKTOP-A8NSVJ8	192.168.1.11	Check	windows 10 pro	Select
WIN-3L25PHS4FBB	192.168.1.25	server2019	windows server 2019 standard evaluation	Select
DESKTOP-3PSAPVN	192.168.1.59	Check	windows 10 pro	Select

Selected Devices (1)

Device Name	Action
AKASH	Remove

Show 10 entries

Showing 1 to 5 of 5 entries

Previous 1 Next

Where can we see Content Search report?

1. Go to → *Manage* → *Task* → *Content Search*.
2. Click on 'Details' button.



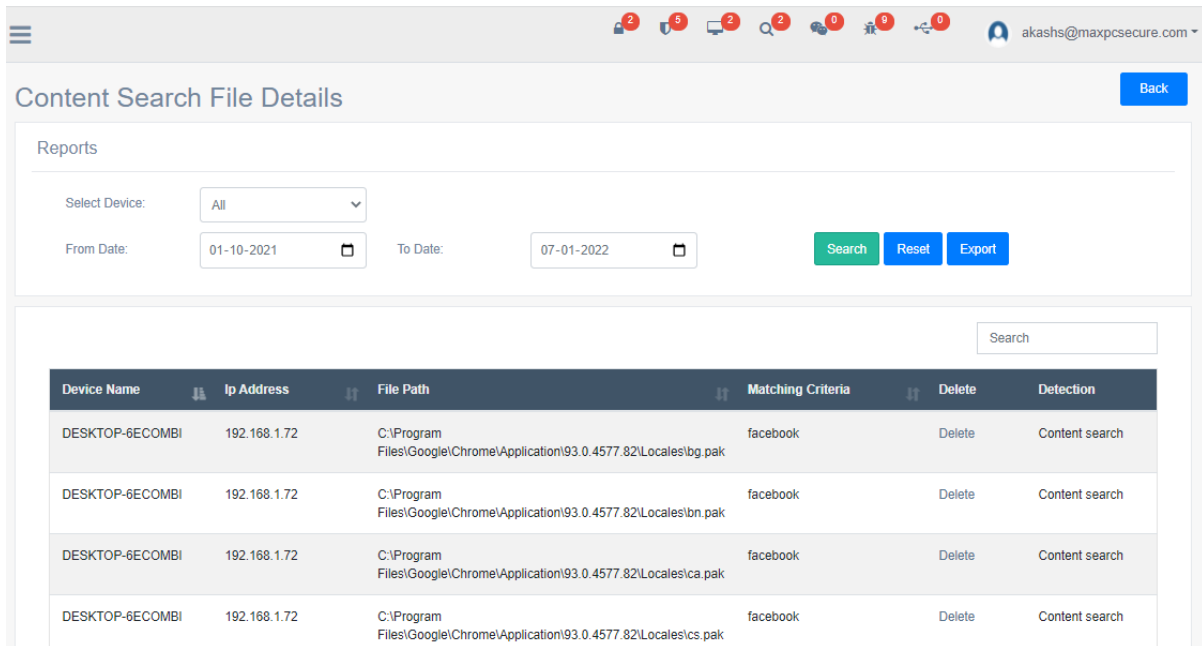
MAX SECURE™

Content Search

Content Search Policy Details

Search

3. It will show report from the last 10 days and also there is an option through custom search report, just select 'From' & 'To' date and Click on 'Search' button.
4. Click on 'Export' button in order to export report.
5. Click on 'Delete' if you want to remove that file permanently from client agent machine.



Content Search File Details Back

Reports

Select Device: All

From Date: 01-10-2021 To Date: 07-01-2022 Search Reset Export


Search

Device Name	Ip Address	File Path	Matching Criteria	Delete	Detection
DESKTOP-6ECOMBI	192.168.1.72	C:\Program Files\Google\Chrome\Application\93.0.4577.82\Locales\bg.pak	facebook	Delete	Content search
DESKTOP-6ECOMBI	192.168.1.72	C:\Program Files\Google\Chrome\Application\93.0.4577.82\Locales\bn.pak	facebook	Delete	Content search
DESKTOP-6ECOMBI	192.168.1.72	C:\Program Files\Google\Chrome\Application\93.0.4577.82\Locales\ca.pak	facebook	Delete	Content search
DESKTOP-6ECOMBI	192.168.1.72	C:\Program Files\Google\Chrome\Application\93.0.4577.82\Locales\cs.pak	facebook	Delete	Content search

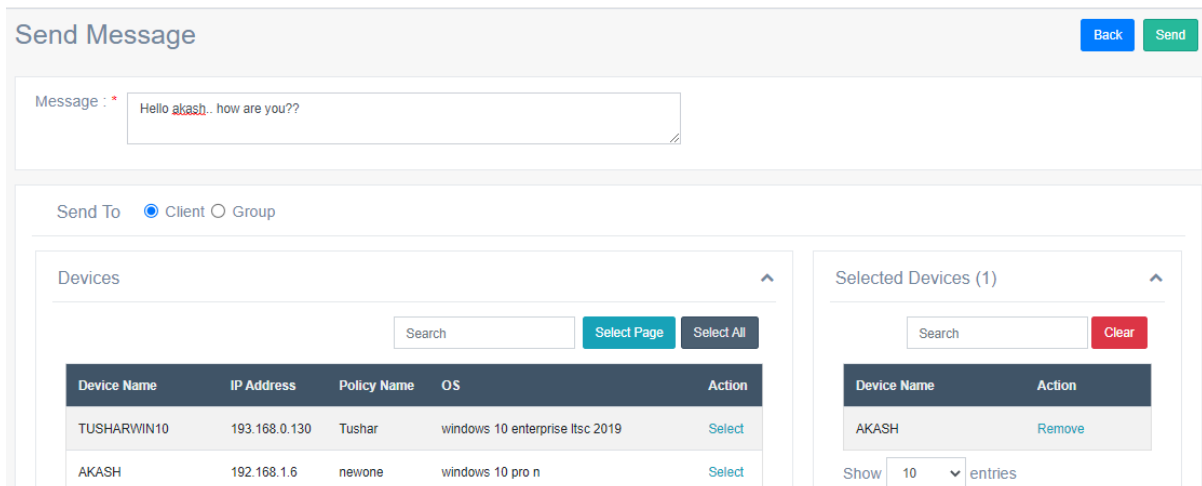
Broadcast Message

It is a messaging service provided to communicate with client agents. It is a two ways messaging platform between dashboard admin and client agents. Admin can send text messages to clients and receive messages.

Client Agents are provisioned to receive messages that are addressed. Messages are displayed to agents by an interactive notification pop-up from, where they can also reply or use 'Max Secure Messenger' to send message to admin.

Also shown as an alert from notification icon on the  top menu of the portal. Admin can also review all the messages sent / received from here.

Note: For viewing sent/received messages go to → *Manage* → *Task* → *Broadcast Message*.



Send Message Back Send

Message : * Hello akash.. how are you??

Send To ☒ Client ☐ Group

Devices

Search Select Page Select All

Device Name	IP Address	Policy Name	OS	Action
TUSHARWIN10	193.168.0.130	Tushar	windows 10 enterprise ltsc 2019	Select
AKASH	192.168.1.6	newone	windows 10 pro n	Select

Selected Devices (1)

Search Clear

Device Name	Action
AKASH	Remove

Show 10 entries

How to send message to client agent?

1. Go to → *Manage* → *Task* → *Broadcast Message*
2. Click on 'Write Message' button shown top right corner of the page.
3. Write your message under the textbox.
4. Select clients/groups from the list shown below.
5. Click on 'Send' button.

Share Files

You can share creative assets with your client agents with 'Share Files'.

Left menu bar → Windows → Share Files allows admin and clients to share files with each other. Files could be any type like pdf, pictures, documents, binaries or any executable etc. if he has any such need.

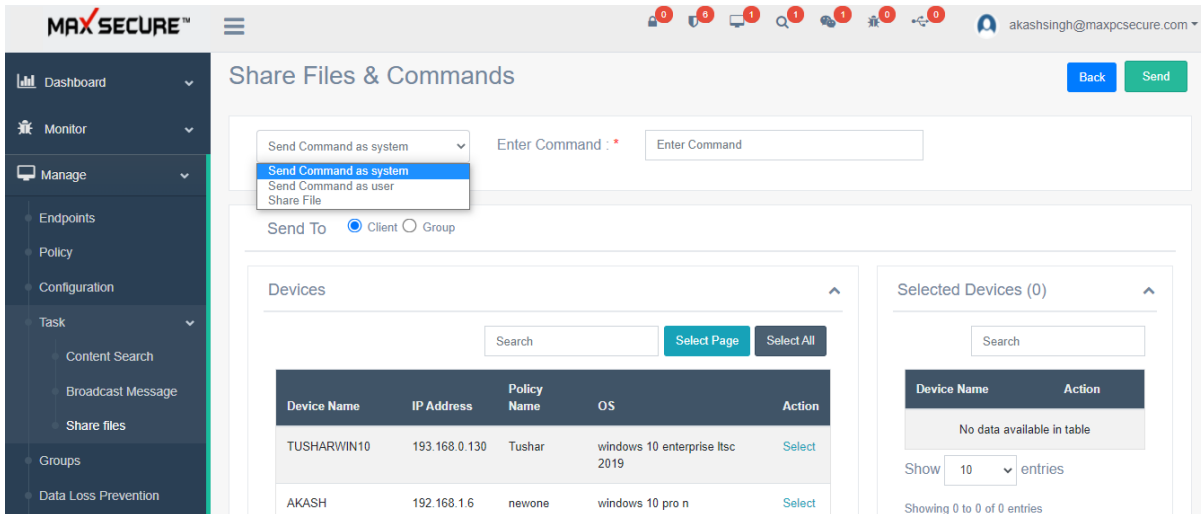
The screenshot shows the 'Share Files & Commands' interface in the MAXSECURE portal. The left sidebar contains navigation links: Dashboard, Monitor, Manage, Endpoints, Policy, Configuration, Task, Groups, Data Loss Prevention, and Vulnerability Scan. The 'Task' menu is expanded, showing 'Content Search', 'Broadcast Message', and 'Share files'. The main content area is titled 'Share Files & Commands' and includes a 'Share File' dropdown, a 'Select File' button, and a 'Choose File' button. Below this, there are radio buttons for 'Send To' (Client or Group). A table of devices is displayed with columns for Device Name, IP Address, Policy Name, OS, and Action. The table lists three devices: TUSHARWIN10, AKASH, and DESKTOP-. To the right of the table is a 'Selected Devices (0)' section with a search bar and a table showing no data available.

Device Name	IP Address	Policy Name	OS	Action
TUSHARWIN10	193.168.0.130	Tushar	windows 10 enterprise ltsc 2019	Select
AKASH	192.168.1.6	newone	windows 10 pro n	Select
DESKTOP-	192.168.1.11	Check	windows 10 pro	Select

Send Command

Admin can send commands which will be executed by client agents. Such as he can give commands to install an application by first sharing/sending the application file with the client then give command line instruction to execute it. Many windows commands can be executed this way remotely. Whatever client agent can run on his PC from command prompt, Admin can execute from the Dashboard.

In addition, Admin can also execute any command remotely, execute any binary on the client agent PC or run almost any command from CMD prompt with administrator privileges.



Share Files & Commands

Send Command as system Enter Command

Send To ☒ Client ☐ Group

Device Name	IP Address	Policy Name	OS	Action
TUSHARWIN10	193.168.0.130	Tushar	windows 10 enterprise ltsc 2019	Select
AKASH	192.168.1.6	newone	windows 10 pro n	Select

Selected Devices (0)

Device Name Action

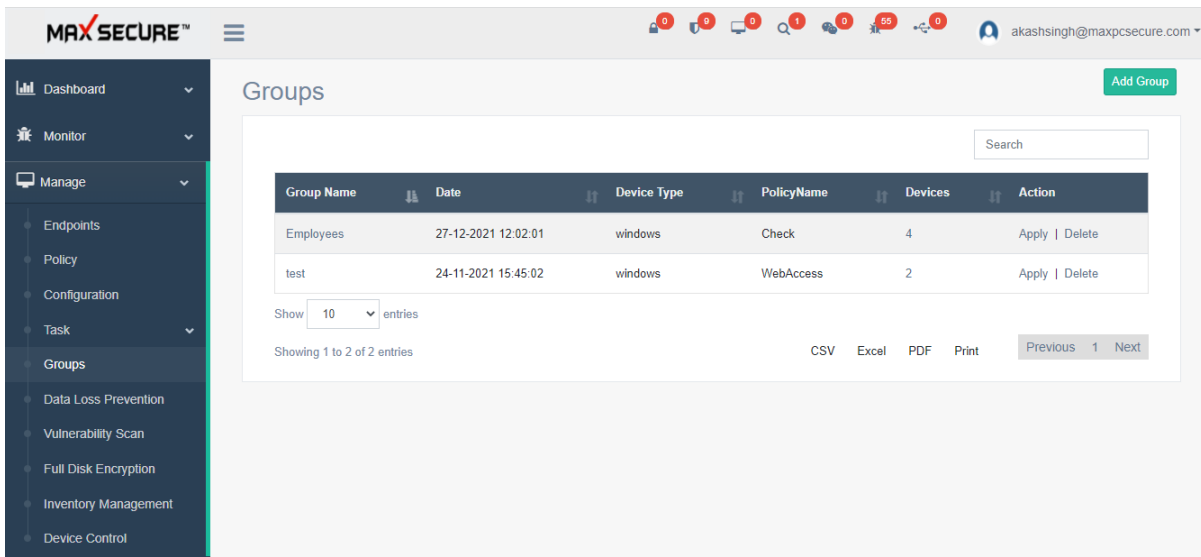
No data available in table

Show 10 entries

Showing 0 to 0 of 0 entries

Groups

- Create Groups for easy management of devices
- Create groups according to your department list or location of offices or job hierarchy



Groups

Search

Group Name	Date	Device Type	PolicyName	Devices	Action
Employees	27-12-2021 12:02:01	windows	Check	4	Apply Delete
test	24-11-2021 15:45:02	windows	WebAccess	2	Apply Delete

Show 10 entries

Showing 1 to 2 of 2 entries

CSV Excel PDF Print Previous 1 Next

Add Group

For example if you have a sales team, development team, account team and administration team. You would like to assign different features or web control or applications or restrictions then you can put them in groups. Create policies and instead of applying to individual devices you can select Groups. If you need to change any features on all of them then just change the policy and apply again to this group.

Another scenario could be that you have teams located on different physical locations. You could put them in different groups naming according to the location and assign similar policies.

Any changes in policy is immediately applied to all the devices under that group.

How to create group?

Click on Add Group button, write group name and then select Client Agent available on the Devices List (It will automatically come to the Selected Clients list showing on the right side of the page) after that click on Save button.

Manage → Groups → Add Group

MAXSECURE™

Create Group [Back] [Save]

Group

Type here the new Group Name, then select devices from the list below and Save.

Group Name : *

Devices List

Devices

Search [Select All] [Select Page]

Device	Ip Address	Policy	OS	Group Name	Action
TUSHARWIN10	193.168.0.130	Tushar	windows 10 enterprise ltsc 2019	test	Select
AKASH	192.168.1.6	WebAccess	windows 10 pro n	test	Select

Selected Devices (2)

Search [Clear]

Device	Action
TUSHARWIN10	Remove
DESKTOP-SBQE1S7	Remove

Show 10 entries

Group page show total created groups with more fields like Group Name, Date, Device Type, Policy Name (shows applied policy to the group), Devices (it shows total number of devices added in that group & after clicking on it you can also see the list of devices added), Action (Apply | Delete) will allow admin to apply Policy to the group & delete will allow to delete that group. Admin can also export Groups details into csv, excel, pdf and give print command also to print this created groups details.

Manage → Groups

The screenshot displays the 'Groups' management interface in the Max Secure Cloud Portal. The left sidebar lists various management categories, with 'Groups' currently selected. The main content area features a table listing existing groups, a search bar, and options to add or manage groups. The table contains the following data:

Group Name	Date	Device Type	PolicyName	Devices	Action
testers	28-12-2021 11:38:11	windows	No Policy Apply	2	Apply Delete
Employees	27-12-2021 12:02:01	windows	Check	3	Apply Delete
test	24-11-2021 15:45:02	windows	WebAccess	1	Apply Delete

Below the table, there is a 'Show 10 entries' dropdown and a 'Showing 1 to 3 of 3 entries' status. At the bottom right of the table area, there are links for 'CSV', 'Excel', 'PDF', and 'Print', along with 'Previous' and 'Next' pagination controls.

Data Loss Prevention (DLP)

Max Endpoint Data Loss Prevention stops sensitive data from moving off devices. For example, Max Endpoint Data Loss Prevention can stop a file that contains Credit Card numbers, PAN numbers, Aadhaar numbers, and Driving License number from being transferred to eSATA, USB, or FireWire-connected media. Max Endpoint Data Loss Prevention stops sensitive files from being transferred to network shares.

Here you can specify the keywords or Rules on content or filename only.

If any such rule is found while copying data, for example to a USB device then tray notification will come up on violation, file copy will be blocked and report will be sent to the portal on such alert.

You can use policies to detect and block confidential or at-risk information moving from devices in your organization. Sensitive or at-risk data can include credit card numbers or names, addresses, and identification numbers. You can configure Max Endpoint Data Loss Prevention to recognize and protect the files that contain sensitive data.

When Max Endpoint Data Loss Prevention detects an activity that violates a policy, a violation is generated. You can review and remediate the violations that display on the Violations screen.

How to create DLP Rule?

Click on Add Rule button, write DLP policy name and then select DLP Rule as per your need, here is the detailing:

DLP Protection: This checkbox is used to turn DLP Protection ON & OFF.

Block File Transfer & Notify: This radio button is to block file from transfer after applied rule violates on Client agent side.

Allow File transfer & Notify: This radio button is to allow file transfer but notify when applied rule violates on Client agent side.

Search includes File Names: This checkbox is to check name of the file if it contains that you added on 'Custom Content' text box or not and if it found so that text you entered on Custom Content field and the file name is same it will prevent that file also. Basically for this one needs to add Custom Content also.

Case Sensitive: This feature is for Custom Content (strings available on file) to prevent it from loss, by checking this it will scan for exact content with exact case (whether it is in upper or lower).

Unicode Search: This feature is for Custom Content (strings available on file) to prevent it from loss, by checking it will read file as Unicode also because by default it will read in ANSI format.

SHA256: This checkbox is to enable/disable feature that can be used to protect file having provided SHA256 (hash).

Add SHA256 Hash Value: This textbox is used to enter SHA256 (hash) value of the file which needs to be protected.

Credit/Debit Card: This checkbox will help to protect Credit/Debit card info available on Client Agent's machine in the form of xls; .doc; .xlsx; .docx; .txt; .log; .ini; etc.

Driving License: This will monitor to prevent the loss of Driving License information available on Client Agent's machine.

PAN card: This will monitor to prevent the loss of your PAN card information available on Client Agent's machine.

Aadhaar Card: This checkbox will help Admin to prevent the loss of your Aadhaar card information available on Client Agent's machine.

Block Extension: This is an independent feature which will protect file having added file type into 'Enter Block Extension' list textbox. It will protect all file with provided file type, now let suppose you want to prevent every .docx file available on your machine now you can simply add .docx into it and set/apply that DLP policy to you and that is it, your purpose will get solve, it will protect every .docx file.

Include Extension: Include extension which watch those files having extensions that you have provided in the Include extension list only.

Manage → Data Loss Prevention

MAXSECURE™

Create Policy

Policy Name :

☒ DLP Protection

☒ Block File Transfer & Notify ☐ Allow File transfer & Notify

☒ Search includes File Names ☒ Case Sensitive ☐ Unicode Search ☐ SHA256

CONDITIONS

☒ Credit/Debit card ☒ Driving License ☒ PAN card ☒ Aadhaar card

☒ Add Custom Content

Add Custom Content :

Key Phrase	Delete
suspicious	<input type="button" value="Delete"/>

DLP page show total number of created DLP rules with more fields like Rule Name, Date, Action (Apply | Delete) will allow admin to apply DLP Rule to Client Agents & delete will allow to delete that DLP Rule from that list.

Data Loss Prevention

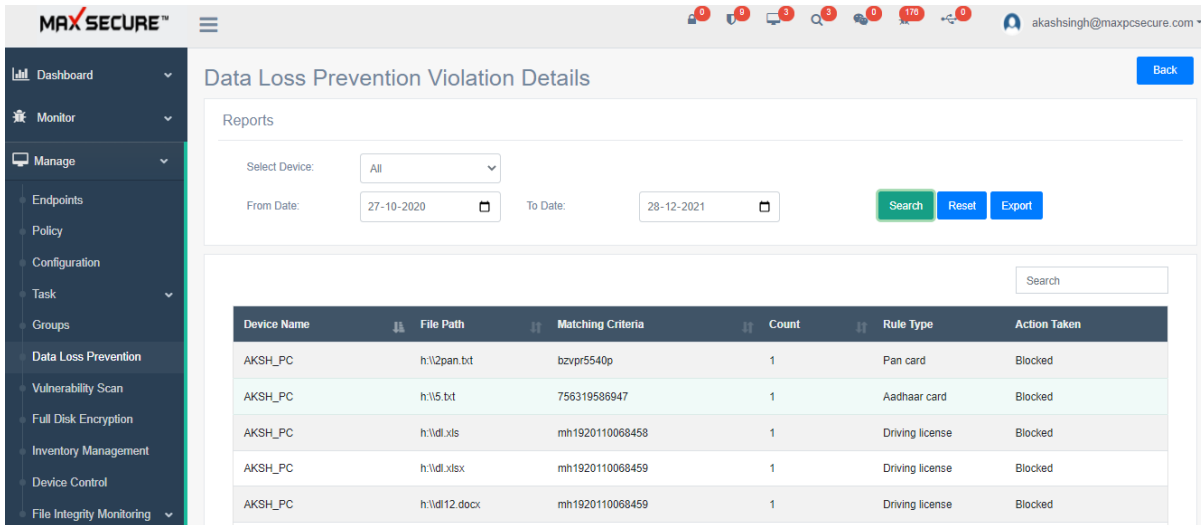
Data Loss Prevention Policy Details

Rule	Date	Action
DLP FRESH	15-12-2021 12:04:57	Apply Delete
addddip	30-11-2021 11:58:11	Apply Delete
newonedip	24-11-2021 16:50:11	Apply Delete
again check	24-11-2021 12:57:39	Apply Delete
dipnewMR	24-11-2021 12:24:43	Apply Delete
dip check	24-11-2021 12:21:29	Apply Delete
dip3	23-11-2021 17:32:25	Apply Delete
dip23	23-11-2021 17:27:53	Apply Delete

How can we see Data Loss Prevention Reports?

Click on Details button available on main DLP page to view DLP reports. When Max Endpoint Data Loss Prevention detects an activity that violates a policy, a violation is generated.

On DLP Reports page we can see details like Device name where DLP rule violates, File Path with file name, Matching Criteria will show the content like Aadhaar number, PAN number, DL number etc., Rule Type shows through which criteria it comes like PAN, Driving License etc., Action Taken shows us after violation detection which action is taken like Blocked or Notified.



Device Name	File Path	Matching Criteria	Count	Rule Type	Action Taken
AKSH_PC	h:\2pan.txt	bzvr5540p	1	Pan card	Blocked
AKSH_PC	h:\5.txt	756319586947	1	Aadhaar card	Blocked
AKSH_PC	h:\dl.xls	mh1920110068458	1	Driving license	Blocked
AKSH_PC	h:\dl.xlsx	mh1920110068459	1	Driving license	Blocked
AKSH_PC	h:\dl12.docx	mh1920110068459	1	Driving license	Blocked

Update Management

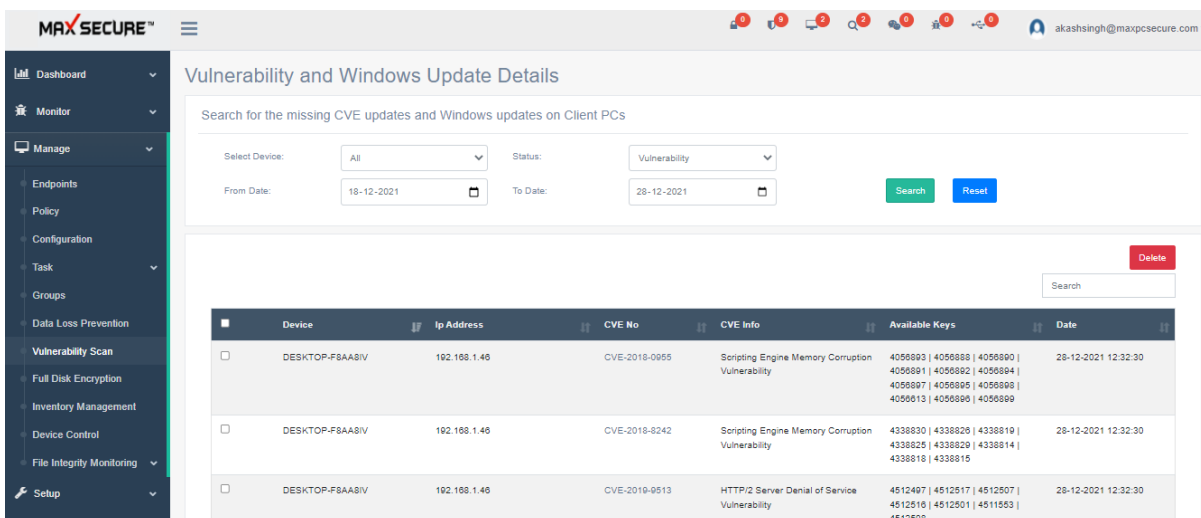
Vulnerability Scan

Left menu bar → Windows → Vulnerability scan provide you on missing windows updates and security updates on all the devices

View results of Windows Updates and CVE vulnerabilities found in all the devices. This shows Admin all the vulnerability on all the devices and he can update them online offline using WSUS server. We also provide document on ow to use that for offline / on premise installation

It is very important to keep your operating system updated for best security practises.

Manage → Update Management → Select status Vulnerability Scan/Windows Update



Device	Ip Address	CVE No	CVE Info	Available Keys	Date
DESKTOP-F8AA8IV	192.168.1.45	CVE-2018-0955	Scripting Engine Memory Corruption Vulnerability	4056890 4056888 4056890 4056891 4056892 4056894 4056897 4056895 4056898 4056913 4056889 4056899	28-12-2021 12:32:30
DESKTOP-F8AA8IV	192.168.1.45	CVE-2018-8242	Scripting Engine Memory Corruption Vulnerability	4338830 4338826 4338819 4338825 4338829 4338814 4338816 4338815	28-12-2021 12:32:30
DESKTOP-F8AA8IV	192.168.1.45	CVE-2019-0513	HTTP/2 Server Denial of Service Vulnerability	4512497 4512517 4512507 4512519 4512501 4511553 4512508	28-12-2021 12:32:30

Software Updates

This will allow Admin to update all client PC software from the server.

Here is a list of Software's that can be updated from server. Software's are available for both 32 and 64 bit operating systems:

1. Notepad++
2. Firefox
3. Thunderbird
4. JDK
5. 7-Zip
6. Putty
7. VLC

Procedure to do the Software Update

1. When Client Agent is installed, it will check for above mentioned software that it is available on the client's machine.
2. Admin can also see the software's updated listed on the portal: **Manage>Update Management>Software Updates.**

MAX SECURE™

Vulnerability, Software updates and Windows Update Details

Search for the missing CVE updates, Software updates...

Select Device: All Status: Software

From Date: 12/0 To Date: 22/0 Search Reset

Update

	Device	Os	Ip Address	Architecture	Software Name	Version
<input type="checkbox"/>	DHEERAJ-PC	windows 7 ultimate	192.168.1.13	vlc_x32	vlc media player	3.0.16
<input type="checkbox"/>	DHEERAJ-PC	windows 7	192.168.1.13	7zip_x64	7-zip 19.00 (x64)	19.00

Activate Windows
Go to PC settings to activate Windows.

3. We can check various information about software like **Device, OS, IP Address, Architecture, Software Name, Version, Available Version, and Date.**

The screenshot displays the 'Vulnerability, Software updates and Windows Update Details' page in the MAXSECURE portal. The left sidebar contains navigation options: Dashboard, Monitor, Manage (with sub-items: Endpoints, Zero Trust Access, Policy, Configuration, Task, Groups, Data Loss Prevention, Update Management, Full Disk Encryption, Inventory Management, Device Control, Server Live Update, File Integrity Monitoring), and a search bar. The main content area has a search bar and filters for 'Select Device' (All), 'Status' (Software Up), 'From Date' (12/03/2), and 'To Date' (22/03/2). Below the filters is a table with columns: Device, Os, Ip Address, Architecture, Software Name, Version, Available Version, and Date. The table lists three devices, all with 'Software Up' status. A tooltip for the first device shows 'vlc media player' is up to date.

Device	Os	Ip Address	Architecture	Software Name	Version	Available Version	Date
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	vlc_x32	vlc media player	3.0.16	3.0.16	14-03-2022 18:13:56
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	7zip_x64	7-zip 19.00 (x64)	19.00	21.07	14-03-2022 18:13:56
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	firefox_x64	mozilla firefox 97.0 (x64)	97.0	96.0	14-03-2022 18:13:56

4. If the software version is already updated, so in this case no update will be done.

This screenshot is similar to the previous one, showing the same software update details page. However, a tooltip for the first device (DHEERAJ-PC) explicitly states 'vlc media player is up to date.' The table data remains the same, showing that the current version (3.0.16) matches the available version (3.0.16).

Device	Os	Ip Address	Architecture	Software Name	Version	Available Version	Date
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	vlc_x32	vlc media player	3.0.16	3.0.16	14-03-2022 18:13:56
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	7zip_x64	7-zip 19.00 (x64)	19.00	21.07	14-03-2022 18:13:56
DHEERAJ-PC	windows 7 ultimate	192.168.1.13	firefox_x64	mozilla firefox 97.0 (x64)	97.0	96.0	14-03-2022 18:13:56

5. To do update, admin can tick the checkbox of the respective software admin wants to update on clients agent machine.

Vulnerability, Software updates and Windows Update Details

Search for the missing CVE updates, Software updates and Win...

Select Device: Status:

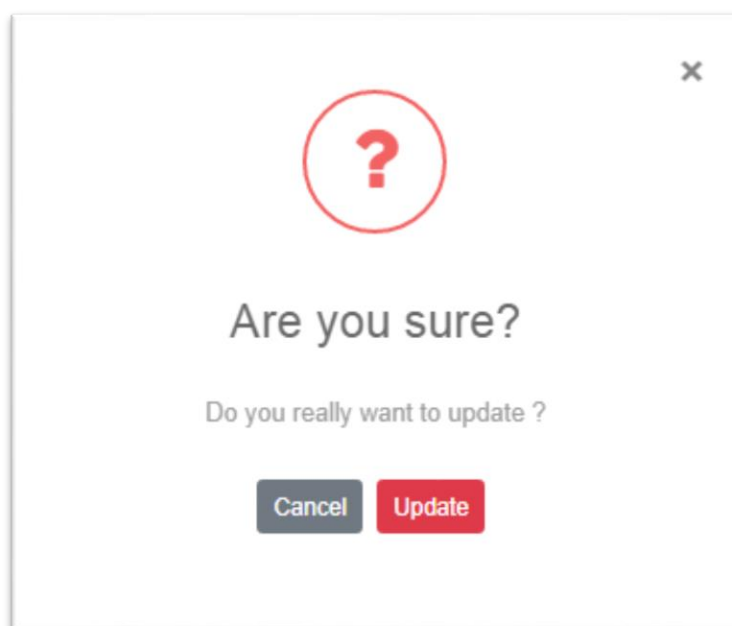
From Date: To Date:

	Device	Os	Ip Address	Architecture	Software Name	Version	Available Version	Date
<input type="checkbox"/>	DHEERAJ-PC	windows 7 ultimate	192.168.1.13	vlc_x32	vlc media player	3.0.16	3.0.16	14-03-2022 18:13:56
<input checked="" type="checkbox"/>	DHEERAJ-PC	windows 7 ultimate	192.168.1.13	7zip_x64	7-zip 19.00 (x64)	19.00	21.07	14-03-2022 18:13:56
<input type="checkbox"/>	DHEERAJ-	windows	192.168.1.13	firefox_x64	mozilla	97.0	96.0	14-03-

Search

Activate Windows
Go to PC settings to activate Windows.

6. Click on 'Update' button a new popup will open, then click on Update.



- After updating the software, it will reflect the latest updated version on the portal.

Full Disk Encryption

Full Disk Encryption prevents other users from gaining unauthorized access to data stored on the user's device.

Remotely install or uninstall FDE on selected Client Agents.

Max Cloud AV for Windows encrypts all logical partitions of hard drives of a device simultaneously or chosen files/folders in a mounted drive.

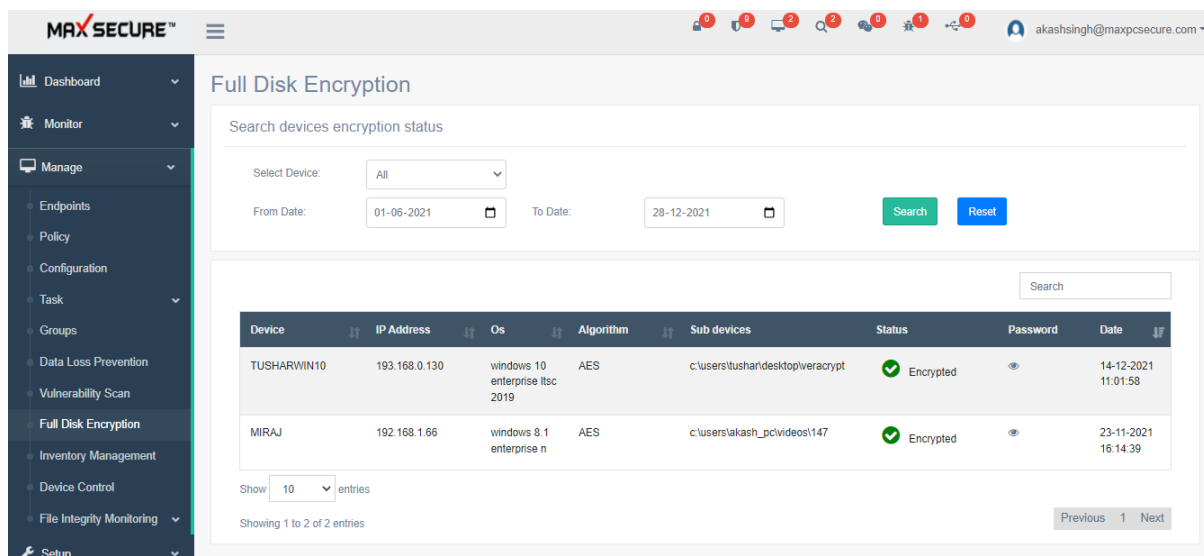
Recovery keys are stored in the Max Cloud AV Portal infrastructure.

Client Agent can choose several encryption algorithms, & admin can monitor that all through over portal.

Admin can also encrypt external USB devices or external hard disks. So that all the data on the device will be protected and can only be opened by Admin having the Client agent software installed and know the password.

Please note here that if you want to encrypt data on External drive and secure it so that it cannot be used anywhere and only when connected to PCs where you have Cloud AV installed and allowed that Device access to this USB from portal to read/copy data. This feature can go long way in securing Data from misuse and theft. To enable this use FDE module from the left menu bar.

Manage → Full Disk Encryption



The screenshot shows the 'Full Disk Encryption' section of the Max Secure portal. The left sidebar contains a navigation menu with options: Dashboard, Monitor, Manage (selected), Endpoints, Policy, Configuration, Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption (highlighted), Inventory Management, Device Control, File Integrity Monitoring, and Setup. The main content area is titled 'Full Disk Encryption' and includes a search bar for 'Search devices encryption status'. Below the search bar are filters for 'Select Device' (set to 'All'), 'From Date' (01-06-2021), and 'To Date' (28-12-2021), with 'Search' and 'Reset' buttons. A table displays the encryption status of two devices:

Device	IP Address	Os	Algorithm	Sub devices	Status	Password	Date
TUSHARWIN10	193.168.0.130	windows 10 enterprise ltsc 2019	AES	c:\users\tushar\desktop\veracrypt	✓ Encrypted	👁	14-12-2021 11:01:58
MIRAJ	192.168.1.66	windows 8.1 enterprise n	AES	c:\users\lakash_pc\videos\147	✓ Encrypted	👁	23-11-2021 16:14:39

Below the table, it shows 'Showing 1 to 2 of 2 entries' and navigation links for 'Previous', '1', and 'Next'.

Inventory Management

Max Endpoint Security-Business provides you the ability to overview and manage your client machine assets in the form of inventories.

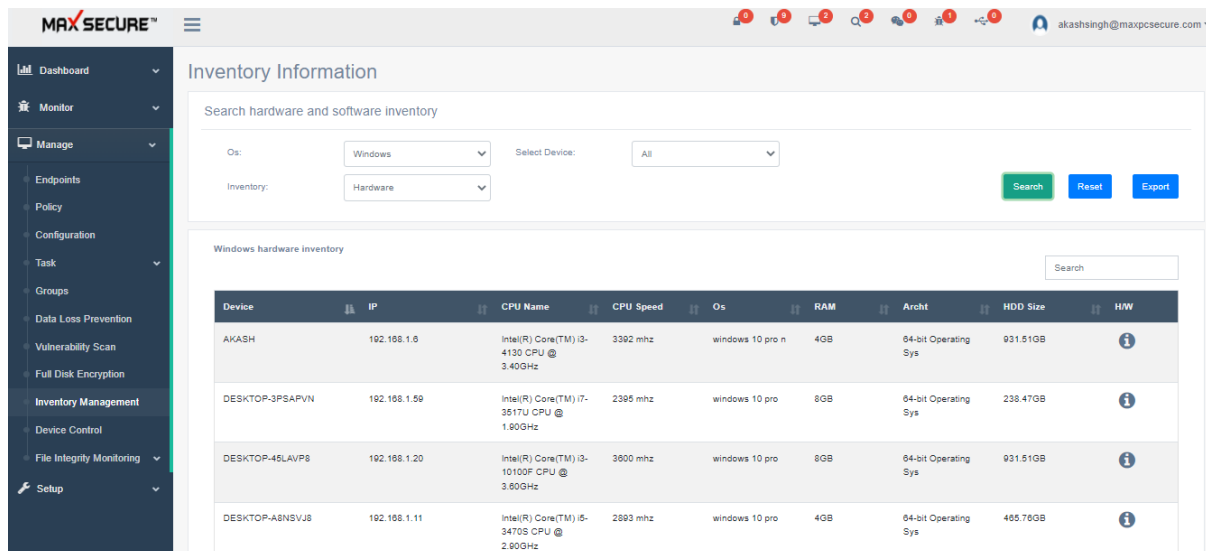
Hardware Inventory

Scan the systems periodically to get complete hardware details of Windows computers like hard disk, network adapters, physical memory, processors etc.

Here it shows inventory of network devices with below information which you can export to excel for reporting:

1. **Device Name:** Device which contains that inventory.
2. **IP address:** IP Address of the device.
3. **CPU Name:** Processor details will be shown here.
4. **CPU Speed:** Clock speed will be shown.
5. **O.S:** Operating System information will be shown here.
6. **RAM:** RAM size will be shown here.
7. **Architecture:** Processor architecture will be shown here.
8. **HDD Size:** Hard-disk size details will be shown here.

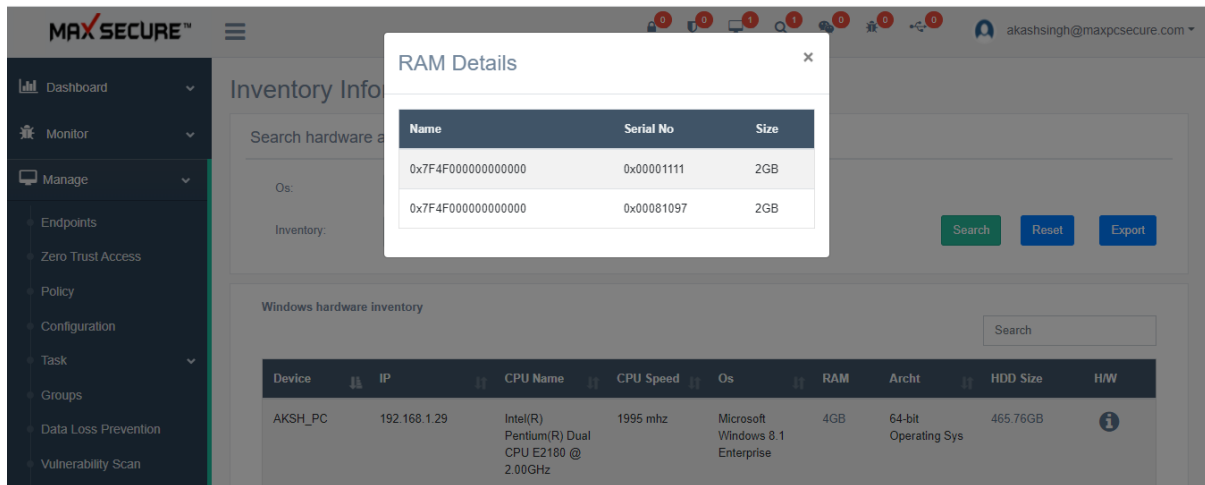
Manage → Inventory Management



The screenshot shows the 'Inventory Information' page in the MAX SECURE interface. It includes a search bar and filters for OS (Windows), Select Device (All), and Inventory (Hardware). Below the filters is a table titled 'Windows hardware inventory' with columns: Device, IP, CPU Name, CPU Speed, Os, RAM, Archt, HDD Size, and HW. The table lists four devices with their respective hardware details.

Device	IP	CPU Name	CPU Speed	Os	RAM	Archt	HDD Size	HW
AKASH	192.168.1.6	Intel(R) Core(TM) i3-4130 CPU @ 3.40GHz	3392 mhz	windows 10 pro n	4GB	64-bit Operating Sys	931.51GB	i
DESKTOP-3PSAPVN	192.168.1.59	Intel(R) Core(TM) i7-3517U CPU @ 1.90GHz	2385 mhz	windows 10 pro	8GB	64-bit Operating Sys	238.47GB	i
DESKTOP-45LAVP8	192.168.1.20	Intel(R) Core(TM) i3-10100F CPU @ 3.60GHz	3600 mhz	windows 10 pro	8GB	64-bit Operating Sys	931.51GB	i
DESKTOP-A8NSVJ8	192.168.1.11	Intel(R) Core(TM) i5-3470S CPU @ 2.90GHz	2893 mhz	windows 10 pro	4GB	64-bit Operating Sys	465.76GB	i

1. **RAM:** It shows RAM details of a client agent machine, and when we click on that, a new popup opens showing 'Name', 'Serial No.', and 'Size' of RAM so in case if there are multiple RAMs, it shows all of them.

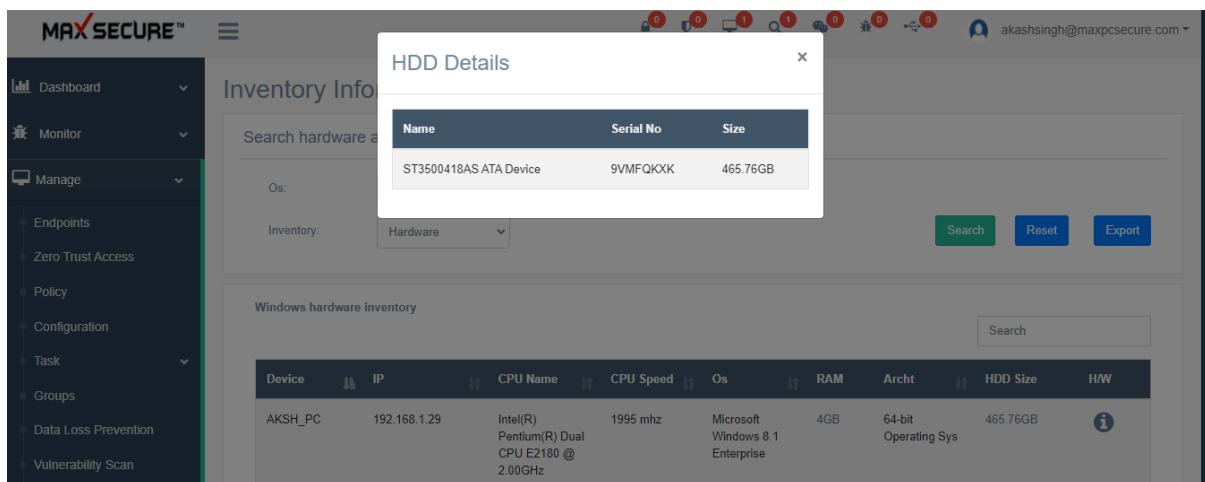


The screenshot shows the MAXSECURE™ interface with a 'RAM Details' pop-up window. The pop-up contains a table with the following data:

Name	Serial No	Size
0x7F4F000000000000	0x00001111	2GB
0x7F4F000000000000	0x00081097	2GB

The background interface shows the 'Inventory Info' section with a search bar and a table of hardware inventory. The table has columns: Device, IP, CPU Name, CPU Speed, Os, RAM, Archt, HDD Size, and H/W. The first row shows data for AKSH_PC.

2. HDD Size: This shows the actual HDD details of a client agent machine, and a pop-up opens that shows the HDD's name, serial number, and size.

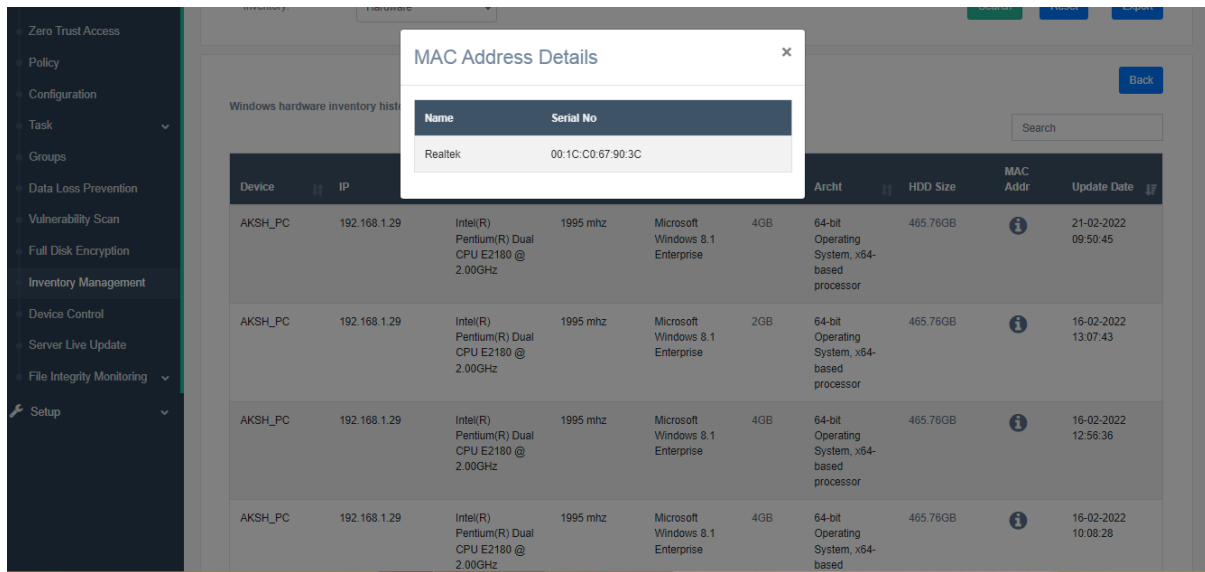



The screenshot shows the MAXSECURE™ interface with a 'HDD Details' pop-up window. The pop-up contains a table with the following data:

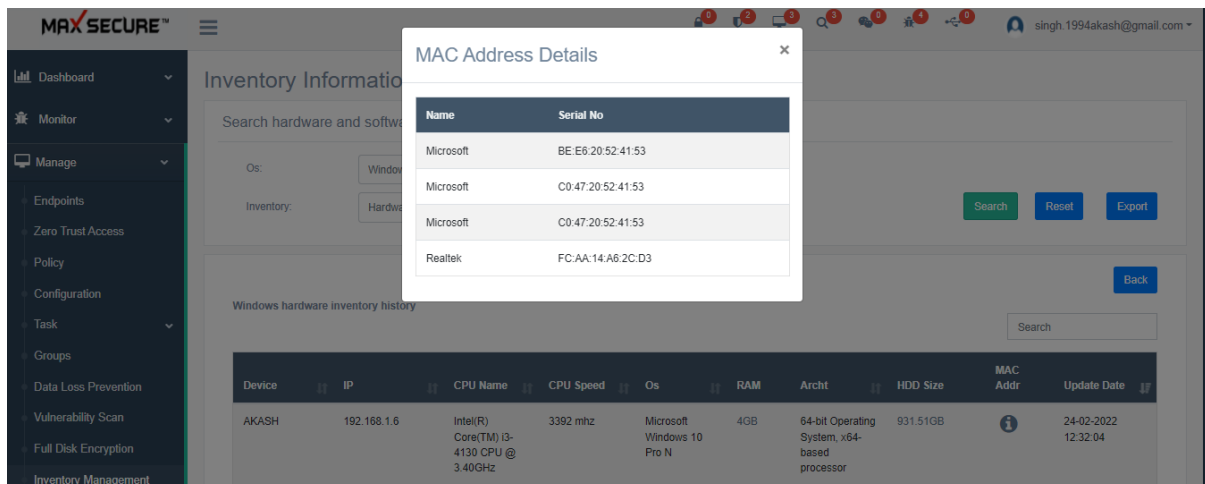
Name	Serial No	Size
ST3500418AS ATA Device	9VMFQKXX	465.76GB

The background interface shows the 'Inventory Info' section with a search bar and a table of hardware inventory. The table has columns: Device, IP, CPU Name, CPU Speed, Os, RAM, Archt, HDD Size, and H/W. The first row shows data for AKSH_PC.

3. H/W: Clicking on the info icon (i), more information will appear, e.g. MAC Address and Update Date. It will show multiple details of one device and will allow us to see if any changes are made to the hardware.



3.1 MAC Address: Clicking on the info icon () will show the MAC address.



3.2 Update Date : The time and date when hardware changes occurred can be found here

More Hardware Information

Admin can also see 'Device Summary' like PC name, OS, RAM, Hard disk size, Motherboard id, Last Shutdown date, etc. and 'System Configuration' like HDD Serial, Windows Key, Office Key, Architecture, etc.

How can we see Device Summary & System Configuration details?

1. Go to → *Manage* → *Endpoints*

2. Click on the desired 'Device Name'
3. By-default it will show 'Device Info'

The screenshot displays the Max Secure Cloud Portal interface. On the left is a dark sidebar with navigation options: Dashboard, Monitor, Manage (with sub-items: Endpoints, Zero Trust Access, Policy, Configuration, Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, File Integrity Monitoring), and Setup. The main content area is titled 'Device Details' and has three tabs: 'Device Info' (selected), 'Lost Device Location', and 'Stolen Pics'. Below the tabs, the device name 'AKSH_PC' and machine ID 'BTNL82100BT1' are shown. The 'Device Info' tab contains two panels: 'DEVICE SUMMARY' and 'SYSTEM CONFIGURATION'. The 'DEVICE SUMMARY' panel lists various attributes of the device, and the 'SYSTEM CONFIGURATION' panel lists system-level details. At the bottom right, there is a 'Activate Windows' watermark.

Attribute	Value
Name	AKSH_PC
Device Type	Desktop
OS	windows 8.1 enterprise
Registration Token	FUU4U871D8B3DH9KDF7A
RAM	4GB
Hard-Disk Size	465.76GB
Mother Board Id	Intel Corporation.BTNL82100BT1
Last Login Date	2/24/2022 10:47:26 AM
Last ShutDown Date	2022-02-24 10:46:21

Attribute	Value
MAC Address	00-1C-C0-67-90-3C
HDD Serial	9VMFQKXK
CPU Name	Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz
CPU Speed	1995 mhz
RAW ID	[4afe-87c0]
Architecture	64-bit Operating Sys
Office Key	OFFICE 15-*GVQXT,OFFICE 16-*WFG99
Windows Key	MHF8N-XY8XB-WVXMC-BTDC7-MKK07

Software Inventory

A complete list of all the installed software details, like the software name, version, and manufacturer details etc.

Admin can see the details like:

Device Name: Device which contains that software.

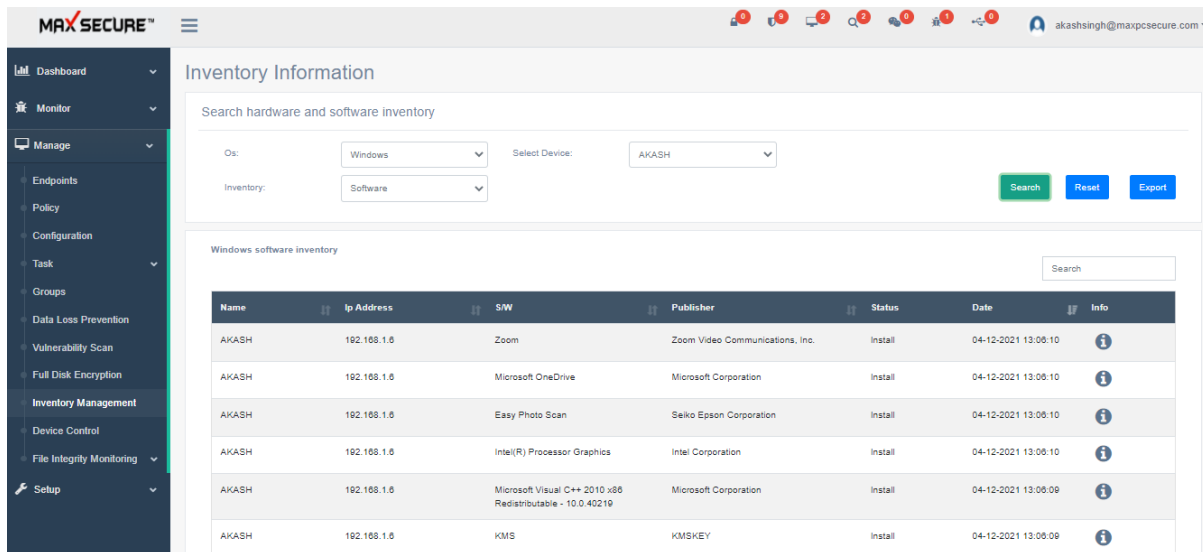
IP address: IP Address of the device which has that software.

Software Name: Name of the software.

Publisher: Name of the company from which this software belongs.

Status: This will show the current status that this software is installed or has been removed/uninstalled.

Info: Clicking on the info icon (i), it will be redirected towards the new detailed page where admin can see software name, its publisher name, software version, installed date and on portal last update date.



Inventory Information

Search hardware and software inventory

Os: Windows Select Device: AKASH Inventory: Software

Search Reset Export

Windows software inventory

Name	Ip Address	S/W	Publisher	Status	Date	Info
AKASH	192.168.1.6	Zoom	Zoom Video Communications, Inc.	Install	04-12-2021 13:06:10	i
AKASH	192.168.1.6	Microsoft OneDrive	Microsoft Corporation	Install	04-12-2021 13:06:10	i
AKASH	192.168.1.6	Easy Photo Scan	Seiko Epson Corporation	Install	04-12-2021 13:06:10	i
AKASH	192.168.1.6	Intel(R) Processor Graphics	Intel Corporation	Install	04-12-2021 13:06:10	i
AKASH	192.168.1.6	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation	Install	04-12-2021 13:06:09	i
AKASH	192.168.1.6	KMS	KMSKEY	Install	04-12-2021 13:06:09	i

Device Control

To enhance productivity, you need to provide your users easy access to data, often outside the network. But the risk of opening the door to malware and data loss through devices is a real concern.

Device Control provides effective, scalable protection. Ideal for servers, fixed-function assets and thin-client or virtualized endpoints, Device Control allows you to lock down endpoints to prevent unauthorized use of devices like Wi-Fi, Bluetooth & Network Adaptors help us to prevent unknown apps from being installed and executed—reducing your attack surface exponentially.

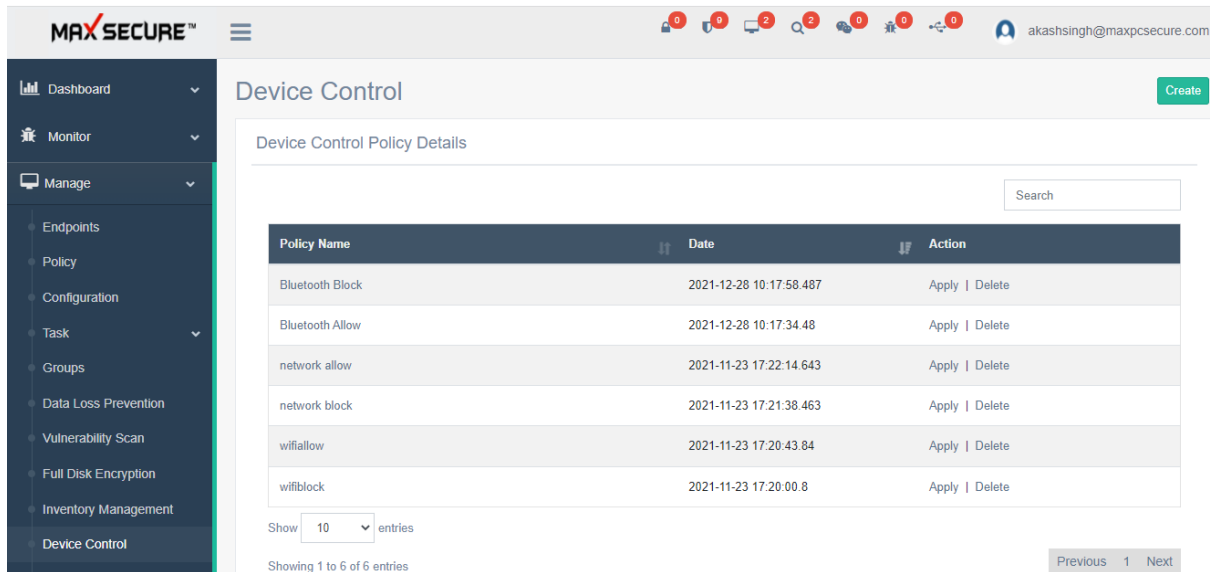
There are 3 steps to add a Device Control policy on the *Manage* → *Device Control* → *Create*
Manage → *Device Control* → *Create* (click on button)

Here we can have control over devices whether these devices are inbuilt or attached externally to Client Agent machines.

It allows admin to block/unblock (allow) following below devices:

1. Bluetooth Devices
2. Wi-Fi Network
3. Network Adaptors

Manage Device Control



Policy Name	Date	Action
Bluetooth Block	2021-12-28 10:17:58.487	Apply Delete
Bluetooth Allow	2021-12-28 10:17:34.48	Apply Delete
network allow	2021-11-23 17:22:14.643	Apply Delete
network block	2021-11-23 17:21:38.463	Apply Delete
wifiallow	2021-11-23 17:20:43.84	Apply Delete
wifi block	2021-11-23 17:20:00.8	Apply Delete

File Integrity Monitor

File integrity monitoring (FIM) is an internal control that performs the act of validating the integrity of an application software files or any specific directory/file using a verification method between the current file state and a known, good baseline. This comparison method involves validation of the file's original baseline and comparing with the current state of the directory/file. Other file attributes can also be used to monitor integrity.

FIM is a cloud solution for detecting and identifying critical changes, incidents, and risks resulting from normal and malicious events.

FIM Policy

From "FIM Policy" we can schedule FIM, when you want to launch integrity check on Client Agent side.

How can we Create FIM Policy?

1. Go to Manage → File Integrity Monitoring → FIM Policy → Create
2. Give FIM Policy name.
3. Here we can schedule FIM to scan daily or weekly.
4. Click on Save button.
5. Apply created policy to client agent.

Note: Turning FIM OFF will require you to make policy in which 'Scan Status' is unchecked and apply it to client agent.

The screenshot shows the 'Create Policy' page in the Max Secure web portal. The left sidebar contains a navigation menu with options: Dashboard, Monitor, Manage, Endpoints, Policy, Configuration, Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, and File Integrity Monitoring. Under 'File Integrity Monitoring', there are sub-options: FIM Policy, FIM Rule, and FIM Details. The main content area is titled 'Create Policy' and has a 'File Integrity Monitoring Policy' header. Below this, there is a 'Policy Name' field with the value 'fmscan'. There are two checkboxes: 'Scan Status' (checked) and 'Scheduler' (checked). Under the 'Scheduler' section, there are two radio buttons: 'Daily' (selected) and 'Weekly'. The 'Daily' option has a time field set to '01:10 PM'. The 'Weekly' option has a day dropdown set to 'Sunday' and a time field set to '01:10 AM'. At the top right of the main content area, there are 'Back' and 'Save' buttons. The user's email 'akashsingh@maxpcsecure.com' is visible in the top right corner.

FIM Rule

Integrity Monitoring rules describe how Cloud Agents should scan for and detect changes to a computer's files and directories. Integrity monitoring rules can be assigned directly to computers (Cloud Agents) or your created group (which may contain multiple computers) directly.

There are four steps to add an Integrity Monitoring rule on the *Manage* → *File Integrity Monitoring* → *FIM Rules* → *Create (Integrity Monitoring Rules)*

To create a new Integrity Monitoring rule, you need to:

1. Add a new rule name.
2. Select whether you monitor directory or file.
3. Enter Integrity Monitoring rule description.
4. Select monitoring path.
5. Select from given option to monitor file/directory removal, content, creation, digital certificate and define rule attributes.
6. You can also include/exclude specific extensions which will monitor all extensions other than available on exclude list or monitor only those extensions which is available on include extensions list or else you can also set this into all extension mode to monitors all file type.
7. Select targeting also whether to monitor files or folder (directory) or files and directory both.
8. Apply created policy to client agent.

The screenshot shows the 'Create Rule' page for File Integrity Monitoring in the Max Secure Cloud Portal. The left sidebar contains navigation links: Dashboard, Monitor, Manage, Endpoints, Policy, Configuration, Task, Groups, Data Loss Prevention, Vulnerability Scan, Full Disk Encryption, Inventory Management, Device Control, File Integrity Monitoring (selected), FIM Policy, FIM Rule, FIM Details, and Setup. The main content area is titled 'Create Rule' and 'File Integrity Monitoring Rule'. It includes a 'Rule Name' field with a placeholder 'FIMRule', a 'Rule Type' dropdown set to 'Directory', a 'Description' text area with placeholder text, a 'Path' field with 'C:\Program Files\New Software', and checkboxes for monitoring directory structure changes (Directory Removal, Directory Creation, Changes To Attributes, Changes To Security Settings). Under 'File Settings', there are checkboxes for File Removal, File Content Changes, File Digital Certificate, File Creation, Changes To Attributes, and Changes To Security Settings. At the bottom, there are 'Type' and 'Targeting' dropdown menus.

FIM Details

Viewing events that occurred when the integrity check task was last run

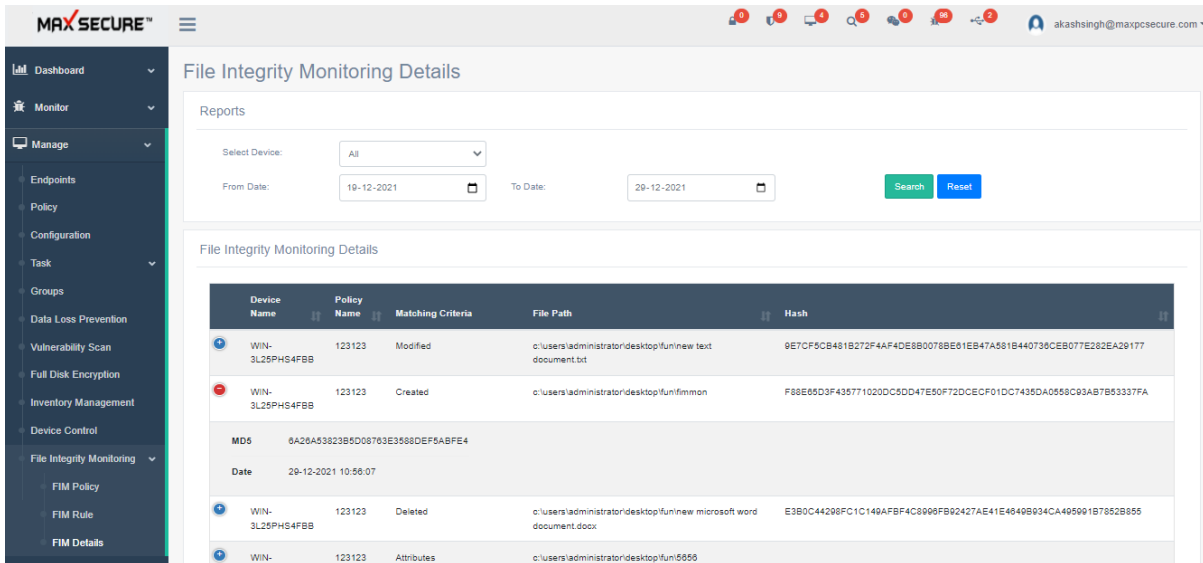
To view the list of events that occurred on the Client Agents machines when the integrity check task was run & found file/directory integrity mismatch during last run and current run.

There are four steps to add an Integrity Monitoring rule on the *Manage*→ *File Integrity Monitoring*→ *FIM Rules*→ *Create (Integrity Monitoring Rules)*

One can see File Integrity Monitor report by the order of event generation date (Select to & from date).

The table shows the following information about each event:

- Device Name
- Rule Name (which rule applied by the Integrity Monitoring component)
- Matching Criteria (which type of modification to the monitored object detected by Integrity Monitoring component)
- File/Folder Path
- File MD5 Signature
- File Hash Signature
- Event generation date



File Integrity Monitoring Details

Reports

Select Device: All

From Date: 19-12-2021 To Date: 29-12-2021

Search Reset

File Integrity Monitoring Details

Device Name	Policy Name	Matching Criteria	File Path	Hash
WIN-3L25PHS4FBB	123123	Modified	c:\users\administrator\desktop\fun\new text document.txt	9E7CF5CB481B272F4AF4DE8B0078BE61EB47A581B440736CEB077E282EA29177
WIN-3L25PHS4FBB	123123	Created	c:\users\administrator\desktop\fun\funmon	F88E65D3F435771020DC6DD47E50F72DCECF01DC7435DA0558C93AB7B53337FA
MD5	6A26A53823B5D06783E3588DEF5ABFE4			
Date	29-12-2021 10:56:07			
WIN-3L25PHS4FBB	123123	Deleted	c:\users\administrator\desktop\fun\new microsoft word document.docx	E3B0C44298FC1C149A4FBF4C8996F9B2427AE41E4649B934CA495901B7852B855
WIN-	123123	Attributes	c:\users\administrator\desktop\fun\5555	

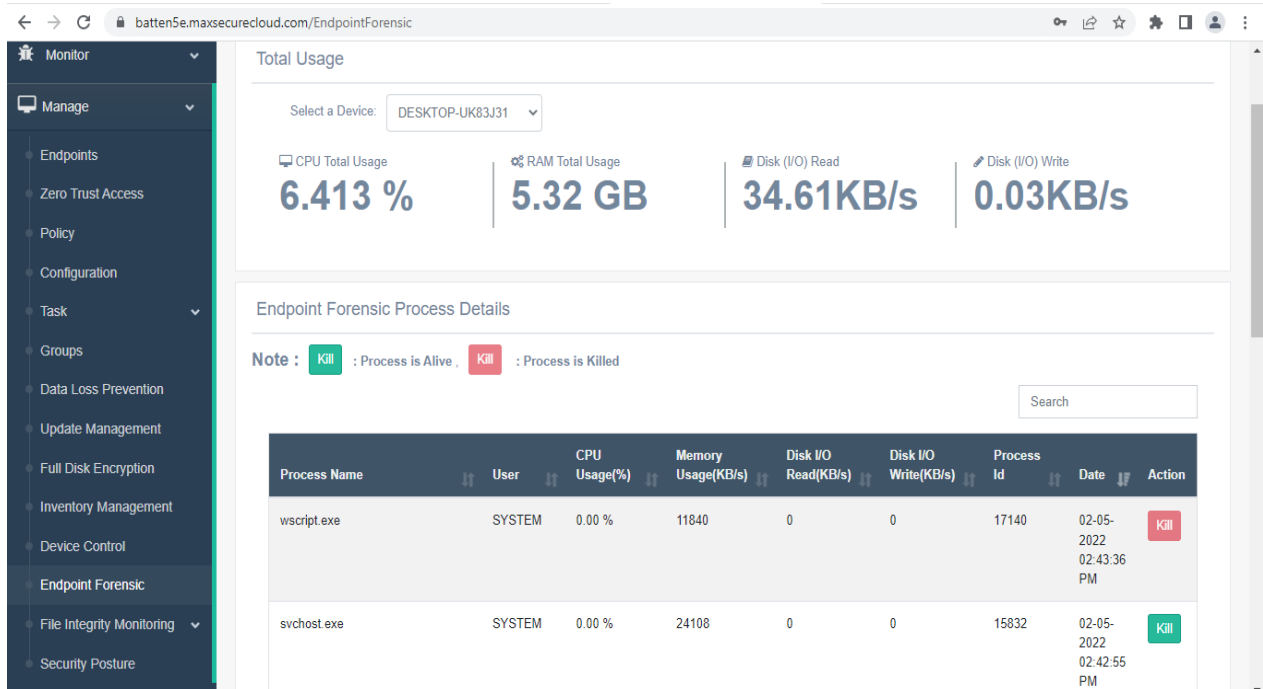
Endpoint Forensic

Endpoint forensics allows teams to remotely Monitor all the processes running on endpoints. By doing this, it's possible to pinpoint processes often used in multi-stage malware and identify specific processes that deviate from normal behavior.

Endpoint Forensics analyzes the behavior of thousands of endpoints for evidence of compromise, including malware and irregular activities, by collecting targeted forensic data.

This remote investigation can be done securely over any network, without requiring endpoint access authorization.

If Any Process Found Suspicious then we can kill that process over Network for that Endpoint



Total Usage

Select a Device: DESKTOP-UK83J31

CPU Total Usage: **6.413 %** | RAM Total Usage: **5.32 GB** | Disk I/O Read: **34.61KB/s** | Disk I/O Write: **0.03KB/s**

Endpoint Forensic Process Details

Note : Kill : Process is Alive , Kill : Process is Killed

Search

Process Name	User	CPU Usage(%)	Memory Usage(KB/s)	Disk I/O Read(KB/s)	Disk I/O Write(KB/s)	Process Id	Date	Action
wsript.exe	SYSTEM	0.00 %	11840	0	0	17140	02-05-2022 02:43:36 PM	Kill
svchost.exe	SYSTEM	0.00 %	24108	0	0	15832	02-05-2022 02:42:55 PM	Kill

How can we Check and Kill Malicious Process?

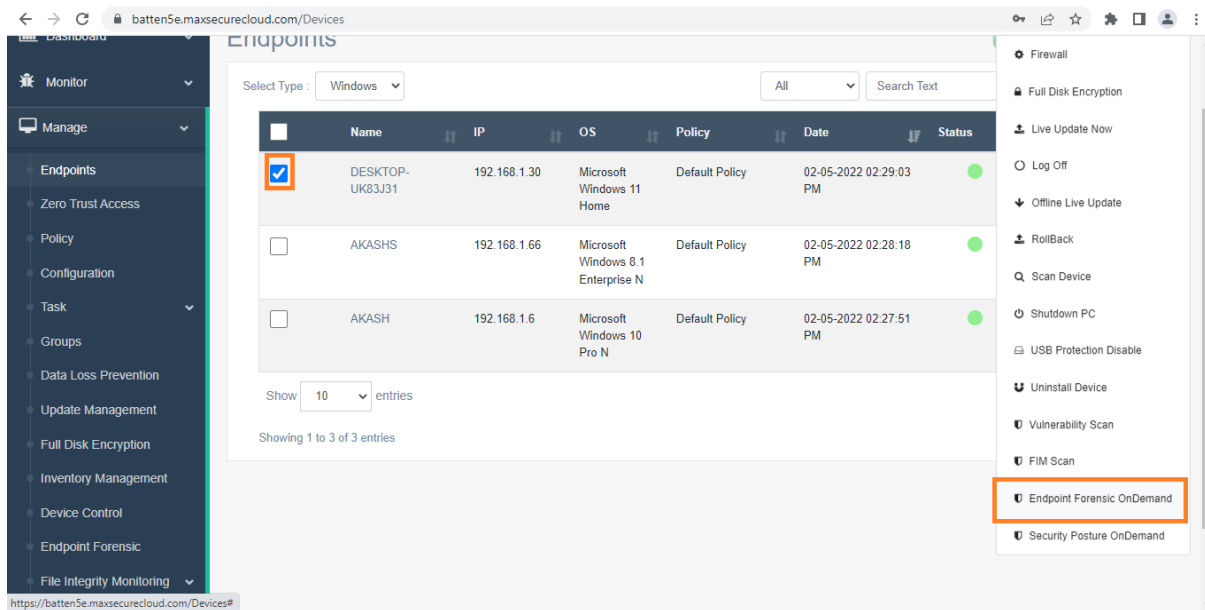
1. Go to Manage → Endpoint forensic → Select Device
2. Find the Process by ProcessName or Process ID
3. Click on Kill Button
4. After the Process is Terminated The Button Color will Change to: Kill

There are Two ways for Getting Data of Endpoint

1. It Will get Automatically once Everyday
2. On-Demand

For On-Demand

- Go to Manage → Endpoints → Select a Device → Click on Actions
- Then Click on → Endpoint Forensic OnDemand

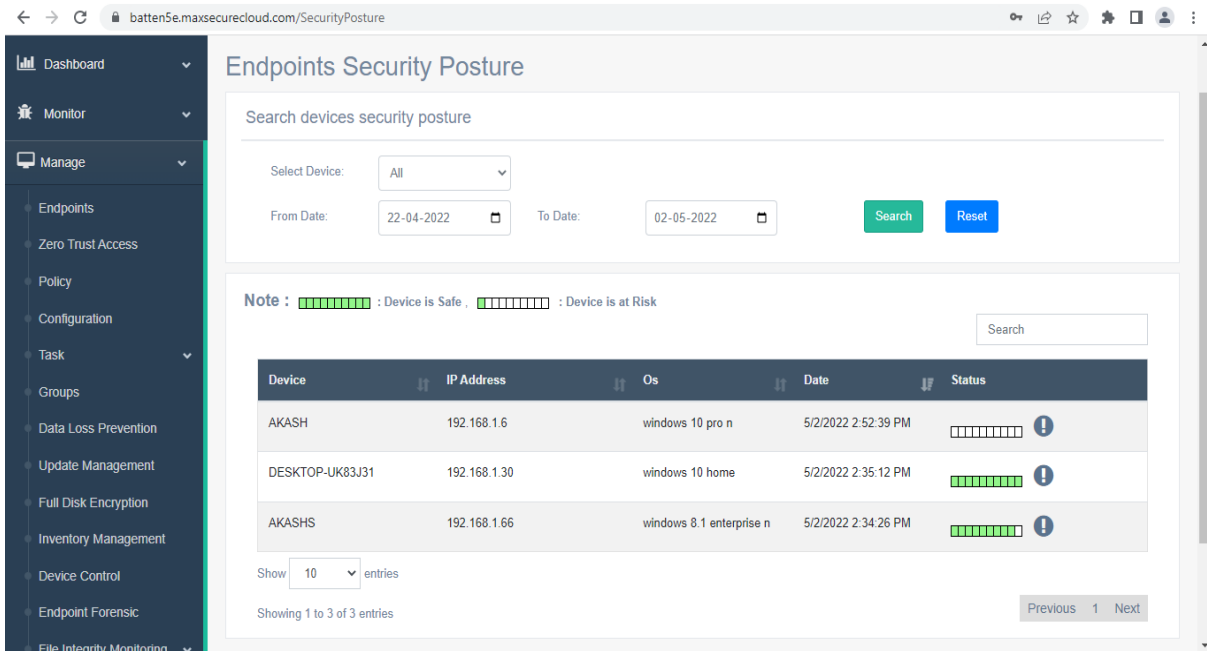


Endpoint Security Posture

Endpoint posture assessment involves orchestrating and performing data collection and evaluating the posture of a given endpoint

Endpoint Security posture assessment typically includes:

1. Collecting the attributes of a given endpoint
2. Verifying that the endpoint's posture is in compliance with enterprise standards and policy.
3. According to the Attributes It shows level indicator whether the device is safe or the device is at risk ,If the indicator is full then the Device is safe and if it is empty means device is vulnerable. (Shown in Below Image)



Endpoints Security Posture

Search devices security posture

Select Device: From Date: To Date:

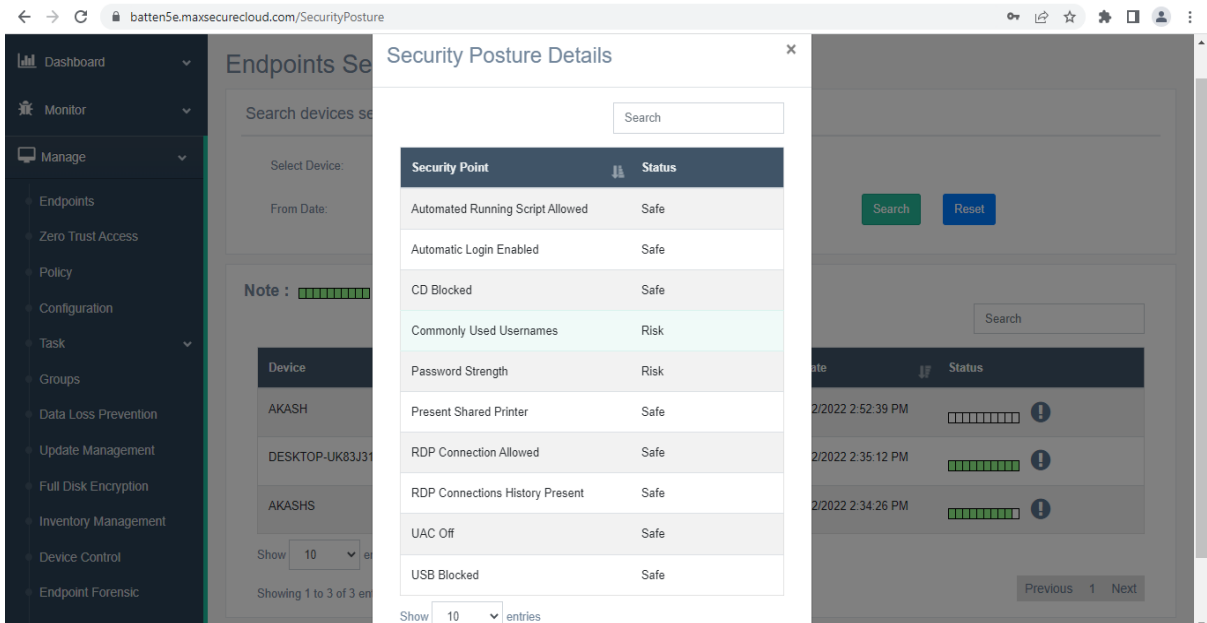
Note : ■■■■■■■■■■ : Device is Safe , ■■■■■■■■■■ : Device is at Risk

Device	IP Address	Os	Date	Status
AKASH	192.168.1.6	windows 10 pro n	5/2/2022 2:52:39 PM	■■■■■■■■■■ !
DESKTOP-UK83J31	192.168.1.30	windows 10 home	5/2/2022 2:35:12 PM	■■■■■■■■■■ !
AKASHS	192.168.1.66	windows 8.1 enterprise n	5/2/2022 2:34:26 PM	■■■■■■■■■■ !

Show entries
Showing 1 to 3 of 3 entries

Previous 1 Next

4. For More Detail->Click on (!) button It will show the parameters with its risk or safe factor.



Security Posture Details

Search devices security posture

Select Device: From Date: To Date:

Note : ■■■■■■■■■■ : Device is Safe , ■■■■■■■■■■ : Device is at Risk

Security Point	Status
Automated Running Script Allowed	Safe
Automatic Login Enabled	Safe
CD Blocked	Safe
Commonly Used Usernames	Risk
Password Strength	Risk
Present Shared Printer	Safe
RDP Connection Allowed	Safe
RDP Connections History Present	Safe
UAC Off	Safe
USB Blocked	Safe

Show entries

There are Two ways for Security Posture Detail of Endpoint

- It Will get Automatically once Everyday
- On-Demand
 Go to Manage → Endpoints → Select a Device → Click on Actions
 Then Click on -> Security Posture OnDemand

Setup

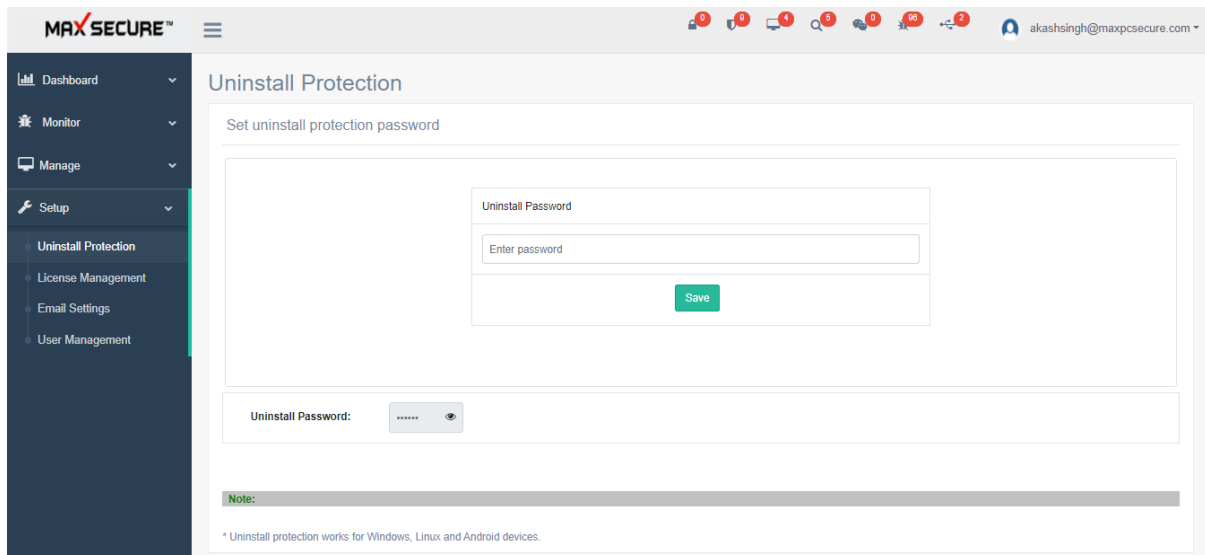
Uninstallation Protection

Uninstallation password makes sure that users do not uninstall the security software from their devices.

Set an uninstallation Password and devices cannot be uninstalled without this password.

Uninstall protection works for Windows, Linux and Android devices.

Setup → Uninstall Protection



The screenshot shows the MAX SECURE web interface. The left sidebar contains a menu with 'Setup' expanded, showing 'Uninstall Protection' as the selected option. The main content area is titled 'Uninstall Protection' and contains a form to 'Set uninstall protection password'. The form has a label 'Uninstall Password' and a text input field with the placeholder 'Enter password'. Below the input field is a green 'Save' button. At the bottom of the form, there is a label 'Uninstall Password:' followed by a masked password field (displayed as '*****') and an eye icon to toggle visibility. A 'Note:' section at the bottom states: '* Uninstall protection works for Windows, Linux and Android devices.'

License Management

Manage Registration Keys

Admin can manage Max Endpoint Security-Business portal registration keys from this page. Here Admin can monitor his registration key whether adding more registration key, renew registration key and many more things.

To manage registration keys, follow these steps:

1. Go to Max Endpoint Security-Business portal
2. Expand Setup, click on License Management

3. Click on 'Manage License' button.

Setup → License Management → Manage License

MAX SECURE

Registration Key Information

Back

Add License Key Renew License Key Generate Activation Key

On-Premises / Offline installation only

Company Name : Max Secure Software

Email-ID : testing@maxpcsecure.com

Total No Of License : 545

Dashboard Monitor Manage Setup Uninstall Protection License Management Email Settings User Management

testing@maxpcsecure.com

About Registration Keys

A registration key is issued from company side while you purchase Max Endpoint Security-Business, and it's used when you deploy cloud agents as per number of licenses you purchased.

Add License Key: Admin can add new registration key in case of increasing total number of client agents. If you want to upgrade your license from present number to a larger number of PCs, click on *Add More Licenses* button. Registration window will open for you to enter the new registration no. Then you can secure more number of PCs with this new license.

To-do this admin needs to go portal *Setup → License Management → click on 'Manage License' button → click on 'Add License Key' button.*

MAX SECURE

Registration Key Information

Back

Add License Key Renew License Key Generate Activation Key

On-Premises / Offline installation only

Company Name : Max Secure Software

Email-ID : testing@maxpcsecure.com

Total No Of License : 545

Dashboard Monitor Manage Setup Uninstall Protection License Management Email Settings User Management

akashsingh@maxpcsecure.com

Add License key

License Key

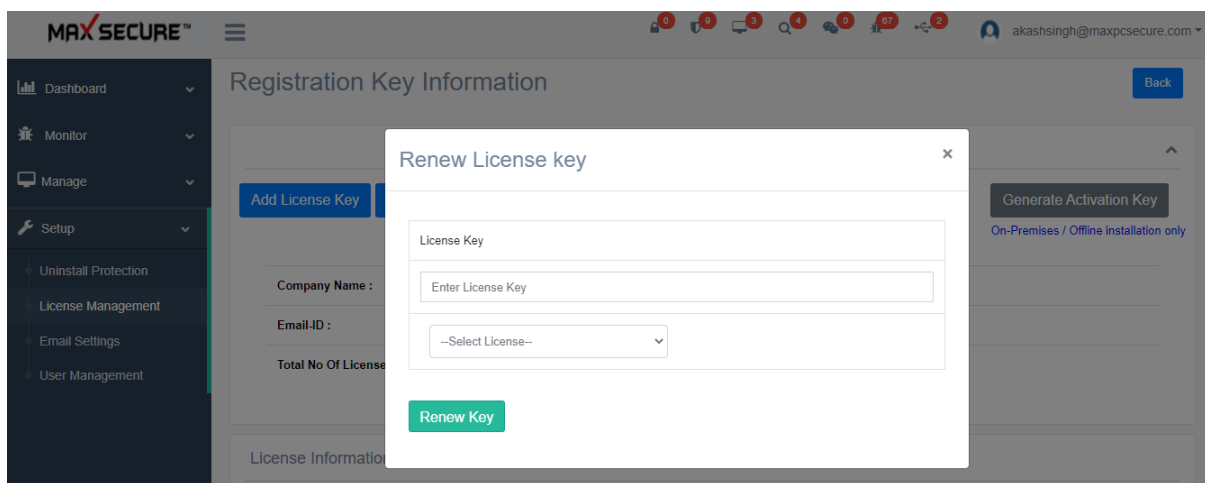
Enter License Key

Save

Renew License Key

Admin can renew registration key in case of increasing validation period (validity). Before or after expiration of Max Endpoint Security-Business portal admin can renew the subscription so as to remain protected client agents from critical Viruses and spyware. Hence a renew key is required to renew subscription of already registered client agents to remain protected. After obtaining renew key, copy the key and paste it on 'Enter License Key' box, select license key from Select License dropdown whose subscription you want to renew then click on 'Renew Key' button.

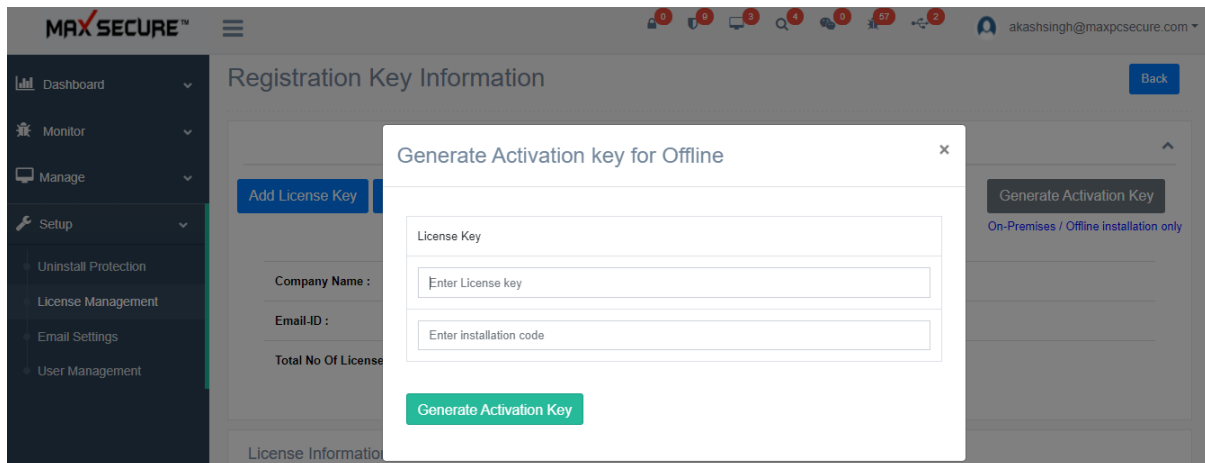
To-do this admin needs to go to portal *Setup*→ *License Management*→ click on 'Manage License' button→ click on 'Renew License Key' button.



Generate Activation Key

Generate Activation Key is used for on-premises/offline installation, this is applicable for Max Endpoint Security-Business Offline mode server installation. Here Admin needs to enter License Key which should be already registered in your respective online portal and then enter the installation code which we can get from the machine where we installed our Max Endpoint Security-Business server setup offline mode, then click on Generate Activation Key this will give you an activation key which will use during registration of Max Endpoint Security-Business server for offline/on-premises mode.

To-do this admin needs to go to portal *Setup*→ *License Management*→ click on 'Manage License' button→ click on 'Generate Activation Key' button.



Registration Key Information Details

Reg. Date: Registration Date shows the date as well time when admin successfully get registered with the respective key, showing time as per IST.

License Key: Displays the Registration Key of Max Secure Endpoint Security-Business.

Total Days: This field will show validation period of a key, for example: you purchased a key for 6 months then will show you 180 days on this field.

Remaining Days: This field will show how many days left to expire validation period of your registration key.

Users: This will show total number of users available in your registration key, it tell us how many client agents we can add.

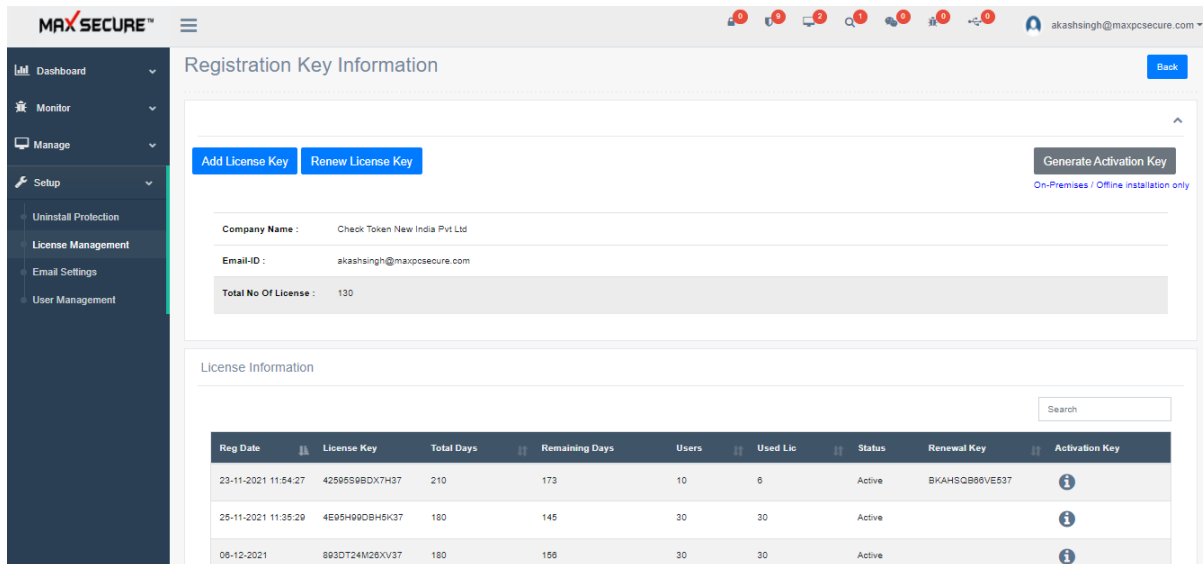
Used License: This field can show you total number of token (licenses) used in that respective key.

Status: This will you the current status of your registration key, it can either be shown active or expired, below is the explanation:

- **Active:** The registration key is valid, and the client agents registered from the token of this key is protected by Max Endpoint Security Business.
- **Expired:** The registration key subscription is expired, and the client agents registered from the token of this key is not protected by Max Endpoint Security-Business. If you want to extend our subscription call on our Customer Care Support.

Renewal Key: Displays key used for renewing license (increase subscription period)

Activation Key: Displays Activation key used in the registration process for Offline/On-Premises Max Endpoint Security- Business portal. It remains empty if used License Key is for Online Max Endpoint Security- Business portal.



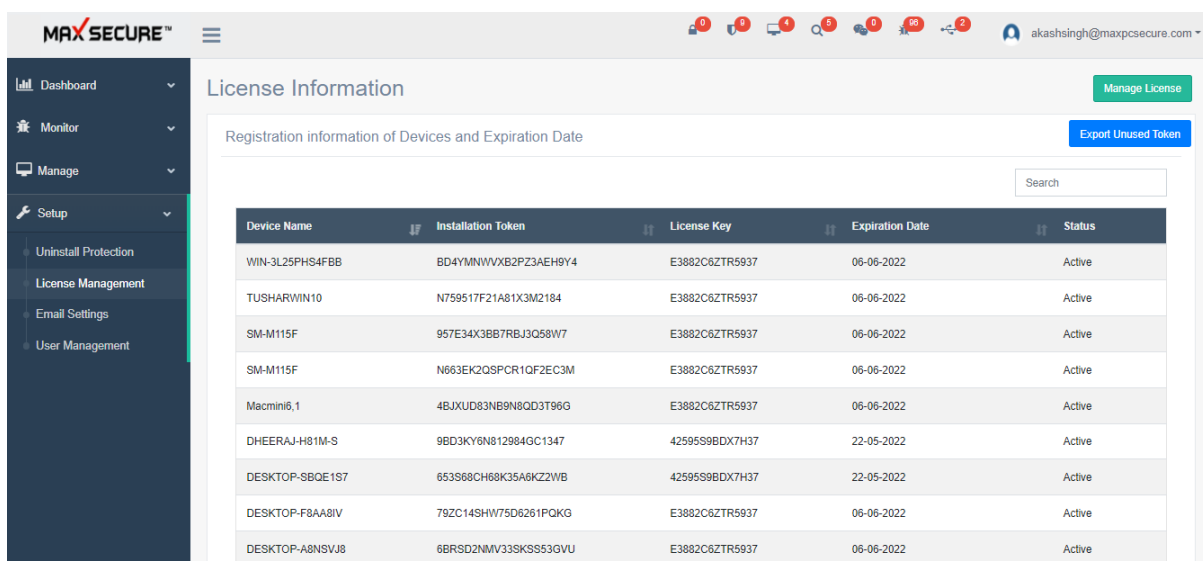
The screenshot shows the 'Registration Key Information' page in the Max Secure portal. The left sidebar contains navigation options: Dashboard, Monitor, Manage, Setup, Uninstall Protection, License Management, Email Settings, and User Management. The main content area has a 'Back' button and buttons for 'Add License Key', 'Renew License Key', and 'Generate Activation Key'. Below these are input fields for 'Company Name' (Check Token New India Pvt Ltd), 'Email-ID' (akashsingh@maxpcsecure.com), and 'Total No Of License' (130). A 'License Information' table is displayed below, showing details for three licenses.

Reg Date	License Key	Total Days	Remaining Days	Users	Used Lic	Status	Renewal Key	Activation Key
23-11-2021 11:54:27	4259559BDX7H37	210	173	10	6	Active	BKAH5QB86VE537	i
25-11-2021 11:35:29	4E95H99DBH5K37	180	145	30	30	Active		i
06-12-2021 12:41:06	693DT24M28XV37	180	156	30	30	Active		i

Client Agent Installation Token Information

When we subscribe to Max Endpoint Security-Business with the help of 'Registration Key', we know that we can protect N number of client agent and each Registration key has certain number of users and for registering any client agent we need 'Registration Token', so from here admin can get the information about each generated token whether it has been used by any client agent or it has been unused after generation.

To check this admin needs to go portal *Setup* → *License Management* →



The screenshot shows the 'License Information' page in the Max Secure portal. The left sidebar contains navigation options: Dashboard, Monitor, Manage, Setup, Uninstall Protection, License Management, Email Settings, and User Management. The main content area has a 'Manage License' button and an 'Export Unused Token' button. Below these is a 'Registration information of Devices and Expiration Date' table.

Device Name	Installation Token	License Key	Expiration Date	Status
WIN-3L25PHS4FBB	BD4YMNWVXB2PZ3AEH9Y4	E3882C6ZTR5937	06-06-2022	Active
TUSHARWIN10	N759517F21A81X3M2184	E3882C6ZTR5937	06-06-2022	Active
SM-M115F	957E34X3BB7RB3JQ58W7	E3882C6ZTR5937	06-06-2022	Active
SM-M115F	N663EK2QSPCR1QF2EC3M	E3882C6ZTR5937	06-06-2022	Active
Macmini6,1	4BJXUD83NB9N8OD3T96G	E3882C6ZTR5937	06-06-2022	Active
DHEERAJ-H81M-S	9BD3KY6N812984GC1347	4259559BDX7H37	22-05-2022	Active
DESKTOP-SBQE1S7	653S88CH68K35A8KZ2WB	4259559BDX7H37	22-05-2022	Active
DESKTOP-F8AA8IV	79ZC14SHW75D6261PQKG	E3882C6ZTR5937	06-06-2022	Active
DESKTOP-A8NSVJ8	6BRSD2NMV33KS953GVU	E3882C6ZTR5937	06-06-2022	Active

It displays following details about installation token:

Device Name: Displays the Client Agent's device name.

Installation Token: Displays generated installation token.

License Key: Displays registered License Key from which this token is generated.

Expiration Date: Displays the subscription expiry date.

Status: Displays the current validation status of token.

Export Used Token: This *button* is available on top right corner of the page which can be used to export all unused token available.

Email Settings

Email Settings will allow the admin to add its email address through which it will send mail to selected client agent, if you set this email address to default.

While adding email id following step should be followed:

1. **SMTP Server:** SMTP stands for Simple Mail Transfer Protocol, without an SMTP server, your email wouldn't make it to its destination. Once you hit "send," your email transforms into a string of code that is then sent to the SMTP server. The SMTP server is able to process that code and pass on the message. If the SMTP server wasn't there to process the message, it would be lost in translation. So here you need to enter **SMTP server** as shown in below *example*:

Common SMTP server providers & settings

SMTP Provider	URL	SMTP Server
Gmail	gmail.com	smtp.gmail.com
Yahoo	mail.yahoo.com	smtp.mail.yahoo.com
Outlook	mail.yahoo.com	smtp-mail.outlook.com

Now for example: If you are entering your Gmail id then enter '*smtp.gmail.com*' under SMTP Server textbox.

2. **SMTP Server Port:** Here we have to enter Outgoing Mail (SMTP) Server Port like for Gmail you need to enter port number 587.
3. **Email From:** Here enter sender email ID from which you need to send email through.
4. **SMTP Login ID:** Enter same ID which you entered in 'Email from' textbox that is sender's email id.
5. **SMTP Password:** Enter password of your entered email address.

6. Set as Default: This checkbox is to set email as default, so that in future we can mail Client Agent report's to them from given/provided email address.

Note: Click on 'Save' button after successful entering all fields.

After adding email addresses we can also edit the email details & can delete the email details. Similarly we can add multiple email ids but can set default email id to one address only.

Setup → Email Settings

MAXSECURE™ Email Settings

Set Email Settings

SMTP Server: Enter SMTP Server

SMTP Server Port: Enter Port

Email From: Email From

SMTP Login ID: SMTP Login ID

SMTP Password: Enter Password

Set As Default: ☐

Save

Server	Port	SMTP ID	Email From	Default	Date	Action
mail.ionos.com	587	miral@maxpcsecure.com	miral@maxpcsecure.com	1	02-12-2021 11:28:31	Edit Delete

Show 10 entries

Showing 1 to 1 of 1 entries

Previous 1 Next

User Management

Work together with User Management

With user management capabilities, one can login as an Admin and create new user roles such as Basic User, Sub-Admin and Admin as well based on the level of access you want them to have. With the help of multi-user access, user can easily manage & taken control over portal operations with their pre-defined access level and can help multiple teams to collaborate effectively.

Below operations are for Super Admin users

- Provide ability to view list of users under a company
- Provide ability to add new user with role (list of roles are fixed)

- Provide ability to edit user details
- Provide ability to update user role
- Provide ability to reset user password (email password in online mode and display on UI in offline mode)
- Provide ability to temporary disable user
- Provide ability to permanently delete user

Below operations are for all users

- Ability to change password
- Ability to login
- Ability to recover password using forgot password
- Ability to change security question

Below are related to implementation of role access matrix:

- Control the left menu items and navigations as per user roles matrix
- Control the UI buttons and actions as per user roles matrix

Role matrix

1. Admin user: Has all the rights as it is now
2. Sub-Admin: has all the rights except that he cannot create/delete users
3. Basic User: Can view things like policies etc. but not take actions/configuration etc.

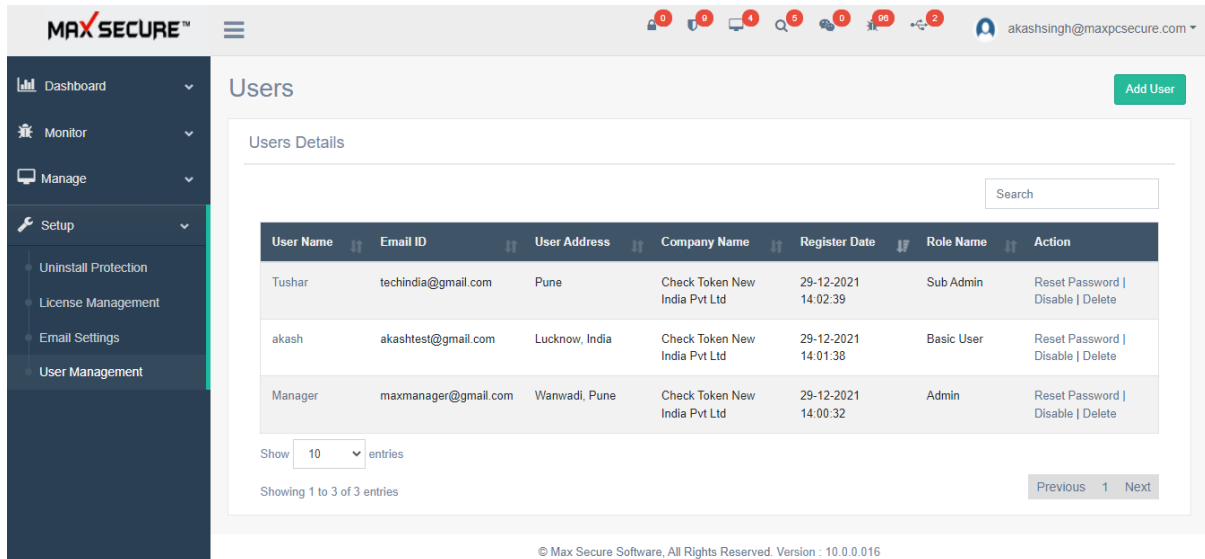
Following is for Windows. Same is true for Mac/Android/Linux:

Access Level	Permissions		
Features	Admin	Sub Admin	Basic User
Under Monitor tab			
1. Detections: Search /Export	Y	Y	Y
2. Alerts	Y	Y	Y
3. Reports	Y	Y	Y
Under Manage tab			

1. Endpoints:			
1.1 Searches	Y	Y	Y
1.2 Add Device	Y	Y	N
1.3 Action	Y	Y	N
2. Policy : Add Policy	Y	Y	N
3. Configurations: Add configuration	Y	Y	N
4. Tasks			
4.1 Content Filter			
4.1.1 Add Content Search Rule	Y	Y	N
4.1.2 Details	Y	Y	Y
4.2 Broadcast Message	Y	Y	Y
4.3 Share Files	Y	Y	Y
5. Groups	Y	Y	N
6. Data Loss Prevention			
6.1 Create content / File rule	Y	Y	N
6.2 Details	Y	Y	Y
7. Vulnerability Scan	Y	Y	Y
8. Full disk Encryption	Y	Y	N
9. Inventory Management	Y	Y	Y
Under Setup tab			
1. Uninstall Protection	Y	Y	N
2. License Information	Y	Y	View only and not Export information
11.1 License Management	Y	Y	View only , not click on any button to do any task

12. Email settings	Y	Y	View only not change /click on Save
--------------------	---	---	-------------------------------------

Setup → User Management

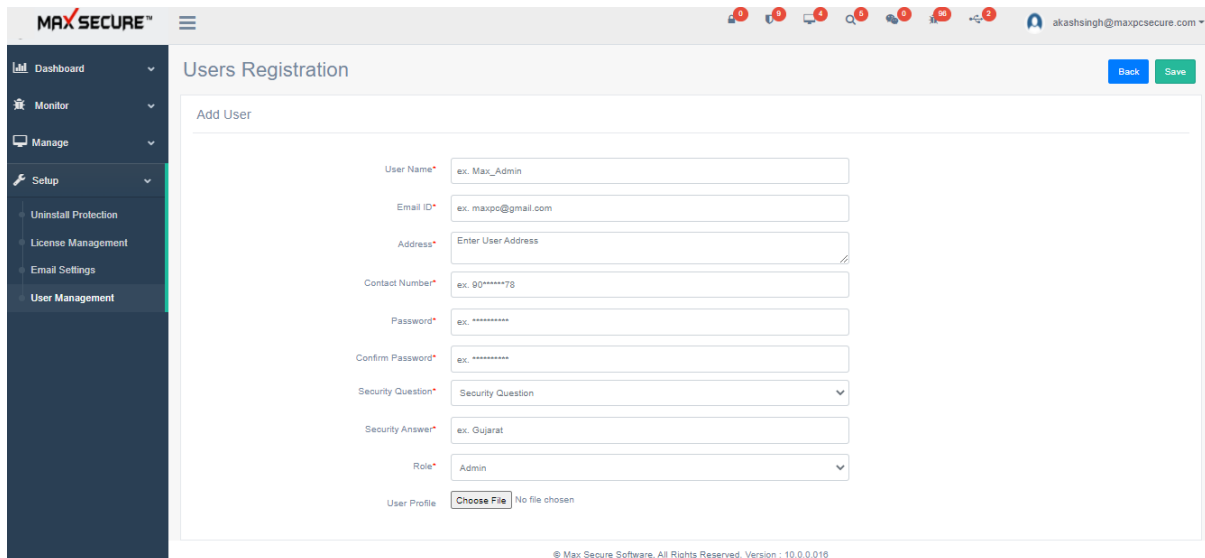


The screenshot shows the 'Users' management interface. On the left is a sidebar with navigation options: Dashboard, Monitor, Manage, Setup (expanded), Uninstall Protection, License Management, Email Settings, and User Management. The main content area is titled 'Users' and includes a search bar and a table of users.

User Name	Email ID	User Address	Company Name	Register Date	Role Name	Action
Tushar	techindia@gmail.com	Pune	Check Token New India Pvt Ltd	29-12-2021 14:02:39	Sub Admin	Reset Password Disable Delete
akash	akashtest@gmail.com	Lucknow, India	Check Token New India Pvt Ltd	29-12-2021 14:01:38	Basic User	Reset Password Disable Delete
Manager	maxmanager@gmail.com	Wanwadi, Pune	Check Token New India Pvt Ltd	29-12-2021 14:00:32	Admin	Reset Password Disable Delete

Below the table, there is a 'Show 10 entries' dropdown and a 'Showing 1 to 3 of 3 entries' indicator. Navigation buttons 'Previous', '1', and 'Next' are at the bottom right of the table area.

Setup → User Management → Add User



The screenshot shows the 'Users Registration' page with the 'Add User' form. The sidebar is the same as in the previous screenshot. The form contains the following fields:

- User Name*: ex. Max_Admin
- Email ID*: ex. maxpc@gmail.com
- Address*: Enter User Address
- Contact Number*: ex. 90*****78
- Password*: ex. *****
- Confirm Password*: ex. *****
- Security Question*: Security Question (dropdown)
- Security Answer*: ex. Gujarat
- Role*: Admin (dropdown)
- User Profile: Choose File (button) No file chosen

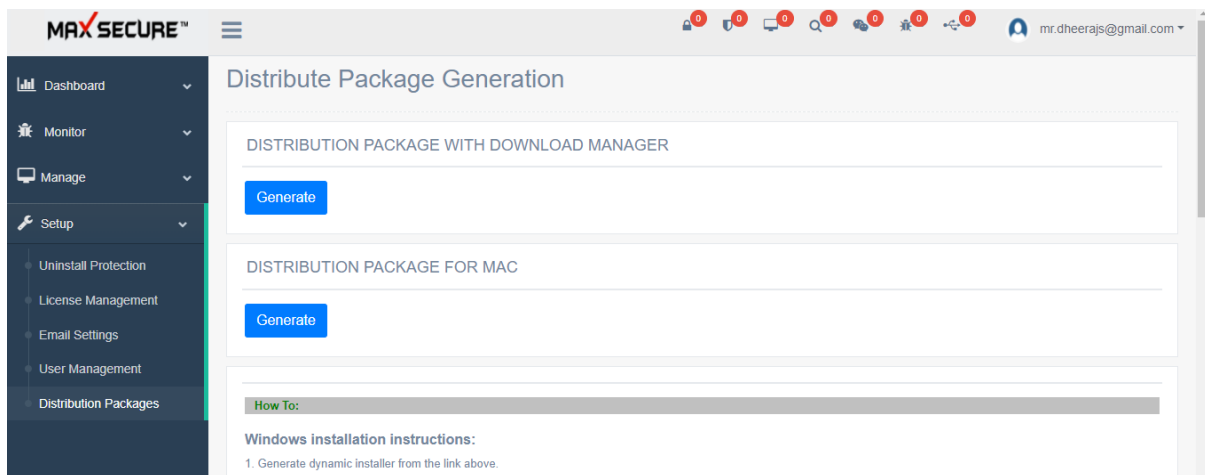
At the top right of the form area are 'Back' and 'Save' buttons. The footer indicates '© Max Secure Software, All Rights Reserved. Version : 10.0.0.016'.

Distribution Packages

Distribution Package Generation:

Dynamic package installer can be generated (for Windows and Mac Only), where you need not use any code to register and client devices will automatically connect to the dashboard right after the installation.

Get them from Setup → Distribution Packages → Distribution Package for Windows or Mac → Click on 'Generate' button then copy that link and hit on the browser.
For Windows devices choose Distribution Package with Download Manager.
For Mac devices choose Distribution Package for MAC.



Contact Us

If you wish to contact us...

Via email - contact us at tech@maxpcsecure.com

Visit our website at <https://maxpcsecure.com/CloudAV.htm>

And drop us an email at <https://www.maxpcsecure.com/contact.htm/>