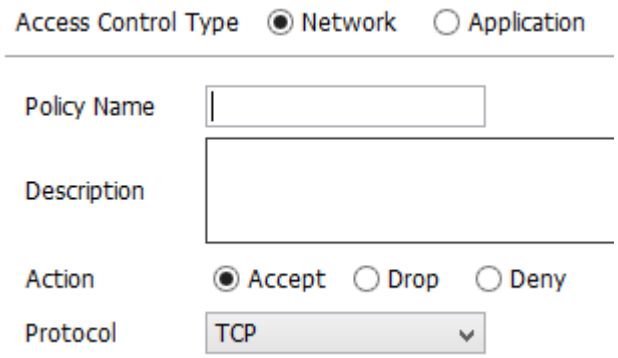
EVEREST NETWORK ACCESS CONTROL

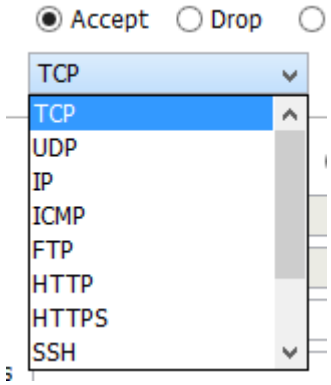
SOLUTION DOCUMENT

COMPLETE NETWORK ACCESS CONTROL SOLUTION PROVIDING END TO END SECURITY & GRANULAR ACCESS WITH EASE

ACCESS CONTROL POLICY



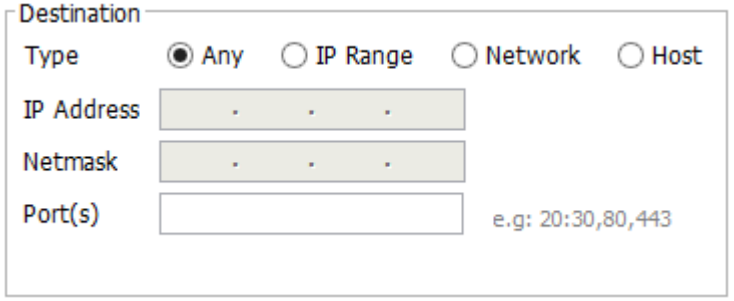
EVEREST NAC provides the functionality to create Network Access Control Policy and choose Accept, Drop or Deny Actions



EVEREST provides you the functionality to choose multiple Protocols to select Access, Drop or Deny Actions based upon your Network or Application requirements

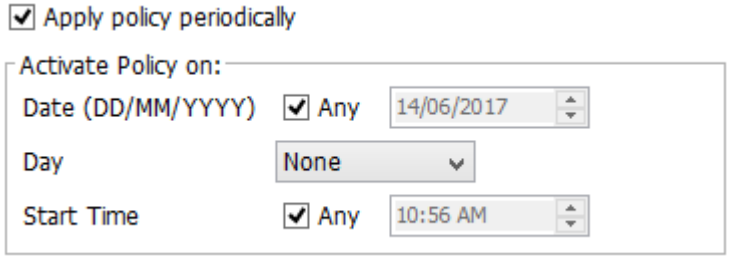
You can apply Access Control Policy based upon Source IP. Network, IP Range or Host IP along with request coming from Source Ports or MAC Address.

Similarly Granular Access Control Policy can be Applied on the basis of Destination IP. Network, IP Range or Host IP along with Destination Ports or MAC Address.

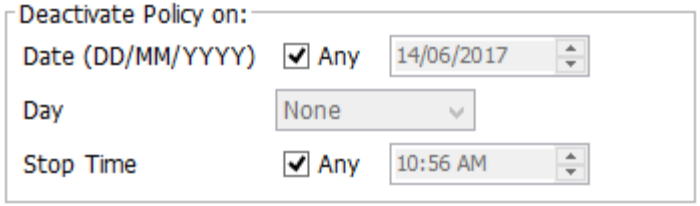


PROVIDING ADVANCED NETWORK ACCESS CONTROLS TILL APPLICATION LEVEL

POLICY ACTIVATION TIME

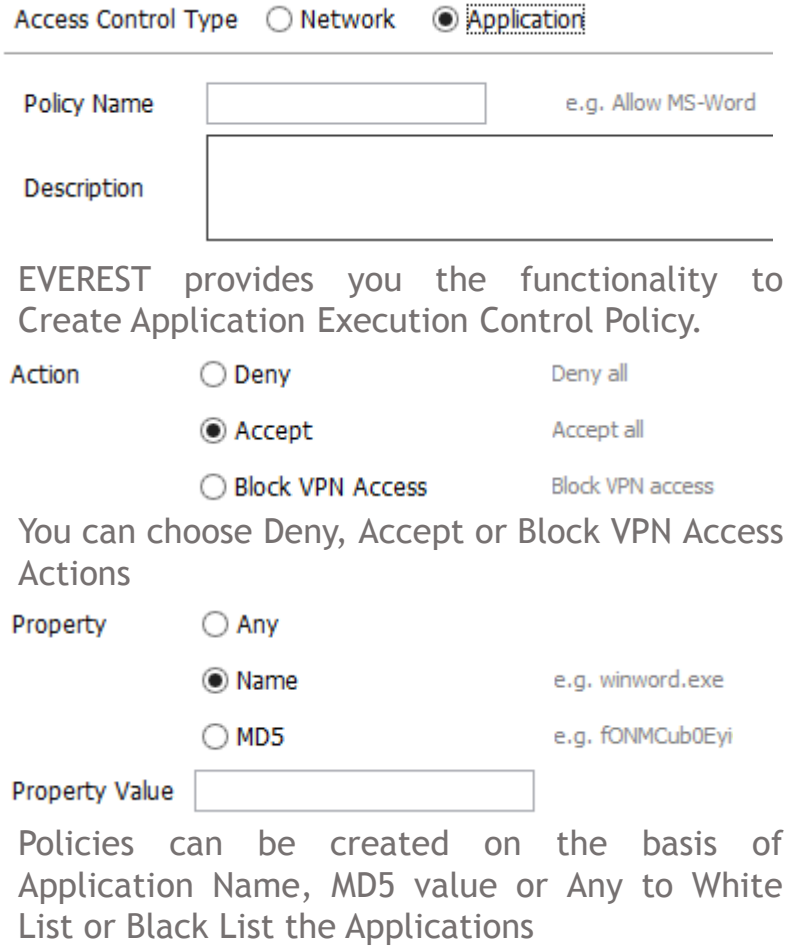


EVEREST provides you the functionality to define date and time to Activate Network Access Policy



Similarly you can define date and time to De-Activate this Network Access Policy, it will automatically De-Activate this Policy from the Date and Time defined. Also you can apply these policies Periodically from time to time

APPLICATION EXECUTION CONTROL



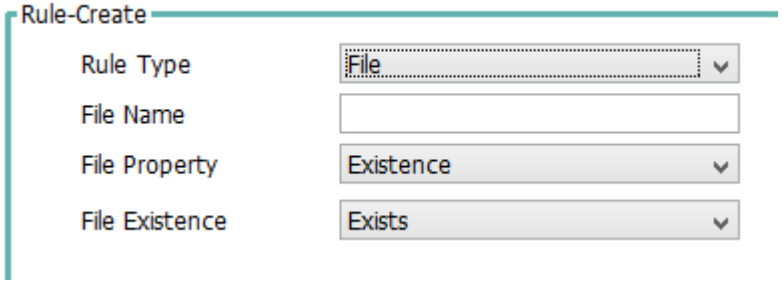
EVEREST provides you the functionality to Create Application Execution Control Policy.

You can choose Deny, Accept or Block VPN Access Actions

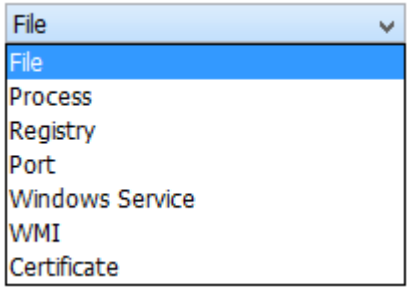
Policies can be created on the basis of Application Name, MD5 value or Any to White List or Black List the Applications

PROVIDING ADVANCED NETWORK ACCESS CONTROLS TILL APPLICATION LEVEL

HOST CHECKER POLICY

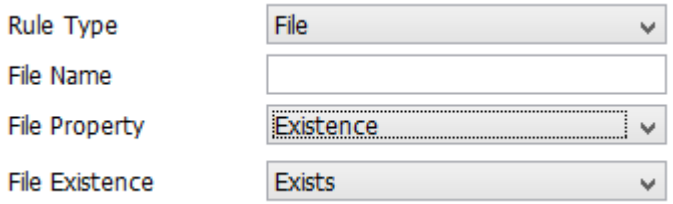


EVEREST provides you the functionality to Scan Incoming Remote User Machines to provide End to End Security & Secure Access. Scanning Rules can be created on the basis of various Parameters like File, Process, Registry, Port, Windows Service, WMI or Certificate

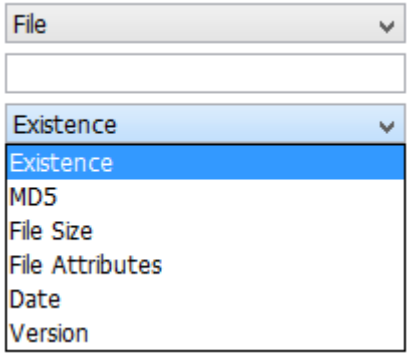


FILE BASED HOST CHECKER

You can create Host Checker Scanning Rule on the basis of File Name with following Property values.



You can choose File Property such as Existence, MD5, File Size, File Attributes, Date, Version



PROVIDING ADVANCED NETWORK ACCESS CONTROLS TILL APPLICATION LEVEL

PROCESS BASED HOST CHECKER

Rule Type	Process
Process Name	
Process Property	Existence
Process State	Running

You can create Host Checker Scanning Rule on the basis of Process Name with following Process State values.

Rule Type	Process
Process Name	
Process Property	Existence
Process State	Running

Running
Not Running

FILE BASED HOST CHECKER

You can create Host Checker Scanning Rule on the basis of Registry Entry Values with following Property values.

Rule Type	Registry
Registry Entry	
Registry Property	Existence
Registry Key Existence	Exists

You can choose Registry Property such as Existence and Check Key Data

Rule Type	Registry
Registry Entry	
Registry Property	Existence
Registry Key Existence	Exists

Exists
Does Not Exist

PROVIDING ADVANCED NETWORK ACCESS CONTROLS TILL APPLICATION LEVEL

WINDOWS SERVICE HOST CHECKER

Rule Type	Windows Service
Service Name	
Service Property	Current State
Service State	Running

You can create Host Checker Scanning Rule on the basis of Windows Service Name Name with following Service Property and Service State.

Rule Type	Windows Service
Service Name	
Service Property	Current State
Service State	Running

Running
Not Running

WMI BASED HOST CHECKER

You can create Host Checker Scanning Rule on the basis of WMI Attributes with following Property values.

Rule Type	WMI
WMI Namespace	SecurityCenter
	root/SecurityCenter
WMI Property	Check attribute value
WMI Class Name	Antivirus
	AntiVirusProduct

You can choose WMI Properties for Existance of Antivirus, Firewall etc.

Rule Type	WMI
WMI Namespace	SecurityCenter
	root/SecurityCenter
WMI Property	Existence of instance
WMI Class Name	Antivirus
	AntiVirusProduct
Instance Existence	Exists

Exists
Does not exist

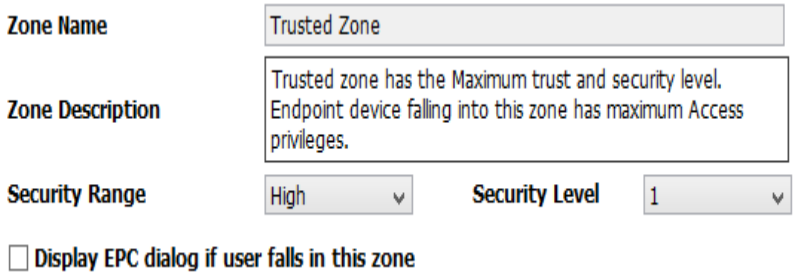
PROVIDING ADVANCED NETWORK ACCESS CONTROLS TILL APPLICATION LEVEL

ACCESS ZONES

EVEREST provides the functionality of Multiple Access Zones as per the result of End User Machine. Depending upon the Posture of End-User Machine, User is put under a particular Zone and Automatically Access Control Policy defined for that Zone is applied onto End-User machine.

Policy Name	Destination IP
Trusted Zone	1
Restricted Zone	3
Un-Trusted Zone	4
Semi-Trusted Zone	2
Quarantine Zone	40

Zones can be self created or Modified as per the Customer Requirements



DIGITAL CERT AUTHENTICATION

EVEREST also provides the functionality of Digital Certificate based Authentication apart to Local Database, AD, Radius and LDAP based Authentication Methods, which provides enhanced level of End to End Security

PROVIDING ADVANCED NETWORK SECURITY, WHAT OUR CUSTOMERS SAY ABOUT US

"We wanted most performing and robust secure remote access solution. We found EVEREST really fast when it comes to talk about our SAP application, EVEREST proves to be next generation product"

Arvind Chauhan - GM - IT, VE Commercial Vehicles Ltd.

"After evaluating all major SSL VPN Products for our SAP Access, we Chose EVEREST for its Innovative Technology, making SAP Access faster and Easy to use"

Naveen Verma - Sr. Manager IT, Daikin Airconditioning India Pvt. Ltd.

"EVEREST CAG Platforms are best suited for Telco Environments, We have not seen such a powerful product with best performance and unique combination of Virtual Environment, making our Cloud based SSL VPN Service more appealing"

J Narayanan - Product Lead, Reliance Communications Ltd.

"Increasing Internet threats on our SAP Server, forced us to look for Secure Access Solution, We got complete Security with EVEREST & additionally got WAN Accelerated Access which was a clear advantage over existing Products"

SK Ambashta - Head IT, Woodland Worldwide

Corporate and Sales Headquarters
EVEREST IMS Technologies Pvt. Ltd.
Office No 108, Bldg No 2, Sector 1
Millennium Business Park
Mahape, Navi Mumbai-400710
Phone: +91-22-41270170