



ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need — more than 90 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 180,000 companies around the world, including nine of every ten Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.



8 out of 10
biggest healthcare
companies

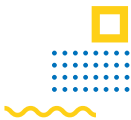


9 of every 10
Fortune 100
companies



8 out of 10
largest financial
services companies

trust ManageEngine to run their IT.



in partnership with



Phone: 1300 72 74 74

Email: manageengine@bluechip.com.au

ManageEngine
a division of Zoho Corp.

For more information:

www.manageengine.com.au

sales@manageengine.com



/bcitaustralia



/bluechip-infotech



/bluechip_it



/bluechip_it



Application Whitelisting

Desktop Central, Mobile Device Manager Plus

- Block applications; identify and auto-uninstall prohibited software
- Lock a device to a single application or multiple
- Block executables and script execution
- Deploy block rules on workstations and servers
- Allow or block apps on mobile devices running Android, iOS, or Windows

Patch Applications

Desktop Central

- Patch 300+ Microsoft, non-Microsoft, macOS, and Linux applications
- Update drivers and BIOS versions
- Detect, approve, download, test, install, and validate patches and service packs
- Schedule patch scans and deployment
- Achieve patch compliance using advanced analytics and audits
- Manage workstations and servers on a LAN or WAN

Configure MS Office Macro Settings

Browser Security Plus, DesktopCentral

- Manage MS Office settings out of the box
- Manage MS Office Macro settings through execution of custom scripts
- Control browser plug-ins, extensions, and allowed sites for Internet Explorer, Edge, Firefox, and Chromerunning Android, iOS, or Windows

Multi-factor Authentication

Password Manager Pro, AD360, Desktop Central

- Use one or more authentication techniques to verify users' identities during the password reset and account unlock process
- Use a secure password vault for privileged and personal accounts
- Enable authentication through AD/LDAP, PhoneFactor, email, RSA SecureID, etc.
- Remotely log in to a wide range of systems and network devices on a LAN or WAN, and record privileged sessions

Restrict Admin Privileges

Password Manager Pro, AD360, Desktop Central

- Manage privileged access to systems, applications, and network devices
- Exert granular control over users' access to resources and passwords
- Delegate role-based access to AD, Exchange, and O365
- Gain visibility into, and manage privileged permissions
- Set role-based access to computers and mobile devices running Android, iOS, or Windows

Daily Backups

Recovery Manager Plus,

Network Configuration Manager

- Perform comprehensive scheduled, incremental object and item-level backups in AD, Exchange, and O365
- Back up the entire database of application configurations, system settings, and password share permissions through scheduled tasks or live data backup
- Perform restart-free granular restoration
- Automate configuration backups from 200+ multi-vendor firewalls, routers, switches, etc.

Patch Operating Systems

Desktop Central, Network Configuration Manager

- Test and deploy OS patches for Windows, macOS, and Linux based on severity
- Validate the status of patch deployment
- Schedule patch scans, and identify the health status of devices
- Identify and manage firmware vulnerabilities
- Perform remote firmware upgrades and OS image transfers

User Application Hardening

Browser Security Plus

- Control browser plug-ins, extensions, and allowed sites
- Leverage browser lockdown, browser isolation, download restrictions, and data leak prevention tools
- Provide or restrict access to web applications

