

Privileged Identity Management for Data Centre Administrators in IT Companies



Are your most powerful users your weakest link?

In the traditional model of access control, anyone who knows the correct username / password combination is granted access by IT systems. This method of access control has always been assumed that if a person has not been provided with a valid username and password, he / she will not be able to access the systems.

Practically, the assumption above is generally found to be untrue. Users regularly share passwords; and administrators tend to share passwords even more frequently.

Thus, while organizations are aiming to provide secure single sign-on to applications for their end users, administrators in a Data Centre present a different kind of challenge – **the privileged ID management problem.**

Case in point – IT Company's Data Centre

Hosting business-critical and sensitive information, the data centre of an IT company is typically managed by a dedicated team of administrators working round-the-clock. The IT infrastructure typically comprises network elements, applications, and servers running diverse operating systems.

Managing access levels for these administrators is essential to ensure security and privacy of data. Ensuring this level of security as well as ease of use presents multiple business and technology challenges.

A typical IT company's data centre relates to the following:

- **Administrators sharing the password**

Within their team, administrators generally prefer ease of use. They end up using generic accounts and share their passwords. This trust based model, while seemingly eases operations, makes the data centre very insecure as it allows no individual level authorization and auditing.

As long as such a trust-based model is being followed, the organization can never be sure about the real access levels of individual members of the administrator team. Ultimately, the business has no way of placing accountability for actions on a specific administrator.

- **Administrator leaving the team/organization**

An IT Company's environment is characterized by high attrition and the above problem is compounded when there is attrition in the administrator team.

Since passwords are shared, when an administrator leaves the team, all passwords need to be changed to something new – a practice that gets rarely followed for its sheer inconvenience. Even if the outgoing administrator used his own user account on the servers, there is a risk of the password being shared to other team members. Locking or removing the privileged account on servers may not be immediately possible.

- **Administrator forgetting the password**

When administrators forget their passwords, the usual helpdesk is ineffective since helpdesks normally do not control administrative access on servers. Such a situation may impact ability of administrators to perform important or urgent tasks. This issue is more strongly felt in an IT company's environment working round the clock.

- **Ensuring that the right person is accessing the systems**

Can it be made sure that only the right person is accessing the servers? With a weak, single-factor password that can be shared, this is not possible. This method always has the risk of password being guessed or broken without the knowledge of the legitimate user.

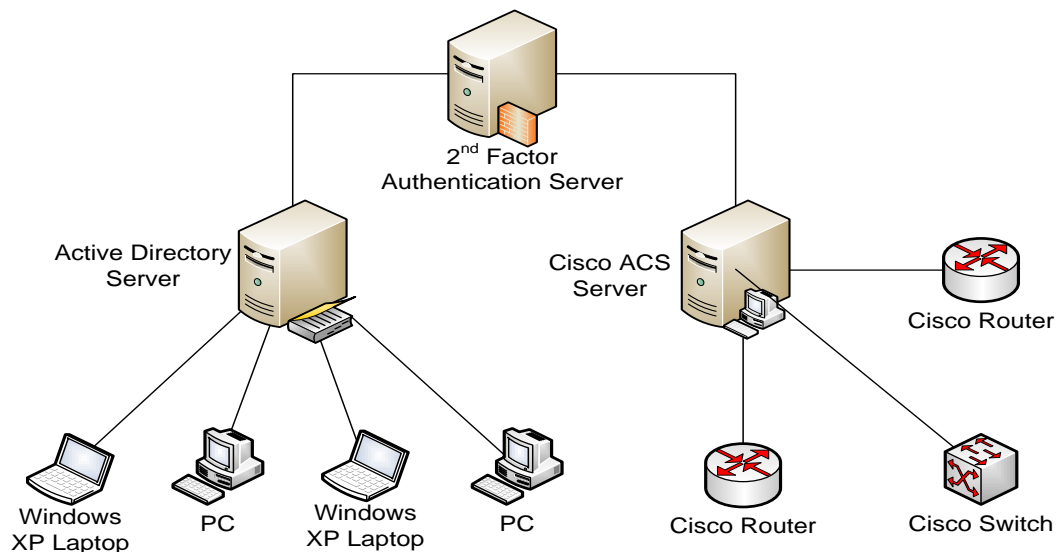


Security experts have long suggested that one of the biggest sources of IT threats comes from the very people charged with building and maintaining corporate computing systems



Solution – Strong Authentication system

- Aujas recommends a strong authentication model to address these business challenges.



Example solution layout integrated with existing MS Active Directory and Cisco ACS

- The strong authentication system plugs into existing systems like Microsoft AD or Cisco ACS. Integration with existing systems allows minimum change and leverages existing IT-security investments.
- The solution can connect to a large variety of applications and systems commonly found in a typical IT company's data centre. The solution can work with various operating systems, business applications, application and web servers, network elements, and even calling systems such as Avaya.
- The strong authentication system requires that when an administrator is accessing a protected system:
 - **Knows a secret (such as a password)**
 - **Possesses a device (say, a hardware token)**
- The administrators shall be able to successfully login only when they are able to provide both the password and token passcode. The token passcode randomly changes every minute, making it impossible to remember, guess, or share the passcode.

Aujas Approach

Aujas takes a step by step approach to design, select, deploy and manage the strong authentication solution in an IT company's Data Centre. During the entire cycle the objective remains to provide quick and incremental return while causing minimum impact on the existing processes.

Analysis of systems and applications in an IT company's data centre

Solution design using two factor authentication technology addressing specific business and technology needs

Assistance in product selection and planning for deployment.

Solution deployment and integration with existing systems

Handover and change management through easy to understand handholding sessions

Periodic performance management and support

Benefits

- Strong Authentication method to access the critical elements in IT infrastructure like servers and network elements.
- Reduced risk posture – ensures that only authorized personnel can access servers – helps the data centre in ensuring quick IT audits.
- Dashboard and detailed reporting for monitoring administrator access patterns – helps in regulatory compliance.
- Productivity gain and ease of use by providing the ability for administrators to manage their own passwords – useful for an IT company's environment where SLAs and TAT metrics are very important.
- Scalable platform for implementing mature identity and access management processes.



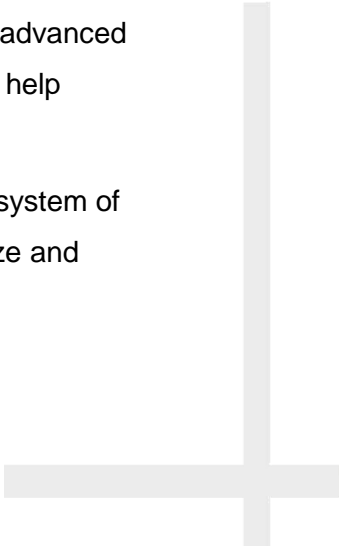
About Aujas

Aujas Networks Pvt. Ltd. (Aujas) is focused on **Information Risk Management Services**. We offer high-end Security consulting, professional and Management Services including IT GRC, Software and Application Security, Identity Management Vulnerability Management, Telecom Security and Training.

Aujas was founded by a core team of security professionals with decades of experience in Security. We are headquartered at **Bangalore**, India.

Our Vision is “To be the best-in-class, pure-play provider of advanced scalable eco-system of people, processes and technology to help customers minimize and mitigate Digital Security risk”.

Our Mission is “To create a differentiated and scalable eco-system of people, processes and technology to help customers minimize and mitigate Digital Security risk”.



Contact Us

For more information please write to contact@aujas.com

www.aujas.com

Bangalore | Mumbai | Delhi | Dubai

Corporate Office

Aujas Networks Pvt. Ltd.

No. 4025/26, 2nd and 3rd Floor

K.R. Road, Jayanagar 7th Block West

Bangalore – 560 082

Phone: +91 080-40528527

