

集成身份管理系统的七项工具 PDF转换可能丢失图片或格式
，建议阅读原文

https://www.100test.com/kao_ti2020/181/2021_2022__E9_9B_86_E6_88_90_E8_BA_AB_E4_c101_181884.htm 许多公司部署了点类型的身份管理产品，这类产品很难进行集成和定制，使复杂的局面更加复杂。而优秀的集成身份管理系统帮助企业降低风险和适应新的变化。通常优秀的集成身份管理系统具有以下七个特征。

基于角色的账户配置 用户账户配置包括以下内容：用户类型；使用的系统、应用和其他业务资源；使用企业资源的级别；创建、更新和删除用户账户。有效的用户配置可以减少包括弱口令在内的安全风险，基于角色的账户配置能够给企业提供集中管理用户身份的能力。管理用户身份员工、客户、供应商、合作伙伴等群体都会拥有独立的在线“身份”，企业可以根据使用者的角色进行管理。在企业内部，用户账户配置是由IT部门部署，并与人力资源应用系统进行集成。不同的用户角色具有预先定义的访问权。当某位员工承担某一特定角色时，这位员工访问企业资源的权限能够动态地根据IT部门预先设定的访问权限进行自动更新。在企业之外，一旦公司吸引了某位客户、供应商或合作伙伴，确保用户身份注册流程简单明了、平滑和安全，使用户相信自己的信息被安全、保密地保存，就变得至关重要。

目录基础设施 身份管理系统需要建立在强健的、可扩展的目录基础设施之上。目录基础设施使企业可以将员工信息分类保存在一个易于访问的分级式结构中。目录信息可以在分布式的环境中同步、复制和链接，跨地域地提供查找能力。

用户认证 检验用户身份的认证方法（如生物测定学、智能卡和数字

证书)是可信交易的基础,使企业能够在检验信息的同时,确保企业与用户之间建立信任通信。单点登录和安全访问单点登录技术可以简化对企业应用的访问流程,减少了记住多个口令的繁琐,提供管理多个系统的统一界面,有助于IT部门减少管理开销。基于Web的企业提供进入系统的不同接入点,使用户可以通过Internet、外联网和内联网进入系统,实现对不同企业资源的安全访问。自我注册和自我管理用户身份的自我注册和自我管理是通过将管理任务下放给最终用户,以减少IT开销和提高企业的生产力。例如,一位用户可以通过提交基于Web的表格,自行向一家企业注册(很少或没有人工干预),就可以立即执行安全的交易,这样可以大大减少系统管理员的工作压力。账户的移动性用户身份能够伴随用户移动而移动,与此同时,用户的访问水平不会因移动性而有所降低,这就要求身份管理基础设施必须具有足够的灵活性以适应这种移动性。此外,身份管理基础设施还必须具有开放性和可扩展性,以支持未来的Web服务以及与其他业务的集成。对企业来说,寻找一种具有以上七个特点并适应未来需要的身份管理系统,不仅将使身份管理更加有效,而且还有助于提高企业运营效率。100Test 下载频道开通,各类考试题目直接下载。详细请访问 www.100test.com