
# Active Directory Security Assessment

## Assess your Enterprise Directory Services environment security today

*An Active Directory Security Assessment helps an organization to identify, quantify and reduce the risks affecting the security of one of the most critical infrastructure components in most IT environments.*

### Key benefits

- **Domain Controllers Security**
  ADSA provides a detailed baseline of your environment with a comparative review based on official Microsoft recommendations. ADSA analyses security settings of your Domain Controllers based on the Microsoft security guidance found in the Security Compliance Manager (SCM) tool.
- **Administrative Memberships**
  ADSA provides a detailed inventory of administrative and privileged memberships.
- **Operational Excellence**
  Is a top priority for all organizations. ADSA will go beyond technology and look at process as well as governance.
- **Knowledge Transfer**
  Sessions will be provided.

## Overview

Active Directory provides mission-critical authentication, authorization and configuration capabilities to manage users, computers, servers and applications throughout an organization's IT infrastructure. As Active Directory provides broad and deep control of environments in which it is deployed, proper configuration and use of an Active Directory infrastructure is critical to secure an organization's systems and applications.

## Why Perform an ADSA?

As organizations' implementations of Active Directory evolve, configuration settings may not be properly maintained, security enhancements may not be implemented and vulnerabilities may begin to appear in an AD installation. An ADSA provides a holistic assessment of the security of an Active Directory installation, not only at a technical level but also at process and governance levels. On completion of an ADSA, the customer is presented with a comprehensive analysis of both technical and non-technical risks. In addition, it presents a prescriptive guidance and prioritization to provide an organization a roadmap to a more secure directory. ADSAs may be repeated on an annual or even a semi-annual basis in order to provide a comprehensive, audit-ready record of the security of an AD installation over its lifetime.

## How the Offering Works

ADSAs are performed via a series of activities on both technical and non-technical fronts. The technical component of the ADSA leverages automated information-gathering scripts, custom and standard system analysis tools to gather in-depth information about the configuration of the directory, privileged accounts, security settings, domain controller configurations and even inappropriate use of privileged accounts. In addition to the information gathering activities, interviews with key teams involved in the various aspects of Active Directory and supporting infrastructures, are performed to identify gaps in process or governance that may also expose the directory to risk.

*Significant cost savings can be realized by leveraging prioritized, actionable guidance to secure existing investments rather than increasing cost and complexity by adding additional security components that may be unnecessary in the presence of a secure AD implementation.*

### Risk Prioritization

An ADSA provides prioritized, structured remediation advice, allowing an organization to easily identify where efforts should be focused.

## Deliverables

The PFE-ADSA deliverables consists of three detailed reports containing information about an organization's domain controller's security configurations, privileged account and group memberships, and an operational and technical review. Risks are identified, prioritized, and remediation approaches are provided, giving the customer actionable guidance that can be used to harden and secure this mission-critical service. Supplemental files containing the full details of each risk are also provided as reference material that is useful to target remediation efforts.

## Higher Security for Systems and Applications

All computers and applications that are joined to or authenticate with Active Directory have critical security dependencies upon Active Directory. By implementing the guidance provided in the ADSA deliverables, the level of security across these complex dependencies is increased. Thus, the overall security status of an organization is significantly improved.

## Maximize Existing Investments in Active Directory

Rather than purchasing additional devices or software to increase security, simple changes to Active Directory and the systems it controls can provide greater incremental security improvements for reduced cost, risk and less effort from administrative staff.

## Engagement Sizing for Active Directory

The ADSA delivery* is sized appropriately to the complexity of your environment during a scoping call. Factors such as the number of domains, domain controllers and network topology are considered. These are examples of typical delivery times:

| Tier | Scoping | Typical Assessment Time | Delivered by |
|---|---|---|---|
| Tier 1 | Tier is determined by the number of domains, domain controllers, users and OS versions. | 5 days | PFE |
| Tier 2 | | 6 days | PFE |
| Tier 3 | | 7 days | PFE |
| Tier 4 | | Custom | PFE |
| Tier 5 | Custom | 20+ days | ACE |

*** Availability may vary by region and by tier level.**

Premier Field Engineering (PFE) is part of Microsoft Services Organization. PFE provides various offerings to Premier Enterprise customers to ensure that their solutions are in line with industry and Microsoft recommended practices.
The Assessment, Consulting and Engineering (ACE) Team is the assessment arm of Microsoft Information Security & Risk Management (ISRM). Tier 5 deliveries provide an in-depth assessment which focuses on additional processes, policies and reviews of the overall infrastructure architecture.

*For more information about Consulting and Support solutions from Microsoft, contact your Microsoft Services representative or visit **www.microsoft.com/services***

This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft | Services