

Deepnet Unified Authentication for Windows Network Logon

The use of strong authentication instead of traditional static passwords to access a Windows network is a necessary critical step to protect enterprise's most critical information assets and valuable data. Unfortunately, most existing strong authentication solutions require additional hardware devices such as smart cards, USB keys or One-Time Password (OTP) hardware tokens, which are expensive to implement, deploy, manage and very inconvenient to the users.

Achieving the right balance of authentication security, without compromising the user experience or the bottom line, has always been a challenging task for businesses.

Deepnet Unified Authentication for Windows Network Logon is a two-factor authentication solution designed specifically for Windows network, without the requirements of new hardware devices. Deepnet Unified Authentication utilizes the devices users already have (computers, mobile phones, PDA etc) or the user's behavioural biometrics (typing pattern, voiceprint), as the second factor. This eliminates the need to distribute new hardware, making the system cost effective, user friendly and simple to manage.

With the built-in RADIUS component and the support for Microsoft Active Directory, Deepnet Unified Authentication for Windows Network Logon can be easily integrated with the customers' existing IT infrastructures.



Log On to Windows

Microsoft
Windows^{XP}
Professional

Copyright © 1985-2001
Microsoft Corporation

Microsoft

Authentication by DEEPNET SECURITY

Authenticator: TypeSense

User name: john.smith

Password: ●●●●●●

OTP: 

Log on to: TESTDOMAIN

Log on using dial-up connection

EN

OK Cancel Shut Down... Options <<

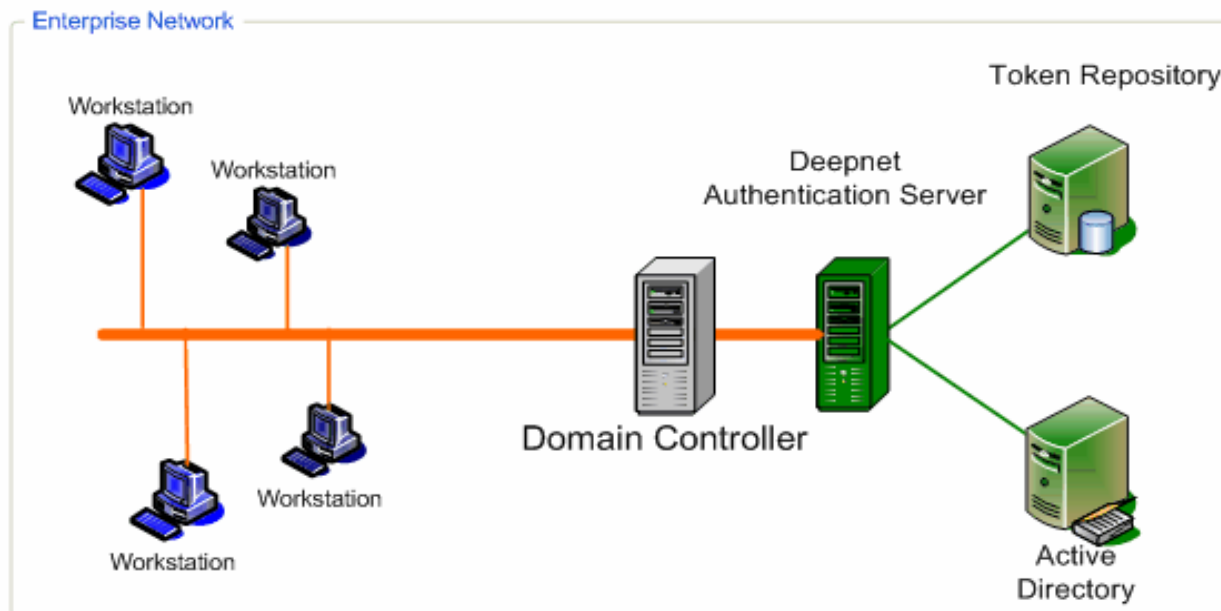
KEY BENEFITS

- Provides a user-friendly and cost-effective strong authentication solution.
- Eliminates password-only related vulnerabilities.
- Manages user account centrally through the Management Console.
- Improves productivity without compromising security.
- Offers flexible choices of authentication credentials and tokens.
- Unifies authentication for all enterprise applications with a single platform.

Technical Overview

Deepnet Unified Authentication for Windows Network Logon consists of the following major components:

- Windows Domain Controller
- Deepnet Authentication Server
- Token Repository server
- Active Directory server



Deepnet Authentication Server and its Token Repository (SQL Server) can be installed and operating on separated machines or on a single machine, depending on the scale of the customer's enterprise network.

Domain Controller

Deepnet Unified Authentication (Windows Logon) supports Microsoft Windows 2003, Windows XP and Windows 2000 servers.

Deepnet Authentication Server

Deepnet Authentication Server is a secure, scalable, cross-platform authentication server that centrally controls access to enterprise networks. Deepnet Authentication Server is designed to be deployable across a wide range of commonly available platforms that supports Java. Therefore, it can run on virtually any operating systems including Windows, Linux, Unix and Sun OS.

Token Repository

Deepnet Authentication Server uses a SQL database server as its token repository. It can be connected to the customer's existing SQL server (MS-SQL 2000/2003, Oracle) or MySQL server which is included in its installation package.

Active Directory

Deepnet Authentication Server supports assignment of tokens to users residing in Active Directory without modification of the directory schema. User data is not imported from the directory into Deepnet Authentication Server. Instead, Deepnet Authentication Server queries the directory during the authentication process to validate the user's status. Changes made in the directory are automatically and immediately reflected in Deepnet Authentication Server