PRODUCT LEAFLET

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

ENTERPRISE SINGLE SIGN ON MANAGER (E-SSOM)

WAAROM INVESTEREN IN EEN SSO-OPLOSSING?
HET INLOGGEN MET GEBRUIKERSNAAM EN WACHTWOORD IS EEN VEROUDERDE, INGEWIKKELDE EN TRAGE TOEGANGSMETHODE DIE BOVENAL GEBRUIKSONVRIENDELIJK IS. EINDGEBRUIKERS KUNNEN DE VELE GEBRUIKERSNAMEN EN WACHTWOORDEN LASTIG ONTHOUDEN. DAAROM HEBBEN ORGANISATIES DE LAATSTE JAREN STEEDS VAKER SINGLE SIGN ON (SSO)-OPLOSSINGEN GEÏMPLEMENTEERD.

De vraag naar SSO-oplossingen is ook toegenomen doordat organisaties de opzet van hun ICT-netwerk wijzigen. Applicaties worden steeds meer verplaatst naar de cloud, waardoor LDAP-achtige connecties niet meer werken, en netwerken worden gevirtualiseerd. Daarnaast moet wet- en regelgeving op het gebied van privacy strikter worden nageleefd. Single Sign On biedt organisaties een geavanceerde oplossing om te voldoen aan de laatste eisen van mobiliteit, beveiliging en eenvoud.

E-SSOM VAN TOOLS4EVER

Tools4evers Enterprise Single Sign On Manager (E-SSOM) is een onderdeel van de Tools4ever Identity Management Software suite. E-SSOM biedt out-of-the-box in één geïntegreerde oplossing onder meer Automated Login (SSO), Multi-factor Authenticatie, Virtual Desktop Integratie (VDI) en gecentraliseerde auditing.

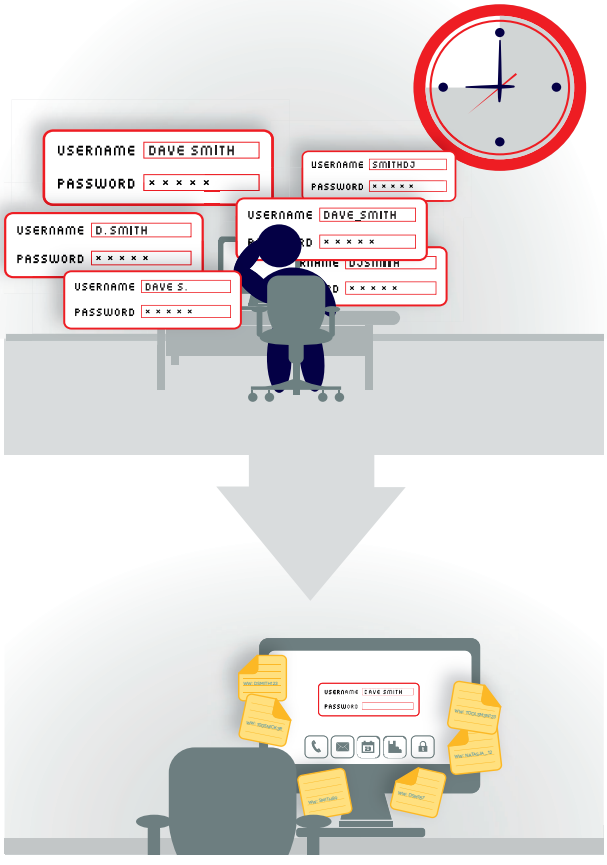
E-SSOM BIEDT HET VOLGENDE:

VOOR DE EINDGEBRUIKER

Eindgebruikers willen eenvoudige en snelle toegang tot hun applicaties. Doordat gebruikers een veelvoud aan gebruikersnamen en wachtwoorden moeten onthouden, vergeten zij regelmatig wachtwoorden en bellen de helpdesk. Ook schrijven zij wachtwoorden op, wat resulteert tot in een onveilige situatie.

Met E-SSOM hoeven gebruikers slechts één gebruikersnaam en wachtwoord te onthouden. Het is zelfs mogelijk om dit te vervangen en in te loggen met een pas en pincode. Iedere willekeurige pas kan hiervoor worden gebruikt, zoals fysieke toegangspas, de kantinepas en parkeerkaart.

One-Touch-Access
Bedrijven met een geavanceerd netwerk met ***Desktop Virtualisatie,*** bijvoorbeeld ziekenhuizen, kunnen profiteren van One-Touch-Access van E-SSOM. De eindgebruiker logt in door bijvoorbeeld een pas op de lezer te leggen of langs de lezer te halen. Binnen enkele seconden krijgt de gebruiker toegang tot de benodigde applicaties.



PRODUCT LEAFLET

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

VOOR DE AFDELING ICT

De afdeling ICT moet vaak tegengestelde eisen op het gebied van toegangsbeveiliging realiseren. Voorbeelden zijn:

- Veilige en tegelijkertijd ook gebruiksvriendelijke toegang;
- Auditgegevens opleveren zonder extra resources;
- Kostenreductie met behoudt van dezelfde graad van dienstverlening.

Veilige én gebruiksvriendelijke toegang is te realiseren door het toepassen van ***two-factor authenticatie***. Gebruikers loggen in met hun pas en een pincode en hebben met Single Sign On direct toegang tot applicaties. Dit is zeer gebruikersvriendelijk, zeker als dit gecombineerd wordt met ***Fast User Switching*** (snel tussen gebruikersaccounts wisselen) of ***Follow Me*** (een openstaande sessie meenemen naar een volgend werkstation) in een VDI omgeving.

Rapportage

Door het centraal vastleggen van de toegangsgegevens in de SQL database van E-SSOM is het mogelijk om elke gewenste rapportage te creëren zonder hiervoor handmatig alle onderliggende systemen te raadplegen.

Kostenbesparing

Dertig procent van de helpdesk calls betreffen vergeten wachtwoorden. Doordat eindgebruikers met E-SSOM nog maar één wachtwoord en gebruikersnaam hoeven te onthouden, is de kans minder groot dat zij wachtwoorden vergeten.

VOOR TOEZICHTHOUDERS (SOX, NEN, HIPAA)

Steeds meer bedrijven worden geconfronteerd met wet- en regelgeving met betrekking tot beveiliging van de toegang tot het netwerk. De naleving ervan wordt steeds strenger gecontroleerd. Eisen concentreren zich vaak tot sterke authenticatie en auditing.

Sterke authenticatie

Wet- en regelgeving eist dat het netwerk en de applicaties worden beveiligd met een sterk wachtwoord. Denk hierbij aan een wachtwoord met minimaal 8 tekens, minimaal een hoofdletter en 2 vreemde tekens dat iedere 90 dagen gewijzigd moet worden.

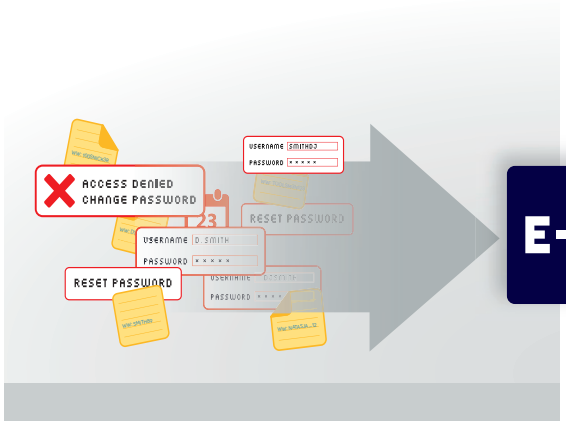
De implementatie van ***sterke wachtwoorden*** heeft consequenties voor het gebruiksgemak. Het alternatief voor sterke wachtwoorden is ***two-factor authenticatie***, oftewel inloggen met een pasje en een pincode. Toezichthouders zien two-factor authenticatie als afdoende en zeer veilig.

Auditing

E-SSOM fungeert als centraal toegangspunt en bepaalt wie toegang krijgt tot welke applicatie(s). Daarnaast slaat E-SSOM alle toegangsacties van de eindgebruikers op.

Op deze manier is het eenvoudig om te rapporteren over wie wanneer toegang heeft gehad tot welke applicatie.

VEEL WACHTWOORDEN EN GEBRUIKERSNAMEN



ONE-TOUCH-ACCESS