



Česká zemědělská univerzita v Praze
**Provozně ekonomická
fakulta**

Diplomová práce
**Zlepšování služeb pro koncové uživatele
pomocí nástroje Identity manager**

Autor: Bc. Martin Toman

Vedoucí práce: Ing. Jiří Vaněk, Ph.D.

Cíl práce

- Návrh implementace nástroje Identity Manager
 - usnadnění práce s identitami
 - zvýšení uživatelského komfortu
- Dílčí cíle:
 - přehled řešené problematiky
 - analýza současného stavu
 - návrh strategie řešení
 - testování, zhodnocení
 - předběžné vyčíslení nákladů
 - uvedení závěrů a doporučení



Metodika

- Teoretická část
 - Přehled řešené problematiky
 - Důraz na Identity Management
 - Porovnání dostupných nástrojů
- Praktická část
 - Analýza servisních požadavků a nastavení účtů
 - Tvorba virtuálního testovacího prostředí
 - Implementace vybraných nástrojů a nastavení funkcí
 - Testování a doporučení dalšího postupu
 - Finanční analýza



Teorie

- Entita
 - Jedinečný objekt schopen samostatné existence
 - Lze rozeznat od ostatních entit
- Identita
 - Shoda charakteristických vlastností v čase a prostoru
 - Totožnost, lze ji ověřit
- Řízení identit (Identity Management)
 - Zajišťuje důvěrnost, integritu a dostupnost informací
 - Každý zaměstnanec má správné přístupy ve správný čas



Představení firmy

- **LINET spol. s r.o.**
- Výroba nemocničních a pečovatelských lůžek
- 15 dceřiných společností
- Prodej ve více než 100 zemích světa
- 1500 uživatelů



IT

- 1 doména
- OS Windows
- HW Dell
- MS SCCM

- 1st level support – 7 lidí
- 2nd level support – 5 lidí
- 3rd level support – 1 člověk



Zjištěné problémy

- Uživatelská hesla s neomezenou platností
 - Chybí funkce pro samoobslužný reset hesla
- Prodleva mezi nástupem zaměstnance a vytvořením účtu
- Odchod zaměstnance / Změna Pozice
 - IT oddělení není informováno



Uživatelská hesla s neomezenou platností

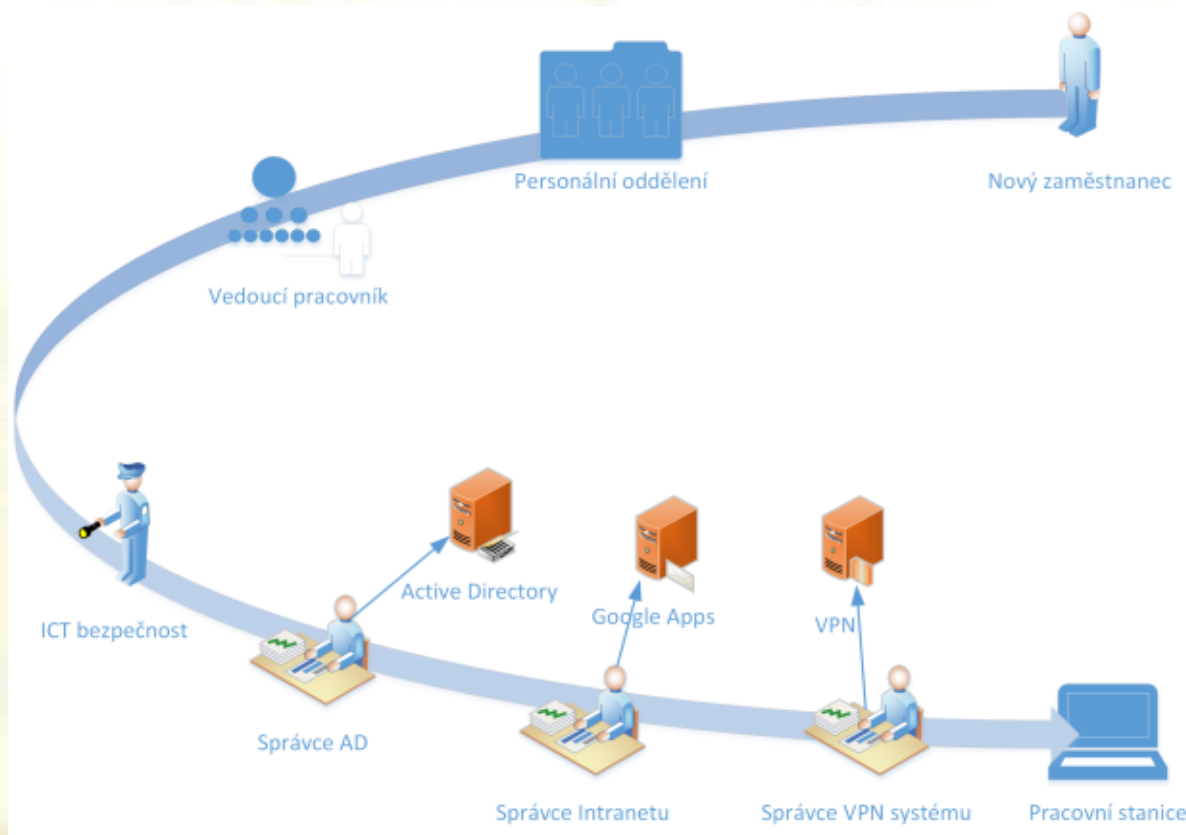
Samoobslužný reset hesla:

- Azure AD
 - Cloud Self-help password reset
 - Vícefaktorové ověření
- Microsoft Identity Manager
 - On-premise Self-help password reset



Nástup zaměstnance – metodický přístup

Problém: Prodleva mezi nástupem zaměstnance a vytvořením účtu

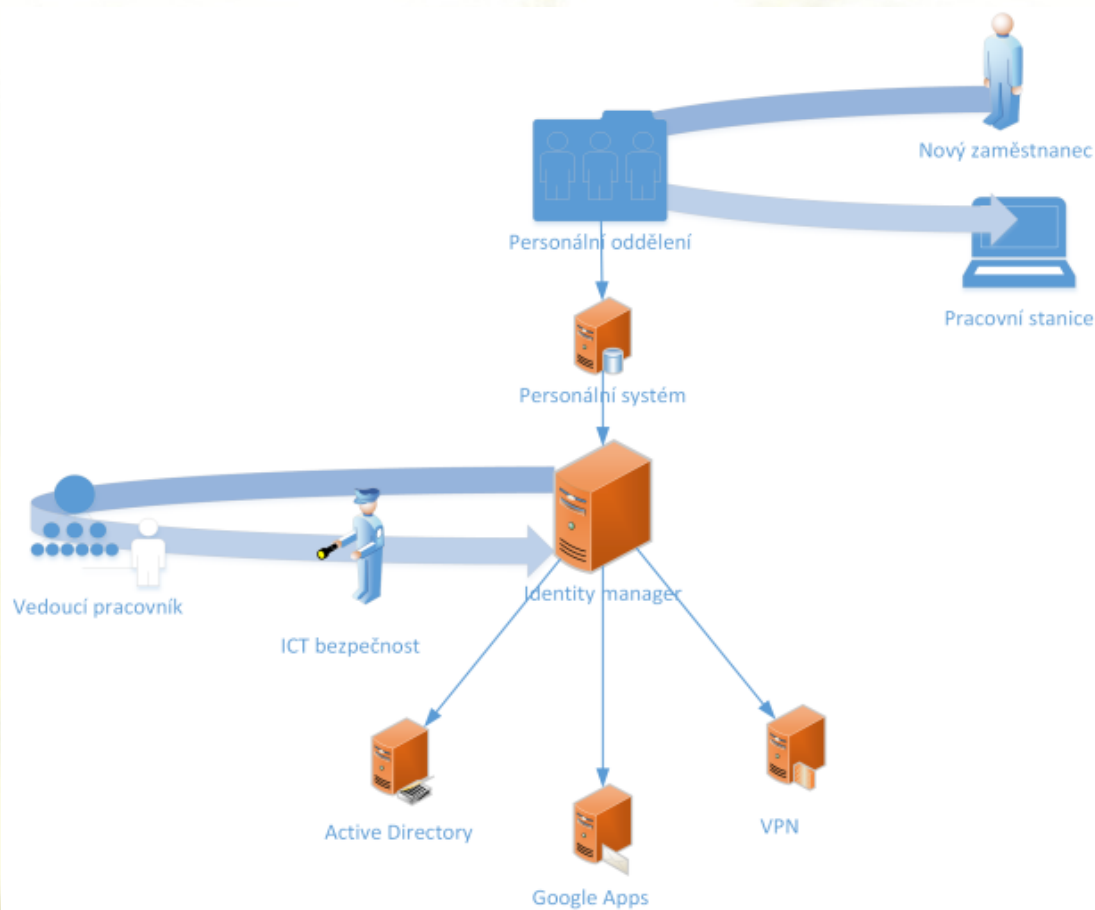


Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Nástup zaměstnance – technický přístup

Řešení: Automatizace procesů - Identity Manager

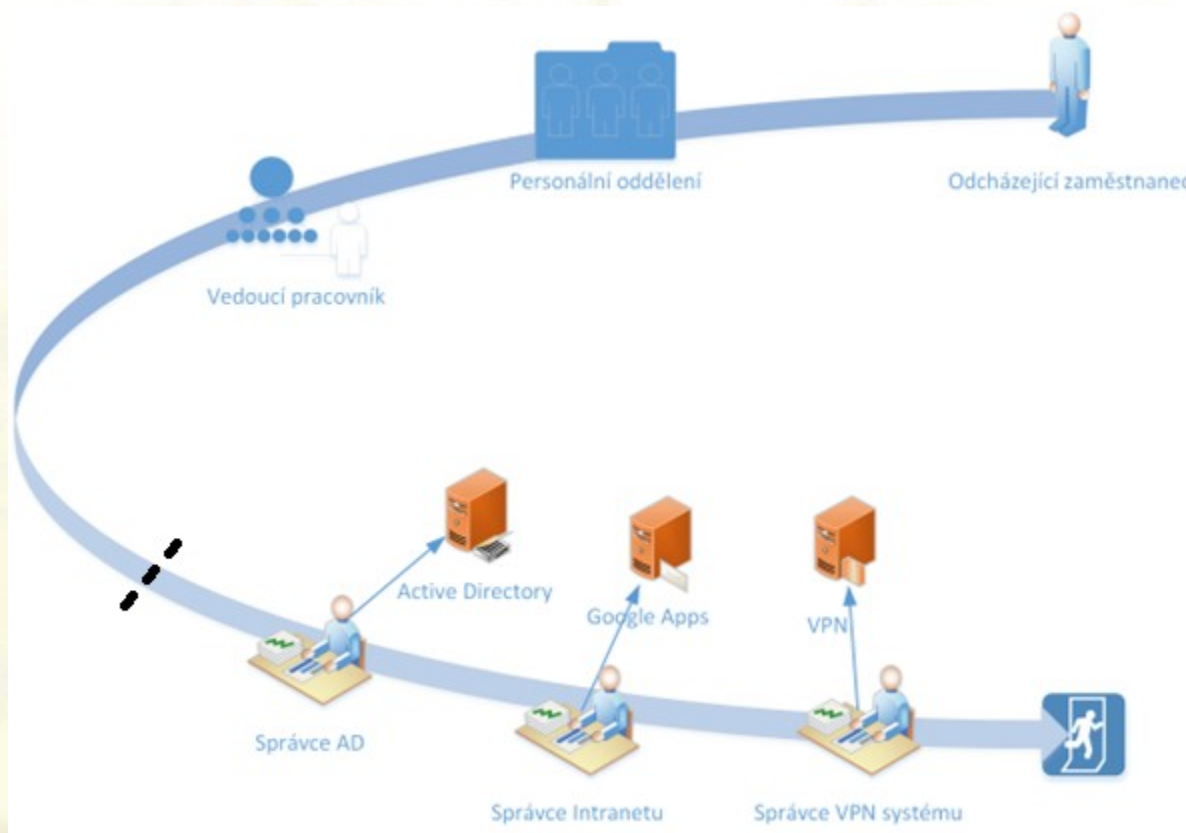


Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Odchod zaměstnance – metodický přístup

Problém: IT oddělení není informováno

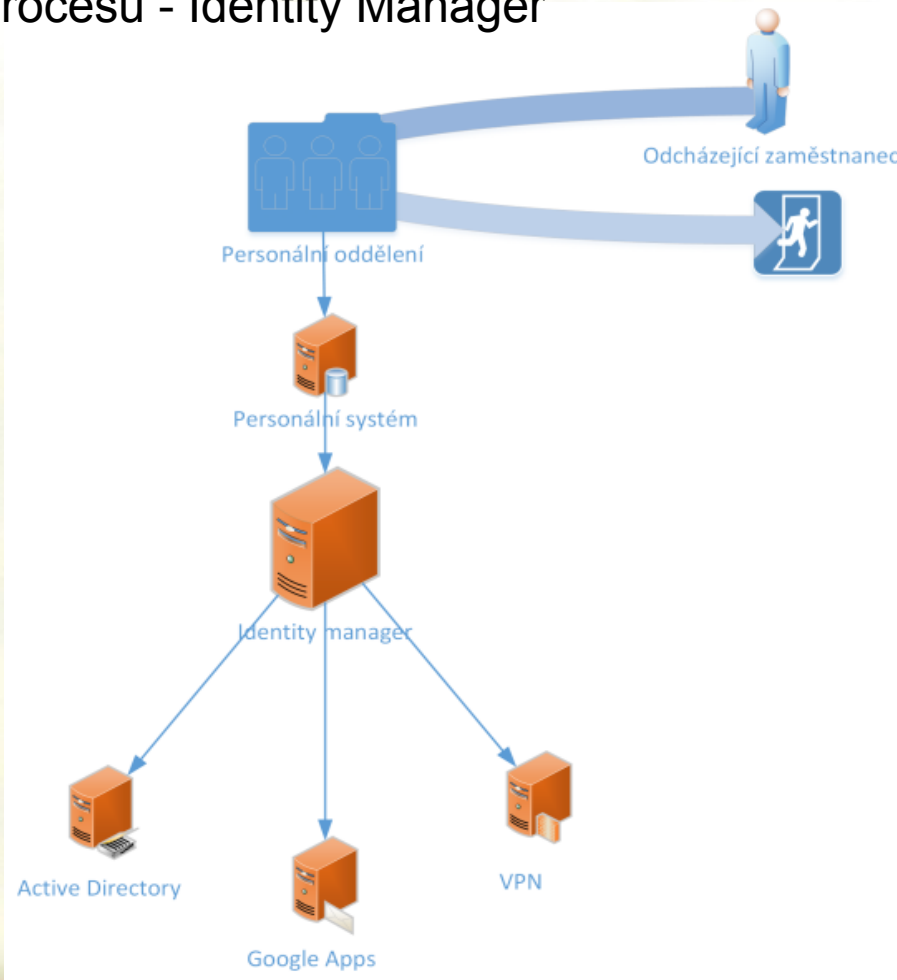


Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Odchod zaměstnance – technický přístup

Řešení: Automatizace procesů - Identity Manager



Testování – samoobslužný reset hesla v Azure

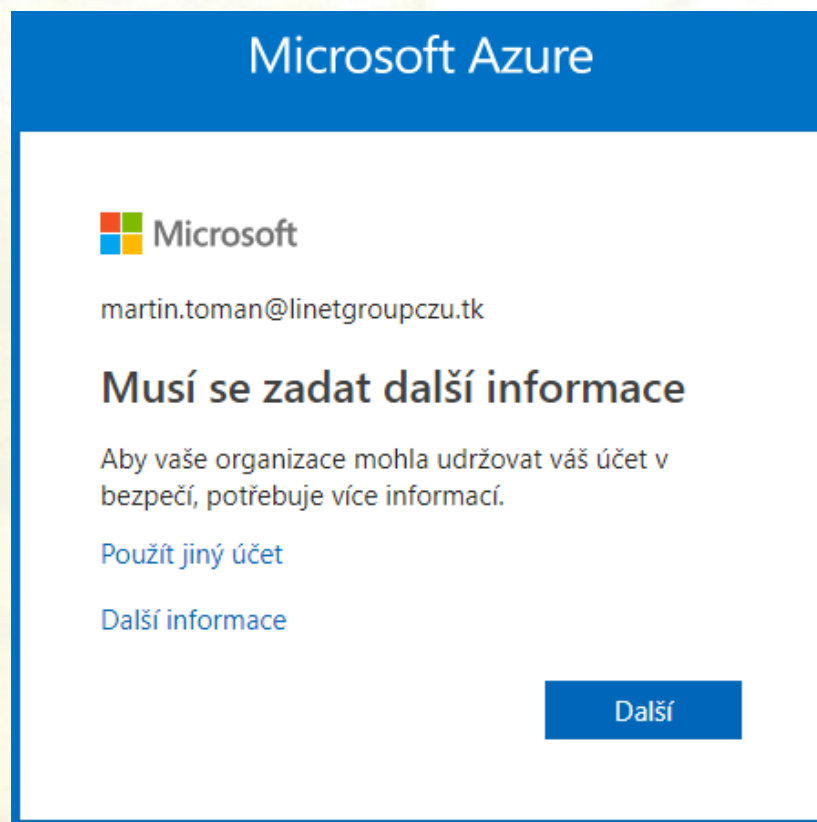


Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Testování – samoobslužný reset hesla v Azure

Portál Azure vyzve k doplnění kontrolních informací po přihlášení



The screenshot shows a Microsoft Azure login page. At the top, it says "Microsoft Azure". Below that is the Microsoft logo and the email address "martin.toman@linetgroupczu.tk". The main heading is "Musí se zadat další informace" (Additional information must be entered). Below this, it explains: "Aby vaše organizace mohla udržovat váš účet v bezpečí, potřebuje více informací." (To help your organization keep your account secure, we need more information). There are two links: "Použít jiný účet" (Use a different account) and "Další informace" (More information). A blue button labeled "Další" (Next) is at the bottom right.



Testování – samoobslužný reset hesla v Azure

Neztraťte přístup ke svému účtu!

Vyberte dole otázky, na které chcete odpovědět. **Správce vyžaduje, abyste nastavili tento počet otázek: 3, a odpovědi musí být nejméně 3 znaků dlouhé.**

Bezpečnostní otázka 1

Otázka1 ▾

Odpověď'1 

Bezpečnostní otázka 2

Otázka2 ▾

Odpověď'2 

Bezpečnostní otázka 3

Otázka3 ▾

Odpověď'3 

uložit odpovědi



Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Testování – samoobslužný reset hesla v Azure

Neztraťte přístup ke svému účtu!

Děkujeme vám! Niže uvedené informace použijeme k obnovení vašeho účtu, pokud byste zapomněli heslo. Kliknutím na tlačítko Dokončit zavřete tuto stránku.

- ✓ Telefon pro ověření - je nastaveno na: +420 [redacted] 09. [Změnit](#)
- ! E-mail pro ověření - není konfigurováno. [Nastavit nyní](#)
- ✓ Je nakonfigurovaný tento počet bezpečnostních otázek: 3. [Změnit](#)

dokončit

zrušit




Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Testování – samoobslužný reset hesla v Azure

Microsoft Azure



Microsoft

← martin.toman@linetgroupczu.tk

Zadat heslo

Heslo

[Nepamatuji si svoje heslo](#)

Přihlásit se



Testování – samoobslužný reset hesla v Azure

Přihlaste se znovu do účtu

ověřovací krok 1 > zvolit nové heslo

Zvolte způsob kontaktování, který bychom měli použít pro ověření:

Poslat mi SMS na mobil

Zvolat mi na mobilní telefon

Odpověď na mé bezpečnostní otázky

Pokud chcete chránit svůj účet, je třeba, abyste níže zadali své celé mobilní telefonní číslo (*****09). Následně vám zašleme textovou zprávu s ověřovacím kódem, který můžete použít k resetování hesla.

09

SMS



Testování – samoobslužný reset hesla v Azure

Přihlaste se znovu do účtu

ověřovací krok 1 ✓ > **zvolit nové heslo**

* Zadejte nové heslo:

* Potvrzení nového hesla:

Dokončit

Zrušit



Testování – samoobslužný reset hesla v Azure

- Výhody
 - Více možností ověření
 - Změna hesla i mimo firmu
- Nevýhody
 - Nutné využít další zařízení pro přístup na internet

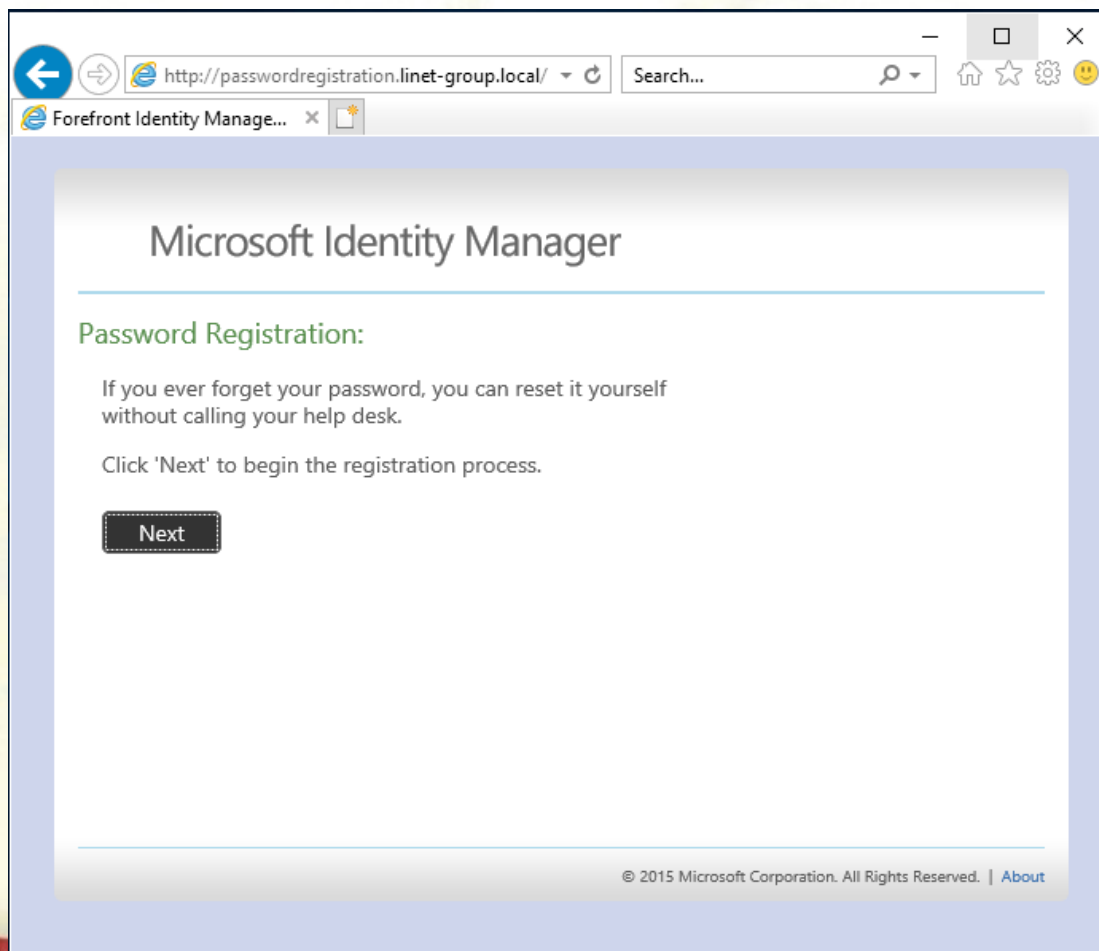


Testování – samoobslužný reset hesla v MIM

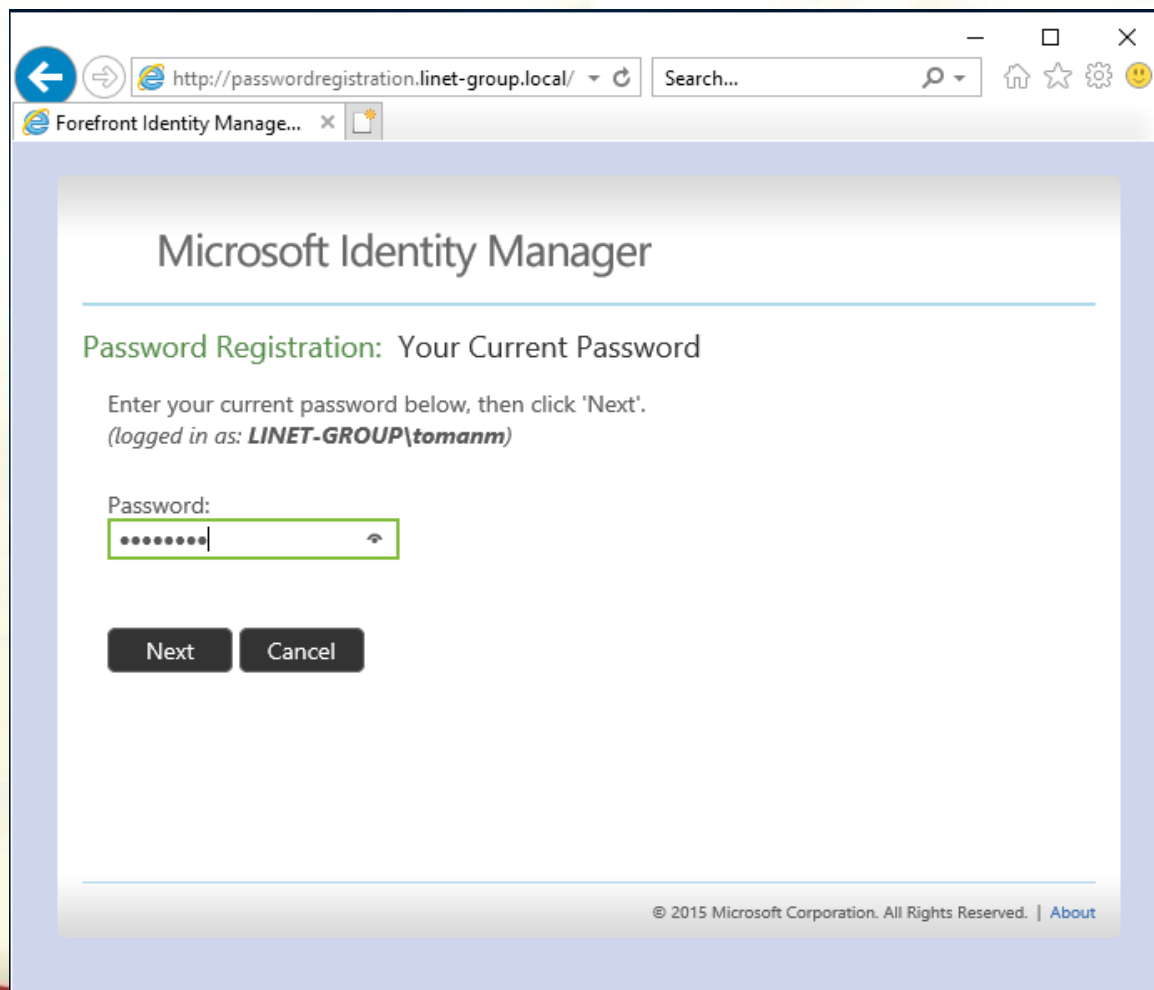


Testování – samoobslužný reset hesla v MIM

Registrace se automaticky otevře po přihlášení do PC



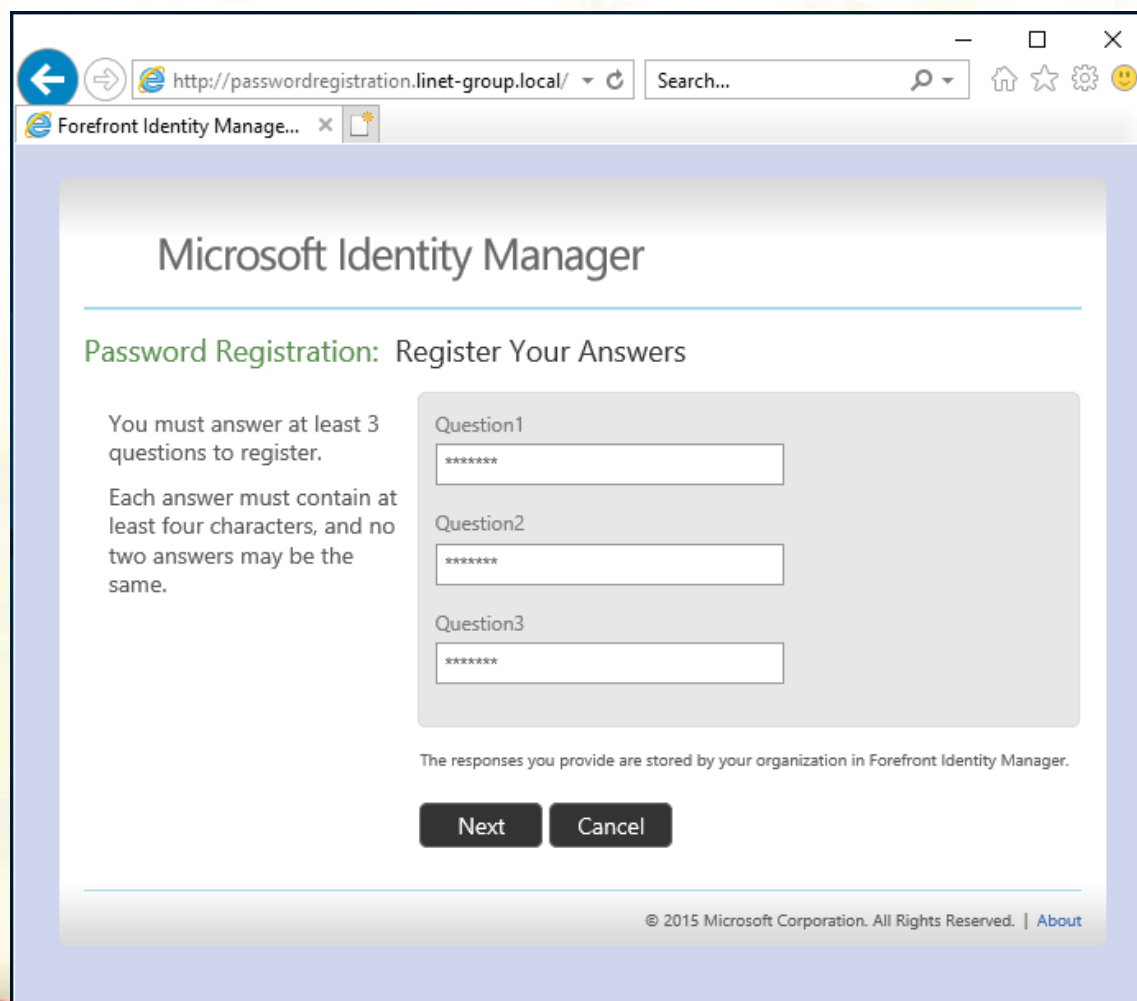
Testování – samoobslužný reset hesla v MIM



The screenshot shows a web browser window with the address bar containing `http://passwordregistration.linnet-group.local/`. The page title is "Microsoft Identity Manager". The main heading is "Password Registration: Your Current Password". Below this, there is a prompt: "Enter your current password below, then click 'Next'. (logged in as: LINET-GROUP\tomannm)". A password input field is shown with a green border and a green outline, containing seven dots. Below the input field are two buttons: "Next" and "Cancel". At the bottom right of the page, there is a copyright notice: "© 2015 Microsoft Corporation. All Rights Reserved. | [About](#)".



Testování – samoobslužný reset hesla v MIM



The screenshot shows a web browser window with the address bar displaying `http://passwordregistration.linnet-group.local/`. The page title is "Forefront Identity Manage...". The main content area is titled "Microsoft Identity Manager" and "Password Registration: Register Your Answers".

You must answer at least 3 questions to register.

Each answer must contain at least four characters, and no two answers may be the same.

Question1

Question2

Question3

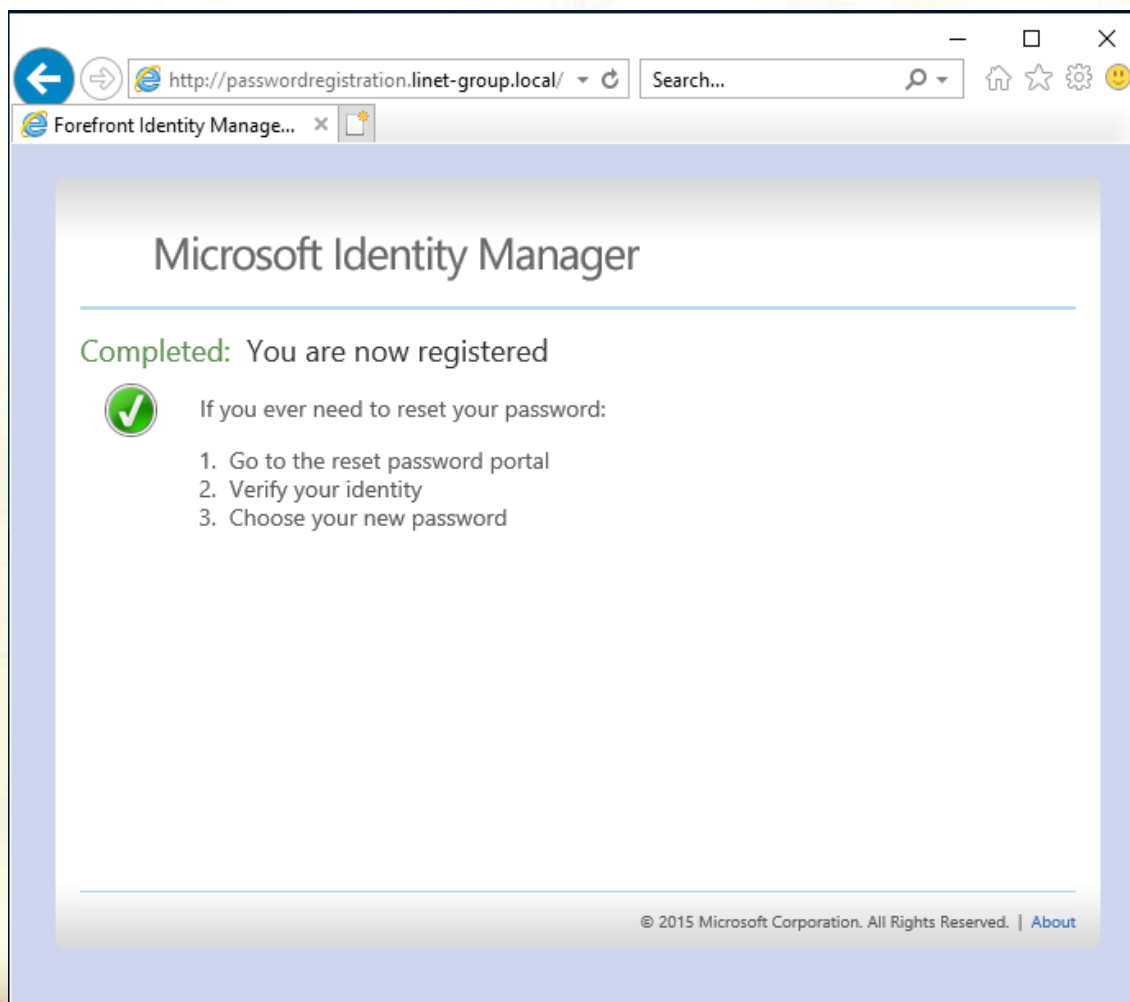
The responses you provide are stored by your organization in Forefront Identity Manager.

Next Cancel

© 2015 Microsoft Corporation. All Rights Reserved. | [About](#)



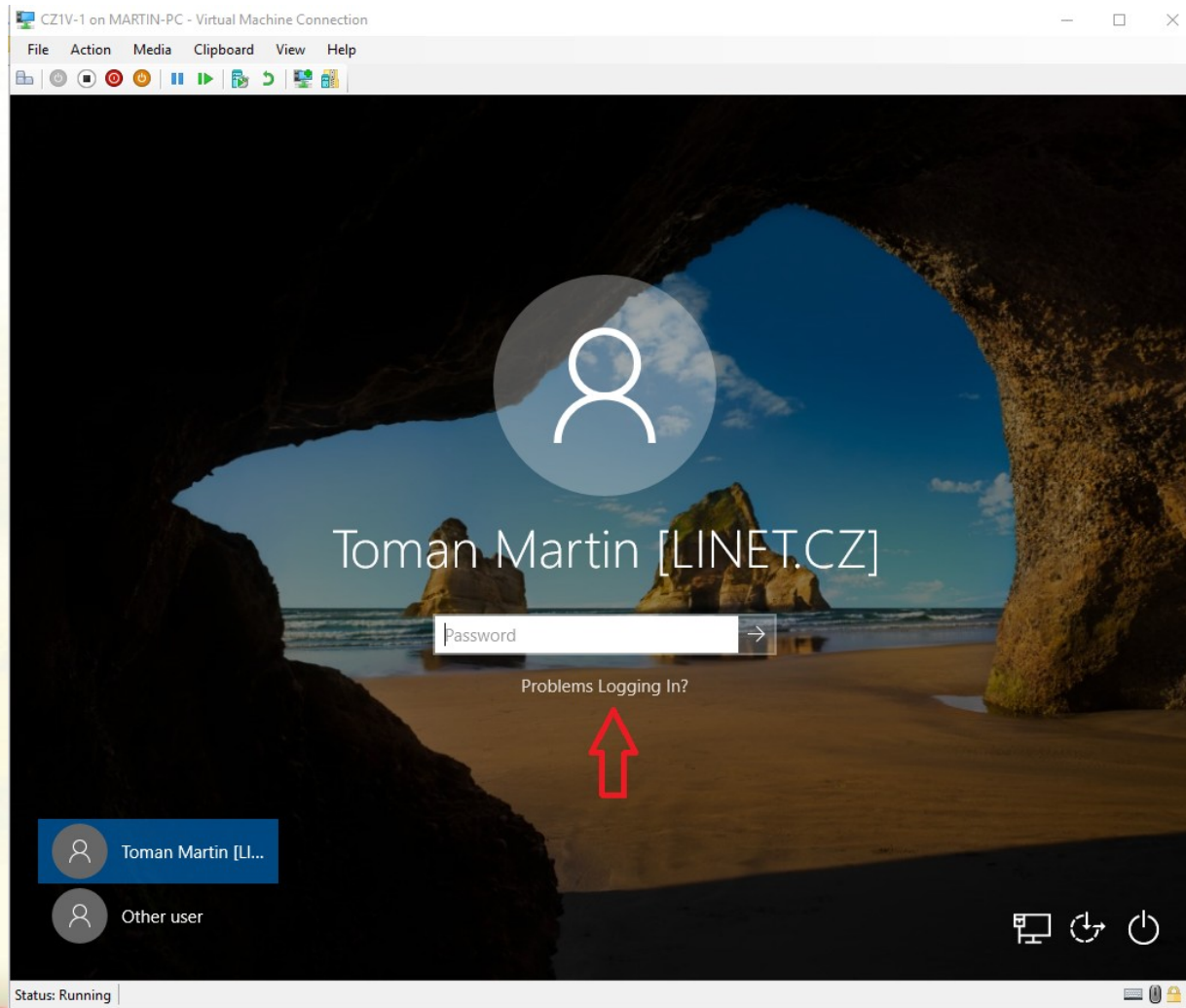
Testování – samoobslužný reset hesla v MIM



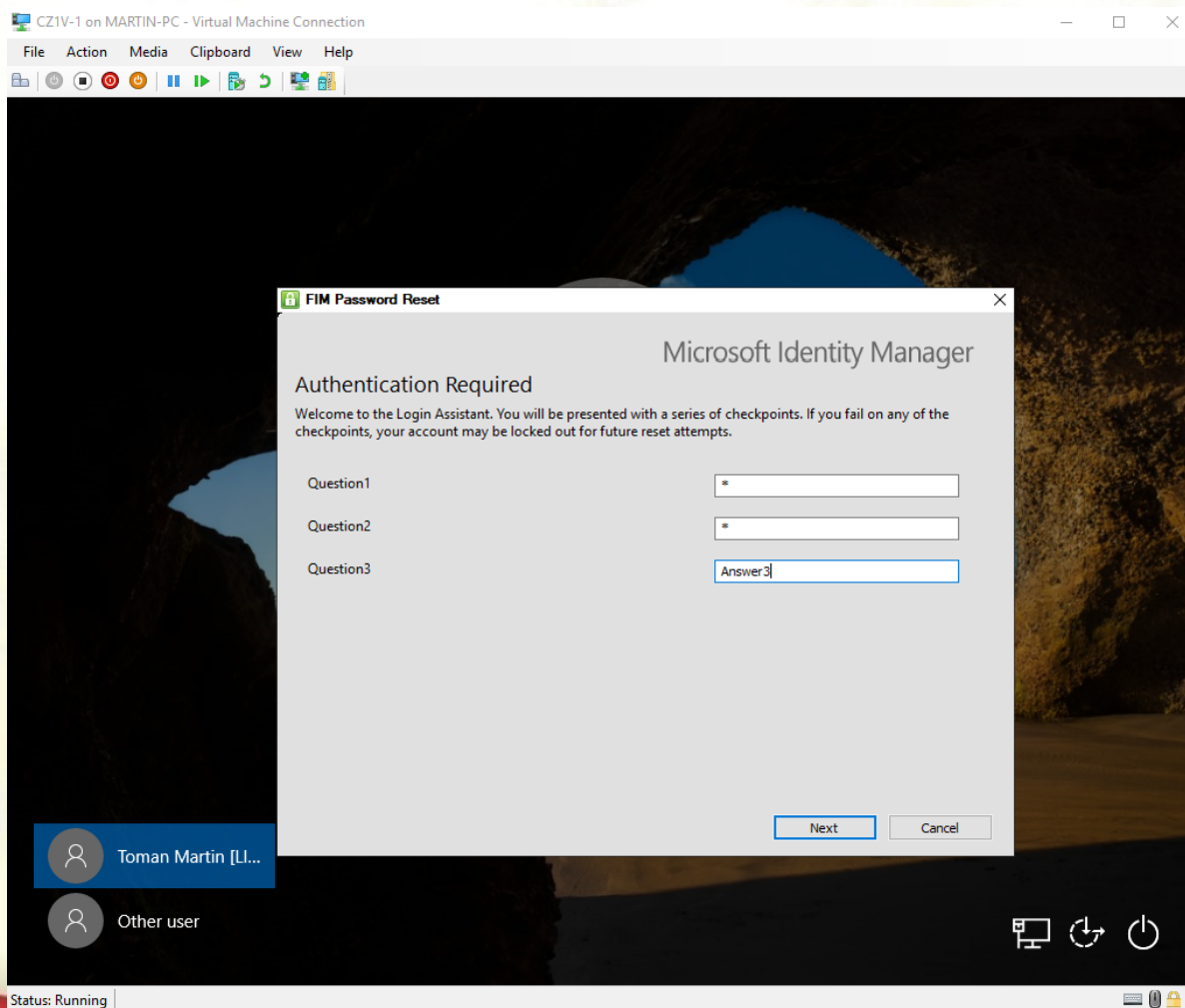
The screenshot shows a web browser window with the address bar containing the URL `http://passwordregistration.linnet-group.local/`. The page title is "Forefront Identity Manage...". The main content area displays the "Microsoft Identity Manager" logo and a confirmation message: "Completed: You are now registered". Below this, a green checkmark icon is followed by the text "If you ever need to reset your password:" and a numbered list of steps: 1. Go to the reset password portal, 2. Verify your identity, and 3. Choose your new password. At the bottom right of the page, there is a copyright notice: "© 2015 Microsoft Corporation. All Rights Reserved. | [About](#)".



Testování – samoobslužný reset hesla v MIM



Testování – samoobslužný reset hesla v MIM



Testování – samoobslužný reset hesla v MIM

FIM Password Reset

Microsoft Identity Manager

You have been authenticated successfully.

Welcome to the Login Assistant. You will be presented with a series of checkpoints. If you fail on any of the checkpoints, your account may be locked out for future reset attempts.

Keep your current password and unlock your account

Enter a new password and unlock your account

Domain\Username:


New password:

Confirm new password:

Note: The user name above may display in a different format than you are accustomed to logging in with. An example of another logon format is tomanm@linetgroupczu.tk.



Testování – samoobslužný reset hesla v MIM

 FIM Password Reset

Microsoft Identity Manager

You have been authenticated successfully.

Welcome to the Login Assistant. You will be presented with a series of checkpoints. If you fail on any of the checkpoints, your account may be locked out for future reset attempts.

Keep your current password and unlock your account


Enter a new password and unlock your account

Domain\Username:

New password:

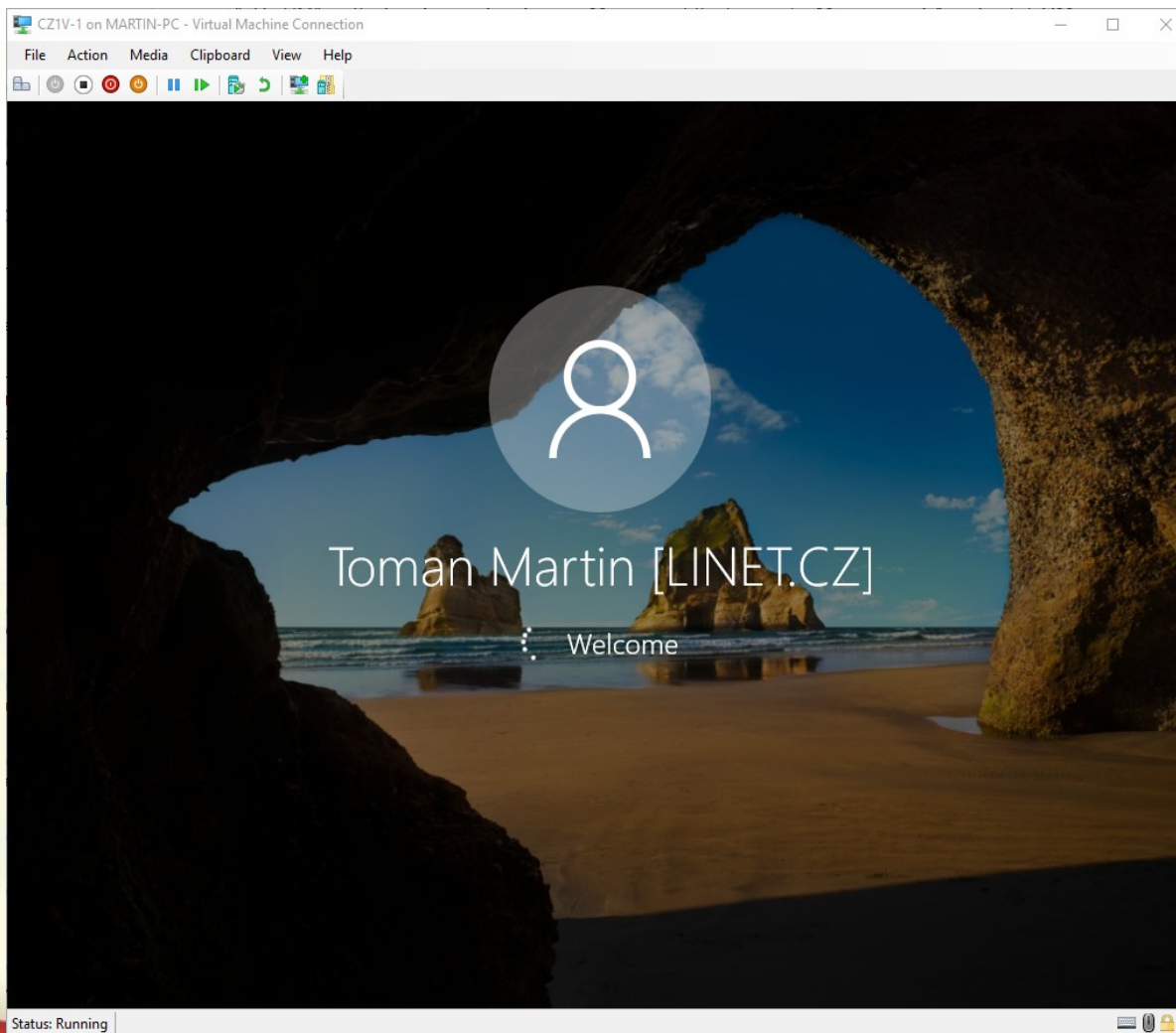
Confirm new password:

Note: The user name above may display in a different format than you are accustomed to logging in with. An example of another logon format is tomanm@linetgroupczu.tk.

 You have successfully reset your password. It may take a few minutes before you are able to login with your new password.



Testování – samoobslužný reset hesla v MIM



Česká zemědělská univerzita v Praze

Provozně ekonomická
fakulta

Testování – samoobslužný reset hesla v MIM

- Výhody
 - Registrace po přihlášení do PC
 - Možnost obnovy na svém PC
- Nevýhody
 - Vícefaktorová autentizace pouze při propojení s Azure



Automatizace procesů – napojení na HR databázi



Česká zemědělská univerzita v Praze

**Provozně ekonomická
fakulta**

Automatizace procesů – napojení na HR databázi

Prostředí MIM

Microsoft Identity Manager

Welcome, administrator

Search for: Search within: All Users

Distribution Groups (DGs)

- Create a new DG
- Manage my DGs
- See my DG memberships
- Join a DG

Distribution Groups (DGs) provide an easy way to send email to a group of users. When you send email to a DG, the email will be delivered to all its members.

Security Groups (SGs)

- Create a new SG
- Manage my SGs
- See my SG memberships
- Join a SG

Security groups (SGs) are used to secure network resources. When permissions to a resource are assigned to a SG, all members of the group can access that resource.

Users, Profiles, and Passwords

- Edit my profile
- Register for password reset

Profiles allow you to see information about users in your organization. You can also update certain information in your profile, such as your phone number, or register to reset your password.

Requests

Administration

- Unlock Users
- Schema Management
- Search Scopes
- Workflows
- Management Policy Rules
- Sets
- Synchronization Rules
- All Resources
- Resource Control Display Configurations
- Home Page Resources
- Navigation Bar Resources

Help

- About Microsoft Identity Manager

Home

Distribution Groups (DGs)

- My DGs
- My DG Memberships

Security Groups (SGs)

- My SGs
- My SG Memberships

Users

- My Profile
- Authentication Workflow
- Registration

Management Policy Rules

- Workflows
- Sets

Requests & Approvals

- Manage My Requests
- Approve Requests
- Search Requests

Privileged Access Management

- PAM Roles
- PAM Requests



Automatizace procesů – napojení na HR databázi

Testovací HR databáze

EmployeeID:10
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Terry
LastName:Adams
UserID:tadams
EmployeeType:Full Time Employee
Manager:




EmployeeID:11
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Jimmy
LastName:Bischoff
UserID:jbischoff
EmployeeType:Full Time Employee
Manager:10

EmployeeID:12
DeltaOperation:Add
Company:LINET-GROUP
FirstName:Lola
LastName:Jacobsen
UserID:ljacobsen
EmployeeType:Full Time Employee
Manager:11



Automatizace procesů – napojení na HR databázi

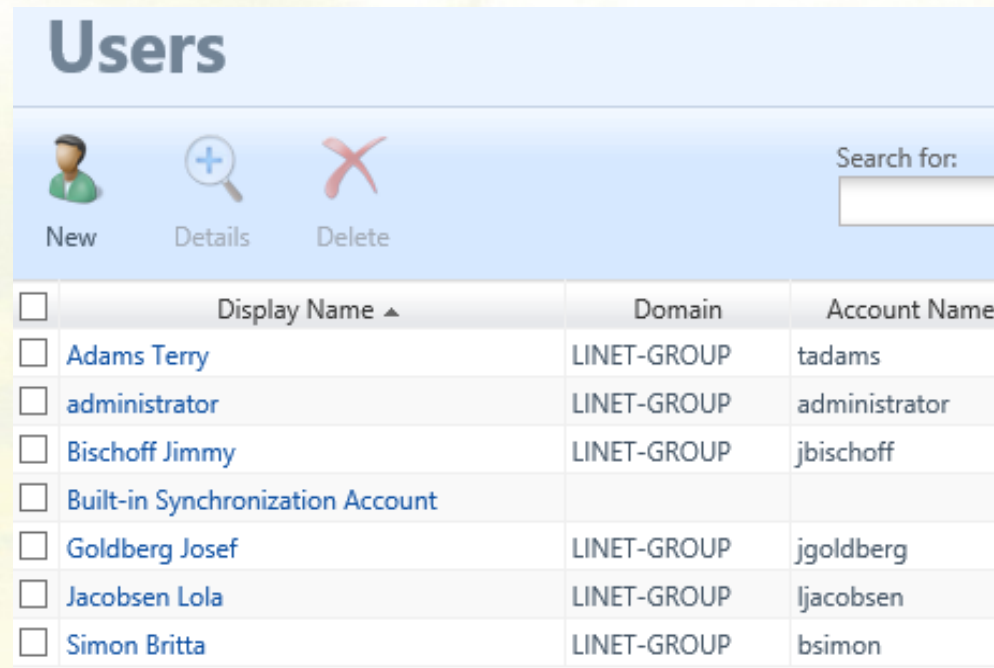
V MIM vytvořeny 2 testovací účty

Users			
  			
New Details Delete			
<input type="checkbox"/>	Display Name ▲	Domain	Account Name
<input type="checkbox"/>	administrator	LINET-GROUP	administrator
<input type="checkbox"/>	Built-in Synchronization Account		
<input type="checkbox"/>	Goldberg Josef	LINET-GROUP	jgoldberg
<input type="checkbox"/>	Simon Britta	LINET-GROUP	bsimon



Automatizace procesů – napojení na HR databázi

Účty v MIM po importu HR databáze

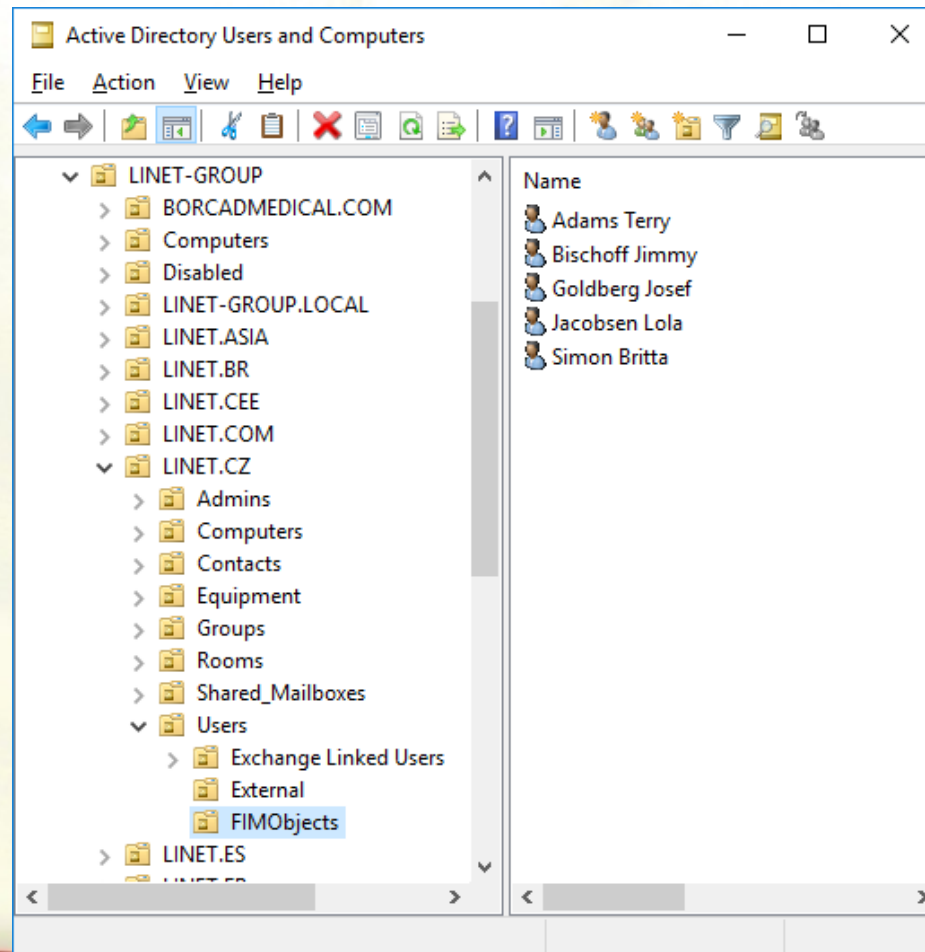


<input type="checkbox"/>	Display Name ▲	Domain	Account Name
<input type="checkbox"/>	Adams Terry	LINET-GROUP	tadams
<input type="checkbox"/>	administrator	LINET-GROUP	administrator
<input type="checkbox"/>	Bischoff Jimmy	LINET-GROUP	jbischoff
<input type="checkbox"/>	Built-in Synchronization Account		
<input type="checkbox"/>	Goldberg Josef	LINET-GROUP	jgoldberg
<input type="checkbox"/>	Jacobsen Lola	LINET-GROUP	ljacobsen
<input type="checkbox"/>	Simon Britta	LINET-GROUP	bsimon



Automatizace procesů – napojení na HR databázi

Účty v AD po synchronizaci s MIM



Automatizace procesů – napojení na HR databázi

- Výhody
 - Rychleji vytvořený účet
 - Účet zrušený ve správnou chvíli
 - Každý zaměstnanec má práva odpovídající pozici
- Nevýhody
 - Složitá prvotní nastavení



Finanční analýza

Náklady	Jednorázové náklady (licence + implementace)	254 055 Kč
	Roční náklady (1500 licencí)	2 430 000 Kč
Úspory	Práce podpory IT (rok)	240 000 Kč
	Předcházení škodě (rok) [Útok 1x/5 let]	25 000 000 Kč
	Nevyčíslitelné úspory - čas a pohodlí uživatelů	



Doporučení dalších kroků

- Implementace MIM do reálného prostředí firmy
- Nastavení testovaných funkcí
- Vyškolení uživatelů
- Otestování funkce PAM pro řízení admin. účtů



Přínos práce

- Výběr vhodného nástroje
- Zjištění všech výhod a nevýhod
- Efektivní vedení projektu při implementaci



Děkuji za pozornost



Česká zemědělská univerzita v Praze

**Provozně ekonomická
fakulta**