# CA information security update

**Pavel Marťák, CISSP** 14.10.2010

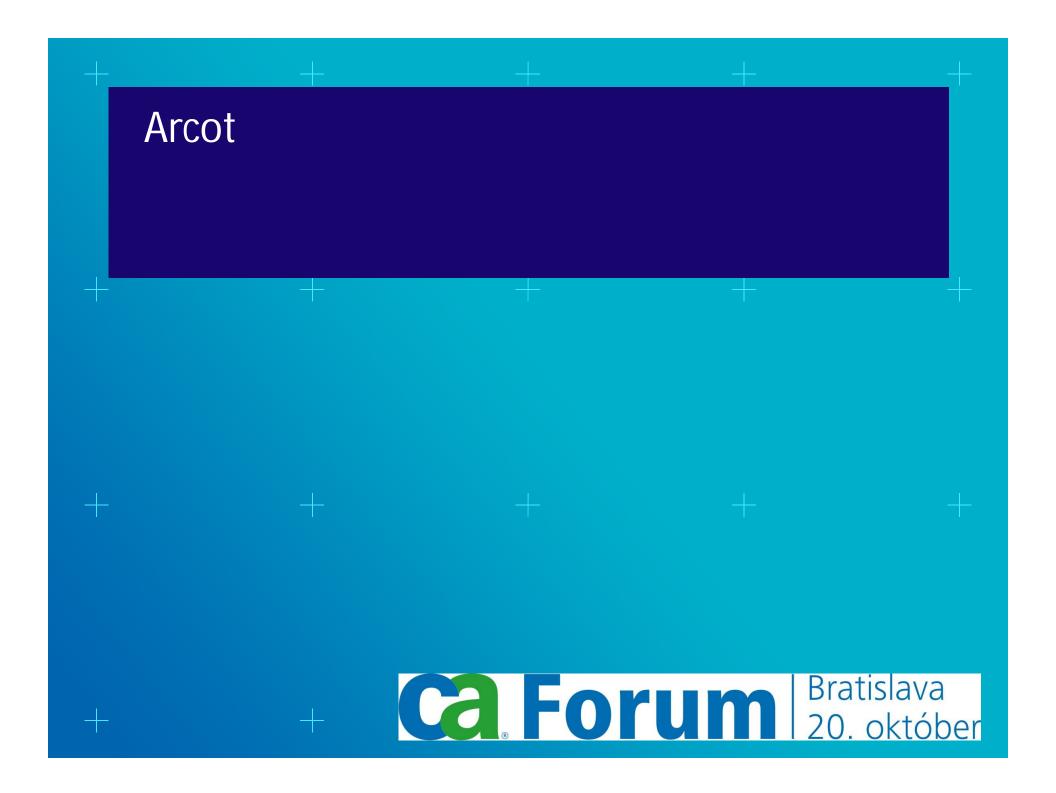


#### Agenda

#### -Arcot

- Identity Lifecycle Management update
- -ELM update
- -AccessControl update





#### Arcot

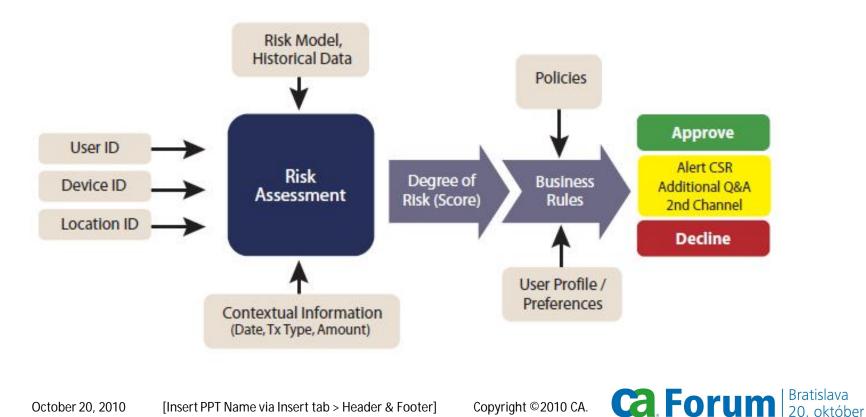
### -Acquisition

- ArcotID provides a unique and patented file-based software approach to the protection of the private key of aPublic Key Infrastructure (PKI) key pair
- WebFort is solution's authentication server providing complete authentication solution – can support PKI, OTP, RADIUS or SAML
- SignFort Arcot signing and authentication technology is embedded in Adobe<sup>®</sup> Acrobat<sup>®</sup> and Reader<sup>®</sup>.



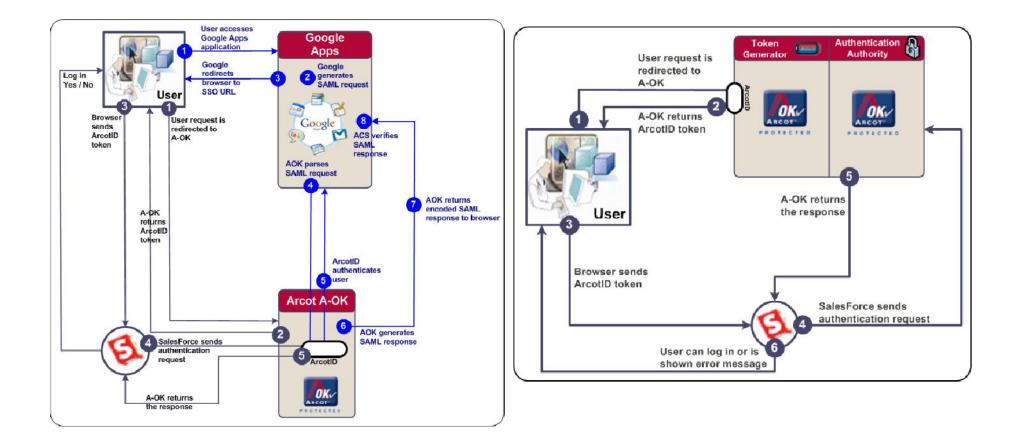
#### **Arcot - RiskFort**

- Defense against on-line fraud
- Uses statistical techniques, such as Bayesian modeling, to compare each transaction against a scoring formula.
- RiskFort periodically updates the formula, based on recent fraud and transaction data.



Copyright ©2010 CA.

#### Arcot – A-OK cloud authentication





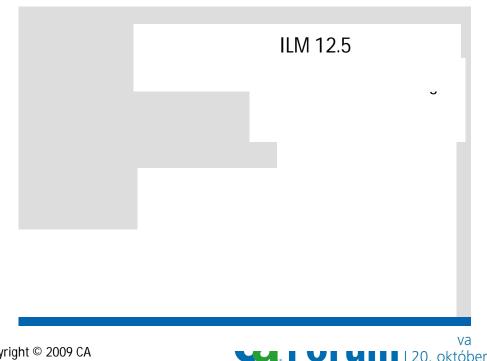
#### Identity Lifecycle Management update



#### **ILM evolution**

#### **Enabling the next generation of Identity Lifecycle Management**

- Embedding real-time identity analytics to supplement process automation with advanced decision support
- Further enhancing automated ILM processes with:
  - Compliance policy checking
  - Role analytics
- Sample use cases:
  - Preventative compliance
  - Out-of-pattern alerting
  - Suggested roles



CA Identity Lifecycle Management Copyright © 2009 CA

### **Preventative Identity policies**

**Proactive Check/Control of SoD violation** 

- Value for client
  - Policies are provided before the task is executed preventative measure
  - Allows to authorized business user to check the employee assignment against business SOD rules proactively
  - Activities based on positive violation check
    - Accept
    - Reject
    - Warning with policy-based workflow process triggering



### Smart provisioning enhancement

Reducing the time of the business approval process during the provisioning.

#### – Value for client

- Authorized business user can ask for recommended roles based of the user profile/attributes
- Can be based on the current position and/or other team member roles based on direct communication with RCM

Profile	Access Roles Admin Roles P	rovisioning Roles Accounts	Groups
Member	▲Role Name	Role Description	Comments
<b>v</b>	ForwardIncADExchange	Basic AD & Exchange capabilities	Required for Insurance users
	ForwardIncAsiaPacificSalesCorporate	Asia Pacific Sales Corporate Role	
	ForwardIncInvestments	Access to investment products	IT users are excluded
<b>v</b>	ForwardIncNorthAmericaSalesCorporate	North America Sales Corporate Role	
<b>v</b>	ForwardIncPreSales	Pre-sales Account Role	
Add a	provisioning role Suggest	Provisioning Roles Copy	from a user

CA Identity Lifecycle Management Copyright © 2009 CA



#### **Policy Xpress**

Wizard GUI driven flexible integration without programming

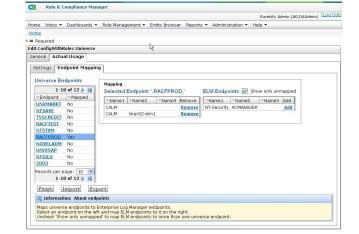
#### – Value for client

- Rapidnes of the implementation, reduce the implementation time
- Moving customization from the low level-programming to wizard driven activities/policies generator
- Reducing the TCO lower the mandays needed for customization demands.
- Reduce the need of custom code development of minimum.
   Customizations are handled as "policies"
- Increase of the user friendliness of the solution



#### **RCM GUI enhancements**

	Eurekify Admin (AD1\EAdmin) (Log Ou
ne Inbox 🔻 Role Management 🔻 Entity Browser Dashboards 🔻 Reports 🔻 Administration 👻 portal.label.	QA
ne > Entity Browser	
iverse: Demo  Configuration: ConfigWithRoles	
	<u></u>
ers Roles Resources Statistics Organization Chart	
elect Fields:	
P- 24 Branches	
evel 1 OrganizationType 🔄 😑 Stamford Branch	
evel 2 Organization 🔄 🤤 🕆 👙 Silicon Valley Branch	
avel 3 Location	
Jpdate Organization Chart - Sharon Johnson	
Sharon Jonnson     A Deer Alex	
- A Hill Gary	
- A German Tom	
- A Purple Mary	
- 🚨 Atek Rogers	
- Saven Werner	
🗏 🗕 🗕 🗕 🗕 🗕	
Hill Silver	
🕀 🤗 Corporate	
🗄 🌺 IT Security	
🕂 🚔 Finance	
🕀 🥔 Human Resources	
🕀 🥔 Application Development 🕀 🖓 Database Administrators	
Batabase Administrators     Batabase Administrators	
B Sales	
A Operations	
🕀 🙆 Marketing Dept.	
🗄 💁 System Management	
😐 🦀	
•••	



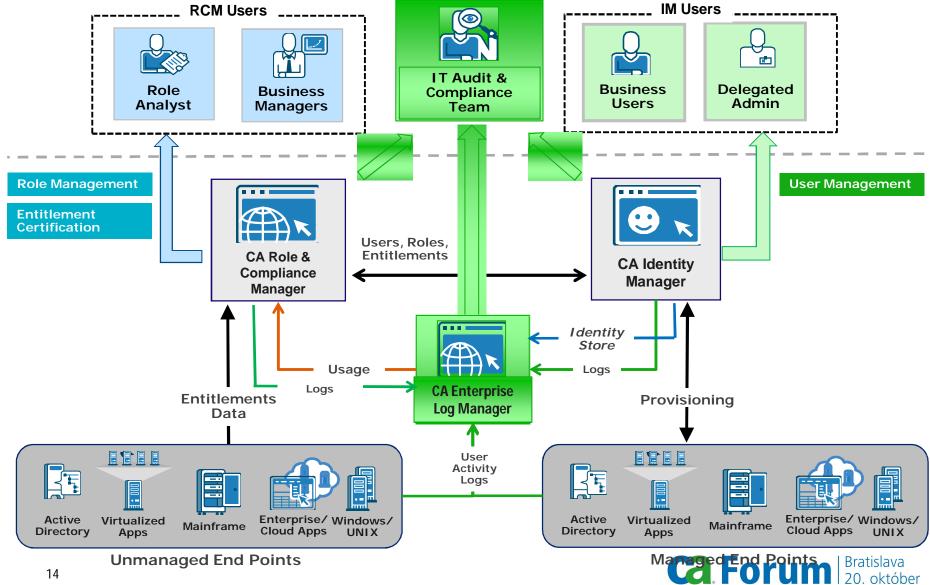
New sneak-peek screenshot



#### Enterprise Log Manager





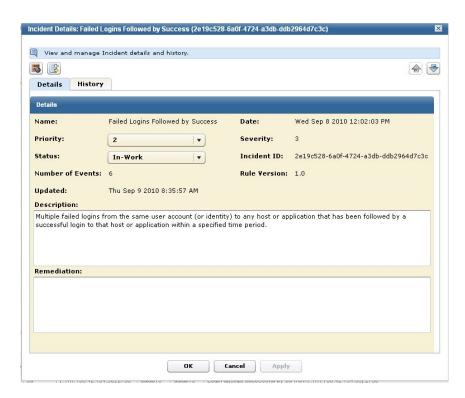


#### ELM - 12.5 Beta

#### -Correlation

#### -Incident Management

Rules	Version		Notification		
					-
🗌 🗀 Infrastructure Management					1
FISMA				•	1
🗌 🗀 Threat Management				•	1
🗌 🗁 Identity				•	100
V C Authorization			Notify-All-Admin	•	
Privileged Group Addition	1.0	•	Notify-All-Admin	•	
Privileged Group Addition Followed by Failed Authen	1.0	•	Notify-All-Admin	•	
V 🗌 🗁 Authentication				•	
Account Guessing - Same Host	1.0	-		•	
Failed Logins - Consecutive	1.0	•		•	
	1.0				
Failed Logins Followed by Success	1.0		Notify-US-Admin		





#### AccessControl



#### **CA Solution Overview**

**UNIX Authentication Broker** 

- Centralize UNIX Administration
- Active Directory Authentication
- Native Integration with AD

#### Privileged User Password Manager

- Control Access to Shared Accounts
- Break Glass Access Request
- Accountability of Shared Account Access



- Manage Fine-Grained Access
   Policies
- Segregation of Duty
- Server Security (Physical/Virtual)
- Auditing Privileged Access

#### CA ELM (Limited License)

- Centrally Manage Audit Logs
- Compliance Reporting





### 12.5 SP3 positions Access Control as a PUPM best-of-breed

- PUPM for Applications IDs to Databases
  - Manage passwords of applications using ODBC or JDBC
  - Does not require changes to the applications

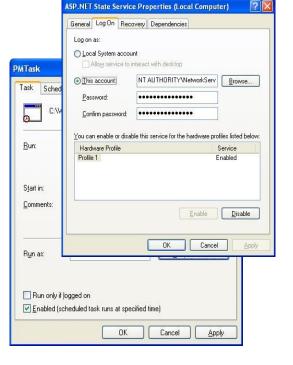
CA Access Control Enterprise Management - Windows Internet Explorer	
🔆 🕑 🔻 🕼 http://adabd:18080/kan/ac/ca12/index.jsp?facesYiewId=/app/page/screen/standard_search.jsp 🔍 🚧 🗙 ն coope	
🚖 🏘 🖸 CA Access Control Enterprise Management	
CA Access Control Enterprise Management	He Untitled - Notepad
CA Access Control Enterprise Management  Togged In ass Administrator to AcAMAN(IMSe AcCMAN) (Logant)  Home World View Policy Management Privileged Accounts Reports Users and Groups System  Accounts Endpoints * Login Application ~ Password Consumers * Password Policy * Exceptions * Audit  Modify Password Consumer: IIS Database Connectivity  Ceneral Privileged Accounts Hosts Users  Consumer Type: Database Connectivity  Description: Consumer Type: Database (ODBC/JDBC/OLEDB/OCI)  Application Path: * Enabled: Accept requests from password consumer  Return to Search  Ccopright & 2010 CA. All rights reserved.	<pre>boundable houses be Edit Forms Yew teb chuml&gt;cttleLAX Flights/cttle&gt; comport Namespace="system.pata"ss comport Namespace="system"ssextem.pata=clabad;utp=aspuser:"ss comport Namespace="system"ssextem.pata=clabad;utp=aspuser:"ss comport Namespace="system"ssextem.pata=clabad;utp=aspuser:"ssextem.pata=sspdemo;LANGUAGE=us_english;" comport no eve Oduccommention objConnection as odbccommention(constring) objConnection.open() 'specify the SQL string comport ss puepties odbcomment(strSQL, objConnection) 'get a datareader objCommand = New odbccommand(strSQL, objConnection) 'get a datareader objCommand = New odbccommand(strSQL, objConnection) 'o the batasinding dgresults.toataSource( objCataReader objCataReader = objCataReader objCataReader = objCataReader objCataReader = objCataReader objCataReader = compata=class() cyScripts <app: catacrid="" id="dgResults" runat="server"></app:></pre>
🛃 start 🔰 ể 🐼 🖉 🚔 🖉 👋 🏷 🛱 S M - 🔯 S M - 🧭 S M - 🏹 S M - 🔯 S M - 🖾 S M - 🖼 S M - 🖼 S M - 🖼 S M - 🖾 S M - 📓 S 🗑 S 👔 S EN 🚺 100% 🖉 🕸 🖉 🖓 🐼 🗘 🕞 🕉 🗗 🖓	y 6.66 AM



# 12.5 SP3 positions Access Control as a PUPM best-of-breed

- PUPM for Windows Services and Scheduled Tasks IDs
  - Agent-less automatic discovery and management with remote WMI

	ss Control Enterprise Management			🙆 • 🗟 • 🖶 • 🔂 • 🚳 •	🛛 - 🖾 💽 🛸 🔝 🚥
CA Acc	ess Control Enterprise	Manageme	nt		
	dministrator to ACLABAD(	the second second second second			
X	View Policy Manageme	N N	d Accounts Reports Users and Groups	System	
ounts 🕨 En	dpoints 🕨 Login Application	Password C	Consumers Password Policy Exceptions	Audit	
ervice Acc	count Discovery Wizard				
Service Ac	count Discovery				Sack Next Finish Cance
			1 2 🖒 3 🖒		
			Service General Summary Accounts Account		
			Properties		
•=Required					
•=Required					
Search Ac		accounts and p	assword consumers:		
Search Ac	counts		assword consumers:	1	_
Search Ac	counts a criteria for searching service a Service Accounts: C Endpo			]	
Search Ac Fill in the Search	counts e criteria for searching service n Service Accounts: O Endpo O Endpo	oint Type	V = V Windows Agentless O Search	]	
Search Ac Fill in the Search Search Re	counts e criteria for searching service n Service Accounts: O Endpo O Endpo	oint Type oint Name	V = V Windows Agentless O Search	1	
Search Ac Fill in the Search Search Re Select th	counts a criteria for searching service a Service Accounts: O Endpo O Endpo suits	oint Type oint Name	V = V Windows Agentless O Search	1	
Search Ac Fill in the Search Search Re Select th	counts a criteria for searching service a Service Accounts: Endpo Endpo suits ne object/s from the results se	oint Type oint Name	V = V Windows Agentless O Search	1	1 - 2 of 2 V
Search Ac Fill in the Search Search Re Select th	counts a criteria for searching service a Service Accounts: Endpo Endpo suits ne object/s from the results se	oint Type oint Name at: \$Type	V = V Windows Agentless O Search	≑Endpoint Name (Type)	1 - 2 of 2 ♥ ♦ Container
Search Ac Fill in the Search Search Re Select th Show: 10	counts e criteria for searching service s Service Accounts: C Endpo Endpo Suits ne object/s from the results se Results / Page	bint Type bint Name et:	V = V Windows Agentless Search	<mark> </mark>	
Search Ac Fill in the Search Search Re Select th Show: 10	counts or criteria for searching service a Service Accounts: Condension Endpoint Endopoint Endpoint Endopoint	oint Type oint Name at: \$Type	v = v Windows Agentless 0 Search v = v * 000		<b>⇔</b> Container
Search Ac Fill in the Search Search Re Select ti Show: 10	counts critena for searching service Service Accounts: C Endpo Suite suite e object/s from the results so Results / Page Account Name ACLAB\serviceuser	oint Type oint Name et: \$ Type \$ Service	Vindows Agentless     Vindows Agentless     Search     ■ = ■ ■	aclabad - AD (Windows Agentless) aclabad - AD (Windows Agentless)	<b>⇔ Container</b> Accounts
Search Ac Fill in the Search Re Select ti Show: 10 Select	counts critena for searching service Service Accounts: C Endpo Suite suite e object/s from the results so Results / Page Account Name ACLAB\serviceuser	oint Type oint Name et: \$ Type \$ Service	Vindows Agentless     Vindows Agentless     Search     ■ = ■ ■	aclabad - AD (Windows Agentless) aclabad - AD (Windows Agentless)	Container Accounts Accounts





May 16-20, 2010 Copyright © 2010 CA. All rights reserved.

# 12.5 SP3 positions Access Control as a PUPM best-of-breed

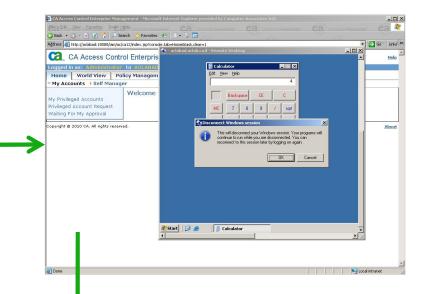
- Automatic login to PUPM
  - Tracking the original ID through advanced AC integration
  - Seamless login to managed systems without exposing the password
  - Session Recording (through 3<sup>rd</sup> party integration)

	My Privileged Accounts				
Search	n the privileged accounts				
	Search Accou	Ints: CAccount Name	▼ = ▼ *	OO Search	
	Opti	ons: 🗖 Show service a	ccounts		
		🗖 Show only my c	hecked-out accounts		
My Privi	leged Accounts				
l View t and Breal		Jse the Actions menu for	each account in order to:	Checkout/Checkin, Show	Password, Automatic Login
Show: 1	l0 Results / Page 💌				
					1 - 7 of 7 💌
Show Details	Account Name	<b>⇔</b> Status	≑Endpoint Name	<b>⇔Endpoint Type</b>	Actions
🔄 Show	🍓 Guest		PERRO15-W2K3 Win	Windows Agentless	Actions
🔄 Show	4 pupm1	Shecked Out	PERRO15-W2K3 Win	Windows Agentless	Actions
Show	🍓 Administrator		PERRO15-W2K8 Win	Windows Agentless	Actions
🔄 Show	🍓 PowerUser	Shecked Out	PERRO15-W2K3 Win	Windows Agentless	Actions
🔼 Hide	🍓 RegularUser	A Checked Out	PERRO15-W2K3 Win	Windows Agentless	Actions
	Last Checkout	28/04/2010 14:46:03	Last Ch	eckout Administrator By:	là -
	Checked-out By:	administrator		by.	
	Container:				
	Password Policy:	default password policy			
	Exclusive Checkout:	false			
🔄 Show	🍓 Administrator		GAD Win2003	Windows Agentless	Actions
	0		0		Le et



#### 12.5 SP3 session recording

ð	A Access Co	ntrol Enterprise Managemer	nt - Microsoft Internet Expl	orer provided by Con	nputer Associal	tes Inti.		_101:		
Ele		v Favorites Tools Help						ca 🦧		
-			📩 Favorites 🛛 🙆 🕹							
Add	ess 💰 http	://adabad:18080/iam/ac/ca12/ini	dex.jsp?task.tag=MyPassword#	ccountsJSFTask				🔁 Go Links i		
C	a ca	Access Control E	nterprise Manage	ment				Help		
Lo	gged in a	s: Administrator to a	ACLABAD(DMS @ ACL	ABAD) (Logout)						
			lanagement Privil	eged Accounts	Reports	Users and Groups	System			
▼ N		its 🕨 Self Manager								
	My Priv	ileged Accounts								
	0									
		My Privileged Account: 1 the privileged account		iteria:						
			unts: C Account Nam			00 Search	1			
		Options: C Show service accounts								
		Opt	Include break							
				/ checked-out ac	counts					
	My Privi	leged Accounts								
Þ	Q View t and Brea	he privileged accounts. k Glass.	Use the Actions menu	for each account	in order to:	Checkout/Checkin, Sho	w Password, Automat	ic Login		
	Show:	10 Results / Page 💌								
							1	- 2 of 2 💌		
	Show Details	Account Name	🕀 Endpoint Name	e 🗘 Endpoi	int Type	<b>⇔</b> Status	Actions			
	Show	🍓 PowerUser	Sample Windows	Windows Age	entless		Actions	•		
	Show	🍇 administrator	Sample Windows	Windows Age	entless		Actions Account Actions			
							Checkout Automatic Login	-		
							Recorded RDP			
							Advanced Logi	n 📘		
創							Locali	ptrapet		



CA A	ccess Control Enter	prise Management -	Microsoft Internet	Explorer provided by	Computer /	Issociates Int	L		ام
• 5		- Comp					ter Asso, otes-		puter Associates - Ca
Back			avorites 😁 🍛 •				×		
dress	http://adabad:18	080/iam/ac/ca12/index	.jsp?facesViewId=/app	/page/ppm/audit/submiti	ed_tasks.jsp				💌 🄁 Go Lin
a	CA Access	Control Ent	erprise Mana	gement					He
	ed in as: Admir			ACLABAD) (Logo	ut)				
Hom	Y		agement P	ivileged Accoun	and the second second	orts Us	ers and Grou	ps Syste	em
Acc	ounts 🕨 Endpoi	200 200 200 200 200 200 200 200 200 200	-	sword Consume		- Article 6 - 12 02			
A	udit Privilege	d Accounts							
	Description	Account name	Endpoint type	Endpoint name	Session Details	Status	Initiated by	▼ Submitted	Last Operation
	[ACLABAD] Check In Privileged Account task	PowerUser	Windows Agentless	Sample Windows		Completed	Administrator	5/27/2010 4:36 PM	Checked in the privileged account on endpoint type: Windows Agentless, endpoint: Sample Windows, account: PowerUser in time: 5/27/10 4:36 PM.
	[ACLABAD] My Privileged Accounts task	PowerUser	Windows Agentless	Sample Window	9	In progress	Administrator	5/27/2010 4:35 PM	
	[ACLABAD] Check In Privileged Account task	PowerUser	Windows Agentless	Sample Windows		Completed	Administrator	5/27/2010 4:34 PM	Checked in the privileged account on endpoint type: Windows Agentless, endpoint: Sample Windows, account: PowerUser in time: 5/27/10 4:34 PM.
0	[ACLABAD] My Privileged Accounts task	PowerUser	Windows Agentless	Sample Windows	2	In progress	Administrator	5/27/2010 4:29 PM	
	[ACLABAD] Modify Endpoint							5/27/2010	

May 16-20, 2010 Copyright © 2010 CA. All rights reserved.



# 12.5 SP3 adds additional enhancements to UNIX security

- Kerberos-based Single Sign On for UNAB
  - Seamless login from or to windows and to other UNIX through Kerberos enabled applications
  - Leverage the native UNIX Kerberos key store
  - Integrates with AD Kerberos
- UNIX Keyboard Logger AC Trace enhancements
  - Enhanced Trace to record interactive sessions for improved compliance
  - Session summary reports on ELM



