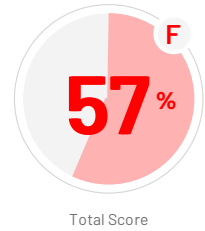


ACTIVE DIRECTORY SECURITY ASSESSMENT REPORT



OVERVIEW








This report summarizes the Active Directory security assessment results. The assessment performed includes querying your Active Directory environment and running a series of security indicator scripts against domains in the selected forest (see appendix for full list of domains included). The report provides an overall risk score as well as detailed results about each Indicator of Exposure (IOE) found. This assessment represents opportunities for enhancing this Active Directory environment from a security perspective in accordance with industry best practices.

[View Appendix 1 - Domains list](#)



























SECURITY INDICATORS

EVALUATED	IOEs FOUND	PASSED	FAILED TO RUN	CANCELED	NOT SELECTED
50/50	 31	 19	 0	 0	0

CRITICAL IOEs FOUND

-  **Anonymous access to Active Directory enabled**
It is possible, though not recommended, to enable anonymous access to AD. This indicator looks for the presence of the flag that enables anonymous access. Anonymous ...
[Read More...](#)
-  **Mimikatz DCShadow in use**
Mimikatz's DCShadow switch allows a user who has compromised an AD domain, to inject arbitrary changes into AD using a "fake" domain controller. These changes bypa...
[Read More...](#)
-  **Reversible passwords found in GPOs**
This indicator looks for GPOs that still contain passwords that can be easily decrypted by an attacker (so called "Cpassword" entries).
[Read More...](#)
-  **Unprivileged users with DC Sync rights on the Domain**
Any security principals with Replicate Changes All or Replicate Directory Changes permissions on domain naming context object can potentially retrieve password hashes fo...
[Read More...](#)
-  **Zerologon vulnerability**
This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthenticated attacker can exp...
[Read More...](#)

ADDITIONAL IOEs FOUND

NAME	SEVERITY LEVEL	
• Built-in domain Administrator account used within the last two weeks.	Warning	 Read More...
• Computer or user accounts with unconstrained delegation	Warning	 Read More...
• Computers and gMSA objects with password last set over 90 days ago	Warning	 Read More...
• Default security descriptor schema changes in the last 90 days	Warning	 Read More...
• Domain Controller owner permissions	Warning	 Read More...
• Enterprise Key Admins with full access to domain	Warning	 Read More...
• Kerberos Golden Ticket susceptibility	Warning	 Read More...
• Non-standard Primary Group IDs	Warning	 Read More...
• Privileged objects with unprivileged owners	Warning	 Read More...
• Privileged users not protected by SDProp	Warning	 Read More...
• Risky RODC credential caching	Warning	 Read More...
• Weak GPO linking delegation at the AD Site level	Warning	 Read More...
• Weak GPO linking delegation at the Domain Controllers OU level	Warning	 Read More...
• Weak GPO linking delegation at the domain level	Warning	 Read More...
• Well-known privileged SIDs in SIDHistory	Warning	 Read More...
• Built-in domain Administrator account password not changed within last 6 months	Informational	 Read More...
• Computers with older OS versions	Informational	 Read More...
• Domains with obsolete functional levels	Informational	 Read More...
• Enabled users that are inactive	Informational	 Read More...
• Normal users can add computer accounts to domain	Informational	 Read More...
• Privileged users that are disabled	Informational	 Read More...
• Protected Users group in use	Informational	 Read More...
• Unprotected accounts with adminCount=1	Informational	 Read More...
• Users with old passwords	Informational	 Read More...
• Users with Password Never Expires flag set	Informational	 Read More...
• Users with risky User Account Control	Informational	 Read More...

CATEGORIES



AD DELEGATION

AD delegation is a critical part of security and compliance. By delegating control over Active ...

[Read More ...](#)



ACCOUNT SECURITY

Account Security indicators pertain to security weaknesses on individual accounts--built-in or ...

[Read More ...](#)



AD INFRASTRUCTURE SECURITY

AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's...

[Read More ...](#)



GROUP POLICY SECURITY

Group Policy Security indicators pertain to the security configuration of GPOs and their ...

[Read More ...](#)

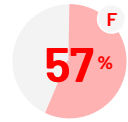


KERBEROS SECURITY

Kerberos Security indicators pertain to the configuration of Kerberos capabilities on computer ...

[Read More ...](#)

AD DELEGATION



WEIGHT

3

EVALUATED

11/11

IOE FOUND

1 7

AD delegation is a critical part of security and compliance. By delegating control over Active Directory, you can grant users or groups permissions without adding users to privileged groups.



SECURITY INDICATOR

Normal users can add computer accounts to domain

IOE Found



SEVERITY

Informational



WEIGHT

3

MITRE ATT&CK FRAMEWORK CATEGORY

Credential Access, Lateral Movement

Description

By default, members of the Authenticated Users group can add up to 10 machine accounts to a domain. The ability to do this confers certain rights on those created machine accounts that can be abused by a variety of Kerberos-based attacks. As a result, if the ms-DS-MachineAccountQuota attribute on the domain naming context head is not set to 0, regular users have this ability.

Likelihood of Compromise

This is a typical (or default) domain configuration. While potentially dangerous, it does not indicate a compromise. If new systems are added to the domain that cannot be accounted for, the additional systems and the user accounts used to add them should be investigated.

Result

One or more domains failed this test.

DistinguishedName	MachineAccountQuota
DC=semperissm,DC=lab	10

Remediation Steps

Set the ms-DS-MachineAccountQuota attribute on the domain NC head to 0 to disable a regular user's ability to add computer accounts



SECURITY INDICATOR

Guest account is enabled

Pass



SEVERITY

Informational



WEIGHT

2

MITRE ATT&CK FRAMEWORK CATEGORY

Discovery

Description

The built-in Active Directory "guest" account allows for passwordless access to AD. In general, this account is disabled in most AD environments. This indicator checks to make sure that this account is disabled.

Likelihood of Compromise

This is not a normal indicator of compromise, but this setting can aid attackers in enumerating accounts and performing password sprays. Abnormally high levels of failed authentication attempts could indicate an active attack.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Non default value on ms-Mcs-AdmPwd SearchFlags

Pass



SEVERITY

Warning



WEIGHT

7

MITRE ATT&CK FRAMEWORK CATEGORY

Credential Access

Description

This indicator looks for changes to searchFlags on the ms-Mcs-AdmPwd schema, which can cause the password to be visible to unintended users allowing an attacker to use it as stealthy backdoor.

Likelihood of Compromise

Even though schema changes are not common, a targeted schema change like this can leave the administrator passwords of 100s or 1000s of computers vulnerable to non-privileged users.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Unprivileged users with DC Sync rights on the Domain

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Critical	8	Credential Access, Privilege Escalation

Description

Any security principals with Replicate Changes All or Replicate Directory Changes permissions on domain naming context object can potentially retrieve password hashes for any and all users in an AD domain. This can then lead to all kinds of credential-theft based attacks, including Golden and Silver Ticket attacks.

Likelihood of Compromise

If a regular user account gets these privileges, it is trivial to retrieve credential material using tools like Mimikatz, for any user in a domain.

Result

Found 1 objects with replication permissions

DistinguishedName	Access	Identity
DC=semperissm,DC=lab	Allow DS-Replication-Get-Changes-All;Allow DS-Replication-Get-Changes	SEMPERISSM\badguy

Remediation Steps

Ensure that users don't have unnecessary replication permissions.



SECURITY INDICATOR

Privileged objects with unprivileged owners

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	6	Privilege Escalation

Description

If a privileged object (as determined by adminCount=1) is owned by an account that is unprivileged, then any compromise of that unprivileged account could result in those privileged objects' delegation being modified, since owners can override any delegation on an object, if only temporarily.

Likelihood of Compromise

Most privileged objects are owned by privileged groups or users. But if a privileged object were to be owned by an unprivileged account, it could be easily taken over. And even though SDProp might correct any delegation done by an attacker who has compromised an owner, the attacker could have up to 1 hour to perform any changes on the privileged object (e.g. group membership changes or password changes) before SDProp corrects it.

Result

Found 1 privileged objects with unprivileged owner

DistinguishedName	Owner
CN=Freddie Curry,OU=IT,OU=AMER,DC=semperissm,DC=lab	NT AUTHORITY\SYSTEM

Remediation Steps

Remove unprivileged owner from privileged objects.



SECURITY INDICATOR

Changes to MS LAPS read permissions

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	8	Credential Access, Lateral Movement

Description

This indicator looks for changes to the security descriptor on computer accounts that could allow inadvertent exposure of local administrator accounts in shops that use the Microsoft LAPS solution (<https://www.microsoft.com/en-us/download/details.aspx?id=46899>). This allows you to spot Access Control List (ACL) changes that could allow an attacker to view the Microsoft LAPS local administrator account password attribute. LAPS provides a way for you to rotate local administrator account passwords on your servers and workstations.

Likelihood of Compromise

Only Domain Administrators and Enterprise Administrators should have access to the LAPS passwords. Other users may use this capability to laterally move through a domain using local administrator accounts.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Privileged users not protected by SDProp

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	5	Credential Access

Description

This indicator looks for privileged users whose adminCount attribute is not set to 1. These users should be managed by SDProp to ensure secure delegation.

Likelihood of Compromise

If privileged users are not protected by SDProp, their ACLs can be changed by an attacker to facilitate changing the user's password. But an attacker would first need to have gained write access to the user object.

Result

Found 4 privileged users that do not have adminCount equal to 1

DistinguishedName
CN=Key Admins,CN=Users,DC=eu,DC=semperissm,DC=lab
CN=Key Admins,CN=Users,DC=semperissm,DC=lab
CN=Enterprise Key Admins,CN=Users,DC=semperissm,DC=lab
CN=S-1-5-21-817735531-4269160403-1409475253-2612,CN=ForeignSecurityPrincipals,DC=semperissm,DC=lab

Remediation Steps

Check why those objects do not have adminCount=1 and set the attribute to 1.



SECURITY INDICATOR

Default security descriptor schema changes in the last 90 days

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	7	Persistence, Lateral Movement, Defense Evasion

Description

This indicator detects changes made to the default security descriptor schema in the last 90 days. If an attacker gets access to the schema instance in a given forest, they can make changes to the defaultSecurityDescriptor attribute on any AD object class. These changes would then propagate as new default Access Control Lists (ACLs) on any newly created object in AD, potentially weakening AD security posture.

Likelihood of Compromise

Changes to the default security descriptor are not common. An admin should know that the change was made and be able to articulate the reason for the change. If the change was not intentional, the likelihood of compromise is very high. The chances of compromise are lower if the change hardens the setting instead of weakening it.

Result

One or more domains failed this test.

DistinguishedName	DateChanged
CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=semperissm,DC=lab	12/11/2020 4:10:36 PM

Remediation Steps

Confirm if any default security descriptor changes have occurred to the detected objects in the last 90 days



SECURITY INDICATOR

Domain Controller owner permissions

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	6	Privilege Escalation, Credential Access

Description

This indicator looks for Domain Controller computer accounts whose owner is not a Domain Admins, Enterprise Admins, or built-in Administrator account, since control of DC machine accounts allows for an easy path to compromising the domain.

Likelihood of Compromise

While Domain Controller objects are typically created during DCPromo by privileged accounts, if an accidental ownership change occurs on a DC object, it can have large consequences for security of the domain, since object owners can change permissions on the object to perform any number of actions.

Result

One or more domains failed this test.

DistinguishedName	Owner
CN=ADSM-EU-DC2,OU=Domain Controllers,DC=eu,DC=semperissm,DC=lab	EU\Ashley.Ward
CN=ADSM-DC3,OU=Domain Controllers,DC=semperissm,DC=lab	SEMPERISSM\darren

Remediation Steps

Ensure that only privileged Tier 0 admin accounts and domain built-in groups such as Enterprise Admins, Domain Admins or Administrators have ownership of Domain Controller computer objects.



SECURITY INDICATOR

Permission changes on AdminSDHolder object

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Critical	10	Privilege Escalation, Defense Evasion

Description

This indicator looks for Access Control List (ACL) changes on the AdminSDHolder object, which could indicate an attempt to modify permissions on privileged objects that are subject to AdminSDHolder (e.g. users or groups with AdminCount=1).

Likelihood of Compromise

Changes to the AdminSDHolder object are very rare. An admin should know that the change was made and be able to articulate the reason for the change. If the change was not intentional, the likelihood of compromise is very high.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Enterprise Key Admins with full access to domain

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	7	Privilege Escalation, Credential Access, Lateral Movement

Description

This indicator looks for evidence of a bug in certain versions of Windows Server 2016 Adprep that granted undue access to the Enterprise Key Admins group.

Likelihood of Compromise

This issue was corrected in a subsequent release of Server 2016 and may not exist in your environment, but checking for it is definitely warranted, since it grants this group the ability to replicate all changes from AD (DCSync Attack).

Result

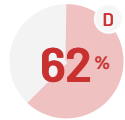
Found 1 domains where the Enterprise Key Admins group has full access

DistinguishedName
DC=semperissm,DC=lab

Remediation Steps

Ensure that users don't have unnecessary permissions. See also [Remediating Enterprise Key Admins Permissions](#)

ACCOUNT SECURITY



WEIGHT

6

EVALUATED

17/17

IOE FOUND

10

Account Security indicators pertain to security weaknesses on individual accounts--built-in or otherwise, within Active Directory



SECURITY INDICATOR

Non-standard Primary Group IDs

IOE Found



SEVERITY

Warning



WEIGHT

8

MITRE ATT&CK FRAMEWORK CATEGORY

Privilege Escalation

Description

This indicator returns a list of all users with primaryGroupID different then 513 (Domain Users) or 514 (Domain Guests) or computers different from 515 (Domain Computers) or 516 (Domain Controllers). Primary Group ID can be used to grant privileged access to a security principal without explicitly adding the principal to a privileged group.

Likelihood of Compromise

Modifying the Primary Group ID is a stealthy way for an attacker to escalate privileges without triggering normal auditing for group membership changes. This should be monitored closely at all times.

Result

Found 4 objects with Primary Group ID of a group they are not member of

DistinguishedName	GroupRID
CN=Bill Auditor,OU=Admin,DC=semperissm,DC=lab	512
CN=Eva Terrell,OU=IT,OU=AMER,DC=semperissm,DC=lab	512
CN=Aline Nielsen,OU=IT,OU=AMER,DC=semperissm,DC=lab	512
CN=SEMP-RODC1,OU=Domain Controllers,DC=semperissm,DC=lab	521

Remediation Steps

Change members Primary Group ID or add the member to the relevant group.



SECURITY INDICATOR

Protected Users group in use

IOE Found



SEVERITY

Informational



WEIGHT

1

MITRE ATT&CK FRAMEWORK CATEGORY

Credential Access

Description

The Protected Users group was introduced in Server 2012-R2 Active Directory to minimize credential exposure for privileged accounts. A user who is in the Protected Users group gets the benefit of changes in behavior related to how their credentials are authenticated to Windows resources. These changes include no longer caching clear-text passwords, even when Windows Digest is enabled, NTLM will no longer cache clear-text passwords, and Kerberos will no longer create DES or RC4 keys. When logging into domain controllers, members of the Protected Users group will no longer authenticate via NTLM (Kerberos only), they will no longer use DES or RC4 for Kerberos pre-authentication, and cannot be delegated with constrained or unconstrained delegation.

Likelihood of Compromise

This is not an indicator of compromise. Ideally, more users will be seen using the Protected Users group.

Result

Found 67 privileged users that are not member of the Protected Users group
[view the full results...](#)

Remediation Steps

Ensure that all privileged users are members of the Protected Users group.



SECURITY INDICATOR

Unprivileged users as DNS Admins

Pass



SEVERITY

Warning



WEIGHT

7

MITRE ATT&CK FRAMEWORK CATEGORY

Execution, Privilege Escalation

Description

This indicator looks for any member of the DNS Admins group that is not a privileged user. DNS Admins isn't considered a protected group but as some research shows, a member of this group (or any user that has write access on DNS Server objects) can load a DLL remotely on the DNS Server (which is often a Domain Controller) running as SYSTEM.

Likelihood of Compromise

DNS Admins membership can sometimes be delegated to non-AD administrators (e.g. Admins with DNS responsibilities outside of AD) and that can result in these accounts being ripe for compromise, that can lead to escalation of privileges on DCs.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Users with risky User Account Control

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Privilege Escalation, Lateral Movement

Description

This indicator identifies user accounts where the Password Not Required, Trusted for Delegation, Passwords Encrypted with DES, Passwords with reversible encryption, or Trusted to Authenticate for Delegation flags are set.

Likelihood of Compromise

If the account is new it could indicate a compromise. If this is not new, clean up the legacy systems, accounts, and settings.

Result

One or more domains failed this test.

UserAccountControl	LastModified	CreatedTime	ManagedBy	MemberOf	DistinguishedName
640	11/19/2020 10:36:34 PM	9/15/2017 12:04:36 AM		CN=Domain Admins,CN=Users,DC=eu,DC=semperissm,DC=lab	CN=Bruce Buck,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab
544	11/22/2020 9:02:44 PM	11/22/2020 9:02:22 PM			CN=TestMeTheUser,OU=Bad,DC=semperissm,DC=lab
640	11/19/2020 10:35:43 PM	5/1/2018 7:01:04 AM			CN=Charlene Herring,OU=HQ,OU=AMER,DC=semperissm,DC=lab
2097664	11/19/2020 10:36:07 PM	5/4/2018 3:23:33 AM			CN=Darla Hopper,OU=HQ,OU=AMER,DC=semperissm,DC=lab

Remediation Steps

These flags all represent potential weaknesses in user accounts, which if left in place, could make these accounts targets of takeover attacks. If these flags are required, ensure that these accounts have the least privileges possible and sufficiently complex passwords that are changed regularly.



SECURITY INDICATOR

Users with Kerberos pre-authentication disabled

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	5	Privilege Escalation, Credential Access, Lateral Movement

Description

This indicator looks for users with Kerberos pre-authentication disabled, which can be targeted for ASREP-Roasting attacks (like 'Keberoasting'). For more information, see <https://social.technet.microsoft.com/wiki/contents/articles/23559-kerberos-pre-authentication-why-it-should-not-be-disabled.aspx>.

Likelihood of Compromise

If an account has Kerberos pre-authentication disabled, it makes it easier for attackers to send dummy requests to a DC to try and crack its Ticket Granting Ticket (TGT).

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Built-in domain Administrator account used within the last two weeks.

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	5	Defense Evasion

Description

This indicator checks to see if the lastLogonTimestamp for the built-in domain Administrator account has been updated within the last two weeks. If so, it could indicate that the user has been compromised.

Likelihood of Compromise

If best practices are followed, this account should not be used regularly, if at all. This indicator failing could indicate a compromise. Ensure any logins to the built-in domain Administrator account are legitimate and accounted for. If not accounted for, a breach is extremely likely.

Result

One or more domains failed this test.

DistinguishedName	LastLogonTimestamp
CN=Administrator,CN=Users,DC=eu,DC=semperissm,DC=lab	1/4/2021 1:09:48 PM
CN=Administrator,CN=Users,DC=semperissm,DC=lab	12/28/2020 12:21:25 PM

Remediation Steps

Ensure that the built-in domain Administrator account is not used regularly and has a complex password known only to highly privileged admins.



SECURITY INDICATOR

Users with Password Never Expires flag set

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	1	Credential Access

Description

This indicator identifies user accounts where the Password Never Expires flag is set. These accounts can be targets for brute force password attacks, given that their passwords may not be strong when they were set. These accounts also tend to be service accounts with privileged access to applications and services, including Kerberos-based services.

Likelihood of Compromise

This is not a normal indicator of compromise. If the account is new and cannot be accounted for by administrators, then the account should be investigated.

Result

One or more domains failed this test.

[view the full results...](#)

Remediation Steps

Move any user accounts away from Password Never Expires by having a good password rotation scheme and ensure any accounts that require this flag have the least privileges required. If this is a service account, considering using Group Managed Service Accounts (gMSA)



SECURITY INDICATOR

Recent privileged account creation activity

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Persistence

Description

This indicator looks for any users or groups that were created within the last month. Privileged accounts and groups are defined by having their adminCount attribute set to 1.

Likelihood of Compromise

In most environments, creation of privileged accounts and groups is tightly controlled and audited. This indicator provides a backstop to that process that allows users to visually inspect whether privileged accounts and groups are being created without prior knowledge.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Unprotected accounts with adminCount=1

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Privilege Escalation

Description

This indicator looks for any users or groups that may have been under the control of SDProp (adminCount=1) but are no longer members of privileged groups and should not be considered privileged.

Likelihood of Compromise

While it's not likely that accounts with adminCount set to 1 will be used in a compromise, it can cause confusion when assessing accounts that have privileged access in the environment.

Result

Found 11 objects with adminCount=1 that are not members of a privileged group
[view the full results...](#)

Remediation Steps

Check why those objects have admintCount=1 and set the attribute back to <not set>.



SECURITY INDICATOR

Users with old passwords

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Discovery

Description

This indicator looks for user accounts who's password haven't changed in over 180 days. This could make these account ripe for password guessing attacks.

Likelihood of Compromise

While a user account whose password hasn't changed in a while isn't in and of itself risky, it could be a target for attackers looking for service accounts or other privileged accounts that may have weaker passwords that have not been required to change.

Result

Found 1201 users whose password has not changed in the last 180 days
[view the full results...](#)

Remediation Steps

Ensure that users change their password at least once every 6 months.



SECURITY INDICATOR

Enabled users that are inactive

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Discovery

Description

This indicator looks for user accounts that are active, but have never been used to log into Active Directory. These kinds of attacks can be targets for attackers who look for accounts that may have weak or default passwords set.

Likelihood of Compromise

While compromise of an unused account is not automatically a problem, reducing these accounts reduces the attack surface of AD.

Result

Found 919 enabled users that have not logged in in the last 30 days
[view the full results...](#)

Remediation Steps

Ensure that unused users are disabled or deleted.



SECURITY INDICATOR

Privileged users that are disabled

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Privilege Escalation

Description

This indicator looks for privileged user accounts, as indicated by their adminCount attribute set to 1, that are disabled. If a privileged account is disabled, it should be removed from its privileged group(s) to prevent inadvertent misuse.

Likelihood of Compromise

When a user is disabled, it tends to not be monitored as closely as active accounts. If this user is also a privileged user, then it becomes a target for takeover if an attacker can enable the account.

Result

Found 1 disabled users with admincount attribute equal to 1

DistinguishedName	MemberOf
CN=Bad Guy,OU=Bad,DC=semperissm,DC=lab	

Remediation Steps

Ensure that privileged groups have only necessary users as members.



SECURITY INDICATOR

Privileged group membership changes in the last 7 days

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	5	Discovery, Privilege Escalation

Description

This indicator looks for changes to the built-in privileged groups within the last 7 days, which could indicate attempts to escalate privilege.

Likelihood of Compromise

Recent additions or deletions to privileged group members could be normal operational changes or could indicate attempts at persistence or cleaning up of tracks after an attack (e.g. detection of temporary group membership changes).

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

AD objects created within the last 10 days

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	4	Discovery

Description

This indicator looks for any AD objects that were created within the last 10 days.

Likelihood of Compromise

In some environments, object creation happens constantly and so finding illegitimate accounts is a process of seeing the recent accounts and ensuring that all look normal.

Result

Found 9 objects that were created in the last 10 days

DistinguishedName	MemberOf
CN={802C5011-291A-46F8-ADC9-11794EFE0BD9},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=Machine,CN={802C5011-291A-46F8-ADC9-11794EFE0BD9},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=User,CN={802C5011-291A-46F8-ADC9-11794EFE0BD9},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN={26418478-23C2-46E0-9C24-7CB6035C4753},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=Machine,CN={26418478-23C2-46E0-9C24-7CB6035C4753},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=User,CN={26418478-23C2-46E0-9C24-7CB6035C4753},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN={9F55DD17-C574-45EA-865E-0663D4231731},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=Machine,CN={9F55DD17-C574-45EA-865E-0663D4231731},CN=Policies,CN=System,DC=semperissm,DC=lab	
CN=User,CN={9F55DD17-C574-45EA-865E-0663D4231731},CN=Policies,CN=System,DC=semperissm,DC=lab	

Remediation Steps

Ensure that the new objects are known and legitimate.



SECURITY INDICATOR

Built-in domain Administrator account password not changed within last 6 months

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	4	Credential Access

Description

This indicator checks to see if the pwdLastSet attribute on the built-in domain Administrator account has been changed within the last 6 months.

Likelihood of Compromise

If the built-in domain Administrator account is not being changed on a regular basis, this account can be vulnerable to brute force password attacks.

Result

One or more domains failed this test.

DistinguishedName	Password Last Set
CN=Administrator,CN=Users,DC=eu,DC=semperissm,DC=lab	2/15/2018 7:58:35 AM
CN=Administrator,CN=Users,DC=semperissm,DC=lab	1/15/2019 7:45:35 PM

Remediation Steps

Ensure that the built-in domain Administrator account password is changed at least twice per year.



SECURITY INDICATOR

Recent SidHistory changes on objects

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	8	Privilege Escalation

Description

This indicator detects any recent changes to sidHistory on objects, including changes to non-privileged accounts where privileged SIDs are added.

Likelihood of Compromise

Attackers need privileged access to AD to be able to write to SIDHistory but if such rights exist, writing privileged SIDs to regular user accounts is a stealthy way of creating backdoor accounts.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Computer Accounts in Privileged Groups

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning 	6	Privilege Escalation

Description

This indicator looks for computer accounts that are a member of built-in privileged groups.

Likelihood of Compromise

If a computer account is a member of a domain privileged group, then anyone that compromises that computer account (i.e. becomes administrator) can act as a member of that group. Generally speaking, there is little reason for normal computer accounts to be part of privileged groups.

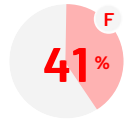
Result

No Evidence of Exposure

Remediation Steps

None

AD INFRASTRUCTURE SECURITY



WEIGHT

7

EVALUATED

10/10

IOE FOUND

8

AD Infrastructure Security indicators pertain to the security configuration of core parts of AD's own infrastructure configuration



SECURITY INDICATOR

Mimikatz DCShadow in use

IOE Found



SEVERITY

Critical



WEIGHT

10

MITRE ATT&CK FRAMEWORK CATEGORY

Persistence, Defense Evasion

Description

Mimikatz's DCShadow switch allows a user who has compromised an AD domain, to inject arbitrary changes into AD using a "fake" domain controller. These changes bypass the security event log and can't be spotted using normal AD tools. This indicator looks for evidence that a machine has been used in this capacity.

Likelihood of Compromise

Mimikatz in an environment is rarely ever a good thing. Indications of this in the domain HAVE the potential to indicate a serious compromise has either occurred OR is in motion.

Result

One or more domains failed this test.

ManagedBy	CreatedDate	DistinguishedName	LastModified
CN=Darren Mar-Elia,OU=Admin,DC=semperissm,DC=lab	12/12/2018 8:44:20 PM	CN=SEMPLABTEST,CN=Computers,DC=semperissm,DC=lab	12/31/2020 10:42:18 AM

Remediation Steps

If a host has been detected that has been used to launch Mimikatz DCShadow attacks, the host should be taken offline to prevent further compromise, and it's logs reviewed to determine the attacking user.



SECURITY INDICATOR

Risky RODC credential caching

IOE Found



SEVERITY

Warning



WEIGHT

5

MITRE ATT&CK FRAMEWORK CATEGORY

Credential Access

Description

On a per-RODC basis, you can control which security principals are allowed to replicate their credentials on an RODC when they logon. If privileged users are in the allow list, that can expose them to credential theft on these RODCs. This indicator looks for a Password Replication Policy that allows privileged objects.

Likelihood of Compromise

Even if a privileged user is in the Password Replication Policy for an RODC, they still have to logon to that RODC for their password to be cached. But, given the general insecure nature of many RODCs (often at sites with poor physical security) this could be trivial to take advantage of once the credentials are cached.

Result

One or more domains failed this test.

DistinguishedName
CN=Matan Liebern,OU=Admin,DC=semperissm,DC=lab
CN=Domain Admins,CN=Users,DC=semperissm,DC=lab
CN=Eduardo Roberts,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Tami Snyder,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Isabella Pickett,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Dan Wright,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Kara Justice,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Eleanor Burton,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Tamera Sims,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Jadyn Harvey,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Harvey Booth,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Elinor Rivera,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Debora Holloway,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Gale Frye,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Jacklyn Galloway,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Gracie Baird,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Dave Marquez,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Kathy Martinez,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Elisa Macias,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Juliet Dudley,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Shari Barber,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Fay Frank,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Ginger Nielsen,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Elena Joyner,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Dale Mcfadden,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Lenore Barr,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Ophelia Estrada,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Danny Huff,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Madelyn Snider,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Geneva Grant,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Candice Rowland,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Jaime Trujillo,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Carolina Armstrong,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Estelle Clay,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Tanisha Le,OU=HR,OU=AMER,DC=semperissm,DC=lab
CN=Herminia Rowe,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab
CN=Susan Hyde,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Marcie Hood,OU=HQ,OU=AMER,DC=semperissm,DC=lab
CN=Millicent Bryan,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Sherrie King,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Candace Stein,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Effie Chase,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=Felicia Pennington,OU=IT,OU=AMER,DC=semperissm,DC=lab
CN=svc AzureADConnect,OU=Admin,DC=semperissm,DC=lab
CN=Joe HelpDesk,OU=Admin,DC=semperissm,DC=lab
CN=Mickey Bresman,OU=Admin,DC=semperissm,DC=lab
CN=Darren Mar-Elia,OU=Admin,DC=semperissm,DC=lab
CN=Administrator,CN=Users,DC=semperissm,DC=lab

Remediation Steps

Privileged users and groups should be removed from RODC password replication policy to prevent those secrets from being replicated to RODCs, which tend to be less secure than read-write DCs. This is managed on a per-RODC basis.



SECURITY INDICATOR

Well-known privileged SIDs in sIDHistory

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	7	Persistence, Privilege Escalation

Description

This indicator looks for all security principals that contain the SIDs of privileged accounts within the sIDHistory attribute. This would allow those security principals to have the same privileges as those privileged accounts, but in a way that is not obvious to see (e.g. through group membership).

Likelihood of Compromise

Writing to sIDHistory requires special privileges. Therefore, anyone who can write to the sIDHistory attribute has likely compromised the domain already, but this method for gaining persistence can be very effective, given the difficulty administrators will have in seeing these kinds of privileged escalations.

Result

Found 11 objects with privileged SIDs inside their sIDHistory [view the full results...](#)

Remediation Steps

Remove SID from the sIDHistory attribute.



SECURITY INDICATOR

Anonymous access to Active Directory enabled

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Critical	7	Initial Access Discovery

Description

It is possible, though not recommended, to enable anonymous access to AD. This indicator looks for the presence of the flag that enables anonymous access. Anonymous access would allow unauthenticated users to query AD.

Likelihood of Compromise

This does not by itself indicate a breach. Anonymous access to Active Directory allows an attacker to enumerate accounts and perform attacks like password sprays and also enumerate the domain to gather information that can model attack paths.

Result

One or more domains failed this test.

DistinguishedName	DSHeuristics	LastModified
CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=semperisssm,DC=lab	0000002	12/11/2020 11:45:35 PM

Remediation Steps

Disable anonymous access unless it is absolutely needed. The dsHeuristics attribute on the CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC= object should be set to disable anonymous access. For more information see [6.1.1.2.4.1.2 dSHeuristics](#)



SECURITY INDICATOR

ZeroLogon vulnerability

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Critical	10	Privilege Escalation

Description

This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthenticated attacker can exploit CVE-2020-1472 to elevate their privileges and get administrative access on the domain.

Likelihood of Compromise

While this exploit was patched by Microsoft, unpatched domain controllers still exist and there is exploit code in the wild that is actively taking advantage of this vulnerability.

Result

Found 5 DCs that are vulnerable to ZeroLogon

DistinguishedName	FQDN
CN=ADSMEU-DC1,OU=Domain Controllers,DC=eu,DC=semperissm,DC=lab	ADSMEU-DC1.eu.semperissm.lab
CN=ADSMEU-DC2,OU=Domain Controllers,DC=eu,DC=semperissm,DC=lab	ADSMEU-DC2.eu.semperissm.lab
CN=ADSM-DC2,OU=Domain Controllers,DC=semperissm,DC=lab	ADSM-DC2.semperissm.lab
CN=ADSM-DC1,OU=Domain Controllers,DC=semperissm,DC=lab	ADSM-DC1.semperissm.lab
CN=ADSM-DC3,OU=Domain Controllers,DC=semperissm,DC=lab	ADSM-DC3.semperissm.lab

Remediation Steps

Patch your servers and make sure that all Microsoft security updates are applied.



SECURITY INDICATOR

Domains with obsolete functional levels

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Reconnaissance

Description

This indicator looks for AD domains that have a domain functional level set to Windows Server 2012-R2 or lower. These lower functional levels mean that newer security features available in AD cannot be leveraged. If the OS version of your domain controllers supports it, you should update to a newer domain functional level to take full advantage of security advancements in AD.

Likelihood of Compromise

While domain functional level is not a weakness in and of itself, an attacker with knowledge of functional levels can adjust their approach to take advantage of lack of security features in AD.

Result

Found 1 domains with low domain functionality level

FunctionalLevel	DomainName
6	semperissm.lab

Remediation Steps

Ensure that your AD domains are running at the highest functional level available for your OS version to ensure access to the latest security improvements. See [Forest and Domain Functional Levels](#).



SECURITY INDICATOR

Anonymous NSPI access to AD enabled

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	6	Initial Access

Description

Anonymous name service provider interface (NSPI) access on AD is a feature that allows anonymous RPC-based binds to AD. This indicator detects when NSPI access is enabled.

Likelihood of Compromise

NSPI access is rarely ever enabled so if you find it enabled, this should be a cause for concern.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

dwAdminSDExMask set on dsHeuristics attribute

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	5	Defense Evasion

Description

This indicator checks if dwAdminSDExMask mask on dsHeuristics has been set, which indicates a change to the SDProp behavior that could

compromise security.

Likelihood of Compromise

Normally the default behavior for AdminSDHolder SDProp should be left intact. If its behavior is modified, this could indicate an attempt at defense evasion.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Computers with older OS versions

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	2	Reconnaissance

Description

This indicator looks for machine accounts that are running versions of Windows older than Server 2012-R2 and Windows 8.1.

Likelihood of Compromise

Computers running older and unsupported OS versions could be targeted with known and or unpatched exploits.

Result

Found 3 computers in the organization that have obsolete OS

DistinguishedName	OperatingSystem	LastLogon
CN=ADSM-DC1,OU=Domain Controllers,DC=semperisssm,DC=lab	Windows Server 2012 R2 Datacenter	1/6/2021 1:01:27 AM
CN=SEMPLABTEST,CN=Computers,DC=semperisssm,DC=lab	Windows Server 2012 R2 Datacenter	12/29/2020 5:46:56 PM
CN=SEMP-RODC1,OU=Domain Controllers,DC=semperisssm,DC=lab	Windows Server 2012 R2 Standard	1/6/2021 2:09:27 PM

Remediation Steps

Where possible, update servers and workstations to later versions with better security features.



SECURITY INDICATOR

Computers and gMSA objects with password last set over 90 days ago

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	6	Credential Access

Description

This indicator looks for computer and group managed service accounts that have not automatically rotated their passwords. These passwords should be changed automatically every 30 days by default.

Likelihood of Compromise

While both computer and gMSA accounts should automatically rotate their passwords every 30 days, objects that are not doing this could show evidence of tampering.

Result

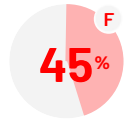
Found 5 computers whose password has not changed in the last 90 days

DistinguishedName	PasswordLastSet
CN=Test1,OU=Computers,OU=AMER,DC=semperisssm,DC=lab	5/23/2018 11:44:45 AM
CN=WINCLIENT1,CN=Computers,DC=semperisssm,DC=lab	10/30/2019 10:20:56 PM
CN=SPLUNKHOST,CN=Computers,DC=semperisssm,DC=lab	6/4/2020 12:37:37 PM
CN=S143999LDA,OU=Computers,OU=AMER,DC=semperisssm,DC=lab	7/13/2020 6:12:33 PM
CN=S1994APP,OU=Computers,OU=AMER,DC=semperisssm,DC=lab	7/13/2020 6:12:48 PM

Remediation Steps

Computers and Managed Service Accounts should change their passwords every 30 days by default, it should be investigated why they did not.

GROUP POLICY SECURITY



WEIGHT

5

EVALUATED

5/5

IOE FOUND

4

Group Policy Security indicators pertain to the security configuration of GPOs and their deployment within AD



SECURITY INDICATOR

Reversible passwords found in GPOs

IOE Found



SEVERITY

Critical



WEIGHT

8

MITRE ATT&CK FRAMEWORK CATEGORY

Credential Access

Description

This indicator looks for GPOs that still contain passwords that can be easily decrypted by an attacker (so called "Cpassword" entries).

Likelihood of Compromise

Many shops stopped using the feature in GP Preferences to set passwords when Microsoft deprecated the feature in Group Policy, but existing password entries may not have been removed. This area is one of the first things attackers look for when they've gained access to an AD environment.

Result

One or more domains failed this test.

GPOName	Domain	PolicyArea	GPOSide
CPassword	semperissm.lab	Local Users and Groups	Computer
CPassword	semperissm.lab	Drives	User

Remediation Steps

If GP Preferences password entries have been found in one or more GPOs, they should be removed immediately. Their encryption key is well known and can be easily cracked, potentially exposing accounts defined in those GPOs.



SECURITY INDICATOR

Weak GPO linking delegation at the domain level

IOE Found



SEVERITY

Warning



WEIGHT

7

MITRE ATT&CK FRAMEWORK CATEGORY

Privilege Escalation, Execution

Description

When non-privileged users can link GPOs at the domain level, they have the ability to effect change across all users and computers in the domain as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-privileged principals who have write permissions on the GPOLink attribute.

Likelihood of Compromise

Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

Result

One or more domains failed this test.

DistinguishedName	Access	Identity
DC=semperissm,DC=lab	Allow: ReadProperty, WriteProperty, GenericExecute on: All Properties	SEMPERISSM\Tier 0 GPO Admins
DC=semperissm,DC=lab	Allow: GenericAll on: All Properties	SEMPERISSM\Enterprise Key Admins
DC=semperissm,DC=lab	Allow: WriteProperty on: gpLink	SEMPERISSM\mickey

Remediation Steps

Unprivileged users should not be able to link GPOs at the domain object level. Doing so essentially gives them the ability to escalate their access, change domain-level security posture and use GPOs to effect all systems and users in AD.



SECURITY INDICATOR

Weak GPO linking delegation at the Domain Controllers OU level

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	7	Privilege Escalation, Execution

Description

When non-privileged users can link GPOs at the Domain Controllers OU level, they have the ability to effect change on domain controllers as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-privileged principals who have write permissions on the GPLink attribute.

Likelihood of Compromise

Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

Result

One or more domains failed this test.

DistinguishedName	Access	Identity
OU=Domain Controllers,DC=semperissm,DC=lab	Allow: GenericAll on: All Properties	SEMPERISSM\Enterprise Key Admins
OU=Domain Controllers,DC=semperissm,DC=lab	Allow: ReadProperty, WriteProperty, GenericExecute on: All Properties	SEMPERISSM\Tier 0 GPO Admins

Remediation Steps

Unprivileged users should not be able to link GPOs at the Domain Controllers OU level. Doing so essentially gives them the ability to escalate their access, change domain-level security posture and use GPOs to effect all systems and users in AD.



SECURITY INDICATOR

Weak GPO linking delegation at the AD Site level

IOE Found



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	7	Privilege Escalation, Execution

Description

When non-privileged users can link GPOs at the AD Site level, they have the ability to effect change on domain controllers as well as potentially elevate access and change domain-wide security posture. This indicator looks for non-privileged principals who have write permissions on the GPLink attribute.

Likelihood of Compromise

Just being able to link GPOs doesn't provide the whole picture. An attacker would need to find or edit a GPO that contains the instructions they want to achieve. However, if an attacker can find an existing GPO that meets their needs, then having this write permission gives them the keys to the kingdom.

Result

One or more domains failed this test.

DistinguishedName	Access	Identity
CN=California,CN=Sites,CN=Configuration,DC=semperissm,DC=lab	Allow: WriteProperty on: gpLink	SEMPERISSM\Desktop Admins

Remediation Steps

Unprivileged users should not be able to link GPOs at the AD Site level. Doing so essentially gives them the ability to escalate their access, change domain-level security posture and use GPOs to effect all systems and users in AD.



SECURITY INDICATOR

Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	4	Privilege Escalation, Execution

Description

The Default Domain Policy and Default Domain Controllers Policy GPOs are special objects within AD, and control domain-wide and Domain Controller wide security settings. This indicator looks for changes to these two special GPOs within the last 7 days.

Likelihood of Compromise

Changes to the Default Domain Policy or Default Domain Controllers Policy should be accounted for by the administrators. If the change can not be accounted for, investigate the change looking for potential weakening of security posture and why the change was made.

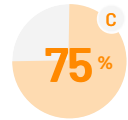
Result

No Evidence of Exposure

Remediation Steps

None

KERBEROS SECURITY



WEIGHT

8

EVALUATED

7/7

IOE FOUND

2

Kerberos Security indicators pertain to the configuration of Kerberos capabilities on computer and user accounts within AD



SECURITY INDICATOR

Computer or user accounts with unconstrained delegation

IOE Found



SEVERITY

Warning



WEIGHT

4

MITRE ATT&CK FRAMEWORK CATEGORY

Privilege Escalation, Credential Access, Lateral Movement

Description

This indicator looks for computer or user accounts that have unconstrained Kerberos delegation defined. Accounts with unconstrained delegation can be more easily targeted for Kerberos-based attacks.

Likelihood of Compromise

Identify and harden accounts if accounts are currently being used for authentication, ensure that the account activity is non-malicious and work to remediate the vulnerable configuration.

Result

One or more domains failed this test.

DistinguishedName	DisplayName	ServicePrincipalName	UserAccountControl
CN=AppServer1,OU=EMEA,DC=eu,DC=semperissm,DC=lab		HOST/AppServer1	528416 [TrustedForDelegation, PasswordNotRequired, WorkstationTrustAccount]
CN=SPLUNKHOST,CN=Computers,DC=semperissm,DC=lab		TERMSRV/SPLUNKHOST	528384 [TrustedForDelegation, WorkstationTrustAccount]

Remediation Steps

Accounts that require Kerberos delegation should be set to constrain that delegation to the particular service or services that require delegation. Attempts should be made to have Kerberos-enabled accounts not be privileged accounts.



SECURITY INDICATOR

Kerberos Golden Ticket susceptibility

IOE Found



SEVERITY

Warning



WEIGHT

4

MITRE ATT&CK FRAMEWORK CATEGORY

Privilege Escalation, Credential Access, Lateral Movement

Description

The krbtgt user account is a special (disabled) user account in every Active Directory domain, that has a special role in Kerberos function. If this account's password is compromised, so-called Golden Ticket attacks can be performed to get access to any resource in a given AD domain. This indicator looks for a krbtgt user account whose password hasn't been changed in the past 180 days.

Likelihood of Compromise

This is a significant issue, but typically requires that an attacker gets access to the krbtgt hash through other compromise methods. This does not directly indicate a compromise but should be remediated.

Result

One or more domains failed this test.

DistinguishedName	PasswordLastSet
CN=krbtgt,CN=Users,DC=eu,DC=semperissm,DC=lab	9/13/2017 1:30:43 PM
CN=krbtgt,CN=Users,DC=semperissm,DC=lab	9/12/2017 5:33:22 PM

Remediation Steps

Microsoft recommends resetting the krbtgt password twice every 180 days to reduce the chance that it could be retrieved and used to generate Golden Tickets. The provide a script to do that here: <https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51>



SECURITY INDICATOR

Privileged users with ServicePrincipalNames defined

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning	5	Privilege Escalation, Credential Access

Description

Similar to injecting privileged account SIDs into the sIDHistory attribute, the Primary Group ID attribute can be used to give a user account stealthy privileged access without explicitly adding them to a privileged group.

Likelihood of Compromise

This is a significant issue that can allow an attacker to elevate privileges in a domain. Audit all accounts where privileged access is possible looking for anomalous access. If found, a breach or ongoing attack should be further investigated.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Computer account takeover through Kerberos resource-based constrained delegation (RBCD)

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	5	Privilege Escalation, Credential Access, Lateral Movement

Description

With sufficient permissions on a computer account and the ability to create another user or computer security principal, it is possible to compromise resources on that computer account using Kerberos resource-based constrained delegation (RBCD). This indicator looks for changes made to the msDS-AllowedToActOnBehalfOfOtherIdentity attribute on computer objects within the last n days to discover if this takeover activity is happening.

Likelihood of Compromise

Identify Kerberos resource-based constrained delegation (RBCD) use requirements and ensure that any credential delegation observed is legitimate and expected.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Users with SPNs defined

Pass



SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational	3	Privilege Escalation

Description

This indicator provides a way to visually inventory all users accounts that have SPNs defined. Generally SPNs are only defined for "Kerberized" services, so if you see an account with an SPN that should not have one, this could be cause for concern.

Likelihood of Compromise

SPNs are generally only defined for service accounts or other services that use Kerberos. If you see it on other accounts, they are worth investigating but it could just be an administrative error.

Result

No Evidence of Exposure

Remediation Steps

None



SECURITY INDICATOR

Objects with Constrained Delegation Configured

Pass

A
100%

SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Informational 	5	Privilege Escalation

Description

This indicator looks for any objects that have values in the msDS-AllowedToDelegateTo attribute (i.e. Constrained Delegation) and does not have the UserAccountControl bit for protocol transition set.

Likelihood of Compromise

While constrained delegation is less likely to be compromised than unconstrained delegation, knowing all of the accounts within your environment that have this defined and ensuring they have strong passwords is a good thing.

Result

No Evidence of Exposure

Remediation Steps

None




SECURITY INDICATOR

Kerberos Protocol Transition Delegation Configured

Pass

A
100%

SEVERITY	WEIGHT	MITRE ATT&CK FRAMEWORK CATEGORY
Warning 	6	Credential Access

Description

This indicator looks for services that have been configured to allow Kerberos protocol transition. This capability basically says that a delegated service can use any available authentication protocol. This means that compromised services can reduce the quality of their authentication protocol to something that is more easily compromised (e.g. NTLM).

Likelihood of Compromise

Protocol transition is not often used but when it is, it should be monitored closely for signs of abuse.

Result

No Evidence of Exposure

Remediation Steps

None

Appendix 1

Domains list

- eu.semperissm.lab
- semperissm.lab

Appendix 2

How do we determine the tests' score

The risk scores included in this report reveal the security posture of the Active Directory environment that was assessed. Risk scores are represented by percentage and letter grade. It is recommended to aim for the highest score possible; a 100% (A) risk score indicates that there were no Indicators of Exposure (IOEs) found for the security indicators that were assessed. The following explanation is intended to help you understand the scoring methodology and factors used to calculate the risk scores presented in this report.

Risk scores:

The Security Assessment report provides the following risk scores:

- **Security Indicator risk score:** Each individual security indicator evaluated is assigned a score according to its internal logic and the results found. The individual security indicator score is assigned a weight (value between 1-10) according to the risk of the IOE found and the likelihood of compromise. This weighted score, together with a general factor of the industry risk, affects the score assigned to the relevant category.
- **Category risk score:** The security indicators included in the tool cover a range of categories that represent different aspects of Active Directory's security posture. The category risk score is based on the test results and weight of each individual security indicator that was evaluated within the relevant category.
- **Overall risk score:** The overall risk score represents the weighted average of the category risk scores.

NOTE: When calculating the risk scores, only security indicators and categories included in the assessment are included (e.g., security indicators that passed and resulting in IOEs found). Security indicators that were not selected, cancelled, or failed to run are not taken into account. For an accurate assessment, it is recommended that you include all security indicators and all domains in the selected forest.

Scoring methods/factors:

Letter grading: Each score is assigned a suitable letter grade according to the following table:

A	90-100
B	80-89
C	70-79
D	60-69
F	0-59

Risk factors: To determine the risk level of a particular security indicator, the following factors are taken into consideration:

- Severity (Informational, Warning, Critical)
- Likelihood of compromise
- The DREAD Threat Probability Matrix

DREAD Threat Probability Matrix

DREAD		High (3)	Medium (2)	Low (1)
Damage potential	How bad would the attack be?	Significant damage: The attacker can subvert the security system and gain full trust authorization.	Moderate damage: The attacker can access/leak sensitive information.	Minimal damage: The attacker can only access/leak trivial information.
Reproducibility	How easy would it be to recreate the attack?	The attack can be consistently reproduced and does not require a specific timing window.	The attack can be reproduced, but only within a specific timing window and in a particular sequence.	The attack is very difficult to reproduce, even with knowledge of the security weakness/vulnerability.
Exploitability	How easy would it be to launch the attack?	A novice programmer could perform the attack with minimal effort.	Requires a skilled programmer to launch the attack and be able to repeat the steps.	Requires an extremely skilled programmer with in-depth knowledge to launch an attack.
Affected users	How many users would be impacted?	A large percentage or all users are impacted; default configuration and key customers are impacted.	A moderate percentage of users are impacted; non-default configuration is impacted.	A very small percentage of users are impacted; anonymous users are affected
Discoverability	How easy would it be for the attacker to discover this exposure?	Easily discovered. Published information explains the vulnerability and attack technique. The vulnerability is found in commonly used features and is very noticeable.	Would require some effort to discover and successfully exploit. The vulnerability is found in a seldomly-used part of the product and only a few users should discover it	Hard to discover. The issue is obscure, and it is unlikely that users would discover a way to cause damage.

Appendix 3

Protected Users group in use result

"DistinguishedName"
"CN=Duane Poole,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab"
"CN=Hazel Bridges,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab"
"CN=Francine Hughes,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab"
"CN=Rosella Nielsen,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab"
"CN=Bruce Buck,OU=IT,OU=EMEA,DC=eu,DC=semperissm,DC=lab"
"CN=Administrator,CN=Users,DC=eu,DC=semperissm,DC=lab"
"CN=Administrator,CN=Users,DC=semperissm,DC=lab"
"CN=Darren Mar-Elia,OU=Admin,DC=semperissm,DC=lab"
"CN=Mickey Bresman,OU=Admin,DC=semperissm,DC=lab"
"CN=svc SAP,OU=Admin,DC=semperissm,DC=lab"
"CN=Joe HelpDesk,OU=Admin,DC=semperissm,DC=lab"
"CN=svc AzureADCconnect,OU=Admin,DC=semperissm,DC=lab"
"CN=Felicia Pennington,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Effie Chase,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Candace Stein,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Sherrie King,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Millicent Bryan,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Marcie Hood,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Susan Hyde,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Herminia Rowe,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Tanisha Le,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Estelle Clay,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Bill Auditor,OU=Admin,DC=semperissm,DC=lab"
"CN=Carolina Armstrong,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Carlene Wilson,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Jaime Trujillo,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Candice Rowland,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Geneva Grant,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Madelyn Snider,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Allyson Patrick,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Danny Huff,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Ophelia Estrada,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Colleen Robertson,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Eva Terrell,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Lenore Barr,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Dale Mcfadden,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Elena Joyner,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Ginger Nielsen,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Selena Evans,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Aline Nielsen,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Fay Frank,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Shari Barber,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Juliet Dudley,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Elisa Macias,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Kathy Martinez,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Rachelle Rosales,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Bad Guy,OU=Bad,DC=semperissm,DC=lab"
"CN=Dave Marquez,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Gracie Baird,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Jacklyn Galloway,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Gale Frye,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Debora Holloway,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Elinor Rivera,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Freddie Curry,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Tabatha Copeland,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Harvey Booth,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Jaclyn Harvey,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Tamera Sims,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Eleanor Burton,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Kara Justice,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Dan Wright,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Isabella Pickett,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Tami Snyder,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Eduardo Roberts,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Carole Castaneda,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Matan Liebern,OU=Admin,DC=semperissm,DC=lab"
"CN=Bill Adams,OU=Admin,DC=semperissm,DC=lab"

Appendix 4

Well-known privileged SIDs in sIDHistory result

"DistinguishedName","SIDHistory"

"CN=Cynthia Meadows,OU=HR,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Byron Mckee,OU=IT,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Theodore Hoover,OU=IT,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Concetta Dudley,OU=HQ,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Connie Byers,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Clare Berg,OU=HQ,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Etta Stanton,OU=IT,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Fay Frank,OU=HQ,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Louis Branch,OU=IT,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Alissa Grant,OU=HR,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

"CN=Cara Caldwell,OU=HQ,OU=AMER,DC=semperissm,DC=lab","S-1-5-21-3072992118-650184829-20450420-519"

Appendix 5

Users with Password Never Expires flag set result

"DistinguishedName","PasswordLastSet","MemberOf","ServicePrincipalName"
"CN=Administrator,CN=Users,DC=eu,DC=semperissm,DC=lab","2/15/2018 7:58:35 AM","CN=Group Policy Creator Owners,CN=Users,DC=eu,DC=semperissm,DC=lab; CN=Domain Admins,CN=Users,DC=eu,DC=semperissm,DC=lab; CN=Administrators,CN=Builtin,DC=eu,DC=semperissm,DC=lab",
"CN=Administrator,CN=Users,DC=semperissm,DC=lab","1/15/2019 7:45:35 PM","CN=ServerPatch_Admins,OU=Admin,DC=semperissm,DC=lab; CN=Message Capture Users,CN=Users,DC=semperissm,DC=lab; CN=Semperis ADSM Service Accounts,OU=Admin,DC=semperissm,DC=lab; CN=Domain Admins,CN=Users,DC=semperissm,DC=lab; CN=Group Policy Creator Owners,CN=Users,DC=semperissm,DC=lab; CN=Administrators,CN=Builtin,DC=semperissm,DC=lab; CN=Schema Admins,CN=Users,DC=semperissm,DC=lab; CN=Enterprise Admins,CN=Users,DC=semperissm,DC=lab; CN=Performance Log Users,CN=Builtin,DC=semperissm,DC=lab",
"CN=Darren Mar-Elia,OU=Admin,DC=semperissm,DC=lab","9/19/2017 8:42:29 AM","CN=ADSM Admins,OU=Admin,DC=semperissm,DC=lab; CN=ADFR Admins,OU=Admin,DC=semperissm,DC=lab; CN=Domain Admins,CN=Users,DC=semperissm,DC=lab; CN=Allowed RODC Password Replication Group,CN=Users,DC=semperissm,DC=lab",
"CN=Mickey Bresman,OU=Admin,DC=semperissm,DC=lab","10/16/2017 1:34:47 PM","CN=Domain Admins,CN=Users,DC=semperissm,DC=lab; CN=Enterprise Admins,CN=Users,DC=semperissm,DC=lab; CN=Allowed RODC Password Replication Group,CN=Users,DC=semperissm,DC=lab",
"CN=svc SAP,OU=Admin,DC=semperissm,DC=lab","10/10/2017 9:17:03 AM","CN=Account Operators,CN=Builtin,DC=semperissm,DC=lab",
"CN=Joe HelpDesk,OU=Admin,DC=semperissm,DC=lab","12/18/2017 9:12:32 AM","CN=Domain Admins,CN=Users,DC=semperissm,DC=lab",
"CN=svc AzureADConnect,OU=Admin,DC=semperissm,DC=lab","12/18/2017 10:18:08 AM","CN=Domain Admins,CN=Users,DC=semperissm,DC=lab",
"CN=Bill Auditor,OU=Admin,DC=semperissm,DC=lab","4/10/2018 12:19:23 PM","CN=AD Auditors,OU=Admin,DC=semperissm,DC=lab",
"CN=TestUser953,OU=HQ,OU=AMER,DC=semperissm,DC=lab","5/4/2018 2:17:12 PM",
"CN=Eloise Roach,OU=HR,OU=AMER,DC=semperissm,DC=lab","5/18/2018 7:14:51 PM","CN=IT Admins--Level 1,OU=Groups,OU=AMER,DC=semperissm,DC=lab",
"CN=ADSN Agent,OU=Admin,DC=semperissm,DC=lab","6/12/2018 1:15:53 PM",
"CN=svc dsp,OU=Admin,DC=semperissm,DC=lab","9/19/2018 8:23:59 AM","CN=Semperis DSP Service Accounts,CN=Users,DC=semperissm,DC=lab",
"CN=Totally L. Pwnd,OU=IT,OU=AMER,DC=semperissm,DC=lab","1/8/2019 11:37:22 AM",

Appendix 6

Unprotected accounts with adminCount=1 result

"DistinguishedName"
"CN=Bill Auditor,OU=Admin,DC=semperissm,DC=lab"
"CN=Carlene Wilson,OU=Branch Office,OU=AMER,DC=semperissm,DC=lab"
"CN=Allyson Patrick,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Colleen Robertson,OU=HQ,OU=AMER,DC=semperissm,DC=lab"
"CN=Eva Terrell,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Selena Evans,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Aline Nielsen,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Bad Guy,OU=Bad,DC=semperissm,DC=lab"
"CN=Freddie Curry,OU=IT,OU=AMER,DC=semperissm,DC=lab"
"CN=Tabatha Copeland,OU=HR,OU=AMER,DC=semperissm,DC=lab"
"CN=Carole Castaneda,OU=HQ,OU=AMER,DC=semperissm,DC=lab"

Appendix 7

Users with old passwords result

"PasswordLastSet","MemberOf","DistinguishedName","ServicePrincipalName"
"9/14/2017 5:04:34 PM","CN=Katherine Aguirre,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Christian Small,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Elvira Peterson,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Kerry Wiggins,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:36 PM","CN=Molly Klein,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:36 PM","CN=Sonja Roach,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:36 PM","CN=Concepcion Le,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Marguerite Massey,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Julie Hamilton,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Lorena Parrish,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Jeanne Butler,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Alisa Lyons,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Fernando Rodgers,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Wade Garza,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Coleen Ramirez,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Richard Graham,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Brent Burch,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Bethany Webb,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Sarah Stevens,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Rowena Lindsey,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Isaac Neal,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Reyna Mcclure,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Gregory Gallegos,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Sofia Fry,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Patrick Palmer,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=Lauri Parker,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=Bobby Shaw,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=Christian Conley,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=Pearl Alexander,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=Vonda Pollard,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=Larry Delgado,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Saundra Preston,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Martina Tillman,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Krystal Mcfadden,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:46 PM","CN=Aurora Parrish,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:46 PM","CN=Randy Day,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:46 PM","CN=Claire Mathis,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:47 PM","CN=Bernice Sloan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:47 PM","CN=Brittney Miller,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:47 PM","CN=Francis Callahan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:48 PM","CN=Crystal Mcpherson,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:48 PM","CN=Katelny Saunders,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:49 PM","CN=Nathan Duncan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:32 PM","CN=Helen Skinner,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:32 PM","CN=Patricia Malone,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:33 PM","CN=Samuel George,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:33 PM","CN=Noreen Carr,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:33 PM","CN=Kristina Lynch,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:34 PM","CN=Johnny Salas,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:34 PM","CN=Celina Smith,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:34 PM","CN=Eula Watson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:34 PM","CN=Lawrence Duke,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Edwin Morton,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Tamera Nixon,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:35 PM","CN=Alexandra O'neill,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:36 PM","CN=Herman Russell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:36 PM","CN=Meagan Wolf,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Daryl Blackwell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Tommie Foreman,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:37 PM","CN=Christian Kennedy,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Evangelina Gregory,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Leta Carter,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:38 PM","CN=Kent Bennett,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Anastasia Powell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Constance Jacobs,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:39 PM","CN=Rochelle Dickerson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Jon Dennis,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Jimmy Haley,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:40 PM","CN=Colette Lawson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Christa Bowen,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Jeff Short,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:41 PM","CN=Leah Stuart,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Sharon York,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Natalia Randolph,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:42 PM","CN=Jasmine Sweet,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=James Cunningham,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=Shelby Hendrix,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:43 PM","CN=Mitchell Sloan,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=David Santana,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=Anthony Rowland,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:44 PM","CN=Cherie Powers,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Fay Rivera,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Cecilia Irwin,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:45 PM","CN=Ashley Ward,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",
"9/14/2017 5:04:46 PM","CN=Kay Ross,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",

Appendix 8

Enabled users that are inactive result

"DistinguishedName","MemberOf","LastLogon"
"CN=Katherine Aguirre,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Christian Small,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Elvira Peterson,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Kerry Wiggins,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Molly Klein,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Sonja Roach,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Concepcion Le,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Marguerite Massey,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Julie Hamilton,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Lorena Parrish,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Jeanne Butler,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Alisa Lyons,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Fernando Rodgers,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Wade Garza,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Coleen Ramirez,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Richard Graham,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Brent Burch,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Bethany Webb,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Sarah Stevens,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Rowena Lindsey,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Isaac Neal,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Reyna Mcdure,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Gregory Gallegos,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Sofia Fry,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Patrick Palmer,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Lauri Parker,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Bobby Shaw,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Christian Conley,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Pearl Alexander,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Vonda Pollard,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Larry Delgado,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Saundra Preston,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Martina Tillman,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Krystal Mcfadden,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Aurora Parrish,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Randy Day,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Claire Mathis,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Bernice Sloan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Brittney Miller,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Francis Callahan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Crystal Mchpherson,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Katelyn Saunders,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Nathan Duncan,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Helen Skinner,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Patricia Malone,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Samuel George,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Noreen Carr,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Kristina Lynch,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Johnny Salas,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Celina Smith,OU=HR,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Eula Watson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Lawrence Duke,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Edwin Morton,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Tamera Nixon,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Alexandra O'neill,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Herman Russell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Meagan Wolf,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Daryl Blackwell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Tommie Foreman,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Christian Kennedy,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Evangelina Gregory,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Leta Carter,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Kent Bennett,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Anastasia Powell,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Constance Jacobs,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Rochelle Dickerson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Jon Dennis,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Jimmy Haley,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Colette Lawson,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Christa Bowen,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Jeff Short,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Leah Stuart,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Sharon York,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Natalia Randolph,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Jasmine Sweet,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=James Cunningham,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Shelby Hendrix,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Mitchell Sloan,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=David Santana,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Anthony Rowland,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Cherie Powers,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Fay Rivera,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Cecilia Irwin,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Ashley Ward,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"
"CN=Kay Ross,OU=HQ,OU=EMEA,DC=eu,DC=semperissm,DC=lab",,"12/31/1600 4:00:00 PM"