Argent Compliance Reports

Sample Reports

GDPR

Table Of Contents

GDPR Computer Management Report

This auditor report shows all computers created, modified, or deleted in Active Directory

This report involves key rights and attributes that may have changed on computers added into any Active Directory container

Unauthorized machines added into the domain, unauthorized rights assigned to machines, or accidental deletions can easily be tracked to find out who, what, where and when the changes were made

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Event Time	Computer Name	Caller User Name	Domain Controller	Remarks
25 Apr 2017 05:14:32	HKNB011	John.Doe	ACME-DC01	Account Disabled
26 Apr 2017 12:26:50	HKNB008	Fred.Smith	ACME-DC01	Account Enabled
26 Apr 2017 14:54:44	HKNB004	Jane.Brown	ACME-DC01	'Password Not Required' - Disabled
26 Apr 2017 14:56:06	HKNB004	Jane.Brown	ACME-DC01	Account Changed
26 Apr 2017 14:58:28	HKNB011	John.Doe	ACME-DC01	Account Enabled
25 Apr 2017 15:17:09	HKNB011	John.Doe	ACME-DC01	Account Disabled
26 Apr 2017 15:22:27	HKNB008	Fred.Smith	ACME-DC01	'Workstation Trust Account' - Enabled
25 Apr 2017 16:33:52	HKNB011	John.Doe	ACME-DC01	Account Changed
26 Apr 2017 16:35:19	HKNB008	Fred.Smith	ACME-DC01	Account Changed

GDPR Domain Controller Activity Report

This audit report shows all authentication requests to the Domain Controller, including both failed and success requests

Administrators must have full visibility on all authentication activity to see if any accounts have been compromised

A security lapse could occur as a result of unsecured accounts or deliberate attacks from intruders

Additionally, this report allows Administrators to see if any existing employees are trying to access critical resources in the domain that they do not have rights to

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)			
Range	Past 14 Days As Of Thu, 27 Apr 2017			
Generated On	Thu, 28 Apr 2017 21:37:06			
Filters	None			
Nodes	**Node**	**Monitoring Group**	**SuperConsole**	
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**	

Logon Time	User Name	Client IP Address	Logon Server	Event Type	Failure Reason
26 Apr 2017 14:35:25	Michelle.Law	10.54.6.108	ACME-DC01	Success	
26 Apr 2017 14:36:11	Mandy.Childs	10.54.6.107	ACME-DC01	Success	
26 Apr 2017 14:42:52	Administrator	10.54.6.123	ACME-DC01	Success	
26 Apr 2017 14:45:13	Administrator	10.54.6.123	ACME-DC01	Success	
26 Apr 2017 14:56:03	Carmen.Pram	10.54.6.104	ACME-DC01	Failure	Pre-authentication information was invalid. Usually means bad password
26 Apr 2017 14:56:06	Carmen.Pram	10.54.6.104	ACME-DC01	Success	
26 Apr 2017 15:09:43	Kay.Clarkson	10.54.6.103	ACME-DC01	Success	
26 Apr 2017 15:15:15	Administrator	10.54.6.123	ACME-DC01	Success	
26 Apr 2017 15:30:23	Administrator	10.54.6.123	ACME-DC01	Success	
26 Apr 2017 17:02:09	Dan.Tisdale	10.54.6.110	ACME-DC01	Success	
26 Apr 2017 17:03:23	John.Doe	10.54.6.178	ACME-DC01	Success	

GDPR GPO Management Report

This audit report shows all Group Policy Objects (GPO) that have been created, modified or deleted, including which attributes have been changed

Group Policy controls critical security measures on the entire domain or specific Organizational Units (OU)

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)			
Range	Past 14 Days As Of Thu, 27 Apr 2017			
Generated On	Thu, 28 Apr 2017 21:37:06			
Filters	None			
Nodes	**Node**	**Monitoring Group**	**SuperConsole**	
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**	

Event Time	User Name	Domain	Message	Remarks
26 Apr 2017 15:00:01	Admin	acme.local	A directory service object was modified: CN={36802C2D-4BD9},CN=Policies,DC=acme,DC=local	Value Added
26 Apr 2017 15:00:01	Admin	acme.local	A directory service object was modified: CN={36802C2D-4BD9},CN=Policies,DC=acme,DC=local	Value Added
26 Apr 2017 15:00:41	Admin	acme.local	A directory service object was modified: cn={36802C2D-4BD9},cn=Policies,DC=acme,DC=local	Value Added
26 Apr 2017 15:00:41	Admin	acme.local	A directory service object was modified: cn={36802C2D-4BD9},cn=Policies,DC=acme,DC=local	Value Deleted
26 Apr 2017 15:00:41	Admin	acme.local	A directory service object was modified: cn={36802C2D-4BD9},cn=Policies,DC=acme,DC=local	Value Added
26 Apr 2017 15:00:41	Admin	acme.local	A directory service object was modified: cn={36802C2D-4BD9},cn=Policies,DC=acme,DC=local	Value Deleted
26 Apr 2017 15:33:54	Admin	acme.local	A directory service object was modified: CN={31B2F340-016D},CN=Policies,DC=acme,DC=local	Value Deleted
26 Apr 2017 15:33:54	Admin	acme.local	A directory service object was modified: CN={31B2F340-016D-11D2},CN=Policies,DC=acme,DC=local	Value Added
26 Apr 2017 15:33:54	Admin	acme.local	A directory service object was modified: CN={31B2F340-016D-11D2},CN=Policies,DC=acme,DC=local	Value Deleted

GDPR Group Management Report

This audit report shows all Domain Groups that have been created, modified or deleted, including which attributes have been changed

Domain Groups control access rights for member users to different machines

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)
Range	Past 14 Days As Of Thu, 27 Apr 2017
Generated On	Thu, 28 Apr 2017 21:37:06
Filters	None

Nodes

Node	Monitoring Group	SuperConsole
*	MG_COMPLIANCE_WINDOWS	WINDOWS

Event Time	Account	Caller User Name	Domain Controller	Messages
26 Apr 2017 14:54:39	Privileged Users	Administrator	ACME-DC01	A security-enabled local group was created.
26 Apr 2017 15:03:12	Privileged Users	Administrator	ACME-DC01	A security-enabled local group was deleted.
26 Apr 2017 15:04:19	Engineers	Administrator	ACME-DC01	A member was added to a security-enabled universal group CN=John.Doe,CN=Users,DC=acme,DC=local
26 Apr 2017 15:05:31	Engineers	Administrator	ACME-DC01	A groups type was changed.
26 Apr 2017 15:06:01	Engineers	Administrator	ACME-DC01	A member was added to a security-enabled universal group CN=Fred.Smith,CN=Users,DC=acme,DC=local

GDPR OU Management Report

This audit report shows all Organizational Units (OU) that have been created, modified or deleted, including which attributes have been changed

OUs are containers on a computer network that allow Administrators to organize groups and users into logical structures

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Event Time	User Name	Domain	Message	Remarks
26 Apr 2017 16:11:30	Administrator	acme.local	A directory service object was modified: OU=Domain Controllers,DC=acme,DC=local	Value Added
26 Apr 2017 17:02:18	Administrator	acme.local	A directory service object was modified: OU=Accounting,DC=acme,DC=local	Value Deleted
26 Apr 2017 17:04:44	Administrator	acme.local	A directory service object was modified: OU=Accounting,DC=acme,DC=local	Value Added
26 Apr 2017 17:08:38	Administrator	acme.local	A directory service object was modified: OU=Support,DC=acme,DC=local	Value Added
26 Apr 2017 17:12:52	Administrator	acme.local	A directory service object was modified: OU=Support,DC=acme,DC=local	Value Deleted

GDPR Domain Policy Changes Report

This audit report shows all critical account policy and password policy changes made, such as account lockouts, password complexity, password length, etc.

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)
Range	Past 14 Days As Of Thu, 27 Apr 2017
Generated On	Thu, 28 Apr 2017 21:37:06
Filters	None

Nodes

Node	Monitoring Group	SuperConsole
*	MG_COMPLIANCE_WINDOWS	WINDOWS

Event Time	Caller User Name	Domain Controller	Remarks
26 Apr 2017 14:49:46	ACME-DC01$	ACME-DC01	Domain Policy was changed: Password Policy
26 Apr 2017 14:55:02	ACME-DC01$	ACME-DC01	Domain Policy was changed: Lockout Policy
26 Apr 2017 14:55:02	ACME-DC01$	ACME-DC01	Domain Policy was changed: Password Policy

GDPR User Management Report

This audit report shows all domain user accounts that have been created, modified or deleted, including which attributes have been changed

User accounts control access into remote machines or even the Domain Controllers

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	MG_COMPLIANCE_WINDOWS	WINDOWS

Event Time	Account	Caller User Name	Domain Controller	Message	Remarks
26 Apr 2017 08:05:02	Dan.Tisdale	Administrator	ACME-DC01	A user account was changed.	Change User Account
26 Apr 2017 15:28:50	Jane.Lee	Administrator	ACME-DC01	A user account was changed.	Change User Account
26 Apr 2017 15:28:50	Jane.Lee	Administrator	ACME-DC01	A user account was created.	Create User Account
26 Apr 2017 15:28:51	Jane.Lee	Administrator	ACME-DC01	A user account was enabled.	Enable User Account
26 Apr 2017 15:28:51	Jane.Lee	Administrator	ACME-DC01	A user account was disabled.	Disable User Account
26 Apr 2017 16:07:55	Test-Account	Administrator	ACME-DC01	A user account was deleted.	Delete User Account

GDPR All File or Folder Changes Report

This audit report shows all file operations (created, modified, deleted) made to servers and paths with file auditing enabled

Critical file paths can be configured on a per-machine basis in the License Manager of Argent for Compliance

Administrators need to maintain full visibility on all changes, which changes were made, and who made the changes

This provides full accountability of actions from employees (or unauthorized users) that have been given the power to perform these privileged user actions

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Event Time	File Server	Object Location	Object Type	Modified Type	Remarks
26 Apr 2017 09:15:32	ACCT-FILE01	E:\Data\Private\Acct\20130201_AP.xls	File	Jane.Clark	File deleted
26 Apr 2017 09:16:09	ACCT-FILE01	E:\Data\Private\HR\Job_Ad.doc	File	Jim.Smith	File modified
26 Apr 2017 09:17:11	ACCT-FILE01	E:\Data\Private\HR\IT\New Folder	Folder	Jim.Smith	Folder created
26 Apr 2017 09:17:11	ACCT-FILE02	E:\Data\Public\WS051.xls	File	Fred.Smith	File modified
26 Apr 2017 10:36:46	ACCT-FILE02	E:\Data\Public\WS051 - Copy.xls	File	Fred.Smith	File deleted
26 Apr 2017 12:15:23	ACCT-FILE02	E:\Data\Private\Acct\20121105_AP.xls	File	Fred.Smith	File deleted

GDPR Logon Duration Report

This audit report shows the logon duration of all users. Users that are still logged on at the time of report generation are marked as "Not Logged Off Yet"

This report helps Administrators understand where, when, and how long users were logged in on a particular machine for

This report also provides insight into the work patterns, absence and attendance of employees based on their logon duration

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Logon Time	Logon Server	User Name	Client IP Address	Client Host Name	Logon Duration	Logon Type
26 Apr 2017 07:04:48	ACME-DC01	John.Doe	10.54.6.178	ACME-DC01	00:01:31	Interactive
26 Apr 2017 14:42:52	ACME-DC01	Administrator	10.54.6.110	ACME-DC01	00:01:30	Interactive
26 Apr 2017 15:22:31	ACME-DC01	Administrator	10.54.6.110	ACME-DC01	01:17:05	RemoteInteractive
26 Apr 2017 15:49:09	ACME-DC01	Fred.Smith	10.54.6.201	ACME-DC01	00:42:07	RemoteInteractive

GDPR Logon Failures Report

This audit report shows all logon failures on the target machines

The presence of a few login failure records is completely normal – users sometimes have fat fingers

But if there are an unusually high number of logon failures, this may indicate a brute force hacker attack

Some logon failures help prompt Administrators to give attention to the user, such as accounts that have been accidentally locked out, password expirations or time restrictions set on the accounts

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Logon Time	User Name	Client IP Address	Client Host Name	Logon Type	Remarks
26 Apr 2017 07:18:33	Bob.Hart	10.54.6.110	HKNB010	Interactive	Unknown user name or bad password.
26 Apr 2017 07:21:03	John.Doe	10.54.6.202	HKNB005	RemoteInteractive	The user has not been granted the requested logon type at this machine.
26 Apr 2017 09:00:34	Bob.Hart	10.54.6.58	HKNB063	RemoteInteractive	Unknown user name or bad password.
26 Apr 2017 09:02:17	Bob.Hart	10.54.6.58	HKNB063	RemoteInteractive	Unknown user name or bad password.
26 Apr 2017 09:02:39	Bob.Hart	10.54.6.58	HKNB063	RemoteInteractive	Unknown user name or bad password.
26 Apr 2017 09:02:57	Bob.Hart	10.54.6.58	HKNB063	RemoteInteractive	Unknown user name or bad password.
26 Apr 2017 10:17:08	Jane.Lee	10.54.6.99	HKNB017	Interactive	The user has not been granted the requested logon type at this machine.

GDPR User Logon Activity Report

This audit report shows all logon/logoff events on all machines, including both successful and failed logons

This audit report is grouped by server, then by logon time

This report helps to paint the entire picture of logon/logoff access across all machines

Successful logins are not always a good thing -- especially if an account was not supposed to have access to a particular machine in the first place

The presence of a few login failure records is completely normal – users sometimes have fat fingers

But if there are an unusually high number of logon failures, this may indicate a brute force hacker attack

Some logon failures help prompt Administrators to give attention to the user, such as accounts that have been accidentally locked out, password expirations or time restrictions set on the accounts

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:06		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Logon Time	User Name	Client IP Address	Client Host Name	Logon Type	Event Type	Failure Reason
26 Apr 2017 07:04:48	John.Doe	10.54.6.178	HKNB035	RemoteInteractive	Successful Logon	
26 Apr 2017 09:02:13	Bob.Hart	10.54.6.58	HKNB063	RemoteInteractive	Failure	Unknown user name or bad password
26 Apr 2017 14:42:52	Administrator	10.54.6.110	ACME-DC01	RemoteInteractive	Successful Logon	
26 Apr 2017 15:22:31	Administrator	10.54.6.110	ACME-DC01	RemoteInteractive	Successful Logon	
26 Apr 2017 15:45:21	Jane.Lee	10.54.6.93	HKNB099	Interactive	Failure	The user has not been granted the requested logon type at this machine
26 Apr 2017 15:51:57	Administrator	10.54.6.62	HKNB023	RemoteInteractive	Successful Logon	
26 Apr 2017 16:18:02	Jane.Lee	10.54.6.93	HKNB099	RemoteInteractive	Failure	Unknown user name or bad password

GDPR Process Tracking Report

This audit report shows all processes that have been created and terminated on the target machine

This report allows Administrators to effectively keep an eye on unauthorized programs that are launched by users

This provides accountability if users are running destructive programs that are consuming network bandwidth or resources on the machine

Additionally, viruses and malware can be spotted

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:07		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Event Time	Machine Name	Account Name	Image File Name	Remarks
26 Apr 2017 15:51:05	ACME-DC01	Administrator	C:\Windows\System32\mmc.exe	A process has been created.
26 Apr 2017 15:51:07	ACME-DC01	Administrator	C:\Windows\System32\mmc.exe	A process has exited.
26 Apr 2017 15:53:30	ACME-DC01	Administrator	C:\Windows\System32\mmc.exe	A new process has been created.
26 Apr 2017 15:53:50	ACME-DC01	Administrator	C:\Windows\System32\mmc.exe	A process has exited.
26 Apr 2017 15:53:54	ACME-DC01	Administrator	C:\Windows\System32\gpupdate.exe	A new process has been created.
26 Apr 2017 15:54:57	ACME-DC01	Administrator	C:\Windows\System32\gpupdate.exe	A process has exited.
26 Apr 2017 16:00:25	ACME-DC01	Dan.Tisdale	C:\App\TSTheme.exe	A process has exited.
26 Apr 2017 16:10:01	ACME-DC01	ACME-DC01$	C:\App\Google\GoogleUpdate.exe	A new process has been created.
26 Apr 2017 16:10:02	ACME-DC01	ACME-DC01$	C:\App\Google\GoogleUpdate.exe	A process has exited.
26 Apr 2017 16:13:32	ACME-DC01	ACME-DC01$	C:\Windows\System32\TSTheme.exe	A new process has been created.

GDPR Scheduled Tasks Report

This audit report shows all scheduled Windows tasks, when they last ran, and remarks on the execution status

This report allows Administrators to effectively keep an eye on unauthorized Windows tasks that are running, or if Windows tasks are running at incorrect times or frequencies

This provides accountability if users are scheduling destructive scripts or batch files that are consuming network bandwidth or resources on the machine

Viruses and malware often keep themselves "alive" through scheduled Windows tasks -- these can easily be spotted with this critical report

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)		
Range	Past 14 Days As Of Thu, 27 Apr 2017		
Generated On	Thu, 28 Apr 2017 21:37:07		
Filters	None		
Nodes	**Node**	**Monitoring Group**	**SuperConsole**
	*	**MG_COMPLIANCE_WINDOWS**	**WINDOWS**

Event Time	Machine Name	Account Name	Task Name	Remarks
26 Apr 2017 14:57:09	ACME-DC01	Administrator	Sync-Backups	A scheduled task was created.
26 Apr 2017 15:02:06	ACME-DC01	Administrator	Sync-Backups	A scheduled task was updated.
26 Apr 2017 15:22:40	ACME-DC01	Administrator	Reminders-SMS-Job	A scheduled task was deleted.
26 Apr 2017 16:03:21	ACME-DC01	Administrator	Reminders-SMS-Job	A scheduled task was created.

GDPR Terminal Sessions Report

This audit report shows all remote terminal service logons on the target machines

Terminal service logons are identified as "RemoteInteractive" logons internally in the Event Logs

This report helps to paint the entire picture of logon/logoff terminal access across all machines

Successful logins are not always a good thing -- especially if an account was not supposed to have access to a particular machine in the first place

The presence of a few login failure records is completely normal – users sometimes have fat fingers

But if there are an unusually high number of logon failures, this may indicate a brute force hacker attack

Some logon failures help prompt Administrators to give attention to the user, such as accounts that have been accidentally locked out, password expirations or time restrictions set on the accounts

Time Zone	All Times In Server Time, UTC -5 (Adjusted for Daylight Savings)
Range	Past 14 Days As Of Thu, 27 Apr 2017
Generated On	Thu, 28 Apr 2017 21:37:07
Filters	None

Nodes

Node	Monitoring Group	SuperConsole
*	MG_COMPLIANCE_WINDOWS	WINDOWS

Event Time	Terminal Server	Domain	User Name	Client IP Address	Client Host Name	Remarks
26 Apr 2017 07:04:48	ACME-DC01	ARGENT	John.Doe	10.54.6.178	ACME-DC01	An account was successfully logged on
26 Apr 2017 07:05:00	ACME-DC01	ARGENT	Fred.Smith	10.54.6.178	ACCT-FILE03	A session was reconnected to a Window Station. Session: RDP-Tcp#0
26 Apr 2017 07:06:19	ACME-DC01	ARGENT	John.Doe	10.54.6.178	ACME-DC01	An account was logged off
26 Apr 2017 07:29:44	ACME-DC01	ARGENT	Fred.Smith	10.54.6.178	ACCT-FILE03	A session was disconnected from a Window Station. Session: RDP-Tcp#0
26 Apr 2017 14:42:52	ACME-DC01	ARGENT	Administrator	10.54.6.110	ACME-DC01	An account was successfully logged on
26 Apr 2017 14:42:59	ACME-DC01	ARGENT	Administrator	10.54.6.110	HKNB010	A session was reconnected to a Window Station. Session: RDP-Tcp#0