

DLP Safetica

Procedimento de instalação e utilização

Código	Proc-10
Versão	V2023.1
Data da Versão	02/02/2023
Criado por	André Iesca Rodrigues
Aprovado por	Douglas Santos Torres de Oliveira ME
Nível de confidencialidade	Interno

Histórico de alterações

Data Alteração	Versão	Alterado por	Descrição alteração		
20/10/2024	V2024.1	Danilo Goes	Revisão		



https://yup.chat



Sumário

DLP	Safetica	1
Proc	edimento de instalação e utilização	1
Histo	órico de alterações	1
1	Introdução	3
2	instalação	3
3	Instalando Safetica em um servidor:	3
4	Safetica Management Console	4
4	Como desinstalar Safetica Client / Safetica Agent	5
5	configurações	7
POL	ITICAS DLP	7
6	Como criar políticas DLP no Safetica	8
7	Configuração da política	8
8	Regras da política	9
9	Aplicação da política	9
10	Como as políticas são avaliadas	10
11	Tipos de política	11
12	modos de política	11
13	Visão geral da regra de política	12
14	Informações gerais sobre WebSafetica	19





1 INTRODUÇÃO

DLP significa "Data Loss Prevention" e é uma tecnologia usada para prevenir vazamentos acidentais ou intencionais de informações confidenciais. A solução Safetica é uma das opções de software de DLP que oferece recursos para proteger dados empresariais importantes, tais como restrições de acesso, criptografia, monitoramento de rede e outros. O objetivo principal é garantir a segurança e a privacidade dos dados da empresa e protegê-los de acessos não autorizados ou de vazamentos acidentais.

2 INSTALAÇÃO

Antes de iniciar a utilização da Solução DLP Safetica, é necessário realizar a instalação e configuração do software. Para isso, siga as seguintes etapas:

- Acesse o site da Safetica e faça o download do software;
- Siga as instruções do assistente de instalação;
- Ao concluir a instalação, acesse a interface de administração da solução;
- Configure as políticas de proteção de dados de acordo com as necessidades da sua empresa.

3 INSTALANDO SAFETICA EM UM SERVIDOR:

- 1. Baixe o pacote de instalação Safetica para o servidor a partir deste link: <u>https://downloads.safetica.com/safetica_setup.exe</u>
- 2. Execute o arquivo de instalação e selecione Instalação automática (recomendado).

Dica: Se você já possui um banco de dados SQL instalado, escolha Instalação manual para instalar cada componente separadamente e conectar o Safetica ao seu servidor. Por favor, siga as instruções no Manual de Instalação Safetica.

- 3. Clique em Avançar para confirmar o Contrato de licença , os requisitos de hardware e os termos de licença do SQL Server .
- 4. Clique em Instalar na tela Pronto para instalar para iniciar a instalação automática do servidor MS SQL Express, Safetica Management Service e Safetica Management Console.
- 5. A instalação pode levar até 30 minutos. Assim que o processo estiver concluído, reinicie o servidor conforme exigido pela instalação do MS SQL Server.



4 SAFETICA MANAGEMENT CONSOLE

Em seguida, execute o Safetica Management Console e faça a configuração inicial e a implantação dos endpoints:

- 1. Execute *o console de gerenciamento Safetica* . A configuração inicial será iniciada automaticamente.
- Verifique a configuração do servidor SMTP (você pode usar as configurações padrão) e digite sua senha de administrador. Isso será usado para acessar o *Safetica Management Console* no futuro. *Nota: A senha não pode ser recuperada se for perdida.*
- 3. Importe o Active Directory, se necessário. Se você não tiver um domínio configurado em sua rede, pode pular esta etapa.

 Clique em Get Downloader Agent e execute este arquivo em pelo menos um terminal. Você precisará distribuir este arquivo para todos os endpoints que serão protegidos pelo Safetica. *Nota: Todas as outras ações nos endpoints serão feitas remotamente usando o Downloader Agent. Dica: você pode implantar o Downloader Agent em seus endpoints no domínio usando uma política de GPO. Para obter mais detalhes, consulte o Manual do usuário ou este artigo. Você também pode usar uma ferramenta de administração remota, por exemplo, <u>ESET PROTECT</u>.*

- 5. Depois de instalar o *Safetica Downloader Agent* em pelo menos um computador, você verá esse computador no *Safetica Management Console*.
- Clique em Registrar endpoints automaticamente . O Safetica Client será instalado em todos os endpoints disponíveis com o Safetica Downloader Agent . Observação: você precisará reinicializar esses endpoints para concluir a instalação.
- 7. Prossiga para a próxima etapa e insira sua chave de licença Safetica.
- 8. Selecione seu perfil padrão preferido e clique em Iniciar proteção .

Depois de concluir a configuração inicial, você poderá acessar todos os recursos do *Safetica Management Console* e visualizar os dados dos endpoints. Recomendamos começar a explorar Safetica com o módulo *Discovery*, que contém todos os recursos de monitoramento e logs de auditoria. Isso lhe dará uma boa base para entender e gerenciar Safetica.





4 COMO DESINSTALAR SAFETICA CLIENT / SAFETICA AGENT

Tanto o Safetica Client quanto o Safetica Agent podem ser desinstalados diretamente no Safetica Management Console.

1. Abra o *Safetica Management Console* e vá para **Manutenção** > **Atualizar** e implantar.

Safetica ONE											-	5 x
DASHEGARD		REPORTS			DISCOVE		WERSAFETICA			ROFLE	SUPPORT	
Endpoint overview	Update an	d deploy Endpoint de	ctivation Integr	ation settings	Endpoint settings	Information collection	n Database management	Access management	License management Categori	rs Comput	er utilization	
+ 7	9	Settings Records									?	×
K, Sample company												1
		V SERVER UPDATE										
			LLMENT									
		All the servers are up	to date. Please upda	te endpoints.								1
		Install version 10.3.3	9 on endpoints Ad	vanced endpoin	t management							- 1
		(and the second s		1640	100	in the second						- 1
		Computer	Operating system	Status	version	Version status						- 1
		PV-EN	Windows Server 201	5 Inactive	9.3.92	Outdated						- 1
		fdgfdsgudgf	Windows 10	Active	10.3.39	Up-to-date						- 1
		· · /			O of 0 ×							- 1
		Use this button to pe	mare the Downloade	Aneritnackane	Deploy the apent to all e	ndonints manually, or e.a.	usina a GPO policy in your Active	Desitory				- 1
		Windows Asset	MacOS Agent Mac	75 limited feature	etet							- 1
	10000	V UPDATE OPTION	E									
	0											

2. Clique **em Gerenciamento de terminal avançado** e, em seguida, clique em **Desinstalar** .

3. Na seção **Configurações de ação**, selecione se deseja desinstalar apenas **Safetica Client** ou **Safetica Client e Safetica Agent.**

Se você desinstalar apenas o **Safetica Client**, nenhuma auditoria ou proteção funcionará. Você poderá instalar o Safetica Client de volta no terminal a qualquer momento.

YUP CHAT - [Restrito - SI/TI] 5



Se você desinstalar **o Safetica Client e o Safetica Agent** , nenhuma auditoria ou proteção funcionará e o Safetica será removido do terminal.



4. Na próxima etapa, selecione de quais **computadores ou grupos** de computadores você deseja executar a desinstalação.

Safetica ONE						- • ×
DASHBOARD		NEPORTS	S Select computers X		PROFILE	G SUPPORT
+ Y K Semple company	8	Endpoint management > Add action 1. Action setting: 2. Computers and groups 1. Specify the additional settings for which you want to unitable COMPUTERS AND GROUPS Extent computers and groups Computer (group) Other Computer (group) (No iterral)	Image: Second		Net	?
	Q,			111100	1000	Carto

 Reinicialize o nó de extremidade e a desinstalação será concluída. Você pode verificar o status da desinstalação em Gerenciamento avançado de endpoints ou na Visão geral de endpoints na seção Manutenção.





Safetica ONE												- ×
E.	◬	Ø		,©	\bigtriangledown				0		٩	
DASHEGARD	ALERTS	REPORTS		DISCOVERY	PROTECTION	WEBSAFETICA			MAINTENANCE	PROFILE	SUPPOR	1
												6
+ v	Ş									2 1	×	~
K Sample company		Go back to Update and deploy										- 1
		ACTIONS SETTINGS										
		Updates are available for dow	nloading and installation in view <u>Update a</u>	d deploy-								
		Install / update Uninstall										
		Installations in progress court	e 0									
		Installation errors count:	0									
		Computer / group	Action				Package Force re	rboot Total pcs - r	ucceeded / waiting for a	boot / failed /	18	
		PC-Nowak	 Uninstall Safetica Client 					■ No 0-0/0/0	/0		Remo	•
												- 1
	,0											~

 Após a desinstalação, você verá a versão 0.0.0 do Safetica Agent e Safetica Client na visão geral do endpoint na seção de manutenção.

5 CONFIGURAÇÕES

POLITICAS DLP

Aqui poderá conhecer melhor como as políticas dlp e regras relacionadas funcionam no safetica one para controlar vários canais de comunicação.

O Safetica ONE usa políticas DLP para proteção de dados em endpoints e para controlar o comportamento do aplicativo.

Cada política DLP consiste em um **tipo** de **política, modo** de política e **regras de política**. As políticas DLP podem ser definidas no **Console de gerenciamento Safetica** em **Proteção** > **Políticas DLP**.

Neste artigo, você aprenderá mais sobre:

<u>Como as políticas são avaliadas</u>
<u>Tipos de política</u>
<u>modos de política</u>
<u>Visão geral da regra de política</u>

https://yup.chat

YUP CHAT – [Restrito – SI/TI] 7



6 COMO CRIAR POLÍTICAS DLP NO SAFETICA

Use políticas DLP para proteger dados em endpoints e controlar o comportamento do aplicativo.

Abra o **Console de gerenciamento Safetica** e vá para **Proteção > Políticas DLP**.

Clique no botão **Nova política** . A criação da política consiste em 3 etapas:

- 1. Configuração da política
- 2. <u>Regras da política</u>
- 3. Aplicação da política

7 CONFIGURAÇÃO DA POLÍTICA

Insira o nome da política, a descrição e escolha seu tipo (Geral, Dados, categoria Aplicativo).

Para **políticas de categoria de aplicativo**, escolha a categoria de aplicativo desejada clicando no botão **Selecionar categoria**.

Para **políticas de dados**, escolha as categorias de dados desejadas clicando no botão **Adicionar categoria**.

As políticas que combinam vários tipos de categorias de dados são rotuladas como **Várias categorias de dados** na lista de políticas DLP. Se você clicar em tal política, verá as categorias de dados específicas que ela inclui à direita em **Detalhes da política** > **Categorias**.

	ALERTS	REPORT		DISCOVE		sue		WEBSAF	ETICA	K MAINTI			SUPPOR	ar.
logs DLP pol	icies Data c	ategories	Zones Disk guard Devic	e control Bitlocker c	evices Bitlocker	r disks								
+	7	0										?	×	
ENUSE				N N										
			DLP policies configure more information in th	the data security in your e le <u>Safetica knowledge base</u>	nvironment. Policies	manag	e general da	a flow, spec	ific data or applica	tions, and they offer DLP actions from sile	ent logging t	to strict blocking	g. You can fir	nd
			First match applies.					^	POLICY DETAIL	s				
			Policy	Туре	Mode				Name	Multiple policy				ī
			1 Multiple policy	Multiple data categories	Block	Edit	Remove		Destation					
			\$ SK_mac_netwrix_CCPA	Data category	Log	Edit	Remove		Description:					
			1 SK_mac_netwrix_CM	Data category	Log	Edit	Remove		Type:	Multiple data categories				
			\$ SK_mac_netwrix_Cre	Data category	Log	Edit	Remove		Categories:	Portugal ID, ERP export, DP - Metadata				
			1 SK_mac_netwrix_Fina	Data category	Log	Edit	Remove		Made	Log and block				
			\$K_mac_netwrix_GDPR	Data category	Log	Edit	Remove		Mode	Log and block				
			1 SK_mac_netwrix_GDP	. Data category	Log	Edit	Remove		Shadow copy:	Disable				
			I SK_mac_netwrix_GLBA	Data category	Log	Edit	Remove		Policy applied to:	Cloud users				
			I SK_mac_netwrix_HIPP	A Data category	Log	Edit	Remove							
			\$K_mac_netwrix_PCI	Data category	Log	Edit	Remove		POLICY RULES					
			1 SK_mac_netwrix_PHI	Data category	Log	Edit	Remove			200000000				-
			\$K_mac_netwrix_PII	Data category	Log	Edit	Remove		Cloud drives:	Block				
			1 DP - general block	General	Block	Edit	Remove		Upload:	Block				
			1 MK_exclusive	Data category	Block	Edit	Remove	1.00	E mail	Plack				
			1 FTcontent	Data category	Block or override	Edit	Remove		E-main	DIOCK				
			I Peronal information	Data category	Block	Edit	Remove		Instant messaging	F Block				
			1 SK_Content	Data category	Log	Edit	Remove		External devices:	Block				
			I SK_General	General	Log	Edit	Remove							
			IM_test_pol	Data category	Notify	Edit	Remove							
			1 Policy name	General	Log	Edit	Remove							
			I IL content scan white.	. General	Log	Edit	Remove							
			1 PB TEst	General	Log	Edit	Remove							
			1 Policy name	General	Log	Edit	Remove							

YUP CHAT - [<u>Restrito - SI/TI</u>] 8



8 REGRAS DA POLÍTICA

Selecione o modo de política e as regras de política .

Para visualizar todas as regras disponíveis, clique em **Personalizar**. Verifique as regras que deseja definir e elas serão colocadas na lista.

Você também pode usar o menu suspenso **Modelo de política para criar uma nova política DLP.** Esses modelos são grupos predefinidos de regras. Cada nova política cria um novo modelo que você pode usar posteriormente ao criar outras políticas DLP.

<mark>Ş</mark> Safetica ONE			_				
DASHBOARD	ALERTS		s DISCOVERY PROTE				
DLP logs DLP pol	icies Data d	ategories	Zones Disk guard Device control Bitlocker devices B	itlocker disks			
+	8	0	DLP policies > Create/edit security policy				?
⊯ VENUSE			1. Policy configuration 2. Policy rules	3. Apply policy			
			POLICY MODE				
			Policy mode:	ide: Enable			
			Shadow copy: Enable	Security policy		×	
			POLICY RULES	Select policy rules			
			Policy template: Built-in: Basic rules	 Customize Rules 		<u> </u>	
			Starter template with basic rules fo	or important data channels.			
			Cloud drives: Block or override	Google Drive			
			Upload: Block or override	OneDrive Business OneDrive Personal		- 11	
			E-mail: Block or override	SharePoint			
			Instant messaging: Block or override	Upload to file share Upload to web mail			
			External devices: Block or override	☑ Upload			
			Learn more in the Safetica Knowledge Base	E-mail Remove al	0//		
			-		OK C	Jancel	
		Q			Previous	Next	Finish Cancel

9 APLICAÇÃO DA POLÍTICA

Clique **em Adicionar usuários**. Na árvore de usuários, escolha um usuário ou grupo ao qual deseja aplicar a política DLP fornecida.

Depois de clicar em **Concluir**, você verá a política na parte inferior da lista de políticas.





BASIC INFORMATIC	N							
DLP policies configure the Safetica knowledge								
the Safetica knowledge	the data security in you	ur environment. Policies	s manage	general da	ta flow, s	specific data or applic	ations, and they offer DLP actions from silent logging to strict blocking. You can find more informatio	n in
	e base.							
New policy								
First match applies.						∧ POLICY DETAI	ILS	
Policy	Туре	Mode				Name:	Multiple policy	
Peronal information	Data category	Block	Edit	Remove		Description:		
SK_Content	Data category	Log	Edit	Remove		Description.		
SK_General	General	Log	Edit	Remove		Туре:	Multiple data categories	
JM_test_pol	Data category	Notify	Edit	Remove		Categories:	Portugal ID, ERP export, DP - Metadata	
Policy name	General	Log	Edit	Remove		Martin	Die de la constante	
JL content scan white	General	Log	Edit	Remove		Mode:	block of overfide	
PB TEst	General	Log	Edit	Remove		Shadow copy:	Enable	
Policy name	General	Log	Edit	Remove		Policy applied to	Cloud users	
FTmetadata	Data category	Block	Edit	Remove				
mktestcontent	Data category	Block	Edit	Remove				
JL_override_test_restri	. Data category	Disable	Edit	Remove				-
JL_override_test_cont	Data category	Disable	Edit	Remove		Cloud drives:	Block or override	
JL_override	General	Disable	Edit	Remove		Upload:	Block or override	
DP - context allow	Data category	Log	Edit	Remove				
TS Variable	Data category	Log	Edit	Remove		E-mail:	BIOCK OF OVERTIDE	
TS context policy	Data category	Block	Edit	Remove	-	Instant messagin	ng: Block or override	
TS General	General	Log	Edit	Remove		External devices:	Block or override	
FTexisting	Data category	Log	Edit	Remove		and an and the set of the set		
FTcontext	Data category	Notify	Edit	Remove				
FTgeneral	General	Log	Edit	Remove				
JV content policy	Data category	Block	Edit	Remove				
Default_SensContent	Data category	Notify	Edit	Remove				
Default_ExistClass_Po	. Data category	Notify	Edit	Remove				
Default_SafMetadata	. Data category	Notify	Edit	Remove				
Default_Context_Policy	Data category	Notify	Edit	Remove				
Default_General	General	Log	Edit	Remove				
FTpolBug	General	Log	Edit	Remove				
FInicnedelajici	Data category	Log	Edit	Remove				
FTSčŕžý	Data category	Log	Edit	Remove				
		Disal, as social is	T alte	D				

10 COMO AS POLÍTICAS SÃO AVALIADAS

As políticas DLP no Safetica ONE são priorizadas e avaliadas de cima para baixo na lista de políticas DLP. Ao alterar a ordem das políticas, você também altera sua prioridade durante a avaliação.

房 Safetica	ONE										
DASH	HBOARD	ALERTS	REPORTS	DISCO		SUPERVISOR	WEBSAFETICA				
DLP logs	DLP policie	s Data ca	tegories Zones Disk	guard Device control	Bitlocker devices	Bitlocker disks					
+	Ą	0								? ×	\sim
,ø VENU:	SE			ATION							
			DLP policies config find more informa	gure the data security in you tion in the Safetica knowled	r environment. Policies n ge base.	manage general data fl	ow, specific data or applica	tions, and they offer DLP actions from silent I	ogging to stri	t blocking. You	can
			New policy								
			🛕 First match applie	25.			A POLICY DETAIL	S			
			Policy	Туре	Mode	<u></u>	Name:	SK_mac_netwrix_CCPA			
			\$K_mac_netwrix_C	CPA Data category	Log	Edit Remove	Description:				
			\$K_mac_netwrix_C	M Data category	Log	Edit Remove	Teres	Data automore			
			I SK_mac_netwrix_C	re Data category	Log	Edit Remove	iype:	Data category			
			I SK_mac_netwrix_F	ina Data category	Log	Edit Remove	Categories:	CCPA			
			I SK_mac_netwrix_G	DPR Data category	Log	Edit Remove	Mode:	Log only			
			I SK_mac_netwnx_G	DP Data category	Log	Edit Remove	Shadow come	Dirable			
			I SK_mac_netwnx_G	LBA Data category	Log	Edit Remove	snadow copy:	Disable			
			I SK_mac_netwnx_F	IIPPA Data category	Log	Edit Kemove	Policy applied to:	PVMB			
			I SK_mac_netwnx_P	CI Data category	Log	Edit Remove					
			I SK_mac_netwnx_P	Data category	Log	Edit Remove	∧ POLICY RULES				
			I SN_mac_netwnx_P Multiple policy	Multiple data category	Plack or override	Edit Remove	Cloud drives:	Log			
			introluple policy	multiple data categor.	block of overfide	cuit Nemove		-			

Como as políticas de DLP são avaliadas:

•Cada política contém uma ou mais regras (por exemplo, para upload, e-mail, dispositivos externos, etc.).

YUP CHAT - [Restrito - SI/TI] 10

•Cada regra é avaliada e aplicada separadamente.





•A primeira correspondência sempre se aplica.

•As ações que não são especificadas em uma política serão gerenciadas por outras políticas colocadas mais abaixo na lista de políticas DLP.

Exemplo: quando uma política é encontrada com uma regra de primeira correspondência para upload, a ação atribuída será executada e o upload não será mais avaliado. A avaliação continuará, no entanto, para outras operações (por exemplo, para e-mail ou dispositivos externos). Elas serão avaliadas por políticas colocadas mais abaixo na lista até que uma primeira correspondência seja encontrada.

As exceções específicas do usuário às políticas podem ser configuradas criando uma nova política DLP, atribuindo-a ao usuário e colocando-a acima das políticas mais gerais.

11 TIPOS DE POLÍTICA

Existem três tipos de políticas DLP no Safetica :

- Políticas gerais gerencie os canais de comunicação selecionados como um todo, por exemplo, todos os dados enviados por e-mail, todos os dados enviados, todos os dados copiados para dispositivos externos etc. As políticas gerais são ótimas para definir limitações gerais do que é permitido e do que não é.
- Políticas de dados gerencie e proteja categorias de dados específicas e suas combinações, por exemplo, números de cartão de crédito, expressões regulares, exportações de CRM, etc.
- Políticas de aplicativos gerencie aplicativos e seu comportamento. Eles são aplicados a categorias de aplicativos. Para gerenciar um único aplicativo, crie uma nova categoria de aplicativo para ele e aplique sua política a essa categoria. As políticas de aplicativos estão disponíveis apenas no Safetica ONE Enterprise. Cópias de sombra não são suportadas por políticas de aplicativos.

Recomendamos colocar políticas DLP gerais e outras menos rígidas na parte inferior da lista. Políticas mais específicas e rígidas podem ser colocadas na parte superior.

12 MODOS DE POLÍTICA

Cada política DLP pode ser definida para 4 modos diferentes que afetam como as regras de política são aplicadas:





- •**Desativado** a política é definida, mas não afeta nada. Este modo é útil quando você prepara uma política que só será aplicada posteriormente.
- •Log only a política audita e registra ações restritas e permitidas.
- Registrar e notificar o usuário é notificado sobre a execução de ações restritas, que também são registradas se executadas. As ações permitidas são registradas apenas. O Safetica ONE não registra: Excluir, Criar, Renomear, Copiar/Mover em um armazenamento físico (exceções: o destino é uma pasta na nuvem; a regra DLP é aplicada à operação).
- •**Registrar e bloquear** as ações restritas são totalmente bloqueadas e registradas. As ações permitidas são registradas apenas.

Regra de política	Descrição	Limitações
Unidades de nuvem	Transferência de arquivos de computadores locais para unidades de nuvem por meio de clientes de sincronização ou interface da web. Pode ser definido para unidades de nuvem em geral ou apenas para unidades de nuvem especificadas (Box, Google Drive, Dropbox, OneDrive Personal, OneDrive Business, SharePoint). Disponível para todas as apólices.	O macOS ainda não oferece suporte ao Box, mas oferece suporte ao iCloud.

13 VISÃO GERAL DA REGRA DE POLÍTICA





Regra de política	Descrição	Limitações
Carregar	Uploads de arquivos via navegador da web para todos os sites, independentemente de sua categoria. Você também pode escolher regras mais específicas Carregar para compartilhamento de arquivo e Carregar para webmail , que são aplicadas somente a sites categorizados como Hospedagem de arquivos e Web mails , respectivamente. O upload também afeta o envio de arquivos por meio de sites de mensagens instantâneas e o upload de arquivos para unidades de nuvem no navegador da web. Disponível para políticas gerais e de dados.	No macOS , as restrições DLP para upload geral funcionam apenas no Safari e no Chrome
O email	Envio de e-mails de clientes de e- mail de desktop. Disponível para políticas gerais e de dados.	Não se aplica ao web mail. No macOS , as restrições DLP funcionam no macOS12+ e apenas para e-mails enviados via Mail.app.
Mensagem instantânea	Envio de arquivos por meio de aplicativos de mensagens instantâneas ou sites categorizados como aplicativos da Web de mensagens instantâneas . Disponível para políticas gerais e de dados.	Aplica-se apenas a arquivos enviados, não a mensagens.



Regra de política	Descrição	Limitações
Dispositivos externos	Transferência de arquivos para dispositivos externos. Disponível para todas as apólices.	Aplica-se apenas a dispositivos conectados como armazenamento em massa USB.
Compartilhamento de arquivos de rede	Transferência de arquivos para compartilhamentos de arquivos de rede. Disponível para políticas gerais e de dados.	Zonas ainda não suportadas para macOS
transferência remota	Transferência remota de arquivos e operações da área de transferência usando estes aplicativos: Microsoft Remote Desktop e Team Viewer . Disponível para políticas gerais e de dados.	Não bloqueia conexões de área de trabalho remota em geral.
<u>git</u>	Executando git push (ou seja, upload de dados de diretórios locais para repositórios Git remotos). Disponível para políticas gerais.	<u>As cópias de</u> <u>sombra</u> não são criadas para o controle do Git.



https://yup.chat

12-T



Regra de política	Descrição	Limitações
Outra conexão de rede	Todo o tráfego de rede, exceto para compartilhamentos de arquivos de rede. Atenção: Ao escolher o modo Log and block , é possível cortar completamente um endpoint da rede. Extremo cuidado deve ser tomado para não definir esta regra incorretamente. Disponível para políticas de aplicativos e políticas de dados do tipo de contexto.	Esta é uma configuração especializada, que pode afetar negativamente a conectividade. As cópias de sombra não são criadas para outras conexões de rede. <u>A substituição do usuário não</u> está disponível para outra conexão de rede. Essas operações serão bloqueadas, mesmo quando a substituição estiver habilitada.
Imprimir	Impressão em geral, inclusive impressão virtual. Você também pode escolher a regra mais específica Impressão virtual , que se aplica apenas à impressão virtual em arquivos. Disponível para todas as apólices.	As cópias de sombra ainda não foram criadas para impressão e impressão virtual. A substituição do usuário não está disponível para impressão e impressão virtual. Essas operações serão bloqueadas, mesmo quando a substituição estiver habilitada.





Regra de política	Descrição	Limitações
		O macOS não suporta impressão virtual .
Prancheta	Copiar texto e imagens de aplicativos restritos via área de transferência. No modo Log e bloco , as operações da área de transferência são permitidas dentro do aplicativo que possui os dados, mas as transferências para outros aplicativos são bloqueadas. Disponível para políticas de dados e aplicativos.	As cópias de sombra não são criadas para operações da área de transferência. A substituição do usuário não está disponível para a área de transferência. Essas operações serão bloqueadas, mesmo quando a substituição estiver habilitada. Essas operações não são registradas. Se você criar uma política somente de log , ela não executará nenhuma ação.



I.I.



Regra de política	Descrição	Limitações
Captura de tela	Capturas de tela, compartilhamento de tela e gravação de tela. Disponível para políticas de dados e aplicativos.	As cópias de sombra não são criadas para operações de captura de tela.
		A substituição do usuário não está disponível para captura de tela. Essas operações serão bloqueadas, mesmo quando a substituição estiver habilitada.
		Essas operações não são registradas. Se você criar uma política somente de log , ela não executará nenhuma ação.
Caminhos locais	Acesso a caminhos especificados em unidades locais. Aviso: Ao escolher o modo Log e bloqueio , é possível cortar completamente um destino de todo o acesso. Extremo cuidado deve ser tomado para não definir esta regra incorretamente.	Esta é uma configuração especializada, que pode afetar negativamente o fluxo de trabalho do usuário.
	Disponível para políticas de aplicativos e políticas de dados do tipo de contexto. Esta regra está disponível apenas no Safetica Enterprise.	As cópias de sombra não são criadas para caminhos locais.



T



Regra de política	Descrição	Limitações
Acesso exclusivo	Lista branca ou lista negra de aplicativos para acessar dados confidenciais. Permite determinar quais aplicativos podem ou não funcionar com dados confidenciais. Aviso: Ao escolher o modo Log e bloqueio , é possível cortar	Esta é uma configuração especializada, que pode afetar negativamente o fluxo de trabalho do usuário.
	completamente certos aplicativos dos dados que eles podem precisar para funcionar corretamente. Extremo cuidado	sombra não são criadas para acesso exclusivo.
	deve ser tomado para não definir esta regra incorretamente.	A substituição do usuário não está disponível para
	Para habilitar o acesso exclusivo para um aplicativo específico, crie uma nova categoria de aplicativo para ele.	acesso exclusivo. Essas operações serão bloqueadas, mesmo quando a
	Disponível para políticas de dados do tipo de contexto.	substituição estiver habilitada.
	Esta regra está disponível apenas no Safetica Enterprise.	Só pode ser definido para categorias de aplicativos inteiras.

YUP CHAT – [<u>Restrito – SI/TI</u>] 18

https://yup.chat



14 INFORMAÇÕES GERAIS SOBRE WEBSAFETICA

O WebSafetica é usado para exibir visões gerais e registros diários e para administração básica do Safetica. As configurações avançadas e a administração são realizadas por meio do console da área de trabalho.



1. Funções e configurações

Aqui você pode alternar entre funções e configurações do WebSafetica.

2. Árvore do usuário

A árvore contém grupos, usuários e computadores, assim como o console da área de trabalho, que pode ser usado para editar a árvore.

3. Intervalo de tempo dos dados exibidos

O calendário pode ser usado para ajustar o intervalo de tempo para o qual os dados devem ser exibidos.

4. Área de exibição

Esta área exibe gráficos, registros e configurações da mesma forma que no console da área de trabalho.

Mais informações sobre Safetica você pode encontrar na página da web support.safetica.com



YUP CHAT - [Restrito - SI/TI] 19

https://yup.chat