

Configuração Entra ID para Bloqueio Office 365

Bloqueio Office 365

Para que o CtrlStation possa aplicar o bloqueio de usuários no Office 365, é necessário efetuar a configuração dentro do Portal Azure (<https://portal.azure.com>) do Entra ID. Para isto basta seguir os passos abaixo.


Configuração Azure

Criação Grupo Azure AD

Primeiro é necessário criar um grupo no Azure AD. Este grupo será controlado inteiramente pelo CtrlStation **não devem ser adicionados usuários manualmente**. Para criar o grupo:

1. Acessar o Portal Azure AD
2. Acessar o menu "Grupos" na página inicial

[Página inicial](#) > [Grupos](#)

 **Grupos** | Todos os grupos ...

LAB3 DVLP

Novo grupo Download de grupos Atualizar Gerenciar o modo de exibição Excluir Tem comentários

Visão Geral (Versão Prévia)

Todos os grupos

Grupos excluídos

Diagnosticar e resolver problemas

Configurações

Atividade

Solução de Problemas e Suporte

O Azure Active Directory agora é Microsoft Entra ID. [Saiba mais](#)

Pesquisar

Adicionar filtro

Modo de busca Contém

3 grupos encontrados

<input type="checkbox"/>	Nome ↑	Id de Objeto	Tipo de grupo
<input type="checkbox"/>	 All Company	0cdc815d-0d62-4c8e-8d4b-a93175bd05d5	Microsoft 365

3. Clicar em "Novo Grupo" e preencher conforme imagem abaixo:

Novo Grupo

Tem comentários?

Tipo de grupo * ⓘ

Segurança

Nome do grupo * ⓘ

CtrlStation - Bloqueados

Descrição do grupo ⓘ

Usuários bloqueados pelo CtrlStation

As funções do Microsoft Entra podem ser atribuídas ao grupo ⓘ

Sim

Não

Tipo de associação * ⓘ

Atribuído

Proprietários

Nenhum proprietário selecionado

Membros

Nenhum membro selecionado

4. Clicar em "Criar" e atualizar a lista de grupos para que o grupo seja exibido:

<input type="checkbox"/>	Nome ↑	Id de Objeto	Tipo de grupo	Tipo de associação	Email	Fonte
<input type="checkbox"/>	All Company	0cdc815d-0d62-4c8e-8d4b-a93175bd05d5	Microsoft 365	Atribuído	allcompany@lab3dvp.onmicrosoft.com	Nuvem
<input checked="" type="checkbox"/>	CtrlStation - Usuários Bloqueados	e9f3a4dc-0e8d-42c6-bffc-aa3125301348	Segurança	Atribuído		Nuvem

5. Copiar o valor da coluna "ID Objeto" e salvar para configuração posterior no CtrlStation

Criação Política Entra ID

Com o grupo criado, podemos seguir com a configuração da política do Entra ID. Para isto:

1. Acessar a tela "Acesso Condicional" pela busca ou menu:

Página inicial >

Acesso Condicional | Visão geral

Microsoft Entra ID

◁ + Criar nova política + Criar nova política com base em modelos Atualizar Tem comentários?

- Visão geral
- Políticas
- Insights e relatórios
- Diagnosticar e resolver problemas
 - Gerenciar
 - Monitoramento
 - Solução de Problemas e Suporte

Criar, gerenciar e monitorar as políticas de Acesso Condicional.

O Acesso Condicional é a ferramenta utilizada pelo Microsoft Entra ID para reunir sinais, tomar decisões e impor políticas organizacionais.

[Saiba mais](#)

2. Clicar em "Criar nova política" e preencher conforme os passos a seguir

3. Preencher o nome e na opção "Usuários" clicar e então selecionar "Selecionar usuários e grupos" e então marcar "Usuários e Grupos" e selecionar o grupo criado anteriormente:

Novo ...

Política de Acesso Condicional

Controlar o acesso com base na política de Acesso Condicional para reunir sinais, tomar decisões e aplicar políticas organizacionais.

[Saiba mais](#)

Controle o acesso com base em a quem a política se aplicará, como usuários e grupos, identidades de carga de trabalho, funções de diretório ou convidados externos. [Saiba mais](#)

Nome *

CtrlStation - Bloqueio

Atribuições

Usuários ⓘ

Usuários específicos incluídos

Recursos de destino ⓘ

Nenhum recurso de destino selecionado

Rede **NOVO** ⓘ

Não configurado

Condições ⓘ

0 condições selecionadas

Controles de acesso

Incluir Excluir

- Nenhum
- Todos os usuários
- Selecionar usuários e grupos

Usuários convidados ou externos ⓘ

Funções do diretório ⓘ

Usuários e grupos

Selecionar

1 grupo

C- CtrlStation - Usuários Bloque... ...

4. No item "Recursos de destino" selecionar "Todos os aplicativos em nuvem":

Novo ...

Política de Acesso Condicional

Controlar o acesso com base na política de Acesso Condicional para reunir sinais, tomar decisões e aplicar políticas organizacionais.

[Saiba mais](#)

Nome *

CtrlStation - Bloqueio ✓

Atribuições

Usuários ⓘ

[Usuários específicos incluídos](#)

Recursos de destino ⓘ

[Todos os aplicativos em nuvem](#)

Rede **NOVO** ⓘ

[Não configurado](#)

Condições ⓘ

[0 condições selecionadas](#)


Controle o acesso com base em todo ou específico tráfego de acesso à rede, aplicativos ou ações na nuvem. [Saiba mais](#)

Selecione a que se aplica essa política

Aplicativos de nuvem

Incluir Excluir

- Nenhum
- Todos os aplicativos em nuvem
- Selecionar aplicativos

 Não perca o acesso. Essa política afeta o portal do Azure. Antes de continuar, verifique se você ou outra pessoa poderá retornar ao portal. Ignore este aviso se você estiver configurando a política de sessão do navegador persistente que funciona corretamente somente quando "Todos os aplicativos de nuvem" estão selecionados. [Saiba mais](#)

5. No item "Conceder" selecionar "Bloquear Acesso":

Conceder



Controlar a imposição de acesso para bloquear ou permitir acesso. [Saiba mais](#)

Bloquear acesso

Permitir acesso

Exige a autenticação multifator

Exigir força de autenticação

Exigir que o dispositivo seja marcado como em conformidade

Exigir dispositivo ingressado no Microsoft Entra híbrido

Exigir o aplicativo cliente aprovado
[Ver a lista de aplicativos do cliente aprovado](#)

Exigir a política de proteção de aplicativo
[Ver a lista de aplicativos do cliente protegidos por política](#)

Para vários controles

Exigir todos os controles selecionados

Exigir um dos controles selecionados

Novo ...

Política de Acesso Condicional

Controlar o acesso com base na política de Acesso Condicional para reunir sinais, tomar decisões e aplicar políticas organizacionais.

[Saiba mais](#) 

Nome *


CtrlStation - Bloqueio



Atribuições

Usuários 

[Usuários específicos incluídos](#)

Recursos de destino 

[Todos os aplicativos em nuvem](#)

Rede **NOVO** 

[Não configurado](#)

Condições 

[0 condições selecionadas](#)

Controles de acesso

Conceder 

[Bloquear acesso](#)

Sessão 

[0 controles selecionados](#)

6. Por fim, alterar a opção "Habilitar Política" para "Ativado":

Habilitar política

Somente relatório

Ativado

Desativado

Criar

7. Clicar em "Criar"

Revisão #1

Criado 16 setembro 2024 14:55:51 por Felipe Weckx

Atualizado: 16 setembro 2024 15:09:38 por Felipe Weckx