Integração do fSense com Microsoft Azure Active Directory

Sumário:

Integração do fSense com dados do Microsoft Entra ID (Azure Active Directory)

Objetivo

Este documento tem como objetivo detalhar o processo de integração entre o fSense e o Microsoft Entra ID (Azure AD), visando a otimização da gestão de recursos humanos e monitoramento de dispositivos na organização. A integração permitirá a busca e sincronização dos dados de usuários e dispositivos do Azure AD com o fSense, com foco na representação dos Usuários como Pessoas.

Além disso, a integração também visa possibilitar a sincronização da hierarquia de Equipes, caso as informações de Departamento e Gerente estejam definidas no Azure AD. Isso proporcionará uma visão mais abrangente da estrutura organizacional da empresa dentro do fSense, facilitando o gerenciamento de equipes de acordo com a hierarquia estabelecida no Azure AD.

Com essa integração, esperamos melhorar a eficiência operacional, garantir a segurança da rede e dos dados, e possibilitar uma tomada de decisão mais informada por parte dos gestores, ao fornecer dados atualizados e precisos sobre usuários e estrutura organizacional diretamente no fSense.

Benefícios da Integração

1. **Centralização de Dados**: A integração permite centralizar os dados de usuários e dispositivos do Azure AD no fSense, proporcionando uma visão unificada e abrangente da infraestrutura de TI da organização.
2. **Monitoramento Eficiente**: Ao integrar o estado de monitoramento dos dispositivos do Azure AD ao fSense, os administradores podem evitar que dispositivos desativados na Organização continuem como monitorados no fSense
3. **Identificação Precisa de Usuários e Dispositivos**: A integração garante a precisão na identificação de usuários e dispositivos.

Dados Necessários do Azure AD para Configuração no fSense

Para configurar a integração entre o fSense e o Azure AD, os seguintes dados são necessários:

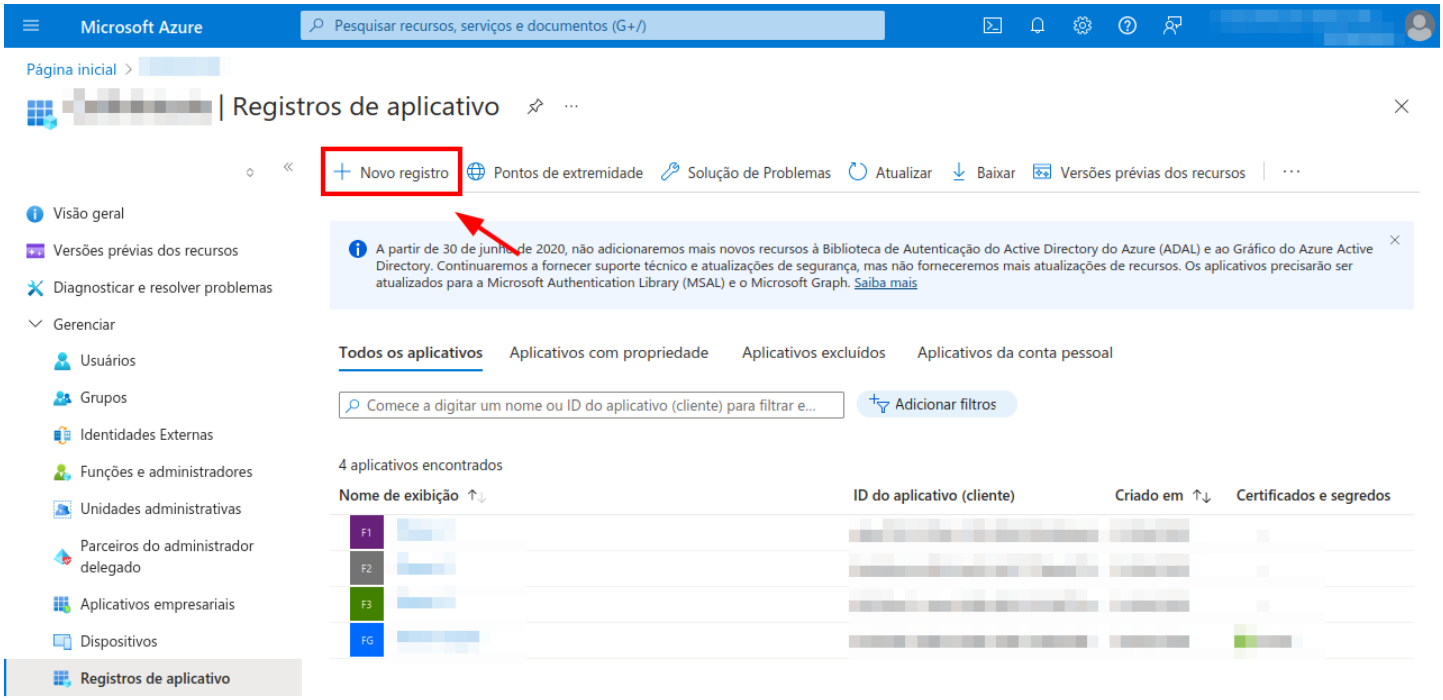
1. **ID do Locatário (Tenant) do Azure AD**: O ID único que identifica o locatário (tenant) do Azure AD associado à organização.
2. **ID do Cliente (Client ID)**: O ID exclusivo atribuído à aplicação registrada no Azure AD, que será usada para autenticar e autorizar a integração com o fSense.
3. **Segredo do Cliente (Client Secret)**: A chave secreta usada pela aplicação registrada no Azure AD para autenticar-se ao solicitar tokens de acesso.
4. **Permissões de Leitura de Usuário e Dispositivo**: As permissões necessárias para acessar os dados de usuários e dispositivos do Azure AD. Isso deve incluir permissões de leitura para usuários e dispositivos, conforme necessário para a integração.

Configuração necessária no Azure

Passo 1 - Acesse sua instância do AD no portal do Azure

- Acesse o portal do Azure em **https://portal.azure.com/**.
- Procure pelo serviço **Azure Active Directory** e acesse.

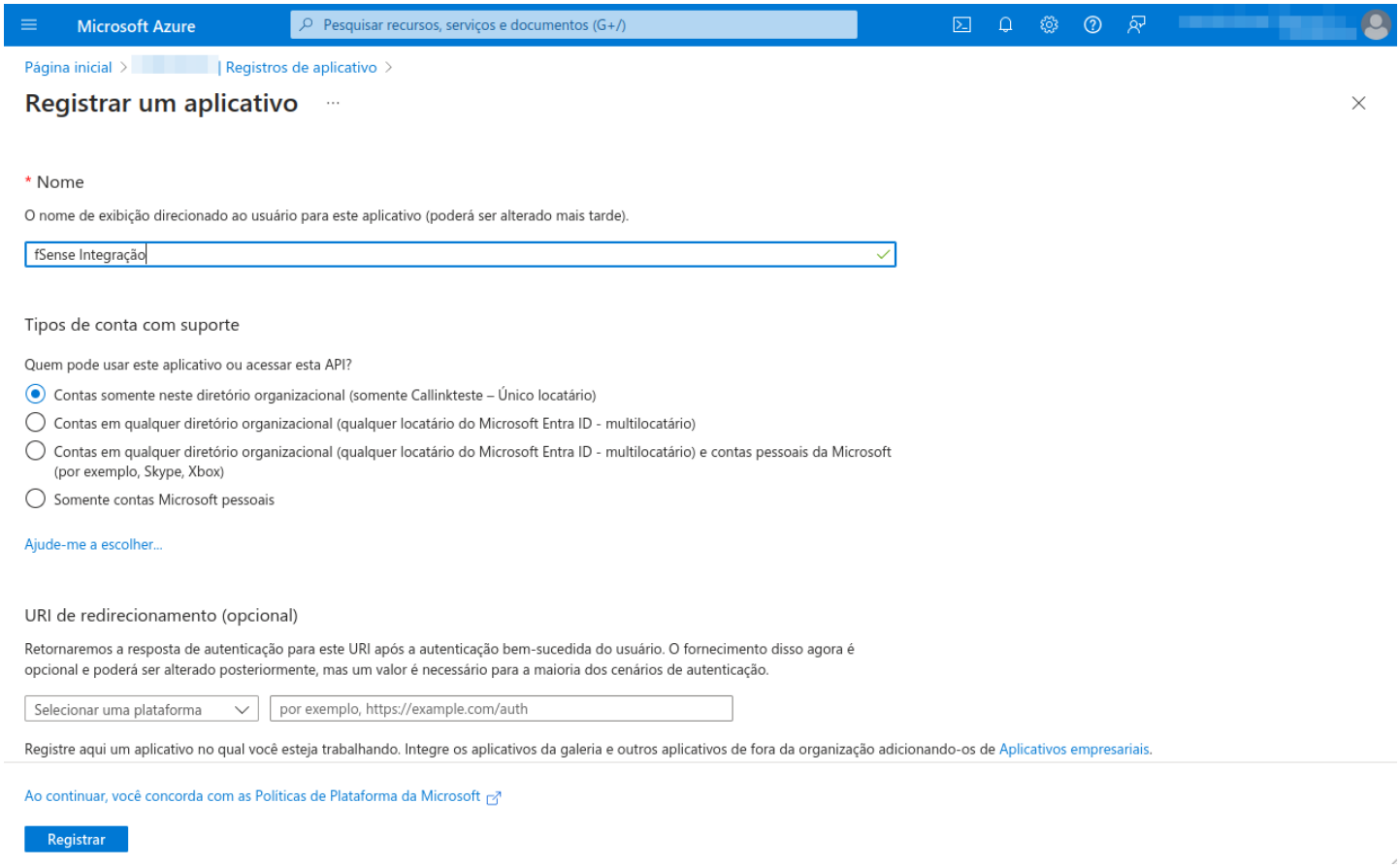
Passo 2 - Acesse Registros de aplicativo e na página do menu clique em Novo registro



Portal Azure AD - Registro de Aplicativos

Passo 3 - Criação do aplicativo

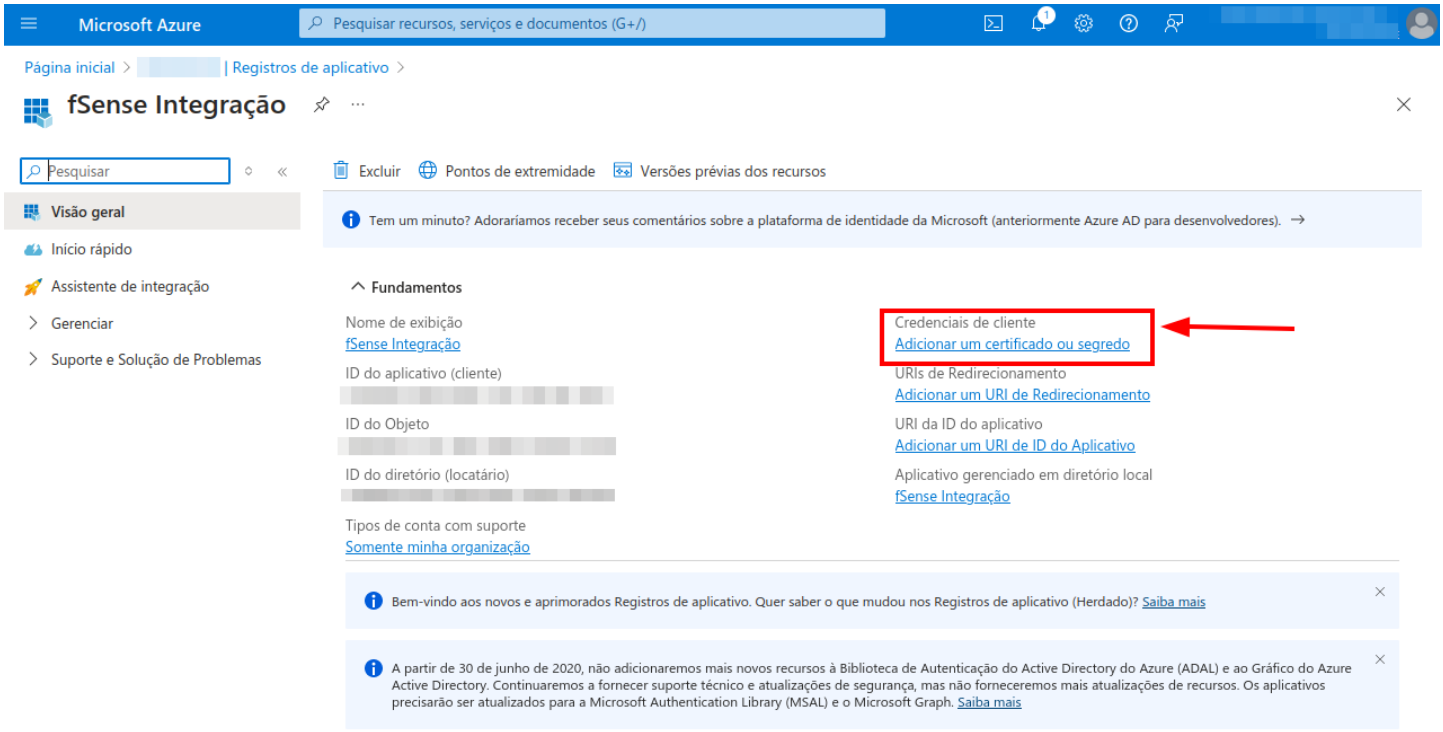
Digite um nome para o aplicativo e clique em Registrar. Para melhor identificação, sugerimos que coloque uma descrição que o vincule ao fSense.



Portal Azure AD - Criação Novo Aplicativo

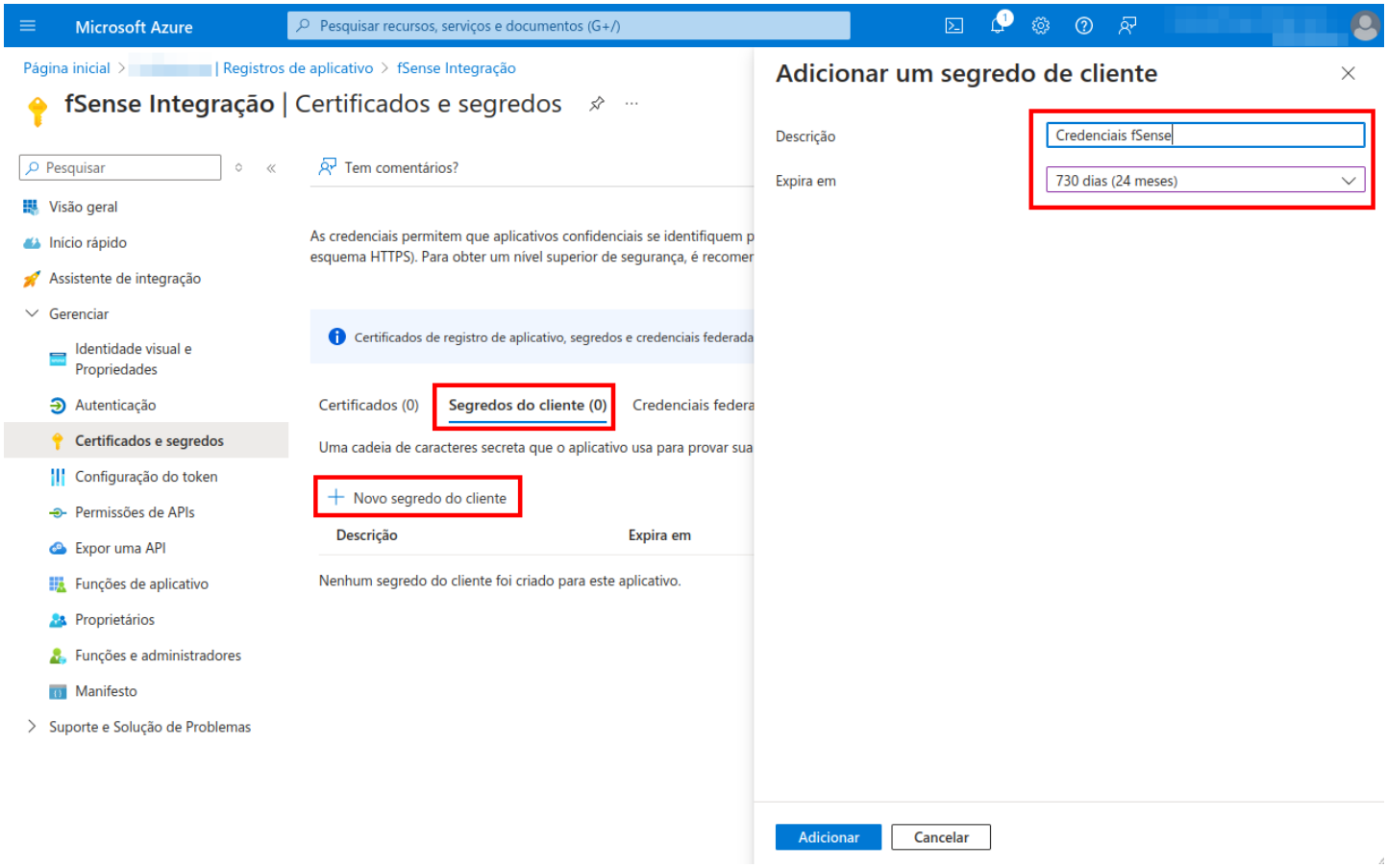
Passo 4 - Adicionando chaves de acesso

Na página do aplicativo, clique em Adicionar um certificado ou segredo



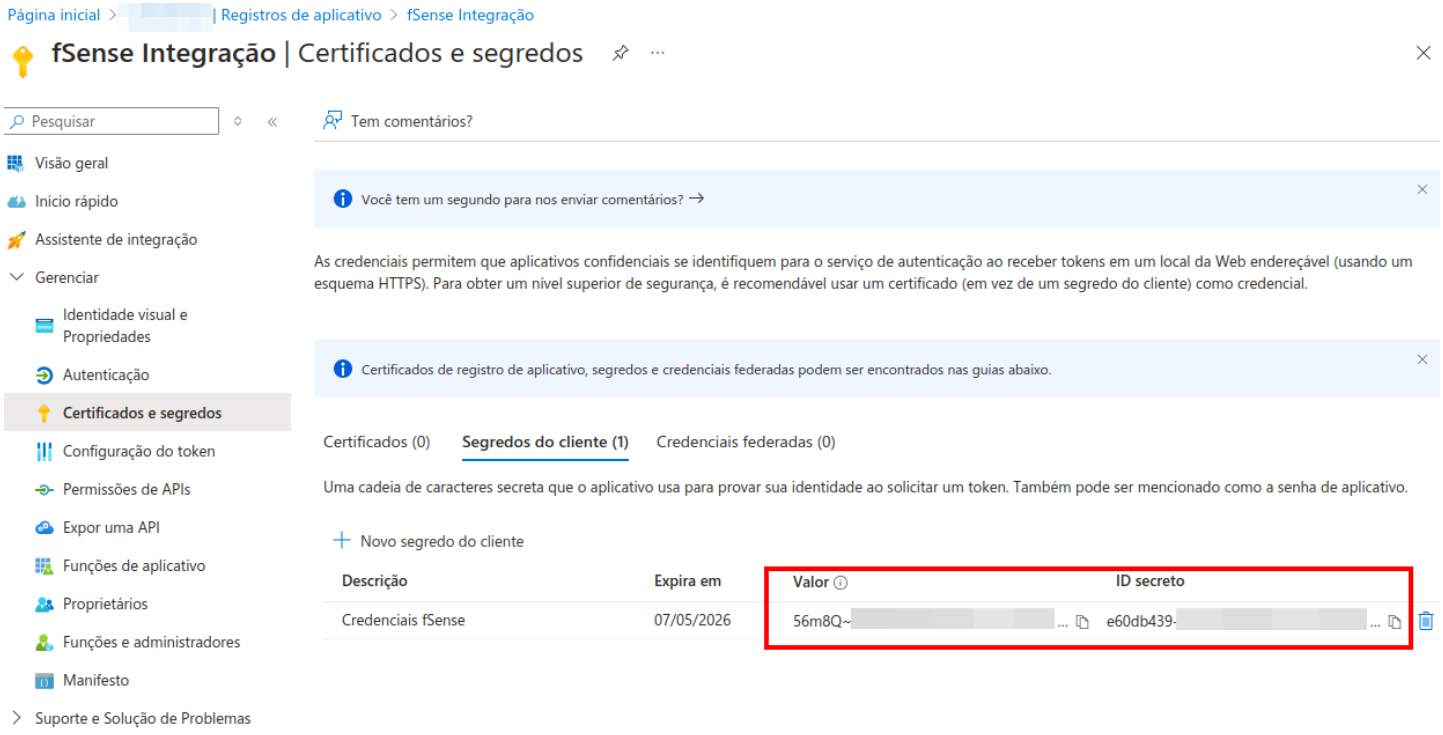
Portal Azure AD - Adicionando credenciais

Na aba Segredos do cliente clique em +Novo Segredo do cliente, defina uma Descrição e o tempo de expiração.



Portal Azure AD - Adiciona Segredo do Cliente

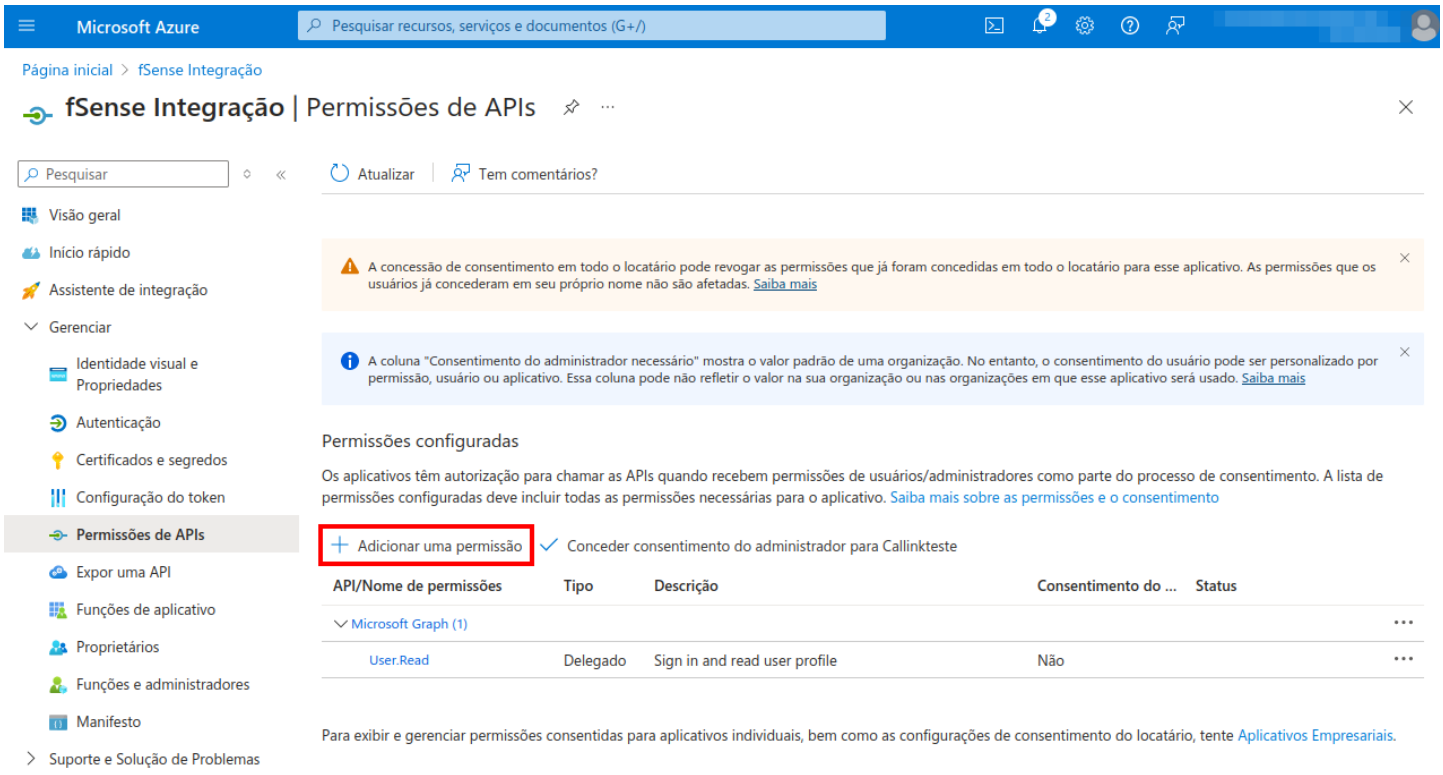
Fique atento aos valores gerados, eles serão necessários para configuração no fSense. “Valor” é seu client secret.



Portal Azure AD - Exemplo das credenciais geradas

Passo 5 : Configurar permissões

Acesse Permissões de APIs e clique em **+Adicionar uma permissão**



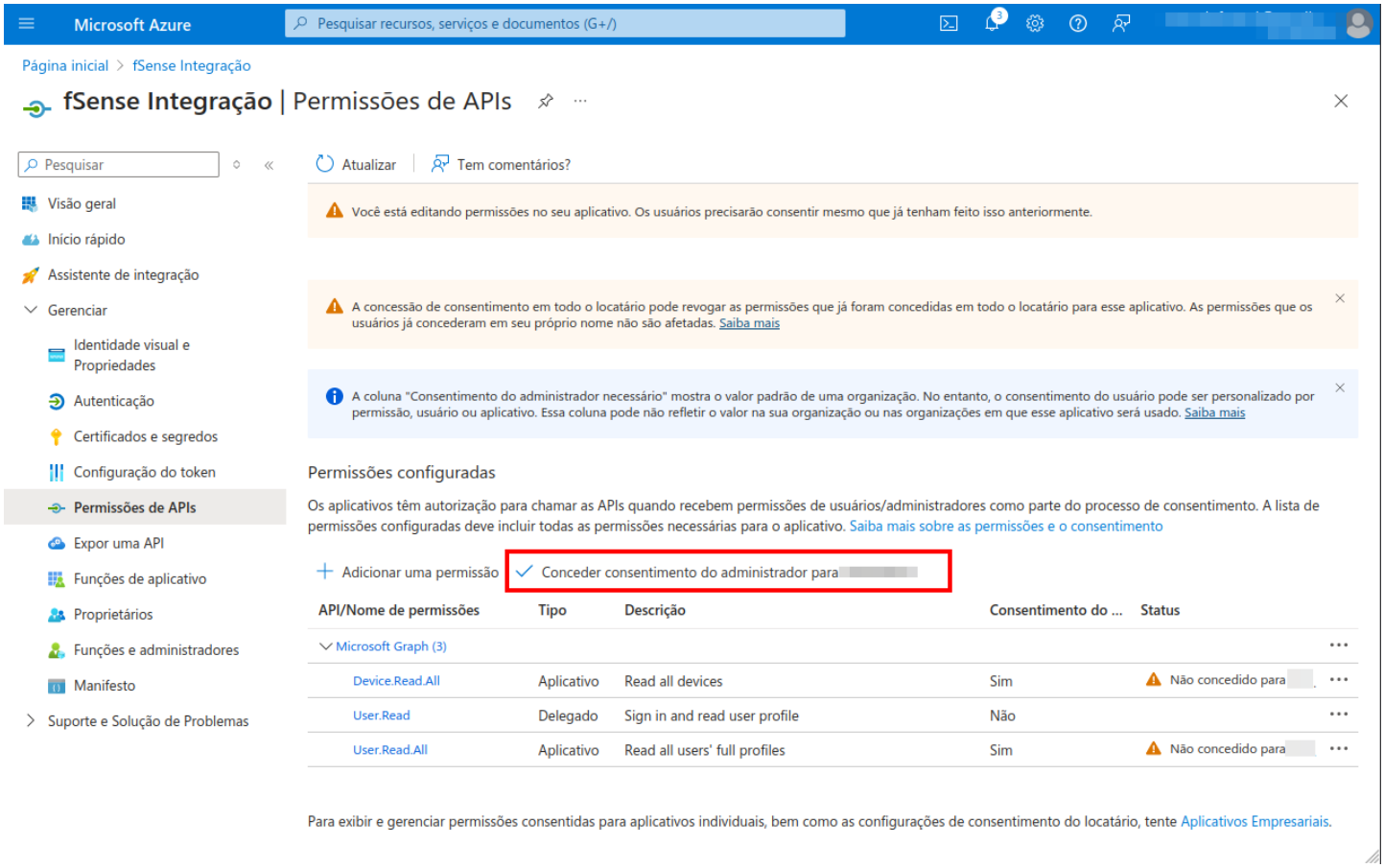
Portal Azure AD - Adiciona Permissões de API

Selecione o tipo Microsoft Graph

Portal Azure AD - Adiciona Graph

Selecione Permissões de aplicativo e adicione as permissões **User.Read.All** e **Device.Read.All**. Clique em Adicionar permissões.

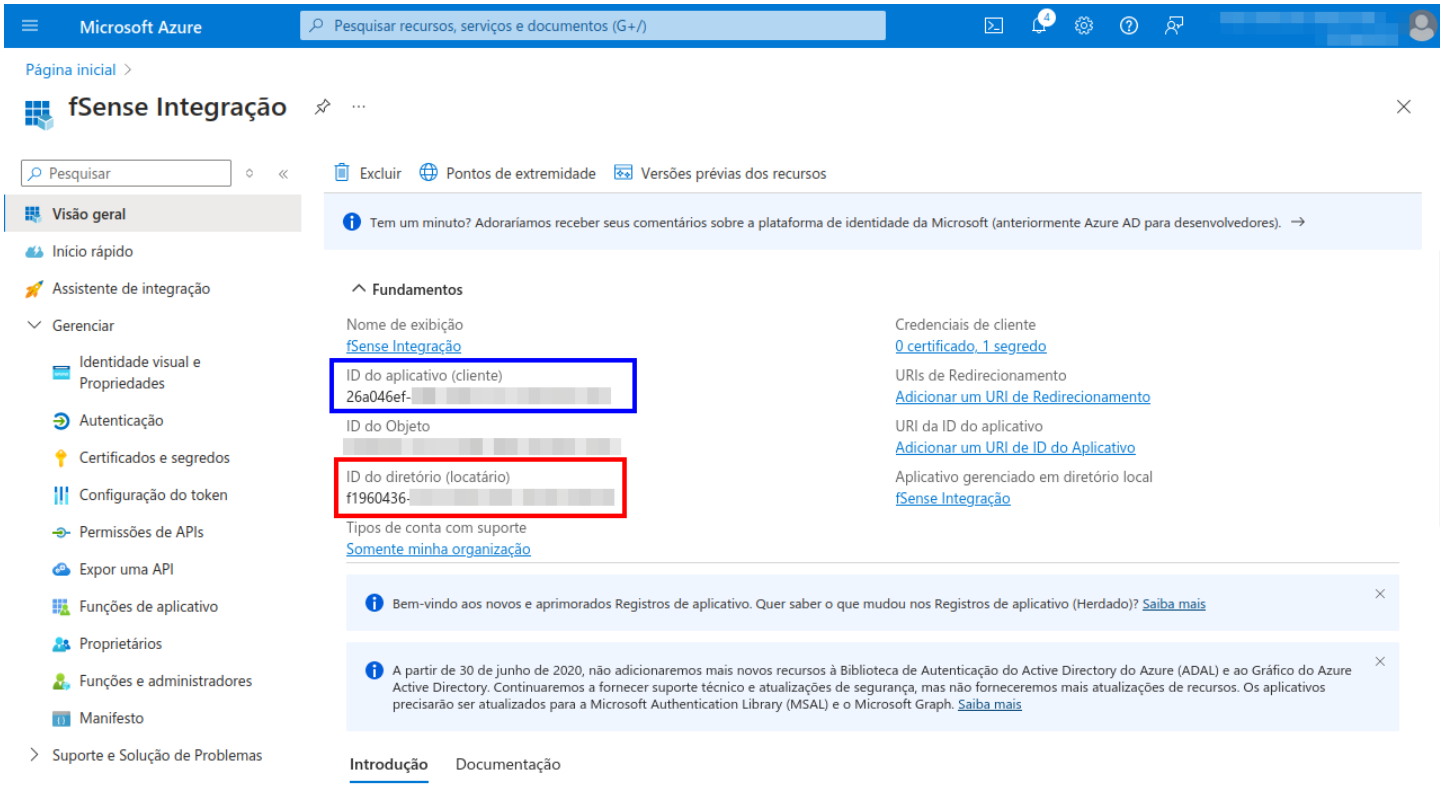
Clique em Conceder consentimento do administrador para `Nome da sua organização`



Portal Azure AD - Conceder Conhecimento Administrador

Passo 6 - Dados restantes

Volte para a tela de Visão geral e anote os dados **“Id do aplicativo (cliente)”**, que é seu **Client ID**, e o **ID do diretório (locatário)**, que é seu **Tenant ID**.



Portal Azure AD - Dados Restantes

Configuração necessária no fSense

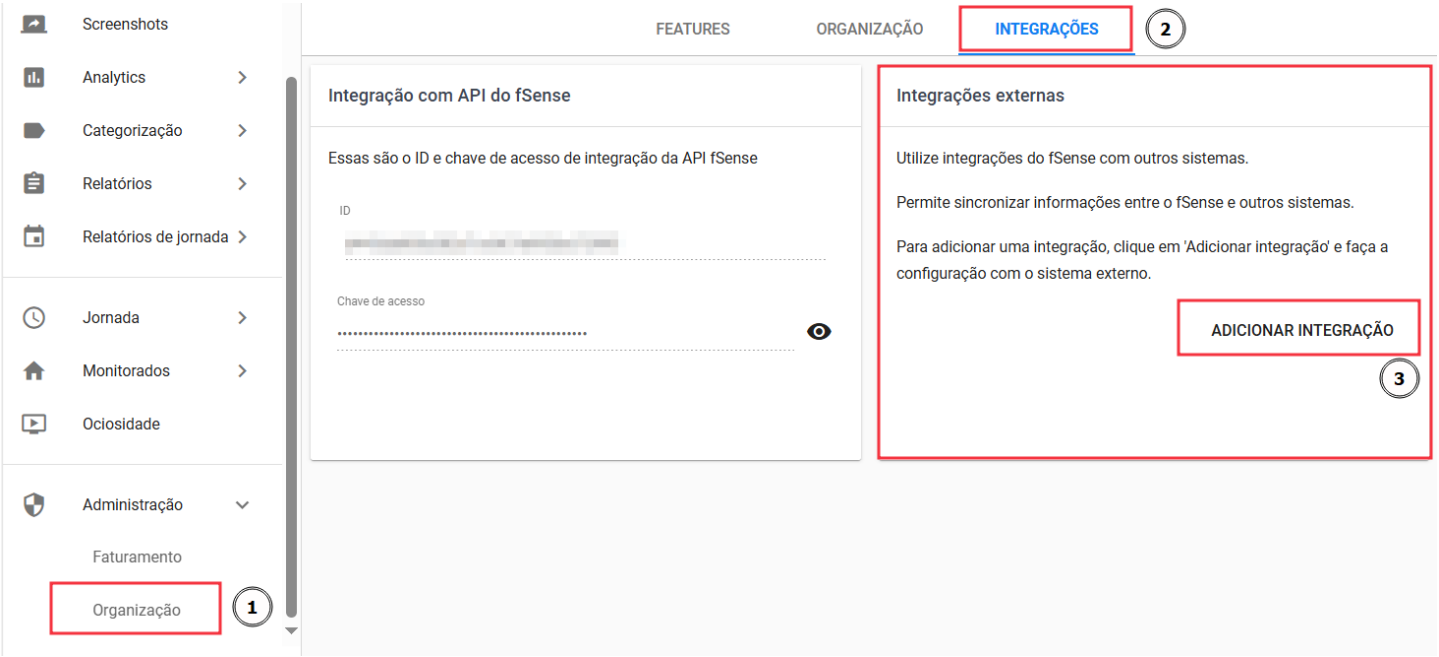
Para habilitar a integração com o **Microsoft Azure**:

1. No Menu Lateral, selecione a opção **Organização**.

2. Em seguida clique na aba **Integrações**.

3. Dentro da aba Integrações, localize o card **Integrações Externas**.

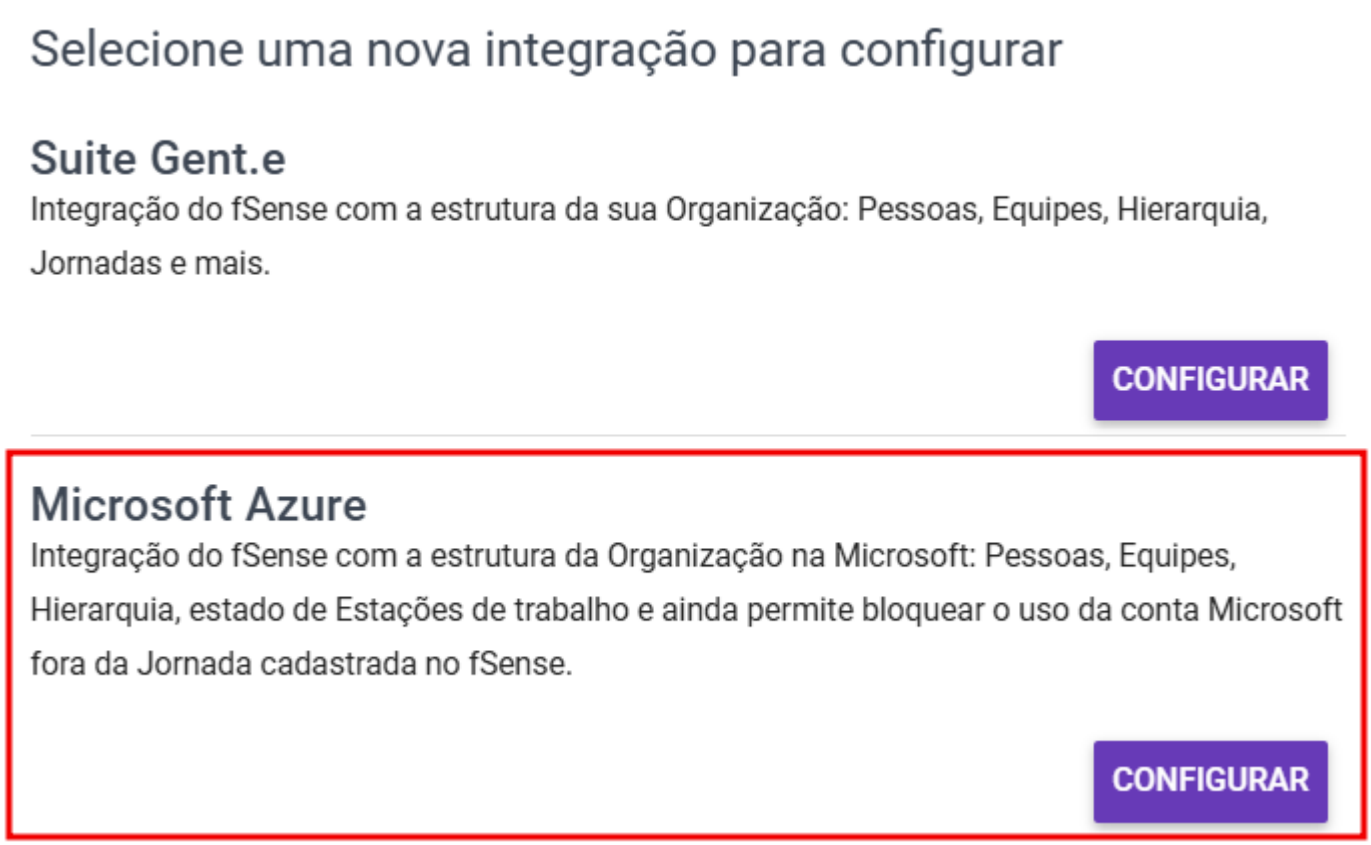
4. No card Integrações Externas, clique no botão **Adicionar Integração**.



fSense Integrações Externas

Configurar a Integração com o Microsoft Azure

1. Selecione a Integração **Microsoft Azure** e clique em **Configurar**.

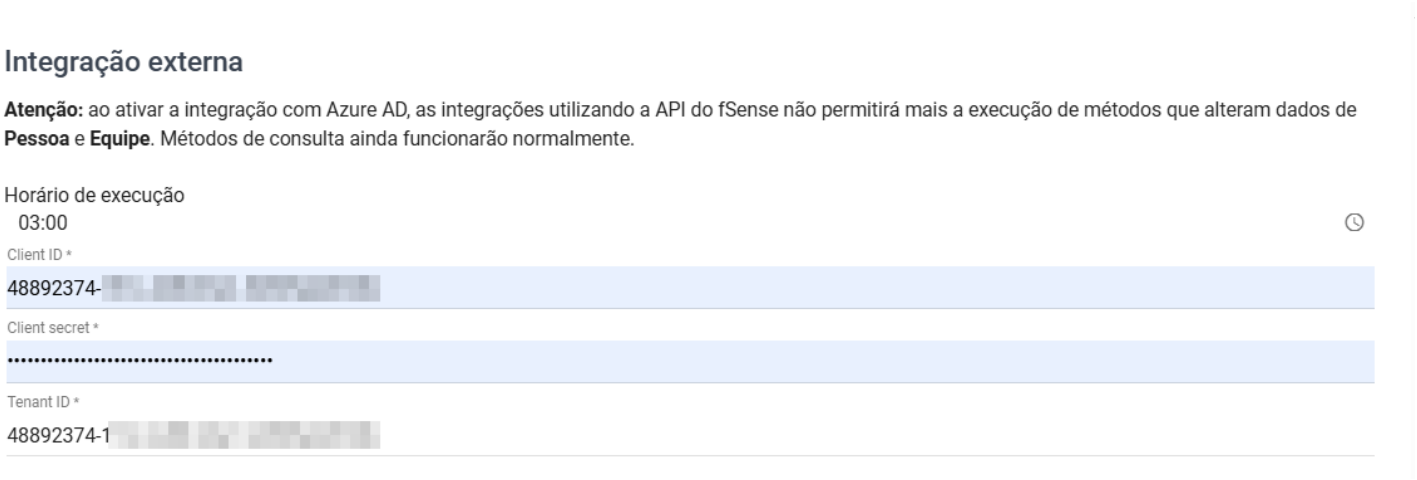


Integração com Microsoft Azure

2. Insira os dados solicitados, horário da execução do processo de sincronização,incluindo o ID do Locatário (Tenant ID) , ID do Cliente (Client ID) e Segredo do Cliente (Client ID) do Azure AD.

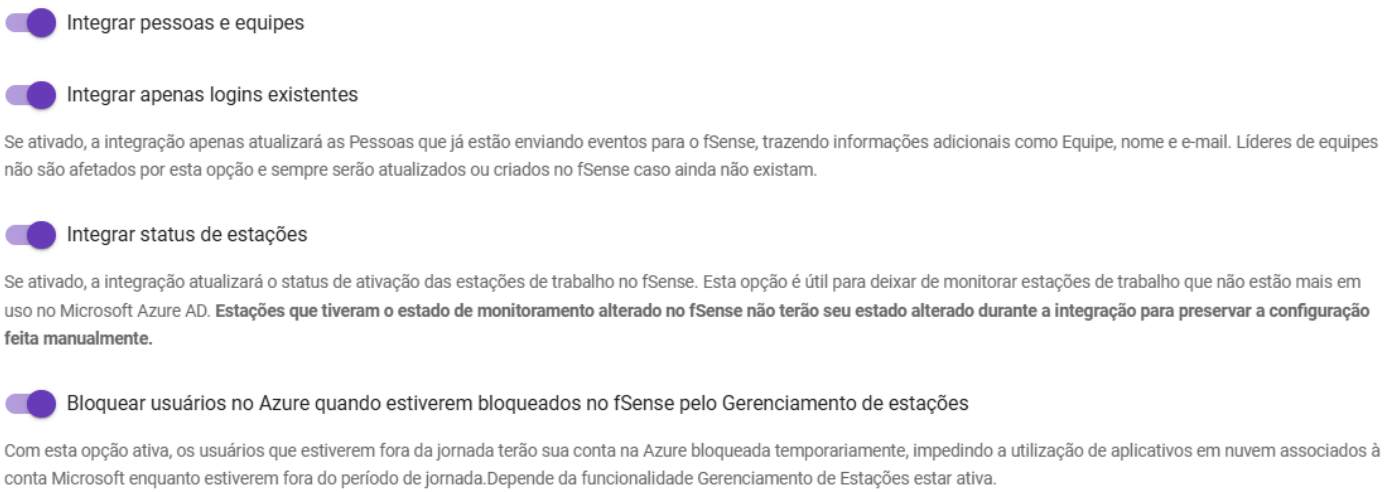
3. Clique em Testar configuração para validar as configurações.

4. Salve as configurações. Sua integração está configurada.



Integração com Microsoft Azure - Tela de Configuração

Parametrização adicional



Integração com Microsoft Azure - Tela de Configuração - Parametrização Adicional

Integrar pessoas e equipes

Ao habilitar essa opção, a integração irá sincronizar automaticamente os usuários do Microsoft Azure, junto com suas equipes, conforme a hierarquia existente.

> ⚠ **IMPORTANTE - RESTRIÇÃO EM INTEGRAÇÃO ADICIONAL**
>
> Ao habilitar a opção **Integrar pessoas e equipes**, não será possível sincronizar pessoas e equipes em outra integração de forma simultânea.

Integrar apenas logins existentes

Esta opção só é exibida caso esteja habilitado **Integrar pessoas e equipes**.

- **Se habilitado**, apenas usuários que já estão enviando dados para o fSense terão seus dados integrados. Isso significa que, se uma determinada estação de trabalho estiver sendo utilizada com o login de usuário "jose_silva" e estiver sendo monitorada pelo fSense, os dados do usuário "jose_silva" no Active Directory serão buscados e atualizados no fSense, como Nome, Equipe e E-mail.

- **Se desabilitado**, todos usuários encontrados no Active Directory serão integrados ao fSense mesmo antes de começarem a enviar eventos.

Integrar status de estações

Essa funcionalidade permite uma gestão mais eficiente das estações de trabalho, sincronizando automaticamente o status de ativação **do Azure AD para o fSense**, enquanto respeita e preserva as configurações manuais feitas pelo administrador no fSense.

- Se ativado, a integração atualizará o status de ativação das estações de trabalho no fSense. Isso significa que, ao habilitar essa opção, a integração entre o fSense e o Azure AD será configurada para manter o status de ativação das estações de trabalho atualizado no fSense. **Ou seja, se uma estação de trabalho for ativada ou desativada no Azure AD, essa mudança será refletida no fSense.**
- A principal vantagem dessa opção é que permite ao administrador parar de monitorar no fSense as estações de trabalho que não estão mais sendo utilizadas no Azure AD.

Assim, o sistema fSense não vai gastar recursos monitorando dispositivos desnecessários.

- Se um administrador **alterou manualmente** o estado de monitoramento de uma estação de trabalho no fSense (por exemplo, decidiu monitorar uma estação específica independentemente do seu status no Azure AD), essa configuração manual será mantida. A integração não vai sobrepor essas alterações feitas manualmente durante a sincronização. Isso evita que mudanças não intencionais ocorram e garante que as preferências do administrador sejam respeitadas.

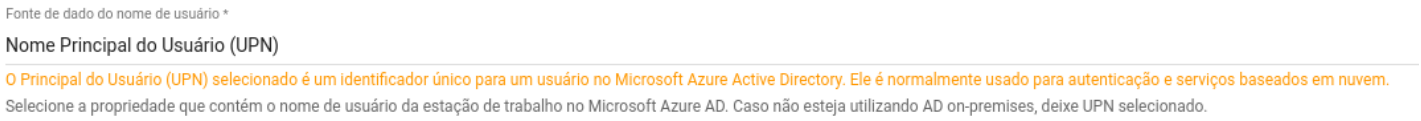
Bloquear usuários no Azure quando estiverem bloqueados no fSense pelo Gerenciamento de Estações

Esta funcionalidade só terá efeito caso a Feature de Gerenciamento de estação estiver habilitada.

Caso esteja habilitada, os usuários existentes tanto no fSense quanto no Azure terão as seguintes ações aplicadas:

- Se o Bloqueio de estação estiver habilitado para o usuário e este estiver **fora do período de Jornada**, será bloqueado no Azure até o próximo período de Jornada e não poderá utilizar sua conta Azure nem aplicativos de nuvem relacionados.
- Se o Bloqueio de estação estiver habilitado para o usuário e este estiver **dentro do período de Jornada**, será desbloqueado no Azure **caso tenha sido bloqueado anteriormente**. Note que o fSense só desbloqueará usuários que tenham sido bloqueados anteriormente pelo sistema de integração. Ou seja, se **o usuário tiver sido bloqueado no Azure pelo painel do Azure**, o fSense não irá desbloqueá-lo.
- Se o Bloqueio de estação não estiver habilitado para um usuário, o fSense não irá realizar qualquer alteração no usuário do Azure.

Fonte de Dados do Nome de Usuário



Integração com Microsoft Azure - Tela de Configuração - Fonte de Dados do Nome de Usuário

- **Nome Principal do Usuário (UPN):** O UPN é um identificador único para um usuário no Microsoft Entra ID (Active Directory). Ele geralmente está no formato de um endereço de email (por exemplo, *usuario@dominio.com*). Ao utilizá-lo, o fSense irá buscar a parte do endereço de email antes do @ e irá mapeá-lo para o campo **Login** no fSense.
- **Nome da Conta do Gerenciador de Contas de Segurança (SAM)**: O Nome da Conta SAM é um identificador único para um usuário dentro de um ambiente Active Directory *on-premises*. O Nome da Conta SAM é usando principalmente em ambientes de rede local onde o AD *on-premises* está implantado.

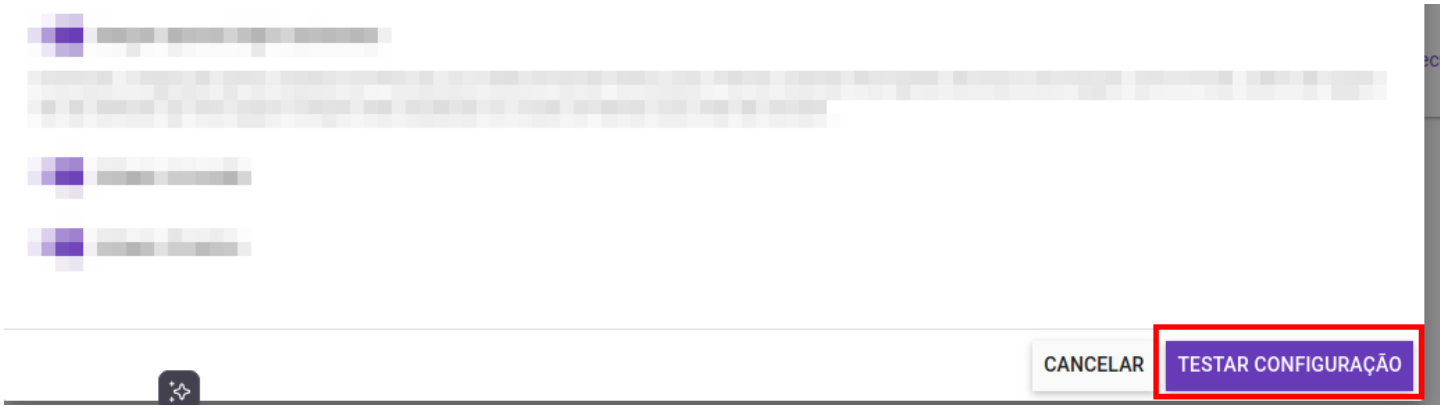
Quando Utilizar cada um:

- Se você está utilizando o **Azure AD (Entra ID)** na nuvem, utilize o UPN.
- Se voce está utilizando um AD **on-premises**, utilize o SAM.

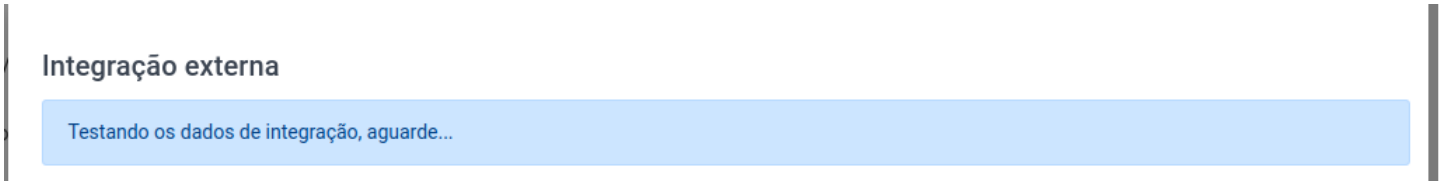
Validação dos dados inseridos

É necessário efetuar a validação dos dados inseridos para garantir que a integração foi configurada corretamente. **Não é possível ativar uma configuração que não passe pelo teste**.

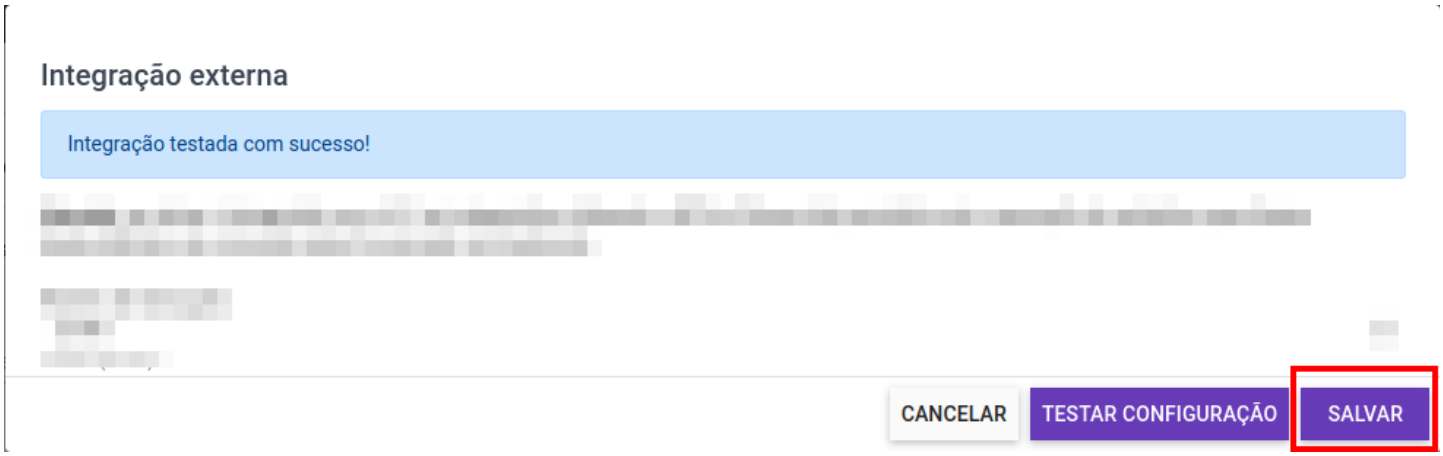
Para isso testar a integração, clique no botão **Testar Configuração**.



Uma mensagem de "Testando os dados de integração, aguarde..." será exibida no topo da tela de configuração. **Aguarde a confirmação do sistema com o resultado da validação**.



Após executada a validação com sucesso, o botão de **Salvar** ficará disponível para que você possa confirmar as configurações e habilitar a integração.

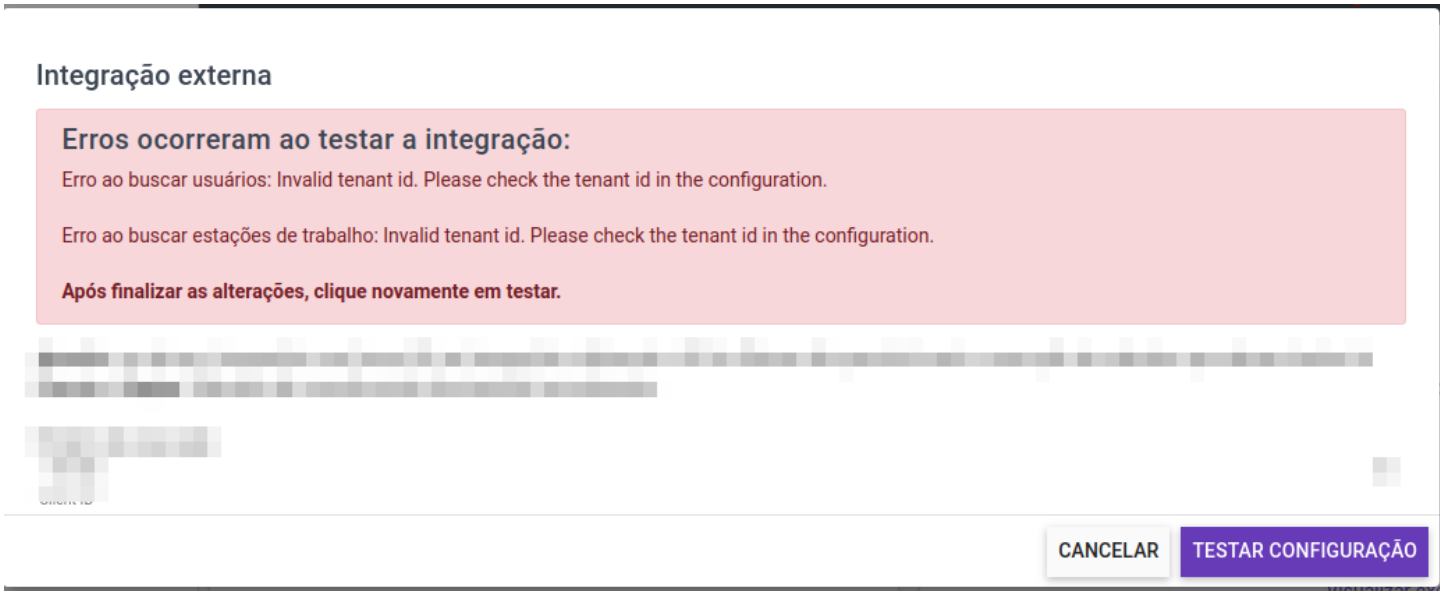


Erros durante a validação

É possível que ocorram erros durante a validação dos dados inseridos. Nesse caso, o sistema exibirá uma mensagem de erro indicando o problema encontrado.

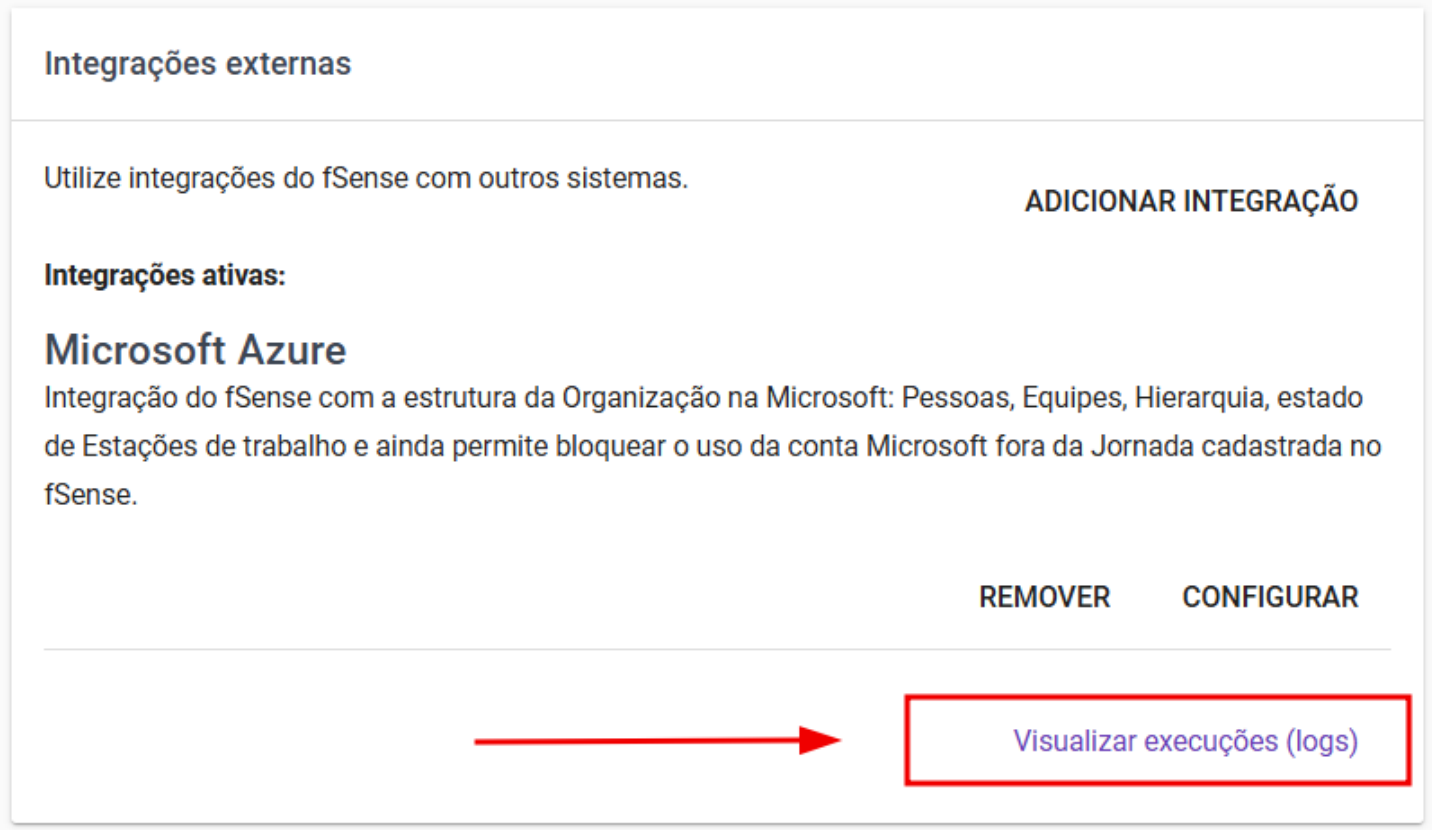
Estes erros podem, na maioria das vezes, serem derivados de dados incorretos ou inválidos inseridos durante a configuração da integração. Para corrigir o erro, verifique os

dados inseridos e faça as correções necessárias. **Não será possível habilitar uma integração que não tenha passado pelo teste com sucesso**.



Visualização de logs

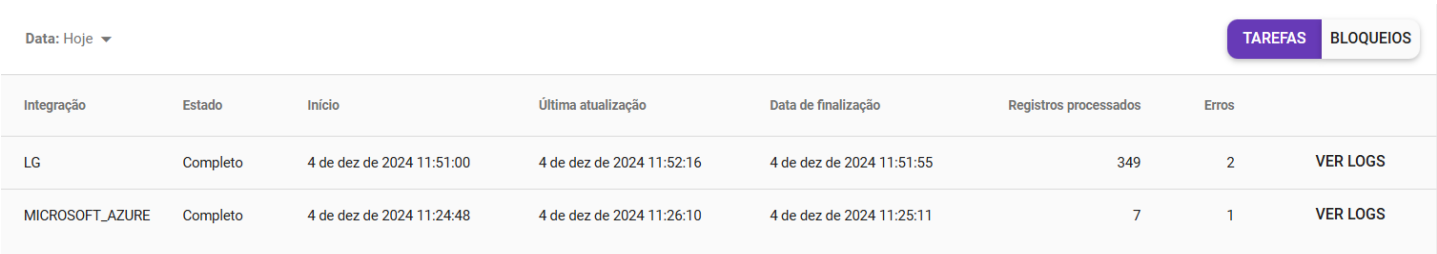
Na parte inferior do card **Integrações Externas**, é possível acompanhar os logs de execuções, horário de execuções, possíveis erros e bloqueios e desbloqueios efetuados por integrações externas. Para isso, clique no link **Visualizar execuções (logs)** do e o sistema irá abrir a tela de logs, com o **Tarefas** e **Bloqueios** executados, detalhados a seguir.



fSense Integração Externa - Visualizar Logs

Tarefas

A tela de tarefas exibe uma lista de execuções da integração.



fSense Integração Externa - Visualizar Tarefas (Logs)

É possível filtrar as tarefas por data de execução utilizando o **Filtro de Data**.

Os detalhes de cada tarefa são:

- **Estado**: exibe o estado atual da tarefa, como pendente, em processamento, completo ou falha.

- **Início**: quando a tarefa foi cadastrada para execução.
- **Última atualização**: último momento onde houve transferência ou processamento de dados.
- **Data de finalização**: quando foi finalizada
- **Registros processados**: quantos registros foram obtidos do sistema externo para processamento
- **Erros**: a quantidade de logs de erros, quando existente
- **Ver logs**: caso existam registros de erros, será possível visualizá-los ao clicar no botão de Ver logs.

Além disso, é possível conferir quais dados foram alterados utilizando a tela de **Histórico de Atividades**.

Bloqueios

A tela de bloqueios exibe uma lista de registros de bloqueios e desbloqueios executados quando a opção de **Bloquear usuários no Azure quando estiverem bloqueados no fSense pelo Gerenciamento de Estações** estiver habilitada.

Os dados são exibidos em ordem decrescente, com os registros mais novos em primeiro.

fSense Integração Externa - Bloqueios (Logs)

Propriedades obtidas pelo fSense

A tabela abaixo detalha como os campos de atributos do **Microsoft Entra ID** serão mapeados para o **fSense** para que a integração funcione conforme o esperado.

Relação de propriedades obtidas pelo fSense

Atributo no Microsoft Entra ID	Campo Correspondente no fSense	Ambiente	Descrição do Mapeamento
Nome de Exibição	**Nome da Pessoa**	Ambos	O campo **Nome de Exibição** no **Microsoft Entra ID** é o nome completo do usuário. Esse nome será definido no **fSense** como o campo **Nome** da Pessoa, utilizado para identificar a pessoa nas interfaces do fSense, dashboards, logs e relatórios.
Nome UPN	**Login**	Apenas em ambiente **Azure AD**	O **Nome UPN** é um identificador único para um usuário no **Microsoft Entra ID (Active Directory)**. Ele geralmente está no formato de um endereço de email (por exemplo, *usuario@dominio.com*). Ao utilizá-lo, o **fSense** irá buscar a parte do endereço de email antes do @ e irá mapeá-lo para o campo **Login** no fSense.
Nome da Conta SAM	**Login**	Apenas em ambiente **AD On-Premises**	O **Nome da Conta SAM** é um identificador único para um usuário dentro de um ambiente **Active Directory** *on-premises*. O **Nome da Conta SAM** é usando

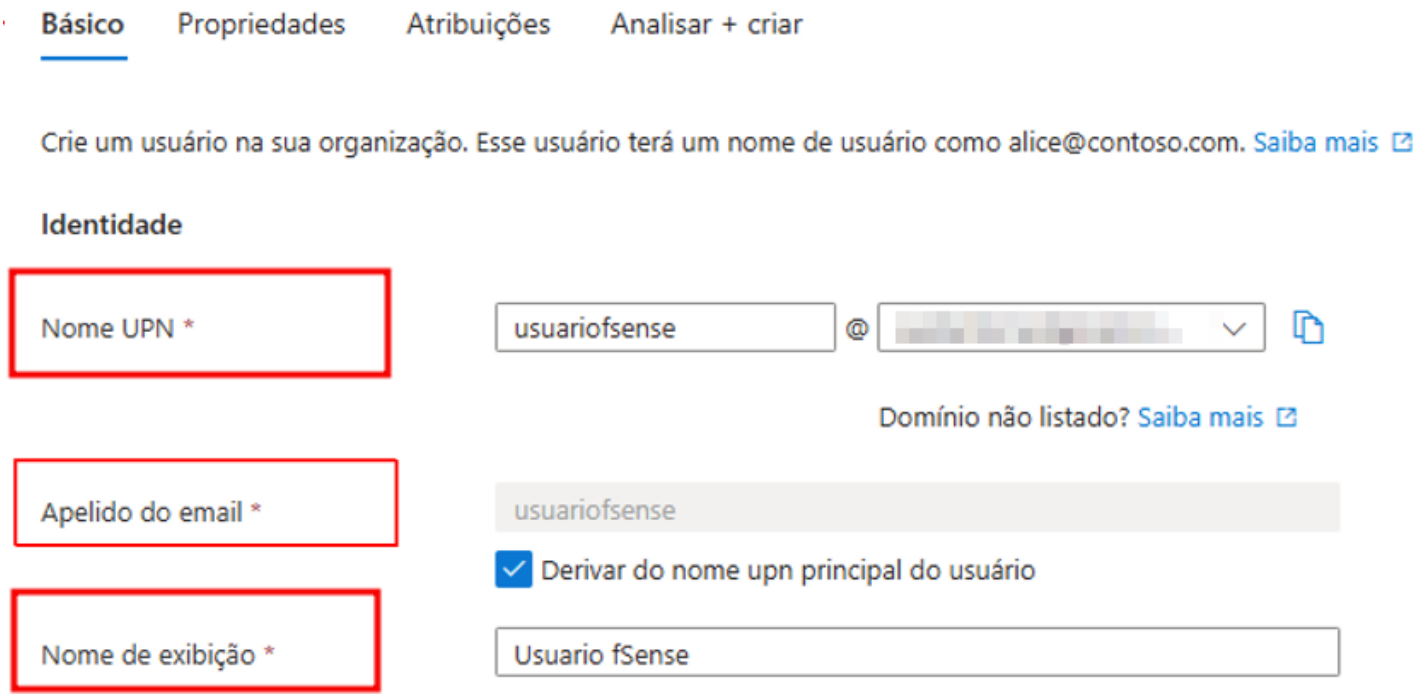
Atributo no Microsoft Entra ID	Campo Correspondente no fSense	Ambiente	Descrição do Mapeamento
			principalmente em ambientes de rede local onde o AD *on-premises* está implantado. Se estiver utilizando um Ambiente AD On-premises, este atributo será mapeado para o campo **Login** no fSense.
ID do Objeto	**Código Externo**	Ambos	O **Id do Objeto** no **Microsoft Entra ID** é um identificador único atribuído a cada usuário no AD, que permite identificar o usuário de forma única. Esse *ID do Objeto* será o atribuído ao campo **Código Externo** no fSense
Email	**Email**	Ambos	O campo **Email** no **Microsoft Entra ID** será mapeado diretamente para o campo **Email** do fSense. Esse campo é utilizado pelo fSense para o envio de notificações, caso o usuário criado seja um líder de equipe e outras funcionalidades relacionadas ao email do usuário.
Departamento	**Equipe**	Ambos	O campo **Departamento** no **Microsoft Entra ID** será mapeado para o campo **Equipe** no fSense. Caso não exista uma equipe no fSense correspondente ao departamento informado, ela será criada automaticamente e o

Atributo no Microsoft Entra ID	Campo Correspondente no fSense	Ambiente	Descrição do Mapeamento
			usuário será alocado na respectiva equipe.
Gerente	**Líder da Equipe**	Ambos	O campo **Gerente** no **Microsoft Entra ID** define o superior hierárquico do usuário. No fSense, este campo será mapeado como **Líder da Equipe**. Se o usuário tiver um gerente definido, este será associado como **Líder da Equipe** no fSense.

Exemplo de Sincronização de Dados de Usuário no Microsoft Entra ID para Integração com fSense

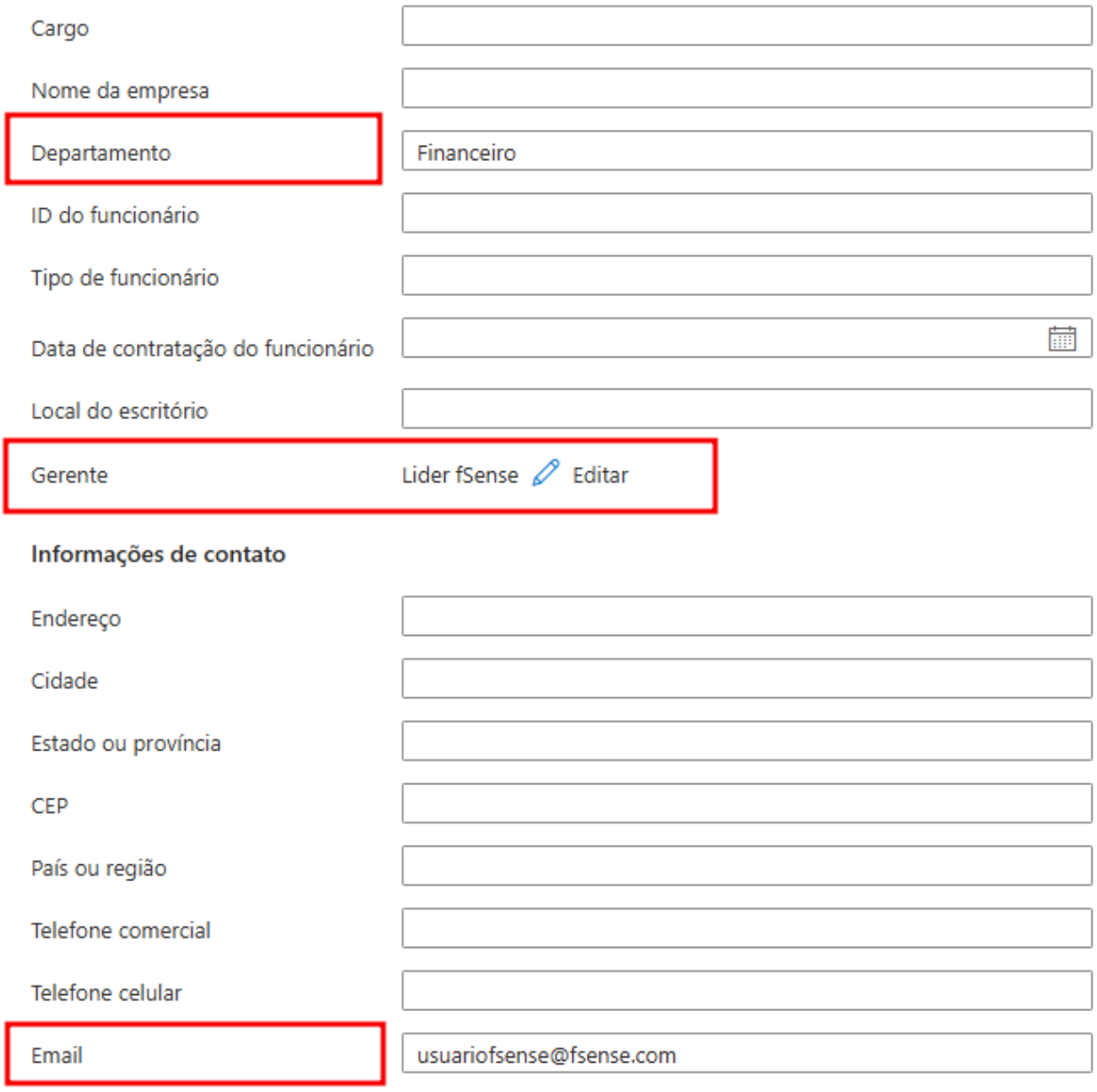
Vejamos um exemplo de um Usuário no **Microsoft Entra ID** que será posteriormente sincronizado com o **fSense**.

- **Nome UPN**: será atribuído ao campo **login** no fSense **caso o ambiente seja Azure AD**.
- **Apelido do email**: será atribuído ao campo **login** no fSense **caso o ambiente seja AD On-Premises**.
- **Nome de Exibição**: Este campo será mapeado no fSense como o campo **Nome** da Pessoa.



Portal Azure - Microsoft Entra ID - Mapeamento de Atributos de Usuário no Microsoft Entra ID - Básico

- **Departamento**: Este campo será mapeado para a **Equipe** no fSense. Caso a equipe não existe, a mesma será criada automaticamente e o usuário alocado na respectiva equipe.
- **Gerente**: Caso haja um superior hierárquico para o usuário, o Gerente informado para o usuário será definido como **Líder da Equipe** no fSense.
- **Email**: Esse campo será definido como o campo **email** do Usuário do **fSense**.



Portal Azure - Microsoft Entra ID - Mapeamento de Atributos de Usuário no Microsoft Entra ID - Propriedades

Atualização dos Dados do Usuário na Próxima Sincronização

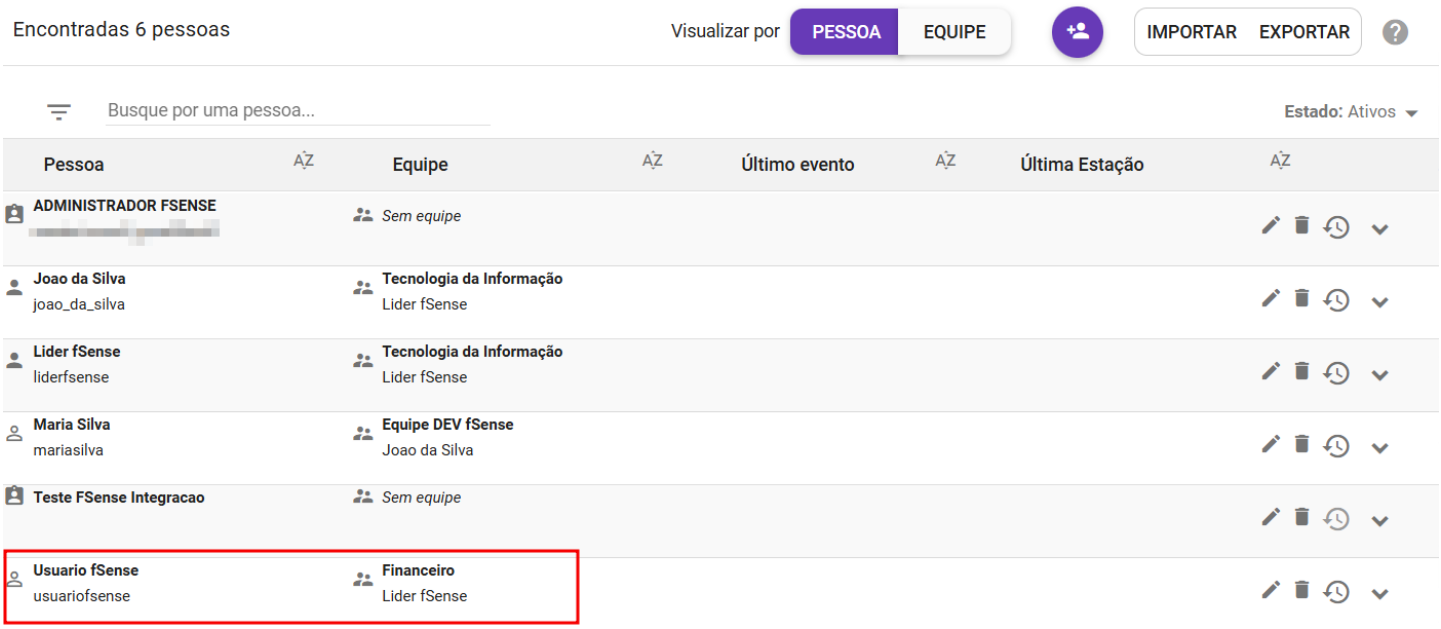
Quando a próxima sincronização programada ocorrer, o **fSense** irá criar ou atualizar as informações do usuário com base nos dados mais recentes do **Microsoft Entra ID**. Os campos mapeados e atualizados incluem:

- **Nome de Exibição** *(Nome da Pessoa)*
- **Nome UPN/Nome da Conta SAM** *(Login)*

- **Email**
- **Departamento** *(Equipe)*
- **Gerente** *(Líder da Equipe)*

Como a sincronização irá funcionar?

- se o usuário já existir no fSense e houver alterações nos dados do **Microsoft Entra ID**, esses dados serão atualizados conforme o mapeamento acima.
- se um usuário não existir no fSense, o fSense criará o usuário, utilizando as informações mais recentes do **Microsoft Entra ID**.
- caso a equipe mapeada ao departamento não exista no **fSense**, ela será criada automaticamente durante a sincronização.
- Se houver alterações na hierarquia, como a definição de um novo **Líder de Equipe**, o **fSense** irá ajustar a hierarquia das equipes conforme necessário.



Sincronização de Usuários com Login Existente

Quando um usuário já existente no **fSense** tem um **Login (UPN ou SAM)** que corresponde a um novo usuário do **Microsoft Entra ID (Active Directory)**, o processo de sincronização entre os sistemas acontece conforme descrito a seguir.

Sincronização de Dados

- **Atualização de Informações:** Se um usuário existir no **Microsoft Entra ID** com o mesmo **UPN/SAM** que já existe no **fSense**, a sincronização entre os sistemas **atualizará as informações do usuário no fSense** para refletir as informações mais recentes do **Active Directory**. A atualização incluirá os seguintes campos:

    - **Nome de Exibição (Nome da Pessoa)**
    - **Email**
    - **ID de Objeto (Código Externo)**
    - **Departamento (Equipe)**
    - **Gerente (Líder da Equipe)**

    Essas informações serão modificadas no fSense de acordo com os dados mais recentes do **Microsoft Entra ID**.

- **Preservação das Configurações Específicas do fSense:** Apesar da atualização dos dados do usuário, as **configurações específicas do fSense** associadas ao usuário **não serão sobrescritas**. Isso inclui:

    - Configurações de **bloqueio de estação**
    - Configurações de **capturas de tela**
    - **Jornadas específicas**
    - **Outras associações e permissões personalizadas** Essas configurações específicas permanecem inalteradas durante o processo de sincronização. O fSense preserva as personalizações feitas, garantindo que o usuário tenha a mesma configuração no fSense, mesmo após a atualização dos dados provenientes do **Microsoft Entra ID**.

Processo de Sincronização

Durante a sincronização, o **fSense** realiza as seguintes verificações e ações:

- **Verificação de Correspondência**: O fSense verifica se o **UPN/SAM** (Login) do usuário no **Microsoft Entra ID** corresponde a um **usuário existente** no fSense para ambientes Azure AD. Para ambientes AD on-premise é verificado o **Nome da Conta SAM** que corresponde a um **usuário existente** no fSense.

- **Atualização de Dados**: Se houver uma correspondência, o fSense **atualiza os dados** do usuário conforme os dados mais recentes do Microsoft Entra ID, como **Nome de Exibição**, **Email** e **ID de Objeto (Código Externo)**, **Departamento (Equipe)**, **Gerente (Líder de Equipe)**.

- **Manutenção das Configurações do fSense**: Mesmo que os dados do usuário sejam atualizados, as configurações específicas do fSense (permissões, bloqueios, configurações de jornada, etc.) **não são sobrescritas** ou alteradas. Essas configurações permanecem intactas.

Impacto da Alteração do UPN ou SAM:

Se o **UPN/SAM** (Login) de um usuário for alterado no **Microsoft Entra ID** e o usuário já tiver sido sincronizado com o fSense, o fSense irá alterar o **login** do usuário **apenas** se ele ainda não tiver enviado eventos para o sistema. Caso contrário, a atualização do usuário irá falhar até que o problema seja corrigido.

Evitar Problemas de Duplicação

Para evitar problemas como duplicação de usuários ou a perda de configurações personalizadas, é importante **manter a consistência** entre os valores do **Código Externo** no fSense e o **UPN** no **Microsoft Entra ID**. Cuidado ao fazer alterações nos **UPNs** ou **SAMS** dos usuários, pois isso pode causar problemas de sincronização.

Requisitos para Integração de Usuários

Usuários Monitorados

Para que um usuário monitorado do AD seja integrado ao fSense, ele precisa ter **pelo menos um dos seguintes campos preenchidos**:

- **Identificador de Dispositivo (Login):** O identificador de dispositivo que associa a pessoa ao usuário do Windows. A falta deste identificador impossibilita que o usuário possa ser monitorado pelo fSense.
- **Email:** Se um usuário monitorado tiver um email, mas não for um Líder de Equipe, ele será integrado ao sistema. No entanto, ele não poderá acessar o fSense, pois não terá

os privilégios necessários. O email servirá apenas para exibição.

Requisitos Adicionais para Líderes de Equipe

- Caso um usuário do AD seja designado como Líder de Equipe (Gerente no Microsoft Entra ID), é **obrigatório que ele possua um endereço de email**. Esse email será utilizado tanto para se autenticar no fSense, quanto para o receber notificações importantes e monitorar suas respectivas equipes através do painel de Gestão do fSense.

Usuários do AD que não serão Integrados

Usuários do AD que não cumprem estes requisitos **NÃO** serão integrados na sincronização.

Observações

⚠ **OBSERVAÇÕES IMPORTANTES**

Restrição na API:

1. Integração de Pessoas e Equipes: Ao habilitar a **Integração de Pessoas e Equipes** em uma **Integração Externa**, as **funcionalidades de escrita da API do fSense serão desabilitadas**. Se uma tentativa de alteração for feita via API, será retornado um **erro**. Essa medida garante que os dados da integração externa não sejam sobrescritos por alterações realizadas via API.

2. Restrição em Integração Adicional: Ao habilitar a opção **Integrar Pessoas e Equipes** nesta integração, não será possível sincronizar pessoas e equipes em outra integração adicional de forma simultânea.

3. Suporte Técnico: Em caso de dificuldades ou dúvidas durante o processo de **integração**, entre em contato com o **Suporte técnico do fSense** para assistência.

4. Registros de alterações: O **Histórico de Atividades** estará disponível para você acompanhar as alterações feitas pela integração entre o **Microsoft Entra ID** e o **fSense**.

5. Registro de alertas e erros: É possível acompanhar alertas e erros do processo de integração no link **Visualizar Execuções (logs)**, que estará disponível no menu de **Integração Externa** depois que a integração for configurada no fSense.