

Guia Básico
**AUTENTICAÇÃO DE
DOIS FATORES (MFA)**

O que é MFA?


O MFA ou Multi-Factor Authentication é o uso de dois ou mais fatores para verificação quanto a autenticidade de algo.

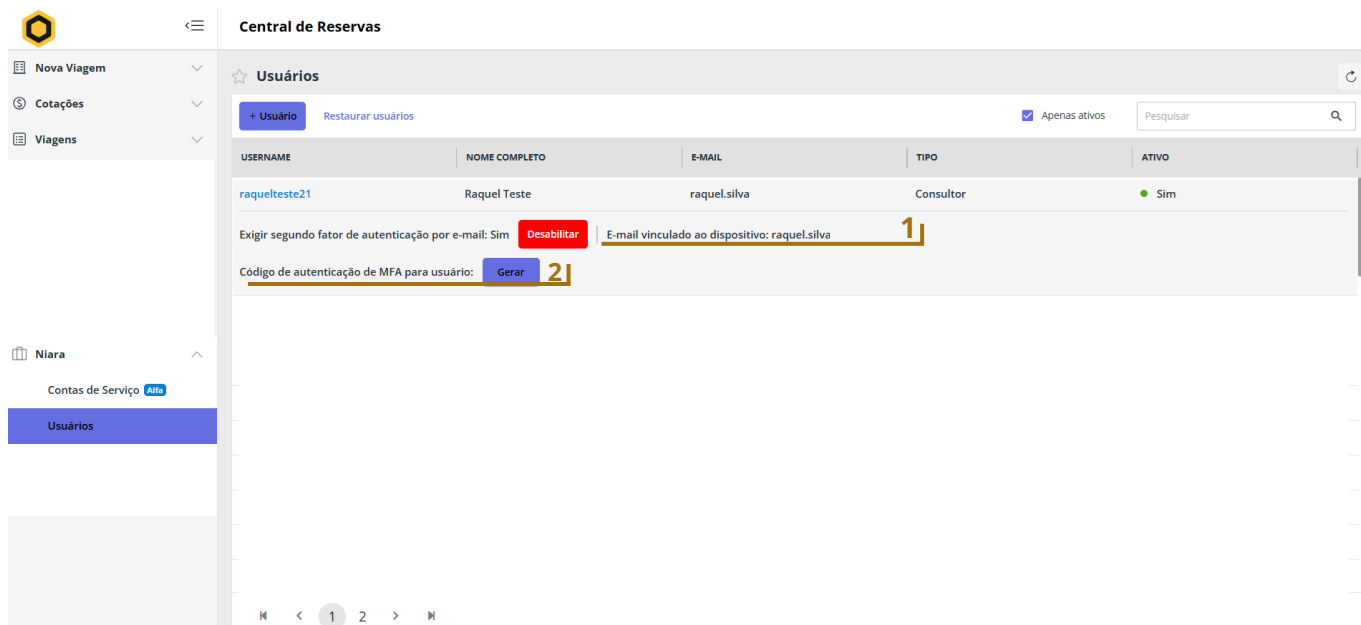
Por que utilizar?

Ao implementar o MFA, a Niara adiciona várias camadas de segurança ao sistema, o que torna possível validar a identidade dos usuários.

Como habilitar?

Após a criação de usuário, é possível definir um fator de segurança para seu acesso. A ativação também pode ser realizada em usuários existentes. Siga o passo a passo:

- 1.O usuário Master poderá acessar a opção **Usuários** no Menu Principal, clicando em **Niara** e em seguida em **Usuários**.
- 2.Ao escolher o usuário, clique no ícone  e selecione a opção de segurança que melhor o atenderá: código via e-mail ou via aplicativo autenticador.



Central de Reservas

Usuários

+ Usuário Restaurar usuários

☒ Apenas ativos Pesquisar

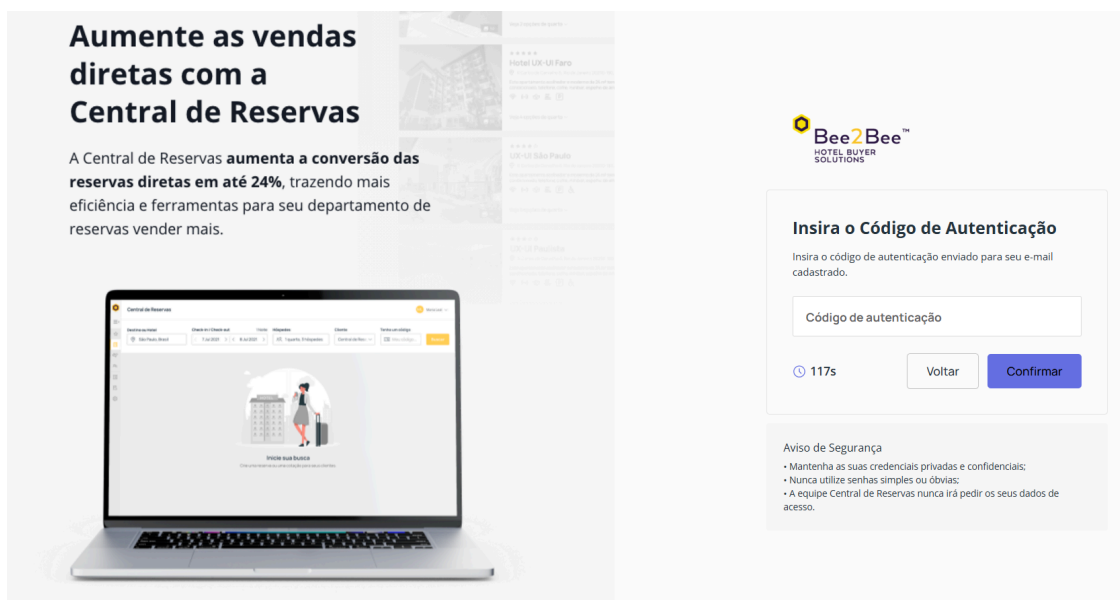
USERNAME	NOME COMPLETO	E-MAIL	TIPO	ATIVO
raquelteste21	Raquel Teste	raquel.silva	Consultor	Sim

Exigir segundo fator de autenticação por e-mail: Sim **Desabilitar** E-mail vinculado ao dispositivo: raquel.silva **1**

Código de autenticação de MFA para usuário: **Gerar** **2**

1. Autenticação via E-mail

Nesse processo, ao acessar a Central de Reservas, será solicitado ao usuário um código de autenticação, conforme a captura de tela abaixo:



O código de autenticação é enviado para o e-mail cadastrado no acesso do usuário. O assunto do e-mail é "Código de Autenticação" e o e-mail remetente é "nts@notification.niara.tech".

Essas informações são importantes para viabilizar o recebimento desse e-mail através das configurações da sua Caixa de Entrada.

IMPORTANTE:

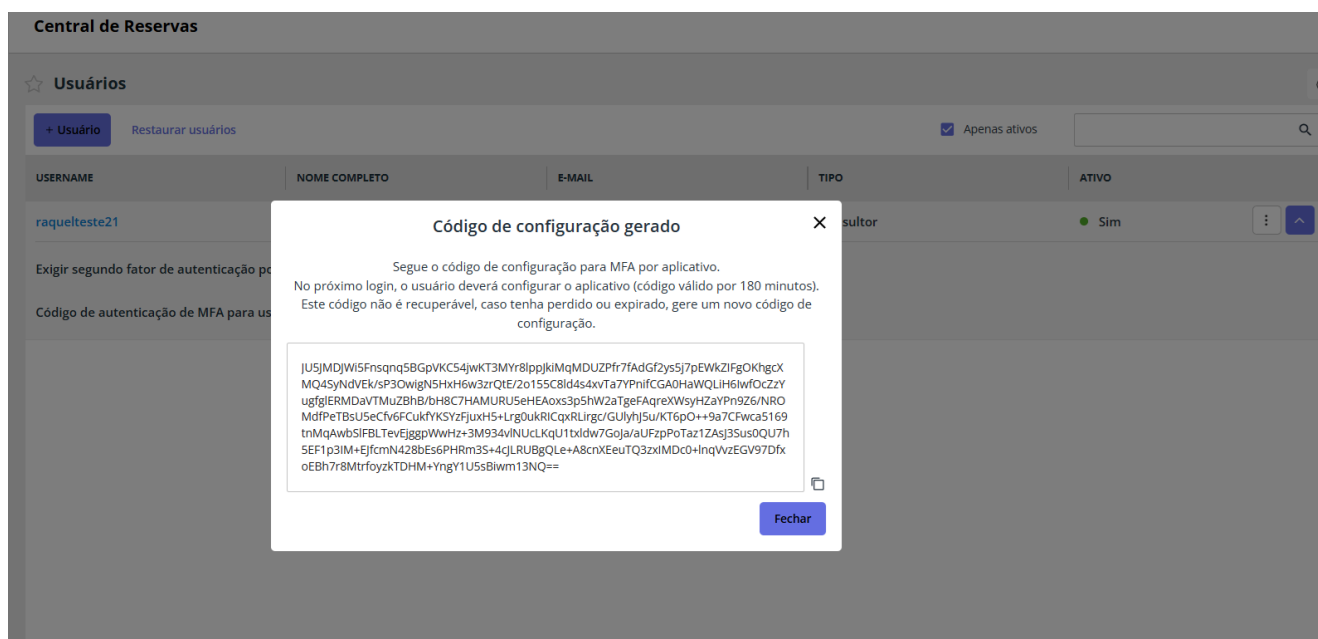
- O código é enviado de maneira automática e imediata. Caso não consiga identificar o recebimento, verifique sua caixa de Spam. Experimente também adicionar o e-mail remetente aos seus contatos seguros.

2. Autenticação via Token (Autenticador)

Nesse processo, o usuário deve escolher um aplicativo autenticador de sua preferência. Indicamos os aplicativos Authy, Microsoft Authenticator ou Google Authenticator.

Ao clicar na opção **Gerar** o sistema gera um código de autenticação (token) que pode ser inserido nos aplicativos autenticadores acima.

O token é válido por 180 minutos.

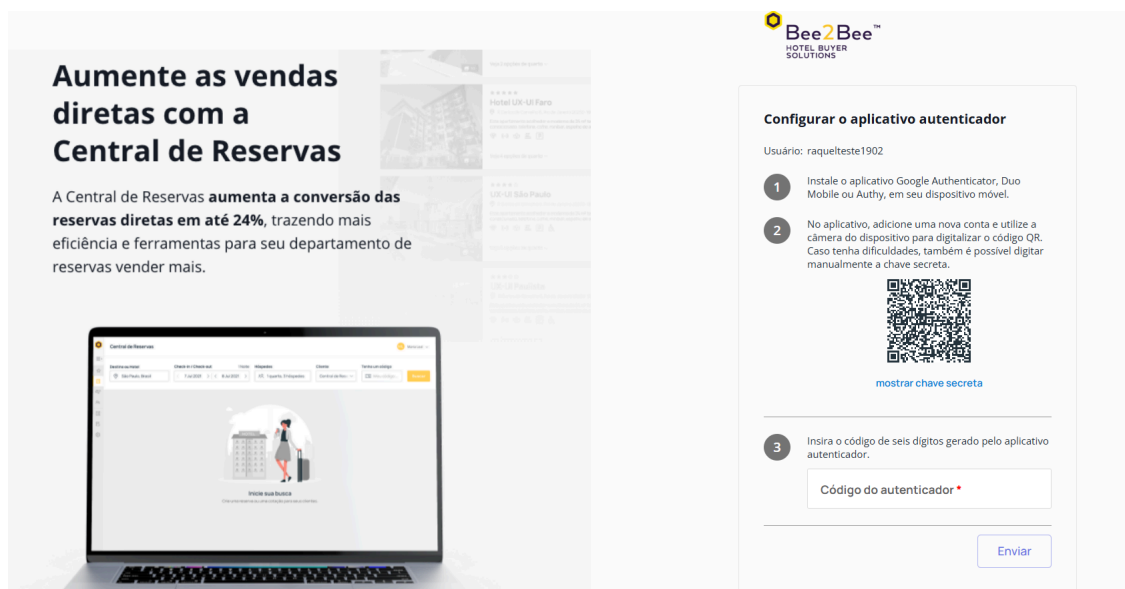


Em seguida, acesse sua Central de Reservas normalmente e insira o login e senha, após a inserção da senha, o sistema solicitará o Token gerado acima e clique em **Continuar**.

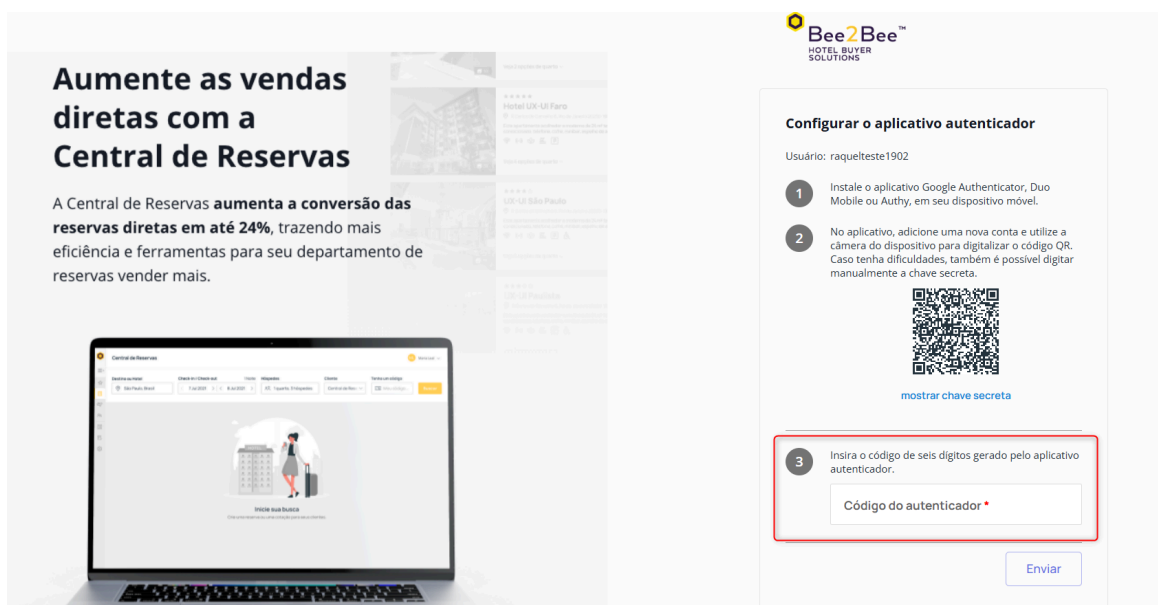


2. Autenticação via Token (Autenticador)

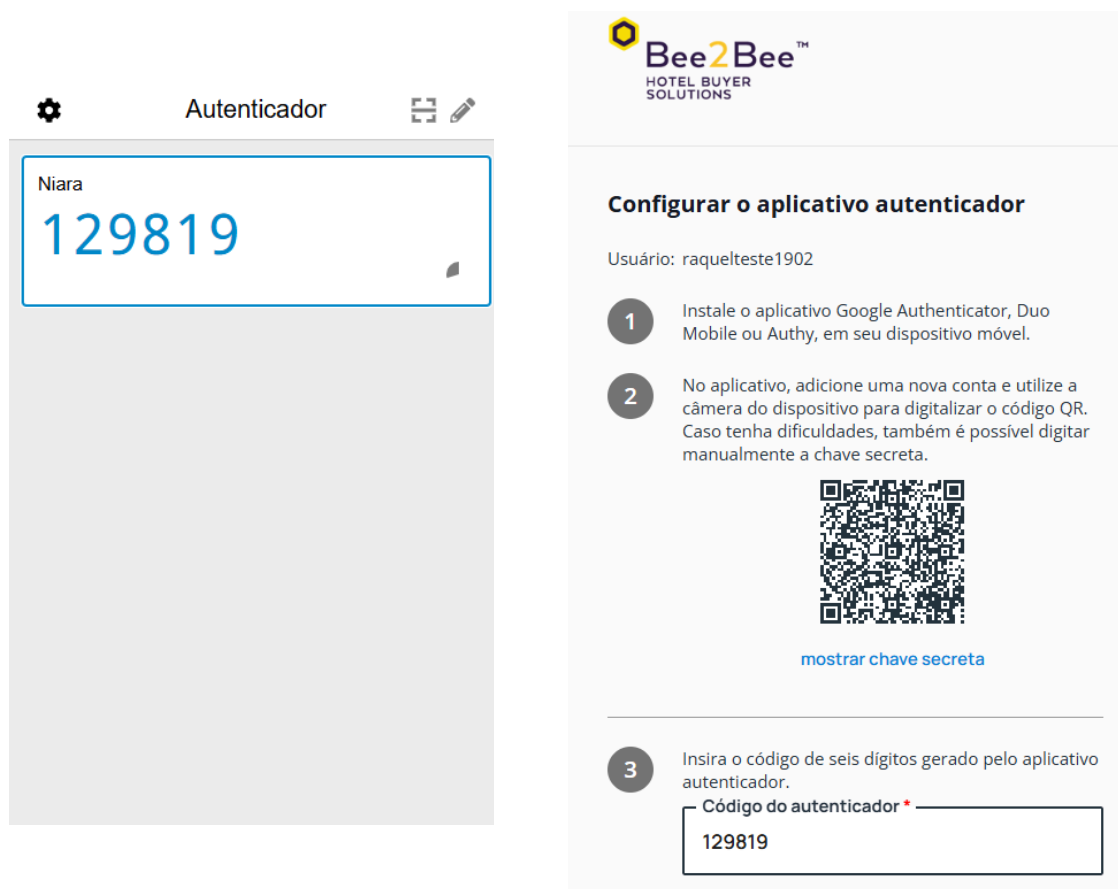
Assim que o Token for adicionado, na próxima tela aparecerá um QR Code que pode ser escaneado pelo seu aplicativo Autenticador de preferência (Google Authenticator, Microsoft Authenticator, etc)



Após essa ação, o aplicativo vai disponibilizar um código de autenticação que deve ser inserido no campo em destaque abaixo:



2. Autenticação via Token (Autenticador)



IMPORTANTE:

- O usuário deve escolher apenas uma solução de autenticação. Para os casos em que deseje seguir com o aplicativo autenticador, é necessário desabilitar o envio do código por e-mail.
- Os e-mails de acesso que foram cadastrados não podem ser alterados. Caso o e-mail fornecido seja um e-mail incorreto ou o usuário não possua mais acesso ao e-mail, é necessário criar um novo usuário.
- O código de autenticação é uma medida complementar de segurança e mandatória. Não é possível desabilitar o fator de segurança. Nesse cenário, indicamos que escolham a opção que melhor atende os usuários do seu estabelecimento.

AUTENTICAÇÃO DE DOIS FATORES (MFA)



PRECISA DE AJUDA - SUPORTE Caso tenha dúvidas, encontre algum erro ou possui alguma sugestão, saiba os canais que pode nos acionar.

Para dúvidas de tarifas, hotéis, condições de pagamento e acordos, acione o Suporte Omnibees.

E-mail: servicedesk@omnibees.com

Telefone: 55 11 4504-0000

Para dúvidas Niara, por favor acione servicedesk@niara.tech

Conheça mais sobre a Niara: <https://niara.tech/>