

API Suite OnBlox — Autenticação por API Token

6 de outubro de 2026 · @Thiago Silva Cruz

Versão: 1.0

Atualizado em: 06/10/2026

Público: Parceiros e integradores

Escopo: Autenticação das APIs da Suite OnBlox (/api/**)

1. Visão geral

Sistemas externos podem consumir as APIs disponibilizadas diretamente pela Suite OnBlox para consultar ou enviar informações, de acordo com os endpoints disponíveis para cada integração.

Toda chamada à API da Suite OnBlox (/api/**) deve incluir o cabeçalho:

```
X-API-Token:  
onbx_SEU_TOKEN_AQUI
```

O token autentica o sistema externo que está acessando a Suite OnBlox e substitui o uso de usuário e senha nas chamadas da API. Ele é gerado na própria Suite OnBlox pelo administrador do cliente e é válido exclusivamente para o ambiente ao qual pertence.

🔑 **Princípio-chave:** Um token não é uma credencial global da OnBlox. Cada cliente possui sua própria URL base e sua própria credencial.

2. Arquitetura da integração

Na versão 1.0, os sistemas externos se comunicam diretamente com as APIs disponibilizadas pela Suite OnBlox .

Fluxo: Sistema externo / ERP → Suite OnBlox → /api/**

Se um parceiro integra seu sistema com mais de um cliente OnBlox, deve manter uma configuração independente para cada cliente.

Cliente A → URL base A + Token A

Cliente B → URL base B + Token B

3. Início rápido

1. Receba do cliente a URL base da Suite OnBlox.
2. Receba um API Token válido.
3. Configure a URL e o token especificamente para aquele cliente.
4. Utilize um dos endpoints disponibilizados pela OnBlox para a integração.
5. Confirme o retorno HTTP da operação.
6. Implemente o tratamento adequado de erros antes de colocar a integração em produção.

```
curl -X GET "https://suite.exemplo.com.br/onblox/api/<endpoint>" \  
-H "X-API-Token: onbx_SEU_TOKEN_AQUI" \  
-H "Accept: application/json"
```

Substitua pelo endpoint disponibilizado para a integração.

4. Como obter o token

O token é gerado na Suite OnBlox do cliente. Um administrador deve acessar:

Configuração da conta > Configuração de APIs > Tokens

1. Informar um nome que identifique a integração, com até 60 caracteres.
2. Definir a validade em dias . Valor 0 = sem vencimento.
3. Escolher a permissão: Somente leitura ou Leitura e escrita .
4. Clicar em Gerar token e copiar o valor apresentado.

“ **Exibição única:** O token tem prefixo onbx_ e aparece uma única vez. A Suite OnBlox mantém somente uma representação segura da credencial. Se o token for perdido, gere um novo.

O token herda o usuário que o gerou. Se esse usuário for desativado, o token deixa de funcionar. Recomenda-se utilizar um usuário dedicado à integração . Cada usuário pode possuir até 5 tokens

5. Como enviar o token

Envie o valor puro do token no cabeçalho HTTP X-API-Token , em todas as requisições.

X-API-Token:

onbx_SEU_TOKEN_AQUI

- Não use Authorization: Bearer
- Não envie prefixos adicionais, aspas ou espaços extras.
- Não envie o token na URL, query string, corpo da requisição ou cookies.
- Não há login prévio nem criação de sessão: o token é a própria credencial.

6. HTTPS obrigatório

Todas as requisições autenticadas devem utilizar HTTPS.

https://cliente.exemplo.com.br/onblox/api/...

⚡ **Importante:** Chamadas autenticadas por HTTP são recusadas.

7. Autenticação e autorização

Autenticação verifica se o token apresentado é válido. Autorização determina quais operações esse token pode executar.

Permissão	GET	POST	PUT/PATCH	DELETE
Somente leitura	Sim	Não	Não	Não
Leitura e escrita	Sim	Sim*	Sim*	Sim*

- Quando a respectiva operação existir e estiver disponibilizada pelo endpoint.

8. Integrações com múltiplos clientes

A mesma aplicação pode integrar diferentes clientes OnBlox. Cada cliente deve possuir configuração independente.

```
{  
  "cliente": "Cliente Exemplo",  
  "baseUrl": "https://cliente.exemplo.com.br/onblox",  
  "apiToken": "${ONBLOX_API_TOKEN}"  
}
```

“ **Isolamento por cliente:** Não utilize um único token global para todos os clientes. Antes de realizar uma chamada, selecione a URL e a credencial correspondentes ao cliente que está sendo processado.

9. Erros de autenticação

Recusas de token retornam status HTTP 401 ou 403 . Decida o tratamento pelo status HTTP; o campo message é destinado a pessoas e não deve ser usado como condição no código.

Status	Mensagem	Causa	O que fazer
401	Token de API ausente. Informe o cabeçalho X-API-Token.	Cabeçalho ausente ou vazio	Enviar X-API-Token em toda chamada
401	Token de API inválido.	Valor incorreto, cortado ou de outro cliente	Conferir token e endereço da Suite OnBlox
401	Token de API revogado. Gere um novo token na Suite OnBlox.	Token revogado pelo cliente	Solicitar novo token
401	Token de API vencido. Gere um novo token na Suite OnBlox.	Validade expirada	Solicitar novo token
401	O usuário dono deste token está desativado.	Usuário que gerou o token foi desativado	Reativar usuário ou gerar token por outro usuário
401	Esta API exige HTTPS.	Chamada feita via HTTP	Utilizar HTTPS

Status	Mensagem	Causa	O que fazer
403	Este token é somente de leitura e não pode executar a operação.	Token sem permissão de escrita	Solicitar token com leitura e escrita

“ **Retry:** Não repita automaticamente chamadas que receberam 401 ou 403: o problema está na credencial ou permissão e não se resolve com nova tentativa.

10. Segurança

- Armazene o token em variável de ambiente ou cofre de segredos.
- Nunca inclua o token no código-fonte ou em repositórios Git.
- Não registre o token em logs ou mensagens de erro.
- Utilize um token diferente para cada integração/sistema.
- Conceda somente a permissão necessária.
- Use um usuário dedicado para integrações.
- Se houver suspeita de vazamento, revogue a credencial imediatamente.

“ **Entrega segura:** Prefira cofre de senhas, gerenciador de segredos ou link de uso único. Evite enviar tokens por e-mail, chat, planilhas ou tickets.

11. Rotação do token

Gerar um novo token não revoga automaticamente os tokens existentes. Isso permite realizar a troca sem interrupção da integração.

1. O cliente gera um novo token na Suite OnBlox.
2. O token é entregue ao parceiro por canal seguro.
3. O parceiro atualiza sua configuração.
4. O funcionamento da nova credencial é validado.
5. O cliente revoga o token antigo.

12. Checklist de homologação

Marque os itens para acompanhar o preparo da integração. O progresso fica salvo somente nesta aba do navegador.

- ☐ Token gerado na Suite OnBlox do cliente.
- ☐ Permissão mínima necessária configurada.
- ☐ Token entregue por canal seguro.
- ☐ Token armazenado em variável de ambiente ou cofre.
- ☐ URL e token configurados individualmente por cliente.
- ☐ Todas as chamadas utilizam HTTPS.
- ☐ Todas as chamadas enviam X-API-Token.
- ☐ Token não aparece em logs ou mensagens de erro.
- ☐ Erros 401/403 não possuem retry automático.
- ☐ Responsável pela rotação da credencial definido.
- ☐ Tokens com validade têm troca planejada antes do vencimento.

13. Suporte

Ao abrir um chamado relacionado à API, informe:

Contexto: Cliente e URL base, sem informações sensíveis.

Requisição: Endpoint, método HTTP, data e horário da chamada.

Retorno: Status HTTP e campo message retornado pela API.

“ **Nunca envie o API Token:** Não envie o token em chamados, e-mails ou mensagens.

Contato OnBlox: contato@onblox.com.br

14. Histórico de revisões

Versão	Data	Alteração
1.0	06/10/2026	Primeira versão publicada para parceiros e sistemas integradores.

Revision #3
Created 6 October 2026 19:18:16 by André Segatto Carrasque
Updated 6 October 2026 20:06:53 by André Segatto Carrasque