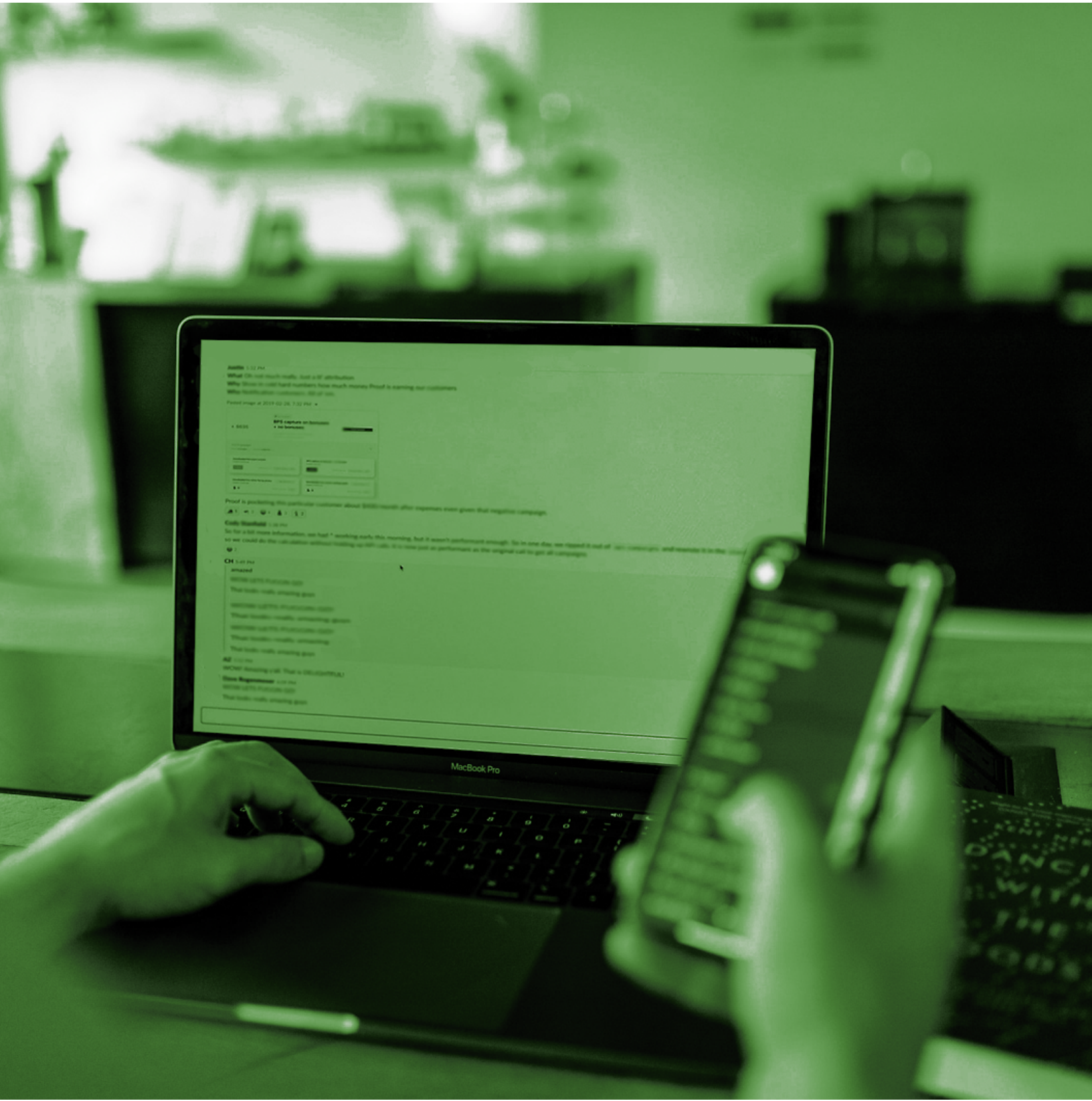
Duo Security ahora es parte de Cisco.

Guía de soporte técnico

Originalmente publicado el 22 de junio de 2016
Versión 4.0 publicada el 25 de marzo de 2020



Términos utilizados frecuentemente

Algunos términos que puede encontrar en los documentos de Duo, entre su equipo de TI interno, o de los usuarios finales:

2FA (autenticación del segundo factor): capa adicional de autenticación más allá de un nombre de usuario o una contraseña. 2FA implica algo que usted sabe (contraseña) y algo que tiene con usted (como Duo Mobile en su smartphone) para evitar que alguien simplemente "conozca" su contraseña y acceda a sus datos. Cuando la 2FA de Duo está habilitada, debe seguir ingresando su nombre de usuario y contraseña; Duo no reemplaza su nombre de usuario y contraseña. Es solo una capa agregada de seguridad sobre las credenciales existentes. Consulte este video para obtener más información.

Panel de administración de Duo: interfaz protegida por inicio de sesión, en la que los administradores de Duo pueden administrar sus usuarios, dispositivos, integraciones, roles, registros, información de facturación, etc.

Duo Prompt: esto permite a los usuarios elegir cómo verificar su identidad cada vez que inician una sesión (por ejemplo, "Duo Push" o "Call") en una aplicación basada en la web. Duo Prompt permite la inscripción y la autenticación en línea.

Código de acceso: estos pueden generarse a través de la aplicación Duo Mobile, SMS (mensaje de texto) o el token de hardware de un usuario.

Plataforma: tipo de dispositivo de autenticación de usuario (iPhone, Android, teléfono fijo, etc.).

Notificación automática (Duo Push): solicitud de autenticación fuera de banda que se envía a la aplicación Duo Mobile en un dispositivo inscrito. Las notificaciones automáticas incluyen información de ubicación del usuario, dirección IP y la aplicación a la que intenta acceder el usuario.

Portal de autoservicio: si el portal de autoservicio se habilitó en el Panel de administración de Duo, esto significa que un usuario puede agregar dispositivos adicionales o actualizar las configuraciones del método de autenticación desde Duo Prompt. Disponible para todas las ediciones de pago de Duo.

Parte 1: Descripción general

¿Por qué necesito esta guía?

La implementación de la autenticación del segundo factor (con frecuencia llamada 2FA) en su empresa puede producir preguntas de los usuarios finales. Si bien Duo se enorgullece de su fácil configuración e interfaz sencilla, entendemos que la experiencia de autenticación de Duo puede ser confusa en un principio para algunas personas, especialmente si nunca han utilizado dos factores anteriormente. Este documento está diseñado con el fin de proporcionarle respuestas rápidas para abordar los problemas que los usuarios finales pueden encontrar al utilizar Duo.

Esta guía está diseñada con el fin de que la utilicen los administradores con roles administrativos específicos para ayudar a los usuarios finales a completar tareas comunes y resolver problemas. Puede leer más información sobre la diferencia entre las cuentas de Duo para los administradores y los usuarios finales aquí.

Duo recomienda tener al menos dos propietarios de Duo para cualquier cuenta determinada. Asimismo, es importante actualizar periódicamente su lista de administradores, ya que los propietarios pueden entrar o salir de su organización. Tener dos Propietarios proporciona acceso redundante al Panel de administración de Duo y garantiza un nivel de acceso más uniforme en caso de que un Propietario no esté disponible. Descubrimos que tener varios propietarios ahorra tiempo a los clientes al permitir que ellos mismos se ocupen de sus necesidades administrativas.

Aquí le presentamos una descripción rápida de los roles y su acceso a las tareas completas dentro del Panel de administración de Duo:

	Rol de propietario	Rol de administrador	Rol de administrador de aplicaciones	Rol de administrador de usuarios	Rol de soporte técnico	Rol de facturación	Función de solo lectura
Ver y descargar registros	✅	✅	✅	✅	✅		✅
Administrar dispositivos 2FA y códigos de desvío	✅	✅		✅	✅		
Administrar usuarios y grupos	✅	✅		✅			
Administrar aplicaciones	✅	✅	✅				
Modificar configuración global	✅	✅					
Ver y administrar facturación	✅					✅	
Administrar otros administradores	✅						

Además, la función Unidades administrativas de Duo permite a los administradores en las ediciones de pago agrupar a los usuarios y a las aplicaciones de Duo, así como asignar privilegios de administración a los administradores designados. Puede obtener más información sobre Unidades administrativas aquí: https://duo.com/docs/administrative-units. Nota: Los administradores que están restringidos no verán usuarios ni aplicaciones en otros grupos.

Parte 2: Inscripción y activación

¿Cómo será la experiencia de inscripción para los usuarios finales?

Los usuarios tienen dos opciones: iniciar el proceso de inscripción desde un dispositivo que no sea con el que planean autenticarse (como una computadora de escritorio o portátil que usarán para acceder a los servicios protegidos por Duo) o con lo que finalmente será su dispositivo de autenticación (como su teléfono móvil).

Inscribirse desde una computadora portátil, una computadora de escritorio u otro dispositivo que no sea de autenticación

Los usuarios comenzarán con el enlace proporcionado en el correo electrónico de inscripción. Al usar el aviso de inscripción, los usuarios pueden escanear un código QR con su dispositivo de autenticación:

Si un usuario dice que no puede escanear el código QR, pídale que verifique que haya permitido el acceso de la aplicación a la cámara del teléfono; de lo contrario, no podrá escanear el código. Encontrará más información sobre este proceso en nuestra Guía de inscripción: https://guide.duo.com/enrollment

Inscribirse desde su dispositivo de autenticación

Con este método, los usuarios comenzarán la configuración desde el correo electrónico de inscripción en su dispositivo móvil, se inscribirán y, finalmente, instalarán Duo Mobile si es necesario. Encontrará más detalles en este artículo de la base de conocimientos: https://help.duo.com/s/article/3890

¿Cómo reenvío los correos electrónicos de inscripción?

Los correos electrónicos se pueden volver a enviar a los usuarios que se hayan creado mediante la inscripción masiva o la sincronización de Active Directory y que aún no hayan completado la inscripción. Siga el proceso que se detalla en el paso 5 de la autoinscripción masiva aquí para volver a enviar correos electrónicos de inscripción: https://duo.com/docs/enrolling_users#bulk-self-enrollment

Parte 3: Autenticación y métodos de autenticación

¿Cómo agrego o activo un nuevo dispositivo de autenticación?

Este proceso explica cómo agregar o activar un nuevo dispositivo de autenticación (por ejemplo, un teléfono móvil, un teléfono fijo, una tableta o un token de U2F) para un usuario. Si el portal de autoservicio dentro de Duo Prompt está habilitado (disponible solo para las ediciones de pago de Duo), los usuarios pueden agregar nuevos dispositivos. Si el portal de autoservicio no está habilitado, solo los administradores pueden agregar dispositivos.

Tenga en cuenta que los usuarios solo pueden agregar un dispositivo nuevo a través del portal de autoservicio si tienen acceso a otro dispositivo de autenticación previamente activado o a un código de desvío. Si no tienen acceso a ninguno de los dos, un administrador debe ayudarlos a agregar un nuevo dispositivo.

Si el portal de autoservicio está habilitado: https://guide.duo.com/add-device
Manualmente mediante el Panel de administración de Duo: https://duo.com/docs/administration-devices

¿Qué debo hacer si un usuario olvida su dispositivo?

¿Tiene un usuario que dejó su token de teléfono o hardware en su casa? Consulte este artículo de la base de conocimiento para conocer las maneras en que puede ayudar: https://help.duo.com/s/article/3302

¿Qué debo hacer si pierdo o me roban mi dispositivo?

Siempre insístale al usuario que se ponga en contacto con un administrador de forma inmediata si pierde o le roban su dispositivo de autenticación de 2FA.

Si el portal de autoservicio está habilitado y un usuario tiene un segundo dispositivo de autenticación, debe acceder inmediatamente al menú "Mis configuraciones y dispositivos" de Duo Prompt y eliminar el dispositivo perdido o robado. Si el usuario no tiene un autoservicio habilitada o un segundo dispositivo de

autenticación, un administrador debe eliminar el dispositivo de Duo después de asegurarse de que se haya agregado un nuevo método de autenticación.

Si el portal de autoservicio está habilitado: https://guide.duo.com/common-issues#lost-phone
Manualmente mediante el Panel de administración de Duo:
https://duo.com/docs/administration-devices#dealing-with-lost-or-stolen-phones

¿Cómo puedo ayudar a los usuarios que necesitan autenticarse en un avión o mientras están viajando a un lugar remoto?

Informe a los usuarios que la aplicación Duo Mobile se puede utilizar para generar códigos de acceso en aviones u otros lugares en los que Duo Push, los nuevos lotes de códigos de acceso entregados por SMS o la devolución de llamadas no estén disponibles. Consulte las guías del usuario final para autenticarse con los códigos de acceso generados Duo Mobile en Android o iOS. Obtenga más información en la Guía de viajes de Duo.

¿Por qué no recibo las notificaciones de Duo Push?

En primer lugar, asegúrese de que el usuario permita la recepción de notificaciones en su teléfono.

Es posible que los usuarios tengan problemas para recibir solicitudes de Push si hay problemas de red entre el teléfono y el servicio de Duo. Muchos teléfonos tienen problemas para determinar si se debe utilizar el canal de datos Wi-Fi o celular cuando se revisan las solicitudes de Push, y el solo hecho de poner el teléfono en el modo aeroplano y luego de nuevo en el modo de funcionamiento normal a menudo resuelve este tipo de problemas si hay una conexión a Internet confiable disponible. De manera similar, el problema puede resolverse apagando la conexión Wi-Fi en el dispositivo y utilizando la conexión de datos celulares. Una notificación Duo Push es de solo 2 KB.

Verifique la hora y la fecha en el teléfono y asegúrese de que sean correctas. Si la fecha y la hora en un teléfono se configuran manualmente, intente cambiar la configuración del dispositivo para sincronizar la fecha y la hora automáticamente con la red.

También hemos creado guías de solución de problemas detalladas para la entrega de Push Duo para iOS: https://help.duo.com/s/article/2051 y Android: https://help.duo.com/s/article/2050. Tenga en cuenta que puede ser necesario un administrador de TI con la capacidad de modificar el acceso a los puertos según el problema específico que se encuentre.

¿Cómo asigno tokens a los usuarios?

Los tokens comprados a través de Duo se importan automáticamente a su cuenta. Los administradores deben importar manualmente la información de token del OTP de proveedores terceros. Al importar tokens, tenga en cuenta que los tokens deben ser exclusivos entre las cuentas de Duo.

Duo admite los tokens de U2F de FIDO, pero los tokens de U2F no se pueden importar o asignar a los usuarios desde el Panel de administración. En cambio, los usuarios se autoinscriben en el token de U2F a través del aviso de inscripción Duo o el portal de autoservicio. Consulte nuestra documentación sobre cómo

habilitar la autenticación de U2F y el proceso de inscripción de U2F para que los usuarios finales obtengan más información.

Para asignar un token a un usuario final:
https://duo.com/docs/administration-devices#assigning-a-token-to-an-end-user

¿Cómo se generan los códigos de desvío?

Un código de desvío es un código de acceso temporal creado por un administrador para un usuario específico. Generalmente, se utilizan como "códigos de respaldo", de modo que los usuarios que tienen problemas con sus dispositivos móviles (por ejemplo, el servicio móvil se interrumpe, el dispositivo se pierde o lo roban, etc.) aún puedan acceder a sus sistemas protegidos por Duo. Los códigos de desvío también se pueden utilizar para permitir que un usuario temporal acceda a las aplicaciones que no admiten la autoinscripción sin haber inscrito un dispositivo. Los códigos de desvío caducan después de haberlos utilizado el número de veces permitido, o después de una cantidad de tiempo definida por el administrador. De manera predeterminada, los códigos de desvío caducan después de un solo uso o después una hora, lo que ocurra primero.

Para generarlos, siga el proceso aquí: https://duo.com/docs/administration-users#generating-a-bypass-code

¿Cómo puedo ayudar a un usuario que está bloqueado?

Un usuario que está en estado "bloqueado" ha pasado el umbral designado para los intentos de autenticación y necesitará que su estado cambie de nuevo a "activo". Obtenga más información sobre los estados de los usuarios y cómo cambiarlos aquí:
https://duo.com/docs/administration-users#changing-user-status

Parte 4: Consejos profesionales

Los usuarios pueden estar en alerta máxima por suplantación de identidad

Si acaba de implementar la educación de Duo internamente, es posible que los usuarios sean sospechosos de las comunicaciones que reciben, como el correo electrónico de inscripción y activación de Duo. Es posible que reciba inquietudes por parte de los usuarios de que están siendo objeto de suplantación de identidad a través de este correo electrónico. Si desea revisar las comunicaciones que se enviaron, puede ver el correo electrónico o la copia de SMS en el Panel de administración de Duo y/o pedirle al usuario que le envíe una copia dell mensaje que recibió para que pueda verificar que es un mensaje seguro y continuar con la inscripción/autenticación.

Anime a los usuarios a usar Duo Push

Siempre anime a los usuarios a usar Duo Push, si es posible. Duo Push es la mejor opción: es conveniente, seguro y el más barato (no hay cargos de telefonía para la autenticación de Push). Los usuarios también pueden usar Push si no tienen servicio celular, y funciona en cualquier país.

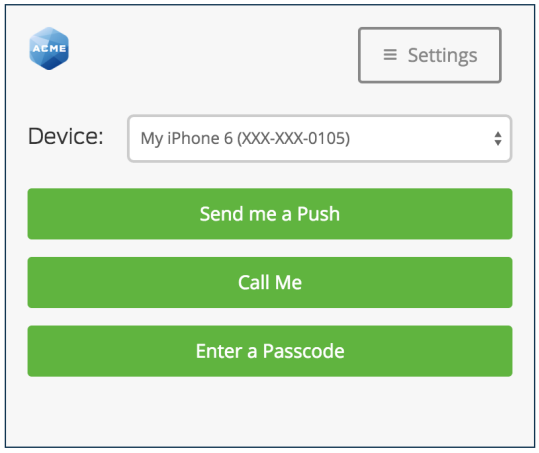
También hemos creado una guía para ayudar a promover Duo Push con los usuarios: https://help.duo.com/s/article/promoting-push

Verifique las identidades de los usuarios con Help Desk Push

Es posible que desee verificar la identidad de los usuarios con un rápido Duo Push antes de ayudarlos o implementar cualquier cambio a su solicitud. Consulte la siguiente documentación para obtener más información sobre cómo utilizar Help Desk Push: https://duo.com/docs/administration-users#verifying-users-with-duo-push

Duo Prompt de un usuario puede formatearse de manera diferente de lo que espera

Si un usuario inicia sesión desde un dispositivo más pequeño (como una tableta) o una pequeña ventana de navegador, Duo Prompt puede verse ligeramente diferente de lo que ha visto en la documentación del usuario final. Sin embargo, tiene las mismas funcionalidades que otros usuarios con los mismos derechos.



Pasar no-reply@duosecurity.com a la lista de excepciones

Si su organización utiliza el filtrado de correo electrónico, pase esta dirección a la lista de excepciones; de lo contrario, los usuarios no podrán recibir correos electrónicos de inscripción o activación.

Los enlaces de activación y los enlaces de inscripción tienen distintas fechas de caducidad.

Un enlace de inscripción caduca en 30 días. Si vuelve a enviar un correo electrónico de inscripción, esto no restablecerá la fecha de inscripción.

Un enlace de activación caduca, de manera predeterminada, después de 24 horas. Los usuarios que recientemente recibieron enlaces de activación desde el Panel de administración de Duo no pueden recibir un nuevo enlace hasta que caduque el enlace existente.

Encontrará más información sobre la mensajería de activación e inscripción en https://duo.com/docs/enrolling_users.

Parte 5: Solución de problemas y soporte

Recursos de solución de problemas

Todos los procesos del Panel de administración de Duo y las recomendaciones de configuración de la aplicación están disponibles en el inicio de la documentación exhaustiva de Duo en duo.com/docs.

help.duo.com es el hogar de la base de conocimientos de Duo: un repositorio de búsqueda de recursos de solución de problemas y contenido de autoservicio.

Visite la comunidad de Duo en community.duo.com para ver si la respuesta que busca está en una publicación anterior o iniciar un debate por su cuenta.

¿Tiene problemas con la autenticación o para acceder al Panel de administración de Duo? Nuestro equipo de soporte actualiza la página de estado de Duo en https://status.duo.com en tiempo real para reflejar cualquier problema de servicio. Los administradores de Duo con el rol de administrador y el rol de Propietario se registran automáticamente para recibir actualizaciones de la página de estado para su implementación.

¡Le recomendamos enfáticamente que se suscriba! Obtenga más información sobre cómo suscribirse a la página de estado..

Consultar el Informe de registro de autenticación puede ser útil para solucionar problemas de inicio de sesión de usuarios. Específicamente, familiarícese con las razones de las autenticaciones denegadas. Obtenga más información en este artículo de la base de conocimientos: https://help.duo.com/s/article/1023

Cómo obtener el mejor soporte posible de Duo

Si no encontró la información que necesitaba, esto es lo que necesitará para comunicarse con el equipo de soporte de Duo:

- Asegúrese de que la persona que se comunique con el soporte aparezca como administrador en el Panel de administración de Duo.
- Si tiene un rol administrativo distinto de Propietario, el soporte de Duo solo podrá ayudarlo con su nivel de acceso.
- Si se trata de dispositivos o aplicaciones fuera de Duo (por ejemplo: Active Directory), asegúrese de que esté disponible un administrador que tenga acceso a ellos.
- Asegúrese de proporcionar capturas de pantalla y archivos de registro siempre que sea posible.
- Su ID de cuenta.
- La capacidad de verificar su identidad a través de la autenticación de Duo. Las instrucciones para habilitar Duo Push para la autenticación del administrador en su smartphone están disponibles aquí: https://duo.com/docs/administration-admins#use-duo-push-for-administrator-authentication

    - Si no puede activar Duo Push para la verificación del administrador, puede tardar más tiempo en validar su identidad al comienzo de una llamada a Soporte, ya que necesitaremos usar otro método.
- Si incluye su proxy de autenticación.cfg u otros archivos confidenciales, asegúrese de no compartir **nunca** una clave secreta (SKEY) a través del texto sin formato. Recomendamos un cifrado GPG.
- Si se ha comunicado previamente con el soporte de Duo sobre el mismo problema, incluya los números de ticket existentes.

Determine cómo y cuándo comunicarse con el soporte de Duo en función de su edición y urgencia: https://help.duo.com/s/article/1441