

Autotask Two-Factor Authentication Release

OUTLINE

- Overview
- Login Workflow
- Administration
- Ordering Tokens
- Pricing
- Supported Login Pages

OVERVIEW

[Two-Factor Authentication](#) (2FA) is an optional, enhanced security feature that enables you to activate a secondary layer of user access control to the Autotask application. The standard username and password is the first layer, and a special, temporary one-time-password is the second layer (or “factor”).

What makes 2FA meaningfully more secure is that the second factor is dynamic and temporal; a one-time-password is dynamically generated on demand by the user, by means of a device called a token, and can only be used at that moment for that particular user. It cannot be shared with or acquired by another individual either inadvertently or intentionally. 2FA is commonly used for access to highly sensitive equipment (like production servers), highly sensitive software applications (like banking websites) and highly sensitive proprietary systems (like enterprise networks).

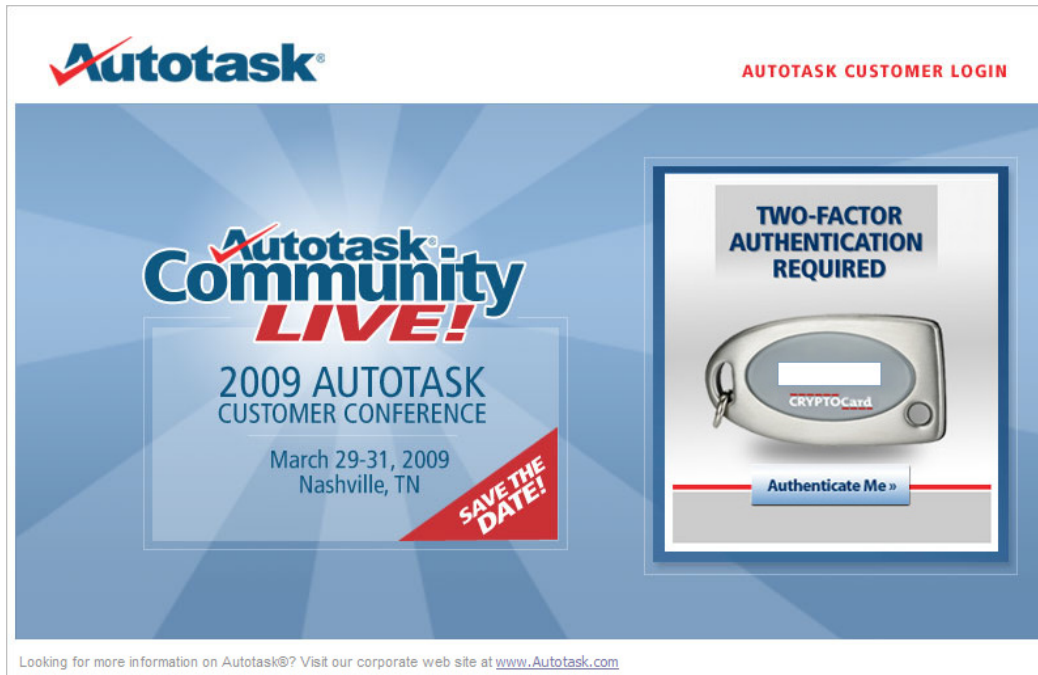
Key Benefits:

- Verifies the identity of all authenticated user sessions (even authorized users cannot “share” or “lend” passwords)
- Adds an extra layer of security protection for sensitive data such as customer lists, configuration management (coming soon to Autotask!) or billing information
- Allows your technicians to log in from remote PC’s in the field without the threat of key-loggers or “pass-along” credential vulnerability



LOGIN

When a user is configured for 2FA the login experience is only slightly different. First, the user enters their standard username and password on the default login page for either Autotask or Autotask LiveMobile. When the standard credentials are authenticated, the user then sees a secondary login page for the One-Time-Password (OTP). The user simply presses the button on the token for an OTP, enters the code and is fully authenticated into your database.



Standard
OTP Login



Autotask
LiveMobile
OTP Login

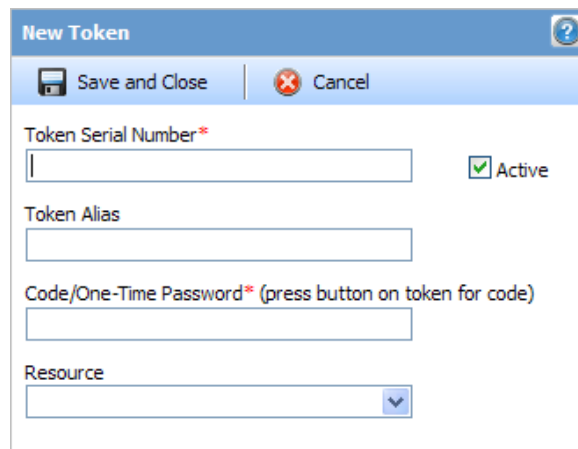
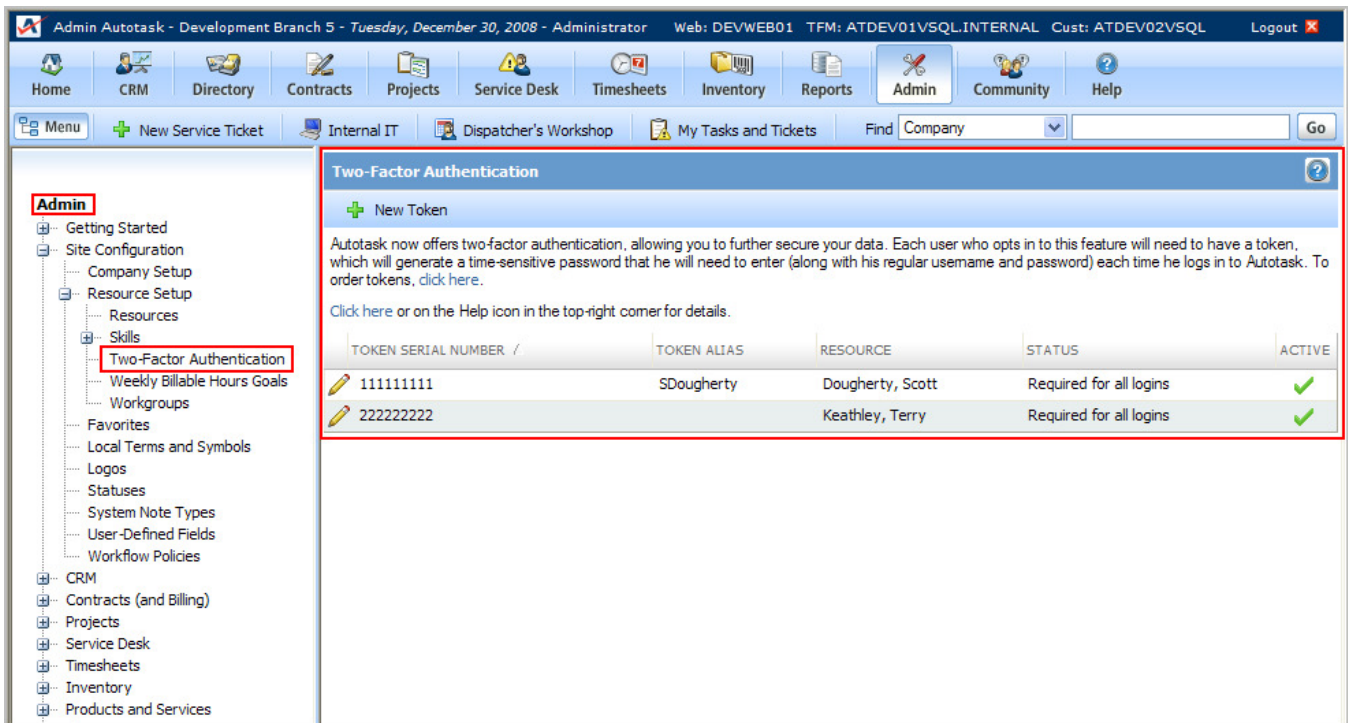
Your Autotask Administrator will have the tools to manage activation and use of 2FA for your resources.

I. Managing Tokens

When you receive your tokens from Autotask, the first step is to enter them into the system. Each resource configured for 2FA must have a unique, active token assigned to their profile.

System entry is simple. Go to Admin > Site Configuration > Resource Setup > Two-Factor Authentication to enter and activate tokens. The first time a new token is added, you will be prompted to test the OTP code one time to verify that you have entered the correct serial number. Once the token is saved, it can be assigned to any active resource, requiring that resource to enter an OTP anytime they login. A token can also be given an alias (i.e. nickname) to make it easier to track and assign.

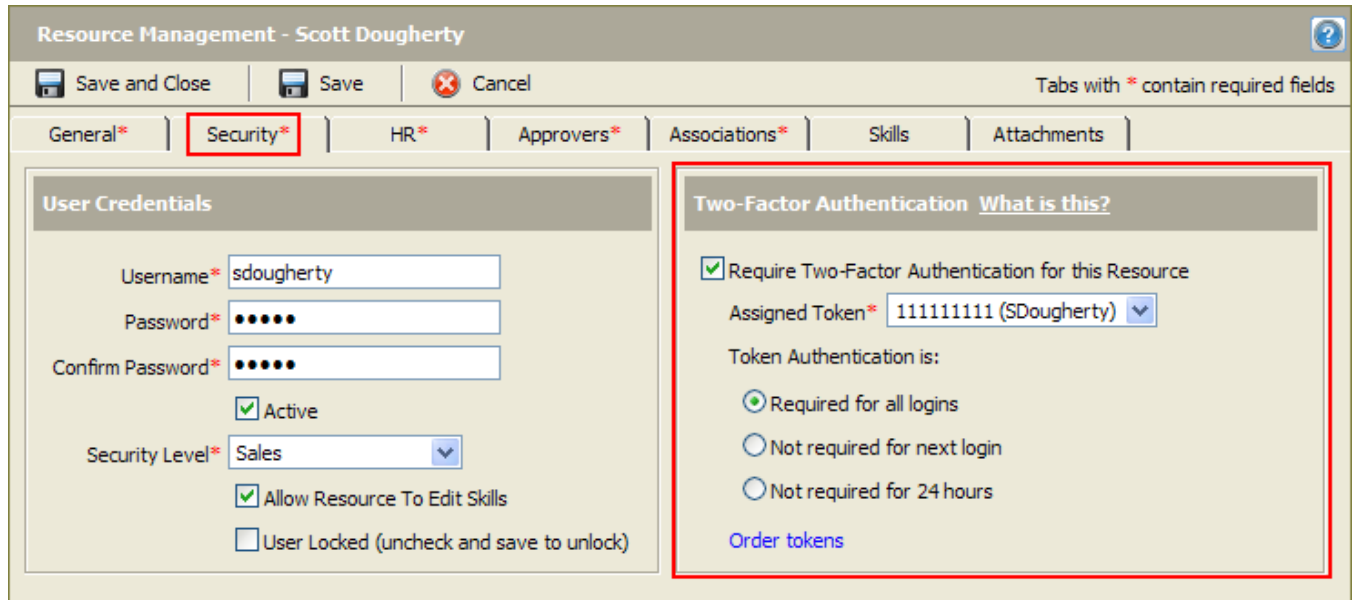
Note – a token can only be entered in the system from the token management page, but it can be assigned to a user from either the token page or the Resource edit page. A token can also be activated and not assigned to a user.



II. Managing Resources

The Resource edit page has a new section in the Security tab for managing 2FA. When the “Required Two-factor Authentication for this Resource” box is checked, the user will be prompted with the secondary OTP entry page before successfully authenticating.

The Resource page also lets you suspend the 2FA login requirement temporarily in the event a user loses their token or mistakenly leaves it home.



Resource Management - Scott Dougherty

Save and Close Save Cancel Tabs with * contain required fields

General* Security* HR* Approvers* Associations* Skills Attachments

User Credentials

Username*: sdougherty

Password*: ●●●●

Confirm Password*: ●●●●

Active

Security Level*: Sales

Allow Resource To Edit Skills

User Locked (uncheck and save to unlock)

Two-Factor Authentication [What is this?](#)

Require Two-Factor Authentication for this Resource

Assigned Token*: 111111111 (SDougherty)

Token Authentication is:

Required for all logins

Not required for next login

Not required for 24 hours

[Order tokens](#)

ORDERING TOKENS

Our token supplier is [CRYPTOCARD](#), a world class provider of enterprise authentication and IT security solutions. The CRYPTOCARD model we are using is highly durable, housed in an aluminum casing, has an average lifespan of 5-7 years and uses user-replaceable batteries.



Tokens must be ordered and purchased from Autotask before implementing 2FA for your users. You can order tokens from the Resource edit page and the token management page (Admin > Site Configuration > Resource Setup > Two-Factor Authentication).

The online order form will show current pricing and allow you to specify quantity and shipping address. Custom inquiries and miscellaneous questions can be sent to tokensales@autotask.com.



The image shows a web form titled "Two-Factor Authentication Token Order Form". At the top left is an image of a CRYPTOCard token. The form contains several sections: a header with the title and token image; a paragraph of instructions; an "Account Information" section with fields for Company Name, Requested By, and Shipping Address; an "Order Information" section with a quantity input field and pricing details; a "Terms & Conditions" section with an acceptance checkbox; and two buttons at the bottom: "Submit Order" and "Cancel".

**Two-Factor Authentication
Token Order Form**

Complete this Order Form to order your CRYPTOCard tokens. Please make any necessary corrections to your shipping address directly in the Shipping Address box below. Your request will be processed within 2 business days and you should receive your tokens within 10 business days (shipment time for international orders may vary). If you have any questions about your order, please email tokensales@autotask.com.

Account Information

Company Name
Development Branch1 INC

Requested By
Autotask Administrator

Shipping Address*
125 Winslow Street
Hudson, NV 45131

Order Information

Number of tokens requested*
\$149 / £115 / €130 per token, plus [shipping & handling](#) (and any applicable taxes and surcharges). This is a limited time special "pay once" pricing offer. Future regular pricing will include an additional monthly service fee for the lifetime of each token.

Note: Shipping and handling costs will be waived for any orders placed before December 31, 2008 and shipped to a US location.

Terms & Conditions

I accept the [Terms & Conditions](#) and understand my company will be billed by Autotask for this token order, in the currency of my Autotask agreement, on my next monthly invoice.

PRICING

The cost for 2FA is \$149 / £115 / €130 per token. This includes the monthly service fee for the lifetime of the token, and is a limited time offer. Later in 2009, there will be a monthly service fee for all tokens purchased after the new rate plan is implemented. Shipping costs (and applicable taxes or surcharges) will be added to each order, and may vary from time to time. Current shipping costs will always be posted on the token order page.

SUPPORTED LOGIN PAGES

2FA works for Autotask, Autotask LiveMobile and any existing authentication workflow that hits the standard login page (e.g. ExecuteCommand API). It is currently supported in the hosted version of Autotask only.