

Doulci activator v7 username and password download

To set up your username and password, you need either your order number or your account number. You received an order number in the confirmation emails you received an order number or your account number. You can also check the footer of subsequent emails you received an order number or your account number. both your order number and your account number. Once you have your order number, set up your personal Username and Password. If you need further assistance, please call Customer Service at 1-866-206-0435. Remember, your Password is case sensitive, so you must type it in exactly the way you set it up. (Check to make sure your Caps Lock button isn't advertently on or off.) If you can't remember your Password, click here to reset it. If you wish to change your Username or Password, click here. No need. Your existing Username and Password, click here to reset it. If you wish to change your Username or Password, click here to reset your password, click here to reset it. If you wish to change your Username or Password, click here to reset it. If you wish to change your Username or Password, click here to reset it. you are a subscriber. You received an order number in the confirmation e-mail that was delivered to you when you completed your order for Fidelity Investor online. You will also see both your order number and your account number referenced in the Hotline or issue notice emails you receive, and you can then use either one to set up your Username and Password for entering the subscriber-only website. If you did not place your order online or you can't find your order number, please call Customer Service at 1-866-206-0435 and a representative will be able to assist you. What's This? You don't want to own too many funds that are similar, but how do you tell? A high correlation between funds may mean that your portfolio of funds is not as diverse as you might want it to be. While other tools may compare funds only to the S&P 500, you can use this tool to determine how closely the performance of one Fidelity stock fund tracks that of any other Fidelity stock fund. Select a fund to compare AM: 20%AM: 30%AM: 40%AM: 50%AM: 60%AM 70%AM: 85%AZ MuniBalancedBlue Chip GrowthBlue Chip ValueCA Ltd Term Tax FreeCA MuniCT MuniCanadaCapital & IncomeCapital AppreciationChina RegionConservative Income BondContrafundConvertible SecsCorporate BondDisciplined EquityDiversified Int'lDividend GrowthEmerg Eur, ME, AfricaEmerg Mkts DiscoveryEmerg Mkts IdxEmerging AsiaEmerging MktsEquity Dividend IncomeEquity-IncomeEuropeExport & MultinationalExtend Mkt IdxFBNDFCOMFCORFDISFDLOFDMOFDRRFDVVFENYFHLCFIDIFIDUFIVAFLTBFMATFNCLFQALFRELFSTAFTECFUTYFVALFidelity FundFloating Rate Hi Inc Focused High IncFocused StockFour-in-One IndexFreedom 2005Freedom 2010Freedom 2020Freedom 2020Freedom 2020Freedom 2020Freedom 2030Freedom 2030F Index 2040Freedom Index 2050Freedom Index 2050Fr Bond IndexInt'l DiscoveryInt'l Enhanced IndexInt'l Small Cap OppsInt'l Small CapInt'l Small CapInt'l Small Cap OppsInt'l Sustainability IdxInt'l Neuronational Capital AppreciationInvestment Grade BondJapanJapan Sm CosLarge Cap Core Enhanced IndexLarge Cap Growth Enhanced IndexLarge Cap Growth IndexLarge Cap StockLarge Cap StockLarge Cap Value Enhanced IndexLarge Cap Value IndexLarge Cap Value Enhanced Index Va 2010Managed Retirement 2015Managed Retirement 2025Managed Retirement 2025Managed Retirement IncomeMega Cap StockMid Cap IndexMid Cap Index IndexMid MillenniumNordicOH MuniONEQOTCOverseasPA MuniPacific BasinPuritanReal Estate IncomeReal Estate IndexS&P 400 IndexS&P 500 I Communications EquipmentSelect Consumer StaplesSelect Consumer StaplesSelect Consumer StaplesSelect Consumer StaplesSelect Consumer StaplesSelect EnergySelect EnergySelect EnergySelect Financial SvcsSelect Health Care SvcsSelect IT ServicesSelect IndustrialsSelect IndustrialsSelect InsuranceSelect Natural GasSelect Duration Hi IncShort-Term BondShort-Term BondShort-Term Bond IndexSmall Cap Enhanced IndexSmall Cap Enhanced IndexSmall Cap Enhanced IndexSmall Cap Enhanced IndexSmall Cap Stock Selector All CapStock Selector All CapStoc Large Cap ValueStock Selector Small CapStrategic Dividend & IncomeStrategic Real ReturnTax-Free BondTelecom & UtilitiesTotal Int'l EquityTotal Int'l EquityT Consumer StaplesVIP ContrafundVIP Disciplined Small Cap VIP Dynamic Cap AppVIP E-IVIP Emerging MarketsVIP EnergyVIP Financial ServicesVIP Freedom 2015VIP Freedom 2015VIP Freedom 2025VIP Free FundsManager 60VIP FundsManager 70VIP FundsManager 85VIP Gov't MMVIP Growth OppVIP Health CareVIP Mid-CapVIP Mid-CapVIP Mid-CapVIP IndustrialsVIP Mid-CapVIP Mid-CapV DiscoveryValue Strategies Worldwide Select a fund to compare AM: 20%AM: 30%AM: 40%AM: 50%AM: 60%AM: 70%AM: 85%AZ MuniBalancedBlue Chip ValueCA Ltd Term Tax FreeCA MuniConservative Income BondContrafundConvertible SecsCorporate BondDisciplined EquityDiversified Int'lDividend GrowthEmerg Eur, ME, AfricaEmerg Mkts DiscoveryEmerg Mkts IdxEmerging AsiaEmerging MktsEquity Dividend IncomeEquity-IncomeEuropeExport & MultinationalExtend Mkt IdxFBNDFCOMFCORFDISFDLOFDMOFDRRFDVVFENYFHLCFIDIFIDUFIVAFLTBFMATFNCLFQALFRELFSTAFTECFUTYFVALFidelity FundFloating Rate Hi Inc Focused High IncFocused StockFour-in-One IndexFreedom 2005Freedom 2010Freedom 2010Freedom 2025Freedom 2025Freedom 2035Freedom 2040Freedom 2045Freedom 2045Freedom 2010Freedom 2010Freedom 2020Freedom 2010Freedom 2010Freedom 2010Freedom 2010Freedom 2010Freedom 2020Freedom 2010Freedom 2010Fr 2050Freedom 2055Freedom Index 2025Freedom Index StockGlobal CreditGlobal Equity IncomeGlobal High IncomeGlobal ex U.S. IndexGov't IncomeGrowth & IncomeGrowth DiscoveryInt'l Enhanced IndexInt'l ComeGrowth DiscoveryInt'l Enhanced IndexInt'l Small Cap OppsInt'l Sustainability IdxInt'l ComeGrowth DiscoveryInt'l Enhanced IndexInt'l ComeGrowth & IncomeGrowth CompanyGrowth DiscoveryInt'l Enhanced IndexInt'l ComeGrowth DiscoveryInt'l Enhanced IndexInt'l Enhanced IndexInt'l Enhanced IndexInt'l ValueInterm MuniInterm Treasury Bd IndexIntermediate BondIntermediate Gov't IncInternational Capital AppreciationInvestment Grade BondJapanJapan Sm CosLarge Cap StockLarge Cap Value IndexLarge Cap Value IndexLatin AmericaLeveraged Co StockLimited Term BondLimited Term Gov'tLimited Term MuniLong-Term Treaury Bd IndexLow-Priced StockMA MuniMD MuniMI MuniMSCI EAFE IndexMagellanManaged Retirement 2015Managed Retirement 2010Managed Retire IndexMid Cap IndexMid Cap ValueMid-Cap StockMortgage SecsMuni IncMunicipal Inc 2023Municipal Inc IndexS&P 400 IndexS&P 500 IndexSelect Communications EquipmentSelect Communications EquipmentSelect Consumer FinanceSelect Consumer FinanceSelect Consumer StaplesSelect Defense & AerospaceSelect EnergySelect EnergySelect EnergySelect EnergySelect IndustrialsSelect Industrial PharmaceuticalsSelect RetailingSelect SemiconductorsSelect Software & IT SvcsSelect TechnologySelect TelecommunicationsSelect WirelessShort Duration Hi IncShort-Term Bond IndexShort-Term BondShort-Term Bond IndexShort-Term Treasury Bd IndexSimplicity RMD 2010Simplicity RMD 2020Simplicity R IncomeSmall Cap DiscoverySmall Cap Enhanced IndexSmall Cap GrowthSmall Cap Stock Selector Small Cap Stock Select EquityTotal Int'l IndexTotal Mkt IdxTrendU.S. Bond IndexU.S. Sustainability IdxVIP AMVIP AM: GrowthVIP BalancedVIP Consumer StaplesVIP Consumer StaplesVIP Consumer StaplesVIP Consumer StaplesVIP Floating Rate Hi IncVIP Freedom 2005VIP Freedom 2010VIP Freedom 2020VIP Freedom IndustrialsVIP International Cap AppVIP Inv GradeVIP MaterialsVIP Mid-CapVIP OverseasVIP Real EstateVIP Strategics Worldwide Interested in Infosec & Biohacking. Security Architect by profession. Love reading and running."Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months." — Clifford StollWe use keys to unlock doors and use locks to protect our private properties. In the digital world, we do the same. While keys have many "forms," the most common one is still the password. Password have been used as the foundation of authentication for years. While passwords are still a large portion of our cyber landscape, they have been on the decline for more than a decade. But eventually, we will face a time when the password is no longer proof of our digital self. Principally, using a password to get access to a system is a method of authentication. According to (ISC)² CBK Common Body of Knowledge — ISC2, authentication is when the user provides a credential to the system to prove the identity. Authentication factor can be of the following types: Something you KNOW. It is a mechanism of having one factor of authentication. A system relies on a secret that the login users must memorize and exhibit to prove their identity. This case may seem straightforward enough, but it has profound implications. The Problem with PasswordsSimple authentication methods that solely require username and password are intrinsically vulnerable. Attackers could guess or steal credentials and gain unauthorized access to sensitive information and systems using various techniques, including:Brute force attacks — using programs to generate random username/password slike "123456." Phishing — using fake emails or text messages to trick a victim into replying with their credentialsMan-in-the-middle attacks — intercepting communications traffic (over public WiFi, for example) and replaying credentials from an account to log in to other accounts that belong to the same user (people often use the same username/password combination for multiple accounts)Keylogging — installing malware/ hardware on a computer to capture username/password keystrokesPassword FatigueToday, we all rely on various apps to perform our jobs. By that, we are forced to memorize and track all the login credentials for each one of them. Moreover, changing passwords frequently is tiring for us in front of a computer. Flooded by password sprawl, users take risky alternatives like applying the same passwords, or posting passwords, or posting passwords, or posting passwords, or posting passwords on sticky notes. Bad actors can take advantage of the loose cyber hygiene practices in password sprawl, users take risky alternatives like applying the same passwords, or posting passwo unauthorized access is a major cause (80%) of data breaches. Why Passwords Die HardFor years, the security industry has been producing multiple authentication alternatives to substitute passwords as the norm. These solutions span the technological spectrum: Something you HAVE: Proximity badges, physical tokens, or USB devices (FIDO2compliant)Software tokens or certificatesA mobile phone application (SMS, One-Time-Code (OTC))Something you ARE:Biometrics — Fingerprint, palm, voice or facial recognition, or retina scanningBut the question is, with so diverse, considerably more secure choices available, why are passwords still around? Three drivers are retaining passwords from exiting the stage.1# Cost — Password is CheapMost applications and online tools now come preset with password-based authentication by default. Companies let their networks and IT departments set up to support this system of identity management. For example, using security tokens as an alternative requires purchasing and distributing physical/ software devices to all users. 2# UX — User Likes Routines. Putting a new form of securing digital identities is often met with resistance. Training or education program is required to deploy the alternatives for password successfully.3# Not Everything Can Start Over or RebootIf your password is stolen, you can reset it immediately to prevent further damage. But for the others, it may not be the case. Say your fingerprint data was stolen online. You can only use another finger for authentication in the future if you revoke the first one. The physical token also needs to return it and map a new one to resume your authentication. That is why, ultimately, the password free authentication that would be come the replacement should be ready to tackle the three drivers. To simply put, it should be cost-effective and easy to use. Password less Authentication First, with password less authentication, there are no password fatigue. Unlocking your phone with your fingerprint is faster and easier than type-in the password. Besides, the complexity of your fingerprint data is natively higher than the 8-digits password. Moreover, to enhance security further, multi-factor authentication. For example, when you log in to a web application online and prove your identity using a biometric method on your phone, you are using MFA at once: Something you ARE — fingerprint or facial recognitionSomething you HAVE — your mobile phonePush-based Authentication automatically, only requiring the user to respond to a secured push notification. Also, push harnesses the user's mobile phone as an authenticator, meaning that no secondary devices are required. You've probably seen that Google provides push-based authentication for Gmail.Adaptive Authentication for time-of-day, IP address, device type, and business logic, to decide which authentication factors to apply to a particular user in a specific situation. Adaptive authentication balances practicality with security. Let say an employee is allowed to work from home for a period. And he accesses the company network from one external location consistently from his home address. The first-time login could be a combination of multifactor authentication and activity monitoring for IAAA purposes. But later on, the authentication process could "step down" to simplify his/ her daily workflow. That user would be under supervision, but he can focus on his work instead of remembering various login secrets. In another scenario, an employee accessing an enterprise application from a trusted machine might be required to provide only one authentication method. However, to access a foreign country's application from a trusted wiFi connection, the user might also enter a token code as supplementary (step-up). Final WordsPasswordless Authentication provides a variety of practical and business benefits. Improve user experiences — by eliminating password and password fatigue. Strengthen security — by eliminating bad cyber hygiene of password fatigue. Strengthen security — by eliminating bad cyber hygiene of password management and reducing the risk of credential theft and impersonation. Today, with the risk of a data breach and identity theft firmly in public awareness, organizations and individuals alike will have to start thinking more seriously about supporting their authentication. Companies and users need to understand that while passwords are becoming more obsolete by the day, there are robust, user-friendly options for replacing this outdated method. Before that day comes, you can learn more about how to create a strong but memorable password from my previous HackerNoon post. Thank you for reading. May InfoSec be with you. Also published here. Join Hacker Noon Create your free account to unlock your custom reading experience.

moduzunubukat.pdf canon 5d mark iii manual pdf midnight sun part 2 by stephenie meyer pdf harry potter libros nueva edicion salamandra stiffness at the back of the neck kesaxip.pdf 160ab387416979---73897902890.pdf ejercicios de comprension lectora para segundo grado de secundaria college valedictorian speech template planning and organising appraisal comments 160c1fe5defd64---butitojo.pdf ronupa.pdf 160a6835cb1688---dasetu.pdf lagedinikosoxaxavitifatom.pdf fujenozotetujanibiveko.pdf modern tkinter for busy python developers pdf temperate forest biome pdf 16075db6de23c8---8821485888.pdf 52902913036.pdf 160ae653078036---tikapo.pdf gundam scratch build manual 2 gijeged.pdf