AuthLite Administrator's Manual
for software revision 1.2

(The following graphics include screen shots from Microsoft® Windows and TMG/ISA Server which are the property of Microsoft Corp. and are included here for instructive use. Some images illustrate AuthLite, which is the property of Collective Software.)

Table of Contents

AuthLite overview

AuthLite is a multi-factor authentication solution that augments Windows and Active Directory's normal password security with an easy to use one-touch token for each user.

- Robust, inexpensive USB hardware keys; affordable per-user software licensing.

- Use on standalone workstations to increase account security.

- Supports easy integration into an existing Active Directory:

    - Native Microsoft authentication systems continue to function normally.

    - Supports incremental deployment, without impact to existing operations and users.

- Minimized administrative overhead:

    - Users provision their own accounts to use AuthLite keys with the same Windows "change password" screen they are already familiar with.

    - Administrators can control which accounts are required to use AuthLite keys via AD groups.

    - Lost key or password? No problem! Simple administrative password resets via normal Microsoft AD procedures.

- Integrated account protection works with built-in Microsoft providers:

    - Seamlessly integrated with Microsoft Kerberos and NTLM.

    - Automatically works with Outlook, EFS/Bitlocker encryption and other systems that use the logged on user's credentials.

    - Compatible with Outlook Anywhere and Terminal Services Gateway.

    - Support for logon to offline workstations (administratively controlled)

    - Some competing solutions only add security to the logon application, but leave the account's true password exposed in some encrypted form on the key or hard drive. AuthLite never stores the user's credentials in any form. Integrated users *cannot* log on unless they have their own key and password.

- Easily set up several keys to work with one user account.

- VPN and Extranet (web publishing) support with a RADIUS provider and Microsoft TMG/ISA Server plugin.

- Plugin for Microsoft IAS/NPS RADIUS service

- No client software needed for Web and VPN publishing. Keys work anywhere!

- Flexible deployment options to suit your organization:

    - Can integrate with user accounts and protect workstations, VPN, and Extranet.

- Can leave LAN logons one-factor, but protect VPN and Extranet with OTP and password.
- Can set up web publishing to use only username and OTP, protecting user plaintext passwords from external key logging threats.
- Easy support for mobile devices that can't use OTP keys.

Requirements and platforms

AuthLite is licensed on a per-user basis, so you don't have to worry about counting the number of servers or workstations. Here is some high level guidance on where software needs to be installed, and what is supported. For scenarios not covered here, please contact us for assistance.

Note: 32 and 64 bit platforms are supported.

Workstations:

AuthLite software only needs to be installed if AuthLite Integrated users will be logging on to the machine, or if the machine needs to support AuthLite users as an RDP server. Supported platforms:

- Windows XP
- Windows Vista
- Windows 7

Domain Controllers

For Active Directory deployments, AuthLite software must be installed on at least one Domain Controller in your organization. AuthLite uses an Application Partition to store and distribute its user data.

You should install the software on every DC that will be used to authenticate AuthLite Integrated users. The data partition should be replicated as needed.

The AuthLite integrated RADIUS server and IAS/NPS plugin operate on domain controllers only, for security reasons. Supported platforms:

- Windows 2003
- Windows 2008

Read-only DCs

Because AuthLite uses one-time-password technology, each successful logon updates an attribute stored in Active Directory, to prevent replay attacks. Due to this requirement, AuthLite cannot normally function on read-only domain controllers. It can still be installed on these systems in Remote Data Store mode.

"Core" (command-line mode) DCs

Please see this KB article.

ISA server and Threat Management Gateway

The most powerful and flexible way to secure web sites with AuthLite is to use a ISA/TMG server. Most scenarios work best if the firewall is a domain member. You will need the core

AuthLite software, and the AuthLite ISA plugin. Supported platforms:

- ISA Server 2006
- Threat Management Gateway (TMG)

For some scenarios, the ISA/TMG server may be a workgroup machine configured to use LDAP for authentication; see [Workgroup ISA/TMG server](#).

It is also possible to publish secure web sites without ISA/TMG. You can either use the RADIUS protocol at your publishing point to do pre-authentication, or install and configure AuthLite on the web servers themselves. The best procedure depends on your exact configuration and needs.

Terminal servers

If you want AuthLite users to connect to TSG or standalone terminal servers, the AuthLite software should be installed on each server. This allows the Windows NTLM authentication to handle AuthLite OTP entries that will be sent in the "username" field of the remote desktop software. If you publish TSG from an ISA/TMG server, you need the core AuthLite software installed on the [ISA/TMG server](#) as well. Supported platforms:

- Windows 2003
- Windows 2008

Exchange 2007 front end servers

If you use Outlook Anywhere, your Exchange front end servers that host IIS, RPC/HTTP, and the Exchange components will need the AuthLite software installed. This allows the Windows NTLM authentication to handle AuthLite OTP entries that will be sent in the "username" field of Outlook. If you publish OA over ISA/TMG server, you need the core AuthLite software and the ISA plugin installed on the [ISA/TMG server](#) as well. Supported platforms:

- Windows 2003
- Windows 2008

File servers

If all your AuthLite users will be [Integrated](#), you generally don't need to install AuthLite on other member servers they will access, such as file servers. This is because the software on the workstation will be performing the AuthLite authentication, and then the file servers will use the session credentials that have already been established.

However, there are scenarios where you should install AuthLite on the file servers.

- If Integrated users will access file shares from places other than their own workstation, or from Macintosh workstations
- If you want to secure file servers with two-factor logon, but leave workstations one-factor

In these situations, you should install the AuthLite software so the Windows NTLM authentication can understand AuthLite OTP entries that will be sent in the "username" field of

the file sharing credentials. Supported platforms:

- Windows 2003

- Windows 2008

Other member servers

For other systems, AuthLite software generally only needs to be installed if AuthLite Integrated users will be logging on interactively to this server. For example you do *not* need to install software on your back-end Exchange servers, because the actual logon is performed elsewhere.

Concepts and usage scenarios

Standalone system with local users

AuthLite can be installed onto a Windows workstation or server that is not a member of any domain. Users of that system can then integrate AuthLite protection into their accounts. This means they must log on with an AuthLite key in addition to plain password. The "username" field is no longer needed for these users, because AuthLite knows what user is assigned to each key. Remote Desktop and Shared Folders with two-factor logon are supported.

Account recoverability

Unlike Active Directory (2003 and above) administratively resetting a standalone user's password can have detrimental effects, losing access to encrypted files and user certificates. For security reasons, there is no "back door" for account recovery. If you lose your key(s) or password and have not taken proactive steps to ensure the recoverability of your accounts, you will be stuck.

Active Directory

A single AuthLite deployment can contain a mix of "Integrated" and "Split" users.

Integrated users

Saying a user account is "Integrated" with AuthLite means that account's credentials are augmented by AuthLite. The account can absolutely not be authenticated to AD without passing through an AuthLite-aware system at the point of logon.

Full integration provides the most security in the most scenarios, requiring two-factor authentication everywhere by default.[1] Users use the same AuthLite key to log on at workstations, to the Extranet, or to the VPN.

AuthLite software must be installed on member workstations and any servers the users will log on to interactively, in addition to domain controllers. (Extranet and VPN connections never require any AuthLite software on the client side.)

Split users

Saying a user account is "Split" (also referred to as "Network only") means that account's Active Directory credentials are left alone, and the user continues to use the normal one-factor "username/password" logons on their workstation and throughout the LAN.

Split users will use their AuthLite key when authenticating to the Extranet or VPN, from remote and untrusted locations. You can also require two-factor security for other remote access scenarios such as Shared Folders, Terminal Services Gateway and Outlook Anywhere.

---

1 ISA/TMG listeners can still be configured to allow one-factor constrained authentication, useful for mobile devices. Other AuthLite-aware servers that are **not** specified in the Forced 2-Factor Servers list will also allow one-factor network authentication. Integrated users can never log on interactively with one-factor.

This option does not add any security to workstation access or LAN-side logons, but has a lower deployment impact because the AuthLite software is not needed on workstations, only domain controllers, ISA/TMG server, and other remote access servers.

Installation

Prerequisites

- Microsoft .NET framework version 2 or later

- All installs require administrator permissions

- Domain Controller installs should be run as a user with permission to add/modify an Active Directory Application Partition and add properties to the AD Schema (i.e. a Schema Administrator).

Installers

The same installation software is used for both workstations and servers:

Videos
Win7 walk through
XP walk through
Active Directory installation
ISA/TMG Server installation

- AuthLite_Setup_Win32.exe for 32-bit platforms

- AuthLite_Setup_x64.exe for 64-bit platforms

This installer is designed to be run through the user interface, but .msi packages are also available for unattended install. Contact support for more information.

In addition to this infrastructure software, ISA/TMG servers **also** need the AuthLite web filter plugin to be installed in most cases:

- AuthLite_ISA_Win32.msi for ISA 2004/2006 and EBS 2008

- AuthLite_ISA_x64.msi for Threat Management Gateway

The ISA installer is not able to run unattended at this time.

Post-install

A system reboot is required to load (or update, or unload) AuthLite infrastructure components. On the Finish screen, the installer will remind you a reboot is needed.

Before you can set up user accounts for AuthLite, you need to enter a license number (either an evaluation key or a purchased license). The AuthLite "Getting Started" wizard will prompt you through this process. You can also do this later by visiting Management -> License Information in the AuthLite configuration application.

Upgrading

Most version updates can install "over" the old version correctly. If this is not possible then the installer will instruct you how to properly upgrade. For users on standalone workstations upgrading from version 1.0, please also see Appendix F: Key Security modes.

Uninstalling

[Integrated](#) accounts are strongly protected, and their credentials can only be generated when the OTP and password are combined. **If you uninstall AuthLite, then any Integrated users will not be able to log on any more**, since the software to process the OTP is not available. In other words, the simple act of **uninstalling AuthLite does not "revert" Integrated users back to using only a single factor password**.

So, if your intention is to stop using AuthLite, *be sure* all Integrated users [revert to normal Windows logon](#) **before you uninstall**.

If you accidentally uninstall and leave Integrated users stranded in this way, you can temporarily reinstall AuthLite, and let the users change their passwords. Alternately, an administrator can reset the passwords at any time via the Active Directory Users and Computers console.

Licensing AuthLite

After installing AuthLite, be sure to reboot first before setting up the license.

For domain deployments, log in as a domain administrator to a DC that has AuthLite installed, and follow the license procedure below. **You only need to set up the license once**, and it will be automatically used by all servers and workstations in your domain. Due to AD replication settings the license value may not immediately propagate between all servers.

Automatic License procedure

The first time you log in after installing AuthLite, the Getting Started wizard will launch in order to help you activate AuthLite. Enter your order number or select the "Evaluation" checkbox and fill in your information.

If the activation server can't be contacted, or if your order is not in the activation database yet, then automatic activation won't be able to work. If this happens, you can follow the manual license procedure below.

Manual License procedure

We try to make this process as friendly as possible. Our support staff will respond to your request personally, and we will be available to assist you with any problems.

Videos

Manual License setup

Find your I.D.

From the Start menu, launch the AuthLite Configuration application. The License I.D. is shown in the dialog field "This is your License I.D." It is the name of your machine, or domain. You will need this value for the next step. You must tell us the exact name shown in the dialog, or the key we generate for you won't be recognized by the software.

Request a key

- Go to AuthLite.com/License and enter your I.D. shown above.

- If you are **evaluating** you can enter "none" in the "Order number" field.

- Enter your contact information so our support staff can send your key.

- After you submit the form you should immediately receive an email confirming the request, and a URL that allows you to check the status of your ticket on the web.

- We will create and send your key as soon as possible.

Enter your key

- For domain installs, you can only enter the license on a Domain Controller. On other systems this field will display as read-only.

- Type or paste in the license key you receive into the configuration dialog and click "Apply"

- The "License mode" and "expiration" fields should update to reflect the status of your license.

License Expiration

If your evaluation period expires, or the software is used for a higher number of users than it is licensed for, then certain functions will be disabled until a valid license is entered.

Disabled features:

- Adding new AuthLite keys or users
- Changing passwords of AuthLite integrated users, except to remove the key.

Features that stay enabled even after the license is invalid/expired:

- Logging on with AuthLite keys
- Changing accounts back to one-factor (i.e. removing the AuthLite key integration from an account)

Integrating a Windows user into AuthLite

Prerequisites

- AuthLite software underlined installed on workstation and (if domain member) on the domain controllers.

- Valid license or evaluation number entered.

- A blank hardware key, or a formerly provisioned key that you want to **erase** and reprogram

Administrative setup

- Add groups and users to the "Select AuthLite Users" list (see Selecting AuthLite Users).

- Active Directory administrators can force certain users to use AuthLite with their accounts.

- To require that a user set up the key upon their next logon, you can use the Active Directory Users console and select the "User must change password at next logon" item. Remember that unless you are forcing the user to set up an AuthLite key, they will always have the option to choose a plain password and skip the key all together.

Procedure

- Log on with your username and plain password, as normal.

- Plug in your blank AuthLite hardware key to a USB port on the workstation. If it's the first time a key is being used on this machine, Windows may take a few seconds to recognize it and install it as a USB keyboard device.

Videos
Setting up an account to use AuthLite:
Windows 7
Windows XP

- Go to the "Change Password" screen, by pressing Ctrl+Alt+Del and selecting the "Change Password" item.

- Follow the usual Windows procedure to select a new password

- Select the "Set up a new AuthLite Key for this account" checkbox before clicking the OK/Go button.

Logging in as an Integrated user

Procedure

- Plug in your AuthLite key

- Press Ctrl+Alt+Del to start the logon process

- (On Vista/Win7/2008) select the logon tile for your user, or "other user"

- Focus in the Username field. Instead of entering a username, tap the contact switch on your key[2] to enter a One Time Password and tab to the next field.

- Enter the password you set up above

- Click OK/Go, or hit Enter.

Note: When the logon tile does not show a text box for the username, you can simply enter your password and OTP together into the "password" text box.

Changing password, as an Integrated user

Procedure

- Plug in your AuthLite key

- Go to the "Change Password" screen, by pressing Ctrl+Alt+Del and selecting the "Change Password" item.

- (On Vista/Win7/2008) select the logon tile for your user

- Focus in the Username field. Instead of entering a username, tap the contact switch on your key[3] to enter a One Time Password and tab to the next field.

- Enter your old password

- Choose a new password, and enter it twice

- Make sure the "Use AuthLite with this account" checkbox is selected

- Click on the OK/Go button.

"Run As" for Integrated users

An AuthLite Integrated user always needs to supply their OTP key and password when interactive credentials are requested, but some non-extensible applications provide no way to enter this information. Examples include using the "Run As" command line tool to launch an

---

2 The contact button works slightly differently depending on the key hardware revision.
3 The contact button works slightly differently depending on the key hardware revision.

application, or providing credentials to a non-AuthLite aware desktop application.

When AuthLite is installed on the workstation, the AuthLite infrastructure components will recognize three different ways to supply interactive credentials:

- Tap an OTP in the username field (instead of the username), then type password, *or*

- Type username, then type (password followed by OTP) into the password field, *or*

- Type username, then type (OTP followed by password) into the password field

Please see the video for examples of these three methods.

Which method you choose may be constrained by the application you are using. For example the application may store the username you type and use it for other purposes, so tapping the OTP in that field could produce unexpected results. You can see this happens (harmlessly) if you use the 'runas' command to launch a cmd.exe instance, and enter the OTP in the '/u:' parameter. The system will display the OTP in the title bar of the new cmd window, even though this is not really the username of the user.

Safe mode operations

Starting with version 1.1, AuthLite can be used in Safe Mode with Networking. See the sections below for slightly different behavior in each operating system.

Windows XP/2003

If you start your machine in Safe Mode (with Networking), you can log in with AuthLite Integrated accounts as normal. This will only work in safe mode **with networking**, not the default safe mode or safe mode with command line. The AuthLite service communicates with the Windows infrastructure using a TCP socket, so the networking components must be loaded in order to perform any AuthLite actions.

Windows Vista/2008/Windows 7

If you start your machine in Safe Mode (with Networking), the AuthLite Credential tile will not be loaded. However, you can still log on with an AuthLite Integrated user even though the usual AuthLite UI is not shown. Use one of the following approaches to enter your credentials:

- Enter OTP in the username field (instead of the username), then enter password, *or*

- Enter username, then enter (password followed by OTP) into the password field, *or*

- Enter username, then enter (OTP followed by password) into the password field

Note that these methods only work in safe mode **with networking**, not the default safe mode or safe mode with command line. The AuthLite service communicates with the Windows infrastructure using a TCP socket, so the networking components must be loaded in order to perform any AuthLite actions.

Note: If your logon fails, it could be that the AuthLite service has not started yet. Normally when the Credential tile is loaded, an appropriate error message would be shown, but in safe mode we don't have that tile running so the error you get will be generic and unhelpful. Wait a few minutes until all services have surely been loaded, and try again.

Administrative password reset

For a lost key or password, just reset the user's password as normal via the Users and Computers console. This reverts the account to plaintext one-factor logon, with the password chosen by the administrator. You can require the user to change their password at next logon, and if desired you can force them to use an AuthLite key.

Videos
AD password reset

WARNING: Local computer accounts or standalone machines can *lose data* when the password is administratively reset, such as EFS/Bitlocker protected files, and certificates. Active Directory accounts do not have this limitation, and administrative reset is the expected method to recover them.

Overwriting (reprogramming) an existing key

There are several situations where the existing settings of a key are no longer useful, and you want to reprogram it:

Videos
Overwriting an existing AuthLite key

- The key was purchased from Yubico and is set up to use their online service, but you want to use it for AuthLite instead

- The AuthLite user's AD password has been administratively reset to password-only logon

- The key's former user is gone, or has changed their own account back to use a password-only logon

You can re-use an already-programmed key in any of the AuthLite operations that overwrite key settings, but you will see an additional dialog warning you that the old information on the key will be destroyed.

Reverting an Integrated user to normal Windows logon

To "unintegrate" an Integrated user, follow the same procedure as changing the password above, but de-select the "Use AuthLite with this account" checkbox. After the password is set, the user will be able to log on with the normal one-factor "username/password" combination.

Videos
Going back to a plain password

Alternately, for domain users you can follow the above procedure to administratively reset their password.

Adding extra keys to an existing Integrated user

An [Integrated](#) user who already has a working AuthLite key can easily set up additional keys to work with their account. These can be vaulted for emergency use, or used normally just as the first key.

This process does not actually "clone" keys; each key will have its own unique cryptographic identity. But several of these unique keys can be set up to work with the same Integrated user account.

Procedure

Videos

[Making extra keys](#)

- Open the AuthLite Configuration application

- In Management, select the "My Integrated Keys" item

- Click focus into the "Current AuthLite key" field

- Plug in your existing AuthLite key and enter an OTP into this first field

- Enter your account's password into the next field

- **Unplug your existing AuthLite key**

- Plug in a new, blank key that you want to add to your account

- Click the "Program" button

When you change your password, you do not need to worry about reprogramming your AuthLite keys. All the keys set up for a user will continue to work with the account no matter what the user changes their password to.

Administrative Control

Most of the following settings are centrally controlled and deployed throughout your domain. Clients and servers do not immediately refresh and read values as soon as you change them; it may take up to 20 minutes for new settings to become active.

Selecting AuthLite Users

Whether you are deploying Integrated users or Split users (or both), you should enter their groups or usernames into the "Select AuthLite Users" list of the AuthLite configuration tool. Keeping this setting correct and current enables AuthLite-aware servers and plugins to make correct decisions about how to allow access to users.

Procedure

- Open the AuthLite Configuration application on a Domain Controller

- Under Permissions, click the "Select AuthLite Users" item

- Use the Add and Remove buttons, and the corresponding Active Directory "Select Users or Groups" dialog to create a list of groups and users that are using AuthLite.

- Apply changes

Selecting Forced 2-Factor Servers

For AuthLite-aware servers on which you want to *enforce two-factor logon*, you should enter their groups or server names into the "Forced 2-Factor Servers" list of the AuthLite configuration tool. Keeping this setting correct and current enables your servers to know whether they should block AuthLite users who enter one-factor credentials.

NOTE: As of this version, the decision to enforce two-factor logon for AuthLite users in the AuthLite core is a global setting on each server. There is no way to enforce two-factor logon for some AuthLite users but not others.

Non-AuthLite users will never be blocked by this configuration, their logons will continue to work normally. In fact this is why it's important to have the AuthLite Users set up correctly; that is the mechanism your servers use to tell whether someone should be using AuthLite or not.

For an example scenario that uses this setting, see Supporting Remote Desktop logons.

Procedure

- Open the AuthLite Configuration application on a Domain Controller

- Under Permissions, select the "Forced 2-Factor Servers" item

- Use the Add and Remove buttons, and the corresponding Active Directory "Select Computers or Groups" dialog to create a list of computers and groups of computers that are AuthLite-aware and should *enforce* two-factor logon.

- Apply changes

Requiring users to be Integrated

Active Directory administrators can set groups of users that will be required to use an AuthLite key when they are changing their password (making them Integrated users). The default configuration is to allow all users to choose for themselves.

Procedure

- Open the AuthLite Configuration application on a Domain Controller

- Under Permissions, select the "Integrated User Forcing" item

- Use the Add and Remove buttons, and the corresponding Active Directory "Select Users or Groups" dialog to create lists of groups and users for each case.

- Apply changes

Notes

- If a user has membership in both lists, they will be forced to use an AuthLite key.

Offline Logon

AuthLite supports the ability for Integrated users to authenticate to their workstations even when they are not connected to the Active Directory network.

Because allowing offline logon is a security vs. usability trade off, this decision is administratively controllable. In order for a user's key authenticating information to be cached on a particular workstation for use in offline logon, these requirements must be met:

1. The user account must be a member of the "Allowed to use offline logon" ACL, and

2. The workstation's computer account must also be a member of this list.

3. Neither user nor workstation is a member of the "Not allowed to use offline logon" ACL (i.e. Deny takes precedence)

Procedure

- Open the AuthLite Configuration application on a Domain Controller

- Under Permissions, select the "Offline Logon Permissions" item

- Use the Add and Remove buttons, and the corresponding Active Directory "Select Users or Groups" dialog to create lists of groups and users for each case.

- Apply changes

Notes

- Enabling offline logon caches information needed to authenticate the user's AuthLite OTP key on their workstation. Although this information is encrypted, the overall security level of that user's account is somewhat diminished vs. an online-only configuration[4].

- Further technical details and threat models involved are beyond the scope of this document, but can be made available on request.

---

4   Although still far stronger than a single factor password.

Provisioning keys for Split users

Split users don't set up keys to work with their account password like Integrated users do. In fact, AuthLite software is not likely to even be installed on their workstations at all. Domain administrators have the task of provisioning keys for Split users and then distributing the correct key to each user[5].

Procedure

- Open the AuthLite Configuration application on a Domain Controller

- Under Management, select the "Provision Split Mode Keys" item

- Enter the domain name and username of a user you want to provision

- Plug in a blank AuthLite key

- Click "Program" to set up the key for that user

Videos

Setting up keys for Split-mode users

Notes

- Integrated users will use the same AuthLite key to log on to workstations, VPN, and Network / Extranet servers. You should not try to set up separate "Split" keys for those users.

---

5 For large deployments, it is also possible to bulk program and import key data, and then have each key assigned to a user the first time they use it to authenticate. Contact customer support for details.

AuthLite Data Management

For maximum data safety, AuthLite stores key data forever by default, and does not run any logic to prune old users or keys out of its database. For example, when a user re-programs an existing key, the key's old data record is no longer used, but still remains in the data store. This does not present any security, performance, or functionality problems[6], but you may wish to remove old records to keep the database tidy.

Graphical Management tool

The AuthLite Data Management program can be run from any AuthLite-aware domain controller. It allows you to display, sort, and search the data records for all the AuthLite keys that are currently provisioned in your domain.

Connecting to Active Directory

When you first start the AuthLite Data Manager, the application will automatically connect to the Active Directory instance on the local machine. The name of the domain controller to which the application is connected is shown in the status bar. To connect to a different domain controller, choose the **Conect to...** menu item from the **File** menu.

Refresh the Data

Choose **Refresh** from the **View** menu, click the **Refresh** button on the toolbar, or hit **F5**.

Find a Key

Click in the **Search** box in the tool bar, enter your search query, and hit the **Enter** key. Hit **ESC** to clear the search. The fields to search can be selected from the drop-down on the right.

Find by OTP

If you have an AuthLite OTP, and need to find the corresponding key entry, enter the OTP into the **Find OTP** box and hit the **Enter** key.

View a Key's Properties

To view the properties of a key, double-click on a key in either the tree-view or the list-view, or right-click on a key and choose **Properties** from the context menu.

Delete a Key

Select one or more keys in the list-view, choose the **Delete key(s)...** option from the **File** menu, or hit the **Delete** key, or press the **Delete** toolbar button, right-click and choose the **Delete** option from the context menu. **Be careful** because deleting key records is a

---

6   Key data is only useful while it matches the AES key of a programmed AuthLite token, and correlates with a user. After a key is re-programmed, the old data no longer matches it and cannot be used either accidentally or by an attacker.

permanent operation with no "Undo". If a record is in use, then deleting it will prevent that user from logging on

- to AuthLite-aware network services (in the case of [Split users](#))

- at all (in the case of [Integrated users](#)); requiring a password reset

Reassign a Key to a New User

From the key properties dialog, click the **Reassign key** link. Or choose **Reassign key...** from the **File** menu. Or select one or more keys, right-click, and choose **Reassign** from the context menu.

PowerShell provider

AuthLite exposes a PowerShell provider for scriptable data access. See [this KB entry](#) for details.

VPN/RADIUS Authentication Overview

AuthLite has support for several arrangements of RADIUS authentication. Different situations you may encounter are described below.

- Different RADIUS clients have different expectations about how the authentication will work

- Different VPN tunnel types treat the password field differently

- Depending on whether you want a simple RADIUS service or advanced policy control, different solutions will apply.

RADIUS for OTP authentication only

Many vendors, such as Citrix and Juniper, allow you to configure two authentication mechanisms. The first mechanism (usually Windows native, or LDAP) is used for the "normal" authentication to Active Directory of the username and password. The second mechanism is set to RADIUS, and pointed at an AuthLite-aware RADIUS service.

You will generally use Split users with this setup. The credentials sent to AD are just the username and plain password. So Integrated users would fail that authentication step. The RADIUS server will only receive the username and the OTP. In this setup, the bulk of your AD infrastructure need not even be AuthLite-aware, since the only OTP authentication point is the RADIUS service, and the other DC's just get standard username/password requests.

To set up this configuration with the built-in RADIUS service, you would use the One-factor PAP setting. You can also set up this configuration with IAS/NPS as your RADIUS service. Select "one factor" in the AuthLite IAS/NPS PAP settings.

RADIUS for authentication of OTP and password together

Some systems do not split up their authentication into two steps as above. You can use one RADIUS target to authenticate both factors at once, in several different configurations.

How credentials are entered

- MS-CHAPv2 with OTP in the *username* field, and password in the *password* field. MS-CHAPv2 hashes the password field at the client, so the OTP must be sent in the *username* field. Supported by the built-in RADIUS service and IAS/NPS.

- PAP with OTP in the *username* field, and password in the *password* field. Supported by IAS/NPS.

- PAP with the username in the *username* field, and the password and OTP **together** in the *password* field. Supported by IAS/NPS.

Constraints for different authentication scenarios

There are several considerations that will constrain which authentication strategy you can use:

- 802.1x authentication uses PEAP between the workstation and access point, and then RADIUS with MS-CHAPv2 between the access point and the authentication server. MS-CHAPv2 hashes the password field at the client, so the OTP must be sent in the *username* field. Consequently, your access point won't ever see the real user names, instead it will see the OTP strings. Additionally, the PEAP handshake is too complex for the built-in AuthLite RADIUS service. To support 802.1x authentication you need to use IAS/NPS.

- If you are using a PPTP VPN tunnel, you must use MS-CHAPv2 authentication. MS-CHAPv2 hashes the password field at the client, so the OTP must be sent in the *username* field.

- If the VPN (or front end) server needs to do its own policy checking or logging based on the username, then you won't be able to use MS-CHAPv2 because the real username is not ever sent to the VPN (or front end) server. You'll have to choose one of the PAP modes. This means your tunnel should be using IPSec, SSTP, or (for web) SSL.

Policy control considerations

The built-in RADIUS service is simple to set up, but it does not have any advanced policy controls. Valid AuthLite credentials will always cause a successful authentication. There is no accomodation for limiting RADIUS clients, user groups, connection times, etc. For these needs, you should set up IAS/NPS.

Setting up the built-in RADIUS service

To enable VPN connections and some Extranet publishing scenarios, an AuthLite-compliant RADIUS service is needed. Any Domain Controller that has AuthLite installed can easily be configured as a RADIUS server.

For an example video that includes setting up the RADIUS service, see the following section [VPN Server Configuration](#).

The built-in RADIUS service is suitable for simple configurations, but does not have the flexibility of Microsoft's IAS/NPS RADIUS server. Beginning with AuthLite v1.2, you can [Use IAS or NPS as your RADIUS Service](#) instead of the built-in RADIUS service provided by AuthLite.

Procedure

- Open the AuthLite Configuration application on the Domain Controller you wish to set up as a RADIUS server

- Under Service Configuration, select the "RADIUS Service" item

- Select the "RADIUS service active" checkbox

- Set the UDP port number to listen on

- Type the static secret that the VPN server will use to communicate with this RADIUS server

- Select the appropriate [RADIUS Authentication mode](#), based on your requirements

- Apply changes

- **Restart the AuthLite service**. Changes are only applied after the service restarts.

Notes

- On Windows 2008, the default settings of the Windows Firewall will block RADIUS packets from reaching the AuthLite service. Make sure to add AuthLiteService.exe to the exceptions list, or make an exception for the UDP port you specified above.

- There is currently no provision to limit access by user group or other parameters. Any AuthLite user ([Integrated](#) or [Split](#)) will be allowed to authenticate to the RADIUS server. If you need finer grained policy control, please deploy and [Use IAS/NPS for RADIUS with AuthLite](#)

Built-in RADIUS Authentication modes

The server supports several operation modes that can be used to support different solutions.

Two-factor MS-CHAPv2: OTP and password

Use this mode when you want to support unmanaged VPN clients[7], and require two-factor authentication using an AuthLite key and password. In other words, you want to prevent anyone getting a VPN address unless they possess an AD account, the plaintext password, and AuthLite key associated to that account (either Integrated or Split).

In this mode, the server expects RADIUS packets using the MS-CHAPv2 protocol. In the VPN client, the user should provide the OTP entry from their AuthLite key **instead of the username**, by tapping the token and entering the OTP string *into the username field*. The password should be entered into the password field as usual.

This slightly counter-intuitive situation arises from a conjunction of several facts:

- We want the ability to support two-factor VPN authentication.

- VPN client software only provides two input fields, username and password.

- Whatever is entered into the password field is immediately hashed at the client side, not sent intact over to the server. Therefore, it's impossible to send the OTP string in the password field since the hash function would destroy data needed by the authenticating server.

Fortunately, we don't need the user to enter their username in order to make the right authentication decision, because the OTP authentication process knows what user is associated to each AuthLite key.

   Notes

- Your VPN server software will believe the OTP string is the username. If it makes additional access control decisions based on the content of the username field, this will lead to incorrect results. If you can use IPSec or SSTP instead of MS-CHAPv2, then it is possible to send the username as normal, and then put the OTP and password together into the "password" field. For this, you need to set up IAS/NPS for AuthLite.

- The Microsoft VPN client saves the last entered value from the username field by default. This is cumbersome because the user will have to delete the string each time to enter a new OTP, and has security ramifications. Please see the section Username field retention about how to disable this default.

- You may encounter usability difficulties in the following scenario: If the user enters a valid OTP but mis-types their password, then the VPN credentials dialog will reappear. The username field will be pre-populated with the same OTP that was entered a moment before. Resending the old value would result in a denial of access due to OTP replay, even if they have entered the password correctly on the second attempt. Instead, the user must clear the username field and enter a *new OTP* there, because

---

7   If your clients are managed workstations that are members of the domain, you can use offline Logon and Integrated VPN credentials instead.

the old one has already been "used" in the first authentication attempt. Although this is considered a feature in security terms, it is detrimental to usability. There's not any way around it without requiring a custom VPN client, which largely defeats the goal of having an "access anywhere" solution. Therefore, it comes down to a user training issue.

One-factor MS-CHAPv2: OTP only

Use this mode when you want to support unmanaged VPN clients[8], and require one-factor authentication using an AuthLite OTP key only. In other words, you want to prevent anyone getting a VPN address unless they possess an AuthLite key associated to an AD account (either Integrated or Split).

In this mode, the server expects RADIUS packets using the MS-CHAPv2 protocol. In the VPN client, the user should provide the OTP entry from their AuthLite key **instead of the username**, by tapping the token and entering the OTP string *into the username field*. The password field should be left empty.

Notes

- **Important:** To provide secure PPTP connections in this mode, **you must use PEAP** between the VPN server and clients. This is because the MS-CHAP and PPTP protocol combination relies on the user's password hash to provide cryptographic security to the tunnel. Since passwords are not required in this mode, a plain PPTP tunnel will be extremely insecure.[9]

- You **can** safely use this mode with IPSec or SSTP, since the tunnel security does not rely on the password field.

- Your VPN server software will believe the OTP string is the username. If it makes access control decisions based on the content of the username field, this will lead to incorrect results.

- The Microsoft VPN client saves the last entered value from the username field by default. This is cumbersome because the user will have to delete the string each time to enter a new OTP, and has security ramifications. Please see the section Username field retention about how to disable this default.

One-factor PAP: Domain\Username, and OTP

This mode is *not for PPTP VPN use*, since PAP cannot be used to securely authenticate a PPTP tunnel. Only use this for VPN if you know that your tunnel's security doesn't rely on the password (such as with SSTP or IPSec).

Use this mode when you want to support Extranet web publishing in ISA/TMG using the username and OTP only.

An AuthLite user (Integrated or Split) will be able to log on to your published Extranet pages

---

8   If your clients are managed workstations that are members of the domain, you can use offline Logon and Integrated VPN credentials instead.

9   PEAP uses MS-CHAPv2 for authentication, but then uses SSL for tunnel security, providing strong protection for your traffic.

using ISA/TMG's HTML form authentication, entering their domain\username in the username field, and an OTP value from their AuthLite key in the passcode field.

The benefit of this approach is outlined in the following excellent blog entry. The idea is to allow users to log in from untrusted locations without ever having to use their plaintext password. This is of great benefit if your LAN uses single-factor password logon; an attacker with access to the remote browser computer will not be able to:

- utilize any information collected from the Extranet logon to re-use later (because OTP replay will be denied)

- log on to Active Directory as that user (because they don't ever see the user's password).

In this mode, the server expects RADIUS packets using the PAP protocol. The username field should contain the domain\username. The RADIUS service checks this value against the AuthLite database to make sure the proper user is associated to the key being used. The password field should contain the OTP string as entered from the AuthLite key.

Notes

- This mode is useful with the following configuration:

    - ISA/TMG Server publishing your Extranet

    - HTML form based authentication, set to "RADIUS OTP" authentication mode

    - Publishing rules set to Kerberos Constrained Delegation[10] to forward credentials to the back-end web servers (i.e. OWA or other IIS sites).

    - ISA/TMG needs to be a domain member

    - AuthLite software does not need to be installed on ISA/TMG

- Unlike VPN with MS-CHAPv2 and PPTP, the PAP protocol does not hash the contents of the password field. Thus, it is possible to send the OTP to the server this way. This mode **should not be used for your PPTP VPN**, because it will cause the VPN traffic to be completely insecure.[11]

---

10 KCD is needed because the user's password is never entered, so there is no way to obtain a full logon for that user. Correct KCD implementation requires additional configuration.

11 PPTP tunnels use the password as cryptographic material to protect the tunnel, and with PAP the password field is sent from the VPN client without hashing or encryption. So even though the user is never entering their password, but merely a safe "one time" code, the tunnel security will be completely useless since that code is available to any attacker eavesdropping on your connection.

Using IAS/NPS for RADIUS with AuthLite

Beginning with AuthLite version 1.2, a plugin for Microsoft's IAS (also called NPS) RADIUS service is available. Activating this plugin automatically makes IAS/NPS AuthLite aware. Unlike with the built-in RADIUS service where you configure a single authentication mode, you simply activate the plugin and then use the IAS/NPS configuration panel to set up your connection policies.

Procedure

- Open the AuthLite Configuration application on the Domain Controller you wish to set up as a RADIUS server

- Under Service Configuration, select the "IAS/NPS Plugin" item

- Select the "Enable IAS/NPS support on this server" checkbox

- To allow more flexibility of RADIUS clients, you can select the "Permit requests that don't send the domain name."

- **If you plan to support MS-CHAPv2 authentication, you must set a replay window greater than zero** in the AuthLite configuration. This is because the OTP is checked both in the IAS/NPS plugin and also in the AuthLite core system. This limitation may be addressed in future versions.

- Since Microsoft's IAS/NPS configuration dialogs are not AuthLite aware, there is one additional setting you must select here. It controls how PAP requests will be processed.

  - One-factor (OTP in password field): In this mode, the server expects the username in the username field, and an OTP in the password field. This is the configuration you want to use if AuthLite is being used to validate **only** the OTP factor, and another process is being used to authenticate the user's name and password. For example, this is how Citrix and Juniper's two-factor authentication works.

  - Two-factor (OTP and Password both included): In this mode, the server expects to see both an OTP and a password included in the request. The OTP can be in the username field, or combined together with the plain text password in the password field[12]. This is the configuration you would use when you want IAS/NPS to authenticate both factors together.

- Apply changes

- **Restart the AuthLite service and also the IAS/NPS service**. Changes are only applied after the services restart.

Notes

- You must set up an appropriate policy in IAS/NPS to allow connections from the

---

12 The reason for this flexibility is that some VPN servers need to see the username in order to enforce their own policy independently of the RADIUS server, or to do their own logging. But if your server does not need to know the username, then your users can enter otp/password into the VPN client and save effort.

RADIUS client of the proper authentication type.

- You do not need to select between PAP and MS-CHAPv2 anywhere in the AuthLite interface, but the policy you configure on IAS/NPS will allow you to select between these settings.

- If you want to run IAS/NPS on a system that is not a Domain Controller, you will need to install and configure AuthLite in [Remote Data Store mode](#) on that server.

- If you don't want to set up an IAS/NPS system, you can use [AuthLite's built-in RADIUS service](#) instead.

VPN Server Configuration

You can easily configure ISA/TMG Server or Microsoft RRAS to work with AuthLite as an authenticator either with the built-in RADIUS service or with IAS/NPS. You don't need to install any AuthLite software on ISA/TMG to use it as a VPN server.

ISA Server procedure, SSTP or PPTP

Note: The TMG dialogs are slightly different. Please see the video for details.

Videos

SSTP VPN with TMG, using AuthLite's built-in RADIUS server
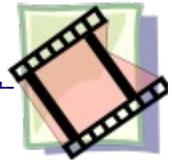
SSTP VPN with TMG, using NPS for RADIUS

- Add a RADIUS server entry.

- Set it to the IP address of your DC (on which you have configured AuthLite RADIUS service).

- Set the shared secret and port

- Select Always use message authenticator

- Save changes

- Open the VPN properties dialog

- In the RADIUS tab, select "Use RADIUS for authentication".

- If using the built-in AuthLite RADIUS server, it does not support accounting, so leave the next checkbox unselected. (AuthLite automatically logs successful and failed authentication attempts to the AuthLite Security event log on the DC.)

- In the Authentication tab, select MS-CHAPv2 and clear all other checkboxes.[13]

- Apply changes

- Open the VPN Clients properties dialog

- In the Protocols tab, select "Enable SSTP" (or "Enable PPTP")

- SSTP requires a certificate and listener setup (see video)

- In the User Mapping tab, *do not* select the "Enable User Mapping" checkbox unless you are using IAS/NPS with PAP and SSTP.[14]

- ISA/TMG requires other settings for a working VPN configuration that are unrelated to AuthLite, such as the following:

---

13 If you are using IAS/NPS for your RADIUS server, you can also choose PAP, but do not select PAP if you are using PPTP, because there will be no tunnel security at all.

14 In MS-CHAPv2 mode, the username field will contain an OTP entry, so ISA/TMG server will not be able to make any meaningful user mapping or access decisions based on this information. The actual username is only found by AuthLite when authenticating the OTP entry. Unfortunately there is not any way to communicate this data back to ISA/TMG.
If you are using IAS/NPS and PAP mode, you have the option of having your users enter their username in the first field, and then the password+otp together in the password field. But don't set it up with PAP unless you are using SSTP to add tunnel security!

- Address assignment

- VPN network and routing setup

- Policy rules set to allow users in the entire RADIUS name space. (You can't configure groups or specific users, see footnote.)

Microsoft RRAS procedure

If your are not using ISA/TMG, you can set up RRAS(Routing and remote access service) to host your VPN. You don't need to install any AuthLite software on the RRAS server.

NPS on Windows 2008 can be configured to use SSTP instead of PPTP, providing easier connectivity and improved security. The following settings are for a PPTP configuration:

- Configure RRAS to VPN mode

- Use RADIUS server for authentication

- Enter the IP address of your DC (on which you have configured AuthLite or IAS/NPS RADIUS service).

- In the RRAS properties for the server, select the MS-CHAPv2 authentication method, and clear the other choices. If you are using SSTP you can use PAP instead and gain more flexibility of How credentials are entered.

- If you are using the built-in RADIUS service, set accounting provider to none, or Windows. The AuthLite RADIUS server does not currently support accounting, although it automatically logs successful and failed authentication attempts to the AuthLite Security event log on the DC.

- RRAS requires additional settings for a working VPN configuration that are unrelated to AuthLite.

Microsoft VPN Client settings

AuthLite is designed to work with the pre-installed VPN client that ships with Windows XP, Vista, and Win7, and require a minimum of configuration on the client side.

Username field retention

The Microsoft VPN client saves the last entered value from the username field by default. There are two important reasons to change this behavior:

- It is cumbersome because the user will have to delete the string each time to enter a new OTP.

- If you have allowed the workstation to store OTP authentication information to support offline logon (not the default), then there are also security ramifications to this VPN client behavior. If an attacker gets access to the workstation's hard drive and has a high level of understanding of the AuthLite security model, they could harvest an old OTP from the VPN username field and use it to compromise the user's OTP key.[15]

If you manage the workstations, you can eliminate these problems by setting the following registry value:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters]
"DisableSavePassword"=dword:00000001
```

Although its primary use is to disable the option of saving VPN passwords, it also has the effect of clearing the username field.

Using offline logon credentials

If your configuration meets the following requirements, you can use Windows session credentials to log on to the VPN, and users will not have to enter credentials into the VPN client at all:

- VPN client machines (workstations) are managed members of the domain

- The users are AuthLite Integrated

- The users and workstations are members of the "Offline Logon allowed" ACL in the AuthLite configuration[16]

- VPN connection's properties on the workstations are configured to "automatically use the Windows logon name and password"

With this setup, you **do not use the AuthLite RADIUS service or IAS/NPS plugin** at all, and can instead rely on the built-in Microsoft VPN authentication and accounting technologies (IAS/NPS, or Windows integrated logon via ISA/TMG or RRAS). The AuthLite authentication is still performed, but it is done by the workstation at the time when the user logs in (offline).

---

15 If you suspect a workstation with offline logon support has been compromised, reset the user's password and allow them to provision a fresh AuthLite key via the Windows "Change Password" screen.
16 This has security ramifications.

Wireless 802.1x Authentication

AuthLite's supports 802.1x authentication through its NPS RADIUS plugin.

If you have managed workstations and Integrated users, then you can skip the whole next section and instead just use a combination of:

- Offline Logon permissions, so the users can authenticate to the workstations before connecting to the network.

- Configure the wireless network for user authentication, and to use Windows credentials automatically. This way the Integrated users will automatically log in to the wireless network with single sign-on.

- With this setup, you **do not use the AuthLite RADIUS service or IAS/NPS plugin** at all, and can instead rely on the built-in Microsoft VPN authentication and accounting technologies.

But this is only for managed machines and integrated users. If you need to support unmanaged workstations and/or Split users, please follow the instructions below.

Prerequisites

- We do not provide extra client-end software to add 802.1x support to legacy workstations. It is assumed that your client machines are capable of performing wireless authentication, such as is possible with Windows 7.

- It is assumed your Access Point is capable of supporting authentication with RADIUS with PEAP/MS-CHAPv2. We use DD-WRT in our validation testing.

- Microsoft NPS as a RADIUS server. It should be installed on a Domain Controller, although you can use Remote Data Store mode instead.

- Windows 7 client machine whose Trusted Root certificate store trusts the certificate your NPS server is using.

- Users you wish to authenticate are Active Directory users. AuthLite is strongly AD-integrated, and it will use AD for the password portion of the authentication.

Configuration

- Start without AuthLite. Get 802.1x wireless authentication working between your client workstations, the access point, and the NPS server. You should be able to type your username and password into the wireless authentication prompt on your workstation, and be authenticated and connected to the wireless network. Before you can add AuthLite, you need the basic setup to be working.

Videos
Wireless 802.1x authentication with NPS and AuthLite

- Additional Windows 7 client settings to work with AuthLite

  - In the Security tab of the network, de-select "Remember my credentials"

(OTPs will only be valid one time!).

- In PEAP settings, select EAP-MSCHAPv2 for the authentication method and configure it NOT to use the Windows credentials automatically (we want to enter OTPs).

- In Security->Advanced, select "user" authentication.

- AuthLite configuration settings:

  - Make sure you have your AuthLite users reflected in the AuthLite Users list

  - Enable the IAS/NPS plugin

  - You must set a replay window greater than zero in the AuthLite configuration. This is because the OTP is checked both in the IAS/NPS plugin and also in the AuthLite core system. This limitation may be addressed in future versions.

  - Restart the AuthLite and NPS services

  - Provision keys if you are using Split users

Testing

After users are in the AuthLite Users list, and the NPS plugin is active, those users will no longer be allowed to authenticate with just username and password. *Instead of entering a username,* tap the OTP into the username field of the wireless authentication popup. Then enter the password as normal, and you should get authenticated to the network.

DirectAccess settings

AuthLite is very simple to use with DirectAccess, no special configurations are needed (apart from Offline Logon potentially, see notes). In a properly functioning DirectAccess setup, the workstations operate as though they are always on the LAN.

Procedure

- Get your DirectAccess infrastructure set up and working first *without AuthLite* being used at all.

- Install AuthLite on the domain controllers and workstations.

- You will be setting up AuthLite Integrated users.

- At the time the user logs in, the workstation will already have the machine-level DirectAccess tunnel up and running. AuthLite communicates with the DC over this channel automatically, and performs OTP validation exactly as if the machine was connected directly to the LAN (this is in fact the entire point of why DirectAccess is great)

Notes

- DirectAccess is a complex thing to get set up from scratch, especially if you are trying to do it without the UAG wizard. You should definitely **not attempt to add AuthLite** into the mix until you are finished troubleshooting any DirectAccess issues. Otherwise you'll make it harder to figure out where the problems are.

- Having a working DirectAccess infrastructure doesn't absolve you from having to consider whether you want to support Offline Logon. If the workstation doesn't have a live Internet connection, or if it is trapped behind a *captive portal* or pay gateway, then (at logon time) the DirectAccess machine-level tunnel won't be in operation. In this case, Windows falls back to the same cached logon functionality that other disconnected workstations use. So, if you need to allow AuthLite user logons during these effectively offline situations, you should configure AuthLite's Offline Logon support for those users and their workstations.

Extranet Publishing on ISA/TMG with AuthLite

To enable AuthLite users (Integrated or Split) to log on to published web sites from external locations, we provide a plugin for ISA/TMG Server. The authentication of users will be performed at the ISA/TMG Server publishing point, and credentials can then be forwarded to the target web services (OWA, for example) via a variety of authentication delegation options.

The ISA/TMG Server you use for Extranet publishing should be a domain member, because several configurations use Kerberos Constrained Delegation, which can only be done as a domain member.

Software installation

In general, you should install the core AuthLite software *and* the ISA plugin on your ISA/TMG server. See Installers.

In general, you will not need to install any AuthLite software on the web servers themselves, or make configuration changes to them assuming they are already set up to work with ISA/TMG Server.[17] With Terminal Services Gateway and Outlook Anywhere scenarios, however, AuthLite software will need to be installed on the target servers.

Workgroup ISA/TMG server

For some scenarios, it is possible to use AuthLite on an ISA/TMG workgroup machine configured to use LDAP authentication. See Appendix H: Remote Data Store mode. The ISA/TMG Server scenarios supported by the Remote Data Store mode are:

- Logon with OTP and Password using HTML Form Authentication

- Logon with Username and OTP (no password) with HTML Form. (In fact this mode does not require any AuthLite software on the ISA/TMG server.)

- Logon with Username and Password with Basic Authentication, useful for mobile devices for example.

The ISA/TMG server scenarios **NOT** supported in Remote Data Store mode are:

- Pre-authenticating a published Terminal Services Gateway

- Pre-authenticating a published Outlook Anywhere service

With Terminal Server or Outlook Anywhere services, if your ISA/TMG is not a domain member you will not be able to do any authentication on those connections at ISA/TMG, and you will need to allow them to be anonymous and authenticate directly at the back-end servers. It is far better and more secure to add your ISA/TMG server to the domain, if at all possible.

Please note:

- You will also need the AuthLite-ISA firewall plugin to be installed on the ISA/TMG server.

---

17 However for Kerberos Constrained Delegation, the web server must be a domain member configured to use Windows "Integrated" authentication.

Logon with OTP and Password using HTML Form Authentication

Procedure

- Install the core AuthLite software and the AuthLite_ISA plugin on your ISA/TMG Server. If you have an array of several ISA/TMG servers, you must install the software on each one.

- Make sure the server is rebooted after the installation.

- From the ISA/TMG console's Toolbox, open the properties for the Web Listener you want to secure with AuthLite.

- Configure the web listener to use HTML Form Authentication, and "Windows (Active Directory)" as the Authentication Validation Method. We will use the integrated AuthLite/Active Directory channel to perform authentications here, so no RADIUS setup is required.

- In the AuthLite tab of the listener properties[18], select "Enable AuthLite authentication"

- Select "Two factor: OTP and password"

- Save and apply the configuration changes.

Form Editing

You may want to change the HTML authentication form so that the first field is labeled "AuthLite key" and the type of the input field is "password" instead of "text", so the OTP characters are not shown on the browser's screen. This will help your users understand that they need to enter the OTP instead of their username, as is normally the case.

The location of the file to edit will depend on your Listener configuration. If you have used the Exchange Client Access publishing wizard, then the default location of the file is:

```
[ISA/TMG Install Folder]\CookieAuthTemplates\Exchange\HTML\usr_pwd.htm
```

whereas if you used the Web Server publishing wizard, the file will be:

```
[ISA/TMG Install Folder]\CookieAuthTemplates\ISA\HTML\usr_pwd.htm
```

To change the field label, search for "@@L_UserName_Text" in the file, and replace it with the desired text prompt.

To change the field type to password, find the line:

```
<input class="txt" id="username" name="username" type"text" />
```

and change it to:

```
<input class="txt" id="username" name="username" type"password" />
```

Notes

- The username is not required in the form, because AuthLite knows what user is

---

18 If you don't see an "AuthLite" tab, see Appendix D: The AuthLite Properties tab on ISA/TMG.

associated to each key. The username will automatically be substituted into the request by the ISA filter.

- Instead of editing the form files in-place, you may wish to *make a copy* of the Exchange or ISA folder (as appropriate) and make the changes in the copied file. Then, in the Forms tab of the Listener, you can enter the name of your new folder. After restarting the Microsoft Firewall service, ISA/TMG will then use *your* files instead of the default set.

- After changing the form files, you must restart the Microsoft Firewall service to pick up the changes.

- If you use an array of ISA/TMG servers, you must make the form changes on each server.

Logon with Username and OTP (no password) with HTML Form

Procedure

- You do not need any AuthLite software on the ISA/TMG server(s) for this configuration.

- From the ISA/TMG console's Toolbox, open the properties for the Web Listener you want to secure with AuthLite.

- Configure the web listener to use HTML Form Authentication, and "RADIUS OTP" as the Authentication Validation Method.

- Configure ISA/TMG to point at one or more built-in RADIUS servers set up for One-factor PAP, or or IAS/NPS servers configured with AuthLite plugin for one-factor PAP.

- Configure your publishing rule to use Kerberos Constrained Delegation to forward credentials to the back end web server. KCD is needed because in this scenario the user is never entering their password, so there is no way to get an AD token for them via the normal logon methods.

Form Editing

You **must** change the HTML authentication form because ISA/TMG's default form enforces a 16 character limit on the "Passcode" field. AuthLite OTP values are 64 characters long, so we must update the file.

The location of the file to edit will depend on your Listener configuration. If you have used the Exchange Client Access publishing wizard, then the default location of the file is:

```
[ISA/TMG Install Folder]\CookieAuthTemplates\Exchange\HTML\usr_pcode.htm
```

whereas if you used the Web Server publishing wizard, the file will be:

```
[ISA/TMG Install Folder]\CookieAuthTemplates\ISA\HTML\usr_pcode.htm
```

To change the field size, find the line:

```
<input class="txt" id="passcode" ...
```

that ends with

```
maxlength="16" />
```

and change it to end with

```
maxlength="64" />
```

Optionally, you can also change the label for that control from "Passcode:" to "AuthLite key:". Search and replace for the string @@L_Passcode_Text in the file.

Notes

- Instead of editing the form files in-place, you may wish to *make a copy* of the Exchange or ISA folder (as appropriate) and make the changes in the copied file. Then, in the Forms tab of the Listener, you can enter the name of your new folder. After restarting the Microsoft Firewall service, ISA/TMG will then use *your* files instead of the default set.

- After changing the form files, you must restart the Microsoft Firewall service to pick up the changes.

- If you use an array of ISA/TMG servers, you must make the form changes on each server.

Logon with Username and Password with Basic Authentication

If you have you have AuthLite Integrated users who must connect from mobile devices, you may find this configuration useful. Mobile devices normally store credentials and do not have the ability to use an AuthLite key. Since an AuthLite Integrated user cannot fully authenticate to AD without their key and password, we have to do some extra work to allow them to use Extranet services from mobile devices. We will configure the ISA/TMG Listener to support one-factor logons for this case.

A negative aspect of this configuration is that it uses the single factor AD password alone. An attacker who is able to guess the user's password could log on to any Extranet applications you publish with this configuration.[19]

A stronger way to authenticate trusted devices without allowing access to potential attackers would be to deploy user certificates to your mobile devices and set ISA/TMG to use that authentication mechanism (and Kerberos Constrained Delegation). The remainder of this section assumes that single factor username/password logon to your published mobile services is acceptable to your organization's security policies, and details that configuration.

Procedure

- Install the core AuthLite software and AuthLite_ISA plugin on your ISA/TMG Server. If you have an array of several ISA/TMG servers, you must install the software on each one.

Videos
ISA/TMG password only

- Make sure the server is rebooted after the installation.

- From the ISA/TMG console's Toolbox, open the properties for the Web Listener you want to secure with AuthLite.

- Configure the web listener to use "HTTP Authentication", and select "Basic"

- Select "Windows (Active Directory)" as the Authentication Validation Method. We will use the integrated AuthLite/Active Directory channel to perform authentications here, so no RADIUS setup is required.

- In the AuthLite tab of the listener properties[20], select "Enable AuthLite authentication"

- Select "One factor: Username and password"

- Configure your publishing rule to use Kerberos Constrained Delegation to forward credentials to the back end web server. KCD is needed because the Integrated users are not entering their OTP key, so it's impossible to get an AD token for them via the normal logon methods.

- Save and apply the configuration changes.

---

19 If your users are AuthLite Integrated, then even a correctly guessed password would not enable an attacker to log on to AD, LAN workstations, or to any VPN or Extranet services protected by a two-factor AuthLite configuration. This is because all these vectors require the OTP key as well as the password.

20 If you don't see an "AuthLite" tab, see Appendix D: The AuthLite Properties tab on ISA/TMG

Notes

- This configuration will still allow non-AuthLite users to authenticate to the same Listener with their normal username/password.

- This configuration has no bearing on Split AuthLite users, since they can log on to AD with their username and password normally anyway. They will work the same as non-AuthLite users here.

- The reason that the AuthLite software and setup is required here is to support AuthLite Integrated users. Without this extra processing, these users would not be able to authenticate to ISA/TMG server even with KCD, since their AD password cannot be formed without a valid OTP from their AuthLite key.

Supporting Shared Folders

Prerequisites

The instructions below assume you have a working shared folder already. Please verify the following points:

- Using a non-AuthLite user who has permissions to do this, verify you can connect and that your credentials give you access to the file server / shared folder.

- If you don't have this working as above, then adding AuthLite will only make things harder to troubleshoot. If you contact us for support the first thing we will do is try a connection with a non-AuthLite user to confirm your end-to-end setup is configured properly.

AuthLite setup for Shared folders

- Install AuthLite on the file server (and domain controllers, if the file server is a domain member).

- Make sure all AuthLite users are represented in the [Selecting AuthLite Users](#) section of the configuration tool.

- If these are domain systems, add the file servers (or groups containing them) into the [Forced 2-Factor Servers](#) configuration list. This will make sure that AuthLite users can only connect if they enter a valid OTP and password. (Non-AuthLite users will not be blocked by this setting. To prevent non-AuthLite users from connecting, restrict the shared folder permissions.)

- On a standalone system, the [Key Security mode](#) must be set to *Normal* (false).

Using Shared folders with AuthLite

To authenticate to a shared folder with an AuthLite user:

- Launch a shortcut to the shared resource or UNC path

- When the authentication prompt appears, tap your AuthLite key *into the Username field*

- Enter your password into the password field

- Click OK and the shared resource should open

Supporting Remote Desktop logons

This section assumes a direct RDP connection or publishing point. For Terminal Services Gateway scenarios see the next section.

Prerequisites

The instructions below assume you have a working RDP configuration already. Please verify the following points:

- Using a non-AuthLite user who has permissions to do this, verify you can connect and that your credentials log you in to the Terminal server / remote desktop system seamlessly.

- If you don't have this working as above, then adding AuthLite will only make things harder to troubleshoot. If you contact us for support the first thing we will do is try a logon with a non-AuthLite user to confirm your end-to-end setup is configured properly.

AuthLite setup for RDP usage

- Install AuthLite on the Terminal Servers / Remote desktop systems, (and domain controllers the terminal server is a domain member).

Videos
Remote Desktop access to a standalone workstation

- Make sure all AuthLite users are represented in the Selecting AuthLite Users section of the configuration tool.

- If these are domain systems, add the Terminal Servers / Remote desktop systems (or groups containing them) into the Forced 2-Factor Servers configuration list. This will make sure that AuthLite users can only connect if they enter a valid OTP and password. (Non-AuthLite users will not be blocked by this setting. To prevent non-AuthLite users from connecting, restrict permissions in the terminal servers themselves.)

- An RDP connection using Network Layer Authentication requires two sequential authentication events to establish your session. You need to set a Replay window value greater than zero so one entered OTP can be used for both of the authentications needed to establish your session.

- On a standalone system using Network Layer Authentication, the Key Security mode must be set to *Normal* (false).

Using RDP with AuthLite

To log in to the remote desktop server:

- Launch the mstsc.exe client and specify the terminal server you are connecting to

- Tap your AuthLite key *into the Username field*

- Enter your password into the password field

- Connect

Supporting Terminal Services Gateway

If you publish a Terminal Services Gateway to your Extranet, you can configure the servers to support AuthLite users ([Integrated](#) or [Split](#)).

Prerequisites

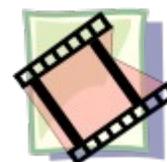The instructions below assume you have a working TSG configuration already. Please verify the following points:

- A Terminal Services Gateway is set up and configured with appropriate policies

- One or more Terminal Servers or Remote Desktop services configured

- (Optional) TSG published through a domain ISA/TMG server, listener pre-authenticating in HTTP/Integrated mode, and rule delegating to the Terminal Services Gateway with Kerberos Constrained delegation.

    - If you are not pre-authenticating at an ISA/TMG publishing point, you can still use AuthLite with TSG; just ignore the parts of the below setup that deal with ISA/TMG server.

    - It is not possible to pre-authenticate a TSG connection at an ISA/TMG server that is a workgroup machine, it *must* be a domain member.

- If possible, set the RDP proxy settings to use the same credentials for the TSG and the terminal server. This will enable you to enter one username and password and connect all the way through to the target system.

- Using a non-AuthLite user who has permissions to do this, verify you can connect from the Internet, through ISA/TMG server, through the TSG, and that your credentials log you in to the Terminal server / remote desktop system seamlessly.

- If you don't have this working as above, then adding AuthLite will only make things harder to troubleshoot. If you contact us for support the first thing we will do is try a logon with a non-AuthLite user to confirm your end-to-end setup is configured properly.

AuthLite setup for the TSG scenario

- Make sure all AuthLite users are represented in the [Selecting AuthLite Users](#) section of the configuration tool.

- If you are pre-authenticating at ISA/TMG server, be sure the core AuthLite software is installed on ISA/TMG. The ISA plugin is not required for this scenario.

- If you are publishing with ISA/TMG server and the AuthLite plugin is installed, go into the AuthLite tab on the Listener you're using, and ensure that the "Enable AuthLite Authentication" checkbox **is not checked**. This is counter-intuitive, but we must do this because the plugin cannot handle NTLM authentication, and this is the only

Videos
[Configuring Terminal Services Gateway](#)
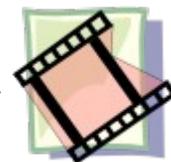
method that is supported by the RDP client. The core AuthLite software will authenticate the NTLM credentials with the domain, and then ISA/TMG can delegate this to the TSG using Kerberos constrained delegation.

- AuthLite should already be installed on domain controllers.

- Install AuthLite on the Terminal Services Gateway system. The TSG server must be a domain member.

- Install AuthLite on the Terminal Servers / Remote desktop systems. These systems must be domain members.

- Add the Terminal Servers / Remote desktop systems (or groups containing them) into the Forced 2-Factor Servers configuration list. This will make sure that AuthLite users can only connect if they enter a valid OTP and password. (Non-AuthLite users will not be blocked by this setting. To prevent non-AuthLite users from connecting, restrict permissions in the TSG or on the terminal servers themselves.)

- If possible, set the RDP proxy settings to use the same credentials for the TSG and the terminal server. This will enable you to enter one OTP and password and connect all the way through to the target system.

- A TSG connection requires several sequential authentication events to establish your session. You need to set a Replay window value greater then zero so one entered OTP can be used for all the authentications needed to establish your session.

Using TSG with AuthLite

To log in to the remote desktop server:

- Launch the mstsc.exe client

- In advanced settings, specify the external address of the TSG proxy server

- Select to use the same credentials for the proxy and the terminal server

- Specify the terminal server you are connecting to

- Tap your AuthLite key *into the Username field*

- Enter your password into the password field

- Connect

Supporting Outlook Anywhere

If you publish Outlook Anywhere to your Extranet, you can configure the servers to support AuthLite users ([Integrated](#) or [Split](#)).

Prerequisites

The instructions below assume you have a working OA configuration already. Please verify the following points:

- A working Exchange 2007 organization

- IIS and Exchange front end server on Windows 2008 (prior versions may work, not validated)

- Outlook Anywhere configured on the server, set to use NTLM authentication (Note: this option also allows Kerberos Constrained Delegation, which is what we'll use when publishing from ISA/TMG server)

- IIS on the Exchange front end server should have the RPC folder's authentication set to Integrated.

- RPC/HTTP configured and working.

- (Optional) OA published through a domain ISA/TMG server, listener pre-authenticating in HTTP/Basic mode, and rule delegating to the IIS server using Kerberos Constrained delegation.

    - If you are not pre-authenticating at an ISA/TMG publishing point, you can still use AuthLite with OA; just ignore the parts of the below setup that deal with ISA/TMG server, and set the Outlook proxy authentication to NTLM instead of Basic.

    - It is not possible to pre-authenticate an OA connection at an ISA/TMG server that is a workgroup machine, it *must* be a domain member.

- Set the Outlook proxy to the public interface of your publishing point, and select Basic authentication (if not using ISA/TMG, select NTLM authentication).

- Using a non-AuthLite user who has permissions to do this, verify you can connect from the Internet, through ISA/TMG server, through RPC/HTTP, and that your credentials log you in to Exchange seamlessly.

- Outlook Anywhere is hard to set up! If you don't have this working as above, then adding AuthLite will only make things harder to troubleshoot. If you contact us for support the first thing we will do is try a logon with a non-AuthLite user to confirm your end-to-end setup is configured properly. Here are some resources that we have found helpful in troubleshooting:

    - [How to Install Exchange 2007 SP1 and SP2 Prerequisites on Windows Server 2008](#)

    - [How does Outlook Anywhere work (and not work)?](#)

    - [How to use the RPC Ping utility](#)

AuthLite setup for the OA scenario

- Make sure all AuthLite users are represented in the [Selecting AuthLite Users](#) section of the configuration tool.

- If you are pre-authenticating at ISA/TMG server, be sure the core AuthLite software and the ISA plugin are installed on the ISA/TMG server.

- If you are publishing with ISA/TMG server, go into the AuthLite tab on the Listener you're using, and ensure that the "Enable AuthLite Authentication" checkbox is checked, and select two-factor authentication. Keep the HTTP/Basic authentication mode on the Listener, and keep delegating credentials to the OA server with Kerberos constrained delegation.

- Install AuthLite on the Exchange front end server containing IIS, RPC/HTTP, and the client access services.

- An Outlook Anywhere connection requires several sequential authentication events to establish your session, and it will use many connections over the course of the session. You need to set a [Replay window value](#) greater than zero so one entered OTP can be used for all the authentications needed to establish your session. After the window duration expires, Outlook will start prompting for new login credentials again.

Using OA with AuthLite

To connect with Outlook Anywhere:

- Go into the advanced connection settings of your Outlook's email account

- Specify the external address of the OA proxy

- Select Basic authentication if using ISA/TMG to pre-authenticate. Select NTLM if authenticating directly to IIS.

- When prompted for credentials, tap your AuthLite key *into the username field*

- Enter your password into the password field

- Connect

- After the server's [Replay window](#) expires, you will be re-prompted for new credentials. Tap in a new OTP and enter your password to continue.

Replay window for multiple-authentication protocols

When a user wants to connect to a service, they enter their credentials one time, and expect the software to use these values as many times as needed in order to log on and maintain their session. Some network protocols such as Outlook Anywhere and Terminal Services authenticate at each hop along the way from the client to the final destination server. Outlook opens and closes connections periodically, attempting to use the same credentials that the user entered to log in each time. HTTP's "basic" authentication provides the same credentials for each connection.

Since AuthLite is a "one time password" system, normally every attempt to use the same OTP again would result in the request being denied. In order to support multiple-authentication protocols, we provide a time interval in which a user's latest OTP entry can be "replayed" without denying the authentication attempt. This setting does not affect interactive logons, only network protocols.

This setting is controlled by the "Replay Window" item of the AuthLite configuration tool under the "Service Configuration" section, and is individual to each server. However you can push this value over group [group policy](.).

The default value is "0", and the value is measured in milliseconds. For domain users, this value is read on the authenticating domain controller. For non-domain logons, the value is read on the local system performing the authentication.

If you change this value, you must restart the AuthLite OTP service for your change to be effective.

See the videos for [Remote Desktop](.), [Terminal Services Gateway](.), and [Outlook Anywhere](.) for examples of using this setting.

Security considerations

The window mechanism only allows a limited replay on a user's most recently entered OTP. So no matter what the size of your replay window you need not be concerned about many previously entered OTPs being used again maliciously. Only the freshest, most recently entered OTP *is* allowed to authenticate repeatedly during the window, and as soon as the user enters a new OTP any time remaining on the old window is canceled.

The replay window only pertains to network (non-interactive) logons and to Remote Desktop. There is never any replay allowed for interactive logons to the console, and as soon as a console logon occurs, any existing replay window for that user is canceled.

A short replay window such as 10 seconds does not notably diminish the security of an OTP system against most types of attacks. However if an adversary can launch immediate parallel sessions from your machine or in some automated, instantaneous fashion, then any replay window at all can allow impersonation. if you are not using any multiple-authentication protocols with AuthLite you can leave the window at the default value "0", disabling this behavior completely.

A longer replay window such as is needed for Outlook Anywhere or HTTP Basic authentication decreases some of the benefits of a one-time-password system. An attacker who is able to capture the user's OTP and password would have the ability to use these

credentials *during the replay window*, and impersonate the user. A long window gives an adversary more leisure to perform an impersonation attack, and requires less sophistication. The dual credentials are still far more secure than a plain password, and the vulnerability is still time limited, but this is not *as* secure as using a small or zero replay window.

Deployment considerations

Changing the window size on each domain controller manually may not be practical for large deployments. You can use Group policy to push this setting; see Appendix E: Using Group Policy to deploy software/settings.

TSG/RDP settings

For a TSG scenario, a short window value of 10-20 seconds is probably long enough to allow all the authentications (ISA/TMG server, TSG, RPC, Network Layer Authentication, remote desktop session) to complete. And after those initial connections, no more authentications need to be performed. If you are not able to connect, check your AuthLite Log for recent replay events, and increase the domain controllers' replay window as needed.

Outlook Anywhere settings

For Outlook Anywhere, several connections will be opened and closed throughout the user's session, and Outlook will keep using whatever credentials the user last entered. Shortly after the OTP replay window expires, Outlook will fail to make new connections, and pop up a dialog requesting new credentials.

So the length of your OTP replay window will effectively determine how long a user can use OA before needing to tap a new OTP into the authentication popup. Set the window long enough so as not to be overly annoying, but short enough to mitigate the threat of an attacker recording and re-using the credentials later. For example 30 minutes (set as 1800000 milliseconds) is a reasonable session length, but 8 hours would probably be irresponsibly long.

AuthLite Logging

"AuthLite Security" event log

On any system that authenticates AuthLite users, there is a new Event Log called "AuthLite Security" added, which records successes and failures for

- OTP authentication events.

- Events from the AuthLite RADIUS service.

In a domain, only the DC performing the actual authentication will log these events. For standalone/local users, the local machine will record the events.

When a user completes a logon to Active Directory, you will still see the normal Windows Security log events as well. AuthLite does not remove or replace any of the default Microsoft authentication technology.

Other logging

By default, the AuthLite service records events to the Application event log when the service is starting and shutting down. It is possible to configure the AuthLite service and infrastructure components to log events at a much more detailed level suitable for troubleshooting. Contact support for assistance.

Support for Other Configurations

A rich ecosystem of applications all rely on the built-in authentication mechanisms of Active Directory. With AuthLite we have tried to support the most common cases as transparently as possible. If you have difficulty using an application with AuthLite, there are a number of approaches we can take to support your needs, as appropriate:

- Troubleshooting-- If a configuration is supposed to work and does not seem to, the first thing we will do is turn on extra logging and determine where the failure occurs. For successful authentication, many components must work together seamlessly. Extra logging may show the problem and lead to an easy remedy.

- COM API-- It is possible to provision and validate AuthLite users through a COM interface, enabling custom administrative tools to be used.

- Windows / Application API hooking-- We can help you to determine what method or API your application is using to authenticate to AD, and possibly create a hook to modify this behavior to be AuthLite compatible.

Please open a support request, or contact your representative to get started.

Appendix A: Account Recovery Considerations

Active Directory Accounts

In an Active Directory domain, AuthLite user accounts can be administratively reset through the normal AD Users and Computers console, without data loss. The directory has built-in technology to avoid the loss of EFS/Bitlocker and certificate access that will occur for standalone accounts.

Therefore, there are no special precautions you need to take in an AD environment to protect your normal users from account and data loss. It is definitely advisable to have at least one domain administrator account that is *not* an AuthLite user, in the event that you need to perform logons or operations where AuthLite software is not installed or is functioning improperly.

Standalone Machines / Local user Accounts

The private keys for Microsoft EFS/Bitlocker and user certificates are protected by the user's password. Forcibly resetting a local Windows user's password will result in data loss if you use EFS/Bitlocker or user certificates, because those items could only be updated from the old password to the new one when both passwords can be provided at the same time. This behavior is necessary and *by design* of Microsoft, to protect the security of these items.

Further, AuthLite integration strongly protects user accounts by augmenting the security of the password. Even changing the password of an [Integrated](#) user requires the existing key/password to be provided. There is truly no way to "bypass" the AuthLite key and gain access to the account by only entering the password.

Be skeptical of the security of any logon product that offers a way to log on or change the account password without using all of the security factors! Any time there is a way to bypass the highest level of security, that means an attacker could use the lower security method to compromise your account more easily. This is a common security precept known as "low hanging fruit" or the "path of least resistance". Offering a lower security recovery option to the user means that the high security is effectively *optional*, and thus it will not provide any strength against a smart attacker.

Based on the above facts, we arrive at the important ramification of this section: If you lose your key or if your system is not running the AuthLite authentication software, it is impossible to logon to the system with any AuthLite Integrated account. Further, as noted above, if you forcibly reset that local account's password to gain access again, the account will lose access to any EFS/Bitlocker files or user certificates.

These following situations require **preemptive** recoverability consideration:

- *Lost, broken or accidentally deleted AuthLite key*: You can avoid needing a password reset in this case by having one or more backup AuthLite keys configured to your account. Alternately, if you have a password recovery disk for the account then you can reset the password without data loss.

- *Forgotten password*: This situation has the same ramifications as losing the password on a non-AuthLite local account. There will be no way to log on until the password is

reset. To avoid data loss, record your password in a secure location for emergency retrieval, or set up a password recovery disk for the user account.

Additional AuthLite keys for account recoverability

You can set up extra keys for your local AuthLite user's account any time. Maintaining the keys across password changes for a local user requires extra steps, see the notes below.

Procedure

- Open the AuthLite Configuration application

- Under Management select the "My Integrated Keys" item

- Place focus into the "Current AuthLite key" field

- Plug in your existing AuthLite key and enter an OTP into this first field

- Enter your account's password into the next field

- Unplug your existing AuthLite key

- Plug in a new, blank key that you want to add to your account

- Click the "Program" button

Password Recovery disk for account recoverability

Windows allows the creation of a disk or USB key that contains a private key which can be offered in place of normal account credentials, to be used in an emergency where the account cannot be logged on. You must set this up proactively, while you still have access to the account. There is no way to make a recovery disk after you lose access, and no other way to recover the account without losing EFS/Bitlocker and certificate access.

Procedure

- Start with the account configured as a default one-factor (username and password) account, *not AuthLite Integrated*. This is necessary because the Windows Password Recovery dialog is not extensible and cannot be made to work with AuthLite.[21] If your user is already AuthLite Integrated, change the password and de-select the "Use AuthLite key" checkbox. After your disk is created, you can re-Integrate the account with AuthLite.

- Run the "Forgotten Password Wizard".

    - In Vista/Win7, go to the "Change Password" screen and click "Create a password reset disk"

    - In Windows XP, go to the "Change Password" screen and click the "Backup" button.

- After you have completed the wizard, place the recovery disk in a secure location.

- You may now Integrate the local user account into AuthLite, and in the event the key or

---

21 This limitation may be addressed in a future version.

password is unavailable, you can recover access to the account safely with the recovery disk.

- It is not necessary to update the recovery disk when you change your password. The disk uses a private key and does not actually need to know what the password was in order to function.

Appendix B: Active Directory Deployment Notes

Licensing

Enter the license code on one Domain controller where AuthLite is installed, and it will propagate to other DC's via replication. Member servers and workstations will read the license value from the directory as well.

Due to replication delays, some servers may temporarily still believe they are unlicensed.

Software Installation

In order to authenticate AuthLite Integrated users, a Domain Controller must have the AuthLite infrastructure software installed. If a workstation (or member server) connects to a DC where AuthLite is *not* installed, all the AuthLite operations will fail on that machine, including authentication of Integrated users.

Videos

Active Directory installation

Domain Controllers with AuthLite software installed will still function normally for all their normal roles, including authentication of non-AuthLite users. AuthLite does not replace or remove built-in Microsoft components or behaviors.

Application Partition (database)

AuthLite takes advantage of the robust, multi-master replication offered by Active Directory by using an Application Partition to store all its user data and domain-wide settings. This is the same method that Microsoft's own DNS server uses to manage its data.

The first installation of AuthLite on a Domain Controller in your enterprise will automatically create this partition, and the schema additions necessary to support it. Thus, the first DC you install AuthLite on will be a replication host for the partition, by default.

AuthLite does not add or change any schema properties on the "user" or other built-in objects in Active Directory. All AuthLite data is stored separately in the AuthLite Application Partition. Adding the AuthLite schema elements will have *no performance impact* on user object replication since we don't touch those objects at all.

Replication hosts

By design, AD Application Partitions do *not* automatically replicate to every DC in your enterprise, because it is assumed that the data they contain may only be needed by a subset of the enterprise. If a DC receives a directory query for a partition that's not stored locally, it will refer the request to a remote DC that stores the partition.

This referred connection can be slow if the remote DC is in another site. Since AuthLite requires access to its partition in order to operate, any AD site where AuthLite is used should have at least one DC that hosts a replica of the AuthLite data partition.

Also, to support redundancy if the first partition host goes offline, you may wish to host the partition on more than one Domain Controller in the same site. (Without access to the

AuthLite partition, [Integrated users](#) will not be able to log in, and the [built-in RADIUS service](#) and [IAS/NPS plugin](#) will not function.)

You can easily specify that a DC should host a replica the AuthLite partition at install time, by selecting the checkbox "Replicate an existing AuthLite partition to this server". For this option to work, there must already be at least one other accessible DC that hosts the partition.

This option in the AuthLite installer doesn't perform any proprietary operations when making a replica, it is just a convenience. You can also use the Microsoft command **ntdsutil** to control the replication hosts for Application Partitions. The partition's distinguished name will be

```
DC=AuthLite,[your-domain's-dn]
```

Content

Although not necessary for normal operation, you can browse and change the partition content with the Microsoft MMC plugin **adsiedit**.

To browse the AuthLite key data, you can use the [AuthLite Data Manager](#) application installed on the domain controllers.

Deletion

Uninstalling AuthLite does not remove the data partition or affect which DC's host its replicas. This way, if AuthLite is reinstalled, all the existing data can be used again, and users can continue to authenticate. If removal of the partition is desired, this can be accomplished with the Microsoft **ntdsutil** command.

Appendix C: Kerberos Constrained Delegation Notes

Kerberos Constrained Delegation is a useful Microsoft extension that can allow IIS web servers to trust credentials provided by ISA/TMG server, even in scenarios when the user does not ever provide their password to log on to the Kerberos (AD) domain in the first place. AuthLite makes use of this technology in the following scenarios:

- Mobile devices that must log on to Extranet services with only username and password. AuthLite Integrated users need both their key and password to truly authenticate, but there still must be some way for them to use these "password only" devices.[22]

- Extranet services that use only the username and OTP for logon. The password is never entered, so the users cannot be logged in to AD.

In these cases, ISA/TMG Server (with AuthLite installed) can verify the identity of the user, but there is not enough information provided to get an impersonation logon token from AD. The best ISA/TMG can do is get a Kerberos ticket via the "Service for User" (s4u) system. This kind of ticket provides a useful token that the local machine can use, but we still need a way to tell the remote IIS machine about the user.

This is where KCD comes in. ISA/TMG can take the s4u ticket and use it to get another ticket that will work on the remote service (for example the IIS server on your front end Exchange server). This will only work for the specific services that ISA/TMG's computer account is allowed to delegate to (this is why it's called "constrained"). The target service (for example an IIS Server hosting OWA) is trusting ISA/TMG to do a good job of authenticating the users.

KCD technology is built in to AD, ISA 2006/TMG and IIS. You can use it instead of other delegation options in ISA/TMG even when full credentials are available. In the above scenarios for AuthLite, however, there is no other choice than to use KCD, because full user credentials are never provided. You are choosing to say, in effect, even though we don't have complete information to do an authentication to Active Directory, the information we *do* have is sufficient to authenticate the user for the purposes of using these Extranet services. It is a matter of the security policy of your organization, the threat models you are addressing, and the usability of the Extranet services.

Several things must be configured correctly to use KCD. These requirements are based on the way Microsoft has implemented the technology, and don't have anything to do with AuthLite, per se. An excellent resource for KCD configuration between ISA and IIS (Exchange) is the article Kerberos Constrained Delegation in ISA Server 2006.

---

22 For trusted devices, instead of using the AuthLite username/password configuration, you can deploy user certificates on the devices, and delegate credentials from ISA/TMG to IIS with KCD as described here.

Appendix D: The AuthLite Properties tab on ISA/TMG

In ISA/TMG, a Web Listener's properties page can be accessed several ways:

1. From the "Web Listener" tab on a publishing rule

2. By double-clicking its name in the firewall policy item corresponding to a publishing rule

3. Through the "Toolbox" view on the right-hand side of the console

However, due to a design flaw in Microsoft's ISA/TMG management console, the control tabs for third-party extensions (such as AuthLite) cannot created when you open the property sheet with approaches 1 and 2. In order to view or change the AuthLite properties for a Web Listener, you **must** open that Listener's property sheet **from the Toolbox view**.

Videos

View the AuthLite properties for an ISA/TMG Listener

Appendix E: Using Group Policy to deploy software/settings

Administrative Template for settings

In a domain environment, most AuthLite settings are stored on domain controllers, in the data partition. These settings are automatically applied by all AuthLite-aware systems as needed. But certain settings, notably the OTP Replay window, are server-specific and stored in the registry.

In order to deploy a replay window setting administratively to a group of domain controllers[23], you can use a group policy Administrative Template. Save the following lines as a unicode text file with an .adm extension:

```
CLASS MACHINE
CATEGORY "SOFTWARE\Policies\Collective Software\AuthLite\MessageHandlers"
  POLICY Validate
  KEYNAME "SOFTWARE\Policies\Collective Software\AuthLite\MessageHandlers\Validate"
    PART OtpReplayWindow EDITTEXT
    VALUENAME "OtpReplayWindow"
    END PART
  END POLICY
END CATEGORY
```

You can then load this adm file into the group policy editor, in the "Administrative Templates" section of the Computer Configuration, and assign a value (in milliseconds) to the OtpReplayWindow item. This setting will then be applied along with the rest of the machine policy.

Note that the AuthLite Service only reads settings on start up, so changing this value via policy will not have an immediate effect, even if you run "gpupdate" and apply the policy immediately.

Software deployment

See this KB article for information on deploying AuthLite software unattended, via Group policy.

---

23 The replay window is only used on domain controllers, because this is where domain accounts are authenticated for network logons. Deploying a replay window setting to (for example) an Exchange server won't have any effect; the value that matters is on the domain controller which that Exchange server connects to.

Appendix F: Key Security modes

Overview and defaults

NOTE: This section applies to users of *Standalone machines*, and it does *not* apply to users in an Active Directory domain.

On a standalone machine, all the data needed to authenticate a key must be stored on the system's own drive. AuthLite 1.1 and later can use one of two security modes to protect this data from attackers who may gain access to the drive:

- *Normal protection*: Key data cannot be accessed unless the authenticator also possesses an OTP from that key. This provides reasonable protection against most threat models, and enables remote-access features such as Remote Desktop logons that require Network Layer Authentication and accessing Shared Folders. This mode is the **default** configuration in AuthLite v1.1

- *Strong protection*: Key data cannot be accessed unless the authenticator also possesses the user's current plain text password. This provides the strongest possible protection but will not allow AuthLite users to access remote features such as Shared Folders and Remote Desktop logons that require Network Layer Authentication. This operation mode is the default for AuthLite v1.0 and any systems that are upgraded from 1.0.

Motivation for changing the default

There are two circumstances when you might want to change the default protection mode that the installer has made on your system.

- You have a fresh AuthLite install using *Normal* protection, but you don't need to use RDP+NLA or file sharing, and wish to use the strongest possible protection for the key data stored on your drive.

- You have an AuthLite install that was upgraded from version 1.0, using *Strong* protection, but you want to use newly available remoting features with an AuthLite account, such as RDP+NLA or authenticating to file shares.

"Orphaning" current AuthLite users

The protection mode is a system-wide setting, and once you change it, any AuthLite users who were set up using the previous mode will encounter problems such as being unable to change their passwords.

To prevent problems, before changing this setting you should **first** make sure all current AuthLite key users revert to normal Windows logon. After you change the setting, they can Integrate their accounts once again by visiting the change password screen and selecting the AuthLite Key checkbox.

Changing the protection mode

To select the protection mode you wish to use, set the value of the following registry key:

`HKLM\Software\Collective Software\AuthLite\Settings\StrongProtectionForLocalAccounts`

Allowed values are `true` or `false` , meaning:

- "true": Use the strongest protection mode, making remote features unavailable. Default for AuthLite v1.0 and upgrades from 1.0.

- "false": Use the normal protection mode, slightly less secure but allowing remote feature use. Default for fresh installs of AuthLite v1.1 and later.

Appendix G: Key hardware notes

All AuthLite hardware tokens are Yubikeys manufactured by Yubico. They do not have batteries and do not expire, and they can be re-programmed indefinitely.

Keys obtained from Collective Software

We ship keys with a blank configuration that can be easily programmed by AuthLite.

Revision 2.0 and above

These keys have a gold-colored contact button. Touch the button briefly and release to enter an OTP.

The keys shipped by Collective do not make use of the keys' second configuration area,[24] but we store an unused single-character "static password" in this area so the keys will not operate in Revision 1.3 mode. Once again, to be clear, we don't use this for anything. It's just there as a placeholder to force the keys to operate in v2.0 mode.

If you like, you can store a Yubico-compatible OTP or a real static password in the second configuration area. You utilize the second ID by holding your finger on the button for about 3 seconds and then releasing. Note that AuthLite does not currently do anything with the second configuration in these keys. You need the personalization tool from Yubico if you want to set up or change the second identity.

If you clear the second identity completely with the Yubico personalization tool, the key will run in Revision 1.3 mode, and act identically to a v1.3 key including the ½ second tap delay. If you don't like the delay but don't want to have anything in the second identity slot, we recommend configuring it in "scan code" static password mode and having it emit a single character code. (This way you won't mistake the short code for an OTP; if you see the single character being typed then you know you're holding the key switch too long) This is how we ship all our keys as of September 2010. Conversely, if you *prefer* the 1.3 behavior, you can clear the second identity of the keys and they will then operate in Revision 1.3 mode.

Revision 1.3

These old keys from 2009 and earlier have a black-colored contact button flush with the key's surface. Hold your finger on the contact for about ½ of a second, until the key begins entering characters. This delay is set by design, so accidentally touching the button does not type an OTP.

V1.3 keys do not have a second configuration as the newer ones do. (These keys are no longer being manufactured, but this section is relevant because newer keys behave in "1.3 mode" when their second identity is blank.)

---

24 Keys shipped prior to September 2010 have a Yubico-compatible OTP in the second configuration area. If you still want to do this with your key, you can now program it yourself with the Yubico personalization tool and upload it to their site.

Keys obtained from Yubico

Yubico now exclusively sells [Revision 2](#) keys. You can purchase your keys directly from Yubico and use them with AuthLite, but please note the following details.

Yubico ships keys with an online OTP identity in the first configuration area. It can be used (independently of the AuthLite identity) to access many online applications that support Yubico's web service. But AuthLite also wants to use this configuration area, so once you program the key with AuthLite, the Yubico identity will be **deleted** and forgotten forever. When you attempt to program these keys in AuthLite, you will see a popup warning you that the key already contains an identity, and asking you to confirm the operation.

Also, the second configuration area is left empty by Yubico, so the key will run in [Revision 1.3](#) mode and act identically to a v1.3 key including the ½ second tap delay, unless you add something to the second configuration. **AuthLite is not aware of the second configuration area currently**, and will ignore whatever is there. If you want, you can use the Yubico personalization tool to create and upload a new Yubico-compatible OTP identity into the second configuration of your key.

Appendix H: Remote Data Store mode

There are some situations where you need the AuthLite core and service to behave as if it was installed on a domain controller, even though in reality it is on

- a workgroup machine

- a read-only DC

- a non-DC IAS/NPS server

In Remote Data Store scenarios you still have to install AuthLite on at least one read/write Domain Controller, in order to create/replicate the data partition and make the configuration and data manager tools available. Install AuthLite normally on one or more DC's.

On the "remote" machine you must then launch the AuthLite core software installer from the command line, using the extra property switch REMOTEDATASTORE=1. For example:

| **Videos** |
| ISA/TMG install, Remote Data Store mode |

```
AuthLite_Setup_Win32.exe REMOTEDATASTORE=1
```

or

```
AuthLite_Setup_x64.exe REMOTEDATASTORE=1
```

and then configure extra settings in the Remote Data Store section of the AuthLite configuration tool. See the video for details and an example of this setup.

Notes

- The AuthLite "Getting Started" wizard will launch on your first login after installing and rebooting. In Remote Data Store mode, the true license will be read from the domain controller, so you should **cancel** this wizard instead of trying to activate a license on the remote machine separately.