

Under the Microscope Password checking

by
Mark
Cornaia

Level: Advanced
Works with: All
Updated: 09/04/2001

The Notes from Support column is brought to you by Lotus Support and features in-depth technical articles that explore how a particular Domino or Notes feature works. This month's article examines the password checking process.

In addition to public key checking and user group access rights to a server, the Notes/Domino authentication mechanism of client-to-server access can be extended using password checking. Quite simply, password checking ensures that users are forced to change their passwords at regular intervals.

This enforced changing of passwords adds an additional level of safety to the authentication process. For example, if someone acquired a user ID file and its password, they would normally be free to access the server using this copy of the ID. However, with password checking enabled, if the victim changes their password on their legitimate ID file, the server is made aware of the change. Thereafter, anyone trying to gain access with the stolen copy of the ID will be refused access to the server.

This article examines how password checking is implemented in Notes/Domino, explores the intricacies of authentication with password checking, and provides some hints and tips for administering—and troubleshooting—the password checking process. This article assumes an advanced level of knowledge of Domino server administration and network architecture.

Password checking basics

When password checking is enabled, the administrator specifies a required change interval (in days) that forces users to change the passwords on their user ID files within the interval. The Notes client prompts a user to change their password as the expiration date of the password draws near.

In addition to the change interval, the administrator can also specify a grace period. This is a time (in days) that indicates how long after the expiration of a password the user has to change their password. In R5, after the change-interval-plus-grace-period elapses, the user is denied access to the server (that is, they are locked out) until the administrator resets their account in their Person document. (Behavior in pre-R4.6.7 clients is slightly different and is described later in this article.)

Both the Notes client and Domino server are involved during the password checking process. The majority of work and enforcement of a Domino server lockout (based on password checking) is actually carried out on the Notes client.

The user's ID file stores the information necessary to calculate the password's expiration date. The ID file includes:

- The date of the last password change
- The number of days until the password expires
- The maximum number of days that a user can go without changing their password
- The current password

- A history of the last 49 passwords used and the dates each password expired

The server also has password checking information, which is stored in the Domino Directory. The Server document for each server includes the "Check passwords on Notes IDs" field, which you use to enable and disable password checking on a server-by-server basis. In addition, each Person document includes the following parameters:

Parameter	Description
Check password?	Used to enable and disable password checking for the user's ID.
Required change interval	Defines the life of a password, or how many days a single password should be valid.
Grace period	Defines the number of days after a required change interval during which the user can still change their password before the Notes client locks them out of the server.
Last change date	A server-based copy of the date the user last changed their password.
Password digest	An encoded version of the password that is retained by the server. When the user logs into the server, the client must provide a matching password during authentication with servers that have password checking enabled.

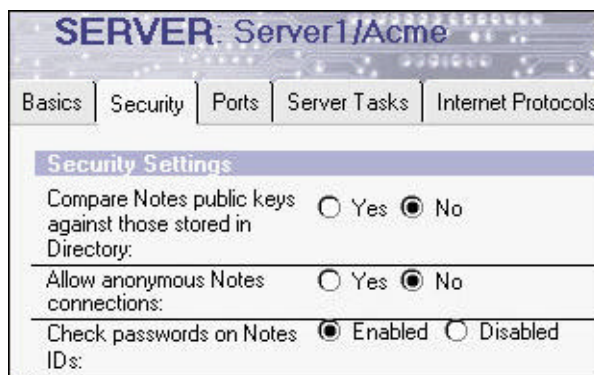
Setting up password checking

To set up password checking, you must enable it on the server and then specify which users it should apply to.

Enabling password checking on the server

You enable password checking on the server using the Server document:

1. Open the server's Server document.
2. On the Security tab, set the "Check passwords on Notes IDs" field to Enabled.



3. Save and close the Server document.
4. Restart the server.

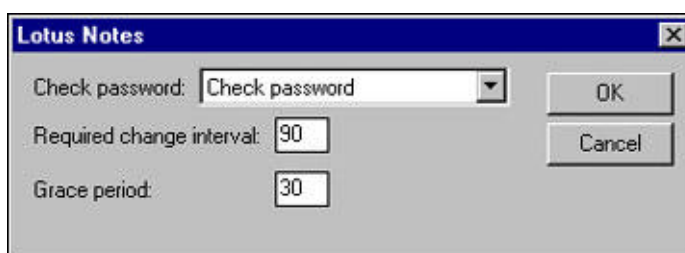
After the server restart, when a Notes client opens a session with this

Domino server, the Notes client reads this field. If the field is enabled, then client-side password checking features are enabled for this server connection. If the field is set to Disabled, the server will not perform any password checks for all clients that authenticate—even if their Person documents are set to enabled. In short, this Server document setting is the master on/off switch for server-side password checking.

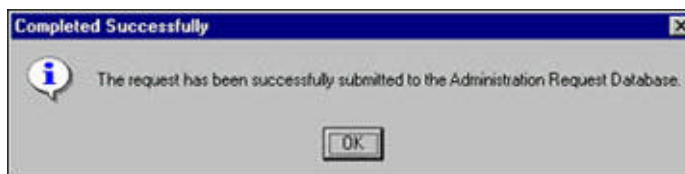
Enabling password checking for users

With the Domino server enabled, the next step is to define which particular users you want to enable password checking for. You use the users' Person documents to do this:

1. Using an Administrator's ID, select the Person documents of the users in the People view of the Domino Directory.
2. Choose Actions - Set Password Fields. A message appears asking you to confirm the change process.
3. Click Yes to confirm that you want to set the password fields for the selected Person documents. Another dialog box appears, requesting more information.



4. There are three options for the Check password list box: Check password, Don't check password, and Lockout ID. Select Check password. (Don't check password is used to disable password checking once it has been enabled for a user, as described in the [Turning off password checking for a user](#) section below. Lockout ID allows the administrator to manually lock out a user from the servers even if the password they enter is correct, as described in the [Locking out a specific user](#) section below.)
5. Enter the required change interval and grace period in days. For example, enter 90 days for the change interval and 30 days for the grace period. This means that the user is required to change their password every 90 days. After this 90 day period elapses, the user will no longer be able to access the server but they have an additional 30 days in which to change their password before they will have to call an administrator to unlock their account.
6. Click OK. Immediately, the Administration Process (Adminp) request is written to the Domino server's Administration Request database (admin4.nsf), and you'll see an acknowledgement message.



How the process completes

You can open the Administration Requests database to see the Set Password Information request in any of the All Request views.

Administration Requests	Date	Schedule Type	Action
Administrative Attention			
All Activity by Server			
All Errors by Date	22/01/10 21		Set Password Information
All Errors by Server			
All Requests by Action			
All Requests by Name	server1/10.06		Put Server's Notes Build Number into Server Record

The actual Administration Process Request document includes the action, server to perform the action, names to perform action on, who requested the action, the changes to be made, and so on.


Administration Process Request

Administration Process Request

▼

Administration Process Request	
*Action:	Set Password Fields
*Server(s) to perform the action:	Administration Server of Public Address Book
*Name(s) to perform the action on:	Mickey User/Acme
*Action requested by:	Joe Admin/Acme
*Name of process to perform action:	Adminp
Check passwords:	Check password
Password change interval:	90
Grace period:	30

Once Adminp has processed the change request, a confirmation document appears in the Administration Requests database. At this point, the process is only partially complete. The configuration is "in place," but the user needs to log into the server to ensure that the password digest data can be successfully sent back to the server.

	Date	Schedule Type	Action
▼ Mickey User/Acme	22/01 10:21		▼ Set Password Information
	22/01 10:25		server1/Acme performed action on: 22/01 10:25
▼ server1/Acme			

You can also check the Administration tab of the Person document, where the Check password, Required change interval, and Grace period fields are now set. Note that the Password digest field will be blank until the user authenticates with the server.

PERSON: Mickey User/Acme Mickey User/Acme @ Acme

Basics | Mail | Work/Home | Other | Miscellaneous | Certificates | Administration

Administration

Owners:

Administrators:

Check password:

Required change interval:

Grace period:

Last change date:

Password digest:





When the user tries to access the server using their ID, certificate authentication with the server occurs first. Then, the Notes client checks to see if the server is enabled for password checking and if so, then checks the user's Person document to see if it too is enabled for password checking. If you've followed the steps given above, both of these checks prove true.

In the example, because this is the first authentication since the password checking request was made, the Notes client finds the pending Adminp request and pulls the grace period and change interval into the user's ID file from the user's Person document. Once this is accepted, the client creates a new change request in the Administration Request database so that the Person document can be updated. This request confirms that the user ID has received the grace period and change interval information and includes the current password digest from the ID file along with today's date as the last change date.

Here is the new structure that has been added to the user ID file:

```
PWD_KEY_HDR
Type: 0000
Version: 0000
LastChanged: TIMEDATE
Innards: 0025 69DC 0039 822B
Text format: 22/01/2001 10:28:08
ExpirationDays: 0000 005A
NextExpirationDays: 0000 005A
NumDomains: 0001
NumOldPwds: 0001
OldPwdTotLen: 0214
```

When Adminp processes the new change request, the password digest is copied into the user's Person document along with the last change date to reflect the password initialization. Adminp creates a confirmation document when this request is processed.

	Date	Schedule Type	Action
▼ Mickey User/Acme			
	22/01 10:21		▼ Set Password Information
	22/01 10:25		server1/Acme performed action on: 22/01 10:25
	22/01 10:28		▼ Change User Password in Address Book
	22/01 10:28		server1/Acme performed action on: 22/01 10:28

If you check the Person document now, you'll see that the password digest and last change date information is complete.

PERSON: Mickey User/Acme Mickey User/Acme @ Acme	
Basics	Mail
Work/Home	Other
Miscellaneous	Certificates
Administration	
Owners:	Mickey User/Acme
Administrators:	
Check password:	Check password
Required change interval:	90
Grace period:	30
Last change date:	10:28:08 Today
Password digest:	AFE1486708060678C3BD72303CED96AE

Now that the Person document contains the password digest of the user's current password, password checking on this ID and for this server is set up and in effect.

Understanding server lockouts

As long as the user changes the password on time—that is, during the change interval—all is well. But what happens when a user doesn't comply? This section examines what determines when a user is advised of a pending lockout or is locked out of a server.

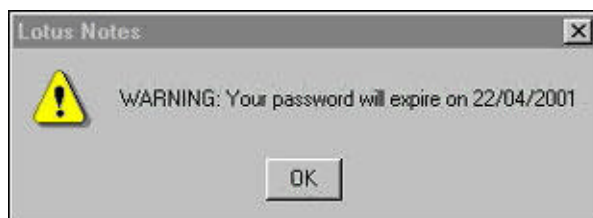
Checking the expiration date status on the client

As we've already seen, the Notes client knows a lot about the user before they actually log into a server. These parameters within the ID are used to trigger events on the client and to display warning messages to users depending on where they are in the password checking cycle.

The NOTES.INI file includes a CertificateExpChecked variable, which defines the current ID file name in use by the client and the date that the user ID was last used. As Notes loads, it checks this setting. If the date listed in the CertificateExpChecked setting is less than today's date, then Notes checks the ID file to ensure that it has a valid in-date certificate and, if necessary, warns the user that their password may expire, based on the following formulas:

Expiration Date = (Last Change Date + Change Interval)

IF (Expiration Date - Today's Date) < (25% of change interval)
THEN display a warning

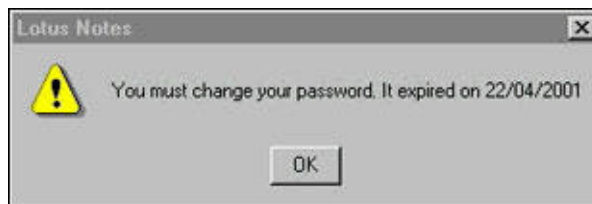


This message will appear once per day, every day that the IF statement is true up until the time the password change interval is past. (Remember, this message will appear without having to connect to a Domino server; the client has all the information it needs within the user's ID file without needing to read the user's Person document.)

Connecting to the server

When a user connects to a server, the client examines the Server document to check if the server is enabled for password checking. If it is, the next check is against the user's Person document to see if the Check password field is enabled.

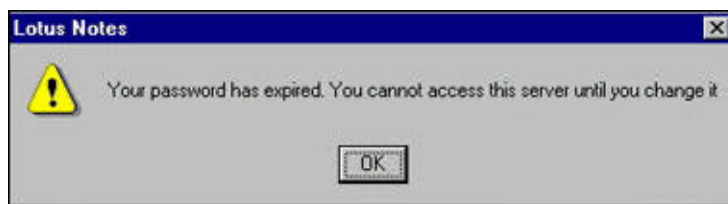
Every day until the user changes their password they will receive the warning message above. They can still access the servers that are enabled for password checking right up to the time their password is due for renewal, that is, when the change interval has passed. At that point, the user will see a new message, explaining that their password has expired. As with the previous error message, this message will occur on the client even before the user tries to connect to a server.



The expiration date in the message is calculated using the formula:

(Last password change date) + (Change interval as stored in ID)

In R4, at this point, the user was able to authenticate and access a server enabled for password checking after clicking OK. They would then enter the grace period, which gave them a few more days to change their password before they were locked out of the server. However, this behavior changed in response to customer requests. In R4.6.7 and later clients and in R5 clients, clicking OK removes the message but does not allow access to a password checking enabled server. Instead, when they try to access the server, they receive another message.



They cannot access the server until they change their password. If they decide to back out and try accessing a server that's not enabled for password checking, they can do so; but they will still see the warnings about an expired password.

In any release, once the password has expired—that is, the password change interval has passed—the client and the user ID file are operating in the grace period.

- In R4.6.7 and later and in R5, the grace period is the time after the password has expired during which the user is able to change their password before the account is locked out. (The user will not be able to log into a server that is enabled for password checking during the grace period.)
- In pre-R4.6.7 clients, the grace period is an extension of the time during which the password can be changed. The user can still access all servers but will receive stronger warnings as time passes until their account is finally locked out at the end of the grace period.

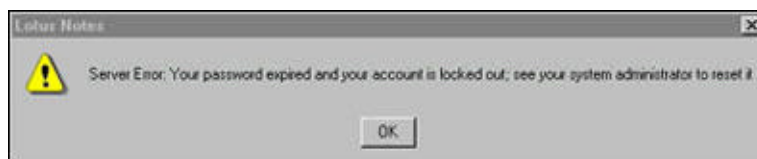
User lockout

In the example, the grace period for the user is set to 30 days and they are

using an R5 client, so they have a 30-day time window in which they must change their password if they want to access any of servers set up to enforce password checking. After this 30 day grace period expires, access can be restored only after the administrator of the server manually resets the user's account by modifying the user's Person document.

Usually a 30-day grace period is quite adequate. Even if the password expires just after a user goes on vacation, for example, they will still be able to change their password and continue working when they return without any administrator intervention (unless, of course, the user's vacation is longer than 30 days).

If the user ignores the password change warnings throughout the grace period, then the next time they access the password checking enabled server they will see a new message, which tells them they are locked out.



In addition to this client warning, the server logs a similar warning.

```
23/05/2001 11:11:21 CN=Mickey User/O=Acme failed to
authenticate: Your password expired and your account is
locked out; see your system administrator to reset it
```

At this point, the Notes client prevents the user from accessing the server. Even if the user changes their password after this period they will be unable to access this server to submit the Adminp password change request. Once the user has seen this error message they have no option but to call an administrator for assistance.

Also be aware that at this point, the digest stored in the Person document is scrambled and so is different than the copy stored in the user ID file. This mechanism provides a safety net for administrators. For example, if a user leaves the organization and the administrator forgets to add them to a Deny Access group, then as long as password checking remains enabled anyone using that user ID will be unable to access the server because the digests will no longer match. (This, however, is no substitute for Deny Access ACL groups.)

Unlocking the account

Only an administrator, who has access to the user's Person document, can unlock a user's account once it is locked out. The steps for unlocking an account are straightforward, but there's opportunity for error if the administrator doesn't complete the whole Adminp process or modifies the wrong fields by mistake.

First, the administrator deletes the password digest in the Person document. The next time the user logs onto the server they will still be denied access, however, because the user ID file still contains an expiration date that has expired. The user must change their password in their user ID file. This updates the password digest in the user ID file; and since there is no digest in the Person document, there is no "password digest check to take place" and the user is granted access. Because the last change date is more recent than recorded in the Person document, the client generates an Adminp request, to inform the server of the new password change.

	Date	Schedule Type	Action
▼ Mickey User/Acme	23/05 11:24		Change User Password in Address Book

After Adminp processes this change request, the Person document for the user will now have the same password digest and last change date as the user's ID file. No changes need to be made to the ID file since this request is a push from the client to the server. The user can now continue accessing the server.

Summary of password checking events

The [Flowchart of password checking events](#) sidebar provides a summary of the password checking cycle. It shows the client and server events and warnings and can help you isolate possible configuration or synchronization issues.

In addition to the previously described messages, there are some additional checks carried out by the server to ensure that digests and dates are kept synchronized. For example, when the client sends the server a user ID's digest that is stamped with a date far in advance of the server time, then there must be something wrong with the client operating system clock. In this situation the client will see the message "Connection failed because of a problem with clock synchronization and password change intervals. Check your clock setting, change your password, or consult your system administrator."

Additional hints and tips

Here is some additional information and tips that will help you administer and troubleshoot password checking.

Working with the Person and Server documents

You should make changes to the grace period and the password change interval using the Adminp actions. Editing these fields directly in the Person document prevents Adminp requests from being generated and subsequently brings user IDs out of sync, which can cause users to be locked out.

Remember that clearing the Last change date field in the Person document is not sufficient to unlock a user ID and allow them to log back onto the server. The correct way to unlock a user's account is to manually clear the Password digest field in the Person document. There is no facility to clear the digest using Adminp (other than by disabling password checking in the ID completely by choosing Action - Set Password Fields and selecting Don't check passwords), so in this case, it is acceptable to edit the Person document directly.

Since client-side warnings occur before the user accesses the server, disabling password checking in the Server document will not suppress these warnings. It will, however, allow the user ID to continue to gain access to the server even if the password has expired. To prevent the warning messages, the user should continue to change passwords according to the Last Change Date, Grace Period, and Expiration Date values stored in the ID.

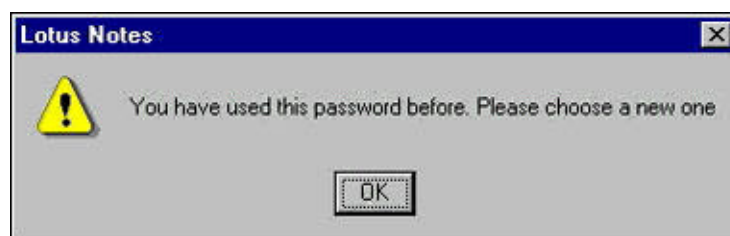
Turning off password checking for a user

The administrator can, of course, switch off password checking at any time for a user (even if the password has expired). Follow the directions in the [Enabling password checking for users](#) section above, only select Don't

check password, which submits the appropriate Adminp request. However, if the ID's password has already expired, the user will need to change their password to reset the password structure inside the ID file. From then on, no client-side password checks are carried out until the ID is re-enabled for password checking.

Reusing passwords

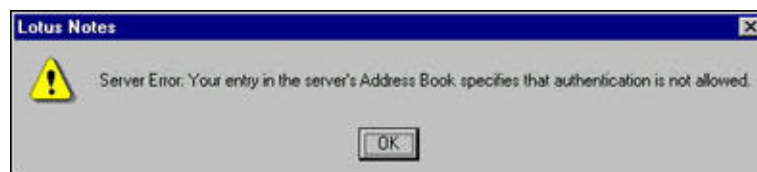
Be aware that the ID file "remembers" up to 49 old passwords. If a user tries to use one of the 49 (case-sensitive) passwords stored in the ID, they will receive a message asking them to choose a different password.



Locking out a specific user

Should you need to lock a specific user out of the server, you can submit an Adminp request to do so. Follow the directions in the [Enabling password checking for users](#) section above, only select Lockout ID for the Password field in the dialog box.

When Adminp processes the request, the Person document is modified so that the Check password field is set to Lockout ID. When the user tries to access this server again, they will receive a message indicating that they are not allowed to authenticate.



Using multiple servers

Throughout this article, we have focused on a single server installation. With a multiple server installation, there are additional points to remember. Because all the changes are made in the administration server's Domino Directory (names.nsf), Domino relies on replication to ensure that other servers receive the updates. Modifying a Person document (for example, clearing the Password digest field) to reset a user account on one server will give the user back their access to all the other servers that have password checking enabled, but only after the Domino Directory has replicated the changes.

Testing before rollout

During pre-rollout testing, customers may experience different behavior than this article describes. Frequently problems occur when Adminp requests do not get processed before all test results are recorded. Before each step, you should confirm that the pending Adminp requests for the user are being processed. For example, if a user changes their password twice, then both Adminp password change requests should be processed before recording the final result. If only the first change request is processed, the password digest information will be out of sync until the second change request updates the Person document. (This can also occur in production servers.)

For these reasons, it's not recommended to test password checking with

grace periods and change intervals of only one or two days.

If you have customized Adminp

Some customers have replaced the Adminp task with their own custom Adminp tool. This article highlights the work carried out by the Adminp task to ensure password checking works. Customized versions of Adminp could generate nonstandard behavior, which might result in breaking the synchronization of the user ID and the Person document.

ABOUT THE AUTHOR

Mark Cornaia has been working at Lotus since 1997. Mark is a member of the World Wide Support Engineering Team, which focuses on resolving high-severity, high-impact customer issues. Based in England, his on-site support destinations have been as close as London and as far away as New Zealand. Prior to joining Lotus, Mark had a career in the Ministry of Defense as Radio and Radar crew chief on the RAF C-130 "Cloud Busters" Metrological Research Hercules aircraft. When he's not working or traveling, you'll find him at auctions buying Disney collectable art, maintaining his house, or watching the Simpsons.

