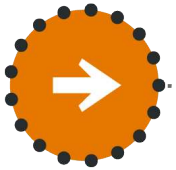
Universal Password Management

Baber Amin
Product Manager
Novell, Inc.
baber@novell.com

Hal Henderson
NMAS Architect
Novell, Inc.
hal@novell.com

Novell®

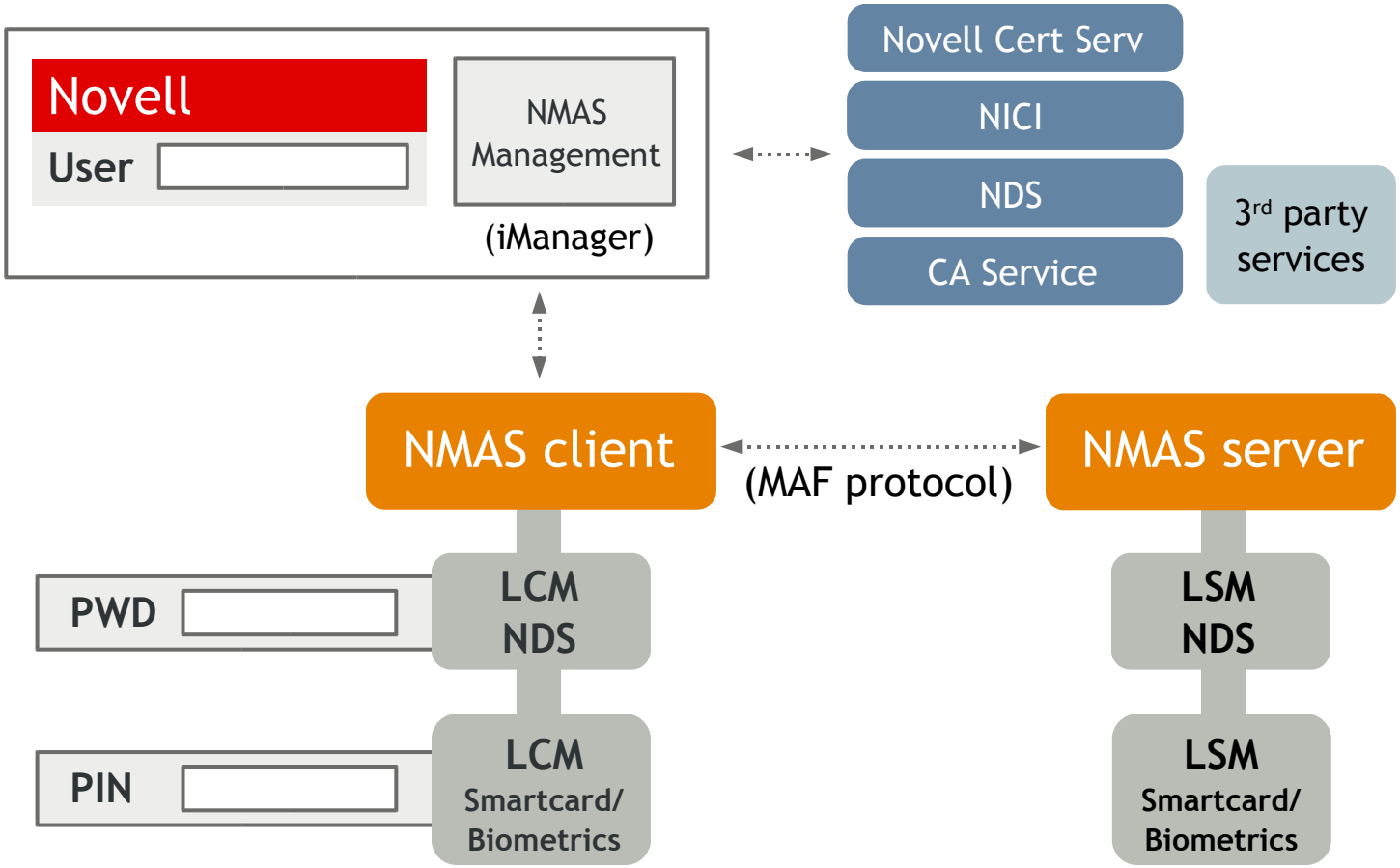
Outline



- Password History
- What is the Universal Password?
- Universal Password Deployment
- Password Synchronization Rules
- Which Password to Use When?
- Frequently Asked Questions
- Q & A

Novell.

Novell Modular Authentication Service (NMAS)



Novell.

Password history

Novell.

Password History
Novell Directory Services® Password

Public and Private keys (RSA) are created and stored on the user object. Can be lengthy to generate key pairs.

Non-reversible--only the "hash" of the password is stored. The customer cannot retrieve the password from eDirectory™.

Used by the Novell Client™, LDAP, and by applications written to the Novell Client APIs

The password is never sent on the wire

Policy can be applied

- Password expiration
- Password minimum length
- Password uniqueness
- Intruder lock
- Time of day restrictions

Novell.

Password History
Simple Password

Originally provided to allow migration from foreign systems, such as iPlanet LDAP directory

- Typically a MD5 or SHA-1 password hash is imported
- However, it can be a clear text password

Password values are stored encrypted with DES or 3DES, based on setup of the tree key

Lower security than NDS Password, since the password is sent across the wire and is stored such that the password can be extracted.

Restrictions

- Does not support extended characters
- No password policy enforced

Novell.

Password History
Enhanced Password

Deprecated in favour of Universal Password

Enhanced Password offers some policy

- Min/Max length
- Repeatable/Consecutive characters

Password Synchronization is one way (flows out from enhanced password to UP and NDS passwords)

Enhanced Password design was not consistent with Simple or UP, and thus offered different security characteristics

Novell.

Universal Password Benefits

- One password for all access to eDirectory
- Enables the use of extended characters in passwords
- Synchronization of passwords from eDirectory to other systems
- Enables advanced password policies

Novell.

Password Management
Password Policies via Universal Password

Available Policies include:

- Min/Max characters
- Repeatable/Consecutive characters
- Exclude list
- Expiration settings
- Numeric/Special characters (!@#$%^`&*())
- Require unique passwords
- Forgotten Passwords

Password Policy Documentation:

www.novell.com/documentation/dirxml20/index.html?page=/documentation/dirxml20/admin/data/ampxjj0.html

Novell.

Universal Password prerequisites

NMAS 2.3 or later must be running on at least one server holding a Read/Write replica of the user object

- For best performance, it is recommended that NMAS 2.3 or later is installed on all servers in the replica ring
- The latest NMAS Server version (currently 2.3.6) is recommended

NICI 2.6 or later must be running on the server where NMAS is running

- The latest NICI version (currently 2.6.5) is recommended

eDirectory 8.7.3 or later must be running on the server where NMAS is running

Novell.

Universal Password prerequisites (cont.)

Replicas of the partition containing the Security Container must be synchronized

eDirectory must be synchronized

The Security Domain Key (a.k.a. Tree key) must be synchronized on all NMAS servers

- It is recommended that the Tree Key is a 3DES keys

`Deployment guide:
http://www.novell.com/documentation/lg/nw65/universal_password/data/front.html

Novell.

Client side considerations

Installs by default on client workstation with 4.9 and later clients

Enables NMAS authentication on workstation

- Allows additional means of authenticating to the network
  - Universal password
  - Biometric devices
  - Smart cards
  - Tokens
  - Proximity cards
  - Etc

Novell.

Universal Password requirements

Universal Password is designed to provide backward compatibility to existing services

Password changes may be configured to automatically synchronize to Simple and NDS passwords

Use of extended characters in Universal Password could break Application compatibility of Simple and NDS password (after synchronization)

- To support compatibility with the use of NDS and Simple passwords, users might have to change their passwords to not include extended characters

Novell.

Universal Password requirements
NetWare 6.5

NetWare® 6.0 and 5.1 servers running CIFS or AFP will continue to have proper operation of passwords

For ease of deployment, on a NetWare 6.5 server UP is turned off by default

Client32 shipping with NetWare 6.5 supports UP

- users will continue to use the NDS password until the administrator is ready to enable UP

iManager plugin is used to associated password policies at the user, the container, the partition, or the tree level

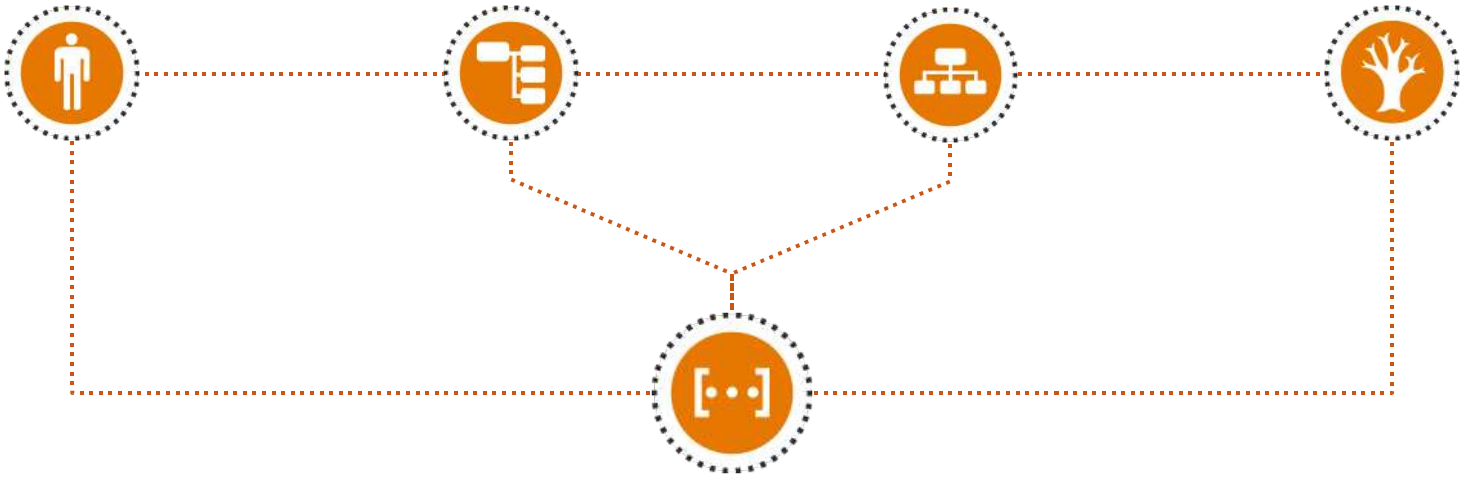
- Sub-containers are not automatically UP enabled
  - The user object, then the direct parent container, followed by the partition root, and ultimately the top of the tree are checked for Password Policy assignment.
  - This discovery scheme does not walk the entire tree. It was chosen for performance reasons.

Novell.

Enabling Universal Password

Enabled for a user, a parent container, a partition root, or tree wide.

- The user object, the direct parent container, the partition root, and the tree (Login Policy object) are checked for a Password Policy assignment.



Novell.

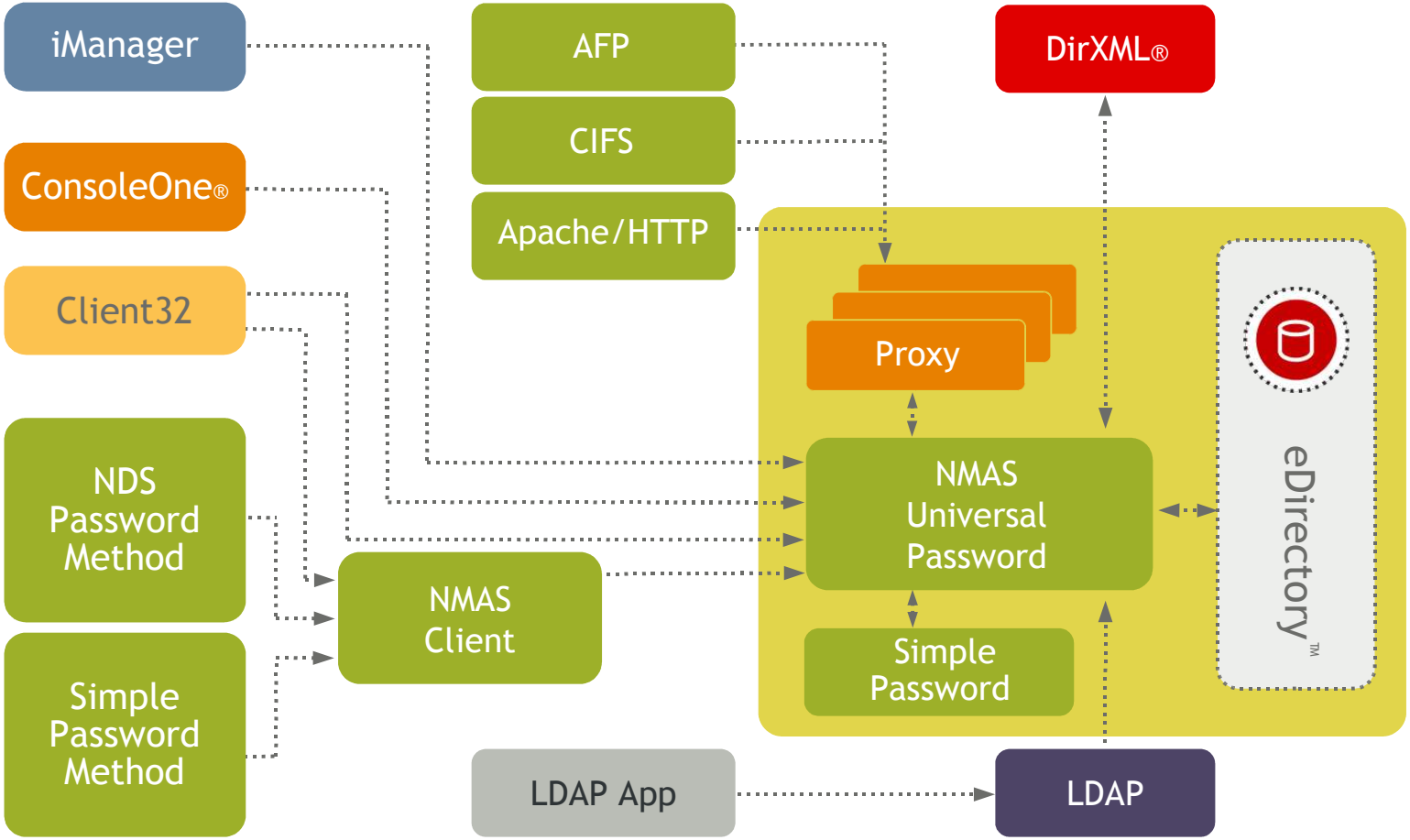
Universal Password usage

Universal Password is authoritative if enabled

- Novell Client™ 4.9 and later authenticates the user using Universal Password
- The Novell client APIs have been modified such that developers can login/set Universal Password through a new set of APIs (available now on the NDK)
- For eDirectory 8.8 LDAP has been modified to authenticate the user using Universal Password

Novell.

Password manager



Novell.

General password synchronization rules

After the Universal Password is enabled, the first password used to authenticate is used to set the other two passwords to match.

- Password synchronization is initiated from the client (if using Novell Client 4.9 or above) if the user logged in with:
  - NDS Password
  - Simple Password (stored as hash)
- Password synchronization is initiated from the server if the user logged in with:
  - Simple Password (stored as clear text)

Novell.

Exceptions

If the Universal Password is enabled but not set

- The NDS password will be used to login, and the Universal Password will be set to the value of the NDS password
- The Simple Password will be set to the value of the Universal Password

If an old Novell Client32™ is used to set the NDS password, next user login with the new Novell Client32 will

- Check timestamp of NDS and Universal Passwords
- Use the password with the latest timestamp to login
- Set the other passwords to match the one used to login

Novell.

Password synchronization rules (cont.)

Example

- Universal Password is enabled but not set
- ICE is used to set the password through an LDIF import
- The ICE –l switch is not used (-l will populate only the Simple Password when the Universal Password is not enabled)

Result

- All three passwords are set during the bulk load operation

Note: For fastest bulk load performance, use iManager to turn off Universal Password before the bulk import. Let NMAS populate the remaining unset passwords at user login time.

Novell.

Password synchronization rules (cont.)

Example

- A user has a NDS password but not a Simple password
- User wants to use CIFS

Result

- They can not login using CIFS until a Universal Password or a Simple Password is set.
- When Universal Password is enabled, and the user authenticates using the Novell Client 4.9, the NDS password is migrated to the Universal Password and the Simple Password. The user can then log in using the Universal Password (which is the same value as the NDS password) using CIFS.
- The CIFS user now has the benefits of Password Policy enforcement

Password synchronization rules (cont.)

Example

- Universal Password is enabled
  - An administrator disables a users NDS password through iManager or other administrative tools,
    - achieved by setting the NDS password to an arbitrary value that is unknown to the user

Result

The Universal Password is set with this same arbitrary value, causing the NDS Password method and the Simple Password method to be disabled.

Does my LDAP application need to change?

No changes necessary

- The LDAP Server on eDirectory 8.7.3 and later has been updated to change Universal Password. The LDAP Server on eDirectory 8.8 has been changed to use Universal Password for bind requests.
- Make sure that your application conforms to the LDAP standard, in that passwords and all data are sent in UTF8 or in the API specified format.
- In an attempt to solve this industry-wide problem, the following language is being added to the next revision of LDAPv3:
  - It is RECOMMENDED that applications prepare textual strings used as password to improve matching. Applications which prepare textural strings used as password are REQUIRED to prepare them as follows:
    - Transcode to Unicode,
    - Apply SASLprep, and
    - Encode as UTF-8.
- SASLprep (Stringprep profile for user names and passwords) is found at http://www.ietf.org/internet-drafts/draft-ietf-sasl-saslprep-02.txt

Novell.

Does my NDAP application need to change?

NWDS APIs

- NWDS API based applications should use the new APIs which specify the password format
  - NWDSLoginEx
  - NWDSChangePwdEx
  - NWDSGenerateKeyPairEx
  - NWDSVerifyPwdEx

These new APIs will be invoked by the utilities supporting extended password changes (iManager, ConsoleOne, Novell Client), when selected to support Extended character support.

New libraries with the APIs have been available since July 2003

Novell.

Which password to use when?

NDS Password

- Compatibility with existing applications
- Non-extractable password
- Password never sent on wire when used with client32

Simple Password

- Preserves passwords from foreign system import
- Preserves format of import (hash or clear text)

Universal Password

- One password for all access to eDirectory
- Enables the use of extended characters in passwords
- Enables advanced password policies
- Synchronization of password from eDirectory to other systems

Novell.

Frequently asked questions

What procedures can be used to troubleshoot NMAS?

- NMAS Server trace messages are output to DSTrace when the NMAS filter is enabled. More information available in TID 10092261.

What happens when the password history limit is reached?

- When the password history limit is reached the user is no longer able to change his/her password until one or more of the passwords expire from the password history.
- This prevents the user from changing passwords enough times for the old password to be removed from the password history and allow the old password from being used again.

Novell.

Frequently asked questions

Does the Universal Password get set to expired when an administrator sets it?

- Yes, if password policy specifies a password expiration interval.
- No, if the password policy does not specify a password expiration interval.
- This is the same as the NDS Password.

When and how is the password expiration calculated?

- Password expiration time is calculated by adding the password expiration interval to the time that the password changed.
- Password expiration time is calculated when the password is set.
- Password expiration time is recalculated during login if the password interval has been changed to a short amount of time.

Novell.

Frequently asked questions

Is it possible to determine if Universal Password, the NDS Password and the Simple Password are in synch?

- A utility called diagpwd is available that can be used to determine the synchronization status of the passwords and the password policy that is effective for one or more users. More information available in TID 2970885.
- The source code for diagpwd is available for download from the Novell source forge at:
- forge.novell.com/modules/xfmod/cvs/cvsbrowse.php/nmas_ldapext/client/diagpwd

Novell.

Frequently asked questions

What is the maximum size for a Universal password?

- The maximum number of characters allowed for a Universal Password is 512
- LDAP standard limits password length to 128 bytes

What rights are needed to install NMAS and the NMAS methods?

- Administrative rights are needed to extend schema and install client methods

Novell.

Frequently asked questions

What if Universal Password is turned off after being enabled for some time?

- Users will return to authenticating using the NDS Password, or the Simple Password.
- Passwords will not be synchronized when passwords are changed.

Why can't the Simple Password be set when the Universal Password is enabled?

- Setting the Simple Password is disallowed to prevent the Simple Password and the Universal Password from having different values.

Novell.

Frequently asked questions

Can you choose on a per user basis which passwords will be synchronized with Universal Password?

- The password policy that is effective for the user specifies if the NDS Password Hash and/or the Simple Password are set when the Universal Password set.
- Universal Password does not provide the capability to set other password (such as the Kerberos password) when the Universal Password is set.

Novell.

Frequently asked questions

How can the Tree Key be changed from a DES key to a 3DES key?

- Use SDIDiag to perform the following operations:
- Use the "SD – R" command to revoke all Tree Keys and generate a single 3DES key.
- Use the "RD -T" command to resynchronize the new Tree Key to all the servers in the tree:
- If an eDirectory server does not get the key after the previous step, restart the server to force the server to retrieve the new Tree Key.
- TID 10088626 describes how to use SDIDiag to verify that the Tree Key has been synchronized to all server.
- TID10086669 describes the SDIDiag commands

Novell.

Question & Answer

Novell®

Novell