IDENTITYAUTOMATION

Definitive Guide to Account Username Conventions

Troy Moreland
Co-Founder & CTO
Identity Automation

Contents

Foreword

WHO IS THIS GUIDE FOR?

This guide was written for identity and access management (IAM) champions and identity management project leads in order to provide you with a sound methodology for developing an enterprise-wide username convention for your organization as part of a new IAM deployment, replacement solution, or system modernization. If your organization has more than one set of credentials for your different systems and applications, this guide will help you consolidate them into a single enterprise-wide username convention.

As your organization's IAM champion, you will need to engage with key players across your organization, including department and business owners who manage data sources and application targets of the IAM system, decision-makers within senior management and at the C-level, and the end-users who provide usability validations. This guide highlights the stakeholder groups involved in each step of the process to ensure you engage with the right people, at the right time.

The methodology presented in this guide is not absolute. You will need to adapt the steps in this guide to fit your organization's particular needs and situation. And while there is no way to fully future-proof a username convention, following the steps in this guide will help set your organization up for success.

About the Author

Troy Moreland

Co-Founder & CTO, Identity Automation

Troy Moreland is an expert technologist in the field of identity and access management. He has more than 20 years of relevant experience, including his leading efforts to select, design, and deploy one of the first commercially successful identity management implementations in the United States. Since Identity Automation's founding, Troy has architected, designed, and implemented identity management solutions for hundreds of organizations including Adobe, CarQuest, Hunter Douglas, eBay, TDBank, Health Canada, Lowe's, Overstock.com, MD Anderson Cancer Center, Kansas University, State of Texas, State of North Carolina and many more.

Overview

During the initial implementation of any Identity and Access Management (IAM) system, the solution provider must coordinate with the customer organization on a variety of settings in order to configure the new or replacement IAM system, such as password policies, challenge questions, authoritative data source systems, audit retention policies, and many others. The goal is to align the IAM configurations and policies with an organization's current governance operating model (e.g. business rules, processes, and security requirements). One of the most important, but also the most challenging configuration options, is defining the company's username convention.

This guide provides the individual driving the project with a detailed approach to creating an effective username convention that serves both current and future needs. By following this approach, you can significantly reduce the time required to define and standardize their username convention. **To further aid in the process, a tear out sheet is included at the end of the guide as a quick reference to the methodology steps.**

Background

The authentication process in most IAM systems comprises two basic elements: identification and verification. Organizations typically deploy a username (e.g. jdoe, jdoe@company.com, jane.doe) as the data value used in the identification step and a password for the verification step.

While it's worth mentioning that there are other authentication credential types (QR Code, Smart Card, Fingerprint Biometrics, etc.), username and password remain the most common, and this guide focuses on the traditional username format for the identification step.

Changing an account username not only affects every user, but the username must be changed in every aspect of the core IAM system and all connected applications.

WHY ACCOUNT USERNAME CONVENTION MATTERS

Before jumping into the details of the account username convention development methodology, it is important to understand why this configuration is so crucial. The main reason being that providing users with single sign-on (SSO) is a critical requirement of the majority of identity management initiatives. To facilitate this, an identity management project lead needs to establish a single identity for each user, with a single username and password, that enables access to all application resources.

The benefits of SSO are well-documented and include enabling easy access to applications, reducing support calls, and decreasing overall security risks. To meet these goals, organizations need an account username convention that will be appropriate for every connected system and user in the organization's digital ecosystem for many years to come. This requires not only considering usernames for employees, but also for the entire universe of contingent users, such as partners, vendors, contractors, and other external audiences.

CHALLENGES

Developing an account username convention for all current and future users of an IAM Service is no small task given that there will never be a single convention that completely satisfies all users. Each user has opinions about what they think a username should or should not be. Furthermore, systems and applications often use different, pre-defined username conventions, such as first initial + last name, firstname.lastname, or email address.

When a single convention is selected for an all-inclusive organizational standard, there is often a “lowest common denominator” or a system that can only support one convention and nothing else. This is called a constraint, and it will be at the center of the methodology described later.

Keep in mind, changing a username is much more involved than changing another attribute, such as job title. Almost everything in the IAM system is connected to or dependent on the username. So, changing a username not only affects every user, but the username must be changed in the core IAM system and all connected applications.

Guiding Principles

When planning a new convention for user accounts, an organization or identity management project lead should take into account four critical drivers:

- Usability
- Security
- Administration
- Audit

While the goal is to develop a convention that balances the four drivers, it is recommended that organizations prioritize them first. Drivers with a lower priority are areas with the most flexibility, which is valuable when making the final username recommendation. Priority also helps prevent any one person or group from influencing the selection process based on their needs alone.

While the goal is to develop a convention that balances the four drivers, it is recommended that organizations prioritize them first for more effective trade-offs.

Note that in some organizations, the technology department sets the priorities, whereas in others, priorities are set by the business or by external factors, such as compliance regulations. Gartner[1] describes other potential considerations in the formation of a username, such as uniqueness, persistency, neutrality, universality, and memorability. Our four drivers, which encompass these key points, are described below.

USABILITY

Usability is a top concern for end users and helps drive adoption of a new username convention, as well as the IAM solution as a whole. The username is one of the very first interactions a user will have with the new system. Organizations **most concerned with keeping users happy** will set usability as the top priority. Name-based conventions, such as "jdoe" or "johndoe," are the most typical account naming conventions in this scenario.

SECURITY

The primary security concern with usernames is unauthorized access, more specifically, the ability of an intruder to guess the username and therefore, know half of the authentication credential. The typical account naming convention in a security prioritized scenario is a **system generated account name that is not directly linked to identity data** in any way. For example, using 4 letters + 4 numbers (e.g. qlvz4426) or combining words from a range of different categories (e.g. biscuitcrispy). Online tools, such as JIMPX, can be used as a

resource for ideas. A randomized account username convention also deals with security concerns around personally identifiable information (PII), since the username values cannot visibly be linked back to a person.

ADMINISTRATION

Username convention plays an important role in the management and support of an IAM solution. **Help desk users must be able to quickly and easily find the user accounts** on which they need to perform a task. Searching by name alone usually returns multiple users with the same first and/or last name. Username is typically used as the key search value, so being able to identify a user based on username is the preferred scenario when administration is prioritized. A typical account naming convention in this scenario is one similiar to Usability and is based on full name, such as "Public, John Q." (e.g. jqpublic) or "Jane Doe" (e.g. jdoe). In the event of a collision, a numerical value is typically appended to the username (e.g. jdoe2).

AUDIT

Organizations need the ability to run reports that show the access history of specific users—who did what and when. This **requires a naming convention where the username does not change** (such as a primary key in a database), since access logs normally only store usernames and not a GUID. A unique identifier from an authoritative data source, such as employee ID for staff or contractor ID for external workers, would be the typical username convention in this prioritized scenario. These are typically numerical identifiers, like 234567890 or 3456543456. However, if the employee or contractor ID is a SSN or Tax ID, an alternative unique identifier is typically used. Although IAM systems support renames and tracking historical accounts, most third-party systems lack this ability. As such, access logs cannot be guaranteed to resolve to the appropriate end user.

These guiding principles are the core of the methodology outlined below and have been the cornerstone of the hundreds of IAM implementations Identity Automation has performed. While there can be exceptions that prohibit utilizing this approach, this guide provides a valuable perspective for any implementation. Additionally, these points are provided under the current environments and market offerings, but future technologies could warrant updates, changes, or additions.

These guiding principles have been the cornerstone of the hundreds of IAM implementations Identity Automation has performed.

Methodology

Organizations typically begin the process of trying to decide what a good username will be by asking what people like or prefer. One person might like email address, another may prefer "firstname.lastname," and a third may prefer it to be the same as his or her employee ID. Essentially, everyone has a personal preference and makes a suggestion based on what he or she finds important.

There are multiple flaws with this approach. It may seem like complying with this would be part of the original drivers—usability. However, while that may be true, you are only going to satisfy a subset of people whose preference aligns with the convention.

Recommended methodology steps:

Step 1: Document Known Constraints - What can the username NOT be and why?

Step 2: Develop and Evaluate Possible Username Algorithms - Document possible conventions with pros, cons, and risks. Exclude known constraints.

Step 3: Review, Recommend, and Next Steps - Give a summary of the analysis with a recommendation for the username convention that best balances the drivers and carries the least risk. Once approved, configure the IAM system with the "policy" and train end-users.

Each of the steps are documented in detail below with general descriptions, context, and specific examples.

STEP 1: DOCUMENT KNOWN CONSTRAINTS

Instead of polling everyone in the organization for their preferences, you, as the project lead should start the process by documenting what conventions won't work. That means documenting any specific characters, formats, parameters, or styles that would create conflicts with current users, applications, systems, business processes, and/or regulatory requirements.

For example, some applications will not accept an email address (e.g. jdoe@company.com) as the username due to the "@" character. Thus, a known technical constraint would then

be that the username convention cannot be an email address due to this application restriction.

Is it important to note that a constraint does not always have to be technical. An organization may have a compliance rule that prohibits username from being name based (e.g. sammie.carter) due to the PII included in that convention.

To gather this specific information, the IAM Project Lead needs to engage with other department technical and business owners, especially those who manage source and target systems that will be integrated with the IAM system. Not only is it important to vet potential constraints with these stakeholders, but such inclusion often brings much needed cooperation from these parties in the future.

Recording known constraints eliminates options that cannot be used or that would create a conflict with a business owner. Some constraints can be removed, but not without impacting integrated services or applications. For example, if the only technical constraint for not using the convention of "firstname.lastname" is that a single application cannot support a username with a "." in it, an organization may choose to postpone the application integration and move forward with the convention.

Below is a list of potential constraints derived from best practice guides[2,3] for selecting username conventions, as well as known technical requirements of current and future target services. This list also demonstrates how to capture and document constraints.

Must work with all current and future target systems to the extent possible.

Username constraints must comply with the most restrictive username policies across all known current systems, as well as any under consideration.

Example: *System 1 has a constraint of a maximum 255 characters for the username, System 2 has a constraint of a maximum 10 characters for the username, System 3 has a constraint of a maximum of 12 characters for the username. Selected username criteria cannot contain more than a maximum of 10 characters to ensure compatibility with System 2.*

Must work for users with multiple affiliations.

Usernames must not contain references to a particular type of user, as there is a possibility of users that are some combination of affiliations.

Example: *An employee of the enterprise is also a customer AND a member of the board.*

Must work for users that move between departments and/or locations.

Usernames must stay static, while the account retains the ability to transition with the user across departments and/or locations.

Example: *Any employee in the Houston, Texas office who moves to the Raleigh, North Carolina office should not have to change his or her username due to a location change.*

Recording known constraints eliminates options that cannot be used or that would create a conflict with a business owner.

Must work for users associated with multiple departments and/or locations.

Usernames must not contain references to a particular department or location, as it is possible to be an member of multiple departments and/or locations.

Example: *An IT manager of one department may be asked to temporarily manage a second department. On record, the manager will be working for both department 300 and 250, but should still only have one username provisioned for all of his or her accounts.*

Must be no longer than X characters.

Long user IDs are not only difficult to remember, but may also be incompatible with current or future systems. Any convention selection needs to align with the most restrictive username length of a target system.

Example: *Many older, legacy systems limit the username convention to 8, 12, or 20 characters.*

Must only contain alphanumeric characters.

Many target systems do not allow or only allow a select few non-alphanumeric characters within the username. Username constraints must adhere to the most restrictive policy in current and known future systems.

Example: *Google Apps does not allow spaces in the username and does not differentiate between the same username with a period and one without (i.e. "j.smith" is evaluated as "jsmith" within the system).*

Must not be a value used to access other systems without a password.

A username must not be used as a single authentication piece for any other system, as usernames are visible to a wide audience. This means the username cannot be considered a confidential value or PII.

Example: *If an Employee ID was used as a username and the corporate cafeteria also used the employee ID as a lunch PIN, then any employee would be able charge the lunch account for another employee just by knowing the other employee's username.*

Should provide at least X number of unique combinations.

Username constraints should provide enough combinations for X number of active users and accommodate the expected influx of new employees, contractors, and customers without being reused. Additionally, username constraints should not only provide enough combinations for the projected user population, but also enough to significantly decrease the probability of a brute force attack against organizational resources.

Example: *Sample use case of 4 billion unique combinations and a current population of 10 million. Using a password strength constraint of a minimum of 8 characters with a minimum of 1 lowercase letter, 1 uppercase letter, and 1 number, there are a possible*

221,919,451,578,090 combinations of passwords for each account. While the number appears impressive, it is still within the realm of cracking for a dedicated individual. The risk can be further mitigated by having a very large namespace of possible usernames. Even if an attacker knows the username naming scheme, 4 billion unique combinations with 2.7 million active accounts makes the odds approximately 1 in 1,480 that an attacker will stumble on an active account on which to attempt the more than 221 trillion password combinations.

Must mitigate risk of vulgarity and other offensive values.

Username naming scheme should minimize or remove the possibility of creating offensive usernames, whether the scheme uses random letters, concatenations of user values, or any other method.

Example: *Usernames should not contain curse words, religious figures, political figures, or politically charged words or statements.*

Must begin with an alpha character (a-z).

Username naming scheme must comply with the most restrictive username policies across all current and known future target systems.

Example: *Some Linux / UNIX system usernames must start with an alpha character. This enables local provisioning of specific departmental business systems with the same username.*

Must be lowercase alpha characters.

Username naming scheme must comply with the most restrictive username policies across all current and known future target systems.

Example: *Some UNIX based systems are case-sensitive, even when using Kerberos authentication against case-insensitive systems.*

Must never be reused by another person.

Auditing requirements for this project demand that audit logs be retained indefinitely and audit actions remain tied to the person to whom they apply. Therefore, a given username should never be used by more than one person.

Example: *Account jsmith is assigned to John Smith. Even after John Smith is no longer within the source data for this project, the account jsmith must never be re-assigned to another user.*

Should never change.

Auditing requirements for this project demand that audit logs be retained indefinitely and audit actions remain tied to the person to whom they apply, regardless of name change, position change, department change, or location change.

Username naming scheme must comply with the most restrictive username policies across all current and known future target systems.

Example: *An employee who worked in the Houston office then moves to the Raleigh office and switches departments should not have his or her username changed because of the different location or department. This list is a representative example of potential constraints an organization may need to consider. However, the rules do change based on an organization's size. A username convention for 50 users is very different that for 500,000 users. The rules shift again when you get to the millions of users. For example, a username convention consisting of 4 letters + 4 numbers (e.g. qlvz4426) would be safe with 50 users, but with millions of users, would generate bad words due to the larger namespace required. As analysis is performed, it is important that any currently known conventions are reused throughout the organization whenever possible. It is also important to show how the current convention or conventions in place are able or unable to meet the necessary requirements. The ability to keep the same convention is very beneficial as long as it works.*

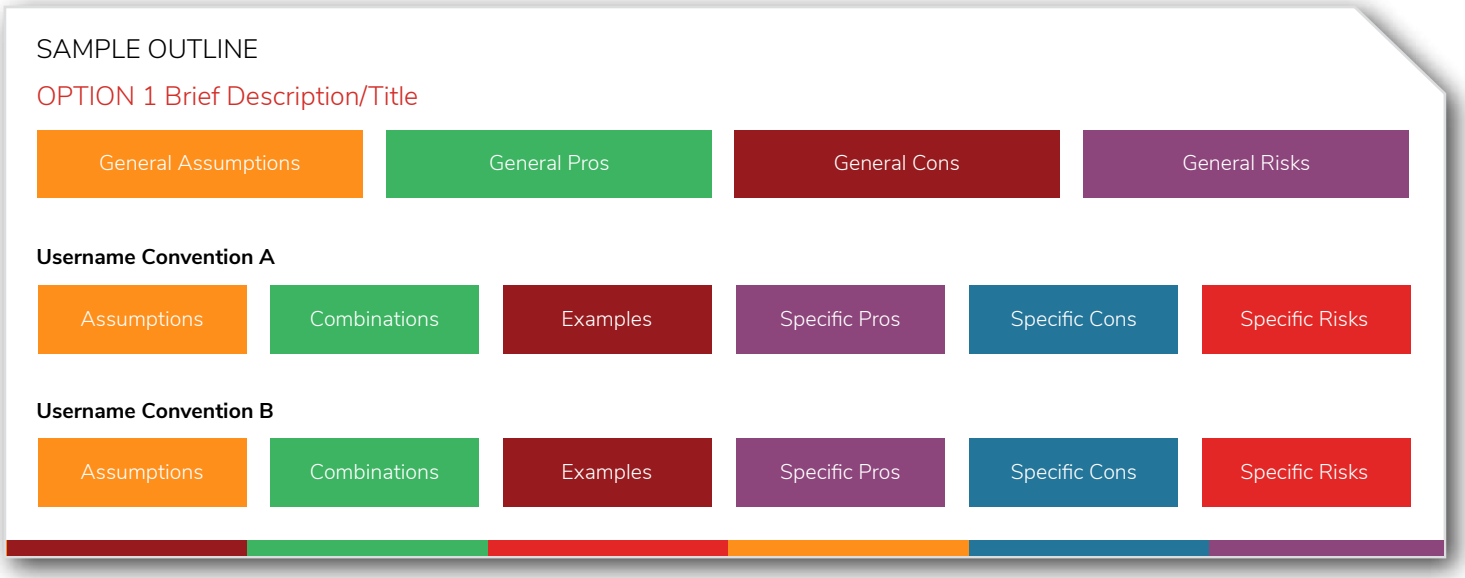
STEP 2: DEVELOP AND EVALUATE POSSIBLE USERNAME ALGORITHMS.

Once all known constraints have been gathered, vetted, and documented, an algorithm (or convention) will need to be developed from the options left after excluding the constraints.

This step can be frustrating if the list of constraints is long, leaving only a short list of viable options. In these instances, the remaining potential username options may have such a negative impact that the constraints must be reconsidered.

For example, the technical restraints of one target system can prevent a great username convention from being created. If this is the case, it may be worth it to exclude this one system and then flag it as an exception.

Below is a sample outline for generating the usernames after considering all the appropriate constraints. This outline would be repeated for all username options.



Example Analysis

Using this outline format, here is a theoretical example analysis for a large enterprise organization that has geographically distributed divisions. The options and conventions described are the documented viable options after excluding conventions with known constraints.

OPTION 1: A single username for all user affiliations in the enterprise (employees, contractors, vendors, partners, and customers)

GENERAL PROS	GENERAL CONS	GENERAL RISKS
• A single username across all user affiliations is a viable option that will be successful across a large scale of applications and users. • This option aligns with the goal of the IAM Service to provide every stakeholder in the organization with a single username and password that will enable access to their business resources. • The IAM Service is self-sustained for username generation, management, and support, with minimum dependencies on external groups/processes. • There will be a better user experience because IAM support structures will be more able to solve issues internally. • This is the only option that meets ALL initial known constraints and exclusions.	• Due to the extensive list of constraints and pure scale of the IAM Service, each of the conventions results in a new username that is not easy to remember or particularly user-friendly.	• There is an unknown set of applications that potentially has issues integrating with IAM because of the multiple affiliation functions. If downstream applications cannot support this function, the integration may not be successful. • Mitigation Strategy: Document this risk and explore the potential issue for each target application during the application planning stage. • A new username convention may result in slow adoption by some departments who currently have a wide-scale convention with which users are already comfortable. • Mitigation Strategy: Provide documentation and justification as to why the username was selected. Understanding how and why the team came to the recommendation can alleviate some pushback. As the new IAM username convention becomes more widespread, other currently used identities can be deprecated to ease the burden on users who have multiple accounts.

Username Convention A: 10 numeric only digits

ASSUMPTIONS	COMBINATIONS	EXAMPLES	SPECIFIC PROS	SPECIFIC CONS	SPECIFIC RISKS
• Removed constraint for "Must begin with alpha character"	[(1^1) * (10^10)] = 10,000,000,000 (10 billion)	• 7443752535 • 4620524743 • 9266179329 • 0195031342 • 3318422617	• Meets most currently known technical criteria and constraints. • Provides enough combinations for all enterprise users for 10+ years given current growth and churn rates.	• A new 10 digit number is not easy to remember. • New number not associated with anything currently used or known. • Potentialcollisions with current employee IDs because they are 10 digits as well.	• Will impact the downstream Unix/Linux system because usernames that begin with numbers are not supported.

Username Convention B: Arbitrary User ID - Random 8 alphanumeric characters with pattern

PATTERN	COMBINATIONS	EXAMPLES	SPECIFIC PROS	SPECIFIC CONS
• Pattern: 4 random letters + 4 random numbers • Excluding vowels (a,e,i,o,u) (26^4)>(21^4) combinations • Excluding potential bad words/numbers [~1000 bad words * combinations] = 10,000,000 exclusions	[(21^4) * (10^4) - 10,000,000] = 1,934,810,000 (~1.9 billion)	• xtwd9417 • rrqx3782 • lcqh9170 • cbdz2371 • kszx7505	• The structure pattern (4 letters + 4 numbers) makes memorization easier because of the concept of chunking. • Meets all currently known technical criteria and constraints. • Provides enough combinations for all users for 10+ years given current growth and churn rates.	• New username will be a change that users may not potentially like. • Easy to type incorrectly because of misheard characters, resulting in operational and security impacts (e.g. the wrong user's password could be reset or the wrong user be given certain entitlements). • A randomly generated string of 4 letters could deploy a potential word that is considered "bad" and must be regenerated for that user. A support process needs to be established to account for bad username allocations and provisioning. • Each "bad" word or number removed will actually remove a total of 10,000 possible combinations, thus eroding the total namespace. • Cannot identify the type of user based on username (good for security, difficult for administration).

STEP 3: REVIEW, RECOMMEND, AND NEXT STEPS.

Once constraints have been documented and the necessary analysis to develop potential options has been performed, it is time to circle back with stakeholders to continue the discussion. It is also recommended that a review be done with a group of soon-to-be impacted end-users.

The review step does three critical things:

1. Validates that the information collected, the analysis process, and documented results are complete and accurate.
2. Promotes inclusion of team members and stakeholders within the organization. Instead of telling them what something will be, they are included in the process and asked for input. This helps people understand how a conclusion/recommendation was reached and garners support for the decisions that are made.
3. Makes the sell easier for technical and business leaders when changes start coming. In addition, the process makes it easier for leadership to defend the username change should any concerns be voiced moving forward.

After the final review and input has been received, the IAM implementation team can develop the final options and a recommendation for a username convention for the IAM Service. The IAM Champion and project team then presents the recommendation to the appropriate decision-makers, typically senior IT leadership or even CIO/CISO level, within the organization.

The recommendation should provide a simple summary overview of the thought process, guiding principles, and recommended username convention. It should show each option and format, including pros, cons, and risks. The goal of the recommended option is to minimize the challenges/risks and maximize benefits for the whole organization, while balancing the four drivers: usability, security, administration, and audit.

Because there is no perfect answer, it is important to take extra time on this step to ensure the best possible recommendation is made. Undoubtedly, there are pros, cons, and risks associated with any recommendation. The key point is that the team should feel the risks associated with the recommended option are manageable and that the pros significantly outweigh the cons. While the increased usability factors obtained with certain options may be appealing, consider potentially significant increased support risks as well.

The following is an example memo and that can be attached to the detailed analysis document for supporting information as needed.

The goal of the recommended option is to minimize the challenges/risks and maximize benefits for the whole organization, while balancing the four drivers: usability, security, administration, and audit.

EXAMPLE MEMO:

IAM Account Username Convention Selection Methodology

Subject: IAM Service Account Username Convention Recommendation

---

Hello IAM Decision Makers,

After much research and discussion with the IAM team and key stakeholders throughout the organization, we have reached a consensus on a recommendation for the IAM Service Account Username Convention. The team recommends Option 1, Convention B: A single username for all user affiliations in the enterprise (employees, contractors, vendors, partners, customers with the format 4 letters + 4 numbers = 8 characters total (with no prefix).

We took extra time on this topic to ensure that the best possible recommendation was made because we know there is no perfect answer. The recommendation reflects a balance between usability, security, administration, and auditability. We have received feedback both for and against Option 1, as well as Option 2.

There are pros, cons, and risks associated with our recommendation, which are detailed in the attached document. However, the team feels the risks with Option 1 are manageable and the pros significantly outweigh the cons. While the increased usability factors obtained with Option 2 were very appealing, with this option, the IAM Service would also have significantly increased support risks.

In the attached document, you will find a detailed narrative of the process followed to develop the recommendation. The pros, cons, and risks for each username option and convention are explored.

The IAM team kindly asks that you review the documentation and let us know if you are aware of any absolute show-stoppers that would prevent us from moving forward with the Option 1 recommendation for the IAM Service Account Username Convention.

Thank you,

IAM Project Champion and team members

Next Steps

Assuming the appropriate decision makers approve the new account username convention, the IAM team can appropriately configure the IAM system with this “policy” and any other technical parameters required to support the convention. Prior to full deployment, it is important for the IAM team to do proper training with end-users regarding the new account username convention. The IAM team should help end-users understand what the change is, remind them why it is being made, and show users a clear BEFORE and AFTER illustration.

No matter how much communication and documentation is provided, expect higher than normal support demand during the initial deployment, as people get used to the new system and username convention. Be patient because the change will be more significant for end-users than for members of teams closer to the IAM project. Focus on the positive aspects of the username change and what it will empower the users to do better, faster, and easier.

Conclusion

This IAM configuration step is not easy, but it is critical. While it takes time and effort to develop the right username convention with this methodology, getting it right the first time is significantly less difficult than having to change the convention after deployment. This guide was developed to steer organizations through this process and help them come out the other side confident in the account username convention they have chosen.

SOURCES

1. “Best Practices in User ID Formation, 2012 Update - Gartner.” 28 Aug. 2012, https://www.gartner.com/doc/2138117/best-practices-user-id-formation.

2. Best Practices in User ID Formation, 2012, Ant Allan, Gartner. https://www.gartner.com/doc/2138117/best-practices-user-id-formation.

3. User Account Naming Conventions, Troy Moreland, Identity Automation. http://blog.identityautomation.com/enterprise/2013/user-account-naming-conventions.

Definitive Guide for Account Username Conventions Cheat Sheet

GUIDING PRINCIPLES

When planning a new convention for user accounts, organizations should take into account four critical drivers:

USABILITY | SECURITY | ADMINISTRATION | AUDIT

While the goal is to develop a convention that balances the four drivers, we recommend that organizations first prioritize the drivers, so that any necessary trade-offs are understood.

METHODOLOGY

STEP 1: DOCUMENT KNOWN CONSTRAINTS

Document any specific characters, formats, parameters, or styles that would create conflicts with current users, applications, systems, business processes, and/or regulatory requirements.

- Must work with all current and future target systems to the extent possible
- Must work for the IAM and target system logging/auditing mechanisms
- Must be available at the time the account is provisioned
- Must work for users with multiple affiliations
- Must work for users that move between departments and/or locations
- Must work for users associated with multiple departments and/or locations
- Must be no longer than X characters
- Must only contain alphanumeric characters
- Must not be a value used to access other systems w/o a password
- Should provide at least X number of unique combinations
- Must mitigate risk of vulgarity and other offensive values
- Must begin with an alpha character (a-z)
- Must be lowercase alpha characters
- Must never be reused by another person
- Should never change

STEP 2: DEVELOP AND ANALYZE POSSIBLE USERNAME ALGORITHMS

Algorithm General Format:

OPTION 1

- General Pros
- General Cons
- General Risks
- Convention A
- Combinations, Examples, Specifics Pros, Cons, Risks
- Convention B
- Combinations, Examples, Specifics Pros, Cons, Risks

OPTION 2

- General Pros
- General Cons
- General Risks
- Convention A
- Combinations, Examples, Specifics Pros, Cons, Risks
- Convention B
- Combinations, Examples, Specifics Pros, Cons, Risks

STEP 3: REVIEW, RECOMMENDATION, AND NEXT STEPS

The final step for the IAM Champion and project team is to present a recommendation for the username convention to the appropriate decision-makers. A simple overview of the thought process, guiding principles, and recommended username convention should be provided.

About Identity Automation

Identity Automation helps organizations embrace security, increase business agility, and deliver an enhanced user experience by providing the most complete identity, access, governance, and administration platform available. We operate globally, with over 950 customers and tens of millions of identities managed across on-premises and cloud resources.

RAPIDIDENTITY™

Identity Automation's RapidIdentity is the smart choice for companies looking to replace outdated, legacy and home-grown identity tools with a proven and highly scalable modern IAM solution. RapidIdentity is available for deployment on premise or in the cloud. Deployments take weeks, rather than months or years, and RapidIdentity offers the broadest set of out-of-the-box and configurable capabilities, including:

- Identity lifecycle management at massive scale
- Single sign-on to web-apps, on-premises, and windows resources
- Remote access controls for contractors, partners, and supply chain vendors
- Self-service and delegated IAM workflows
- Integrated privileged account management
- MFA with fourteen supported authentication methods
- Certification campaigns, reporting, and analytics

IDENTITY AUTOMATION

7102 N Sam Houston Pkwy W, Ste 300
Houston, TX 77064, USA

Phone: +1 281-220-0021
Email: info@identityautomation.com
www.identityautomation.com

IDENTITY AUTOMATION™